Dual Relationship Between Impossible Differentials and Zero Correlation Linear Hulls of SIMON-Like Ciphers

Xuan Shen[1], Ruilin Li[2], Bing Sun[1](✉), Lei Cheng[1], Chao Li[1](✉), and Maodong Liao[3]

[1] College of Science, National University of Defense Technology,
Changsha 410073, People's Republic of China
shenxuan_08@163.com, happy_come@163.com, chenglei_1111@163.com,
academic_lc@163.com

[2] School of Electronic Science, National University of Defense Technology,
Changsha 410073, People's Republic of China
securitylrl@163.com

[3] Academy of Mathematics and Systems Science, Chinese Academy of Sciences,
Beijing 100190, People's Republic of China
liaomd278@163.com

Abstract. As far as we know, for impossible differentials and zero correlation linear hulls of SIMON-like ciphers (denoted as SIMON in our paper), the distinguishers previously constructed by the miss-in-the-middle technique are all based on bit-level contradictions. Under this condition, our results on the two kinds of distinguishers are presented as follows:

Firstly, by introducing both the diffusion matrix and the dual cipher of SIMON, we establish some links between impossible differentials and zero correlation linear hulls for SIMON and its dual cipher. For SIMON, we prove that there is a one-to-one correspondence between impossible differentials and zero correlation linear hulls. Meanwhile, for SIMON and its dual cipher, we show that there is also a one-to-one correspondence between impossible differentials of one cipher and zero correlation linear hulls of the dual one. Secondly, we show that impossible differentials and zero correlation linear hulls of SIMON can be constructed by a matrix calculation approach. Finally, when applying our method to SIMON with some specific parameters, we show that SIMON with parameter (1,0,2) recommended at CRYPTO 2015 is worse than the original SIMON with respect to security against impossible differential and zero correlation linear cryptanalysis.

Keywords: SIMON-like ciphers · Impossible differential
Zero correlation linear hull

The work in this paper is supported by National Key R&D Program of China (No: 2017YFB0802000), the National Natural Science Foundation of China (No: 61672530, 61402515, 61772545), the Project of Hunan Province Department of Education (No: 16B086) and Open Research Fund of Hunan Provincial Key Laboratory of Network Investigational Technology (No: 2016WLZC018).

J. K. Liu and P. Samarati (Eds.): ISPEC 2017, LNCS 10701, pp. 237–255, 2017.
https://doi.org/10.1007/978-3-319-72359-4_14

1 Introduction

With the development of network techniques, information security has been increasingly important. Due to the restrictions in constrained environments like RFID tags, many lightweight block ciphers have been designed to protect data confidentiality in those devices, such as PRESENT [1], LED [2], LBlock [3], PICCOLO [4], PRINCE [5].

In 2013, SIMON [6] was designed by National Security Agency (NSA) as a lightweight block cipher. It uses only simple operations such as XOR, bitwise AND and bit rotation to improve its implementation performance. After it was published, a large number of cryptanalysis on SIMON were proposed [7–16].

To investigate the design principle of the rotation number selection of SIMON, some cryptanalysts focused on SIMON-like ciphers that only differ at the rotation number. At CRYPTO 2015, Kölbl *et al.* [22] studied the differential and linear properties of SIMON-like ciphers with block sizes no more than 64-bit. They recommended three parameters (12,5,3), (1,0,2) and (7,0,2). Among them, SIMON-like ciphers with parameters (12,5,3) and (1,0,2) have better differential and linear properties than those of the original SIMON. Moreover, the parameter (7,0,2) cipher has the best diffusion when it is restricted to $b = 0$ for all possible choices. At ACNS 2016, Kondo *et al.* [20] constructed some impossible differential and integral distinguishers of SIMON-like ciphers whose block sizes are only restricted to 32-bit. They found the parameter (12,5,3) may be a good alternative parameter to the original one against differential, linear, impossible differential as well as integral attacks. Recently, Zhang *et al.* [21] presented a security evaluation for SIMON-like ciphers against integral attack and showed that among all possible choices of the rotation numbers, there exist 120 parameters that are equal or superior to the original one with respect to the length of integral distinguishers.

As far as we know, for SIMON-like ciphers with arbitrary rotation number and all block sizes, there is no literature on impossible differentials and zero correlation linear hulls. We mainly focus on these two kinds of distinguishers in this paper. Impossible differential cryptanalysis was independently proposed by Knudsen [23] and Biham *et al.* [24]. The most popular impossible differential is the so-called truncated impossible differential, which is independent of the choices of S-boxes. Several approaches have been proposed to derive truncated impossible differentials of a block cipher effectively such as $\mathcal{U}$-method [25], UID-method [26] and the extended tool of the former two methods generalized by Wu and Wang [27]. To search impossible differential distinguishers we mainly use the *miss-in-the-middle* method, by which the contradictions are obtained in the middle matching from the encryption and decryption directions. Zero correlation linear cryptanalysis was firstly proposed by Bogdanov and Rijmen [28]. The main idea is to construct some linear characteristics with correlation exactly zero, which is similar to impossible differential cryptanalysis.

At CRYPTO 2015, Sun *et al.* proposed the concept of "structure", which contains all ciphers that only differ at the nonlinear parts, to characterize those cryptanalytic methods that are independent of the details of the S-boxes [29].

Furthermore, with the help of "dual structure", they built a link between impossible differential and zero correlation linear cryptanalysis, e.g., *an impossible differential of a structure always implies a zero correlation linear hull of the corresponding dual structure*. However, the nonlinear component of SIMON-like ciphers is made up of XOR, bit-wise AND and rotation, which often have a weak confusion and diffusion. When applying the concept of "structure" to SIMON-like ciphers, we can only get 4-round impossible differentials and 4-round zero correlation linear hulls, respectively, which are far less than the known results. Therefore, the concept of "structure" can not be directly applied to get an accurate security margin for SIMON-like ciphers and the link built by Sun *et al.* can not be applied to SIMON-like ciphers. Thus, it motives us to study how to get a relatively tight security evaluation and build the link between impossible differentials and zero correlation linear hulls of SIMON-like ciphers in a new way.

