

# Compact Representation for Division Property

Yosuke Todo<sup>1,2(✉)</sup> and Masakatu Morii<sup>2</sup>

<sup>1</sup> NTT Secure Platform Laboratories, Tokyo, Japan

`todo.yosuke@lab.ntt.co.jp`

<sup>2</sup> Kobe University, Kobe, Japan

**Abstract.** The division property, which is a new method to find integral characteristics, was proposed at Eurocrypt 2015. Thereafter, some applications and improvements have been proposed. The bit-based division property is also one of such improvements, and the accurate integral characteristic of SIMON32 is theoretically proved. In this paper, we propose the compact representation for the bit-based division property. The disadvantage of the bit-based division property is that it cannot be applied to block ciphers whose block length is over 32 because of high time and memory complexity. The compact representation partially solves this problem, and we apply this technique to 64-bit block cipher PRESENT to illustrate our method. We can accurately evaluate the propagation characteristic of the bit-based division property thanks to the compact representation. As a result, we find 9-round integral characteristics, and the characteristic is improved by two rounds than previous best characteristic. Moreover, we attack 12-round PRESENT-80 and 13-round PRESENT-128 by using this new characteristic.

**Keywords:** Integral cryptanalysis · Division property · Compact representation · PRESENT

## 1 Introduction

The concept of an integral cryptanalysis was first introduced as the dedicated attack against block cipher SQUARE [4], and Knudsen and Wagner then formalized the dedicated attack as the integral attack [6]. The integral cryptanalysis is applied to many ciphers, and this is nowadays one of the most powerful cryptanalyses [6, 8, 16, 17]. The integral cryptanalysis mainly consists of two parts: a search for integral characteristics and key recovery. The propagation of the integral property [6] and the degree estimation<sup>1</sup> [5, 7] have been used as well-known methods to find integral characteristics.

At Eurocrypt 2015, the division property, which is a novel technique to find integral characteristics, was proposed [12]. This technique is the generalization of the integral property that can also exploit the algebraic degree at the same time. After the proposal, the new understanding of the division property and new applications have been proposed [2, 10, 11, 14, 18].

---

<sup>1</sup> This method is often called the higher-order differential attack [5, 7].

At FSE 2016, the bit-based division property, which is a new variant of the division property, was proposed [14]<sup>2</sup>. To analyze  $n$ -bit block ciphers with  $m$   $\ell$ -bit S-boxes, the conventional division property decomposes  $n$ -bit value into  $m$   $\ell$ -bit values, and the division property  $\mathcal{D}_{\mathbb{K}}^m$  is used. For convenience, we call this-type division property an integer-based division property. On the other hand, the bit-based division property decomposes  $n$ -bit value into  $n$  1-bit values, i.e.,  $\mathcal{D}_{\mathbb{K}}^{1^n}$  is used. The bit-based division property can find more accurate integral characteristics than the integer-based division property. Actually, the bit-based division property proves the 15-round integral characteristic of SIMON32, and it is tight [14].

**Our Contribution.** In this paper, we propose a *compact representation* for the bit-based division property against S-box-based ciphers. A disadvantage of the bit-based division property is that it requires about  $2^n$  time and memory complexity to evaluate  $n$ -bit block ciphers. Therefore, the application is limited to block ciphers with small block length like SIMON32 in [14]. Moreover, at CRYPTO 2016, Boura and Canteaut introduced the parity set, which is the so-called bit-based division property for an S-box [2], but the application is also limited to the low-data distinguisher for a few rounds of PRESENT [1]. The compact representation partially solves this problem, and we can get high-data distinguishers by reducing time and memory complexity. To demonstrate the advantage of the compact representation, we apply our new technique to PRESENT. As a result, we find new 9-round integral characteristics. Since the previous best characteristic is 7-round one [15], our new characteristic is improved by two rounds. Moreover, we attack 12-round PRESENT-80 and 13-round PRESENT-128 by using the new integral characteristic. Zhang et al. discussed the security of PRESENT against the integral attack in [19] and attacked 10-round PRESENT-80 and 11-round PRESENT-128 by using the match-through-the-S-box (MTTS) technique. Therefore, our new attack is also improved by two rounds.

## 2 Preliminaries

### 2.1 Notations

We make the distinction between the addition of  $\mathbb{F}_2^n$  and addition of  $\mathbb{Z}$ , and we use  $\oplus$  and  $+$  as the addition of  $\mathbb{F}_2^n$  and addition of  $\mathbb{Z}$ , respectively. For any  $a \in \mathbb{F}_2^n$ , the  $i$ th element is expressed in  $a[i]$ , and the Hamming weight  $w(a)$  is calculated as  $w(a) = \sum_{i=1}^n a[i]$ . For any  $\mathbf{a} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$ , the vectorial Hamming weight of  $\mathbf{a}$  is defined as  $W(\mathbf{a}) = (w(a_1), w(a_2), \dots, w(a_m)) \in \mathbb{Z}^m$ . Moreover, for any  $\mathbf{k} \in \mathbb{Z}^m$  and  $\mathbf{k}' \in \mathbb{Z}^m$ , we define  $\mathbf{k} \succeq \mathbf{k}'$  if  $k_i \geq k'_i$  for all  $i$  ( $1 \leq i \leq m$ ). Otherwise,  $\mathbf{k} \not\succeq \mathbf{k}'$ . Let  $\mathbb{K}$  be the set of  $\mathbf{k}$ , and  $|\mathbb{K}|$  denotes the number of elements in  $\mathbb{K}$ .

<sup>2</sup> In [14], they proposed two variants of the bit-based division property: the conventional bit-based division property and the bit-based division property using three subsets. In this paper, we focus on the conventional bit-based division property.

## 2.2 Integral Attack

The integral attack was first introduced by Daemen et al. to evaluate the security of SQUARE [4], and then it was formalized by Knudsen and Wagner [6]. Attackers first prepare  $N$  chosen plaintexts and encrypt them  $R$  rounds. If the XOR of all encrypted texts becomes 0, we say that the cipher has an  $R$ -round integral characteristic with  $N$  chosen plaintexts. Finally, we analyze the entire cipher by using the integral characteristic. There are two classical approaches to find integral characteristics. The first one is the propagation of the integral property [6] and another is based on the degree estimation [5, 7].

## 2.3 Division Property

The division property proposed in [12] is a new method to find integral characteristics. This section briefly shows the definition and propagation rules. Please refer to [12] in detail.

