Hindawi
IET Information Security
Volume 2024, Article ID 6164262, 14 pages
https://doi.org/10.1049/2024/6164262

Research Article

Automated Differential-Linear Cryptanalysis for AND-RX Ciphers

Wenya Li, Kai Zhang, and Bin Hu

PLA SSF Information Engineering University, Zhengzhou 450001, China

Correspondence should be addressed to Kai Zhang; zhkai2010@139.com

Received 26 September 2023; Revised 27 December 2023; Accepted 6 May 2024; Published 21 May 2024

Academic Editor: Yong Yu

Differential and linear cryptanalysis are two important methods to evaluate the security of block ciphers. Building on these two methods, differential-linear (DL) cryptanalysis was introduced by Langford and Hellman in 1994. This cryptanalytic method has been not only extensively researched but also proven to be effective. In this paper, a security evaluation framework for AND-RX ciphers against DL cryptanalysis is proposed, which is denoted as $\mathscr{K}6$. In addition to modeling the structure of all the possible differential trails and linear trails at the bit level, we introduce a method to calculate this structure round by round. Based on this approach, an automatic algorithm is proposed to construct the DL distinguisher. Unlike previous methods, $\mathscr{K}6$ uses a truncated differential and a linear hull instead of a differential characteristic and a linear approximation, which brings the bias of the DL distinguisher close to the experimental value. To validate the effectiveness of the framework, $\mathscr{K}6$ is applied to Simon and Simeck, which are two typical AND-RX ciphers. With the automatic algorithm, we discover an 11-round DL distinguisher of Simon32 with bias $2^{-14.89}$ and a 12-round DL distinguisher of Simeck32 with bias $2^{-14.89}$. Moreover, the 14-round DL distinguisher of Simon48 with bias $2^{-22.30}$ is longer than the longest DL distinguisher currently known. In addition, the framework $\mathscr{K}6$ shows advantages when analyzing ciphers with large block sizes. As far as we know, for Simon64/96/128 and Simeck48/64, the first DL distinguishers are obtained with our framework. The DL distinguishers are 16, 23, 32, 17, and 22 rounds of Simon64/96/128 and Simeck48/64 with bias $2^{-24.31}$, $2^{-47.57}$, $2^{-60.75}$, $2^{-22.54}$, and $2^{-31.41}$, respectively. To prove the correctness of distinguishers, experiments on Simon32 and Simeck32 have been performed. The experimental bias are $2^{-13.76}$ and $2^{-14.82}$, respectively. Comparisons of the theoretical and experimental results show good agreement.

1. Introduction

1.1. Background. Differential and linear cryptanalysis are two powerful techniques for analyzing the security of block ciphers. Differential cryptanalysis was first proposed by Biham and Shamir [1], and linear cryptanalysis was introduced by Matsui [2]. While avoiding long differential characteristics and linear approximations seems to be sufficient for the cipher against differential and linear cryptanalysis, it turns out that short characteristics and approximations can also be utilized to break the cipher. Differential-linear (DL for short) cryptanalysis proposed by Langford and Hellman in 1994 [3] first demonstrates this fact. In 2002, Biham et al. [4] presented an enhancement of DL cryptanalysis, which is based on two independence assumptions. Several subsequent papers aimed at taking into consideration multiple linear approximations instead of a single one and at formalizing the assumption. Liu et al. [5] and Lu [6] are the research results of the former research direction. In 2017, Blondeau et al. [7] gave an exact expression of the bias under the sole assumption that the two parts of the cipher are independent. Some cryptanalysts have studied DL cryptanalysis from other perspectives. In 2019, Bar-On et al. [8] took into account the dependency between the differential and linear approximation and presented the Differential-Linear Connectivity Table to get a more accurate bias of the DL distinguisher. In 2021, Liu et al. [9] developed a new theory of estimation of the DL bias from an algebraic perspective.

AND-RX cipher is a class of symmetric primitives that consists of three operations—AND, Rotation, and XOR. There are many AND-RX ciphers, such as Simon and Simeck. Simon [10] is a family of lightweight block ciphers published by the

Table 1: Summary of all DL distinguishers of Simon and Simeck.

Cipher	Block size	Length of distinguisher	Bias	Reference
Simon	32	15[†]	$2^{-30.36}$	[13]
		13[‡]	2^{-13}	[14]
		12[*]	$2^{-12.69}$	[15]
		11	$2^{-14.89}$	Section 4.1
	48	13	2^{-21}	[14]
		14	$2^{-22.30}$	Section 4.1
	64	16	$2^{-24.31}$	Section 4.1
	96	23	$2^{-47.57}$	Section 4.1
	128	32	$2^{-60.75}$	Section 4.1
Simeck	32	13[*]	$2^{-14.03}$	[15]
		12	$2^{-14.89}$	Section 4.2
	48	17	$2^{-22.54}$	Section 4.2
	64	22	$2^{-31.41}$	Section 4.2

[†] The number of plaintexts required by this distinguisher exceeds the total number of plaintexts. [‡] There is a mistake in this distinguisher. The output difference for the fourth round should be (∗∗∗0 ∗01∗ ∗∗∗∗ 0000 00∗∗ 0000 1∗∗0 ∗000) instead of (0∗∗0 ∗010 ∗∗∗∗ 0000 00∗∗ 0000 1∗∗0 ∗000).
[*] The two results are obtained by experiments and lack theoretical analysis.

National Security Agency in 2013. Due to the Feistel structure and simple round function, Simon has significant advantages in terms of hardware implementation. Inspired by this design idea, Yang et al. [11] presented another family of lightweight block ciphers, named Simeck, in which only the rotation constant and key schedule are different from Simon.

1.2. Related Work. In recent years, there have been more and more security evaluations on the symmetric primitives against DL cryptanalysis, such as attacks on Serpent (AES finalist, 1999) [6, 8, 9, 12] and Ascon (CAESAR finalist, 2014) [8, 9]. For AND-RX ciphers, there are some results on Simon and Simeck.

In 2018, the first DL cryptanalysis of Simon was proposed by Chen and Zhang [13]. They constructed a 15-round DL distinguisher of Simon32 with bias $2^{-30.36}$, which is too small to produce an effective attack. In 2022, Hu et al. [14] constructed a 13-round DL distinguisher of Simon32 with bias 2^{-13} (a mistake is shown in the note in Table 1) and a 13-round DL distinguisher of Simon48 with bias 2^{-21}, which led to a 16-round attack on Simon32 and a 16-round attack on Simon48, respectively. The DL distinguishers constructed above are all based on a differential characteristic and a linear approximation. In 2023, Zhang et al. [15] used statistical analysis to search for suitable DL distinguishers of Simon32 and Simeck32. They found a 12-round DL distinguisher of Simon32 with bias $2^{-12.69}$ and a 13-round DL distinguisher of Simeck32 with bias $2^{-14.03}$. Then, attacks against 20-round Simon32 and 21-round Simeck32 can be obtained with the distinguishers, respectively. However, statistical analysis is useless for Simon and Simeck, with a block size greater than 32.