For most ciphers which adopt S-boxes, the contradiction is found when the difference/mask is zero from encryption/decryption direction and non-zero from the other direction. However, for SIMON-like ciphers, the contradiction sometimes could be built at the bit level, e.g., we could compute the exact values of some bits of the difference/mask from both the encryption and decryption directions. To the best of our knowledge, all impossible differentials and zero correlation linear hulls of SIMON-like ciphers found so far are constructed based on the bit-level contradictions. Therefore, we are going to investigate the properties of impossible differential and zero correlation linear distinguishers for SIMON-like ciphers based on bit-level contradictions.

Our Contribution. In this paper, we use SIMON to denote the family of SIMON-like ciphers with the rotation number (a, b, c). Furthermore, with the diffusion matrix defined in our paper, we build some links between impossible differentials and zero correlation linear hulls for SIMON and Dual-SIMON (see Definition 1 in Sect. 2.2) based on bit-level contradictions in Fig. 1.

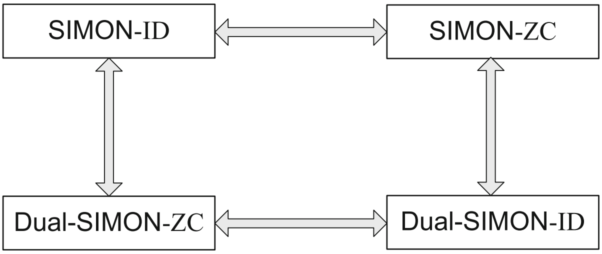

Fig. 1. Links between impossible differentials (ID) and zero correlation linear hulls (ZC) for SIMON and Dual-SIMON

(1) With the diffusion matrix, for SIMON, we prove that there is a one-to-one correspondence between impossible differentials and zero correlation linear

hulls. Meanwhile, for SIMON and Dual-SIMON, we show that there is also a one-to-one correspondence between impossible differentials of one cipher and zero correlation linear hulls of the dual one, which extends the link built by Sun *et al.* at CRYPTO 2015 for Sbox-based ciphers.

(2) With our method, we can construct impossible differentials and zero correlation linear hulls of SIMON based on bit-level contradictions. Furthermore, when applying our method to SIMON with some specific parameters, some results are obtained.
   - We show that SIMON with parameter (12,5,3) may not be a good alternative to the original SIMON against impossible differential and zero correlation linear attack when the block size is larger than 32-bit.
   - We present that SIMON with parameter (1,0,2) is worse than the original SIMON with respect to the resistance against impossible differential and zero correlation linear attacks.

Organization. The remainder of this paper is organized as follows. In Sect. 2, we give some notations and concepts that will be used in this paper. Moreover, we also present the brief description of SIMON-like ciphers. Then, we introduce the definition of the diffusion matrix and give some properties about it in Sect. 3. After that, some links between impossible differentials and zero correlation linear hulls of SIMON-like ciphers are presented in Sect. 4. In Sect. 5, we apply our matrix-based method to SIMON with some parameters. Finally, Sect. 6 concludes this paper.

2 Preliminary

2.1 Notations and Concepts

In this subsection, we give some notations in Table 1, which will be used in the rest of this paper. Note that all vectors used in our paper are *row vectors* and X_0 is the least significant bit for a vector $X = (X_{n-1}, X_{n-2}, \cdots, X_1, X_0)$.

Table 1. Notations used in this paper

$\oplus$	XOR operation
$\lll l, \ggg l$	Left and right rotation for l bits, respectively
&	Bitwise AND operation
X^i	The i-th round state
X^i_j	The j-th bit of X^i
X_j	The j-th bit of vector X
K^i	The i-th round subkey
Y^T	Transpose of vector Y
M^T	Transpose of matrix M
$\varepsilon_{\{i_1,i_2,\cdots,i_t\}}$	The $\{i_1, i_2, \cdots, i_t\}$-th bits of vector ε are 1 and the others are 0

We recall the concepts of impossible differential and zero correlation linear hull of a vectorial function.

Given a function G: $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^k$, let $\delta \in \mathbb{F}_2^n$ and $\Delta \in \mathbb{F}_2^k$. The differential probability $\delta \rightarrow \Delta$ is defined as

$$p(\delta \xrightarrow{G} \Delta) \triangleq \frac{\#\{X \in \mathbb{F}_2^n | G(X) \oplus G(X \oplus \delta) = \Delta\}}{2^n}.$$

If $p(\delta \xrightarrow{G} \Delta) = 0$, then $\delta \rightarrow \Delta$ is called an *impossible differential* of G [23,24].

Let $\Gamma X = (\Gamma X_{n-1}, \Gamma X_{n-2}, \cdots, \Gamma X_1, \Gamma X_0) \in \mathbb{F}_2^n, X \in \mathbb{F}_2^n$. Then

$$\Gamma X \cdot X \triangleq \bigoplus_{i, \Gamma X_i = 1} X_i$$

denotes the inner product of ΓX and X. It is notable that the inner product of ΓX and X can be written as $(\Gamma X)X^T$ where the multiplication is defined as matrix multiplication.

For a function G: $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^k$, the correlation of the linear approximation for an n-bit input mask ΓX and a k-bit output mask ΓY is defined by

$$c(\Gamma X \cdot X \oplus \Gamma Y \cdot G(X)) \triangleq \frac{1}{2^n} \sum_{X \in \mathbb{F}_2^n} (-1)^{\Gamma X \cdot X \oplus \Gamma Y \cdot G(X)}.$$

If $c(\Gamma X \cdot X \oplus \Gamma Y \cdot G(X)) = 0$, then $\Gamma X \rightarrow \Gamma Y$ is called an *zero correlation linear hull* of G [28].

2.2 Brief Description of SIMON-Like Ciphers

SIMON-like ciphers are based on Feistel structures. Let $X^i = (X_L^i || X_R^i) = (X_{2n-1}^i, X_{2n-2}^i, \ldots, X_n^i || X_{n-1}^i, X_{n-2}^i, \ldots, X_0^i)$, where $2n$ denotes the block size and $2n \in \{32, 48, 64, 96, 128\}$.