**Bit Product Function.** The division property of a multiset is evaluated by using the bit product function defined as follows. Let  $\pi_u : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$  be a bit product function for any  $u \in \mathbb{F}_2^n$ . Let  $x \in \mathbb{F}_2^n$  be the input and  $\pi_u(x)$  be the AND of  $x[i]$  satisfying  $u[i] = 1$ , i.e., it is defined as

$$\pi_u(x) := \prod_{i=1}^n x[i]^{u[i]}.$$

Notice that  $x[i]^1 = x[i]$  and  $x[i]^0 = 1$ . Let  $\pi_{\mathbf{u}} : (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m}) \rightarrow \mathbb{F}_2$  be a bit product function for any  $\mathbf{u} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$ . Let  $\mathbf{x} \in (\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$  be the input and  $\pi_{\mathbf{u}}(\mathbf{x})$  be defined as

$$\pi_{\mathbf{u}}(\mathbf{x}) := \prod_{i=1}^m \pi_{u_i}(x_i).$$

The bit product function also appears in the Algebraic Normal Form (ANF) of a Boolean function. The ANF of a Boolean function  $f$  is represented as

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u^f \left( \prod_{i=1}^n x[i]^{u[i]} \right) = \bigoplus_{u \in \mathbb{F}_2^n} a_u^f \pi_u(x),$$

where  $a_u^f \in \mathbb{F}_2$  is a constant value depending on  $f$  and  $u$ .

### Definition of Division Property.

**Definition 1 (Division Property [12]).** Let  $\mathbb{X}$  be a multiset whose elements take a value of  $(\mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} \times \cdots \times \mathbb{F}_2^{n_m})$ . When the multiset  $\mathbb{X}$  has the division

property  $\mathcal{D}_{\mathbb{K}}^{n_1, n_2, \dots, n_m}$ , where  $\mathbb{K}$  denotes a set of  $m$ -dimensional vectors whose  $i$ th element takes a value between 0 and  $n_i$ , it fulfills the following conditions:

$$\bigoplus_{x \in \mathbb{X}} \pi_u(x) = \begin{cases} \text{unknown} & \text{if there are } \mathbf{k} \in \mathbb{K} \text{ s.t. } W(\mathbf{u}) \succeq \mathbf{k}, \\ 0 & \text{otherwise.} \end{cases}$$

See [12] to better understand the concept in detail, and [10] and [11] help readers understand the division property. In this paper, the division property for  $(\mathbb{F}_2^n)^m$  is referred to as  $\mathcal{D}_{\mathbb{K}}^m$  for the simplicity<sup>3</sup>. If there are  $\mathbf{k} \in \mathbb{K}$  and  $\mathbf{k}' \in \mathbb{K}$  satisfying  $\mathbf{k} \succeq \mathbf{k}'$  in the division property  $\mathcal{D}_{\mathbb{K}}^{n_1, n_2, \dots, n_m}$ ,  $\mathbf{k}$  can be removed from  $\mathbb{K}$  because the vector  $\mathbf{k}$  is redundant.

Some propagation rules for the division property are proven in [12], and the rules are summarized in [11]. We omit the description of the propagation rules in this paper because it is not always necessary to understand this paper.

## 2.4 Bit-Based Division Property

The bit-based division property was introduced in [14]. They showed two bit-based division properties: the conventional bit-based division property and the bit-based division property using three subsets. In this paper, we only focus on the conventional bit-based division property. To analyze  $n$ -bit block ciphers, the conventional division property uses  $\mathcal{D}_{\mathbb{K}}^{\ell_1, \ell_2, \dots, \ell_m}$ , where  $\ell_i$  and  $m$  are chosen by attackers in the range of  $n = \sum_{i=1}^m \ell_i$ . This paper focuses on the conventional bit-based division property, i.e.,  $\mathcal{D}_{\mathbb{K}}^{1^n}$ . Note that it is not against the definition of the conventional division property.

**Propagation Characteristic for S-Box.** Let us consider the propagation characteristic of the bit-based division property for an S-box. Similar observation was shown by Boura and Canteaut in [2], and they introduced a new concept called the parity set as follows.

**Definition 2 (Parity Set).** Let  $\mathbb{X}$  be a set whose elements take a value of  $\mathbb{F}_2^n$ . Its parity set is defined as

$$\mathcal{U}(\mathbb{X}) = \left\{ u \in \mathbb{F}_2^n \mid \bigoplus_{x \in \mathbb{X}} \pi_u(x) = 1 \right\}.$$

Assuming  $\mathbb{X}$  has the division property  $\mathcal{D}_{\mathbb{K}}^n$ ,

$$\mathcal{U}(\mathbb{X}) \subseteq \{u \in \mathbb{F}_2^n : w(u) \geq k\}.$$

Let  $\mathbb{X}$  and  $S(\mathbb{X})$  denote the input set and output set of the S-box, respectively. Then, the parity set of  $S(\mathbb{X})$  fulfills

$$\mathcal{U}(S(\mathbb{X})) \subseteq \bigcup_{u \in \mathcal{U}(\mathbb{X})} V_s(u),$$

**Table 1.** Sets  $V_S(u)$  for all  $u \in \mathbb{F}_2^4$  for the PRESENT S-box. All four-bit values are represented in hexadecimal notation. The rightmost bit of the word corresponds to the least significant bit.

	$V_S(u)$															
	0x0	0x1	0x2	0x4	0x8	0x3	0x5	0x9	0x6	0xA	0xC	0x7	0xB	0xD	0xE	0xF
$u = 0x0$	x			x	x						x					
$u = 0x1$		x			x		x				x					
$u = 0x2$			x		x				x		x					
$u = 0x4$		x		x				x			x					
$u = 0x8$		x	x	x	x	x					x					
$u = 0x3$				x		x	x	x	x	x	x		x			
$u = 0x5$							x	x			x					
$u = 0x9$				x		x	x		x	x					x	
$u = 0x6$		x			x			x	x	x	x					
$u = 0xA$			x	x			x	x		x		x	x	x	x	x
$u = 0xC$			x			x		x			x					
$u = 0x7$			x		x	x		x	x				x	x		
$u = 0xB$			x	x	x	x			x	x	x	x		x		x
$u = 0xD$			x	x	x			x		x		x			x	
$u = 0xE$							x					x	x	x	x	x
$u = 0xF$																x

where

$$V_s(u) = \{v \in \mathbb{F}_2^n \mid \text{ANF of } (\pi_v \circ S) \text{ contains } \pi_u(x)\}.$$

The definition of the parity set trivially derives the following proposition.

