

Differential Attacks on Lightweight Block Ciphers PRESENT, PRIDE, and RECTANGLE Revisited

Cihangir Tezcan^{1,2(✉)}, Galip Oral Okan¹, Asuman Şenol¹, Erol Doğan¹,
Furkan Yücebaş¹, and Nazife Baykal¹

¹ CYDES Laboratory, Department of Cyber Security, Informatics Institute,
Middle East Technical University, Ankara, Turkey
`cihangir@metu.edu.tr`

² Department of Mathematics, Middle East Technical University, Ankara, Turkey

Abstract. Differential distribution and linear approximation tables are the main security criteria for S-box designers. However, there are other S-box properties that, if overlooked by cryptanalysts, can result in erroneous results in theoretical attacks. In this paper we focus on two such properties, namely undisturbed bits and differential factors. We go on to identify several inconsistencies in published attacks against the lightweight block ciphers PRESENT, PRIDE, and RECTANGLE and present our corrections.

Keywords: Block cipher · Lightweight · Differential attack · Differential factor · Undisturbed bit

1 Introduction

Confusion layer of symmetric cryptography algorithms mostly consists of substitution boxes (S-boxes) and in order to provide better security against known attacks, S-boxes are selected depending on their cryptographic properties. Low non-linear and differential uniformity [16] provide resistance against linear [15] and differential cryptanalysis [3], respectively and most of the time these are the only properties designers focus on. However, it has been shown that high algebraic degrees and branch numbers make the cipher more resistant against algebraic [7] and cube [9] attacks. Moreover, lack of undisturbed bits [22] provides resistance against truncated [12], impossible [2], and improbable [21] differential cryptanalysis. It was shown in [14] that undisturbed bits are actually linear structures in coordinate functions. Therefore, linear structures should be avoided to be more secure against these kinds of attacks. Resistance against side-channel attacks like differential power analysis [13] can be obtained depending on the number of shares [4] in threshold implementations. Implementation invariant resistance against these attacks can be obtained by using S-boxes with a low transparency order [17], but this alone is not sufficient to ensure a satisfactory

level of security [6]. Finally, it was shown in [24] that S-boxes may have properties called differential factors which partition the key space into two or more disjoint sets that are indistinguishable by differential cryptanalytic techniques.

In this work, we focus on undisturbed bits and differential factors which appear mostly in lightweight ciphers since they generally use small S-boxes. These properties are sometimes overlooked by attackers and designers alike. We analyzed the differential attacks in the literature on lightweight ciphers and we show that the differential attacks on PRESENT, PRIDE, and RECTANGLE require some correction. We first show that the 16-round differential attack of [25] on PRESENT needs to guess 8 more bits of the key to work due to the undisturbed bits. Secondly, we show that the 18-round differential attack of [29] and 19-round differential attack of [26] on PRIDE cannot capture 6 and 4 bits of the key, respectively due to differential factors. Thus, the true time complexities of the exhaustive searches performed at the end of these attacks are greater by a factor of 2^6 and 2^4 compared to the claimed values. Finally, we show that the time complexity of the 19-round related-key differential attack of [19] on the initial version of RECTANGLE can be reduced by a factor of $2^{1.07}$ with the help of two differential factors.

2 Preliminaries

2.1 PRESENT

PRESENT [5] is a 31-round SPN (Substitution Permutation Network) type block cipher with block size of 64 bits that supports 80 and 128-bit secret keys. It has been internationally standardized by ISO/IEC 29192-2:2012 [10] as a lightweight block cipher. The round function of PRESENT, which is depicted in Fig. 1, is the same for both versions of PRESENT and consists of standard operations such as subkey XOR, substitution and permutation. At the beginning of each round, the 64-bit input of the round function is XORed with the subkey. Immediately after the subkey XOR, 16 identical 4×4 S-boxes are used in parallel as a non-linear substitution layer and finally a permutation is performed so as to provide diffusion.

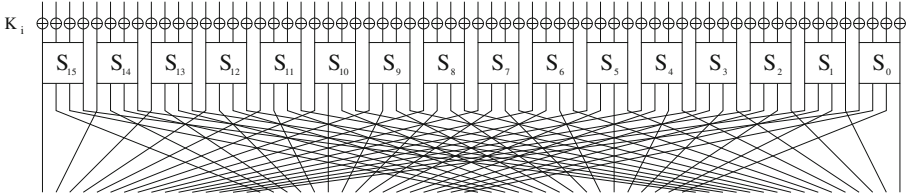


Fig. 1. Round function of PRESENT

2.2 PRIDE

PRIDE [1] is a 20-round SPN type block cipher with a block size of 64 bits and 128-bit secret key. It uses the FX construction [11], where the first half of the secret key is used for pre-whitening and post-whitening. The latter half is used to generate round keys. The overall structure is shown in Fig. 2.

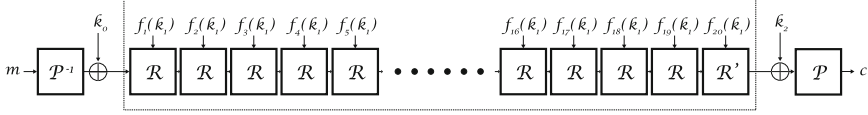


Fig. 2. Overall structure of PRIDE

The first 19 rounds use the same round function \mathcal{R} , composed of successive key addition, substitution and linear layers. The substitution layer features 16 identical 4×4 S-boxes in parallel. PRIDE's linear layer is made up of three sublayers, and has been specially designed to run efficiently in software implementations on 8-bit micro-controllers. The last round function \mathcal{R}' omits the linear layer. The round functions are shown in Fig. 3.