Traceablepattern was first proposed in [16]. Until now, *traceablepattern* has been applied to several cryptanalytic methods, and many good distinguishers are obtained by this technique. For a meet-in-the-middle attack, a general automatic framework $\mathscr{K}2$ was proposed with the splice-and-cut technique [17]. For impossible differential cryptanalysis, an automatic framework $\mathscr{K}3$ was constructed for AND-RX ciphers [18]. For rotational-XOR differential cryptanalysis, an automatic framework $\mathscr{K}5$ was proposed for AND-RX ciphers in [19]. Actually, this paper is a continuation of our teem's series of work. We focus on the application of *traceablepattern* to DL cryptanalysis and establish an automatic framework $\mathscr{K}6$ to search for the DL distinguisher of AND-RX ciphers.

1.3. Our Contributions. In this paper, our overall contribution is establishing an automatic framework $\mathscr{K}6$ to construct the distinguisher and evaluate the security of AND-RX cipher against DL cryptanalysis. The specific implementation includes the following three aspects.

(1) Model the structure for all the possible DL trails

For difference and mask, the concept of *traceablepattern* is proposed to describe the structure at the bit level. The *patternoperation* is presented to characterize the propagation rules of the *traceablepattern* between different components —AND, Rotation, and XOR. Further, the structure for the possible DL trails is modeled.

(2) Establish an automatic framework to construct the DL distinguisher

Based on *traceablepattern* and *patternoperation*, combined with DL cryptanalysis, an automatic framework, denoted $\mathscr{K}6$, is proposed to construct the DL distinguisher. According to the input difference and *patternoperation*, the truncated differential can be calculated round by round. The probability of truncated differential is 1 larger than that of differential characteristic. Similarly, according to the input mask, the output mask, and *patternoperation*, the linear hull is represented with *traceablepatterns*. The correlation of linear hull is calculated by summing the correlations of all linear approximations, so it is larger than that of only one linear approximation. If it is difficult to calculate the correlation of linear hull, the cipher can be decomposed into a cascade of several subciphers to reduce the search space. Further, the space of all the possible DL trails is obtained, and the bias of the DL distinguisher is calculated with Matsui's Piling-up lemma. Namely, the DL distinguisher built with $\mathscr{K}6$ consists of a truncated differential and a linear hull instead of a differential characteristic and a linear approximation. This method of constructing the DL distinguisher is different from the previous analysis. Theoretically, it makes the theoretical bias of the DL distinguisher close to the experimental value. Moreover, since the search space is reduced by decomposing the cipher into a cascade of several subciphers, our framework is suitable for ciphers with large block sizes. Some of the previous methods are not applicable.

(3) Apply and verify

To show the effectiveness of $\mathscr{K}6$, Simon and Simeck, the two famous AND-RX ciphers, are investigated. Among the results of all block sizes, the DL distinguisher of Simon48 is 14

TABLE 2: Notations in this paper.

Notation	Description
Simon n	Simon with block size n, $n \in \{32, 48, 64, 96, 128\}$
Simeck n	Simeck with block size n, $n \in \{32, 48, 64\}$
$S_i = (S_i^L, S_i^R)$	Intermediate value of the ith round
$X_i = (X_i^L, X_i^R)$	Difference of the ith round
$Y_i = (Y_i^L, Y_i^R)$	Mask of the ith round
TP_x	Difference/mask of x represented with *traceablepattern*
RK_i	Subkey of the ith round
&	Bitwise AND
$\lll$	Left rotation
$\oplus$	Bitwise XOR

rounds, which is longer than the current longest DL distinguisher. As far as we know, for Simon64/96/128 and Simeck48/64, the DL distinguishers proposed in this paper are the first DL distinguishers. The comparisons with previous results are in Table 1.

To prove the correctness of the DL distinguishers, experimental verifications on Simon32 and Simeck32 are given. The experimental bias of the 11-round distinguisher of Simon32 is $2^{-13.76}$, and the experimental bias of the 12-round distinguisher of Simeck32 is $2^{-14.82}$. The experimental results match the theoretical analysis well.

1.4. Organization of the Paper. The rest of this paper is organized as follows. In Section 2, we give an overview of DL cryptanalysis and provide detailed descriptions of Simon and Simeck. In Section 3, we propose an automatic framework to search for the DL distinguisher of AND-RX ciphers. In Section 4, we apply the framework to Simon and Simeck. In Section 5, we summarize this paper.

2. Preliminaries

2.1. Notations. The notations used in this paper are illustrated in Table 2.

2.2. DL Cryptanalysis. Let $E : \{0, 1\}^n \rightarrow \{0, 1\}^n$ be an r-round cipher that can be decomposed into a cascade $E = E_1 \circ E_0$, as shown in Figure 1, where E_0 and E_1 consist of r_0 and r_1 rounds, respectively. Assume that there is a differential characteristic $X_0 \xrightarrow{p} X_{r_0}$ for E_0, namely an input difference X_0 to E_0 leads to an output difference X_{r_0} from E_0 with probability as follows:

$$p = \frac{\#\{S | E_0(S) \oplus E_0(S \oplus X_0) = X_{r_0}, S \in \{0, 1\}^n\}}{2^n}. \tag{1}$$

Similarly, assume that there also is a linear approximation $Y_{r_0} \xrightarrow{c} Y_r$ for E_1, namely a random input/output pair (S_{r_0}, S_r) of E_1 satisfies $Y_{r_0} \cdot S_{r_0} = Y_r \cdot S_r$ with correlation as follows:

$$c = 2\left(\frac{\#\{S | S \cdot Y_{r_0} = E_1(S) \cdot Y_r, S \in \{0, 1\}^n\}}{2^n} - \frac{1}{2}\right). \tag{2}$$

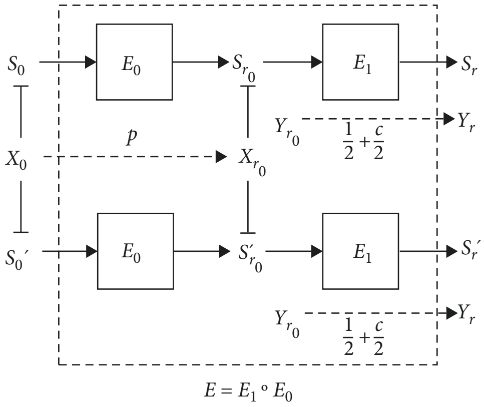


FIGURE 1: General structure for differential-linear cryptanalysis.