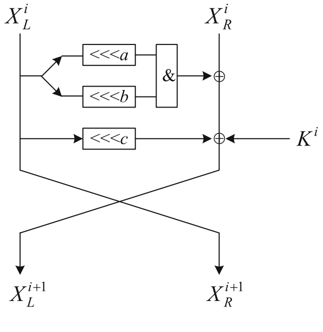

Fig. 2. The round function of SIMON-like ciphers

According to the Feistel structure described in Fig. 2, the round function is given below

$$\begin{cases} X_L^{i+1} = f(X_L^i) \oplus X_R^i \oplus K^i, \\ X_R^{i+1} = X_L^i, \end{cases}$$

where the f-function is defined by

$$f(X) = (X_{\lll a} \& X_{\lll b}) \oplus X_{\lll c}, 0 \leq a, b, c \leq n-1.$$

Note that when $(a, b, c) = (1, 8, 2)$, it is the original SIMON.

In this paper, we are going to investigate impossible differentials and zero correlation linear hulls of SIMON-like ciphers which are often independent of the details of the key schedule. We refer to [6] for the details of the key schedule. Moreover, we give the following definition to study the links between impossible differentials and zero correlation linear hulls of SIMON-like ciphers.

Definition 1. *For any specific instance of the SIMON-like ciphers with rotation number (a, b, c), the dual cipher is defined as the one with rotation number $(n-a, n-b, n-c)$. If n and (a, b, c) are clear from the context, we simply use SIMON and Dual-SIMON as the specific instance SIMON-like cipher and its dual cipher.*

3 Diffusion Matrix and Its Properties

For a vectorial boolean function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, we can always associate F with a graph $\mathcal{G}$ which has $2n$ vertices, denoted by $X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}$. There are 3 types of edges e_{ij} in $\mathcal{G}$:

$e_{ij} = 0$ means that Y_j is not inverted when the value of X_i is changed;
$e_{ij} = 1$ means that Y_j is always inverted when the value of X_i is changed;
$e_{ij} = \lambda$ means that Y_j is sometimes inverted and sometimes not inverted when the value of X_i is changed.

If we do not investigate the exact value of F but only focus on the 3 types of relations between X_i and Y_j, we can get that

$$\begin{pmatrix} Y_{n-1} \\ Y_{n-2} \\ \vdots \\ Y_0 \end{pmatrix} \triangleq \begin{pmatrix} e_{(n-1)(n-1)} & e_{(n-2)(n-1)} & \cdots & e_{0(n-1)} \\ e_{(n-1)(n-2)} & e_{(n-2)(n-2)} & \cdots & e_{0(n-2)} \\ \vdots & \vdots & \cdots & \vdots \\ e_{(n-1)0} & e_{(n-2)0} & \cdots & e_{00} \end{pmatrix}_{n \times n} \begin{pmatrix} X_{n-1} \\ X_{n-2} \\ \vdots \\ X_0 \end{pmatrix} = E \begin{pmatrix} X_{n-1} \\ X_{n-2} \\ \vdots \\ X_0 \end{pmatrix}.$$

Note that all vectors used in our paper are *row vectors*. The above equation could be written as $Y^T = EX^T$, where $X = (X_{n-1}, X_{n-2}, \cdots, X_0), Y = (Y_{n-1}, Y_{n-2}, \cdots, Y_0)$. The matrix E is used to characterize the *bit pattern* propagation from the bit pattern of X to the bit pattern of Y. We give the following example to describe the matrix E.

Example 1. Let $F : \mathbb{F}_2^3 \rightarrow \mathbb{F}_2^3$ be a boolean function which is presented below

$$\begin{cases} Y_2 = X_2 \oplus X_1 X_0, \\ Y_1 = X_2 X_1, \\ Y_0 = X_2 X_0 \oplus X_1 \oplus X_0. \end{cases}$$

Then,

$$E = \begin{pmatrix} e_{22} & e_{12} & e_{02} \\ e_{21} & e_{11} & e_{01} \\ e_{20} & e_{10} & e_{00} \end{pmatrix} = \begin{pmatrix} 1 & \lambda & \lambda \\ \lambda & \lambda & 0 \\ \lambda & 1 & \lambda \end{pmatrix}.$$

For the matrix E, it is called the diffusion matrix of F as follows.

Definition 2 (Diffusion matrix of F). *For a vectorial boolean function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, the diffusion matrix of F is defined as*

$$E = (a_{ij})_{n \times n}, \;\; a_{ij} = e_{(n-1-j)(n-1-i)}, 0 \le i, j \le (n-1).$$

There are 3 kinds of elements $\{0, 1, \lambda\}$ in the diffusion matrix E, and addition and multiplication tables are shown in Tables 2 and 3, respectively.

Table 2. Addition table

$+$	0	1	λ
0	0	1	λ
1	1	0	λ
λ	λ	λ	λ

Table 3. Multiplication table

$\times$	0	1	λ
0	0	0	0
1	0	1	λ
λ	0	λ	λ

Many block ciphers adopt S-boxes as their nonlinear components, which could be also regarded as the vectorial boolean functions. Due to the principle of designing S-boxes, there should not be 1 or 0 in the diffusion matrix of S-boxes. However, for lower diffusion block ciphers, such as SIMON-like ciphers, there are many entries of 1 and 0 in the diffusion matrices.

For each component boolean function of the f-function used in the SIMON-like ciphers, say $Y_j = (X_{i_1} \& X_{i_2}) \oplus X_{i_3}$, it is obvious for e_{ij} that

$$e_{ij} = \begin{cases} \lambda & i = i_1, i_2; \\ 1 & i = i_3; \\ 0 & i \neq i_1, i_2, i_3. \end{cases}$$

We recall the definition of $circ[x_0 x_1 \cdots x_{n-1}]$, which is defined as

$$circ[x_0 x_1 \cdots x_{n-1}] \triangleq \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & \cdots & x_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_0 \end{pmatrix}.$$

For SIMON, we define $L_{[n,a,b,c]} = circ[x_0 x_1 \cdots x_{n-1}]$, where

$$x_j = \begin{cases} \lambda & j = a, b; \\ 1 & j = c; \\ 0 & j \neq a, b, c. \end{cases}$$

In the following theorem, we show that $L_{[n,a,b,c]}$ could be used to characterize the diffusion matrix of the f-function.