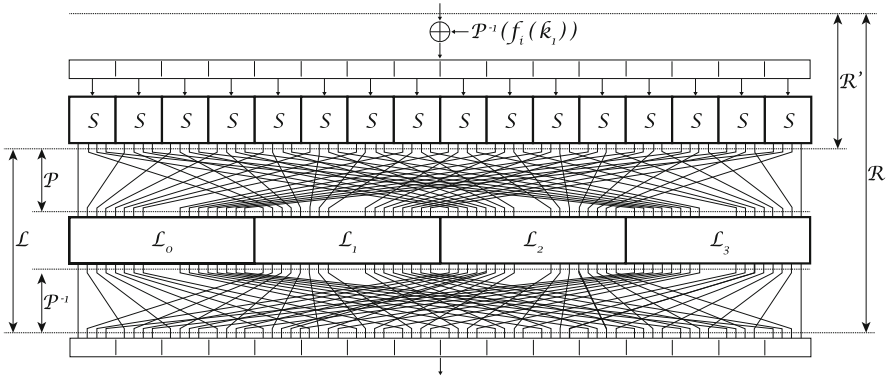


Fig. 3. Round function of PRIDE

In order to be consistent with the previous attacks on PRIDE, we use the notation that is presented in Table 1.

Table 1. PRIDE notation conventions

I_r	The input of the r -th round
X_r	The state after the key addition layer of the r -th round
Y_r	The state after the substitution layer of the r -th round
Z_r	The state after the permutation layer of the r -th round
W_r	The state after the matrix layer of the r -th round
O_r	The output of the r -th round
ΔX	The XOR difference of X and X'

2.3 RECTANGLE

RECTANGLE [28] is a lightweight block cipher with an SPN structure. This algorithm allows lightweight and fast implementations using bit-slice techniques. Its block length is 64 bits and its key length can be 80 bits or 128 bits. The substitution layer consists of 16 identical 4×4 S-boxes applied in parallel. This S-box can be implemented with only 12 basic logical instructions. The permutation layer contains only 3 rotations. 64-bit intermediate values of the cipher state can be showed as 4×16 rectangular array of bits

$$\begin{bmatrix} w_{15} & w_{14} & w_{13} & \dots & w_0 \\ w_{31} & w_{30} & w_{29} & \dots & w_{16} \\ w_{47} & w_{46} & w_{45} & \dots & w_{32} \\ w_{63} & w_{62} & w_{61} & \dots & w_{48} \end{bmatrix}$$

RECTANGLE has 25 rounds. Each round is composed of three steps: AddRoundkey, SubColumn and ShiftRow. In the AddRoundkey step, the cipher state is XORed with the rightmost 64 bits of the round subkey. In the SubColumn step, the S-box is applied to each column of the cipher state in parallel. In the ShiftRow step, the last three rows are left rotated 1, 12, and 13 bits, respectively. After 25 rounds of iterations, there is a final subkey XOR.

The key schedule of RECTANGLE is composed of three steps. The S-box is the same as in a round transformation. The key arranged as a 5×16 array of bits like in figure:

$$\begin{bmatrix} k_{0,15} & k_{0,14} & k_{0,13} & \dots & k_{0,0} \\ k_{1,15} & k_{1,14} & k_{1,13} & \dots & k_{1,0} \\ k_{2,15} & k_{2,14} & k_{2,13} & \dots & k_{2,0} \\ k_{3,15} & k_{3,14} & k_{3,13} & \dots & k_{3,0} \\ k_{4,15} & k_{4,14} & k_{4,13} & \dots & k_{4,0} \end{bmatrix}$$

The 64-bit round subkey is composed of the first 4 rows of the current contents of the key. After this step, the key is updated as follows:

1. Applying S-box to the bits at the 4 uppermost and the 4 rightmost columns
2. Applying a 1-round generalized Feistel transformation
3. XORing a 5-bit round constant with the 5-bit key state

Finally K_{25} is extracted from the updated key state. The round constants are generated by a 5-bit LFSR.

The initial design of RECTANGLE, which is now referred to as REC-0, has a different key schedule and uses the inverse of RECTANGLE's S-box.

2.4 Differential Factors

Definition 1 ([24]). *Let S be a function from \mathbb{F}_2^n to \mathbb{F}_2^m . For all $x, y \in \mathbb{F}_2^n$ that satisfy $S(x) \oplus S(y) = \mu$, if we also have $S(x \oplus \lambda) \oplus S(y \oplus \lambda) = \mu$, then we say that the S-box has a differential factor λ for the output difference μ . (i.e. μ remains invariant for λ).*

Theorem 1 ([24]). *If a bijective S-box S has a differential factor λ for an output difference μ , then S^{-1} has a differential factor μ for the output difference λ .*

Before showing the effect of differential factors on differential attacks, we recall the definition of advantage.

Definition 2 ([18]). *If an attack on an m -bit key gets the correct value ranked among the top r out of 2^m possible candidates, we say the attack obtained an $(m - \log(r))$ -bit advantage over exhaustive search.*

Theorem 2 ([24]). *In a block cipher let an S-box S contain a differential factor λ for an output difference μ and the partial round key k is XORed with the input of S . If an input pair provides the output difference μ under a partial subkey k' , then the same output difference is observed under the partial subkey $k' \oplus \lambda$. Therefore, during a differential attack involving the guess of a partial subkey corresponding to the output difference μ , the advantage of the cryptanalyst is reduced by 1 bit and the time complexity of this key guess step is halved.*

Differential factors of PRESENT, PRIDE and RECTANGLE's S-boxes are provided in Table 2.