In order to distinguish E from a random permutation with DL cryptanalysis, the adversary needs to obtain the bias by checking whether the pairs (S_r, S_r') satisfy $Y_r \cdot S_r = Y_r \cdot S_r'$ when the pairs (S_0, S_0') satisfy $S_0 \oplus S_0' = X_0$. The bias of the r-round DL distinguisher $X_0 \xrightarrow{\varepsilon} Y_r$ is defined as follows:

$$\varepsilon = \frac{\#\{S | E(S) \cdot Y_r = E(S \oplus X_0) \cdot Y_r, S \in \{0, 1\}^n\}}{2^n} - \frac{1}{2}. \tag{3}$$

Since the cipher behaves randomly, assume that $Y_r \cdot S_r = Y_r \cdot S_r'$ holds in half of the cases where the pairs do not satisfy the difference. Therefore, the overall bias of the DL distinguisher is as follows:

$$\varepsilon = 2p\left(\frac{c}{2}\right)^2 = \frac{1}{2}pc^2. \tag{4}$$

Therefore, the adversary can distinguish E from a random permutation with $\mathcal{O}(p^{-2}c^{-4})$ chosen plaintexts when p, c are sufficiently large.

In general, the correlation of an r_1-round linear trail is calculated as follows:

$$c_{trail} = \prod_{j=1}^{r_1} c_j, \tag{5}$$

where c_j is the correlation of the linear approximation $Y_{j-1} \rightarrow Y_j$, and the correlation of an r_1-round linear hull $Y_0 \rightarrow Y_{r_1}$ is calculated as follows:

$$c_{hull} = \sum_{Y_1, Y_2, \ldots Y_{r_1 - 1}} c_{trail}. \tag{6}$$

Usually, c_{hull} for E_1 is hard to evaluate, but it matches the experimental value much more than c_{trail}. Note that many previous analyses take c_{trail} as the correlation for E_1.

Table 3: Parameters of Simon and simeck.

Cipher	Block size	Key size	Rounds
Simon	32	64	32
	48	72	36
		96	36
	64	96	42
		128	44
	96	96	52
		144	54
	128	128	68
		192	69
		256	72
Simeck	32	64	32
	48	96	36
	64	128	44

However, the framework $\mathscr{K}6$ allows the adversary to take into account c_{hull} for E_1.

Moreover, if the linear approximation for E_1 is made by concatenating several short-round linear approximations, according to Matsui's Piling-up lemma [2], the correlation is calculated as follows:

$$c = \prod_{j=0}^{m} c^j, \tag{7}$$

where $E_1 = E_1^m \circ \ldots \circ E_1^0$, and the correlation of the linear approximation for E_1^j is $c^j, j \in \{0, 1, \ldots, m\}$.

2.3. Descriptions of Simon and Simeck. Both Simon and Simeck are lightweight block ciphers with the Feistel structure. Based on the block size and key size, Simon has 10 versions, and Simeck has 3. The parameters are shown in Table 3. Cryptographers often omit the key size and denote the two ciphers as Simon$n$ with block size n, $n \in \{32, 48, 64, 96, 128\}$ and Simeck$n$ with block size n, $n \in \{32, 48, 64\}$. The intermediate value of the ith round S_i is divided into two parts with $\frac{n}{2}$ bits named S_i^L and S_i^R. They correspond to intermediate values of the left and right parts of the Feistel structure. Simon follows a very simple round function:

$$S_{i+1}^R = S_i^L, \tag{8}$$

$$S_{i+1}^L = S_i^R \oplus f(S_i^L) \oplus RK_{i+1}, \tag{9}$$

$$f(x) = ((x \lll 1) \& (x \lll 8)) \oplus (x \lll 2). \tag{10}$$

Simeck has the same round function but with different rotation constants:

$$f(x) = (x \& (x \lll 5)) \oplus (x \lll 1). \tag{11}$$

The round functions of Simon and Simeck are depicted in Figure 2.

3. Automatic Search for the DL Distinguisher of AND-RX Ciphers

In this section, an automatic framework is established to search for the DL distinguisher of AND-RX ciphers, denoted as $\mathscr{K}6$. First, the general idea of the framework is introduced, then the main techniques used in this framework are presented, and finally, the details for this method are illustrated in the Algorithm.

3.1. Overview of the Framework. In general, a high-probability differential characteristic for E_0 and a high-correlation linear approximation for E_1 can be combined into an efficient DL distinguisher for the entire cipher E. Based on this fact, we construct the DL distinguisher by concatenating a truncated differential ($p = 1$) and a linear hull. Theoretically, the theoretical bias of the distinguisher made by our framework matches the experimental value well. Applications in Section 4 illustrate it experimentally.

If the time complexity to calculate the correlation of the linear hull for E_1 is too large, decompose E_1 into a cascade $E_1 = E_1^m \circ \ldots \circ E_1^0$, and the correlation for E_1 can be obtained with Equation (7). According to Equation (4), the overall bias of the DL distinguisher is as follows:

$$\varepsilon = \frac{1}{2}\left(\prod_{j=0}^{m} c_{hull}^{j}\right)^2, \tag{12}$$

where c_{hull}^j is the correlation of the linear hull for E_1^j.

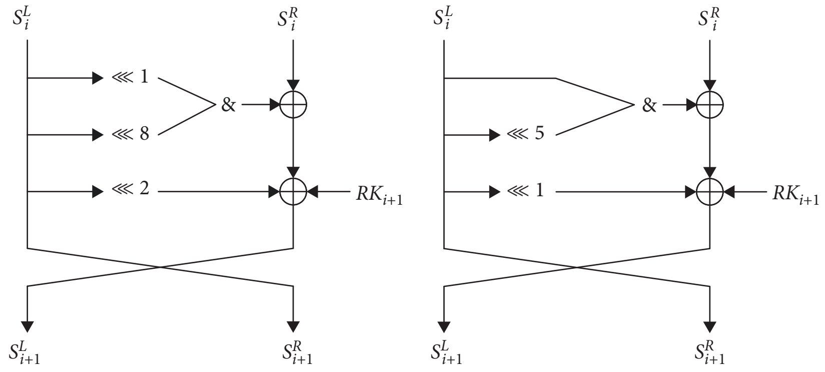
3.2. Traceable pattern for DL Cryptanalysis. To accurately describe the structure of the differential and linear trail at the bit level, we present a concept of *traceable pattern* for DL cryptanalysis. Meanwhile, to characterize the propagation property of the difference and linear mask between different cipher modules, the *pattern operation* for AND-RX ciphers is introduced. Based on the *traceable pattern* and *pattern operation*, we can construct a DL distinguisher and calculate its bias.

For all possible trails, the difference/mask of each state bit is generally 0, 1, or uncertain. To depict this property, we define the *traceable pattern* at the bit level, as shown in Table 4. Notice that the *traceable pattern* is equal to the difference/mask of the bit when the difference/mask is 0 or 1.

In this way, the difference/mask of each bit of the intermediate state can be accurately described by a *traceable pattern*. If the *traceable pattern* can be calculated round by round, the space comprised of all possible differential trails and linear trails can be derived. Therefore, in order to model the calculating rule between *traceable patterns*, we define the *pattern operation* for the differential part, the linear part, and the connected part. Since AND-RX ciphers contain only three possible operations—AND, Rotation, and XOR, we only consider *pattern operation* for these operations.

(1) Differential part

AND: If $z = x \& y$, $TP_z = TP_x \widehat{\&} TP_y$.
Rotation: If $y = x \lll r$, $TP_y = TP_x \lll r$.



(a)

(b)

Figure 2: Round functions of Simon (a) and Simeck (b).