Theorem 1. *For SIMON, we use E_f to denote the diffusion matrix of the f-function. Then,*

$$E_f = L_{[n,a,b,c]}.$$

Example 2. For SIMON with parameter (0,1,2) and 8-bit block size, the f-function is defined by

$$f(X) = (X \& X_{\lll 1}) \oplus X_{\lll 2}.$$

Then,

$$\begin{cases} Y_3 = X_3 X_2 \oplus X_1, \\ Y_2 = X_2 X_1 \oplus X_0, \\ Y_1 = X_1 X_0 \oplus X_3, \\ Y_0 = X_0 X_3 \oplus X_2. \end{cases}$$

Thus,

$$E_f = L_{[4,0,1,2]} = circ[\lambda\lambda 10] = \begin{pmatrix} \lambda & \lambda & 1 & 0 \\ 0 & \lambda & \lambda & 1 \\ 1 & 0 & \lambda & \lambda \\ \lambda & 1 & 0 & \lambda \end{pmatrix}$$

Remark 1. Let ΔX and ΔY be the input and output differences of the f-function, respectively. Obviously, we have $\Delta Y^T = E_f \Delta X^T = L_{[n,a,b,c]} \Delta X^T$ with the definition of E_f and Theorem 1.

Remark 2. The method illustrated above could be extended to linear cases: Let ΓX and ΓY be the input and output masks of the f-function, respectively. Since $Y^T = E_f X^T = L_{[n,a,b,c]} X^T$, we have $(\Gamma X) X^T = (\Gamma Y) Y^T = \Gamma Y (L_{[n,a,b,c]} X^T)$. Thus, $\Gamma X = \Gamma Y L_{[n,a,b,c]}$.

Corollary 1. *For SIMON, we use $D_{[2n,a,b,c]}$ to denote the diffusion matrix of the round function. Then,*

$$D_{[2n,a,b,c]} = \begin{pmatrix} L_{[n,a,b,c]} & I_{n \times n} \\ I_{n \times n} & O_{n \times n} \end{pmatrix},$$

where $I_{n \times n}$ is the $n \times n$ identity matrix and $O_{n \times n}$ is the $n \times n$ zero matrix.

According to the definition of $D_{[2n,a,b,c]}$, we have $\left(X^{s+1}\right)^T = D_{[2n,a,b,c]} \left(X^s\right)^T$, which is similar to $Y^T = L_{[n,a,b,c]}X^T$. Furthermore, $\left(X^{s+t}\right)^T = D^t_{[2n,a,b,c]}\left(X^s\right)^T$.

Let $D^t_{[2n,a,b,c]} = \left(d^{(t)}_{ij}\right)$, where $d^{(t)}_{ij}$ stands for the i-th row and j-th column element of $D^t_{[2n,a,b,c]}$. There are 3 kinds of values for $d^{(t)}_{ij}$ and their meanings are similar to those of 3 types of edges e_{ij}.

$d^{(t)}_{ij} = 0$ means that X^{s+t}_j is not inverted when the value of X^s_i is changed;
$d^{(t)}_{ij} = 1$ means that X^{s+t}_j is always inverted when the value of X^s_i is changed;
$d^{(t)}_{ij} = \lambda$ means that X^{s+t}_j is sometimes inverted and sometimes not inverted when the value of X^s_i is changed.

Remark 3. Let ΔX^s and ΔX^{s+t} be the input difference of the s-th and $(s+t)$-th round, respectively. We have $\left(\Delta X^{s+t}\right)^T = D^t_{[2n,a,b,c]}\left(\Delta X^s\right)^T$. Furthermore, this method could also be applied to characterize linear trails.

For $D^t_{[2n,a,b,c]}$, we give the following proposition.

Proposition 1. *Let*

$$D^t_{[2n,a,b,c]} = \begin{pmatrix} D^{(t)}_{11} & D^{(t)}_{12} \\ D^{(t)}_{21} & D^{(t)}_{22} \end{pmatrix}, t \geq 1.$$

Then all $D^{(t)}_{11}, D^{(t)}_{12}, D^{(t)}_{21}, D^{(t)}_{22}$ are $n \times n$ circulant sub-matrices and

$$D^{(t+2)}_{22} = D^{(t+1)}_{12} = D^{(t+1)}_{21} = D^{(t)}_{11}.$$

Proposition 1 can be directly obtained by calculating the power of $D_{[2n,a,b,c]}$. It indicates that we only need to consider $D^{(t)}_{22}$ to characterize the maximum round number r that contains 1 or 0 in $D^t_{[2n,a,b,c]}$. In other words, there does not exist 0 or 1 in $D^t_{[2n,a,b,c]}$ when $t \geq r+1$. Furthermore, we use r_1 and r_0 to denote the maximum round number that contains 1 and 0 in $D^t_{[2n,a,b,c]}$, respectively. And r_1 and r_0 are defined as

$$r_1 = \max\{t | \exists\{i, j_1, j_2, \cdots, j_k\}, \underset{j_1,j_2,\cdots,j_k}{\oplus} {d_{ij}}^{(t)} = 1\};$$

$$r_0 = \max\{t | \exists\{i, j_1, j_2, \cdots, j_k\}, \underset{j_1,j_2,\cdots,j_k}{\oplus} {d_{ij}}^{(t)} = 0\},$$

where $\underset{j_1,j_2,\cdots,j_k}{\oplus} {d_{ij}}^{(t)}$ is denoted as the XOR sum of $d^{(t)}_{ij_1}, d^{(t)}_{ij_2}, \cdots, d^{(t)}_{ij_k}$ and $d^{(t)}_{ij} \in \{0,1\}, j = j_1, j_2, \cdots, j_k$, $1 \leq k < n$.

According to the Feistel structure, when a bit of the output difference after r_1 rounds from the encryption direction is 1 and the same bit of the output difference after (r_0-1) rounds from the decryption direction is 0, an (r_1+r_0-1)-round impossible differential of SIMON could be constructed based on bit-level contradictions. Therefore, we give the following proposition.