2.5 Undisturbed Bits

Definition 3 ([22]). *For a specific input difference of an S-box, if some bits of the output difference remain invariant, then we call such bits undisturbed.*

Undisturbed bits of PRESENT, PRIDE and RECTANGLE's S-boxes are provided in Table 3.

Table 2. Differential factors of PRESENT, PRIDE and RECTANGLE’s S-boxes

S-box	0123456789ABCDEF	λ	μ
PRESENT	C56B90AD3EF84712	1	5
PRESENT	C56B90AD3EF84712	F	F
PRIDE	048F15E927ACBD63	1	1
PRIDE	048F15E927ACBD63	8	8
RECTANGLE	65CA1E79B03D8F42	2	4
RECTANGLE	65CA1E79B03D8F42	E	C

Table 3. Undisturbed bits of PRESENT, PRIDE and RECTANGLE’s S-boxes

S-box	Input diff.	Output diff.	Output diff.	Input diff.
PRESENT	1001	???0	0101	???0
PRESENT	0001	???1	0001	???1
PRESENT	1000	???1	0100	???1
PRIDE	0001	01??	0001	01??
PRIDE	0010	1???	0010	1???
PRIDE	0011	1???	0011	1???
PRIDE	1000	?0??	1000	?0??
PRIDE	1001	?1??	1001	?1??
RECTANGLE	0001	??1?	0010	?11?
RECTANGLE	0100	??11	0100	?1??
RECTANGLE	0101	??0?	0110	?0??
RECTANGLE	1000	???1	1100	???1
RECTANGLE	1100	???0	1110	???0

3 Differential Attacks on Lightweight Block Ciphers

3.1 Differential Attacks on PRESENT

Resistance of PRESENT against differential cryptanalysis is provided by the designers [5] in terms of active S-boxes. The best known differential attack on PRESENT is provided in [25] by adding two rounds to the bottom of the 24 different 14-round differentials which has different input and same output difference. Recently, it was shown in [23] that this attack overlooks 6 differential factors and therefore the number of bits that are actually captured is 6 fewer than what is claimed. In this work we give another correction to this attack due to undisturbed bits.

16-Round Differential Attack. The 16-round differential attack of [25] adds two rounds to the bottom of the 24 different 14-round differentials which has

different input and same output difference. These differentials hold with probability $p = 2^{-62}$ and Δ_1 is an example for these differentials

$$\Delta_1 : 07000000000000700 \rightarrow_{14r} 0000000900000009$$

The output difference of the characteristics activates the S-boxes S_0 and S_8 in the round 15 and $S_4, S_6, S_8, S_{10}, S_{12}$, and S_{14} in the round 16 which is shown in Table 4. Thus, this differential attack captures 32 bits of the key with a time complexity of $2^{33.18}$ 2-round PRESENT encryptions, a data complexity of 2^{64} chosen plaintexts, and a memory complexity of 2^{32} 6-bit counters. This part of the attack works with a success probability of 99.9999939% and then the remaining 48 bits are obtained via exhaustive search which requires 2^{48} 16-round PRESENT encryptions.

Table 4. 16-round differential attack of [25]. Values that need to be obtained are shown in bold.

Rounds	x_{15}	x_{14}	x_{13}	x_{12}	x_{11}	x_{10}	x_9	x_8	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0
<i>Differences in Bits</i>																
$X_{1,I}$	0000	0111	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0111	0000	0000
<i>14-Round Differential Δ_1</i>																
$X_{14,P}$	0000	0000	0000	0000	0000	0000	0000	1001	0000	0000	0000	0000	0000	0000	0000	1001
$X_{15,S}$	0000	0000	0000	0000	0000	0000	0000	???0	0000	0000	0000	0000	0000	0000	0000	???0
$X_{15,P}$	0000	000?	0000	000?	0000	000?	0000	000?	0000	000?	0000	000?	0000	0000	0000	0000
$X_{16,S}$	0000	????	0000	????	0000	????	0000	????	0000	????	0000	????	0000	0000	0000	0000

However, the activated S-boxes of the round 16 have the input difference 1 and inverse of PRESENT's S-box has a differential factor $\lambda = 5$ for $\mu = 1$. Thus, $\mu = 1$ coincides with the input difference of these six S-boxes and it was shown in [23] that the advantage of this attack is actually 26 bits instead of 32 bits. This theoretical result is also experimentally verified by removing the first few rounds of the 14-round differential so that it remains within our computational power.

This observation reduces the time complexity of the first part of the attack to $2^{27.18}$ 2-round PRESENT encryptions and the memory complexity to 2^{26} 6-bit counters. However, the time complexity of exhaustive search for the remaining bits of the key is 2^{54} 16-round PRESENT encryptions, instead of 2^{48} as it was claimed.

We further give a correction to this attack due to the undisturbed bits. Since the input difference 9 for the S-box only activates the most significant three bits, it was assumed that we need to capture the values of three S-boxes in the 16-th round. However, we cannot verify the characteristic without knowing the all four bits of the S-box output in the 15-th round. We provided the parts that need to be obtained in bold in Table 4. Thus, the attacker also needs to guess the 16-th round subkeys corresponding to S_0 and S_2 . But the attackers advantage increases by 6 instead of 8 bits due to the following property.