Table 4: *Traceable pattern* for DL cryptanalysis.

Traceable pattern	Description
0	The difference/mask of this bit is 0
1	The difference/mask of this bit is 1
2	The difference/mask of this bit is uncertain

Table 5: Calculating rules for $\widehat{\&}$ and $\widehat{\oplus}$.

$\widehat{\&}$	**0**	**1**	**2**
0	0	2	2
1	2	2	2
2	2	2	2

$\widehat{\oplus}$	**0**	**1**	**2**
0	0	1	2
1	1	0	2
2	2	2	2

XOR: If $z = x \oplus y$, $TP_z = TP_x \widehat{\oplus} TP_y$.

The bitwise calculating rules for $\widehat{\&}$ and $\widehat{\oplus}$ are illustrated in Table 5.

(2) Linear part

AND: If $x\&y = z$, $(TP_x, TP_y) = \widehat{\&}^{-1}(TP_z)$.

Rotation: If $y = x \lll r$, $TP_y = TP_x \lll r$.

XOR: If $z = x \oplus y$, $TP_z = TP_x \widehat{\oplus} TP_y$.

According to the calculating rules for $\widehat{\&}$, $\widehat{\&}^{-1}$ is illustrated in Table 6.

(3) Connected Part

Let $S^0 = (s_1^0, \ldots, s_n^0)$ be the output difference for E_0, $S^1 = (s_1^1, \ldots, s_n^1)$ be the input mask for E_1, $TP_{S^0} = (TP_{s_1^0}, \ldots, TP_{s_n^0})$, and $TP_{S^1} = (TP_{s_1^1}, \ldots, TP_{s_n^1})$. Then define an operation “$\widehat{\cdot}$” as $TP_{S^0} \widehat{\cdot} TP_{S^1} = \sum_{i=1}^{n} TP_{s_i^0} \times TP_{s_i^1}$. If $TP_{S^0} \widehat{\cdot} TP_{S^1} = 0$, $S^0 \cdot S^1 = 0$.

Table 6: Calculating rules for $\widehat{\&}^{-1}$.

x	**0**	**1**	**2**
$\widehat{\&}^{-1}(x)$	(0,0)	(2,2)	(2,2)

3.3. Automatic Search for the DL Distinguisher. For our automatic framework $\mathscr{K}6$, the DL distinguisher targets an $(r_0 + r_1)$ -round AND-RX cipher denoted by E. It can be decomposed as $E = E_1 \circ E_0$, where E_0 consists of r_0 rounds, and E_1 consists of r_1 rounds.

For the differential part E_0, TP_{X_0} is equal to X_0. According to the *pattern operation*, TP_{X_i} can be accurately calculated round by round. In particular, using a distinguisher with a single active bit in the input and output can make the adversary add more rounds of key-recovery than using a distinguisher with multiple active bits. Therefore, the longest truncated differential is obtained by exhaustive searching TP_{X_0} with a single active bit. In other words, there is only one bit with $TP = 1$, and all the other bits have $TP = 0$ in X_0. The longest truncated differential is obtained with the difference part in the Algorithm. Therefore, for E_0, the probability p is equal to 1, and $r_0 = r_{\max}$.

For the connected part, $TP_{X_{r_0}} \widehat{\cdot} TP_{Y_0}$ should be equal to 0. According to the output difference $TP_{X_{r_0}}$ of E_0, there may be multiple masks that meet the conditions. For instance, if $TP_{X_{r_0}}$ is (2,2,2,2,2,2,0,0), TP_{Y_0} can be (0,0,0,0,0,0,0,1), (0,0,0,0,0,0,1,0), or (0,0,0,0,0,0,1,1). However, (0,0,0,0,0,0,0,1) and (0,0,0,0,0,0,1,0) will lead to a much longer distinguisher (because they have fewer active bits). Therefore, we choose the mask with fewer active bits as the input mask $Y_0 (= TP_{Y_0})$ of E_1 in the following part.

For the linear part E_1, we focus on how to search for a high-correlation linear hull with input mask Y_0 and calculate its correlation. First, using the algorithm of searching for the optimal linear trail and the method of calculating the correlation of the round function, we can select one target round number R and the corresponding output mask Y_R. Then, the space of all possible linear trails can be determined with the round function and *pattern operation*. Finally, the correlation of the linear hull $Y_0 \rightarrow Y_R$ can be obtained by calculating

```
Input: the round function of target cipher
output: the DL distinguisher
Preliminary:
1: Search for the optimal linear trail of the target cipher;
2: Set the formula for calculating the correlation of the target cipher round function;
Differential part:
Step 1: Let $X=(0,\ldots,0,1)$, $X_{\max}=(0,\ldots,0)$, $r_{\max}=0$, and $num=0$.
Step 2: For $a\in\{0,1,\ldots,n-1\}$
        Let $X_0=X\lll a$, and $r=0$. If $num\neq n$, do the following substeps.
            Substep 1: Let $r\leftarrow r+1$.
            Substep 2: Calculate $TP_{X_r}$ according to the round function and pattern operation in the encryption direction;
            Substep 3: Count the traceable pattern "2" in $TP_{X_r}$ and denote as num;
        If $r-1>r_{\max}$, let $r_{\max}=r-1$, and $X_{\max}=X_0$.
Step 3: Let $X_0=X_{\max}$. Output $TP_{X_0}(=X_0)$ and $TP_{X_i}=R(TP_{X_{i-1}})$, $i\in\{1,2,\ldots,r_{\max}\}$.
Connected part:
Step 4: Choose the mask $Y_0(=TP_{Y_0})$ which satisfies $TP_{X_{r_0}}\widehat{\cdot}TP_{Y_0}=0$ as the input mask in the following part.
Linear part:
Step 5: According to Preliminary 1 and 2, select one optimal linear trail with target round number $R$, the input mask $Y_0$, and the output
        mask $Y'_R$.
Step 6: For $i=0; i<R; i++$
            Calculate $Y_{i+1}$ according to the round function and pattern operation in the encryption direction.
        Let $\mathscr{Y}=\{Y_i, i=0,\ldots,R\}$, which is the space of all possible linear trails with round number $R$ and input mask $Y_0$.
Step 7: For $i=R; i>0; i--$
            Calculate $Y'_{i-1}$ according to the round function and pattern operation in the decryption direction.
        Let $\mathscr{Y}'=\{Y'_i, i=0,\ldots,R\}$, which is the space of all possible linear trails with the round number $R$ and output mask $Y'_R$.
Step 8: Obtain the space of all possible linear trails with round number $R$, input mask $Y_0$, and output mask $Y'_R$ by calculating the
        intersection of $\mathscr{Y}$ and $\mathscr{Y}'$. Count the traceable pattern "2" in this space and denote it as num.
Step 9: Calculate the correlations of all possible linear trails in the space, namely the correlation of linear hull with round number $R$,
        input mask $Y_0$, and output mask $Y'_R$.
Step 10: If num is too large to fulfill Step 9, decompose the initial optimal linear trail into several parts. Then perform Steps 5–9 for each
         part, respectively. Finally, calculate the overall correlation $c$ by using Matsui's Piling-up lemma.
```

ALGORITHM 1: Automatic search for the DL distinguisher for AND-RX ciphers.

the correlation of every trail in this space and summing them up. However, there may be a case where there are so many trails in the space that it is impossible to calculate the correlation of every trail. In this case, we can decompose the optimal linear trail into a cascade and calculate the correlation of each part by the above steps. The integral correlation for E_1 can be obtained by using Equation (7). Moreover, if the integral bias for E does not achieve expectation (such as too small a bias like the bias in [13]), we can choose a new R to calculate again. Denote the final round number as r_1 and the corresponding correlation as c. All details are in the linear part of the Algorithm.