Proposition 2. *For SIMON, there exist* $(r_1 + r_0 - 1)$*-round impossible differential distinguishers.*

With the definition of r_1 and r_0, we know that the longest impossible differential distinguishers based on bit-level contradictions are bounded by r_1+r_0-1. Since r_1 and r_0 are determined by $D_{[2n,a,b,c]}$ which is only related to the block size $2n$ and the rotation number (a, b, c), the longest impossible differentials of SIMON based on bit-level contradictions are only determined by the four parameters (n, a, b, c). Moreover, all impossible differentials based on bit-level contradictions could be constructed by the matrix-based approach.

Example 3. For SIMON with parameter (0,1,2) and 8-bit block size, which has been given in Example 2, we have

$$D_{[8,0,1,2]} = \begin{pmatrix} \lambda & \lambda & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & \lambda & \lambda & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & \lambda & \lambda & 0 & 0 & 1 & 0 \\ \lambda & 1 & 0 & \lambda & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}, D^2_{[8,0,1,2]} = \begin{pmatrix} \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & 1 & 0 \\ \lambda & \lambda & \lambda & \lambda & 0 & \lambda & \lambda & 1 \\ \lambda & \lambda & \lambda & \lambda & 1 & 0 & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & 1 & 0 & \lambda \\ \lambda & \lambda & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & \lambda & \lambda & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & \lambda & \lambda & 0 & 0 & 1 & 0 \\ \lambda & 1 & 0 & \lambda & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$D^3_{[8,0,1,2]} = \begin{pmatrix} \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & 1 & 0 \\ \lambda & \lambda & \lambda & \lambda & 0 & \lambda & \lambda & 1 \\ \lambda & \lambda & \lambda & \lambda & 1 & 0 & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & 1 & 0 & \lambda \end{pmatrix}, D^4_{[8,0,1,2]} = \begin{pmatrix} \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \\ \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda & \lambda \end{pmatrix}.$$

Therefore, $r_0 = r_1 = 3$ and a 5-round impossible differential $(0, \varepsilon_0) \to (\varepsilon_3, 0)$ is constructed as follows:

$$(0000, 0001) \xrightarrow{D_{[8,0,1,2]}} (0001, 0000) \xrightarrow{D_{[8,0,1,2]}} (01\lambda\lambda, 0001) \xrightarrow{D_{[8,0,1,2]}} (\lambda\lambda\lambda\lambda, \mathbf{01}\lambda\lambda)$$

$$(1000, \lambda\mathbf{01}\lambda) \xleftarrow{D_{[8,0,1,2]}} (0000, 1000) \xleftarrow{D_{[8,0,1,2]}} (1000, 0000).$$

It should be pointed out that the differentials from decryption direction of the above 5-round impossible differential are interchanged the left and right branch differentials before working by $D_{[8,0,1,2]}$ as well as after working by $D_{[8,0,1,2]}$.

4 Links Between Impossible Differentials and Zero Correlation Linear Hulls of SIMON-Like Ciphers

In this section, we mainly study the links between impossible differentials and zero correlation linear hulls of SIMON-like ciphers. To prove our results, we give the definition of the index permutation P and present a proposition about it.

We use P to denote the index permutation mapping the index i to $(n-i) \pmod{n}$. It can be expressed as $Pv = P(v_{n-1}v_{n-2}\cdots v_1 v_0) = (v_1 v_2 \cdots v_{n-1} v_0)$ and we define $Pv = v \times M$, where M is the corresponding index permutation matrix

$$M = \begin{pmatrix} 0\,0 \cdots 0\,1\,0 \\ 0\,0 \cdots 1\,0\,0 \\ \vdots\;\vdots\; \ddots\; \vdots\;\vdots\;\vdots \\ 0\,1 \cdots 0\,0\,0 \\ 1\,0 \cdots 0\,0\,0 \\ 0\,0 \cdots 0\,0\,1 \end{pmatrix}_{n\times n} .$$

Obviously, the index permutation matrix M is symmetric, i.e., $M = M^T$. Since $v = P^2 v = P(vM) = vM^2$, $M^2 = I_{n\times n}$. Therefore, M is involutional. Thus, $M = M^{-1} = M^T$. Furthermore, we present the relations among $L^T_{[n,a,b,c]}$, $L_{[n,n-a,n-b,n-c]}$ and $L_{[n,a,b,c]}$ in the following proposition:

Proposition 3. *Let M be the index permutation matrix and $L_{[n,a,b,c]}$ be the diffusion matrix of the f-function. Then,*

$$L^T_{[n,a,b,c]} = L_{[n,n-a,n-b,n-c]} = M^{-1} L_{[n,a,b,c]} M.$$

Proposition 3 can be directly verified. With the definition of the index permutation P and Proposition 3, we give the following theorem to show the link between impossible differentials of SIMON and zero correlation linear hulls of SIMON based on bit-level contradictions.

Theorem 2. *Based on bit-level contradictions, $(\delta^1, \delta^0) \rightarrow (\delta^{r+1}, \delta^r)$ is an impossible differential of SIMON if and only if $(P\delta^0, P\delta^1) \rightarrow (P\delta^r, P\delta^{r+1})$ is a zero correlation linear hull of SIMON, where P is the index permutation.*

Sketch of the proof. After studying the link between one round differential characteristic and one round linear trail, we prove that there exists a one-to-one correspondence between them. Then, the relationship could be extended to iterated rounds. Finally, with the help of *miss-in-the-middle* method, Theorem 2 can be proved based on bit-level contradictions. The details of the proof are presented in Appendix A.

The above approach could be also exploited to build the link between impossible differentials and zero correlation linear hulls of SIMON and Dual-SIMON. We only need to note $L^T_{[n,a,b,c]} = L_{[n,n-a,n-b,n-c]}$ shown in Proposition 3. Then, the corollary is given below.