Property 1. Inverse of PRESENT's S-box S has the property $lsb(S^{-1}(x)) = lsb(S^{-1}(x \oplus 5))$ where lsb is the least significant bit.

Thus, a correct differential attack on 16-round PRESENT needs to guess 32 key bits in the 16-th round that correspond to the nibbles $x_0, x_2, x_4, x_6, x_8, x_{10}, x_{12}, x_{14}$ and 8 key bits in the 15-th round. However, this attack provides 32-bit advantage to the attacker instead of 40 bits because of the 6 differential factors corresponding to the nibbles $x_4, x_6, x_8, x_{10}, x_{12}, x_{14}$ and the application of Property 1 to the nibbles x_0 and x_2 . Thus, the whole 80-bit key can be obtained after an exhaustive search that requires 2^{48} 16-round PRESENT encryptions.

3.2 Differential Attacks on PRIDE

18-Round Differential Attack. An 18-round differential attack on PRIDE is provided in [29] by adding one round to the top and two rounds to the bottom of a 15-round characteristic. This attack is summarized in Table 5.

Since this attack activates 16 S-boxes, authors try to capture corresponding 64-bit round keys which require 2^{66} 18-round PRIDE encryptions and recover the remaining 64 bits via exhaustive search with time complexity of 2^{64} 18-round PRIDE encryptions. However, this attack overlooks both the differential factors and undisturbed bits of PRIDE which can be used to reduce the time complexity of first part of the attack. On the other, the 6 differential factors that are shown in Table 5 prevent the attacker from capturing 6 bits of the key. Hence the exhaustive search at the end of the attack requires 2^{70} 18-round PRIDE encryptions instead of 2^{64} . Thus, the correct time complexity of this attack is 2^{70} 18-round PRIDE encryptions, not 2^{66} .

Table 5. 18-round differential attack of [29]. Differences $\mu = 8$ which have differential factors $\lambda = 8$ are shown in bold.

Rounds	x_{15}	x_{14}	x_{13}	x_{12}	x_{11}	x_{10}	x_9	x_8	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0
<i>Differences in Bits</i>																
ΔI_1	0000	0000	0000	0000	0000	????	0000	0000	0000	????	0000	0000	0000	????	0000	0000
ΔX_1	0000	0000	0000	0000	0000	????	0000	0000	0000	????	0000	0000	0000	????	0000	0000
ΔY_1	0000	0000	0000	0000	0000	1000	0000	0000	0000	1000	0000	0000	0000	1000	0000	0000
ΔZ_1	0000	0100	0100	0100	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔW_1	0100	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔI_2	0000	1000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
<i>15-Round Differential</i>																
ΔX_{17}	0000	0000	0000	0000	0000	1000	0000	0000	0000	1000	0000	0000	0000	1000	0000	0000
ΔY_{17}	0000	0000	0000	0000	0000	????	0000	0000	0000	????	0000	0000	0000	????	0000	0000
ΔZ_{17}	0000	0700	0700	0700	0000	0700	0700	0700	0000	0700	0700	0700	0000	0700	0700	0700
ΔW_{17}	0700	0700	0700	0700	0070	??70	0770	0770	??70	??70	0070	0770	0700	0700	0700	0700
ΔI_{18}	0070	70??	0770	0000	0700	??0?	0770	0000	0000	????	07??	0000	0000	????	0700	0000
ΔX_{18}	0070	70??	0770	0000	0700	??0?	0770	0000	0000	????	07??	0000	0000	????	0700	0000
ΔY_{18}	????	????	????	0000	????	????	????	0000	0000	????	????	0000	0000	????	????	0000
ΔO_{18}	????	????	????	0000	????	????	????	0000	0000	????	????	0000	0000	????	????	0000

19-Round Differential Attack. The 18-round attack of [29] neglects the undisturbed bits in PRIDE. This observation has been noted in [26], and the attack has been improved to cover 19 rounds. However, this attack also fails to recognize the implications of the differential factors present in PRIDE’s S-box.

The attack leverages the fact that an input difference of 8 yields an S-box output difference of 8 with statistically significant probability in order to identify 109 1-round characteristics that are used to construct 15-round iterative characteristics. Coincidentally, 8 happens to be a differential factor. The only difference amongst the various characteristics is which of the two nibbles holds a value of 8. It follows that the published attack fails to recover 4 bits of the key: two in the second round and another two in the penultimate round. These corrections increase the overall time complexity from 2^{63} to 2^{64} 19-round PRIDE encryptions (Table 6).

Table 6. 19-round differential attack of [26]. Differences $\mu = 8$ which have differential factors $\lambda = 8$ are shown in bold.