In summary, we obtain an r_0+r_1-round DL distinguisher which consists of an r_0-round truncated differential with probability 1 and an r_1-round linear hull with correlation c. According to Equation (4), the bias of the DL distinguisher is as follows:

$$\varepsilon=\frac{1}{2}c^2. \tag{13}$$

4. Applications

In order to show the effectiveness of our framework $\mathscr{K}6$, applications to Simon and Simeck, two typical AND-RX ciphers, are presented. The aim is also to evaluate the security of Simon and Simeck of all block sizes against DL cryptanalysis. In addition to constructing DL distinguishers of Simon32, Simon48, and Simeck32, we obtain the first DL distinguishers of Simon64, Simon96, Simon128, Simeck48, and Simeck64.

4.1. Application to Simon. For the Simon family, the differential part of the DL distinguisher can be obtained with the Algorithm. The input and output differences represented with *traceablepatterns* are shown in Table 7. Details of the trails are exhibited in the Appendix.

Before searching for the linear hull of Simon, Algorithm 1 in [20] can help us obtain the initial optimal linear trail needed in the preliminary of the Algorithm. Meanwhile, we utilize Algorithm 2 in [20] to calculate the correlation of the

Table 7: The truncated differentials of Simon represented with *traceable patterns*.

Cipher	Rounds	$TP_{X_0}(=X_0)$	$TP_{X_{r_0}}$
Simon32	6	$(0000000000000000, 0000000000000010)$	$(2222222222222222, 2222221222222020)$
Simon48	7	$(000000000000000000000000,$ $000000000000000000000010)$	$(222222222222222222222222,$ $222222222222222222222220)$
Simon64	8	$(00000000000000000000000000000000,$ $00000000000000000000000000000010)$	$(22222222222222222222222222222222,$ $22222222222222222222222222222020)$
Simon96	10	$(000000000000000000000000$ $000000000000000000000000,$ 000000000000000000000000 $000000000000000000000010)$	$(222222222222222222222222$ $222222222222222222222222,$ 222222222222222222222222 $222222222222222222222020)$
Simon128	12	$(00000000000000000000000000000000$ $00000000000000000000000000000000,$ $00000000000000000000000000000000$ $00000000000000000000000000000010)$	$(22222222222222222222222222222222$ $22222222222222222222222222222222,$ $22222222222222222222222222222222$ $22222222222222222222222222222020)$

Table 8: The linear hulls of Simon in hexadecimal notation.

Cipher	Rounds	The input mask	The output mask	Bias	Time (s)
Simon32	0–5	$(0000, 0001)$	$(1101, 4040)$	$2^{-13.89}$	0.004
Simon48	0–7	$(000000, 000001)$	$(011001, 000400)$	$2^{-21.30}$	11.314
Simon64	0–8	$(00000000, 00000001)$	$(00040000, 01110001)$	$2^{-23.31}$	184.785
Simon96	0–6	$(000000000000, 000000000001)$	$(404000000000, 011000000001)$	$2^{-17.46}$	0.092
	6–13	$(404000000000, 011000000001)$	$(100000000001, 400000000000)$	$2^{-15.56}$	30,732.442
Simon128	0–7	$(0000000000000000, 0000000000000001)$	$(0110000000000001, 0184000000000000)$	$2^{-21.31}$	15.045
	7–14	$(0110000000000001, 0184000000000000)$	$(4000000000000000, 0000000000000001)$	$2^{-14.62}$	3,942.410
	14–20	$(4000000000000000, 0000000000000001)$	$(0400000000000000, 1100000000000001)$	$2^{-6.60}$	0.015

Table 9: The DL distinguishers of Simon in hexadecimal notation.

Cipher	Rounds	The input difference	The output mask	Bias
Simon32	11	$(0000, 0002)$	$(1101, 4040)$	$2^{-14.89}$
Simon48	14	$(000000, 000002)$	$(011001, 000400)$	$2^{-22.30}$
Simon64	16	$(00000000, 00000002)$	$(00040000, 01110001)$	$2^{-24.31}$
Simon96	23	$(000000000000, 000000000002)$	$(100000000001, 400000000000)$	$2^{-47.57}$
Simon128	32	$(0000000000000000, 0000000000000002)$	$(0400000000000000, 1100000000000001)$	$2^{-60.75}$

round function of Simon. For Simon32, Simon48, and Simon64, an appropriate linear hull can be constructed without decomposing the initial optimal linear trail. For Simon96 and Simon128, the trail is decomposed into several parts. The linear hulls are described in Table 8. The space of all possible linear trails represented with *traceable patterns* is exhibited in the Appendix.

Review the description of DL cryptanalysis in Section 2.2; the DL distinguishers of the Simon family are constructed in Table 9. For the framework $\mathscr{K}6$, the bias of the DL distinguisher can be calculated by Equation (13). To validate the correctness of $\mathscr{K}6$, experiments are performed on an 11-round distinguisher of Simon32. The experimental results closely match the theoretical analysis (Table 10). In practice, the Algorithm runs on a 12-core personal laptop with 16 GB of RAM.

4.2. Application to Simeck

4.2. Application to Simeck. For Simeck with all block sizes, the input and output differences of the longest truncated differential are represented with *traceable patterns* and shown in Table 11. Details of the differential part are displayed in the Appendix.

For Simeck, the methods of obtaining the initial optimal linear trail and calculating the correlation of the round function are the same as the methods for Simon. With the framework $\mathscr{K}6$, a linear hull of Simeck32 is obtained without decomposing the initial optimal linear trail. However, for Simeck48 and Simeck64, the initial trail is decomposed into two parts, respectively. The linear hulls are given in Table 12. The space of all possible linear trails represented with *traceable patterns* can be found in the Appendix.

Table 10: The experimental results of the DL distinguisher of Simon32.

Number of plaintexts	Success rate (%)	Bias	Time (s)
$2^{30.78}$	48.6	$2^{-13.93}$	153,875.467
$2^{31.78}$	78.5	$2^{-13.82}$	283,777.699
2^{32}	96.7	$2^{-13.76}$	325,313.444

Table 11: The truncated differentials of Simeck represented with *traceable patterns*.

