Hindawi
IET Information Security
Volume 2024, Article ID 8315115, 39 pages
https://doi.org/10.1049/2024/8315115

Research Article

MILP/MIQCP-Based Fully Automatic Method of Searching for Differential-Linear Distinguishers for SIMON-Like Ciphers

Yanyan Zhou, Senpeng Wang, and Bin Hu

PLA Information Engineering University, Zhengzhou 450000, China

Correspondence should be addressed to Senpeng Wang; wsp2110@126.com

Received 8 July 2023; Revised 27 September 2023; Accepted 6 October 2023; Published 12 January 2024

Academic Editor: Qichun Wang

Differential-linear (DL) cryptanalysis is an important cryptanalytic method in cryptography and has received extensive attention from the cryptography community since its proposal by Langford and Hellman in 1994. At CT-RSA 2023, Bellini et al. introduced continuous difference propagations of XOR, rotation, and modulo-addition operations and proposed a fully automatic method using Mixed-Integer Linear Programing (MILP) and Mixed-Integer Quadratic Constraint Programing (MIQCP) techniques to search for DL distinguishers of Addition-Rotation-XOR (ARX) ciphers. In this paper, we propose continuous difference propagation of AND operation and construct an MILP/MIQCP-based fully automatic model of searching for DL distinguishers of SIMON-like ciphers. We apply the fully automatic model to all versions of SIMON and SIMECK. As a result, for SIMON, we find 13 and 14-round DL distinguishers of SIMON32, 15, 16, and 17-round DL distinguishers of SIMON48, 20-round DL distinguishers of SIMON64, 25 and 26-round DL distinguishers of SIMON96, 31 and 32-round DL distinguishers of SIMON128. For SIMECK, we find 14-round DL distinguishers of SIMECK32, 17 and 18-round DL distinguishers of SIMECK48, 22, 23, 24, and 25-round DL distinguishers of SIMECK64. As far as we know, our results are currently the best.

1. Introduction

In 1994, Langford and Hellman [1] proposed differential-linear (DL) cryptanalysis based on differential cryptanalysis introduced by Biham and Shamir [2] and linear cryptanalysis introduced by Matsui [3]. An entire cipher E can be decomposed as a cascade $E = E_2 \circ E_1$, a differential distinguisher and a linear distinguisher are applied to sub ciphers E_1 and E_2, respectively. Assume that the differential $\Delta_{in} \xrightarrow{E_1} \Delta_m$ holds with probability p, the linear approximation $\Gamma_m \xrightarrow{E_2} \Gamma_{\text{out}}$ is satisfied with correlation q. Under the assumption that E_1 and E_2 are independent, the correlation of the DL distinguisher is pq^2. Figure 1 shows the overview of the DL distinguisher. DL cryptanalysis has attracted a lot of researches since its introduction.

In 2017, Blondeau et al. [4] developed a concise theory of DL cryptanalysis and gave a close estimate of the bias under the sole assumption that the two parts of the cipher are independent. They also revisited the previous methods of estimating DL bias proposed by Biham et al. [5].

At EUROCRYPT 2019, Bar-On et al. [6] took the effects of dependency between the two sub ciphers E_1 and E_2 into account, then proposed the differential-linear connectivity table (DLCT). Here, the cipher E can be divided into three subciphers E_1, E_m, and E_2, namely, $E = E_2 \circ E_m \circ E_1$, where the correlation r of E_m is experimentally evaluated. Thus, the correlation of the DL distinguisher can be estimated as prq^2. The overall framework of the DL distinguisher is depicted in Figure 2.

At EUROCRYPT 2021, Liu et al. [7] generalized the technique proposed by Morawiecki et al. [8] and proposed a practical method for estimating the bias of (rotational) DL distinguishers for Addition-Rotation-XOR (ARX) ciphers in the special case where the output linear mask is a unit vector. Subsequently, at CRYPTO 2022, Niu et al. [9] computed the (rotational) DL correlation of modulo additions for arbitrary output linear masks, based on which a technique for evaluating the (rotational) DL correlation of ARX ciphers was derived.

At CRYPTO 2021, Liu et al. [10] re-investigated the basic principles and methods of DL cryptanalysis from an algebraic perspective and proposed the algebraic transitional forms (ATF) technique to estimate the DL bias of non-ARX ciphers.

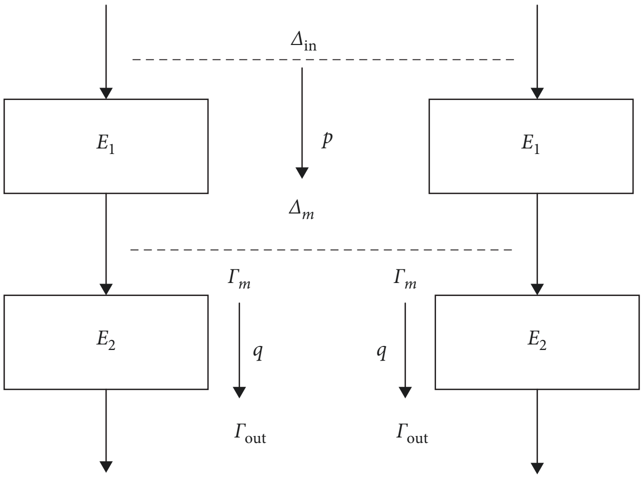

Figure 1: A classical structure of DL distinguisher.

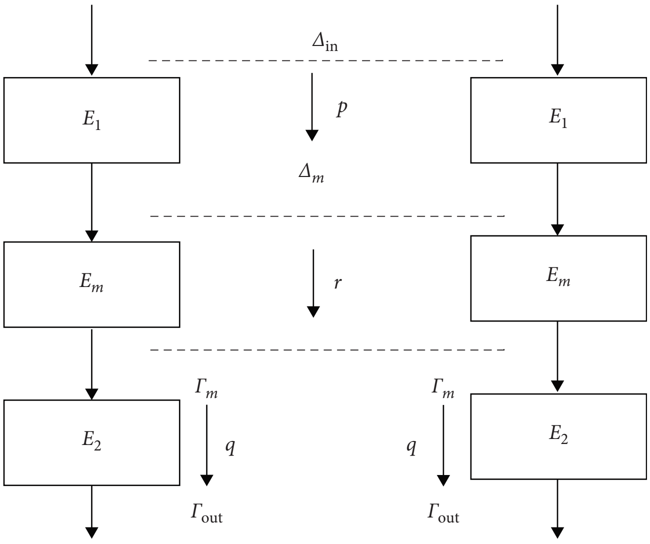

Figure 2: An improved structure of DL distinguisher.

Note that it does not require any assumptions in theory for the estimation of bias from the algebraic perspective. For more researches and applications of DL cryptanalysis, see [11–14].

However, there is no effective method that can automatically search for good DL distinguishers in the above researches on DL cryptanalysis. At CT-RSA 2023, Bellini et al. [15] presented a fully automatic method of searching for DL distinguishers for ARX ciphers by using Mixed-Integer Linear Programing (MILP) and Mixed-Integer Quadratic Constraint Programing (MIQCP) techniques. They improved the correlations of the best 9 and 10-round DL distinguishers on Speck32/64. Also, it is the first time a DL distinguisher reached 11 rounds for Speck32/64.

In this paper, we will explore how to fully automatically search for DL distinguishers for SIMON-like ciphers by using MILP and MIQCP techniques.

1.1. Related Works. There are various papers published on the cryptanalysis of SIMON-like ciphers [16–24]. Especially, there are many different techniques and automatic tools in the literature for finding differential, linear distinguishers on SIMON-like ciphers. In 2015, Sun et al. [18] constructed mixed-integer programing models whose feasible region is exactly the set of all valid differential characteristics of SIMON. In 2015, Abed et al. [16] stated an algorithm for the calculation of the differential probabilities but without further explanation. Kölbl et al. [20] derived efficiently computable and easily implementable expressions for the exact differential and linear behavior of SIMON-like round functions. Moreover, they used those expressions for a computer-aided approach based on Boolean satisfiability problem or satisfiability modulo theories (SAT/SMT) solvers to find both optimal differential and linear characteristics for SIMON. In 2021, Sun et al. [22] put forward a new encoding method to convert Matsui's bounding conditions into Boolean formulas and integrated the bounding conditions into the SAT method, which accelerated the search for differential and linear characteristics for SIMON-like ciphers.

For finding DL distinguishers for SIMON-like ciphers, in 2018, Chen et al. [23] constructed a 13-round DL distinguisher with bias $2^{-30.36}$ and presented key recovery attacks on 17-round and 18-round SIMON32, respectively. However, Hu et al. [24] pointed there are some problems in the calculation process of this method. In 2022, Hu et al. [24] constructed 13-round DL distinguishers for SIMON32 and SIMON48, respectively, and showed 16-round key recovery attacks on SIMON32 and SIMON48, respectively.

Note that there are no relevant researches on searching for DL distinguishers of SIMECK and larger instances of SIMON (SIMON64, SIMON96, SIMON128), and there is no effective method that can automatically search for good DL distinguishers for SIMON-like ciphers. This paper will intend to fill this vacancy.

1.2. Our Contribution. The new MILP/MIQCP model to find DL distinguishers for ARX ciphers was given by Bellini et al. [15], but the MILP/MIQCP techniques could not be applied to SIMON-like ciphers. Inspired by this, we propose continuous difference propagation of AND operation for the first time. Therefore, we construct an MILP/MIQCP model to fully automatically search for DL distinguishers for SIMON-like ciphers. Recall that we have three parts in the DL distinguisher with improved structure, including the differential part (top part), the DL part (middle part), and the linear part (bottom part), so we need to consider the models of these three parts, separately.

Firstly, according to efficient computation for the exact differential behavior of SIMON-like round functions [20], we construct the differential model of SIMON-like ciphers by using MILP techniques. For the linear part, we consider the AND operation in the round function as independent S-boxes, then exploit the model-generating method for S-boxes to complete the formation of the linear MILP model.

Secondly, we propose continuous difference propagation of the AND operation, then model the DL part (middle part) of SIMON-like ciphers. So, we obtain the MILP/MIQCP-

Table 1: The DL distinguishers for round-reduced SIMON and SIMECK.

Cipher	Round	Theoretical correlation	Experimental correlation	References
SIMON32	13	2^{-12}	$2^{-11.45}$	[24]
	13	$2^{-16.63}$	$2^{-11.19}$	This work
	14	$2^{-18.63}$	$2^{-14.83}$[a]	This work
SIMON48	13	2^{-20}	–	[24]
	15	$2^{-20.19}$	$2^{-16.41}$[a]	This work
	16	$2^{-22.66}$	$2^{-18.33}$[a]	This work
	17	$2^{-24.66}$	$2^{-20.39}$[a]	This work
SIMON64	20	$2^{-34.58}$	$2^{-28.64}$[a]	This work
SIMON96	25	$2^{-46.66}$	$2^{-42.46}$[a]	This work
	26	$2^{-50.66}$	$2^{-45.69}$[a]	This work
SIMON128	31	$2^{-62.70}$	$2^{-58.78}$[a]	This work
	32	$2^{-66.70}$	$2^{-63.99}$[a]	This work
SIMECK32	14	$2^{-16.63}$	$2^{-15.57}$[a]	This work
SIMECK48	17	$2^{-22.37}$	$2^{-15.43}$[a]	This work
	18	$2^{-24.75}$	$2^{-17.88}$[a]	This work
SIMECK64	22	$2^{-32.90}$	$2^{-24.59}$[a]	This work
	23	$2^{-36.13}$	$2^{-25.45}$[a]	This work
	24	$2^{-38.13}$	$2^{-27.17}$[a]	This work
	25	$2^{-41.04}$	$2^{-29.65}$[a]	This work

Note: [a]Due to the complexity of the data, the experimental correlation refers to the segmented experimental validation of theoretical correlation. For more details, see Section 4 and the Appendix.

based fully automatic model to search for DL distinguishers of SIMON-like ciphers.

Finally, to illustrate the effectiveness of our fully automatic model, we apply it to search for DL distinguishers of all versions of SIMON and SIMECK and verify experimentally the correlations of our DL distinguishers. To the best of our knowledge, it is the first time that DL distinguishers of all versions of SIMON and SIMECK have been found. Compared to previous DL distinguishers, for SIMON32 and SIMON48, our distinguishers have increased by 1 and 4 rounds, respectively. For SIMON64, SIMON96, SIMON128, and all versions of SIMECK, it is the first time that the DL distinguishers have been found. As far as we know, our DL distinguishers are currently the best for SIMON and SIMECK. Our results are given in Table 1.

1.3. Outline. The rest of this paper is organized as follows: In Section 2, we introduce notations and preliminaries used in this paper. In Section 3, we propose a fully automatic model to find DL distinguishers for SIMON-like ciphers. In Section 4, the fully automatic model is applied to all versions of SIMON and SIMECK, and all improved results are experimentally verified. We conclude this paper with some open problems in Section 5.

2. Notations and Preliminaries

In this paper, we will use the following notations. Let $x=(x_0, \ldots, x_{n-1}), y=(y_0, \ldots, y_{n-1}) \in \mathbb{F}_2^n$, we denote by x_i the i-th bit of x. The bitwise XOR operation of x and y is denoted as $x \oplus y$. The bitwise AND operation of x and y is denoted as $x \odot y$. $x \lll t$ denotes rotation of x by t bits to the left. $\mathscr{B}$ denotes the set of real numbers between 1 and -1, namely, $-1 \leq \mathscr{B} \leq 1$. $\mathbb{R}$ denotes the real number domain. X_L^i and X_R^i denote left half and right half of the i-th round input, respectively.

MILP is a kind of programing problem of optimizing (minimizing or maximizing) a linear objective function $f(x_1, x_2, \ldots, x_n)$. The objective function and constraints are linear, and all or some of the decision variables x_i, $1 \leq i \leq n$ in the problem are restricted to be integers. For example, an MILP model is as follows, consisting of three parts: objective function, constraints, and variables.

$$\begin{array}{ll} \text{maximize} & \\ & x_1 + x_2 + 2x_3 \\ \text{subject to} & \\ & x_1 + x_2 \geq 1 \\ & x_1 + 2x_2 + 3x_3 \leq 4 \\ \text{binary} & x_1, x_2, x_3. \end{array} \quad (1)$$

MIQCP is a class of programing problems that optimize an objective function (quadratic or linear) given a set of quadratic constraints. The constraints can be inequalities or equations. When we want to invoke the Gurobi optimizer to solve a question, we need to translate the question into the form of MILP/MIQP problem.

Lemma 1. *[3] (Piling-up Lemma). Let $Z_0, \ldots, Z_{m-1}$ be m independent binary random variables with $Pr[Z_i = 0] = p_i$. Then we have that*

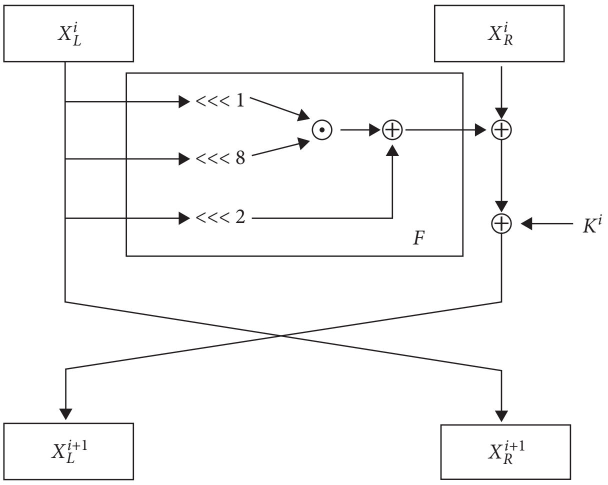

Figure 3: Round function of SIMON.

$$Pr[Z_0 \oplus \cdots \oplus Z_{m-1} = 0] = \frac{1}{2} + 2^{m-1}\prod_{i=0}^{m-1}\left(p_i - \frac{1}{2}\right), \tag{2}$$

or alternatively, $2Pr[Z_0 \oplus \cdots \oplus Z_{m-1} = 0] - 1 = \prod_{i=0}^{m-1}(2p_i - 1)$.