Rounds	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}
<i>Differences in Bits</i>																
ΔI_1	????	????	????	0000	????	0000	????	0000	????	????	0000	0000	????	????	0000	0000
ΔX_1	????	????	????	0000	????	0000	????	0000	????	????	0000	0000	????	????	0000	0000
ΔY_1	?00?	00?0	00?0	0000	?00?	0000	00?0	0000	?0??	00?0	0000	0000	?00?	00?0	0000	0000
ΔZ_1	?000	?000	?000	?000	0000	0000	0000	0000	0??0	00?0	??00	0?00	?000	?000	?000	?000
ΔW_1	0000	?000	?000	0000	0000	0000	0000	0000	0000	?000	?000	0000	0000	?000	?000	0000
ΔI_2	0000	0000	0000	0000	?0??	0000	0000	0000	?0??	0000	0000	0000	0000	0000	0000	0000
ΔX_2	0000	0000	0000	0000	?0??	0000	0000	0000	?0??	0000	0000	0000	0000	0000	0000	0000
ΔY_2	0000	0000	0000	0000	1000	0000	0000	0000	1000	0000	0000	0000	0000	0000	0000	0000
ΔZ_2	0000	1000	1000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔW_2	0000	1000	1000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔI_3	0000	0000	0000	0000	1000	0000	0000	0000	1000	0000	0000	0000	0000	0000	0000	0000
<i>15-Round Differential</i>																
ΔX_{18}	0000	0000	0000	0000	1000	0000	0000	0000	1000	0000	0000	0000	0000	0000	0000	0000
ΔY_{18}	0000	0000	0000	0000	?0??	0000	0000	0000	?0??	0000	0000	0000	0000	0000	0000	0000
ΔZ_{18}	0000	?000	?000	0000	0000	0000	0000	0000	0000	?000	?000	0000	0000	?000	?000	0000
ΔW_{18}	?000	?000	?000	?000	0000	0000	0000	0000	??00	000?	??00	0000	?000	?000	?000	?000
ΔI_{19}	?0??	00?0	0000	0000	?00?	0000	0000	00?0	?0??	00?0	0000	0000	?00?	0000	0000	0000
ΔX_{19}	?0??	00?0	0000	0000	?00?	0000	0000	00?0	?0??	00?0	0000	0000	?00?	0000	0000	0000
ΔY_{19}	????	????	0000	0000	????	0000	0000	????	????	????	0000	0000	????	0000	0000	0000
ΔO_{19}	????	????	0000	0000	????	0000	0000	????	????	????	0000	0000	????	0000	0000	0000

20-Round Related-Key Differential Attack. 20-round related-key differential attacks that break the full PRIDE are provided in [8]. One of the attacks tries to capture 68 bits of the key by using an 18-round path and performs 2^{60} encryptions to capture the remaining bits. Due to a single differential factor, this attack’s actual time complexity is 2^{61} . Another attack of [8] tries to capture 80 bits of the key by using a 17-round path and performs 2^{48} encryptions to capture the remaining bits. This time there are four differential factors and the

Table 7. One of the 20-round differential attacks of [8]. Differences $\mu = 8$ which have differential factors $\lambda = 8$ are shown in bold.

Rounds	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}
<i>Differences in Bits</i>																
ΔI_1	????	0000	0000	0000	????	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔX_1	????	0000	0000	0000	????	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔY_1	1000	0000	0000	0000	1000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔZ_1	1000	1000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔW_1	1000	1000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔI_1	1000	0000	0000	0000	1000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔI_{19}	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔX_{19}	1000	0000	0000	0000	1000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔY_{19}	????	0000	0000	0000	????	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
ΔZ_{19}	?000	?000	0000	0000	?000	?000	0000	0000	?000	?000	0000	0000	?000	?000	0000	0000
ΔW_{19}	?000	?000	?000	?000	?00?	?00?	?000	?000	?00?	?00?	?000	?000	?000	?000	?000	?000
ΔI_{20}	????	0000	0000	0?00	????	0000	0000	0?00	????	0000	0000	0000	????	0000	0000	0000
ΔX_{20}	????	0000	0000	0?00	????	0000	0000	0?00	????	0000	0000	0000	????	0000	0000	0000
ΔY_{20}	????	0000	0000	????	????	0000	0000	????	????	0000	0000	0000	????	0000	0000	0000
$\oplus \Delta k_0$????	0000	0000	????	????	0000	0000	????	????	0000	0000	0000	????	0000	0000	0000
ΔC	?00?	?00?	?000	?000	?00?	?00?	?000	?000	?00?	?00?	?000	?000	?00?	?00?	?000	?000

exhaustive search at the end of the attack should be 2^{52} encryptions instead of 2^{48} . This attack is summarized in Table 7. Moreover, like the 18-round attack of [29], these attacks neglect the undisturbed bits of PRIDE’s S-box that are provided in Table 3 and therefore an improvement can be made as in the case of 19-round attack of [26]. However, since “PRIDE does not claim any resistance against related-key attacks” [1], these 20-round related-key attacks do not violate the security claims of the designers.

3.3 Differential Attacks on RECTANGLE

A 19-round related-key differential attack on the initial version of RECTANGLE, which is now referred to as REC-0, is presented in [19] (also published in Chinese [20]). Due to this attack and the software performance, the designers revised the key schedule.

19-Round Related-Key Differential Attack. In order to obtain related-key differential characteristics, differences of the 2nd round and the 16th round subkeys ΔK_2 and ΔK_{16} are fixed in [19]. Then the input and output differences ΔI_2 and ΔO_{18} are fixed as in Table 8 and 1254 characteristics with a total probability of $2^{60.5}$ is obtained with MILP based methods. 19 rounds are attacked by adding two rounds to the top and the bottom of these characteristics and the attack is summarized in Table 8.

The attack of [19] collects data using 2^x structures having the difference ΔI_0 and it is expected that $2^{x+34.54}$ pairs satisfy ΔO_{18} . The key guess part of the attack consists of 4 steps which are partial encryption of the 1st round, partial

Table 8. 19-round differential attack of REC-0. Output differences $\mu = 4$ that have differential factors $\lambda = 2$, and input differences $\mu = 2$ that have differential factors $\lambda = 4$ are shown in bold.