Cipher	Rounds	$TP_{X_0}(=X_0)$	$TP_{X_{r_0}}$
Simeck32	7	(0000000000000000, 0000000000000100)	(2222222222222222, 2222222222222220)
Simeck48	8	(000000000000000000000000, 000000000000000000100000)	(222222222222222222222222, 222222222222222222202220)
Simeck64	10	(00000000000000000000000000000000, 00000000000000000000000000001000)	(22222222222222222222222222222222, 22222222222222222222222222222220)

Table 12: The linear hulls of Simeck in hexadecimal notation.

Cipher	Rounds	The input mask	The output mask	Bias	Time (s)
Simeck32	0–5	(0000, 0001)	(5001, 8000)	$2^{-13.89}$	0.009
Simeck48	0–7	(000000, 000001)	(100001, 000000)	$2^{-17.54}$	0.382
	7–9	(100001, 000000)	(100001, 800000)	$2^{-3.00}$	0.013
Simeck64	0–7	(00000000, 00000001)	(10000001, 00000000)	$2^{-17.54}$	0.441
	7–12	(10000001, 00000000)	(20000000, 40000001)	$2^{-7.44}$	0.511

Table 13: The DL distinguishers of Simeck in hexadecimal notation.

Cipher	Rounds	The input difference	The output mask	Bias
Simeck32	12	(0000, 0004)	(5001, 8000)	$2^{-14.89}$
Simeck48	17	(000000, 000020)	(100001, 800000)	$2^{-22.54}$
Simeck64	22	(00000000, 00000008)	(20000000, 40000001)	$2^{-31.41}$

Table 14: The experimental results of the DL distinguisher of Simeck32.

Number of plaintexts	Success rate (%)	Bias	Time (s)
$2^{30.78}$	48.6	$2^{-14.48}$	155,961.629
$2^{31.78}$	78.5	$2^{-14.80}$	312,643.001
2^{32}	96.7	$2^{-14.82}$	362,679.692

Table 13 is a summary of the DL distinguishers of Simeck. For Simeck32, some experiments have been performed to show whether the theoretical analysis matches the experimental result, as seen in Table 14.

5. Conclusion

In this paper, we proposed an automatic framework for constructing the DL distinguisher of AND-RX ciphers, denoted as $\mathscr{K}6$. The DL distinguisher consists of a truncated differential and a linear hull. To validate the effectiveness of our framework, some applications are demonstrated. We found 11-round, 14-round, 16-round, 23-round, 32-round, 12-round, 17-round, and 22-round DL distinguisher of Simon32, Simon48, Simon64, Simon96, Simon128, Simeck32, Simeck48, and Simeck64 with bias $2^{-14.89}$, $2^{-22.30}$, $2^{-24.31}$, $2^{-47.57}$, $2^{-60.75}$, $2^{-14.89}$, $2^{-22.54}$, and $2^{-31.41}$, respectively. The experimental bias of the 11-round distinguisher of Simon32 is $2^{-13.76}$. The experimental bias of the 12-round distinguisher of Simeck32 is $2^{-14.82}$. The experimental results match the theoretical analysis well. These applications indicate that our framework is effective for the AND-RX cipher with a large block size. In other words, the practicability of our framework is not affected by the block size of the target cipher. For instance, the time complexity of searching for the DL distinguisher of an AND-RX cipher with a large block size using the method mentioned in [15] will be larger than that using the framework $\mathscr{K}6$. Therefore, the framework $\mathscr{K}6$ is a generic method to search for the DL distinguisher of AND-RX ciphers. More block ciphers will be analyzed with this framework, which will be left as future work.

Appendix

The DL distinguishers of Simon and Simeck represented with *traceable patterns* are shown in Tables 15–22.

Table 15: The DL distinguisher of Simon32 represented with *traceable patterns*.

Round	The left part	The right part
0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
1	0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
2	0,0,0,0,0,0,2,0,0,0,0,0,1,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
3	0,0,0,0,2,2,0,0,0,0,1,2,2,0,2,0	0,0,0,0,0,0,2,0,0,0,0,0,1,2,0,0
4	0,0,2,2,2,0,2,0,1,2,2,2,2,2,0,0	0,0,0,0,2,2,0,0,0,0,1,2,2,0,2,0
5	2,2,2,2,2,2,1,2,2,2,2,2,2,0,2,0	0,0,2,2,2,0,2,0,1,2,2,2,2,2,0,0
6	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2	2,2,2,2,2,2,1,2,2,2,2,2,2,0,2,0
6	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
7	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0
8	2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0	0,2,2,1,0,0,0,0,2,2,0,0,0,0,0,2
9	0,2,2,1,0,0,0,0,2,2,0,0,0,0,0,2	2,0,0,0,2,1,0,2,0,0,0,2,0,0,0,0
10	2,0,0,0,2,1,0,2,0,0,0,2,0,0,0,0	0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,1
11	0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,1	0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0

Table 16: The DL distinguisher of Simon48 represented with *traceable patterns*.

Round	The left part	The right part
0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
1	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
2	0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,1,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
3	0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,1,2,2,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,1,2,0,0
4	0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,1,2,2,2,0,2,2,0	0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,1,2,2,0,1,0
5	0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,1,0	0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,1,2,2,2,0,2,2,0
6	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0	0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,1,0
7	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0
7	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
8	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
9	2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,2,2,1,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,1
10	0,2,2,1,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,1	2,0,2,2,2,1,0,2,0,2,2,2,0,0,0,0,2,2,0,0,0,0,0,2
11	2,0,2,2,2,1,0,2,0,2,2,2,0,0,0,0,2,2,0,0,0,0,0,2	0,2,2,2,0,0,0,1,2,2,2,0,0,2,0,2,0,2,0,0,0,0,0,1
12	0,2,2,2,0,0,0,1,2,2,2,0,0,2,0,2,0,2,0,0,0,0,0,1	2,1,0,0,0,0,0,2,2,1,0,0,2,0,0,2,0,0,0,2,0,0,0,0
13	2,1,0,0,0,0,0,2,2,1,0,0,2,0,0,2,0,0,0,2,0,0,0,0	0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,1
14	0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,1	0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0

Table 17: The DL distinguisher of Simon64 represented with *traceable patterns*.

Round	The left part	The right part
0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
1	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
2	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,1,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
3	0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,1,2,2,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,1,2,0,0
4	0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,1,2,2,2,0,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,1,2,2,0,1,0
5	0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,2,2,2,2,2,2,1,2,2,2,2,2,2,0,2,0	0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,1,2,2,2,0,2,0,0
6	0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,0	0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,2,2,2,2,2,2,1,2,2,2,2,2,2,0,2,0
7	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0	0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,0
8	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0

Table 17: Continued.