Proposition 1. *[7] Let a, b, a', and b' be n-bit strings with $Pr[a_{i-t} \neq a_i'] = p_i$ and $Pr[b_{i-t} \neq b_i'] = q_i$. Then*

$$Pr[(a \odot b)_{i-t} \neq (a' \odot b')_i] = \frac{1}{2}(p_i + q_i - p_i q_i). \tag{3}$$

According to Proposition 1, it's easy to obtain Corollary 1.

Corollary 1. *Let x, y, x', and $y' \in \mathbb{F}_2$, if $Pr[x \neq x'] = p_1$, $Pr[y \neq y'] = p_2$, then*

$$Pr[x \odot y \neq x' \odot y'] = \frac{1}{2}(p_1 + p_2 - p_1 p_2). \tag{4}$$

2.1. Description of SIMON-Like Ciphers. SIMON is a family of lightweight block ciphers designed by the US National Security Agency. There are 10 versions of SIMON. The SIMON block cipher with an n-bit word (a $2n$-bit block) is denoted as SIMON $2n$, where n is required to be 16, 24, 32, 48, or 64. SIMON $2n$ with an m-word (mn-bit) key is referred to as SIMON$2n/mn$, where $m = 2, 3, 4$. For example, SIMON32/64 refers to the version of SIMON acting on 32-bit plaintext blocks and using a 64-bit key. All versions of SIMON use similar round functions. The round function of SIMON is depicted in Figure 3.

Let the input of i-th round be (X_L^i, X_R^i), so the i-th round function is described in the following:

$$\begin{cases} X_L^{i+1} = X_R^i \oplus F(X_L^i) \oplus K^i \\ X_R^{i+1} = X_L^i \end{cases}, \tag{5}$$

where

$$F(x) = ((x \lll a) \odot (x \lll b)) \oplus (x \lll c), a = 1, b = 8, c = 2. \tag{6}$$

The key scheduling of SIMON depends on the size of the master key. For a detailed description of SIMON, please refer to the study of Beaulieu et al. [25].

SIMECK is a new family of lightweight block ciphers that combines the good design components from both SIMON and SPECK. There are three versions of SIMECK, namely SIMECK32/64, SIMECK48/96, and SIMECK64/128. The round function of SIMECK is similar to SIMON, but the rotation constants are different, namely, $a = 0$, $b = 5$, and $c = 1$. For a detailed description of SIMECK, please refer to the study of Yang et al. [26].

2.2. Continuous Difference Propagation. Coutinho et al. [27] proposed a new technique called Continuous Diffusion Analysis (CDA), which allows them to generalize cryptographic algorithms by transforming bits into probabilities or correlations. They presented continuous generalizations of some cryptographic operations (such as the XOR, addition modulo, S-box, etc.) and expressed bits as probabilities or correlations. For example, for the XOR operation $a = b_1 \oplus b_2$, where b_1, $b_2 \in \mathbb{F}_2$ are independent random variables. a is equal to 1 either when $b_1 = 0$ and $b_2 = 1$ or when $b_1 = 1$ and $b_2 = 0$. Let $Pr[a = 1] = p_3$, $Pr[b_1 = 1] = p_1$, and $Pr[b_2 = 1] = p_2$. Therefore, $p_3 = (1 - p_1) \times p_2 + p_1 \times (1 - p_2)$. Expressing p_1, p_2, and p_3 as functions of their correlations ϵ_{p_1}, ϵ_{p_2}, $\epsilon_{p_3} \in \mathscr{B} = \{x \in \mathbb{R} : -1 \leq x \leq 1\}$, they defined the continuous generalization of XOR operation as $\epsilon_{p_1} \oplus_{\mathscr{C}} \epsilon_{p_2} = \epsilon_{p_3} = -\epsilon_{p_1}\epsilon_{p_2}$.

Inspired by Coutinho's idea, Bellini et al. [15] constructed continuous functions for the difference propagation of ARX operations. For instance, assume (a, b) and (a', b') are two pairs of inputs of $\oplus$, $Pr[\Delta a = 1] = Pr[a \oplus a' = 1] = p$, $Pr[\Delta b = 1] = Pr[b \oplus b' = 1] = q$. Therefore, $Pr[\Delta a \oplus \Delta b = 1] = p(1 - q) + (1 - p)q$. Expressing p, q as functions of their correlations ϵ_p, ϵ_q, they defined the continuous difference propagation for $\oplus$ as $-\epsilon_p\epsilon_q$. Also, they defined more formally continuous difference propagation in Definition 1.

Definition 1. [15] Let $f(x_1, x_2, \ldots, x_n)$ be a function with input variables belonging to $\mathbb{F}_2^n$, and with output in $\mathbb{F}_2^m$, the continuous difference propagation of f, denoted as $f_{\mathscr{C}\Delta}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, is a function that maps input variables from $\mathscr{B}^n$ to $\mathscr{B}^m$, and describes the correlation between an input difference for f and each bit of its output difference. The exact form of the function $f_{\mathscr{C}\Delta}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ will depend on the specific properties of the function f.

According to this definition, they obtained some propositions describing continuous difference propagations for

ARX operations. The continuous difference propagations of XOR, left and right rotation are as follows:

Proposition 2. *[15] (Continuous difference propagation of XOR). Let $x, y \in \mathscr{B}$, then the continuous difference propagation of XOR is given by $x \oplus_{\mathscr{C}\Delta} y = -xy$.*

Proposition 3. *[15] (Continuous difference propagation of Left and Right Rotation). Let $x = (x_0, \ldots, x_{n-1}) \in \mathscr{B}^n$ and $r \in \mathbb{Z}$ such that $0 \leq r \leq n-1$, then the continuous difference propagation of the rotation to the left, and to the right, by r, respectively, is given by the following:*

$$(x_0, \ldots, x_{n-1}) \lll_{\mathscr{C}\Delta, r} = ((x_r, \ldots, x_{n-1}), x_0, \ldots, x_{r-1}), \tag{7}$$

$$(x_0, \ldots, x_{n-1}) \ggg_{\mathscr{C}\Delta, r} = ((x_{n-r}, \ldots, x_{n-1}), x_0, \ldots, x_{n-1-r}). \tag{8}$$

3. Fully Automatic Model of Finding DL Distinguishers with MILP/MIQCP

We use MILP/MIQCP techniques to model the entire DL distinguishers. Recall that the DL distinguisher with improved structure consists of three parts, namely, the differential part (top part), the DL part (middle part), and the linear part (bottom part). Therefore, we need to model these three parts, respectively.

3.1. Differential MILP Model of SIMON-Like Ciphers. Kölbl et al. [20] derived efficiently computable and easily implementable expressions for the exact differential of SIMON-like round functions, see Theorem 1.

Theorem 1. *[20] Let $f(x) = (x \lll a) \odot (x \lll b) \oplus (x \lll c)$, and α and β be an input and an output difference, where $\gcd(n, a-b) = 1$, n even, and $a > b$. Then with*

$$\text{varibits} = (\alpha \lll a) \vee (\alpha \lll b), \tag{9}$$

and

$$\text{doublebits} = (\alpha \lll b) \odot \overline{(\alpha \lll a)} \odot (\alpha \lll (2a - b)), \tag{10}$$

and

$$\gamma = \beta \oplus (\alpha \lll c), \tag{11}$$

we have that the probability that difference α goes to difference β is as follows:

$$Pr(\alpha \to \beta) = \begin{cases} 2^{-n+1} & \text{if} \alpha = 1 \text{ and } \mathrm{wt}(\gamma) \equiv 0 \bmod 2 \\ 2^{-\mathrm{wt}(\text{varibits} \ \oplus \ \text{doublebits})} & \text{if} \alpha \neq 1, \gamma \odot \overline{\text{varibits}} = 0 \text{ and } (\gamma \oplus \\ & (\gamma \lll (a-b))) \odot \text{doublebits} = 0 \\ 0 & \text{else.} \end{cases} \tag{12}$$

According to Theorem 1, Kölbl et al. [20] used those expressions for a computer-aided approach based on SAT/SMT solvers. Instead, we construct the differential MILP model of SIMON-like round function based on Theorem 1.

Differential Model (SIMON-Like Round Function). For the n-bit SIMON-like round function, we denote α and β as the input and output differences, respectively. Additionally, three n-bit variables varibits, doublebits, and z are incorporated so that we can evaluate the differential probability. If α is not an all-ones vector, the differential is valid if and only if the values of α, β, varibits, doublebits, and z validate all the constraints listed below:

$$0 \leq i \leq n-1 \begin{cases} -\text{varibits}_i + \alpha_{(i+a)\text{mod}n} + \alpha_{(i+b)\text{mod}n} \geq 0 \\ \text{varibits}_i - \alpha_{(i+b)\text{mod}n} \geq 0 \\ \text{varibits}_i - \alpha_{(i+a)\text{mod}n} \geq \\ -\text{doublebits}_i - \alpha_{(i+a)\text{mod}n} \geq 0 \\ -\text{doublebits}_i + \alpha_{(i+2a-b)\text{mod}n} \geq 0 \\ -\text{doublebits}_i + \alpha_{(i+b)\text{mod}n} \geq 0 \\ \text{doublebits}_i - \alpha_{(i+b)\text{mod}n} + \alpha_{(i+a)\text{mod}n} - \alpha_{(i+2a-b)\text{mod}n} \geq -1 \\ \alpha_{(i+c)\text{mod}n} + \beta_i - z_i \geq 0 \\ \alpha_{(i+c)\text{mod}n} - \beta_i + z_i \geq 0 \\ -\alpha_{(i+c)\text{mod}n} + \beta_i + z_i \geq 0 \\ -\alpha_{(i+c)\text{mod}n} - \beta_i - z_i \geq -2 \\ -z_i + \text{varibits}_i \geq 0 \\ z_i - z_{(i+a-b \,\text{mod}n)} - \text{doublebits}_i \geq -1 \\ -z_i + z_{(i+a-b \,\text{mod}n)} - \text{doublebits}_i \geq -1 \end{cases} . \tag{13}$$

The weight of the possible differential is $\sum_{i=0}^{n-1}(\text{varibits}_i \oplus \text{doublebits}_i)$.

3.2. Linear MILP Model of SIMON-Like Ciphers. Kölbl et al. (cf. Theorem 5) [20] perfectly handled the dependency and derived efficient computation for the exact linear behavior of SIMON-like round functions. However, because of the difficulty of encoding this model with Boolean equations, Sun et al. [22] regarded the AND operations in the round function as independent S-boxes and exploited the model-generating method for S-boxes to complete the linear SAT model. Similarly, we regard the AND operations as independent S-boxes. After computing its linear approximation table (LAT), we obtain the linear MILP model.

Linear Model (SIMON-Like Round Function). For the n-bit SIMON-like round function, we denote the input and output linear masks as α and β, respectively. Two auxiliary n-bit variables γ^0 and γ^1 are employed to record the two input masks of the AND operation. After one round of encryption, we denote the right half of the output linear mask as γ^2. To estimate the linear correlation, we also import an n-bit variable z. The correlation of the linear approximation is nonzero if the values of α, β, γ^0, γ^1, and γ^2 validate all the constraints listed in the following:

$$0 \leq i \leq n-1 \begin{cases} -\gamma_i^0 + z_i \geq 0 \\ -\gamma_i^1 + z_i \geq 0 \\ -\beta_i + z_i \geq 0 \\ \beta_i - z_i \geq 0 \\ \alpha_i \oplus \beta_{(i-c)\bmod n} \oplus \gamma^0_{(i-a)\bmod n} \oplus \gamma^1_{(i-b)\bmod n} = \gamma_i^2 \end{cases}, \tag{14}$$

where MILP model of the equation $\alpha_i \oplus \beta_{(i-c)\bmod n} \oplus \gamma^0_{(i-a)\bmod n} \oplus \gamma^1_{(i-b)\bmod n} = \gamma_i^2 (0 \leq i \leq n-1)$ as follows:

$$0 \leq i \leq n-1 \begin{cases} \alpha_i - \beta_{(i-c)\bmod n} + \gamma^0_{(i-a)\bmod n} - \gamma^1_{(i-b)\bmod n} + \gamma_i^2 \geq -2 \\ \alpha_i + \beta_{(i-c)\bmod n} - \gamma^0_{(i-a)\bmod n} - \gamma^1_{(i-b)\bmod n} - \gamma_i^2 \geq -2 \\ \alpha_i - \beta_{(i-c)\bmod n} - \gamma^0_{(i-a)\bmod n} + \gamma^1_{(i-b)\bmod n} - \gamma_i^2 \geq -2 \\ \alpha_i + \beta_{(i-c)\bmod n} + \gamma^0_{(i-a)\bmod n} + \gamma^1_{(i-b)\bmod n} - \gamma_i^2 \geq 0 \\ \alpha_i + \beta_{(i-c)\bmod n} + \gamma^0_{(i-a)\bmod n} - \gamma^1_{(i-b)\bmod n} + \gamma_i^2 \geq 0 \\ \alpha_i + \beta_{(i-c)\bmod n} - \gamma^0_{(i-a)\bmod n} + \gamma^1_{(i-b)\bmod n} + \gamma_i^2 \geq 0 \\ -\alpha_i + \beta_{(i-c)\bmod n} + \gamma^0_{(i-a)\bmod n} + \gamma^1_{(i-b)\bmod n} + \gamma_i^2 \geq 0 \\ \alpha_i - \beta_{(i-c)\bmod n} + \gamma^0_{(i-a)\bmod n} + \gamma^1_{(i-b)\bmod n} + \gamma_i^2 \geq 0 \\ -\alpha_i + \beta_{(i-c)\bmod n} + \gamma^0_{(i-a)\bmod n} - \gamma^1_{(i-b)\bmod n} - \gamma_i^2 \geq -2 \\ -\alpha_i + \beta_{(i-c)\bmod n} - \gamma^0_{(i-a)\bmod n} + \gamma^1_{(i-b)\bmod n} - \gamma_i^2 \geq -2 \\ -\alpha_i - \beta_{(i-c)\bmod n} + \gamma^0_{(i-a)\bmod n} + \gamma^1_{(i-b)\bmod n} - \gamma_i^2 \geq -2 \\ -\alpha_i - \beta_{(i-c)\bmod n} - \gamma^0_{(i-a)\bmod n} - \gamma^1_{(i-b)\bmod n} - \gamma_i^2 \geq -4 \\ -\alpha_i - \beta_{(i-c)\bmod n} - \gamma^0_{(i-a)\bmod n} + \gamma^1_{(i-b)\bmod n} + \gamma_i^2 \geq -2 \\ -\alpha_i - \beta_{(i-c)\bmod n} + \gamma^0_{(i-a)\bmod n} - \gamma^1_{(i-b)\bmod n} + \gamma_i^2 \geq -2 \\ \alpha_i - \beta_{(i-c)\bmod n} - \gamma^0_{(i-a)\bmod n} - \gamma^1_{(i-b)\bmod n} + \gamma_i^2 \geq -2 \\ -\alpha_i + \beta_{(i-c)\bmod n} - \gamma^0_{(i-a)\bmod n} - \gamma^1_{(i-b)\bmod n} + \gamma_i^2 \geq -2. \end{cases} \tag{15}$$

The value of $\sum_{i=0}^{n-1} z_i$ equals the opposite number of the binary logarithm of the absolute value of the correlation.

3.3. Middle Part Model of SIMON-Like Ciphers.

To model the middle part of ARX ciphers, Bellini et al. [15] proposed the continuous difference propagations of ARX operations (see Section 2.2) and modeled the continuous difference propagation using the MILP/MIQCP syntax over $\mathscr{B}$. Inspired by this, to model the middle part of SIMON-like ciphers, we first propose the continuous difference propagation of AND operation, then model the continuous difference propagation of SIMON-like ciphers using the MILP/MIQCP syntax over $\mathscr{B}$.