Corollary 2. *Based on bit-level contradictions, $(\delta^1, \delta^0) \rightarrow (\delta^{r+1}, \delta^r)$ is an impossible differential of SIMON if and only if $(\delta^0, \delta^1) \rightarrow (\delta^r, \delta^{r+1})$ is a zero correlation linear hull of Dual-SIMON.*

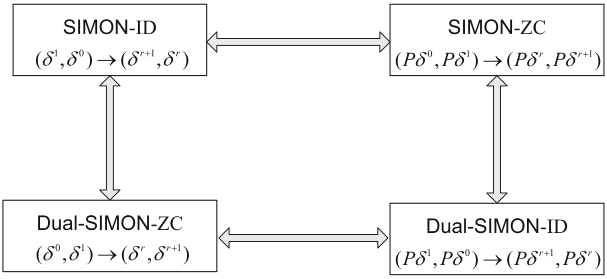
SIMON-ID
$(\delta^1,\delta^0)\to(\delta^{r+1},\delta^r)$
SIMON-ZC
$(P\delta^0,P\delta^1)\to(P\delta^r,P\delta^{r+1})$
Dual-SIMON-ZC
$(\delta^0,\delta^1)\to(\delta^r,\delta^{r+1})$
Dual-SIMON-ID
$(P\delta^1,P\delta^0)\to(P\delta^{r+1},P\delta^r)$

Fig. 3. Links between impossible differentials (ID) and zero correlation linear hulls (ZC) for SIMON and Dual-SIMON

Combining Theorem 2 and Corollary 2, we establish the links between impossible differentials and zero correlation linear hulls for SIMON and Dual-SIMON depicted in Fig. 3.

Especially, when $a+b=n, c=\frac{n}{2}$, SIMON is the same as Dual-SIMON. Thus, with Theorem 2 and Corollary 2, we get that if $(\delta^1,\delta^0)\to(\delta^{r+1},\delta^r)$ is an impossible differential/zero correlation linear hull of SIMON, both $(P\delta^0,P\delta^1)\to(P\delta^r,P\delta^{r+1})$ and $(\delta^0,\delta^1)\to(\delta^r,\delta^{r+1})$ are zero correlation linear hulls/impossible differentials of SIMON.

Corollary 3. *For SIMON and Dual-SIMON, there exist* (r_1+r_0-1)*-round impossible differentials and zero correlation linear hulls.*

Proof. With the links built in Fig. 3, for SIMON and Dual-SIMON, we get that they are the same for the length of impossible differentials and zero correlation linear hulls based on bit-level contradictions. Moreover, with Proposition 2, there are (r_1+r_0-1)-round impossible differentials of SIMON. Therefore, there exist (r_1+r_0-1)-round impossible differentials and zero correlation linear hulls for SIMON and Dual-SIMON.

With the definitions of r_1 and r_0, for SIMON and Dual-SIMON, the length of impossible differentials and zero correlation linear hulls based on bit-level contradictions could be bounded by r_1+r_0-1, which is only determined by the block size $2n$ and the rotation number (a,b,c).

Example 4. For the original SIMON with 32-bit block size, we have

$$D_{[32,1,8,2]}=\begin{pmatrix} L_{[16,1,8,2]} & I_{16\times 16} \\ I_{16\times 16} & O_{16\times 16} \end{pmatrix}.$$

By calculating the power of the matrix $D_{[32,1,8,2]}$, we get that $r_1=r_0=6$. According to Corollary 3, there are 11-round impossible differential and zero correlation linear hull distinguishers. In [13], the authors presented the impossible differential $(0,\varepsilon_0)\xrightarrow{11}(\varepsilon_9,0)$ and the zero correlation linear hull $(\varepsilon_0,0)\xrightarrow{11}(0,\varepsilon_7)$, which are consistent with our result.

5 Applications

At CRYPTO 2015, Kölbl *et al.* recommended the three parameters (12,5,3), (7,0,2) and (1,0,2). SIMON with these three parameters are regarded to be promising when compared with the original SIMON for the differential and linear properties. Meanwhile, SIMECK [17–19] is a family of lightweight block ciphers proposed at CHES 2015, which could be viewed as SIMON with parameter (5,0,1).

In this section, we study SIMON with these parameters on impossible differential and zero correlation linear distinguishers. SIMON with parameter (a, b, c) is called SIMON$[a, b, c]$ for short. With our matrix-based method, we present the length of impossible differential and zero correlation linear distinguishers of the original SIMON with all block sizes in Table 4. The results are consistent with previous results.

Table 4. The length of the distinguishers for SIMON

Block size	r_1	r_0	ID/ZC
32	6	6	11
48	6	7	12
64	6	8	13
96	7	10	16
128	8	12	19

The length of impossible differentials and zero correlation linear hulls of SIMECK with all block sizes are shown in Table 5. 11/13/15-round zero correlation linear distinguishers of SIMECK32/48/64 have been presented in [30]. According to Theorem 2, we can directly prove without any search that there are also 11/13/15-round impossible differential distinguishers for SIMECK32/48/64, respectively. The results are also given in [31] where 11/13/15-round impossible differential distinguishers for SIMECK32/48/64 are searched with the help of computer search.

Table 5. The length of the distinguishers for SIMECK

Block size	r_1	r_0	ID/ZC
32	5	7	11
48	6	8	13
64	6	10	15

For SIMON with the three parameters recommended in [22], they have good performance on the differential and linear properties. However, in Table 6, the length of ID/ZC distinguishers of SIMON with the three parameters are no shorter than those of the original SIMON (SIMON$[1,8,2]$). Especially, for SIMON$[1,0,2]$, the length of the distinguishers are much longer than those of the original SIMON. From this point, SIMON$[1,0,2]$ is worse than the original SIMON and it is necessary to evaluate the security again. We present a 17-round impossible differential distinguisher as an example in Appendix B. For SIMON$[12,5,3]$, it is considered as a good alternative to the original SIMON for differential, linear, impossible differential and integral attacks in [20]. However, the block size considered in [20] is only 32-bit. Compared with the original SIMON for various block sizes, the length of ID/ZC distinguishers of SIMON$[12,5,3]$ have 1 round more than those of the original SIMON when the block size takes 48-bit and 96-bit in Table 6. Therefore, SIMON$[12,5,3]$ needs to be further evaluated with all block sizes against impossible differential and zero correlation linear attacks.