Round	The left part	The right part
8	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
9	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
10	2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,2,2,1,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
11	0,2,2,1,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,0,2,2,2,1,0,2,0,2,2,2,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0
12	2,0,2,2,2,1,0,2,0,2,2,2,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0	0,2,2,1,0,2,0,1,2,2,2,0,0,2,0,2,0,2,2,0,0,0,0,0,2,2,0,0,0,0,0,2
13	0,2,2,1,0,2,0,1,2,2,2,0,0,2,0,2,0,2,2,0,0,0,0,0,2,2,0,0,0,0,0,2	2,1,0,0,0,0,0,2,2,1,0,0,2,0,0,2,2,0,0,2,0,0,0,2,0,0,0,0,0,0,0,0
14	2,1,0,0,0,0,0,2,2,1,0,0,2,0,0,2,2,0,0,2,0,0,0,2,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,1,0,0,0,1,0,0,2,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,1
15	0,0,0,0,0,0,0,1,0,0,0,1,0,0,2,0,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,1	0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
16	0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1

Table 18: The DL distinguisher of Simon96 represented with *traceable patterns*.

Round	The left part	The right part
0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
1	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
2	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,1,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
3	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,1,2,2,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,1,2,0,0
4	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0, 0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,1,2,2,2,0,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,1,2,2,0,1,0
5	0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0, 0,0,2,2,2,0,2,0,2,2,2,2,2,2,1,2,2,2,2,2,2,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0, 0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,1,2,2,2,0,2,0,0
6	0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,1,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0, 0,0,2,2,2,0,2,0,2,2,2,2,2,2,1,2,2,2,2,2,2,0,1,0
7	0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0	0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,1,2,0,0
8	0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,0	0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0
9	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0	0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,0
10	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0
10	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
11	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
12	2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,2,2,1,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
13	0,2,2,1,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,0,0,2,2,1,0,2,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
14	2,0,0,2,2,1,0,2,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,2,1,0,0,0,1,0,2,2,0,0,0,0,0,0,2,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
15	0,0,2,1,0,0,0,1,0,2,2,0,0,0,0,0,0,2,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
16	0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
17	0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,0,0,0,0,0,0,2,2,0,0,0,2,1,0,2,0,0,0,2,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
18	2,0,0,0,0,0,0,2,2,0,0,0,2,1,0,2,0,0,0,2,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,2,2,0,0,0,0,1,2,2,2,1,0,2,2,2,2,2,0,0,0,2,0,2, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
19	0,2,2,0,0,0,0,1,2,2,2,1,0,2,2,2,2,2,0,0,0,2,0,2, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,1,2,2,2,0,0,2,2,2,2,2,0,0,2,2,2,2,0,0,0,2,0,2, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0

Table 18: Continued.

Round	The left part	The right part
20	2,1,2,2,2,0,0,2,2,2,2,2,0,0,2,2,2,2,0,0,0,2,0,2, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,2,2,1,0,2,2,1,2,2,0,0,2,2,0,2,0,0,0,2,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
21	0,2,2,1,0,2,2,1,2,2,0,0,2,2,0,2,0,0,0,2,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,0,0,0,2,1,0,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
22	2,0,0,0,2,1,0,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
23	0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0

Table 19: The DL distinguisher of Simon128 represented with *traceable patterns*.

Round	The left part	The right part
0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
1	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
2	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,1,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
3	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,1,2,2,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,1,2,0,0
4	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,1,2,2,2,0,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,1,2,2,0,1,0
5	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0, 0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,2,2,2,2,2,2,1,2,2,2,2,2,2,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,1,2,2,2,0,2,0,0
6	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0, 0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,1,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0, 0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,2,2,2,2,2,2,1,2,2,2,2,2,2,0,1,0
7	0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,1,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0, 0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,1,2,0,0
8	0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,1,0
9	0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0	0,0,0,0,0,0,2,0,0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0,0
10	0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,0	0,0,0,0,2,2,0,0,0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0
11	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0	0,0,2,2,2,0,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,0
12	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2, 2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0
12	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
13	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
14	2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,2,2,1,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
15	0,2,2,1,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,0,2,2,2,1,0,2,0,2,2,2,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
16	2,0,2,2,2,1,0,2,0,2,2,2,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,2,2,1,0,0,0,1,2,2,2,0,0,2,0,2,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
17	0,2,2,1,0,0,0,1,2,2,2,0,0,2,0,2,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,1,0,0,0,0,0,2,2,1,0,0,2,0,0,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0

Table 19: Continued.

Round	The left part	The right part
18	2,1,0,0,0,0,0,2,2,1,0,0,2,0,0,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
19	0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
20	0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,1,2,2,1,1,0,0,2,2,2,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
21	0,0,0,0,0,0,0,1,2,2,1,1,0,0,2,2,2,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,1,0,0,0,0,0,2,2,2,2,2,2,0,0,2,2,2,0,2,0,0,0,2,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
22	2,1,0,0,0,0,0,2,2,2,2,2,2,0,0,2,2,2,0,2,0,0,0,2,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,2,2,1,0,0,0,1,2,2,0,2,2,2,0,2,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
23	0,2,2,1,0,0,0,1,2,2,0,2,2,2,0,2,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,0,0,2,2,1,0,2,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
24	2,0,0,2,2,1,0,2,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
25	0,0,2,1,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
26	0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
27	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
28	2,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,2,2,0,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
29	0,2,2,0,0,0,0,0,2,2,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	2,1,0,0,2,0,0,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
30	2,1,0,0,2,0,0,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,1,0,0,2,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
31	0,0,0,1,0,0,2,0,0,0,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
32	0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1

Table 20: The DL distinguisher of Simeck32 represented with *traceable patterns*.

Round	The left part	The right part
0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0
1	0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
2	0,0,0,0,0,0,0,0,2,0,0,0,1,2,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0
3	0,0,0,2,0,0,0,2,2,0,0,1,2,2,0,0	0,0,0,0,0,0,0,0,2,0,0,0,1,2,0,0
4	0,0,2,2,0,0,2,2,2,0,1,2,2,2,2,0	0,0,0,2,0,0,0,2,2,0,0,1,2,2,0,0
5	0,2,2,2,0,2,2,2,2,2,2,2,2,2,2,0	0,0,2,2,0,0,2,2,2,0,1,2,2,2,2,0
6	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0	0,2,2,2,0,2,2,2,2,2,2,2,2,2,2,0
7	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0
7	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
8	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	1,0,0,0,2,0,0,0,0,0,0,0,0,0,0,2
9	1,0,0,0,2,0,0,0,0,0,0,0,0,0,0,2	2,1,0,0,2,2,0,0,0,2,0,0,0,0,0,2
10	2,1,0,0,2,2,0,0,0,2,0,0,0,0,0,2	0,2,1,0,2,0,2,0,0,0,0,0,0,0,0,2
11	0,2,1,0,2,0,2,0,0,0,0,0,0,0,0,2	0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,1
12	0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,1	1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0

Table 21: The DL distinguisher of Simeck48 represented with *traceable patterns*.