**Proposition 1.** *Let  $\mathbb{X}$  be a multiset whose elements take a value of  $\mathbb{F}_2^n$ . When the multiset  $\mathbb{X}$  has the bit-based division property  $\mathcal{D}_{\mathbb{K}}^{1^n}$ , the parity set of  $\mathbb{X}$  fulfills*

$$\mathcal{U}(\mathbb{X}) \subseteq \{u \in \mathbb{F}_2^n : \text{there are } k \in \mathbb{K} \text{ satisfying } u \succeq k\}.$$

Moreover, assuming  $\mathcal{U}(\mathbb{X}) \subseteq \mathbb{K}'$ , the set  $\mathbb{X}$  has the bit-based division property  $\mathcal{D}_{\mathbb{K}'}^{1^n}$ .

Proposition 1 shows that the bit-based division property of  $S(\mathbb{X})$  can be evaluated from that of  $\mathbb{X}$  via the parity set.

**Case of PRESENT S-Box.** As an example, let us consider the case of the PRESENT S-box. Let  $(x_4, x_3, x_2, x_1)$  and  $(y_4, y_3, y_2, y_1)$  be the input and output

<sup>3</sup> In [12], the division property was referred to as  $\mathcal{D}_{\mathbb{K}}^{n,m}$ .

**Table 2.** Propagation of the bit-based division property for PRESENT S-box. Vectors on  $\mathbb{F}_2^4$  are represented an hexadecimal notation.

$k$ of input $\mathcal{D}_k^{1^4}$	$\mathbb{K}$ of output $\mathcal{D}_{\mathbb{K}}^{1^4}$	$k$ of input $\mathcal{D}_k^{1^4}$	$\mathbb{K}$ of output $\mathcal{D}_{\mathbb{K}}^{1^4}$
0x0	{0x0}	0x8	{0x1, 0x2, 0x4, 0x8}
0x1	{0x1, 0x2, 0x4, 0x8}	0x9	{0x2, 0x4, 0x8}
0x2	{0x1, 0x2, 0x4, 0x8}	0xA	{0x2, 0x4, 0x8}
0x3	{0x2, 0x4, 0x8}	0xB	{0x2, 0x4, 0x8}
0x4	{0x1, 0x2, 0x4, 0x8}	0xC	{0x2, 0x4, 0x8}
0x5	{0x2, 0x4, 0x8}	0xD	{0x2, 0x4, 0x8}
0x6	{0x1, 0x2, 0x8}	0xE	{0x5, 0xB, 0xE}
0x7	{0x2, 0x8}	0xF	{0xF}

of the S-box, respectively, and the algebraic normal form of the PRESENT S-box is described as

$$\begin{aligned}
y_4 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3 + x_1 + x_2 + x_4 + 1, \\
y_3 &= x_1x_2x_4 + x_1x_3x_4 + x_1x_2 + x_1x_4 + x_2x_4 + x_3 + x_4 + 1, \\
y_2 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_4 + x_3x_4 + x_2 + x_4, \\
y_1 &= x_2x_3 + x_1 + x_3 + x_4.
\end{aligned}$$

Table 1 shows sets of  $V_S(u)$  for all  $u \in \mathbb{F}_2^4$  for the PRESENT S-box. Assuming that  $\mathbb{X}$  fulfills  $\mathcal{D}_k^{1^4}$ , let  $\mathcal{D}_{\mathbb{K}'}^{1^4}$  be the bit-based division property of  $S(\mathbb{X})$  and  $\mathbb{K}'$  is

$$\mathbb{K}' = \cup_{u \in \mathcal{U}(\mathbb{X})} V_S(u), \quad \mathcal{U}(\mathbb{X}) \subseteq \{u \in \mathbb{F}_2^n : u \succeq k\}$$

from Proposition 1. We compute  $\mathbb{K}'$  for any  $k \in \mathbb{F}_2^4$  and then remove redundant vectors. Table 2 shows the propagation characteristic of the bit-based division property for the PRESENT S-box.

### 3 Compact Representation for Division Property

#### 3.1 Motivation

We can find more accurate integral characteristics by using the bit-based division property than the integer-based division property. However, this evaluation requires about  $2^n$  time and memory complexity for  $n$ -bit block ciphers. Therefore, the bit-based division property is applied to small block-length ciphers like SIMON32 in [14]. Moreover, the application of the parity set is limited to the low-data distinguisher for a few rounds of PRESENT [2]. It is an open problem to apply the bit-based division property to high-data distinguishers for non small block-length cipher.

### 3.2 General Idea

The compact representation for the bit-based division property partially solves this problem. We focus on the fact that different division properties cause the same division property through an S-box. Then, we regard the different properties as the same property, and it helps us to evaluate the propagation characteristic efficiently.

**Compact Representation for PRESENT S-box.** The focus is that there are some input division properties whose output division property is the same. For example, the output division property from  $\mathcal{D}_{\{0x1\}}^{1^4}$  is  $\mathcal{D}_{\{0x1, 0x2, 0x4, 0x8\}}^{1^4}$ , which is the same as that from  $\mathcal{D}_{\{0x2\}}^{1^4}$ . In the compact representation, we regard their input properties as the same input property. Table 3 shows the compact representation for PRESENT S-box. While sixteen values are used to represent the bit-based division property, only seven values  $\{\bar{0}, \bar{1}, \bar{3}, \bar{6}, \bar{7}, \bar{E}, \bar{F}\}$  are used in the compact representation. For simplicity, let  $\mathbb{S}_c$  be

$$\mathbb{S}_c = \{\bar{0}, \bar{1}, \bar{3}, \bar{6}, \bar{7}, \bar{E}, \bar{F}\}.$$

**Table 3.** Compact representation for PRESENT S-box.

Compact	Real property	Output property	Redundant
$\bar{0}$	$\{0x0\}$	$\{0x0\}$	$\bar{0}, \bar{1}, \bar{3}, \bar{6}, \bar{7}, \bar{E}, \bar{F}$
$\bar{1}$	$\{0x1, 0x2, 0x4, 0x8\}$	$\{0x1, 0x2, 0x4, 0x8\}$	$\bar{1}, \bar{3}, \bar{6}, \bar{7}, \bar{E}, \bar{F}$
$\bar{3}$	$\{0x3, 0x5, 0x9, 0xA, 0xB, 0xC, 0xD\}$	$\{0x2, 0x4, 0x8\}$	$\bar{3}, \bar{7}, \bar{E}, \bar{F}$
$\bar{6}$	$\{0x6\}$	$\{0x1, 0x2, 0x8\}$	$\bar{6}, \bar{7}, \bar{E}, \bar{F}$
$\bar{7}$	$\{0x7\}$	$\{0x2, 0x8\}$	$\bar{7}, \bar{F}$
$\bar{E}$	$\{0xE\}$	$\{0x5, 0xB, 0xE\}$	$\bar{E}, \bar{F}$
$\bar{F}$	$\{0xF\}$	$\{0xF\}$	$\bar{F}$