Proposition 4. *(Continuous Difference Propagation of AND). Let $x, y \in \mathscr{B}$, then the continuous difference propagation of AND is given by $x \odot_{\mathscr{C}\Delta} y = \frac{1}{4}(x + y - xy - 1)$.*

Proof 1. Suppose a, b, a', and $b' \in \mathbb{F}_2$, $Pr(a \neq a') = p$, and $Pr(b \neq b') = q$. According to Corollary 1, if $Pr(a \neq a') = p$ and $Pr(b \neq b') = q$, we have $Pr(a \odot b \neq a' \odot b') = \frac{1}{2}(p + q - pq)$. Replacing the probabilities with their expressions involving their respective correlations $x, y \in \mathscr{B}$, we have$Pr(a \odot b \neq a' \odot b') = \frac{1}{8}(x + y - xy + 3)$, so $x \odot_{\mathscr{C}\Delta} y = \frac{1}{4}(x + y - xy - 1)$. □

In the following, we regard $a \times b$ as the multiplication of a and b in $\mathscr{B}$. According to Proposition 4, we model constraints of AND operation using the MILP/MIQCP syntax over $\mathscr{B}$.

Constraints of AND Operation. For every AND operation with input $a \in \mathscr{B}^n$ and $b \in \mathscr{B}^n$ and output $c \in \mathscr{B}^n$, we have n constraints:

$$c_j = \frac{1}{4}\left(a_j + b_j - a_j \times b_j - 1\right), \tag{16}$$

for $0 \leq j \leq n-1$.

SIMON-like ciphers also include XOR operation and left rotation operation. Bellini et al. [15] showed the constraints of them.

Constraints of XOR Operation [15]. For every XOR operation with input $a \in \mathscr{B}^n$ and $b \in \mathscr{B}^n$ and output $c \in \mathscr{B}^n$, we have n constraints:

$$c_j = -a_j \times b_j, \tag{17}$$

for $0 \leq j \leq n-1$.

Constraints of Left Rotation Operation [15]. For every left rotation operation with input $a \in \mathscr{B}^n$ and output $c \in \mathscr{B}^n$, we have n constraints:

$$c_j = a_{(j+r) \bmod n}, \tag{18}$$

for $0 \leq j \leq n-1$, where r is left rotation constant.

Constraints of R-Round SIMON-Like Cipher. For all rounds, we need $2n(R+1)$ variables belonging to $\mathscr{B}$ to represent the states of SIMON. The count of the number of equations is as follows: nR equalities to model the XOR operation. nR equalities to model the AND operation. Summing up, we have a total of $2nR$ constraints to model the continuous difference propagation framework for SIMON-like ciphers.

Objective Function of the Middle Part Model. For the objective function of the middle part, given the correlation r, we need to minimize the function $-\log_2|r|$. Beaulieu et al. [25] found a linear function $g(r)$ to approximate $-\log_2|r|$ such that $g(r) \leq -\log_2|r|$.

$$g(r)=\begin{cases} -19,931.570r+29.897, & 0\leq r\leq 0.001\\ -584.962r+10.135, & 0.001\leq r\leq 0.004\\ -192.645r+8.506, & 0.004\leq r\leq 0.014\\ -50.626r+6.575, & 0.014\leq r\leq 0.053\\ -11.87r+4.483, & 0.053\leq r\leq 0.142\\ -8.613r+4.020, & 0.142\leq r\leq 0.246\\ -3.761r+2.825, & 0.246\leq r\leq 0.595\\ -1.444r+1.444, & 0.595\leq r\leq 0.998 \end{cases}. \tag{19}$$

In addition, to connect the top part with the middle part, we use the method in the study of Bellini et al. [15] to translate the differential output bits into real numbers belonging to $\mathscr{B}$. Specifically, the value 1 in a specific position in the output of the differential part indicates that there is a difference in that position, so the probability is 1.0, which results in a correlation 1.0. In contrast, the value 0 means that there is no difference in that position, so the probability is 0.0, and the correlation is -1.0. In other words, the correlation in that certain position with output bit 1 is 1.0, and the correlation in that certain position with output bit 0 is -1.0.

Assume $(t_0,\ldots,t_{n-1})\in\mathbb{F}_2^n$ is the output difference of the differential part, and $\left(m_0^{input},\ldots,m_{n-1}^{input}\right)\in\mathscr{B}^n$ is the input difference of the middle part. There are the constraints $m_j^{input}=1.0\in\mathscr{B}$ if $t_j=1$, otherwise $m_j^{input}=-1.0\in\mathscr{B}$. To connect the middle part with the linear part, suppose $(l_0,\ldots,l_{n-1})\in\mathbb{F}_2^n$ is the input mask of the linear part, and $\left(m_0^{output},\ldots,m_{n-1}^{output}\right)\in\mathscr{B}^n$ is the output of the middle part. Since the correlation of the middle part $r=\prod_{i=0}^{n-1}l_j\times m_j^{input}$ can not be 0, there is the constraint $r>0.0$.

Objective Function of the Entire Model. We denote x and y as the exponents of the differential and linear parts, respectively. By applying Lemma 1 (piling-up lemma), we need to minimize the exponents of the three parts, namely, $x+g(r)+2y$.

Thus, we construct the fully automatic model to find DL distinguishers of SIMON-like ciphers. Note that as the number of rounds increases, it becomes increasingly difficult to find a good DL trail for larger instances of SIMON-like ciphers. Therefore, we apply one strategy to obtain good DL distinguishers for larger instances of SIMON-like ciphers.

One Strategy to Obtain Good DL Distinguishers. First, we obtain the optimal differential trail for a certain number of rounds by using the SAT method presented in the study of Sun et al. [22]. Second, we extend the optimal differential trail by a DL trail (the middle part) and a linear trail (the bottom part) by using our fully automatic model.

4. Applications to SIMON-Like Ciphers

In this section, we apply the fully automatic model to search for DL distinguishers for SIMON-like ciphers. For clarity and convenience, if a DL distinguisher has the x-round top part, the y-round middle part, and the z-round bottom part, we say that the DL distinguisher uses configuration $(x+y+z)$. Our MILP/MIQCP models have been implemented using MiniZinc and solved with Gurobi.

4.1. Applications to SIMON. We apply the fully automatic model to all versions of SIMON. Our DL distinguishers are shown in Table 2.

For SIMON32, we found two DL distinguishers for 13 and 14 rounds. To obtain the 13-round distinguisher, we try all configurations regarding the number of rounds for the top, middle, and bottom parts. In this case, for the 13-round DL distinguisher, the best theoretical correlation is found by using configuration $(5,5,3)$. For the 14-round DL distinguisher, in the same way, we try all configurations. In this case, the best theoretical correlation is found by using configuration $(5,5,4)$. The details of the two distinguishers are covered in Tables 4 and 5.

For SIMON48, we found three DL distinguishers for 15, 16, and 17 rounds. Similarly, we try all configurations regarding the number of rounds for the top, middle, and bottom parts. In these cases, the best theoretical correlation for the 15-round DL distinguisher is found by using configuration $(7,4,4)$, the best theoretical correlation for the 16-round DL distinguisher is found by using configuration $(7,5,4)$, and the best theoretical correlation for the 17-round DL distinguisher is found by using configuration $(7,6,4)$. The details of these distinguishers can be found in Tables 6–8.

For SIMON64, we obtain a DL distinguisher for 20 rounds by using the strategy in Section 3.3. Likewise, we try all configurations regarding the number of rounds for the top, middle, and bottom parts, and the DL distinguisher by using configuration $(7,7,6)$ is found. The details of the distinguisher are shown in Table 9.

For SIMON96, we obtain two DL distinguishers for 25 and 26 rounds by using the strategy in Section 3.3. In the same way, the 25-round DL distinguisher by using configuration $(10,6,9)$ and 26-round DL distinguishers by using configuration $(11,6,9)$ are found. The details of the two distinguishers are provided in Tables 10 and 11.

For SIMON128, we obtain two DL distinguishers for 31 and 32 rounds by using the strategy in Section 3.3. In the same way, the 31-round DL distinguisher by using configuration $(10,9,12)$ and the 32-round DL distinguishers by using configuration $(11,9,12)$ are found. Please check Tables 12 and 13 for the details of the two distinguishers.

4.2. Applications to SIMECK. In this section, we apply the fully automatic model to search for DL distinguishers for SIMECK. It is the first time that DL distinguishers for SIMECK have been obtained. These DL distinguishers are shown in Table 3.

For SIMECK32, we find a DL distinguisher for 14 rounds. To obtain the 14-round distinguisher, we try all configurations

Table 2: The DL distinguishers of reduced-round SIMON.

Cipher	Round	Configuration	Correlation		References
			Theory	Experiment	
SIMON32	13	—	2^{-12}	$2^{-11.45}$	[24]
	13	$5+5+3$	$2^{-16.63}$	$2^{-11.19}$ [a]	This work
	14	$5+5+4$	$2^{-18.63}$	$2^{-14.83}$ [b]	This work
SIMON48	13	-	2^{-20}	—	[24]
	15	$7+4+4$	$2^{-20.19}$	$2^{-16.41}$ [b]	This work
	16	$7+5+4$	$2^{-22.66}$	$2^{-18.33}$ [b]	This work
	17	$7+6+4$	$2^{-24.66}$	$2^{-20.39}$ [b]	This work
SIMON64	20	$7+7+6$	$2^{-34.58}$	$2^{-28.64}$ [b]	This work
SIMON96	25	$10+6+9$	$2^{-46.66}$	$2^{-42.46}$ [c]	This work
	26	$11+6+9$	$2^{-50.66}$	$2^{-45.69}$ [c]	This work
SIMON128	31	$10+9+12$	$2^{-62.70}$	$2^{-58.78}$ [d]	This work
	32	$11+9+12$	$2^{-66.70}$	$2^{-63.99}$ [d]	This work

Note: [a] Practical correlation. The sample size for 13-round SIMON32 is 2^{32}, where we randomly chose 100 master keys. [b] Segmented experimental validation of theoretical correlation. Specifically, regarding the top and middle parts as a DL distinguisher, we obtain an experimental DL correlation with 2^{32} sample sizes and 100 random master keys. For the bottom linear part, we obtain an experimental linear correlation. Finally, the experimental correlations are obtained based on piling-up lemma. [c] Segmented experimental validation of theoretical correlation. Specifically, for the top, middle and bottom parts, we obtain an experimental differential probability, an experimental DL correlation, and an experimental linear correlation, respectively. Finally, the experimental correlations are obtained based on piling-up lemma. [d] Segmented experimental validation of theoretical correlation. Specifically, for the top and middle parts, we obtain an experimental differential probability and an experimental DL correlation, respectively. Finally, the experimental correlations are obtained based on piling-up lemma.

Table 3: The DL distinguishers of reduced-round SIMECK.

Cipher	Round	Configuration	Correlation		References
			Theory	Experiment [a]	
SIMECK32	14	$5+5+4$	$2^{-16.63}$	$2^{-15.57}$	This work
SIMECK48	17	$6+6+5$	$2^{-22.37}$	$2^{-15.43}$	This work
	18	$6+6+6$	$2^{-24.75}$	$2^{-17.88}$	This work
SIMECK64	22	$7+7+8$	$2^{-32.90}$	$2^{-24.59}$	This work
	23	$7+7+9$	$2^{-36.13}$	$2^{-25.45}$	This work
	24	$7+7+10$	$2^{-38.13}$	$2^{-27.17}$	This work
	25	$7+7+11$	$2^{-41.04}$	$2^{-29.65}$	This work

Note: [a] Segmented experimental validation of theoretical correlation. Specifically, regrading the top and middle parts as a DL distinguisher, we obtain an experimental DL correlation with 2^{32} sample sizes and 100 random master keys. For the bottom linear part, we obtain an experimental linear correlation. Finally, the experimental correlations are obtained based on piling-up lemma.

regarding the number of rounds for the top, middle, and bottom parts. In this case, the best theoretical correlation is found by using configuration $(5+5+4)$. The details of the distinguisher can be found in Table 14.

For SIMECK48, we find two DL distinguishers for 17 and 18 rounds. Similarly, we try all configurations regarding the number of rounds for the top, middle, and bottom parts. In these cases, the best theoretical correlation for the 17-round DL distinguisher is found by using configuration $(6,6,5)$, the best theoretical correlation for the 18-round DL distinguishers by using configuration $(6,6,6)$ is found. The details of the two distinguishers are shown in Tables 15 and 16.

For SIMECK64, we find four DL distinguishers for 22, 23, 24, and 25 rounds by using the strategy in Section 3.3. The 22-round DL distinguisher by using configuration $(7,7,8)$, 23-round DL distinguishers by using configuration $(7,7,9)$, 24-round DL distinguishers by using configuration $(7,7,10)$, and 25-round DL distinguishers by using configuration $(7,7,11)$ are found. The details of these distinguishers are in Tables 17–20.

5. Conclusion and Open Problems

In this work, we consider how to construct the MILP/MIQCP model to fully automatically search for DL distinguishers of SIMON-like ciphers. For the top part of the model, we first construct the differential MILP model of SIMON-like ciphers according to efficient computation for the exact differential behavior of SIMON-like round functions. For the middle part, we obtain continuous difference propagation of AND operation, so we can model the middle part of SIMON-like ciphers. For the bottom part, we construct the linear MILP model of SIMON-like ciphers by regarding AND operation as independent S-boxes. After that, we apply the MILP/MIQCP model to SIMON and SIMECK. It is the first time that the DL distinguishers for full versions of SIMON and SIMECK have been obtained. To the best of our knowledge, our fully automatic model finds the best DL distinguishers for SIMON and SIMECK at present. We believe that the fully automatic model can be applied to SPN ciphers. Of course, the primary problem to be solved is how to characterize the continuous difference propagation of S-boxes, which is also our future work.

Appendix

Details of the DL Distinguishers

In the Tables 4–20, the first column shows the number of rounds. The second column shows the differential, DL, or linear trails of the DL distinguishers presented in Section 4. In the DL part, we have rows and subrows. Each row represents a state of the DL trail, and each subrow represents correlation of every bit of that state.

Table 4: Thirteen-round DL distinguisher for SIMON32 with the theoretical correlation $2^{-16.63}$ and experimental correlation $2^{-11.19}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-8}, $0.64(=2^{-0.63})$, and 2^{-4}, respectively.

	Differential part							
0	00001000000000000010001000001000							
1	00000010000000000000100000000000							
2	00000000000000000000001000000000							
3	00000010000000000000000000000000							
4	00001000000000000000001000000000							
5	00100010000000000000100000000000							
	DL part							
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
6	1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0	−1.0
	−1.0	−1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
7	−0.5	−1.0	0.5	0.0	−0.5	−1.0	0.5	−1.0
	0.0	−0.25	−1.0	−1.0	0.0	−0.25	1.0	0.0
	1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0	−1.0
	−1.0	−1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0
8	−0.25	0.0	−0.2499	−0.75	0.25	0.0	0.0	−0.0625
	−0.4687	−1.0	0.0	−0.0625	0.4687	0.0	0.0	−0.75
	−0.5	−1.0	0.5	0.0	−0.5	−1.0	0.5	−1.0
	0.0	−0.25	−1.0	−1.0	0.0	−0.25	1.0	0.0
9	−0.0459	−0.4687	−0.0546	0.0	0.0	−0.1556	0.0622	−0.6425
	0.0	−0.0039	0.1556	0.0	0.0	−0.0468	0.1093	0.0
	−0.25	0.0	−0.2499	−0.75	0.25	0.0	0.0	−0.0625
	−0.4687	−1.0	0.0	−0.0625	0.4687	0.0	0.0	−0.75
10	−0.0050	0.0	0.0	−0.0029	−0.0039	0.0	0.0	−0.00006
	0.0191	0.0	0.0	0.0007	−0.0134	0.0	0.0	−0.1509
	−0.0458	−0.4687	−0.0546	0.0	0.0	−0.0156	0.0622	−0.6425
	0.0	−0.0039	0.1556	0.0	0.0	−0.0468	0.1093	0.0
	Linear part							
	00000000000000000000000100000000							
11	00000001000000000000000001000001							
12	00000000010000010000000000010000							
13	00000000000100000000000001000101							

Note: The experimental correlation is $2^{-11.19}$ under 2^{32} sample sizes and 100 random keys.