Table 6. The length of the distinguishers for SIMON with different parameters

ID/ZC	32-bit	48-bit	64-bit	96-bit	128-bit
(1,8,2)	11	12	13	16	19
(12,5,3)	11	13	13	17	19
(7,0,2)	13	15	17	19	21
(1,0,2)	17	25	33	49	65

6 Conclusion

In this paper, we investigated impossible differentials and zero correlation linear hulls of SIMON. By introducing the diffusion matrix, we established some links between impossible differentials and zero correlation linear hulls for SIMON and Dual-SIMON based on bit-level contradictions. Furthermore, when applying our matrix-based method to SIMON with some specific parameters, SIMON with parameter (1,0,2) is worse than the original SIMON with respect to security against impossible differential and zero correlation linear attacks. Thus, it is necessary to evaluate the security again. In brief, our results can provide more generic security evaluation against impossible differentials and zero correlation linear hulls of SIMON-like ciphers.

Acknowledgment. The authors would like to thank the anonymous reviewers for their useful comments, and Yunwen Liu, Yi Zhang for fruitful discussions.

Appendix A. Proof of Theorem 2

Proof. The differential and linear propagations of SIMON are shown in Fig. 4.

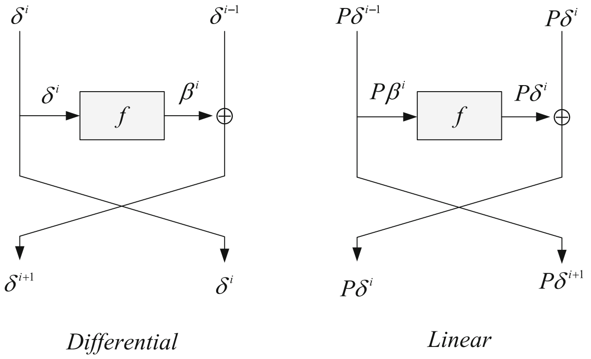

Fig. 4. Differential (left) and linear (right) propagations of SIMON

For the round function of SIMON, we prove that there is a one-to-one correspondence between the differential propagation $(\delta^i, \delta^{i-1}) \rightarrow (\delta^{i+1}, \delta^i)$ and the linear propagation $(P\delta^{i-1}, P\delta^i) \rightarrow (P\delta^i, P\delta^{i+1})$.

According to the definition of the diffusion matrix, we know that the differential propagation of the f-function is $\left(\beta^i\right)^T = L_{[n,a,b,c]}\left(\delta^i\right)^T$. Meanwhile, the linear propagation of the f-function is $P\beta^i = \left(P\delta^i\right)L_{[n,a,b,c]}$. Since $\delta^{i+1} = \delta^{i-1} \oplus \beta^i \Leftrightarrow P\delta^{i+1} = P\delta^{i-1} \oplus P\beta^i$, we could prove the one-to-one correspondence between one round differential propagation and one round linear propagation of SIMON if

$$\left(\beta^i\right)^T = L_{[n,a,b,c]}\left(\delta^i\right)^T \Leftrightarrow P\beta^i = P\delta^i L_{[n,a,b,c]}.$$

With Proposition 3, $L^T_{[n,a,b,c]} = M^{-1}L_{[n,a,b,c]}M$. Therefore,

$$\begin{aligned}\left(\beta^i\right)^T = L_{[n,a,b,c]}\left(\delta^i\right)^T &\Leftrightarrow \beta^i = \delta^i L^T_{[n,a,b,c]},\\ &\Leftrightarrow \beta^i = \delta^i M^{-1}L_{[n,a,b,c]}M,\\ &\Leftrightarrow \beta^i M^{-1} = \delta^i M^{-1}L_{[n,a,b,c]}.\end{aligned}$$

Since $M^{-1} = M$,

$$\left(\beta^i\right)^T = L_{[n,a,b,c]}\left(\delta^i\right)^T \Leftrightarrow \beta^i M = \delta^i M L_{[n,a,b,c]}.$$

According to the definition of P, $P\beta^i = \beta^i M, P\delta^i = \delta^i M$. Then,

$$\left(\beta^i\right)^T = L_{[n,a,b,c]}\left(\delta^i\right)^T \Leftrightarrow P\beta^i = P\delta^i L_{[n,a,b,c]}.$$

Therefore, we have proved that there is a one-to-one correspondence between the differential propagation $(\delta^i, \delta^{i-1}) \rightarrow (\delta^{i+1}, \delta^i)$ and the linear propagation $(P\delta^{i-1}, P\delta^i) \rightarrow (P\delta^i, P\delta^{i+1})$.

Naturally, considering i-round differential and linear propagations, we get that there is a one-to-one correspondence between the differential characteristic

$$\left(\delta^1, \delta^0\right) \rightarrow \left(\delta^2, \delta^1\right) \rightarrow \cdots \rightarrow \left(\delta^{i+1}, \delta^i\right)$$

and the linear trail

$$\left(P\delta^0, P\delta^1\right) \rightarrow \left(P\delta^1, P\delta^2\right) \rightarrow \cdots \rightarrow \left(P\delta^i, P\delta^{i+1}\right).$$

Since constructing impossible differentials and zero correlation linear hulls of SIMON are based on bit-level contractions in this paper, $(\delta^1, \delta^0) \rightarrow (\delta^{r+1}, \delta^r)$ is an impossible differential if and only if $(P\delta^0, P\delta^1) \rightarrow (P\delta^r, P\delta^{r+1})$ is a zero correlation linear hull.

Appendix B. An Impossible Differential

See Table 7.