Round	The left part	The right part
0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0
1	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
2	0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,1,2,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0
3	0,0,0,0,0,0,0,0,2,0,0,0,2,2,0,0,1,2,2,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,1,2,0,0,0,0,0
4	0,0,0,2,0,0,0,2,2,0,0,2,2,2,0,1,2,2,2,0,0,0,0,0	0,0,0,0,0,0,0,0,2,0,0,0,2,2,0,0,1,2,2,0,0,0,0,0
5	0,0,2,2,0,0,2,2,2,0,2,2,2,2,1,2,2,2,2,0,0,0,2,0	0,0,0,2,0,0,0,2,2,0,0,2,2,2,0,1,2,2,2,0,0,0,0,0
6	0,2,2,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,0,2,2,0	0,0,2,2,0,0,2,2,2,0,2,2,2,2,1,2,2,2,2,0,0,0,2,0
7	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,2,2,0	0,2,2,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,0,2,2,0
8	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,2,2,0
8	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
9	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	1,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2
10	1,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2	2,1,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,2
11	2,1,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,2	2,2,1,0,2,2,2,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,2
12	2,2,1,0,2,2,2,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,2	2,1,0,1,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,2
13	2,1,0,1,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,2	1,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2
14	1,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2	0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
15	0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
16	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
17	0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0

Table 22: The DL distinguisher of Simeck64 represented with *traceable patterns*.

Round	The left part	The right part
0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0
1	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
2	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,1,2,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0
3	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,2,2,0,0,1,2,2,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,1,2,0,0,0
4	0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,2,2,0,0,2,2,2,0,1,2,2,2,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,2,2,0,0,1,2,2,0,0,0
5	0,0,0,0,0,0,0,0,2,0,0,0,2,2,0,0,2,2,2,0,2,2,2,2,1,2,2,2,2,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,2,0,0,0,2,2,0,0,2,2,2,0,1,2,2,2,0,0,0
6	0,0,0,2,0,0,0,2,2,0,0,2,2,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,0,0	0,0,0,0,0,0,0,0,2,0,0,0,2,2,0,0,2,2,2,0,2,2,2,2,1,2,2,2,2,0,0,0
7	0,0,2,2,0,0,2,2,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0	0,0,0,2,0,0,0,2,2,0,0,2,2,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,0,0
8	0,2,2,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0	0,0,2,2,0,0,2,2,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0,2,0
9	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0	0,2,2,2,0,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0
10	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2	2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,2,0
10	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
11	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	1,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2
12	1,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2	2,1,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2
13	2,1,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2	2,2,1,0,2,2,2,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2
14	2,2,1,0,2,2,2,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2	2,1,0,1,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2
15	2,1,0,1,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2	1,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2
16	1,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2	0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
17	0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
18	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
19	0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	1,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2
20	1,0,0,2,2,0,0,0,2,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,2	0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1
21	0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1	0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
22	0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0	0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1

Data Availability

No underlying data were collected or produced in this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper. In addition, we confirm there are no conflicts of interest for all authors (Wenya Li, Kai Zhang, and Bin Hu).

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China under grant no. 61802437, the Joint Fund Project of Science and Technology Research and Development Plan of Henan Province (Application Research) under grant no. 232103810042, and the Outstanding Youth Program of Henan Province under grant no. 242300421173.

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[2] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT'93*, vol. 765 of *Lecture Notes in Computer Science*, pp. 386–397, Springer, Norway, 1994.

[3] S. K. Langford and M. E. Hellman, "Differential-linear cryptanalysis," in *Advances in Cryptology—CRYPTO'94*, vol. 839 of *Lecture Notes in Computer Science*, pp. 21–25, Springer, Santa Barbara, California, USA, 1994.

[4] E. Biham, O. Dunkelman, and N. Keller, "Enhancing differential-linear cryptanalysis," in *Advances in Cryptology —ASIACRYPT 2002*, vol. 2501 of *Lecture Notes in Computer Science*, pp. 254–266, Springer, 2002.

[5] Z. Liu, D. Gu, J. Zhang, and W. Li, "Differential-multiple linear cryptanalysis," in *Information Security and Cryptology*, vol. 6151 of *Lecture Notes in Computer*, pp. 35–49, Springer, Beijing, China, 2009.

[6] J. Lu, "A methodology for differential-linear cryptanalysis and its applications," *Designs, Codes and Cryptography*, vol. 77, no. 1, pp. 11–48, 2015.

[7] C. Blondeau, G. Leander, and K. Nyberg, "Differential-linear cryptanalysis revisited," *Journal of Cryptology*, vol. 30, no. 3, pp. 859–888, 2017.

[8] A. Bar-On, O. Dunkelman, N. Keller, and A. Weizman, "DLCT: a new tool for differential-linear cryptanalysis," in *Advances in Cryptology–EUROCRYPT 2019*, vol. 11476 of *Lecture Notes in Computer Science*, pp. 313–342, Springer, Darmstadt, Germany, 2019.

[9] M. Liu, X. Lu, and D. Lin, "Differential-linear cryptanalysis from an algebraic perspective," in *Advances in Cryptology–CRYPTO 2021*, vol. 12827 of *Lecture Notes in Computer Science*, pp. 247–277, Springer, Cham, 2021.

[10] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, IEEE, San Francisco, CA, USA, 2015.

[11] G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong, "The simeck family of lightweight block ciphers," in *Cryptographic Hardware and Embedded Systems–CHES 2015*, vol. 9293 of *Lecture Notes in Computer Science*, pp. 307–329, Springer, Saint-Malo, France, 2015.

[12] O. Dunkelman, S. Indesteege, and N. Keller, "A differential-linear attack on 12-round serpent," in *Progress in Cryptology-INDOCRYPT 2008*, vol. 5365, pp. 308–321, Springer, Kharagpur, India, 2008.

[13] Y. Chen and W. Zhang, "Differential-linear cryptanalysis of SIMON32/64," *International Journal of Embedded Systems*, vol. 10, no. 3, pp. 196–202, 2018.

[14] Y. Hu, Z. Dai, and B. Sun, "Differential-linear cryptanalysis ofthe simon algorithm," *Netinfb Security*, vol. 22, no. 9, pp. 63–75, 2022.

[15] F. Zhang, F. Li, and W. Zhang, "Differential-linear cryptanalsis on SIMECK32/64 and SIMON32/64," *Journal of Physics: Conference Series*, vol. 2504, Article ID 012068, 2023.

[16] K. Zhang, X. Lai, J. Guan, and B. Hu, "Weak rotational property and its application," *Designs, Codes and Cryptography*, vol. 91, pp. 3187–3214, 2023.

[17] K. Zhang, X. Lai, L. Wang et al., "Meet-in-the-middle attack with splice-and-cut technique and a general automatic framework," *Designs, Codes and Cryptography*, vol. 91, pp. 2845–2878, 2023.

[18] K. Zhang, S. Wang, X. Lai et al., "Impossible differential cryptanalysis and a security evaluation framework for AND-RX ciphers," *IEEE Transactions on Information Theory*, 2024.

[19] K. Zhang, X. Lai, L. Wang et al., "Rotational-XOR differential cryptanalysis and an automatic framework for AND-RX ciphers," *IEEE Transactions on Information Theory*, vol. 69, no. 2, pp. 1282–1294, 2023.

[20] Z. Liu, Y. Li, L. Jiao, and M. Wang, "On the upper bound of squared correlation of SIMON-like functions and its applications," *IET Information Security*, vol. 16, no. 3, pp. 220–234, 2022.