Note that we have to check the original vectors when we remove redundant vectors. Assuming that the division property is  $\mathcal{D}_{\{\bar{3}, \bar{6}, \bar{E}\}}$ , each original vectors are represented as

$$\bar{3} \rightarrow \{0x3, 0x5, 0x9, 0xA, 0xB, 0xC, 0xD\}, \quad \bar{6} \rightarrow \{0x6\}, \quad \bar{E} \rightarrow \{0xE\}.$$

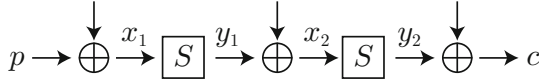
Therefore,  $\bar{E}$  is redundant because  $0xE \succeq 0xA$ . On the other hand, there is not a vector  $\mathbf{k}$  satisfying  $0x6 \succeq \mathbf{k}$  in  $\mathbf{k} \in \{0x3, 0x5, 0x9, 0xA, 0xB, 0xC, 0xD\}$ . As a result, after remove redundant vectors, the division property becomes  $\mathcal{D}_{\{\bar{3}, \bar{6}\}}$ . The right-end column in Table 3 shows redundant vectors by the compact representation.

### 3.3 Toy Cipher Using PRESENT S-box

We apply the compact representation to the input division property of S-boxes, and the propagated output division property is not represented by the compact representation. We need to carefully apply the compact representation to the output division property, which depends on the structure of a target cipher. For simplicity, let us consider a key-alternating cipher underlying PRESENT S-box, where the block length is 4 bits, and Fig. 1 shows the 2-round cipher. Let  $p$  and  $c$  be the plaintext and ciphertext, and  $x_i$  and  $y_i$  denote the input and output of the  $i$ th S-box, respectively. Note that the division property does not change for constant addition. Then, our aim is to evaluate the division property of  $c$ , and it is enough to manage only the compact representation of the division property in  $x_2$ . Our next aim is to evaluate the compact representation in  $x_2$ . Then, it is enough to manage only the compact representation in  $x_1$  and the following propagation characteristic is applied.

$$\begin{aligned}
\{\bar{0}\} &\rightarrow \{0x0\} \rightarrow \{\bar{0}\}, \\
\{\bar{1}\} &\rightarrow \{0x1, 0x2, 0x4, 0x8\} \rightarrow \{\bar{1}\}, \\
\{\bar{3}\} &\rightarrow \{0x2, 0x4, 0x8\} \rightarrow \{\bar{1}\}, \\
\{\bar{6}\} &\rightarrow \{0x1, 0x2, 0x8\} \rightarrow \{\bar{1}\}, \\
\{\bar{7}\} &\rightarrow \{0x2, 0x8\} \rightarrow \{\bar{1}\}, \\
\{\bar{E}\} &\rightarrow \{0x5, 0xB, 0xE\} \rightarrow \{\bar{3}, (\bar{E})\}, \\
\{\bar{F}\} &\rightarrow \{0xF\} \rightarrow \{\bar{F}\}.
\end{aligned}$$

Note that the property  $\bar{E}$  derives  $\bar{3}$  and  $\bar{E}$ , but  $\bar{E}$  is redundant.



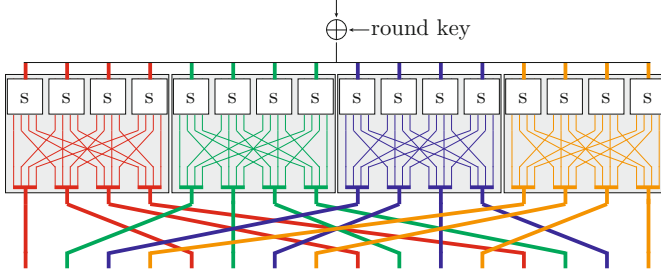
**Fig. 1.** Key-alternating cipher underlying PRESENT S-box.

*Example 1.* Assuming the division property of  $p$  is  $\{\bar{E}\}$ , the division property of  $x_1$  is also  $\{\bar{E}\}$  because the division property is independent of the constant XORing. Applying the first S-box, the division property of  $y_1$  is  $\{\bar{3}, \bar{E}\}$ , and  $\bar{E}$  is redundant. Since the division property is independent of the constant XORing, the division property of  $x_2$  is  $\{\bar{3}\}$ . Applying the second S-box, the bit-based division property of  $y_2$  is  $\mathcal{D}_{\{0x2, 0x4, 0x8\}}^{1^4}$ , and the bit-based division property of  $c$  is also  $\mathcal{D}_{\{0x2, 0x4, 0x8\}}^{1^4}$ . Therefore, the least significant bit of  $c$  is balanced.

### 3.4 Core Function of PRESENT

PRESENT does not have simple key-alternating structure like Fig. 1. There is a bit permutation in the diffusion part of the round function, and we can decompose the round function of PRESENT into four subfunctions. Figure 2 shows the





**Fig. 2.** Equivalent circuit of round function of PRESENT.

---

**Algorithm 1.** Generate propagation characteristic table for the sub function

---

```

1: procedure evalSubFunction( $\mathbf{k} \in (\mathbb{S}_c)^4$ )
2:    $\mathbb{K}_i$  is the set of the propagated division property from  $k_i$  through the S-box.
3:    $\mathbb{K}'$  is an empty set.
4:   for all  $(x, y, z, w) \in (\mathbb{K}_4 \times \mathbb{K}_3 \times \mathbb{K}_2 \times \mathbb{K}_1)$  do
5:      $k'_4 \leftarrow \text{compact}(x_4 \| y_4 \| z_4 \| w_4)$ 
6:      $k'_3 \leftarrow \text{compact}(x_3 \| y_3 \| z_3 \| w_3)$ 
7:      $k'_2 \leftarrow \text{compact}(x_2 \| y_2 \| z_2 \| w_2)$ 
8:      $k'_1 \leftarrow \text{compact}(x_1 \| y_1 \| z_1 \| w_1)$ 
9:      $\mathbb{K}' = \mathbb{K}' \cup \{\mathbf{k}'\}$ 
10:  end for
11:  remove redundant vectors from  $\mathbb{K}'$ 
12:  return  $\mathbb{K}'$ 
13: end procedure

```

---

equivalent circuit of the round function of PRESENT. The input and output of every sub function are four four-bit values, and the position of each four-bit value then moves. Since this equivalent circuit does not have bit-oriented permutation except the interior of sub functions, we first generate the propagation characteristic table of sub functions under the compact representation. Then, we evaluate the propagation characteristic of round functions from the table under the compact representation.