Table 7. A 17-round impossible differential of SIMON$[1, 0, 2]$ with 32-bit block size

Round	Left	Right
0	0000000000000000	0000000000000001
1	0000000000000001	0000000000000000
2	00000000000001λλ	0000000000000001
3	000000000001λλλλ	00000000000001λλ
4	0000000001λλλλλλ	000000000001λλλλ
5	00000001λλλλλλλλ	0000000001λλλλλλ
6	000001λλλλλλλλλλ	00000001λλλλλλλλ
7	0001λλλλλλλλλλλλ	000001λλλλλλλλλλ
8	01λλλλλλλλλλλλλλ	0001λλλλλλλλλλλλ
9	λλλλλλλλλλλλλλλλ	0**1**λλλλλλλλλλλλλλ
8	λ0001λλλλλλλλλλλ	λ**0**1λλλλλλλλλλλλλ
7	λ000001λλλλλλλλλ	λ0001λλλλλλλλλλλ
6	λ00000001λλλλλλλ	λ000001λλλλλλλλλ
5	λ0000000001λλλλλ	λ00000001λλλλλλλ
4	λ000000000001λλλ	λ0000000001λλλλλ
3	λ00000000000001λ	λ000000000001λλλ
2	1000000000000000	λ00000000000001λ
1	0000000000000000	1000000000000000
0	1000000000000000	0000000000000000

References

1. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_31
2. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23951-9_22
3. Wu, W., Zhang, L.: LBlock: a lightweight block cipher. In: Lopez, J., Tsudik, G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 327–344. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21554-4_19
4. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: *Piccolo*: an ultra-lightweight blockcipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 342–357. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23951-9_23
5. Borghoff, J., et al.: PRINCE – a low-latency block cipher for pervasive computing applications. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_14
6. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404 (2013). http://eprint.iacr.org/
7. Abed, F., List, E., Lucks, S., Wenzel, J.: Differential cryptanalysis of round-reduced Simon and Speck. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 525–545. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46706-0_27
8. Biryukov, A., Roy, A., Velichkov, V.: Differential analysis of block ciphers SIMON and SPECK. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 546–570. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46706-0_28
9. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 158–178. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_9
10. Abdelraheem, M.A., Alizadeh, J., Alkhzaimi, H.A., Aref, M.R., Bagheri, N., Gauravaram, P.: Improved linear cryptanalysis of reduced-round SIMON-32 and SIMON-48. In: Biryukov, A., Goyal, V. (eds.) INDOCRYPT 2015. LNCS, vol. 9462, pp. 153–179. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-26617-6_9
11. Chen, H., Wang, X.: Improved linear hull attack on round-reduced Simon with dynamic key-guessing techniques. In: Peyrin, T. (ed.) FSE 2016. LNCS, vol. 9783, pp. 428–449. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-52993-5_22
12. Raddum, H.: Algebraic analysis of the simon block cipher family. In: Lauter, K., Rodríguez-Henríquez, F. (eds.) LATINCRYPT 2015. LNCS, vol. 9230, pp. 157–169. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22174-8_9

13. Wang, Q., Liu, Z., Varıcı, K., Sasaki, Y., Rijmen, V., Todo, Y.: Cryptanalysis of reduced-round SIMON32 and SIMON48. In: Meier, W., Mukhopadhyay, D. (eds.) INDOCRYPT 2014. LNCS, vol. 8885, pp. 143–160. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-13039-2_9
14. Sun, L., Fu, K., Wang, M.: Improved zero-correlation cryptanalysis on SIMON. In: Lin, D., Wang, X.F., Yung, M. (eds.) Inscrypt 2015. LNCS, vol. 9589, pp. 125–143. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-38898-4_8
15. Todo, Y., Morii, M.: Bit-based division property and application to Simon family. In: Peyrin, T. (ed.) FSE 2016. LNCS, vol. 9783, pp. 357–377. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-52993-5_18
16. Xiang, Z., Zhang, W., Bao, Z., Lin, D.: Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 648–678. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_24
17. Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G.: The Simeck family of lightweight block ciphers. In: Güneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 307–329. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48324-4_16
18. Bagheri, N.: Linear cryptanalysis of reduced-round SIMECK variants. In: Biryukov, A., Goyal, V. (eds.) INDOCRYPT 2015. LNCS, vol. 9462, pp. 140–152. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-26617-6_8
19. Kölbl, S., Roy, A.: A brief comparison of Simon and Simeck. Cryptology ePrint Archive, Report 2015/706 (2015). http://eprint.iacr.org/
20. Kondo, K., Sasaki, Y., Iwata, T.: On the design rationale of Simon block cipher: integral attacks and impossible differential attacks against Simon variants. In: Manulis, M., Sadeghi, A.-R., Schneider, S. (eds.) ACNS 2016. LNCS, vol. 9696, pp. 518–536. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39555-5_28
21. Zhang, H., Wu, W.: Structural evaluation for Simon-like designs against integral attack. In: Bao, F., Chen, L., Deng, R.H., Wang, G. (eds.) ISPEC 2016. LNCS, vol. 10060, pp. 194–208. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-49151-6_14
22. Kölbl, S., Leander, G., Tiessen, T.: Observations on the SIMON block cipher family. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 161–185. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_8
23. Knudsen, L.R.: DEAL-a 128-bit block cipher. Technical report, Department of Informatics, University of Bergen, Norway (1998)
24. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_2
25. Kim, J., Hong, S., Lim, J.: Impossible differential cryptanalysis using matrix method. Discrete Math. **310**(5), 988–1002 (2010)
26. Luo, Y., Lai, X., Wu, Z., Gong, G.: A unified method for finding impossible differentials of block cipher structures. Inf. Sci. **263**, 211–220 (2014)
27. Wu, S., Wang, M.: Automatic search of truncated impossible differentials for word-oriented block ciphers. In: Galbraith, S., Nandi, M. (eds.) INDOCRYPT 2012. LNCS, vol. 7668, pp. 283–302. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34931-7_17

28. Bogdanov, A., Rijmen, V.: Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Des. Codes Crypt. **70**(3), 369–383 (2014)
29. Sun, B., Liu, Z., Rijmen, V., Li, R., Cheng, L., Wang, Q., Alkhzaimi, H., Li, C.: Links among impossible differential, integral and zero correlation linear cryptanalysis. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 95–115. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_5
30. Zhang, K., Guan, J., Hu, B., Lin, D.: Security evaluation on Simeck against zero correlation linear cryptanalysis. Cryptology ePrint Archive, Report 2015/911 (2015). http://eprint.iacr.org/
31. AlTawy, R., Rohit, R., He, M., Mandal, K., Yang, G., Gong, G.: sLiSCP: Simeck-based permutations for lightweight sponge cryptographic primitives. Cryptology ePrint Archive, Report 2017/747 (2017). http://eprint.iacr.org/