Rounds	x_{15}	x_{14}	x_{13}	x_{12}	x_{11}	x_{10}	x_9	x_8	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0
<i>Differences in Bits</i>																
ΔI_0	0000	????	????	????	0000	????	????	????	????	????	0000	0000	????	0000	0000	0000
ΔO_0	0000	0?00	??00	?000	0000	000?	001?	0?10	0?00	?000	0000	0000	0000	0000	0000	0000
ΔI_1	0000	0000	0000	0000	0000	??1?	????	0000	0000	0000	0000	0000	??0?	0000	0000	0000
ΔO_1	0000	0000	0000	0000	0000	0001	0010	0000	0000	0000	0000	0000	0101	0000	0000	0000
<i>15-Round Differential Δ_1</i>																
ΔI_{17}	0000	0000	0000	0000	0000	0000	0001	0000	0000	0000	0000	0000	0000	0000	0000	0100
ΔO_{17}	0000	0000	0000	0000	0000	0000	????	0000	0000	0000	0000	0000	0000	0000	0000	?1??
ΔI_{18}	0000	0000	?000	0100	0100	00?0	00*?	0000	000*	?000	0?00	0000	0000	0000	00?0	000?
ΔO_{18}	0000	0000	????	?1??	?1??	????	????	0000	????	????	????	0000	0000	0000	????	????

encryption of the 2nd round, partial decryption of the 18th round, and partial decryption of the 17th round. These steps have approximate time complexities of $2^{x+40.54}$, $2^{x+39.54}$, $2^{x+38.54}$, and $2^{x+28.54}$ 19-round REC-0 encryptions, respectively.

Since REC-0 uses the inverse S-box of RECTANGLE, it has a differential $\lambda = 4$ for $\mu = 2$ by Theorem 1. Since these differential factors are two rounds away from the characteristic, Theorem 2 do not apply. However, we can still use the differential factors of the round 1 to reduce the time complexity of the attack due to the following property.

Property 2. The differential factor $\lambda = 4$ for $\mu = 2$ flips the value of the bit that corresponds to $\mu = 2$. Namely, the second bits from the right of $S(x)$ and $S(y \oplus 4)$ are the same (similarly for $S(y)$ and $S(x \oplus 4)$).

Property 2 allows us to guess only half of the keys that correspond to the two S-boxes x_{14} and x_7 in the first round. Therefore, if we start guessing keys from these two S-boxes, we reduce the time complexity of the first step of the attack of [19] by a factor of 2^2 . However, since the differential factors flips the values of the bits according to Property 2, we need to also try the complements of the two key bits $K_0^{(3,10)} = K_1^{(3,3)}$ and $K_0^{(0,16)} = K_1^{(0,3)}$ in step 2 to avoid missing the correct key. We do not make any changes on the steps 3 and 4 of the attack because the inverse of Rec-0 does not have property like Property 2. Thus, the differential factors at round 18 do not have any effect on the attack. Steps of our modified attack have time complexities of $2^{x+38.29}$, $2^{x+39.29}$, $2^{x+38.55}$, and $2^{x+28.54}$ 19-round encryptions, respectively. If we choose $x = 26$ as in [19], we get a time complexity of $2^{66.35}$ 19-round encryptions compared to $2^{67.42}$ of the original attack. Details of our modified attack is provided in Appendix A.

Table 9. 14-round difference propagation of [27]. Output differences which have differential factors are shown in bold, which are $\mu = 2$ for the S-box and $\mu = 4$ for its inverse.

Input difference of round 0	Output difference of round 13
0000000000000000	0000000000000000
0010000100000000	0000000000000010
0000000100000000	0001000000000000
0000000000000000	0000000000000000

18-Round Differential Attack. Revising the key schedule of REC-0 made RECTANGLE more secure against related-key attacks and the above 19-round related-key differential attack is not applicable to RECTANGLE. In the single-key scenario, designers provided in [27] a 14-round difference propagation with probability $2^{-62.83}$ and it is presented in Table 9. Designers claim that they can mount an attack on 18-round RECTANGLE using this 14-round characteristic without giving the exact details of this attack. This is the highest number of rounds the designers can break.

Since RECTANGLE replaced the S-box of REC-0 with its inverse, the 14-round characteristic contains two differential factors as shown in Table 9. Therefore attacks on RECTANGLE using this or similar characteristics should consider the effects of differential factors. The time complexity of the 18-round attack is given as $2^{78.67}$ 18-round encryptions for an 80-bit seed key and $2^{126.66}$ 18-round encryptions for a 128-bit seed key. However, these complexities can be marginally larger in practice due to these two differential factors.

4 Conclusion

In this work, we have shown that there exist properties of S-boxes other than difference distribution and linear approximation that are fundamental to the security of lightweight block ciphers. In general, verifying theoretical attacks experimentally is infeasible due to the time, data, and memory complexity involved. Nevertheless, we were able to verify the theoretical results we have put forward through a series of experiments using reduced versions of the attacks in question. We believe that cryptanalysis would benefit from the practice of verifying theoretical results by experimenting on the reduced versions.

Acknowledgment. The work of Cihangir Tezcan was supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) under the grant 115E447 titled “Quasi-Differential Factors and Time Complexity of Block Cipher Attacks”.

A Modified 19-Round Related-Key Attack on REC-0

Step 1: Guess the value of a part of subkey bits of K_0 .