Table 5: Fourteen-round DL distinguisher for SIMON32 with theoretical correlation $2^{-18.63}$ and experimental correlation $2^{-14.83}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-8}, $0.64(=2^{-0.63})$, and 2^{-5}, respectively.

				Differential part				
0	00000000000010000000000000100010							
1	00000000000000100000000000001000							
2	00000000000000000000000000000010							
3	00000000000000100000000000000000							
4	00000000000010000000000000000010							
5	00000000001000100000000000001000							
				DL part				
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
6	−1.0	−1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0
	1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	1.0	−1.0
7	0.0	−0.25	−1.0	−1.0	0.0	−0.25	1.0	0.0
	−0.5	−1.0	0.5	0.0	−0.5	−1.0	0.5	−1.0
	−1.0	−1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0
	1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0	−1.0
8	−0.4687	−1.0	0.0	−0.0625	0.4687	-9.51×2^{-9}	0.0	−0.75
	−0.25	0.0	−0.25	−0.75	0.25	0.0	0.0	−0.0625
	0.0	−0.25	−1.0	−1.0	0.0	−0.25	1.0	0.0
	−0.5	−1.0	0.5	0.0	−0.5	−1.0	0.5	−1.0
9	0.0	−0.0039	0.1556	-2.38×2^{-9}	0.0	−0.0468	0.1093	0.0
	−0.0458	−0.4687	−0.0546	0.0	-4.15×2^{-7}	−0.0156	0.0622	−0.6425
	−0.4687	−1.0	0.0	−0.0625	0.4687	-9.51×2^{-9}	0.0	−0.75
	−0.25	0.0	−0.25	−0.75	0.25	0.0	0.0	−0.0625
10	0.0191	-7.37×2^{-10}	0.0	−0.0007	−0.0134	0.0	0.0	−0.1509
	−0.0050	0.0	0.0	−0.0029	−0.0039	0.0	0.0	0.00006
	0.0	−0.0039	0.1556	-2.38×2^{-9}	0.0	−0.0468	0.1093	0.0
	−0.0458	−0.4687	−0.05468	0.0	-4.15×2^{-7}	−0.0156	0.0622	−0.6425
				Linear part				
	00000000000000000000000000000001							
11	00000000000000010100000000000000							
12	01000000000000000001000000000001							
13	00010000000000010000010000000000							
14	00000100000000000001000100000001							

Note: The experimental correlation of the first 10 (5 + 5) rounds is $2^{-5.49}$ under 2^{23} sample sizes and 100 random keys, the experimental correlation of the 4 rounds at the bottom is $2^{-4.67}$ under 2^{15} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-5.49}\times(2^{-4.67})^2=2^{-14.83}$.

TABLE 6: Fifteen-round DL distinguisher for SIMON48 with theoretical correlation $2^{-20.19}$ and experimental correlation $2^{-16.41}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-14}, $0.875(=2^{-0.19})$, and 2^{-3}, respectively.

Differential part								
0	100000000000000000000000001000100000000000000010							
1	001000100000000000000000100000000000000000000000							
2	000010000000000000000000001000100000000000000000							
3	000000100000000000000000000010000000000000000000							
4	000000000000000000000000000000100000000000000000							
5	000000100000000000000000000000000000000000000000							
6	000010000000000000000000000000100000000000000000							
7	001000100000000000000000000010000000000000000000							
DL part								
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
9	−0.5	−1.0	1.0	0.0	−0.5	−1.0	1.0	−1.0
	−1.0	−1.0	−0.50	−1.0	−1.0	−1.0	−0.5	−1.0
	0.0	−0.25	−1.0	−1.0	0.0	−0.25	1.0	0.0
	1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	0.0	−1.0	−1.0	−1.0	0.0	−1.0
10	−1.0	0.0	−0.1875	−0.75	1.0	0.0	−0.75	−1.0
	−0.2499	−0.4687	−1.0	−0.9999	−0.25	−0.4687	0.0	−0.0625
	−0.4687	−1.0	0.0	−0.0625	0.4687	0.0	0.0	−0.75
	−0.5	−1.0	1.0	0.0	−0.5	−1.0	1.0	−1.0
	−1.0	−1.0	−0.50	−1.0	−1.0	−1.0	−0.5	−1.0
	0.0	−0.25	−1.0	−1.0	0.0	−0.25	1.0	0.0
11	−0.0292	−0.3270	−0.8750	0.0	−0.1171	−0.6425	0.1249	−0.1556
	−0.5393	−0.9999	−0.0625	−0.1556	0.0	−0.0156	−0.0622	−0.6425
	0.0	−0.0039	0.1478	0.0	0.0	−0.0468	0.7656	-3.41×2^{-12}
	−1.0	0.0	−0.1875	−0.75	1.0	0.0	−0.75	−1.0
	−0.2499	−0.4687	−1.0	−0.9999	−0.25	−0.4687	0.0	−0.0625
	−0.4687	−1.0	0.0	−0.0625	0.4687	0.0	0.0	−0.75
Linear part								
	001000000000000000000000100000000000000000000000							
12	100000000000000000000000000000000000000000000000							
13	000000000000000000000000100000000000000000000000							
14	100000000000000000000000001000000000000000000000							
15	001000000000000000000000100010000000000000000000							

Note: The experimental correlation of the first 11 (7 + 4) rounds is $2^{-10.43}$ under 2^{32} sample sizes and 100 random keys, the experimental correlation of the 4 rounds at the bottom is $2^{-2.99}$ under 2^{15} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-10.43}\times(2^{-2.99})^2=2^{-16.41}$.

Table 7: Sixteen-round DL distinguisher for SIMON48 with theoretical correlation $2^{-22.66}$ and experimental correlation $2^{-18.33}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are $2^{-14}, 0.63(=2^{-0.66})$, and 2^{-4}, respectively.

	Differential part							
0	000001000000000000000000000100010001000000000000							
1	000000010001000000000000000001000000000000000000							
2	000000000100000000000000000000010001000000000000							
3	000000000001000000000000000000000100000000000000							
4	000000000000000000000000000000000001000000000000							
5	000000000001000000000000000000000000000000000000							
6	000000000100000000000000000000000001000000000000							
7	000000010001000000000000000000000100000000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	1.0
	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	−1.0	−1.0	−1.0	0.0	−1.0	1.0	0.0	−1.0
	−1.0	−1.0	0.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	0.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	1.0
	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
9	−1.0	0.0	−0.2500	1.0	0.0	−0.5	−1.0	1.0
	0.0	−0.5	−1.0	1.0	−1.0	−1.0	−1.0	−0.5
	−1.0	−1.0	−1.0	−0.5000	−1.0	0.0	−0.25	−1.0
	−1.0	−1.0	−1.0	0.0	−1.0	1.0	0.0	−1.0
	−1.0	−1.0	0.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	0.0
10	−0.0625	0.4688	0.0	0.0	−0.75	−1.0	0.0	−0.1875
	−0.75	1.0	0.0	−0.7500	−1.0	−0.25	−0.4688	−1.0
	−1.0	−0.2500	−0.4688	0.0	−0.0625	−0.4688	−1.0	0.0
	−1.0	0.0	−0.2500	1.0	0.0	−0.5	−1.0	1.0
	0.0	−0.5	−1.0	1.0	−1.0	−1.0	−1.0	−0.5
	−1.0	−1.0	−1.0	−0.5000	−1.0	0.0	−0.25	−1.0
11	0.0	0.0	−0.0469	0.7656	0.0	−0.0293	−0.3270	−0.875
	0.0	−0.1172	−0.6426	0.125	−0.1556	−0.5393	−1.0	−0.0625
	−0.1556	0.0	−0.0156	−0.0623	−0.6426	0.0	−0.0039	0.1479
	−0.0625	0.4688	0.0	0.0	−0.75	−1.0	0.0	−0.1875
	−0.75	1.0	0.0	−0.75	−1.0	−0.25	−0.4688	−1.0
	−1.0	−0.2500	−0.4688	0.0	−0.0625	−0.4688	−1.0	0.0
12	−0.0007	−0.1049	0.0	0.0	−0.0729	−0.4468	0.0	−0.0058
	−0.1556	−0.0513	0.0	−0.1241	−0.6321	−0.0078	−0.0195	0.0
	−0.0039	−0.0040	−0.0837	0.0	−0.00006	0.0179	0.0	0.0
	0.0	0.0	−0.0469	0.7656	0.0	−0.0293	−0.3270	−0.875
	0.0	−0.1172	−0.6426	0.125	−0.1556	−0.5393	−1.0	−0.0625
	−0.1556	0.0	−0.0156	−0.0623	−0.6426	0.0	−0.0039	0.1479
	Linear part							
	000000000000100000000000000000000000000000000000							
13	000000000000000000000000000000000000100000000000							
14	000000000000100000000000000000000000001000000000							
15	000000000000001000000000000000000000100010000000							
16	000000000000100010000000000000000000000000100000							

Note: The experimental correlation of the first 12 (7 + 5) rounds is $2^{-10.97}$ under 2^{32} sample sizes and 100 random keys, the experimental correlation of the 4 rounds at the bottom is $2^{-3.68}$ under 2^{15} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-10.97} \times (2^{-3.68})^2 = 2^{-18.33}$.

Table 8: Seventeen-round DL distinguisher for SIMON48 with theoretical correlation $2^{-24.66}$ and experimental correlation $2^{-20.39}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-14}, $0.63(=2^{-0.66})$, and 2^{-5}, respectively.

	Differential part							
0	000000100000000000000000000010001000100000000000							
1	000000001000100000000000000000100000000000000000							
2	000000000010000000000000000000001000100000000000							
3	000000000000100000000000000000000010000000000000							
4	000000000000000000000000000000000000100000000000							
5	000000000000100000000000000000000000000000000000							
6	000000000010000000000000000000000000100000000000							
7	000000001000100000000000000000000010000000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	0.0	−1.0	−1.0	−1.0	0.0	−1.0	0.9999	0.0
	−1.0	−1.0	−1.0	0.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
9	−1.0	−1.0	0.0	−0.25	0.9999	0.0	−0.5	−1.0
	1.0	0.0	−0.5	−1.0	1.0	−1.0	−1.0	−1.0
	−0.5	−1.0	−1.0	−1.0	−0.5	−1.0	0.0	−0.25
	0.0	−1.0	−1.0	−1.0	0.0	−1.0	0.9999	0.0
	−1.0	−1.0	−1.0	0.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
10	0.0	−0.0625	0.4688	0.0	0.0	−0.75	−0.9999	2.73×2^{-11}
	−0.1875	−0.75	0.9999	0.0	−0.75	−1.0	−0.25	−0.4688
	−1.0	−1.0	−0.25	−0.4688	0.0	−0.0625	−0.4688	−1.0
	−1.0	−1.0	0.0	−0.25	0.9999	0.0	−0.5	−1.0
	1.0	0.0	−0.5	−1.0	1.0	−1.0	−1.0	−1.0
	−0.5	−1.0	−1.0	−1.0	−0.5	−1.0	0.0	−0.25
11	0.1479	0.0	0.0	−0.0469	0.7656	0.0	−0.0293	−0.3270
	−0.8750	0.0	−0.1172	−0.6426	0.1250	−0.1556	−0.5393	−1.0
	−0.0625	−0.1556	0.0	−0.0156	−0.0623	−0.6426	0.0	−0.0039
	0.0	−0.0625	0.4688	0.0	0.0	−0.75	−0.9999	2.72×2^{-11}
	−0.1875	−0.75	0.9999	0.0	−0.75	−1.0	−0.2500	−0.4688
	−1.0	−1.0	−0.2450	−0.4688	0.0	−0.0625	−0.4688	−1.0
12	0.0	−0.0007	−0.1049	6.82×2^{-13}	0.0	−0.0729	−0.4468	0.0
	−0.0058	−0.1556	−0.0513	0.0	−0.1241	−0.6321	−0.0078	−0.0195
	−0.0	−0.0039	−0.0040	−0.0837	0.0	−0.00006	0.0179	−0.0
	0.1479	0.0	0.0	−0.0469	0.7656	0.0	−0.0293	−0.3270
	−0.8750	0.0	−0.1172	−0.6426	0.1250	−0.1556	−0.5393	−1.0
	−0.0625	−0.1556	0.0	−0.0156	−0.0623	−0.6426	0.0	−0.0039
13	0.0039	0.0	0.0	−0.0009	0.1032	0.0	−0.00004	−0.0130
	−0.0130	-4.19×2^{-17}	−0.0037	−0.1237	0.0004	−0.0008	0.0	−0.0010
	−0.00006	−0.0033	0.0	-2.38×2^{-7}	0.0003	0.0	0.0	-7.15×2^{-7}
	0.0	−0.0007	−0.1049	6.82×2^{-13}	0.0	−0.0729	−0.4468	0.0
	−0.0058	−0.1556	−0.0513	0.0	−0.1241	−0.6321	−0.0078	−0.0195
	−0.0	−0.0039	−0.0040	−0.0837	0.0	−0.00006	0.0179	−0.0

Table 8: Continued.

	Linear part
	000000000000000000000000000000000000010000000000
14	000000000000010000000000000000000000000100000000
15	000000000000000100000000000000000000010001000000
16	000000000000010001000000000000000000000000010000
17	000000000000000000010000000000000000010001000100

Note: The experimental correlation of the first 13 $(7+6)$ rounds is $2^{-10.99}$ under 2^{32} sample sizes and 100 random keys, the experimental correlation of the 4 rounds at the bottom is $2^{-4.70}$ under 2^{18} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-10.99} \times (2^{-4.70})^2 = 2^{-20.39}$.

Table 9: Twenty-round DL distinguisher for SIMON64 with theoretical correlation $2^{-34.58}$ and experimental correlation $2^{-28.64}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are $2^{-14}, 0.66(=2^{-0.58})$, and 2^{-10}, respectively.

	Differential part (optimal differential trail)							
0	0000000000100000000000000000000000000000100010001000000000000000							
7	0000000000001000100000000000000000000000000000100000000000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	−1.0	−1.0	−1.0	−1.0	−0.0	−1.0	−1.0	−1.0
	−0.0	−1.0	1.0	−0.0	−1.0	−1.0	−1.0	−0.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
9	−0.5	−1.0	−0.0	−0.25	−1.0	−1.0	−0.0	−0.25
	1.0	−0.0	−0.5	−1.0	1.0	−0.0	−0.5	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−0.5	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−0.0	−1.0	−1.0	−1.0
	−0.0	−1.0	1.0	−0.0	−1.0	−1.0	−1.0	−0.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
10	−0.0	−0.0625	−0.4688	−1.0	−0.0	−0.0625	0.4688	−0.0
	−0.0	−0.75	−1.0	−0.0	−0.25	−0.75	1.0	−0.0
	−1.0	−1.0	−1.0	−1.0	−0.75	−1.0	−1.0	−1.0
	−0.75	−1.0	−0.25	−0.4688	−1.0	−1.0	−0.25	−0.4688
	−0.5	−1.0	−0.0	−0.25	−1.0	−1.0	−0.0	−0.25
	1.0	−0.0	−0.5	−1.0	1.0	−0.0	−0.5	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−0.5	−1.0	−1.0	−1.0

Table 9: Continued.