**Propagation Characteristic for Sub Function.** Let  $\mathbf{k} = (k_4, k_3, k_2, k_1) \in (\mathbb{S}_c)^4$  be the input division property of the sub function. Then, the output division property  $\mathbb{K}$  is the set whose elements are vectors in  $(\mathbb{S}_c)^4$ . Algorithm 1 shows the algorithm to generate the propagation characteristic table under the compact representation for the sub function. Here, **compact** is a function that converts from the bit-based division property to the compact representation.

*Example 2 (Propagation characteristic from  $(\bar{3}, \bar{6}, \bar{7}, \bar{F})$ ).* The output bit-based division property of each S-box is evaluated from the corresponding compact representation as

---

**Algorithm 2.** Generate propagation characteristic table for the sub function
 

---

```

1: procedure evalRoundFunction( $\mathbf{k} \in (\mathbb{S}_c)^{16}$ )
2:    $\mathbb{K}_i \leftarrow \text{evalSubFunction}([k_{4*i+4}, k_{4*i+3}, k_{4*i+2}, k_{4*i+1}])$ 
3:   for all  $(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) \in (\mathbb{K}_4 \times \mathbb{K}_3 \times \mathbb{K}_2 \times \mathbb{K}_1)$  do
4:      $k'_{16} = x_4, k'_{12} = x_3, k'_8 = x_2, k'_4 = x_1$ 
5:      $k'_{15} = y_4, k'_{11} = y_3, k'_7 = y_2, k'_3 = y_1$ 
6:      $k'_{14} = z_4, k'_{10} = z_3, k'_6 = z_2, k'_2 = z_1$ 
7:      $k'_{13} = w_4, k'_9 = w_3, k'_5 = w_2, k'_1 = w_1$ 
8:      $\mathbb{K}' = \mathbb{K}' \cup \{\mathbf{k}'\}$ 
9:   end for
10:  remove redundant vectors from  $\mathbb{K}'$ 
11:  return  $\mathbb{K}'$ 
12: end procedure

```

---

$$\bar{3} \rightarrow \{0x2, 0x4, 0x8\}, \quad \bar{6} \rightarrow \{0x1, 0x2, 0x8\}, \quad \bar{7} \rightarrow \{0x2, 0x8\}, \quad \bar{F} \rightarrow \{0xF\}.$$

Then, let  $\mathcal{D}_{\mathbb{K}'}^{14}$  be the output bit-based division property, and  $\mathbb{K}'$  is represented as  $18(= 3 \times 3 \times 2 \times 1)$  vectors

$$\begin{aligned} & (0x11B5), (0x3195), (0x11F1), (0x31D1), (0x51B1), (0x7191), \\ & (0x1935), (0x3915), (0x1971), (0x3951), (0x5931), (0x7911), \\ & (0x9135), (0xB115), (0x9171), (0xB151), (0xD131), (0xF111). \end{aligned}$$

Then, the compact representation of 18 vectors is

$$\begin{aligned} & (\bar{1}\bar{1}\bar{3}\bar{3}), (\bar{3}\bar{1}\bar{3}\bar{3}), (\bar{1}\bar{1}\bar{F}\bar{1}), (\bar{3}\bar{1}\bar{3}\bar{1}), (\bar{3}\bar{1}\bar{3}\bar{1}), (\bar{7}\bar{1}\bar{3}\bar{1}), (\bar{1}\bar{3}\bar{3}\bar{3}), (\bar{3}\bar{3}\bar{1}\bar{3}), (\bar{1}\bar{3}\bar{7}\bar{1}), \\ & (\bar{3}\bar{3}\bar{3}\bar{1}), (\bar{3}\bar{3}\bar{3}\bar{1}), (\bar{7}\bar{3}\bar{1}\bar{1}), (\bar{3}\bar{1}\bar{3}\bar{3}), (\bar{3}\bar{1}\bar{1}\bar{3}), (\bar{3}\bar{1}\bar{7}\bar{1}), (\bar{3}\bar{1}\bar{3}\bar{1}), (\bar{3}\bar{1}\bar{3}\bar{1}), (\bar{F}\bar{1}\bar{1}\bar{1}). \end{aligned}$$

After remove redundant vectors, the output division property is represented as

$$(\bar{1}\bar{1}\bar{3}\bar{3}), (\bar{1}\bar{1}\bar{F}\bar{1}), (\bar{3}\bar{1}\bar{3}\bar{1}), (\bar{1}\bar{3}\bar{7}\bar{1}), (\bar{7}\bar{3}\bar{1}\bar{1}), (\bar{3}\bar{1}\bar{1}\bar{3}), (\bar{F}\bar{1}\bar{1}\bar{1})$$

by the compact representation.

## 4 Improved Integral Attack on PRESENT

### 4.1 New Algorithm to Find Integral Characteristics

We show a new algorithm to find integral characteristics of PRESENT by using the compact representation of the division property. Note that the given integral characteristic is the same as that given by the accurate propagation characteristic of the bit-based division property.

The input of the algorithm is the bit-based division property of the plaintext set. The algorithm first converts from this bit-based division property to the corresponding compact representation. In every round function, the algorithm evaluates the propagation characteristic for four sub functions independently and the relocation of 16 four-bit values. Algorithm 2 shows the algorithm to evaluate the propagation characteristic for round functions. This evaluation is repeated until there is no integral characteristic in the output of the round function.

**7-Round Integral Characteristic Revisited.** We first revisit the 16th order integral characteristic [15], where the lsb in the output of the 7-round PRESENT is balanced when the least sixteen bits are active and the others are constant. The bit-based division property of the plaintext set is  $\mathcal{D}_{0x00000000000000FF}^{164}$ , and the compact representation is

$$\overline{00000000000000FF}.$$

Ciphertexts encrypted one round have the following compact representation

$$\overline{000F000F000F000F}.$$

Moreover, ciphertexts encrypted two rounds have the following compact representation

$$\overline{1111111111111111}.$$

Table 4 shows the propagation characteristic, where we perfectly remove redundant vectors. After six rounds, we get 70 elements in the compact representation. We finally apply additional one-round function, and the propagated bit-based division property does not include  $0x0000000000000001$ . Therefore, the lsb in the output of the 7-round PRESENT is balanced.