1. Guess $K_0^{(14)}$ and compute the output difference of the 14rd S-box for each remaining plaintext pair; i.e. $S(P^{(14)} \oplus K_0^{(14)}) \oplus S(P'^{(14)} \oplus K_0^{(14)} \oplus \Delta K_0^{(14)})$. This step has time complexity $2 \cdot 2^{x+34.54} \cdot 2^3 \cdot \frac{1}{16} \cdot \frac{1}{19} = 2^{x+30.29}$. If the difference does not have the form ?000, discard the pair. Then the number of expected remaining pairs is $2^{x+28.54}$.
2. Guess $K_0^{(7)}$ and compute the output difference of the 7th S-box for each remaining plaintext pair; i.e. $S(P^{(7)} \oplus K_0^{(7)}) \oplus S(P'^{(7)} \oplus K_0^{(7)} \oplus \Delta K_0^{(7)})$. This step has time complexity $2 \cdot 2^{x+31.54} \cdot 2^6 \cdot \frac{1}{16} \cdot \frac{1}{19} = 2^{x+30.29}$. If the difference does not have the form ?000, discard the pair. Then the number of expected remaining pairs is $2^{x+28.54}$.
3. Repeatedly guess $K_0^{(3)}$, $K_0^{(6)}$, $K_0^{(8)}$, $K_0^{(9)}$, $K_0^{(10)}$, $K_0^{(12)}$, $K_0^{(13)}$. There are $2^{x+8.54}$ right pairs left. This step has time complexity $2 \cdot (2^{x+38.54} \cdot 2^{x+39.54} \cdot 2^{x+40.54} \cdot 2^{x+41.54} \cdot 2^{x+42.54} \cdot 2^{x+43.54} \cdot 2^{x+44.54}) \cdot \frac{1}{16} \cdot \frac{1}{19} = 2^{x+38.29}$.

Step 2: Guess the value of a part of subkey bits of K_0 by guessing some bits of K_0 and K_1 .

1. Since many bits of K_1 are obtained from K_0 directly by shifting and adding constant, we only need to guess some bits for a column in K_1 . For the 3rd column of K_1 , by the key schedule we have $(K_1^{(0,3)}, K_1^{(1,3)}, K_1^{(2,3)}, K_1^{(3,3)}) = (K_0^{(0,16)}, K_0^{(1,14)}, K_0^{(2,12)}, K_0^{(3,10)})$. Therefore, we need to guess $K_0^{(0,16)} = K_1^{(0,3)}$ and we also need $K_0^{(3,10)} = K_1^{(3,3)}$ because $K_1^{(3,3)}$ was flipped when we apply Substitution operation to $K_1^{(2,7)}$, $K_1^{(3,10)}$ are flipped when we apply Substitution operation to $K_1^{(2,15)}$ because of Property 2. Then the number of expected remaining pairs is $2^{x+4.54}$.
2. Guess the bits $K_0^{(1,1)}$, $K_0^{(2,19)}$, $K_0^{(3,17)}$, and then check up whether $S(I_1^{(10)} \oplus K_1^{(10)}) \oplus S(I'^{(10)} \oplus K_1^{(10)} \oplus \Delta K_1^{(10)}) = 1000$. On average, there are $2^{x+0.54}$ right pairs left.
3. Similarly, as the previous step, guess the bits $K_0^{(0,2)}$, $K_1^{(1,9)}$, $K_0^{(2,18)}$, $K_0^{(3,16)}$, then there are $2^{x-3.46}$ right pairs left on average.

In step 2, time complexity is $2 \cdot (2^{x+45.54} \cdot 2^{x+44.54} \cdot 2^{x+44.54}) \cdot \frac{1}{16} \cdot \frac{1}{19} = 2^{x+39.29}$.

Step 3: Guess the value of a part of subkey bits of K_{19} . This step is identical to the Step 3 of [19] and has a time complexity of $2^{38.55}$.

Step 4: The involved secret bits of K_{18} have guessed in Step 1–3, and we do not need to guess any other secret bits. Add one to the corresponding counter, if there is a right pair left. This step is identical to the Step 3 of [19] and has a time complexity of $2^{28.54}$.

Step 5: If the counter is larger than 1, keep the guess of the subkey bits as the candidates of the right subkeys. For each survived candidate, compute the seed key by doing an exhaustive search for other secret bits.

Therefore, the total time complexity is $2^{66.35}$ 19-round REC-0 encryptions, data complexity is 2^{62} chosen plaintexts since $x = 26$, and the memory complexity is 2^{72} key counters.