11	−0.0623	−0.6426	−0.0	−0.0039	0.1556	−0.0	−0.0	−0.0469
	0.875	−0.0	−0.0625	−0.4688	−0.7656	−0.0	−0.25	−1.0
	0.875	−1.0	−0.4688	−0.6426	−1.0	−1.0	−0.4688	−0.6426
	−0.125	−0.1556	−0.5393	−1.0	−0.0625	−0.1556	−0.0	−0.0156
	−0.0	−0.0625	−0.4688	−1.0	−0.0	−0.0625	0.4688	−0.0
	−0.0	−0.75	−1.0	−0.0	−0.25	−0.75	1.0	−0.0
	−1.0	−1.0	−1.0	−1.0	−0.75	−1.0	−1.0	−1.0
	−0.75	−1.0	−0.25	−0.4688	−1.0	−1.0	−0.25	−0.4688
12	−0.0	−0.00006	0.0195	−0.0	−0.0	−0.0007	−0.1342	−0.0
	−0.0	−0.1868	−0.4129	−0.0	−0.0313	−0.4688	−0.6426	−0.0
	−0.2637	−0.2727	−0.6321	−1.0	−0.1868	−0.2727	−0.0513	−0.0445
	−0.1241	−0.6321	−0.0078	−0.0195	−0.0	−0.0039	−0.0040	−0.0837
	−0.0623	−0.6426	−0.0	−0.0039	0.1556	−0.0	−0.0	−0.0469
	0.875	−0.0	−0.0625	−0.4688	−0.7656	−0.0	−0.25	−1.0
	0.875	−1.0	−0.4688	−0.6426	−1.0	−1.0	−0.4688	−0.6426
	−0.125	−0.1556	−0.5393	−1.0	−0.0625	−0.1556	−0.0	−0.0156
13	0.0003	−0.0	−0.0	-7.15×2^{-7}	0.0054	−0.0	−0.0	−0.0022
	0.1355	−0.0	−0.0008	−0.1133	−0.2144	−0.0	−0.0173	−0.09
	0.1978	−0.6659	−0.0441	−0.0530	−0.0163	−0.0117	−0.0153	−0.1237
	−0.0004	−0.0008	−0.0	−0.0010	−0.00006	−0.0033	−0.0	-2.38×2^{-7}
	−0.0	−0.00006	0.0195	−0.0	−0.0	−0.0007	−0.1342	−0.0
	−0.0	−0.1868	−0.4129	−0.0	−0.0313	−0.4688	−0.6426	−0.0
	−0.2637	−0.2727	−0.6321	−1.0	−0.1868	−0.2727	−0.0513	−0.0445
	−0.1241	−0.6321	−0.0078	−0.0195	−0.0	−0.0039	−0.0040	−0.0837
14	−0.0	-1.09×2^{-11}	−0.00002	−0.0	−0.0	-4.01×2^{-7}	0.0046	−0.0
	−0.0	−0.0088	−0.0257	−0.0	−0.00014	−0.0109	0.0352	−0.0
	−0.0048	−0.0038	−0.0027	−0.0030	−0.0007	−0.0086	-5.75×2^{-6}	-8.48×2^{-6}
	−0.0	−0.0002	-1.21×2^{-7}	−0.00001	−0.0	-2.33×2^{-10}	2.99×2^{-7}	−0.0
	0.0003	−0.0	−0.0	-7.15×2^{-7}	0.0054	−0.0	−0.0	−0.0022
	0.1355	−0.0	−0.00080	−0.1133	−0.2144	−0.0	−0.0173	−0.0900
	0.1978	−0.6659	−0.0441	−0.0530	−0.0163	−0.0117	−0.0153	−0.1237
	−0.0004	−0.0008	−0.0	−0.0010	−0.00006	−0.0033	−0.0	-2.38×2^{-7}
Linear part								
	0000000000000000000000000000000000000000000000000100000000000000							
15	0000000000000000010000000000000000000000000000000001000000000000							
16	0000000000000000000100000000000000000000000000000100010000000000							
17	0000000000000000010001000000000000000000000000000000000100000000							
18	0000000000000000000000010000000000000000000000000100010001000000							
19	0000000000000000010001000100000000000000000000000001000000010000							
20	0000000000000000000100000001000000000000000000000100000001000100							

Note: The experimental correlation of the first 14 (7 + 7) rounds is $2^{-10.52}$ under 2^{32} sample sizes and 100 random keys, the experimental correlation of the 6 rounds at the bottom is $2^{-9.06}$ under 2^{25} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-10.52}\times(2^{-9.06})^2 = 2^{-28.64}$.

Table 10: Twenty-five-round DL distinguisher for SIMON96 with theoretical correlation $2^{-46.66}$ and experimental correlation $2^{-42.46}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-26}, $0.63(=2^{-0.66})$, and 2^{-10}, respectively.

	Differential part (optimal differential trail)							
0	000000000000000000010001000100000000000000000000							
	000000000000000001000000010000000000000000000000							
10	000000000000000000010001000100000000000000000000							
	000000000000000000000100000000000000000000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	1.0
	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
11	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−0.0	−1.0	−1.0	−1.0	−0.0
	−1.0	1.0	−0.0	−0.0	−1.0	−1.0	−0.0	−1.0
	−1.0	1.0	−0.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	1.0
	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
12	−1.0	−1.0	−1.0	−0.5	−1.0	−1.0	−1.0	−0.5
	−1.0	−0.0	−0.25	−0.5	−1.0	−0.0	−0.25	1.0
	−0.0	−0.0	−0.25	1.0	−0.0	−0.5	−1.0	−1.0
	−0.0	−0.5	−1.0	1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−0.0	−1.0	−1.0	−1.0	−0.0
	−1.0	1.0	−0.0	−0.0	−1.0	−1.0	−0.0	−1.0
	−1.0	1.0	−0.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
13	−1.0	−0.25	−0.4688	−0.75	−1.0	−0.25	−0.4688	−0.0
	−0.0625	−0.156	−0.4688	−0.0	−0.0625	0.4688	−0.0	−0.0
	−0.0625	−0.4688	−0.0	−0.0	−0.75	−1.0	−0.0	−0.25
	−0.75	−1.0	−0.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−0.75	−1.0	−1.0	−1.0	−0.75
	−1.0	−1.0	−1.0	−0.5	−1.0	−1.0	−1.0	−0.5
	−1.0	−0.0	−0.25	−0.5	−1.0	−0.0	−0.25	1.0
	−0.0	−0.0	−0.25	1.0	−0.0	−0.5	−1.0	−1.0
	−0.0	−0.5	−1.0	1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0

Table 10: Continued.

14	−0.1556	−0.3184	−0.6426	−0.0625	−0.1556	−0.0	−0.0156	−0.0208
	−0.1440	−0.0	−0.0039	0.0623	−0.0	−0.0	−0.0039	0.1556
	−0.0	−0.0	−0.0469	0.875	−0.0	−0.0625	−0.4688	−0.875
	−0.0	−0.25	−1.0	1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−0.875	−1.0	−1.0	−1.0	−0.875
	−1.0	−0.4688	−0.6426	−0.875	−1.0	−0.4688	−0.6426	−0.125
	−1.0	−0.25	−0.4688	−0.75	−1.0	−0.25	−0.4688	−0.0
	−0.0625	−0.1563	−0.4688	−0.0	−0.0625	0.4688	−0.0	−0.0
	−0.0625	−0.4688	−0.0	−0.0	−0.75	−1.0	−0.0	−0.25
	−0.75	−1.0	−0.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−0.75	−1.0	−1.0	−1.0	−0.75
15	−0.2423	−0.0064	−0.0195	−0.0	−0.0039	−0.0013	−0.0173	−0.0
	−0.00006	0.0024	−0.0	−0.0	−0.00006	−0.0195	−0.0	−0.0
	−0.0007	0.1342	−0.0	−0.0	−0.1868	−0.6426	−0.0	−0.0313
	−0.46875	1.0	−0.0	−0.9375	−1.0	−1.0	−1.0	−0.9375
	−1.0	−0.6426	−0.77	−0.9375	−1.0	−0.6426	−0.77	−0.2637
	−0.2727	−0.4737	−0.77	−0.1868	−0.2727	−0.0513	−0.0445	−0.0704
	−0.1556	−0.3184	−0.6426	−0.0625	−0.1556	−0.0	−0.0156	−0.0208
	−0.1440	−0.0	−0.0039	0.0623	−0.0	−0.0	−0.0039	0.1556
	−0.0	−0.0	−0.0469	0.875	−0.0	−0.0625	−0.4688	−0.875
	−0.0	−0.25	−1.0	1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−0.875	−1.0	−1.0	−1.0	−0.875
	−1.0	−0.4688	−0.6426	−0.875	−1.0	−0.4688	−0.6426	−0.125
16	−0.0008	−0.0	−0.0006	−0.00002	−0.0007	−0.0	-2.38×2^{-7}	0.00001
	−0.0	−0.0	-5.96×2^{-8}	0.0003	−0.0	−0.0	-7.15×2^{-7}	−0.0054
	−0.0	−0.0	−0.0022	0.3232	−0.0	−0.00098	−0.1133	0.6225
	−0.0	−0.0962	−0.8573	0.9688	−1.0	−0.77	−0.8573	−0.4060
	−0.4024	−0.6114	−0.8573	−0.3336	−0.4024	−0.1227	−0.09	−0.1412
	−0.3524	−0.0390	−0.0530	−0.0143	−0.0117	−0.0086	−0.0424	−0.0002
	−0.2423	−0.0064	−0.0195	−0.0	−0.0039	−0.0013	−0.0173	−0.0
	−0.00006	0.0024	−0.0	−0.0	−0.00006	−0.0195	−0.0	−0.0
	−0.0007	0.1342	−0.0	−0.0	−0.1868	−0.6426	−0.0	−0.03125
	−0.46875	1.0	−0.0	−0.9375	−1.0	−1.0	−1.0	−0.9375
	−1.0	−0.6426	−0.77	−0.9375	−1.0	−0.6426	−0.77	−0.2637
	−0.2727	−0.4737	−0.77	−0.1868	−0.2727	−0.0513	−0.0445	−0.0704
	Linear part							
	000000000000000000000000001000100010000000000000							
	000000000000000000000000000000001000000000000000							
17	000000000000000000000000000000001000000000000000							
	000000000000000000000000001000100000000000000000							
18	000000000000000000000000001000100000000000000000							
	000000000000000000000000000010000000000000000000							
19	000000000000000000000000000010000000000000000000							
	000000000000000000000000001000000000000000000000							
20	000000000000000000000000001000000000000000000000							
	000000000000000000000000000000000000000000000000							
21	000000000000000000000000000000000000000000000000							
	000000000000000000000000001000000000000000000000							
22	000000000000000000000000001000000000000000000000							
	000000000000000000000000000100000000000000000000							
23	000000000000000000000000000100000000000000000000							
	000000000000000000000000001000100000000000000000							
24	000000000000000000000000001000100000000000000000							
	000000000000000000000000000000001000000000000000							
25	000000000000000000000000000000001000000000000000							
	000000000000000000000000001000100010000000000000							

Note: The experimental correlation of the first 10 rounds is $2^{-23.39}$ under 2^{32} sample sizes and 100 random keys, the experimental correlation of the 6 rounds at the DL part is $2^{-0.51}$ under 2^{8} sample sizes and 100 random keys, the experimental correlation of the 9 rounds at the bottom is $2^{-9.28}$ under 2^{28} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-23.39} \times 2^{-0.51} \times (2^{-9.28})^2 = 2^{-42.46}$.

Table 11: Twenty-six-round DL distinguisher for SIMON96 with theoretical correlation $2^{-50.66}$ and experimental correlation $2^{-45.69}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-30}, $0.63(=2^{-0.66})$, and 2^{-10}, respectively.

	Differential part (optimal differential trail)							
0	000000010000000010000000000000000000000000000000 000001000100000000100000000000000000000000000000							
11	000000000100010001000000000000000000000000000000 000000000001000000000000000000000000000000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0
	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
12	−1.0	−0.0	−1.0	−1.0	−1.0	−0.0	−1.0	1.0
	−0.0	−0.0	−1.0	−1.0	−0.0	−1.0	−1.0	1.0
	−0.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0
	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
13	−0.25	−0.5	−1.0	−0.0	−0.25	1.0	−0.0	−0.0
	−0.25	1.0	−0.0	−0.5	−1.0	−1.0	−0.0	−0.5
	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.5	−1.0	−1.0	−1.0	−0.5	−1.0	−0.0
	−1.0	−0.0	−1.0	−1.0	−1.0	−0.0	−1.0	1.0
	−0.0	−0.0	−1.0	−1.0	−0.0	−1.0	−1.0	1.0
	−0.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
14	−0.4688	−0.0	−0.0625	0.4688	−0.0	−0.0	−0.0625	−0.4688
	−0.0	−0.0	−0.75	−1.0	−0.0	−0.25	−0.75	−1.0
	−0.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.75	−1.0	−1.0	−1.0	−0.75	−1.0	−0.25
	−0.4688	−0.75	−1.0	−0.25	−0.4688	−0.0	−0.0625	−0.1563
	−0.25	−0.5	−1.0	−0.0	−0.25	1.0	−0.0	−0.0
	−0.25	1.0	−0.0	−0.5	−1.0	−1.0	−0.0	−0.5

Table 11: Continued.

	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.5	−1.0	−1.0	−1.0	−0.5	−1.0	−0.0
15	−0.0039	0.0623	−0.0	−0.0	−0.0039	0.1556	−0.0	−0.0
	−0.0468	0.875	−0.0	−0.0625	−0.4688	−0.875	−0.0	−0.25
	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.875	−1.0	−1.0	−1.0	−0.875	−1.0	−0.4688
	−0.6426	−0.875	−1.0	−0.4688	−0.6426	−0.125	−0.1556	−0.3184
	−0.6426	−0.0625	−0.1556	−0.0	−0.0156	−0.0208	−0.1440	−0.0
	−0.4688	−0.0	−0.0625	0.4688	−0.0	−0.0	−0.0625	−0.4688
	−0.0	−0.0	−0.75	−1.0	−0.0	−0.25	−0.75	−1.0
	−0.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.75	−1.0	−1.0	−1.0	−0.75	−1.0	−0.25
	−0.4688	−0.75	−1.0	−0.25	−0.4688	−0.0	−0.0625	−0.1563
16	−0.0	−0.0	−0.00006	−0.0195	−0.0	−0.0	−0.0007	0.1342
	−0.0	−0.0	−0.1868	−0.6426	−0.0	−0.0313	−0.4688	1.0
	−0.0	−0.9375	−1.0	−1.0	−1.0	−0.9375	−1.0	−0.6426
	−0.77	−0.9375	−1.0	−0.6426	−0.77	−0.2637	−0.2727	−0.4737
	−0.77	−0.1868	−0.2727	−0.0513	−0.0445	−0.0704	−0.2423	−0.0064
	−0.0195	−0.0	−0.0039	−0.0013	−0.0173	−0.0	−0.00006	0.0024
	−0.0039	0.0623	−0.0	−0.0	−0.0039	0.1556	−0.0	−0.0
	−0.0469	0.875	−0.0	−0.0625	−0.4688	−0.875	−0.0	−0.25
	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.875	−1.0	−1.0	−1.0	−0.875	−1.0	−0.4688
	−0.6426	−0.875	−1.0	−0.4688	−0.6426	−0.125	−0.1556	−0.3184
	−0.6426	−0.0625	−0.1556	−0.0	−0.0156	−0.0208	−0.1440	−0.0
17	-5.96×2^{-8}	0.0003	−0.0	−0.0	-7.15×2^{-7}	−0.0054	−0.0	−0.0
	−0.0022	0.3232	−0.0	−0.00098	−0.1133	0.6225	−0.0	−0.0962
	−0.8573	0.9688	−1.0	−0.77	−0.8573	−0.4060	−0.4024	−0.6114
	−0.8573	−0.3336	−0.4024	−0.1227	−0.09	−0.1412	−0.3524	−0.039
	−0.0530	−0.0143	−0.0117	−0.0086	−0.0424	−0.0002	−0.0008	−0.0
	−0.0006	−0.00002	−0.0007	−0.0	-2.38×2^{-7}	0.00001	−0.0	−0.0
	−0.0	−0.0	−0.00006	−0.0195	−0.0	−0.0	−0.0007	0.1342
	−0.0	−0.0	−0.1868	−0.6426	−0.0	−0.0313	−0.4688	1.0
	−0.0	−0.9375	−1.0	−1.0	−1.0	−0.9375	−1.0	−0.6426
	−0.77	−0.9375	−1.0	−0.6426	−0.77	−0.2637	−0.2727	−0.4737
	−0.77	−0.1868	−0.2727	−0.0513	−0.0445	−0.0704	−0.2423	−0.0064
	−0.0195	−0.0	−0.0039	−0.0013	−0.0173	−0.0	−0.00006	0.0024
	Linear Part							
	000000000000000010001000100000000000000000000000							
	000000000000000000000010000000000000000000000000							
18	000000000000000000000010000000000000000000000000							
	000000000000000010001000000000000000000000000000							
19	000000000000000010001000000000000000000000000000							
	000000000000000000100000000000000000000000000000							
20	000000000000000000100000000000000000000000000000							
	000000000000000010000000000000000000000000000000							
21	000000000000000010000000000000000000000000000000							
	000000000000000000000000000000000000000000000000							

Table 11: Continued.