**Table 4.** Propagation from  $\mathcal{D}_{0x00000000000000FF}^{164}$

#rounds	0	1	2	3	4	5	6	7 <sup>a</sup>
$\mathbb{K}$	1	1	1	707281	349316	1450	70	63

<sup>a</sup>We do not use the compact representation in the final round.

**New 9-Round Integral Characteristic.** We next search for integral characteristics exploiting more number of active bits. Let us recall Table 3. Then, the propagated characteristic from  $\bar{E}$  is  $\{0x5, 0xB, 0xE\}$ , and the output bit-based division property is most far from *unknown property* except for  $\bar{F}$ .

**Table 5.** Propagation from  $\mathcal{D}_{0xFFFFFFF0}^{164}$

#rounds	0	1	2	3	4	5	6	7	8	9 <sup>a</sup>
$\mathbb{K}$	1	1	81	8277	136421	2497368	343121	1393	70	63

<sup>a</sup>We do not use the compact representation in the final round.

We prepare the plaintext set that the least significant four bits are passive and the others are active, and the compact representation is

$$\overline{FFFFFFFFFFFFFFFFF0}.$$

**Table 6.** Propagation from  $\mathcal{D}_{0\text{xFFFFFFFFFFFFFFFF}}^{164}$ 

#rounds	0	1	2	3	4	5	6	7	8	9 <sup>a</sup>
$ \mathbb{K} $	1	1	15	174	1053	96251	444174	19749	188	376

<sup>a</sup>We do not use the compact representation in the final round.

Ciphertexts encrypted one round have the following compact representation

$\overline{\text{FFFE}}\overline{\text{FFFFFF}}\overline{\text{FF}}\overline{\text{FF}}, \overline{\text{FFFFFF}}\overline{\text{FFFFFF}}\overline{\text{FF}}\overline{\text{FF}}, \overline{\text{FFFFFF}}\overline{\text{FFFFFF}}\overline{\text{FF}}\overline{\text{FF}}, \overline{\text{FFFFFF}}\overline{\text{FFFFFF}}\overline{\text{FF}}\overline{\text{E}}.$

Moreover, the compact representation of ciphertexts encrypted two rounds consists of 81 elements, where all representations are represented by only  $\overline{\text{E}}$  and  $\overline{\text{F}}$ . After eight rounds, we get 70 elements in the compact representation. We finally apply additional one-round function, and the propagated bit-based division property does not include  $0\text{x}0000000000000001$ . Therefore, the lsb in the output of the 9-round PRESENT is balanced. Table 5 shows the propagation characteristic, where we perfectly remove redundant vectors.

The number of rounds that integral characteristics cover is clearly maximized when the number of active bits is 63. Therefore, we moreover search for integral characteristics exploiting  $2^{63}$  chosen plaintexts. Then, we prepare the plaintext set that the least significant bit is passive and the others are active, and the compact representation is

$\overline{\text{FFFF}}\overline{\text{FFFF}}\overline{\text{FFFF}}\overline{\text{FF}}\overline{\text{E}}.$

Ciphertexts encrypted one round have the following compact representation

$\overline{\text{FFE}}\overline{\text{FFFFFF}}\overline{\text{FF}}\overline{\text{FF}}, \overline{\text{FFFFFF}}\overline{\text{FFFFFF}}\overline{\text{FF}}\overline{\text{FF}}, \overline{\text{FFFFFF}}\overline{\text{FFFFFF}}\overline{\text{FF}}\overline{\text{E}}.$

Moreover, the compact representation of ciphertexts encrypted two rounds consists of 15 elements, where all compact representations are represented by only  $\overline{\text{E}}$  and  $\overline{\text{F}}$ . After eight rounds, we get 188 elements in the compact representation. We finally apply additional one-round function, and the integral property is

$0\text{xEEE0EEE0EEE0EEE0},$

where E means that the 1st bit is balanced, and 0 means that all bits are balanced, i.e., 28 bits are balanced. Table 6 shows the propagation characteristic, where we perfectly remove redundant vectors.

## 4.2 Key Recovery with MTTS Technique and FFT Key Recovery

We attack 12-round PRESENT-80 and 13-round PRESENT-128 by using new 9-round integral characteristics. Our attack uses the match-through-the-S-box (MTTS) technique [19] and FFT key recovery [13]. We briefly explain their previous techniques.

*Match-through-the-S-box (MTTS) Technique* [19]. The MTTS technique was proposed by Zhang et al., and it is the extension of the meet-in-the-middle technique [9]. Let  $x = (x_4, x_3, x_2, x_1)$  and  $y = (y_4, y_3, y_2, y_1)$  be the input and output of the PRESENT S-box. Assuming that  $x_1$  is balanced over a chosen plaintext set  $\Lambda$ , the aim is to recover round keys such that  $\bigoplus_{\Lambda} x_1 = 0$ . Then,  $x_1 = y_4 y_2 \oplus y_3 \oplus y_1 \oplus 1$  from the ANF of  $S^{-1}$ , and  $\bigoplus_{\Lambda} y_4 y_2 = \bigoplus_{\Lambda} y_3 \oplus y_1$  because  $\bigoplus_{\Lambda} x_1 = 0$ . Therefore, we independently evaluate the XOR of  $y_4 y_2$  and that of  $y_3 \oplus y_1$ , and we then search for round keys that two XORs take the same value. In [19], Zhang et al. attacked 10-round PRESENT-80 and 11-round PRESENT-128 by using the MTTS technique.

*Fast Fourier Transform (FFT) Key Recovery Technique* [13]. The FFT key recovery was proposed by Todo and Aoki, and it was originally used for the linear cryptanalysis in [3]. We now evaluate the XOR

$$\bigoplus_{\Lambda} f_{k_1}(c \oplus k_2),$$

where  $f_{k_1}$  is a Boolean function depending on a round key  $k_1$ . Moreover,  $\kappa_1$  and  $\kappa_2$  are bit lengths of  $k_1$  and  $k_2$ , respectively. Then, we can evaluate XORs over all  $(k_1, k_2)$  with  $3\kappa_2 2^{\kappa_1 + \kappa_2}$  time complexity. Note that the time complexity does not depend on the number of chosen plaintexts. Therefore, we can easily evaluate the time complexity by only counting the bit length of involved round keys.