References

1. Albrecht, M.R., Driessen, B., Kavun, E.B., Leander, G., Paar, C., Yalçın, T.: Block ciphers – focus on the linear layer (feat. PRIDE). In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 57–76. Springer, Heidelberg (2014). doi:[10.1007/978-3-662-44371-2_4](https://doi.org/10.1007/978-3-662-44371-2_4)
2. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. *J. Cryptol.* **18**(4), 291–311 (2005)
3. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. *J. Cryptol.* **4**(1), 3–72 (1991)
4. Bilgin, B., Nikova, S., Nikov, V., Rijmen, V., Stütz, G.: Threshold implementations of all 3×3 and 4×4 S-boxes. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 76–91. Springer, Heidelberg (2012). doi:[10.1007/978-3-642-33027-8_5](https://doi.org/10.1007/978-3-642-33027-8_5)
5. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsøe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhe, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007). doi:[10.1007/978-3-540-74735-2_31](https://doi.org/10.1007/978-3-540-74735-2_31)
6. Chakraborty, K., Sarkar, S., Maitra, S., Mazumdar, B., Mukhopadhyay, D., Prouff, E.: Redefining the transparency order. *Cryptology ePrint Archive*, Report 2014/367 (2014)
7. Courtois, N.T., Pieprzyk, J.: Cryptanalysis of Block ciphers with overdefined systems of equations. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 267–287. Springer, Heidelberg (2002). doi:[10.1007/3-540-36178-2_17](https://doi.org/10.1007/3-540-36178-2_17)
8. Dai, Y., Chen, S.: Cryptanalysis of full pride block cipher. *Cryptology ePrint Archive*, Report 2014/987 (2014). <http://eprint.iacr.org/2014/987>
9. Dinur, I., Shamir, A.: Cube attacks on tweakable black box polynomials. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 278–299. Springer, Heidelberg (2009). doi:[10.1007/978-3-642-01001-9_16](https://doi.org/10.1007/978-3-642-01001-9_16)
10. ISO/IEC 29192–2:2012: Information technology - security techniques - lightweight cryptography - part 2: Block ciphers (2011)
11. Kilian, J., Rogaway, P.: How to protect DES against exhaustive key search (an analysis of DESX). *J. Cryptol.* **14**(1), 17–35 (2001)
12. Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (1995). doi:[10.1007/3-540-60590-8_16](https://doi.org/10.1007/3-540-60590-8_16)
13. Kocher, P., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999). doi:[10.1007/3-540-48405-1_25](https://doi.org/10.1007/3-540-48405-1_25)
14. Makarim, R.H., Tezcan, C.: Relating undisturbed bits to other properties of substitution boxes. In: Eisenbarth, T., Öztürk, E. (eds.) LightSec 2014. LNCS, vol. 8898, pp. 109–125. Springer, Cham (2015). doi:[10.1007/978-3-319-16363-5_7](https://doi.org/10.1007/978-3-319-16363-5_7)

15. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseht, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994). doi:[10.1007/3-540-48285-7_33](https://doi.org/10.1007/3-540-48285-7_33)
16. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseht, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg (1994). doi:[10.1007/3-540-48285-7_6](https://doi.org/10.1007/3-540-48285-7_6)
17. Prouff, E.: DPA attacks and S-boxes. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 424–441. Springer, Heidelberg (2005). doi:[10.1007/11502760_29](https://doi.org/10.1007/11502760_29)
18. Selçuk, A.A.: On probability of success in linear and differential cryptanalysis. *J. Cryptol.* **21**(1), 131–147 (2008)
19. Shan, J., Hu, L., Song, L., Sun, S., Ma, X.: Related-key differential attack on round reduced rectangle-80. Cryptology ePrint Archive, Report 2014/986 (2014). <http://eprint.iacr.org/2014/986>
20. Shan, J., Hu, L., Song, L., Sun, S., Ma, X.: Related-key differential attack on 19-round reduced rectangle-80. *J. Cryptol. Res.* **2**(1), 54 (2015). <http://www.jcr.cacrnet.org.cn:8080/mmxb/EN/abstract/abstract73.shtml>
21. Tezcan, C.: The improbable differential attack: cryptanalysis of reduced round CLEFIA. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 197–209. Springer, Heidelberg (2010). doi:[10.1007/978-3-642-17401-8_15](https://doi.org/10.1007/978-3-642-17401-8_15)
22. Tezcan, C.: Improbable differential attacks on present using undisturbed bits. *J. Comput. Appl. Math.* **259**, 503–511 (2014)
23. Tezcan, C.: Differential factors revisited: corrected attacks on PRESENT and SERPENT. In: Güneysu, T., Leander, G., Moradi, A. (eds.) LightSec 2015. LNCS, vol. 9542, pp. 21–33. Springer, Cham (2016). doi:[10.1007/978-3-319-29078-2_2](https://doi.org/10.1007/978-3-319-29078-2_2)
24. Tezcan, C., Özbudak, F.: Differential factors: improved attacks on SERPENT. In: Eisenbarth, T., Öztürk, E. (eds.) LightSec 2014. LNCS, vol. 8898, pp. 69–84. Springer, Cham (2015). doi:[10.1007/978-3-319-16363-5_5](https://doi.org/10.1007/978-3-319-16363-5_5)
25. Wang, M.: Differential cryptanalysis of reduced-round PRESENT. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 40–49. Springer, Heidelberg (2008). doi:[10.1007/978-3-540-68164-9_4](https://doi.org/10.1007/978-3-540-68164-9_4)
26. Yang, Q., Hu, L., Sun, S., Qiao, K., Song, L., Shan, J., Ma, X.: Improved differential analysis of block cipher PRIDE. In: Lopez, J., Wu, Y. (eds.) ISPEC 2015. LNCS, vol. 9065, pp. 209–219. Springer, Cham (2015). doi:[10.1007/978-3-319-17533-1_15](https://doi.org/10.1007/978-3-319-17533-1_15)
27. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I.: Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms. Cryptology ePrint Archive, Report 2014/084 (2014). <http://eprint.iacr.org/2014/084>
28. Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., Verbauwhede, I.: Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms. *Sci. China Inf. Sci.* **58**(12), 1–15 (2015)
29. Zhao, J., Wang, X., Wang, M., Dong, X.: Differential analysis on block cipher pride. Cryptology ePrint Archive, Report 2014/525 (2014). <http://eprint.iacr.org/>

Lightweight Cryptography for Security and Privacy
5th International Workshop, LightSec 2016, Aksaray,
Turkey, September 21-22, 2016, Revised Selected
Papers
Bogdanov, A. (Ed.)
2017, VII, 149 p. 34 illus., Softcover
ISBN: 978-3-319-55713-7