22	000000000000000000000000000000000000000000000000 000000000000000010000000000000000000000000000000
23	000000000000000010000000000000000000000000000000 000000000000000000100000000000000000000000000000
24	000000000000000000100000000000000000000000000000 000000000000000010001000000000000000000000000000
25	000000000000000010001000000000000000000000000000 000000000000000000000010000000000000000000000000
26	000000000000000000000010000000000000000000000000 000000000000000010001000100000000000000000000000

Note: The experimental correlation of the first 11 rounds is $2^{-26.60}$ under 2^{32} sample sizes and 100 random keys, the experimental correlation of the 6 rounds at the DL part is $2^{-0.49}$ under 2^{8} sample sizes and 100 random keys, the experimental correlation of the 9 rounds at the bottom is $2^{-9.30}$ under 2^{28} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-26.60} \times 2^{-0.49} \times (2^{-9.30})^2 = 2^{-45.69}$.

Table 12: Thirty-one-round DL distinguisher for SIMON128 with theoretical correlation $2^{-62.70}$ and experimental correlation $2^{-58.78}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-26}, $0.61(=2^{-0.70})$, and 2^{-18}, respectively.

	Differential part (optimal differential trail)							
0	0000000000000000000000000000000000000000100010001000000000000000 0000000000000000000000000000000000000010000000100000000000000000							
10	0000000000000000000000000000000000000000100010001000000000000000 0000000000000000000000000000000000000000001000000000000000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
11	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.0	−1.0	−1.0	−1.0	−0.0	−1.0	1.0	−0.0
	−0.0	−1.0	−1.0	−0.0	−1.0	−1.0	1.0	−0.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0

Table 12: Continued.

	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
12	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.5	−1.0	−1.0	−1.0	−0.5	−1.0	−0.0	−0.25
	−0.5	−1.0	−0.0	−0.25	1.0	−0.0	−0.0	−0.25
	1.0	−0.0	−0.5	−1.0	−1.0	−0.0	−0.5	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.0	−1.0	−1.0	−1.0	−0.0	−1.0	1.0	−0.0
	−0.0	−1.0	−1.0	−0.0	−1.0	−1.0	1.0	−0.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
13	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.75	−1.0	−1.0	−1.0	−0.75	−1.0	−0.25	−0.4688
	−0.75	−1.0	−0.25	−0.4688	−0.0	−0.0625	−0.1563	−0.4688
	−0.0	−0.0625	0.4688	−0.0	−0.0	−0.0625	−0.4688	−0.0
	−0.0	−0.75	−1.0	−0.0	−0.25	−0.75	−1.0	−0.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.5	−1.0	−1.0	−1.0	−0.5	−1.0	−0.0	−0.25
	−0.5	−1.0	−0.0	−0.25	1.0	−0.0	−0.0	−0.25
	1.0	−0.0	−0.5	−1.0	−1.0	−0.0	−0.5	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
14	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.875	−1.0	−1.0	−1.0	−0.875	−1.0	−0.4688	−0.6426
	−0.875	−1.0	−0.4688	−0.6426	−0.125	−0.1556	−0.3184	−0.6426
	−0.0625	−0.1556	−0.0	−0.0156	−0.0208	−0.1440	−0.0	−0.0039
	0.0623	−0.0	−0.0	−0.0039	0.1556	−0.0	−0.0	−0.0469
	0.875	−0.0,	−0.0625	−0.4688	−0.875	−0.0	−0.25	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0,	−1.0	−1.0	−1.0
	−0.75	−1.0	−1.0	−1.0	−0.75	−1.0	−0.25	−0.4688
	−0.75	−1.0	−0.25	−0.4688	−0.0	−0.0625	−0.1563	−0.4688
	−0.0	−0.0625	0.4688	−0.0	−0.0	−0.0625	−0.4688	−0.0
	−0.0	−0.75	−1.0	−0.0	−0.25	−0.75	−1.0	−0.0

Table 12: Continued.

	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
15	−0.9375	−1.0	−1.0	−1.0	−0.9375	−1.0	−0.6426	−0.77
	−0.9375	−1.0	−0.6426	−0.77	−0.2637	−0.2727	−0.4737	−0.77
	−0.1868	−0.2727	−0.0513	−0.0445	−0.0704	−0.2423	−0.0064	−0.0195
	−0.0	−0.0039	−0.0013	−0.0173	−0.0	−0.00006	0.0024	−0.0
	−0.0	−0.00006	−0.0195	−0.0	−0.0	−0.0007	0.1342	−0.0
	−0.0	−0.1868	−0.6426	−0.0	−0.03125	−0.4688	1.0	−0.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.875	−1.0	−1.0	−1.0	−0.875	−1.0	−0.4688	−0.6426
	−0.875	−1.0	−0.4688	−0.6426	−0.125	−0.1556	−0.3184	−0.6426
	−0.0625	−0.1556	−0.0	−0.0156	−0.0208	−0.1440	−0.0	−0.0039
	0.0623	−0.0	−0.0	−0.0039	0.1556	−0.0	−0.0	−0.0469
	0.875	−0.0	−0.0625	−0.46875	−0.875	−0.0	−0.25	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
16	−0.9688	−1.0	−0.77	−0.8573	−0.4060	−0.4024	−0.6114	−0.8573
	−0.3336	−0.4024	−0.1227	−0.09	−0.1412	−0.3524	−0.0390	−0.0530
	−0.0143	−0.0117	−0.0086	−0.0424	−0.0002	−0.0008	−0.0	−0.0006
	−0.00002	−0.0007	−0.0	-2.38×2^{-7}	0.00001	−0.0	−0.0	-5.96×2^{-8}
	0.0003	−0.0	−0.0	-7.15×2^{-7}	−0.0054	−0.0	−0.0	−0.0022
	0.3336	−0.0	−0.00098	−0.1133	0.6426	−0.0	−0.125	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.9688	−1.0	−1.0	−1.0	−0.9688	−1.0	−0.77	−0.8573
	−0.9375	−1.0	−1.0	−1.0	−0.9375	−1.0	−0.6426	−0.77
	−0.9375	−1.0	−0.6426	−0.77	−0.2637	−0.2727	−0.4737	−0.77
	−0.1868	−0.2727	−0.0513	−0.0445	−0.0704	−0.2423	−0.0064	−0.0195
	−0.0	−0.0039	−0.0013	−0.017	−0.0	−0.00006	0.0024	−0.0
	−0.0	−0.00006	−0.0195	−0.0	−0.0	−0.0007	0.1342	−0.0
	−0.0	−0.1868	−0.6426	−0.0	−0.0313	−0.4688	1.0	−0.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
17	−0.4813	−0.5320	−0.2116	−0.1542	−0.2293	−0.4671	−0.1034	−0.1088
	−0.0409	−0.0255	−0.0249	−0.0807	−0.0035	−0.0038	−0.0018	−0.0023
	−0.0004	−0.0029	-3.33×2^{-6}	-8.47×2^{-6}	−0.0	−0.00003	-3.32×2^{-8}	-3.28×2^{-6}
	−0.0	-2.33×2^{-10}	4.17×2^{-9}	−0.0	−0.0	-9.09×2^{-13}	-1.85×2^{-7}	−0.0
	−0.0	-1.09×2^{-11}	−0.00002	−0.0	−0.0	-4.01×2^{-7}	−0.0126	−0.0
	−0.0	−0.0106	0.2298	−0.0	−0.0020	−0.2637	−1.0	−0.0
	−0.9844	−1.0	−1.0	−1.0	−0.9844	−1.0	−0.8573	−0.9142
	−0.9844	−1.0	−0.8573	−0.9142	−0.5413	−0.5320	−0.7248	−0.9142
	−0.9688	−1.0	−0.77	−0.8573	−0.4060	−0.4024	−0.6114	−0.8573
	−0.3336	−0.4024	−0.1227	−0.09	−0.1412	−0.3524	−0.0390	−0.0530
	−0.0143	−0.0117	−0.0086	−0.0424	−0.00025	−0.0008	−0.0	−0.0006
	−0.00002	−0.0007	−0.0	-2.38×2^{-7}	0.00001	−0.0	−0.0	-5.96×2^{-8}
	0.0003	−0.0	−0.0	-7.15×2^{-7}	−0.0054	−0.0	−0.0	−0.0022
	0.3336	−0.0	−0.0010	−0.1133	0.6426	−0.0	−0.125	−1.0
	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.9688	−1.0	−1.0	−1.0	−0.9688	−1.0	−0.77	−0.8573
18	−0.0817	−0.0479	−0.0522	−0.1330	−0.0155	−0.0121	−0.0069	−0.0057
	−0.0021	−0.0083	−0.0001	−0.00008	−0.00006	−0.0002	-3.98×2^{-6}	−0.00003

Table 12: Continued.

	-1.19×2^{-8}	-2.48×2^{-8}	−0.0	-4.03×2^{-7}	-2.07×2^{-12}	-6.24×2^{-10}	−0.0	-3.65×2^{-14}
	2.15×2^{-14}	−0.0	−0.0	-5.42×2^{-20}	5.85×2^{-13}	−0.0	−0.0	-1.63×2^{-19}
	1.99×2^{-9}	−0.0	−0.0	-7.17×2^{-14}	−0.00001	−0.0	−0.0	-5.79×2^{-6}
	−0.0384	−0.0	-9.54×2^{-7}	−0.0150	0.4028	−0.0	−0.0571	−0.9496
	0.9922	−1.0	−0.9142	−0.9496	−0.6607	−0.6503	−0.8125	−0.9496
	−0.6151	−0.6503	−0.3138	−0.2366	−0.3306	−0.5783	−0.1957	−0.1873
	−0.4813	−0.5320	−0.2116	−0.1542	−0.2293	−0.4671	−0.1034	−0.1088
	−0.0409	−0.0255	−0.0249	−0.0807	−0.0035	−0.0038	−0.0018	−0.0023
	−0.0004	−0.0029	-3.33×2^{-6}	-8.47×2^{-6}	−0.0	−0.00003	-3.32×2^{-8}	-3.28×2^{-6}
	−0.0	-2.33×2^{-10}	4.17×2^{-9}	−0.0	−0.0	-9.09×2^{-13}	-1.85×2^{-7}	−0.0
	−0.0	-1.09×2^{-11}	−0.00002	−0.0	−0.0	-4.01×2^{-7}	−0.0126	−0.0
	−0.0	−0.0106	0.2298	−0.0	−0.0020	−0.2637	−1.0	−0.0
	−0.9844	−1.0	−1.0	−1.0	−0.9844	−1.0	−0.8573	−0.9142
	−0.9844	−1.0	−0.8573	−0.9142	−0.5413	−0.5320	−0.7248	−0.9142
19	−0.0066	−0.0188	−0.0009	−0.0005	−0.0004	−0.0007	−0.00005	−0.0002
	-1.19×2^{-6}	-5.42×2^{-7}	-3.94×2^{-7}	-4.08×2^{-6}	-3.46×2^{-9}	-3.63×2^{-8}	-5.32×2^{-12}	-1.42×2^{-11}
	−0.0	-2.94×2^{-10}	-1.72×2^{-18}	-1.32×2^{-15}	−0.0	-3.47×2^{-19}	1.79×2^{-22}	−0.0
	−0.0	-3.16×2^{-30}	-6.10×2^{-22}	−0.0	−0.0	-3.70×2^{-32}	9.18×2^{-17}	−0.0
	−0.0	-1.96×2^{-25}	-1.12×2^{-10}	−0.0	−0.0	-5.81×2^{-13}	−0.0001	−0.0
	−0.0	−0.00007	−0.0450	−0.0	−0.00004	−0.1092	0.8765	−0.0
	−0.7267	−0.7499	−0.4231	−0.3339	−0.4391	−0.6791	−0.3073	−0.2850
	−0.1379	−0.0814	−0.0922	−0.1992	−0.0424	−0.0301	−0.0177	−0.0119
	−0.0817	−0.0479	−0.0522	−0.1330	−0.0155	−0.0121	−0.0069	−0.0057
	−0.0021	−0.0083	−0.0001	−0.00008	−0.00006	−0.0002	-3.98×2^{-6}	−0.00003
	-3.46×2^{-9}	-1.19×2^{-8}	-2.48×2^{-8}	−0.0	-4.03×2^{-7}	-2.0654×2^{-12}	-6.24×2^{-10}	$-0.0,\ -3.65\times2^{-14}$
	2.15×2^{-14}	−0.0	−0.0	-5.42×2^{-20}	5.85×2^{-13}	−0.0	−0.0	-1.63×2^{-19}
	1.99×2^{-9}	−0.0	−0.0	-7.17×2^{-14}	−0.00001	−0.0	−0.0	-5.79×2^{-6}
	−0.0384	−0.0	-9.54×2^{-7}	−0.0150	0.4028	−0.0	−0.0571	−0.9496
	0.9922	−1.0	−0.9142	−0.9496	−0.6607	−0.6503	−0.8125	−0.9496
	−0.6151	−0.6503	−0.3138	−0.2366	−0.3306	−0.5783	−0.1957	−0.1873
	Linear part							
	0000000000000000000000000000000000000000000000000000010000000000 0000000000000000000000000000000000000000000000010001000000000000							
20	0000000000000000000000000000000000000000000000010001000000000000 0000000000000000000000000000000000000000000000000100000000000000							
21	0000000000000000000000000000000000000000000000000100000000000000 0000000000000000000000000000000000000000000000010000000000000000							
22	0000000000000000000000000000000000000000000000010000000000000000 0000000000000000000000000000000000000000000000000000000000000000							
23	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000010000000000000000							
24	0000000000000000000000000000000000000000000000010000000000000000 0000000000000000000000000000000000000000000000000100000000000000							
25	0000000000000000000000000000000000000000000000000100000000000000 0000000000000000000000000000000000000000000000010001000000000000							
26	0000000000000000000000000000000000000000000000010001000000000000 0000000000000000000000000000000000000000000000000000010000000000							
27	0000000000000000000000000000000000000000000000000000010000000000 0000000000000000000000000000000000000000000000010001000100000000							
28	0000000000000000000000000000000000000000000000010001000100000000 0000000000000000000000000000000000000000000000000100000001000000							

Table 12: Continued.