**Integral Attack Against 12-Round PRESENT-80.** Let  $X^i$  be the input of the  $(i + 1)$ th round function, and  $Y^i$  is computed as  $Y^i = X^i \oplus K^i$ , where  $K^i$  denotes the round key. Moreover,  $X^i[j]$ ,  $Y^i[j]$ , and  $K^i[j]$  denote the  $j$ th bit of  $X^i$ ,  $Y^i$ , and  $K^i$  from the right hand, respectively. Here,  $X^0$  is plaintexts, and  $Y^i$  is ciphertexts in  $i$ -round PRESENT. Figure 3 shows the 3-round key recovery for PRESENT.

In the first step, we choose  $2^{60}$ -plaintext sets (denoted by  $\Lambda$ ) and get corresponding ciphertexts after 12-round encryption. We store frequencies of two 32-bit values

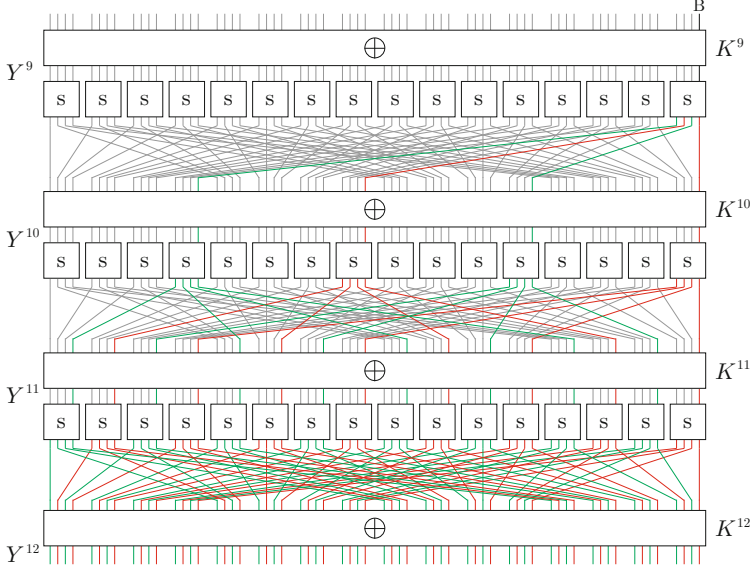
$$Y_E = (Y^{12}[0], Y^{12}[2], \dots, Y^{12}[62]) \quad Y_O = (Y^{12}[1], Y^{12}[3], \dots, Y^{12}[63])$$

into voting tables.

In the second step, we compute the XOR of  $(X^{10}[16] \times X^{10}[48])$  from  $Y_E$  by guessing involved round keys. The XOR is computed as

$$\bigoplus_{\Lambda} (X^{10}[16] \times X^{10}[48]) = f_{K^{10}[16,48], K^{11}[0,8,\dots,56]}(Y_E \oplus K_E^{12}),$$

where  $K_E^{12} = (K^{12}[0], K^{12}[2], \dots, K^{12}[62])$ . The FFT key recovery can evaluate the XOR with the time complexity  $3 \times 32 \times 2^{2+8+32} = 3 \times 2^{47}$ . Note that this time



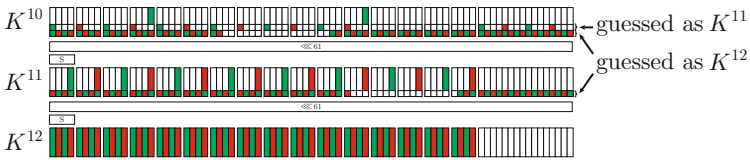
**Fig. 3.** 3-Round key recovery for PRESENT.

complexity is negligible because we already use  $2^{60}$  time complexity to prepare chosen plaintexts.

In the third step, we compute the XOR of  $(X^{10}[0] \oplus X^{10}[32])$  from  $Y_O$  by guessing involved round keys. The XOR is computed as

$$\bigoplus_A (X^{10}[0] \oplus X^{10}[32]) = f'_{K^{11}[4,12,\dots,60]}(Y_O \oplus K_O^{12}).$$

where  $K_O^{12} = (K^{12}[1], K^{12}[3], \dots, K^{12}[63])$ . Note that we do not need to guess  $K^{10}[0]$  and  $K^{10}[32]$  because they relate to  $\bigoplus_A (X^{10}[0] \oplus X^{10}[32])$  linearly. Then, the XOR is evaluated with the time complexity  $3 \times 32 \times 2^{8+32} = 3 \times 2^{45}$ , and it is also negligible.



**Fig. 4.** Involved round keys of PRESENT-80.

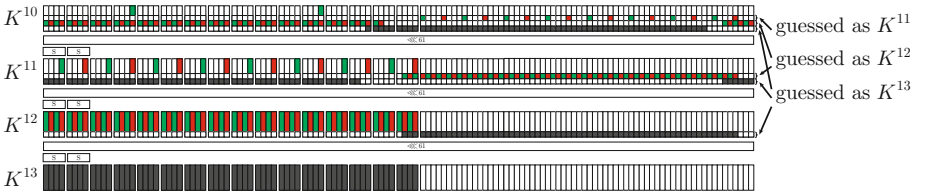
In the fourth step, we search for round keys satisfying

$$\bigoplus_A (X^{10}[16]X^{10}[48]) = \bigoplus_A (X^{10}[0] \oplus X^{10}[32]).$$

Since involved round keys are 42 bits and 40 bits, the total is over 80 bits. However, from the key scheduling algorithm, the total bit length of involved round keys reduces to 68 bits (see Fig. 4). Therefore, by repeating this procedure  $N$  times, we can reduce the key space to  $2^{68-N}$ .

Finally, we exhaustively search remaining keys, and the time complexity is  $2^{80-N}$ . Therefore, the data complexity is  $N \times 2^{60}$ , and the time complexity is  $(N \times 2^{60} + 2^{80-N})$  for  $N \in \{1, 2, \dots, 16\}$ .

**Integral Attack Against 13-Round PRESENT-128.** We attack 13-round PRESENT-128 by using the similar strategy as the 12-round attack. We do not write the procedure in detail because of the page limitation.