29	0000000000000000000000000000000000000000000000000100000001000000 0000000000000000000000000000000000000000000000010000000100010000
30	0000000000000000000000000000000000000000000000010000000100010000 0000000000000000000000000000000000000000000000000000000000000100
31	0000000000000000000000000000000000000000000000000000000000000100 0000010000000000000000000000000000000000000000010000000100010001

Note: The experimental correlation of the first 10 rounds is $2^{-22.47}$ under 2^{32} sample sizes and 100 random keys, and the experimental correlation of the 9 rounds at the DL part is $2^{-0.31}$ under 2^{8} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-22.47} \times 2^{-0.31} \times (2^{-18})^2 = 2^{-58.78}$.

Table 13: Thirty-two-round DL distinguisher for SIMON128 with theoretical correlation $2^{-66.70}$ and experimental correlation $2^{-63.99}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-30}, $0.61(=2^{-0.70})$, and 2^{-18}, respectively.

	Differential part (optimal differential trail)							
0	0000000000000000000001000000010000000000000000000000000000000000 0000000000000000000100010000000100000000000000000000000000000000							
11	0000000000000000000000010001000100000000000000000000000000000000 0000000000000000000000000100000000000000000000000000000000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	1.0
	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
12	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.0
	−1.0	−1.0	−1.0	−0.0	−1.0	1.0	−0.0	−0.0
	−1.0	−1.0	−0.0	−1.0	−1.0	1.0	−0.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	1.0
	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0

Table 13: Continued.

13	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.5
	−1.0	−1.0	−1.0	−0.5	−1.0	−0.0	−0.25	−0.5
	−1.0	−0.0	−0.25	1.0	−0.0	−0.0	−0.25	1.0
	−0.0	−0.5	−1.0	−1.0	−0.0	−0.5	−1.0	1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.0
	−1.0	−1.0	−1.0	−0.0	−1.0	1.0	−0.0	−0.0
	−1.0	−1.0	−0.0	−1.0	−1.0	1.0	−0.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
14	−1.0	−1.0	−1.0	−0.75	−1.0	−0.25	−0.4688	−0.75
	−1.0	−0.25	−0.4688	−0.0	−0.0625	−0.1563	−0.4688	−0.0
	−0.0625	0.4688	−0.0	−0.0	−0.0625	−0.4688	−0.0	−0.0
	−0.75	−1.0	−0.0	−0.25	−0.75	−1.0	−0.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.75
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.5
	−1.0	−1.0	−1.0	−0.5	−1.0	−0.0	−0.25	−0.5
	−1.0	−0.0	−0.25	1.0	−0.0	−0.0	−0.25	1.0
	−0.0	−0.5	−1.0	−1.0	−0.0	−0.5	−1.0	1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
15	−1.0	−0.4688	−0.6426	−0.125	−0.1556	−0.3184	−0.6426	−0.0625
	−0.1556	−0.0	−0.0156	−0.0208	−0.1440	−0.0	−0.0039	0.0623
	−0.0	−0.0	−0.0039	0.1556	−0.0	−0.0	−0.0469	0.875
	−0.0	−0.0625	−0.4688	−0.875	−0.0	−0.25	−1.0	1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.875
	−1.0	−1.0	−1.0	−0.875	−1.0	−0.4688	−0.6426	−0.875
	−1.0	−1.0	−1.0	−0.75	−1.0	−0.25	−0.4688	−0.75
	−1.0	−0.25	−0.4688	−0.0	−0.0625	−0.15625	−0.4688	−0.0
	−0.0625	0.4688	−0.0	−0.0	−0.0625	−0.4688	−0.0	−0.0
	−0.75	−1.0	−0.0	−0.25	−0.75	−1.0	−0.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.75
16	−0.2727	−0.0513	−0.0445	−0.0704	−0.2423	−0.0064	−0.0195	−0.0
	−0.0039	−0.0013	−0.0173	−0.0	−0.00006	0.0024	−0.0	−0.0
	−0.0000	−0.0195	−0.0	−0.0	−0.0007	0.1342	−0.0	−0.0
	−0.1868	−0.6426	−0.0	−0.03125	−0.4688	1.0	−0.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.9375

Table 13: Continued.

	−1.0	−1.0	−1.0	−0.9375	−1.0	−0.6426	−0.77	−0.9375
	−1.0	−0.6426	−0.77	−0.2637	−0.2727	−0.4737	−0.77	−0.1868
	−1.0	−0.4688	−0.6426	−0.125	−0.1556	−0.3184	−0.6426	−0.0625
	−0.1556	−0.0	−0.0156	−0.0208	−0.1440	−0.0	−0.0039	0.0623
	−0.0	−0.0	−0.0039	0.1556	−0.0	−0.0	−0.0469	0.875
	−0.0	−0.0625	−0.4688	−0.875	−0.0	−0.25	−1.0	1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.875
	−1.0	−1.0	−1.0	−0.875	−1.0	−0.4688	−0.6426	−0.875
17	−0.0117	−0.0086	−0.0424	−0.0002	−0.0008	−0.0	−0.0006	−0.00002
	−0.0007	−0.0	-2.38×2^{-7}	0.00001	−0.0	−0.0	-5.96×2^{-8}	0.0003
	−0.0	−0.0	-7.15×2^{-7}	−0.0054	−0.0	−0.0	−0.0022	0.3336
	−0.0	−0.00098	−0.1133	0.6426	−0.0	−0.125	−1.0	1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.9688
	−1.0	−1.0	−1.0	−0.9688	−1.0	−0.77	−0.8573	−0.9688
	−1.0	−0.77	−0.8573	−0.4060	−0.4024	−0.6114	−0.8573	−0.3336
	−0.4024	−0.1227	−0.09	−0.1412	−0.3524	−0.0390	−0.0530	−0.0143
	−0.2727	−0.0513	−0.0445	−0.0704	−0.2423	−0.0064	−0.0195	−0.0
	−0.0039	−0.0013	−0.0173	−0.0	−0.0000	0.0024	−0.0	−0.0
	−0.00006	−0.0195	−0.0	−0.0	−0.0007	0.1342	−0.0	−0.0
	−0.1868	−0.6426	−0.0	−0.0313	−0.4688	1.0	−0.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.9375
	−1.0	−1.0	−1.0	−0.9375	−1.0	−0.6426	−0.77	−0.9375
	−1.0	−0.6426	−0.77	−0.2637	−0.2727	−0.4737	−0.77	−0.1868
18	−0.0029	-3.33×2^{-6}	-8.47×2^{-6}	−0.0	−0.00003	-3.32×2^{-8}	-3.28×2^{-6}	−0.0
	-2.3283×2^{-10}	4.17×2^{-9}	−0.0	−0.0	-9.09×2^{-13}	-1.85×2^{-7}	−0.0	−0.0
	-1.09×2^{-11}	−0.00002	−0.0	−0.0	-4.01×2^{-7}	−0.0126	−0.0	−0.0
	−0.0106	0.2298	−0.0	−0.0020	−0.2637	−1.0	−0.0	−0.9844
	−1.0	−1.0	−1.0	−0.9844	−1.0	−0.8573	−0.9142	−0.9844
	−1.0	−0.8573	−0.9142	−0.5413	−0.5320	−0.7248	−0.9142	−0.4813
	−0.5320	−0.2116	−0.1542	−0.2293	−0.4671	−0.1034	−0.1088	−0.0409
	−0.0255	−0.0249	−0.0807	−0.0035	−0.0038	−0.0018	−0.0023	−0.0004
	−0.0117	−0.0086	−0.0424	−0.0002	−0.0008	−0.0	−0.0006	−0.00002
	−0.0007	−0.0	-2.38×2^{-7}	0.00001	−0.0	−0.0	-5.96×2^{-8}	0.0003
	−0.0	−0.0	-7.15×2^{-7}	−0.0054	−0.0	−0.0	−0.0022	0.3336
	−0.0	−0.0010	−0.1133	0.6426	−0.0	−0.125	−1.0	1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.96875
	−1.0	−1.0	−1.0	−0.9688	−1.0	−0.77	−0.8573	−0.9688
	−1.0	−0.77	−0.8573	−0.4060	−0.4024	−0.6114	−0.8573	−0.3336
	−0.4024	−0.1227	−0.08997	−0.1412	−0.3524	−0.0390	−0.0530	−0.0143
19	-2.48×2^{-8}	−0.0	-4.03×2^{-7}	-2.07×2^{-12}	-6.24×2^{-10}	−0.0	-3.65×2^{-14}	2.15×2^{-14}
	−0.0	−0.0	-5.42×2^{-20}	5.85×2^{-13}	−0.0	−0.0	-1.63×2^{-19}	1.99×2^{-9}
	−0.0	−0.0	-7.17×2^{-14}	−0.00001	−0.0	−0.0	-5.79×2^{-6}	−0.0384
	−0.0	-9.54×2^{-7}	−0.0150	0.4028	−0.0	−0.0571	−0.9496	0.9922
	−1.0	−0.9142	−0.9496	−0.6607	−0.6503	−0.8125	−0.9496	−0.6151
	−0.6503	−0.3138	−0.2366	−0.3306	−0.5783	−0.1957	−0.1873	−0.0817
	−0.0479	−0.0522	−0.1330	−0.0155	−0.0121	−0.0069	−0.0057	−0.0021
	−0.0083	−0.0001	−0.00008	−0.00006	−0.0002	-3.98×2^{-6}	−0.00003	-1.19×2^{-8}
	−0.0029	-3.33×2^{-6}	-8.47×2^{-6}	−0.0	−0.00003	-3.32×2^{-8}	-3.28×2^{-6}	−0.0
	-2.33×2^{-10}	4.17×2^{-9}	−0.0	−0.0	-9.09×2^{-13}	-1.85×2^{-7}	−0.0	−0.0

TABLE 13: Continued.

	-1.09×2^{-11}	−0.00002	−0.0	−0.0	-4.01×2^{-7}	−0.0126	−0.0	−0.0
	−0.0106	0.2298	−0.0	−0.0020	−0.2637	−1.0	−0.0	−0.9844
	−1.0	−1.0	−1.0	−0.9844	−1.0	−0.8573	−0.9142	−0.9844
	−1.0	−0.8573	−0.9142	−0.5413	−0.5320	−0.7248	−0.9142	−0.4813
	−0.5320	−0.2116	−0.1542	−0.2293	−0.4671	−0.1034	−0.1088	−0.0409
	−0.0255	−0.0249	−0.0807	−0.0035	−0.0038	−0.0018	−0.0023	−0.0004
20	-2.94×2^{-10}	-1.72×2^{-18}	-1.32×2^{-15}	−0.0	-3.47×2^{-19}	1.79×2^{-22}	−0.0	−0.0
	-3.16×2^{-30}	-6.10×2^{-22}	−0.0	−0.0	-3.70×2^{-32}	9.18×2^{-17}	−0.0	−0.0
	-1.96×2^{-25}	-1.12×2^{-10}	−0.0	−0.0	-5.81×2^{-13}	−0.0001	−0.0	−0.0
	−0.00007	−0.0450	−0.0	−0.00004	−0.1092	0.8765	−0.0	−0.7267
	−0.7499	−0.4231	−0.3339	−0.4391	−0.6791	−0.3073	−0.2850	−0.1379
	−0.0814	−0.0922	−0.1992	−0.0424	−0.0301	−0.0177	−0.0119	−0.0066
	−0.0188	−0.0009	−0.0005	−0.0004	−0.0007	−0.00005	−0.0002	-1.19×2^{-6}
	-5.42×2^{-7}	-3.94×2^{-7}	-4.08×2^{-6}	-3.46×2^{-9}	-3.63×2^{-8}	-5.32×2^{-12}	-1.42×2^{-11}	−0.0
	-2.48×2^{-8}	−0.0	-4.03×2^{-7}	-2.07×2^{-12}	-6.24×2^{-10}	−0.0	-3.65×2^{-14}	-2.15×2^{-14}
	−0.0	−0.0	-5.42×2^{-20}	5.85×2^{-13}	−0.0	−0.0	-1.63×2^{-19}	1.99×2^{-9}
	−0.0	−0.0	-7.17×2^{-14}	−0.00001	−0.0	−0.0	-5.79×2^{-6}	−0.0384
	−0.0	-9.54×2^{-7}	−0.0150	0.4028	−0.0	−0.0571	−0.9496	0.9922
	−1.0	−0.9142	−0.9496	−0.6607	−0.6503	−0.8125	−0.9496	−0.6151
	−0.6503	−0.3138	−0.2366	−0.3306	−0.5783	−0.1957	−0.1873	−0.0817
	−0.0479	−0.0522	−0.1330	−0.0155	−0.0121	−0.0069	−0.0057	−0.0021
	−0.0083	−0.0001	−0.00008	−0.00006	−0.0002	-3.98×2^{-6}	−0.00003	-1.19×2^{-8}
	Linear part							
	0000000000000000000000000000000000001000000000000000000000000000 0000000000000000000000000000001000100000000000000000000000000000							
21	0000000000000000000000000000001000100000000000000000000000000000 0000000000000000000000000000000010000000000000000000000000000000							
22	0000000000000000000000000000000010000000000000000000000000000000 0000000000000000000000000000001000000000000000000000000000000000							
23	0000000000000000000000000000001000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000							
24	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000001000000000000000000000000000000000							
25	0000000000000000000000000000001000000000000000000000000000000000 0000000000000000000000000000000010000000000000000000000000000000							
26	0000000000000000000000000000000010000000000000000000000000000000 0000000000000000000000000000001000100000000000000000000000000000							
27	0000000000000000000000000000001000100000000000000000000000000000 0000000000000000000000000000000000001000000000000000000000000000							
28	0000000000000000000000000000000000001000000000000000000000000000 0000000000000000000000000000001000100010000000000000000000000000							
29	0000000000000000000000000000001000100010000000000000000000000000 0000000000000000000000000000000010000000100000000000000000000000							
30	00000000000000000000000000000000100000001000000000000000000000000 0000000000000000000000000000001000000010001000000000000000000000							
31	0000000000000000000000000000001000000010001000000000000000000000 0000000000000000000000000000000000000000000010000000000000000000							
32	0000000000000000000000000000000000000000000010000000000000000000 0000000000000000000000000000001000000010001000100000000000000000							

Note: The experimental correlation of the first 11 rounds is $2^{-27.68}$ under 2^{32} sample sizes and 100 random keys, and the experimental correlation of the 9 rounds at the DL part is $2^{-0.31}$ under 2^{8} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-27.68}\times2^{-0.31}\times(2^{-18})^2=2^{-63.99}$.

Table 14: Fourteen-round DL distinguisher for SIMECK32 with theoretical correlation $2^{-16.63}$ and experimental correlation $2^{-15.57}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part is $2^{-10}, 0.64(=2^{-0.63})$, and 2^{-3}, respectively.

	Differential part							
0	00100000000000000111010000000000							
1	00010100000000000001000000000000							
2	00001000000000000001010000000000							
3	00000100000000000000100000000000							
4	00000000000000000000100000000000							
5	00000100000000000000000000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
6	0.0	−1.0	−1.0	−1.0	1.0	0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
7	−0.25	−1.0	−1.0	0.9999	0.0	0.50	−1.0	−1.0
	−1.0	−1.0	−0.9999	−0.50	−1.0	−1.0	−1.0	0.0
	0.0	−1.0	−1.0	−1.0	1.0	0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	0.0	−1.0	0.9999	0.0	−0.2450	0.0	−0.75	−1.0
	−1.0	−0.9999	−0.2450	−0.4688	−1.0	−1.0	0.0	−0.0625
	−0.25	−1.0	−1.0	0.9999	0.0	0.50	−1.0	−1.0
	−1.0	−1.0	−0.9999	−0.50	−1.0	−1.0	−1.0	0.0
9	−0.0625	0.8750	0.0	0.1250	0.0	0.1172	−0.6426	−1.0
	−0.9999	−0.1250	−0.1556	−0.1836	−1.0	0.0	−0.0156	0.0
	0.0	−1.0	0.9999	0.0	−0.2450	0.0	−0.75	−1.0
	−1.0	−0.9999	−0.2450	−0.4688	−1.0	−1.0	0.0	−0.0625
10	0.0	0.0	−0.0625	0.0	0.0082	0.0	−0.3645	−1.0
	−0.0625	−0.0445	−0.0133	−0.1474	0.0	−0.0039	0.0	−0.0010
	−0.0625	0.8750	0.0	0.1250	0.0	0.1172	−0.6426	−1.0
	−0.9999	−0.1250	−0.1556	−0.1836	−1.0	0.0	−0.0156	0.0
	Linear part							
	00000001000000000000001000000000							
11	00000010000000000000000000000000							
12	00000000000000000000001000000000							
13	00000010000000000000000100000000							
14	00000001000000000000001010001000							

Note: The experimental correlation of the first 10 (5 + 5) rounds is $2^{-9.57}$ under 2^{32} sample sizes and 100 random keys, and the experimental correlation of the 4 rounds at the bottom is 2^{-3} under 2^{15} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-9.57} \times (2^{-3})^2 = 2^{-15.57}$.