**Fig. 5.** Involved round keys of PRESENT-128.

As a result, the FFT key recovery can evaluate the XOR of  $(X^{10}[16] \times X^{10}[48])$  with the time complexity  $3 \times 64 \times 2^{2+8+32+64} = 3 \times 2^{112}$ . Moreover, the FFT key recovery can evaluate the XOR of  $(X^{10}[0] \oplus X^{10}[32])$  with the time complexity  $3 \times 64 \times 2^{8+32+64} = 3 \times 2^{110}$ . While involved round keys are 112 bits and 110 bits, the total bit length of involved round keys reduces to 126 bits because of the key scheduling algorithm (see Fig. 5). Therefore, by repeating the procedure  $N$  times, we can reduce the key space to  $2^{126-N}$ . Finally, we exhaustively search remaining keys. The time complexity is  $2^{128-N}$ , and it is the dominant complexity. Therefore, the data complexity is  $N \times 2^{60}$ , and the time complexity is  $2^{128-N}$  for  $N \in \{1, 2, \dots, 16\}$ .

## 5 Conclusion

We proposed the compact representation for the bit-based division property in this paper. It is difficult to apply the bit-based division property to block ciphers whose block length is over 32 because of high time and memory complexity. The compact representation partially solves this problem. To demonstrate the advantage of our method, we applied this technique to 64-bit block cipher PRESENT. As a result, we attacked 12-round PRESENT-80 and 13-round PRESENT-128 by using new 9-round integral characteristic, and they are improved by two rounds than the previous best integral attacks.

## References

1. 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., Verbaauwhede, 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)
2. Boura, C., Canteaut, A.: Another view of the division property (2016). (Accepted to CRYPTO2016). <https://eprint.iacr.org/2016/554>
3. Collard, B., Standaert, F.-X., Quisquater, J.-J.: Improving the time complexity of Matsui’s linear cryptanalysis. In: Nam, K.-H., Rhee, G. (eds.) ICISC 2007. LNCS, vol. 4817, pp. 77–88. Springer, Heidelberg (2007). doi:[10.1007/978-3-540-76788-6\\_7](https://doi.org/10.1007/978-3-540-76788-6_7)
4. Daemen, J., Knudsen, L., Rijmen, V.: The block cipher Square. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997). doi:[10.1007/BFb0052343](https://doi.org/10.1007/BFb0052343)
5. 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)
6. Knudsen, L., Wagner, D.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002). doi:[10.1007/3-540-45661-9\\_9](https://doi.org/10.1007/3-540-45661-9_9)
7. Lai, X.: Higher order derivatives and differential cryptanalysis. In: Blahut, R.E., Costello, D.J., Maurer, U., Mittelholzer, T. (eds.) Communications and Cryptography. The Springer International Series in Engineering and Computer Science, vol. 276, pp. 227–233. Springer, Heidelberg (1994)
8. Li, Y., Wu, W., Zhang, L.: Improved integral attacks on reduced-round CLEFIA block cipher. In: Jung, S., Yung, M. (eds.) WISA 2011. LNCS, vol. 7115, pp. 28–39. Springer, Heidelberg (2012). doi:[10.1007/978-3-642-27890-7\\_3](https://doi.org/10.1007/978-3-642-27890-7_3)
9. Sasaki, Y., Wang, L.: Meet-in-the-middle technique for integral attacks against feistel ciphers. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 234–251. Springer, Heidelberg (2013). doi:[10.1007/978-3-642-35999-6\\_16](https://doi.org/10.1007/978-3-642-35999-6_16)
10. Sun, B., Hai, X., Zhang, W., Cheng, L., Yang, Z.: New observation on division property. IACR Cryptology ePrint Archive 2015, 459 (2015). <http://eprint.iacr.org/2015/459>
11. Todo, Y.: Integral cryptanalysis on full MISTY1. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 413–432. Springer, Heidelberg (2015). doi:[10.1007/978-3-662-47989-6\\_20](https://doi.org/10.1007/978-3-662-47989-6_20)
12. Todo, Y.: Structural evaluation by generalized integral property. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 287–314. Springer, Heidelberg (2015). doi:[10.1007/978-3-662-46800-5\\_12](https://doi.org/10.1007/978-3-662-46800-5_12)
13. Todo, Y., Aoki, K.: FFT key recovery for integral attack. In: Gritzalis, D., Kiayias, A., Askoxylakis, I. (eds.) CANS 2014. LNCS, vol. 8813, pp. 64–81. Springer, Heidelberg (2014). doi:[10.1007/978-3-319-12280-9\\_5](https://doi.org/10.1007/978-3-319-12280-9_5)
14. Todo, Y., Morii, M.: Bit-based division property and application to Simon family. IACR Cryptology ePrint Archive 2016, 285 (2016). (Accepted to FSE2016). <https://eprint.iacr.org/2016/285>
15. Wu, S., Wang, M.: Integral attacks on reduced-round PRESENT. In: Qing, S., Zhou, J., Liu, D. (eds.) ICICS 2013. LNCS, vol. 8233, pp. 331–345. Springer, Heidelberg (2013). doi:[10.1007/978-3-319-02726-5\\_24](https://doi.org/10.1007/978-3-319-02726-5_24)
16. Yeom, Y., Park, S., Kim, I.: On the security of CAMELLIA against the square attack. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 89–99. Springer, Heidelberg (2002). doi:[10.1007/3-540-45661-9\\_7](https://doi.org/10.1007/3-540-45661-9_7)



17. Z'aba, M.R., Raddum, H., Henricksen, M., Dawson, E.: Bit-pattern based integral attack. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 363–381. Springer, Heidelberg (2008). doi:[10.1007/978-3-540-71039-4\\_23](https://doi.org/10.1007/978-3-540-71039-4_23)
18. Zhang, H., Wu, W.: Structural evaluation for generalized feistel structures and applications to LBlock and TWINE. In: Biryukov, A., Goyal, V. (eds.) INDOCRYPT 2015. LNCS, vol. 9462, pp. 218–237. Springer, Heidelberg (2015). doi:[10.1007/978-3-319-26617-6\\_12](https://doi.org/10.1007/978-3-319-26617-6_12)
19. Zhang, H., Wu, W., Wang, Y.: Integral attack against bit-oriented block ciphers. In: Kwon, S., Yun, A. (eds.) ICISC 2015. LNCS, vol. 9558, pp. 102–118. Springer, Heidelberg (2016). doi:[10.1007/978-3-319-30840-1\\_7](https://doi.org/10.1007/978-3-319-30840-1_7)

Cryptology and Network Security

15th International Conference, CANS 2016, Milan, Italy,

November 14-16, 2016, Proceedings

Foresti, S.; Persiano, G. (Eds.)

2016, XVI, 762 p. 116 illus., Softcover

ISBN: 978-3-319-48964-3