Table 15: Seventeen-round DL distinguisher for SIMECK48 with theoretical correlation $2^{-22.37}$ and experimental correlation $2^{-15.43}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-12}, $0.77(=2^{-0.37})$, and 2^{-5}, respectively.

	Differential part							
0	000000000000100000000000000000000000101000000000							
1	000000000000010000000000000000000000010000000000							
2	000000000000000000000000000000000000010000000000							
3	000000000000010000000000000000000000000000000000							
4	000000000000100000000000000000000000010000000000							
5	000000000001010000000000000000000000010000000000							
6	000000000010000000000000000000000000101000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
7	−1.0	−1.0	−1.0	−1.0	−1.0	0.0	−1.0	−1.0
	−1.0	1.0	0.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	−0.5	−1.0	−1.0	−1.0	0.0	−0.25	-9.09×2^{-13}	−1.0
	0.0	0.0	−0.5	-9.09×2^{-13}	1.0	0.0	−0.9999	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	0.0	−1.0	−1.0
	−1.0	1.0	0.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
9	−0.4688	−0.50	−1.0	0.0	−0.0625	0.0	−0.25	0.0
	0.0	0.25	0.0	−0.50	-5.46×2^{-12}	0.50	−0.9999	−1.0
	−1.0	−1.0	−1.0	−0.75	−1.0	−1.0	−1.0	−0.25
	−0.5	−1.0	−1.0	−1.0	0.0	−0.25	-9.09×2^{-13}	−1.0
	0.0	0.0	−0.5	-9.09×2^{-13}	1.0	0.0	−0.9999	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
10	−0.0918	−0.4688	0.0	−0.0156	0.0	−0.0156	0.0	-1.21×2^{-13}
	0.0	0.0	−0.1250	2.39×2^{-12}	−0.25	-2.04×2^{-11}	−0.8750	−1.0
	−1.0	−1.0	−0.4688	−0.6426	−0.75	−1.0	−0.1250	−0.1556
	−0.4688	−0.50	−1.0	0.0	−0.0625	0.0	−0.25	0.0
	0.0	0.25	0.0	−0.50	5.46×2^{-12}	0.50	−0.9999	−1.0
	−1.0	−1.0	−1.0	−0.750	−1.0	−1.0	−1.0	−0.25
11	−0.0609	6.90×2^{-13}	−0.0039	3.11×2^{-13}	−0.00024	0.0	0.0	0.0
	1.33×2^{-13}	0.0146	0.0	−0.0625	0.0	0.1606	−0.77	−0.8750
	−1.0	−0.2637	−0.2727	−0.2522	−0.6426	−0.0625	−0.0445	−0.0066
	−0.0918	−0.4688	0.0	−0.0156	0.0	−0.0156	0.0	-1.21×2^{-13}
	0.0	0.0	−0.1250	2.39×2^{-12}	−0.25	-2.04×2^{-11}	−0.8750	−1.0
	−1.0	−1.0	−0.4688	−0.6426	−0.75	−1.0	−0.1250	−0.1556
12	0.0	−0.0005	0.0	-9.54×10^{-7}	0.0	0.0	0.0	0.0
	0.0	0.0	−0.0037	0.0	0.0127	-2.34×10^{-11}	−0.4242	−0.77
	−0.1401	−0.09	−0.0379	−0.1371	−0.0193	−0.0119	−0.0002	−0.0024
	−0.0609	6.90×10^{-13}	−0.0039	3.11×10^{-13}	−0.0002	0.0	0.0	0.0
	1.33×10^{-13}	0.0146	0.0	−0.0625	0.0	0.1606	−0.77	−0.8750
	−1.0	−0.2637	−0.2727	−0.2522	−0.6426	−0.0625	−0.0445	−0.0066

Table 15: Continued.

	Linear part
	000000000000000100000000000000000000000000000000
13	000000000000000000000000000000000000000100000000
14	000000000000000100000000000000000000000010000000
15	000000000000000010000000000000000000000101000000
16	000000000000000101000000000000000000000001000000
17	000000000000000000100000000000000000000101010000

Note: The experimental correlation of the first 12 (6 + 6) rounds is $2^{-6.13}$ under 2^{32} sample sizes and 100 random keys, and the experimental correlation of the 5 rounds at the bottom is $2^{-4.65}$ under 2^{18} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-6.13} \times (2^{-4.65})^2 = 2^{-15.43}$.

Table 16: Eighteen-round DL distinguisher for SIMECK48 with theoretical correlation $2^{-24.75}$ and experimental correlation $2^{-17.88}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-12}, $0.59(=2^{-0.75})$, and 2^{-6}, respectively.

	Differential part
0	000000000000000000001000000000000000000000010100
1	000000000000000000000100000000000000000000001000
2	000000000000000000000000000000000000000000000100
3	000000000000000000000100000000000000000000000000
4	000000000000000000001000000000000000000000000100
5	000000000000000000010100000000000000000000001000
6	000000000000000000100000000000000000000000010100

	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	1.0	−1.0	−1.0
7	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	0.0	−1.0	−1.0
	−1.0	1.0	0.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.5	−1.0	−1.0	−1.0	0.0	−0.25	0.0	−1.0
	0.0	0.0	−0.5	0.0	1.0	0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	0.0	−1.0	−1.0
	−1.0	1.0	0.0	1.0	−1.0	1.0	−1.0	−1.0
9	−1.0	−1.0	−1.0	−0.75	−1.0	−1.0	−1.0	−0.25
	−0.4688	−0.5	−1.0	0.0	−0.0625	0.0	−0.25	0.0
	0.0	0.25	0.0	−0.5	0.0	0.5	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−0.5	−1.0	−1.0	−1.0	0.0	−0.25	0.0	−1.0
	0.0	0.0	−0.5	0.0	1.0	0.0	−1.0	−1.0
10	−1.0	−1.0	−0.4688	−0.6426	−0.75	−1.0	−0.1250	−0.1556
	−0.0918	−0.4688	0.0	−0.0156	0.0	−0.0156	0.0	0.0
	0.0	0.0	−0.1250	0.0	−0.25	0.0	−0.875	−1.0
	−1.0	−1.0	−1.0	−0.75	−1.0	−1.0	−1.0	−0.25

Table 16: Continued.

	−0.4688	−0.5	−1.0	0.0	−0.0625	0.0	−0.25	0.0
	0.0	0.25	0.0	−0.5	0.0	0.5	−1.0	−1.0
11	−1.0	−0.2637	−0.2727	−0.2522	−0.6426	−0.0625	−0.0445	−0.0066
	−0.0609	0.0	−0.0039	0.0	−0.0002	0.0	0.0	0.0
	0.0	0.0146	0.0	−0.0625	0.0	0.1606	−0.77	−0.875
	−1.0	−1.0	−0.4688	−0.6426	−0.75	−1.0	−0.1250	−0.1556
	−0.0918	−0.4688	0.0	−0.0156	0.0	−0.0156	0.0	0.0
	0.0	0.0	−0.1250	0.0	−0.25	0.0	−0.875	−1.0
12	−0.1401	−0.09	−0.0379	−0.1371	−0.0192	−0.0119	−0.0002	−0.0024
	0.0	−0.0005	0.0	-9.54×10^{-7}	0.0	0.0	1.51×2^{-13}	0.0
	0.0	0.0	−0.0037	0.0	0.0127	0.0	−0.4242	−0.77
	−1.0	−0.2637	−0.2727	−0.2522	−0.6426	−0.0625	−0.0445	−0.0066
	−0.0609	0.0	−0.0039	0.0	−0.0002	0.0	0.0	0.0
	0.0	0.0146	0.0	−0.0625	0.0	0.1606	−0.77	−0.875
Linear part								
	000000000000000000000001000000000000000000000010							
13	000000000000000000000010000000000000000000000000							
14	000000000000000000000000000000000000000000000010							
15	000000000000000000000010000000000000000000000001							
16	000000000000000000000011000000000000000000000010							
17	100000000000000000000010010000000000000000000000							
18	010000000000000000000000101000000000000000000010							

Note: The experimental correlation of the first 12 (6 + 6) rounds is $2^{-6.54}$ under 2^{32} sample sizes and 100 random keys, and the experimental correlation of the 6 rounds at the bottom is $2^{-5.67}$ under 2^{18} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-6.54}\times(2^{-5.67})^2 = 2^{-17.88}$.

Table 17: Twenty-two-round DL distinguisher for SIMECK64 with theoretical correlation $2^{-32.90}$ and experimental correlation $2^{-24.59}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-14}, $0.53(=2^{-0.44})$, and 2^{-9}, respectively.

Differential part (optimal differential trail)								
0	0000000000000000001000000000000000000000000000000101010000000000							
7	0000000000000000001010000000000000000000000000000000100000000000							
DL part								
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.0	−1.0
	−0.0	−1.0	1.0	−0.0	−1.0	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
9	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.5	−1.0	−0.5	−1.0	−0.0	−0.25	−0.0

Table 17: Continued.

	−0.25	1.0	−0.0	0.5	−0.0	0.5	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.0	−1.0
	−0.0	−1.0	1.0	−0.0	−1.0	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
10	−1.0	−1.0	−1.0	−1.0	−0.75	−1.0	−0.75	−1.0
	−0.25	−0.4688	−0.25	−0.4688	−0.0	−0.0625	−0.0	−0.0625
	−0.0	−0.0	−0.25	−0.0	0.25	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.5	−1.0	−0.5	−1.0	−0.0	−0.25	−0.0
	−0.25	1.0	−0.0	0.5	−0.0	0.5	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
11	−1.0	−0.875	−1.0	−0.4688	−0.6426	−0.4688	−0.6426	−0.125
	−0.1556	−0.0459	−0.1556	−0.0	−0.0156	−0.0	−0.0039	−0.0
	−0.0	0.125	−0.0	−0.0625	−0.0	0.25	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.875
	−1.0	−1.0	−1.0	−1.0	−0.75	−1.0	−0.75	−1.0
	−0.25	−0.4688	−0.25	−0.4688	−0.0	−0.0625	−0.0	−0.0625
	−0.0	−0.0	−0.25	−0.0	0.25	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
12	−0.6426	−0.77	−0.2637	−0.2727	−0.1510	−0.2727	−0.0385	−0.0445
	−0.0033	−0.0192	−0.0	−0.0018	−0.0	−0.00006	−0.0	−0.0
	−0.0	−0.0	−0.0078	−0.0	−0.0313	−0.0	−1.0	−1.0
	−1.0	−1.0	−0.9375	−1.0	−0.9375	−1.0	−0.6426	−0.77
	−1.0	−0.875	−1.0	−0.4688	−0.6426	−0.4688	−0.6426	−0.125
	−0.1556	−0.0459	−0.1556	−0.0	−0.0156	−0.0	−0.0039	−0.0
	−0.0	0.125	−0.0	−0.0625	−0.0	0.25	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.875
13	−0.4024	−0.1060	−0.09	−0.0226	−0.0514	−0.0057	−0.0074	−0.0001
	−0.0007	−0.0	−0.00007	−0.0	-2.38×2^{-7}	−0.0	−0.0	−0.0
	−0.0	0.0005	−0.0	−0.0010	−0.0	0.1211	−1.0	−0.9688
	−1.0	−0.77	−0.8573	−0.77	−0.8573	−0.4060	−0.4024	−0.2864
	−0.6426	−0.77	−0.2637	−0.2727	−0.1510	−0.2727	−0.0385	−0.0445
	−0.0033	−0.019	−0.0	−0.0018	−0.0	−0.00006	−0.0	−0.0
	−0.0	−0.0	−0.0078	−0.0	−0.0313	−0.0	−1.0	−1.0
	−1.0	−1.0	−0.9375	−1.0	−0.9375	−1.0	−0.6426	−0.77
14	−0.0240	−0.0193	−0.0016	−0.0036	−0.0002	−0.0005	−0.000001	−0.000008
	−0.0	-3.41×2^{-7}	−0.0	-1.09×2^{-10}	−0.0	−0.0	−0.0	−0.0
	−0.0	−0.0	−0.000003	−0.0	0.0017	−0.0	−0.8573	−0.9142
	−0.5413	−0.5320	−0.4311	−0.5320	−0.1955	−0.1542	−0.0660	−0.1048
	−0.4024	−0.1060	−0.09	−0.0226	−0.0514	−0.0057	−0.0074	−0.0001
	−0.0007	−0.0	−0.00007	−0.0	-2.38×2^{-7}	−0.0	−0.0	−0.0
	−0.0	0.0005	−0.0	−0.00097	−0.0	0.1211	−1.0	−0.9688
	−1.0	−0.77	−0.8573	−0.77	−0.8573	−0.4060	−0.4024	−0.2864
	Linear part							
	0000000000000000000000000100000000000000000000000000001010000000							
15	0000000000000000000000101000000000000000000000000000000100000000							
16	0000000000000000000000010000000000000000000000000000001000000000							
17	0000000000000000000000100000000000000000000000000000000000000000							
18	0000000000000000000000000000000000000000000000000000001000000000							

Table 17: Continued.

19	0000000000000000000000100000000000000000000000000000000100000000
20	0000000000000000000000010000000000000000000000000000001010000000
21	0000000000000000000000101000000000000000000000000000000001000000
22	0000000000000000000000000100000000000000000000000000001010100000

Note: The experimental correlation of the first 14 (7 + 7) rounds is $2^{-8.03}$ under 2^{32} sample sizes and 100 random keys, and the experimental correlation of the 8 rounds at the bottom is $2^{-8.28}$ under 2^{25} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-8.03} \times (2^{-8.28})^2 = 2^{-24.59}$.

Table 18: Twenty-three-round DL distinguisher for SIMECK64 with theoretical correlation $2^{-36.13}$ and experimental correlation $2^{-25.45}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-14}, $0.91(=2^{-0.13})$, and 2^{-11}, respectively.

	Differential part (optimal differential trail)							
0	0000000000000000001000000000000000000000000000000101010000000000							
7	0000000000000000000101000000000000000000000000000000100000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.0	−1.0
	−0.0	−1.0	1.0	−0.0	−1.0	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
9	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.5	−1.0	−0.5	−1.0	−0.0	−0.25	−0.0
	−0.25	1.0	−0.0	0.5	−0.0	0.5	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.0	−1.0
	−0.0	−1.0	1.0	−0.0	−1.0	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
10	−1.0	−1.0	−1.0	−1.0	−0.75	−1.0	−0.75	−1.0
	−0.25	−0.4688	−0.25	−0.4688	−0.0	−0.0625	−0.0	−0.0625
	−0.0	−0.0	−0.25	−0.0	0.25	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.5	−1.0	−0.5	−1.0	−0.0	−0.25	−0.0
	−0.25	1.0	−0.0	0.5	−0.0	0.5	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
11	−1.0	−0.875	−1.0	−0.4688	−0.6426	−0.4688	−0.6426	−0.125
	−0.1556	−0.0459	−0.1556	−0.0	−0.0156	−0.0	−0.0039	−0.0
	−0.0	0.125	−0.0	−0.0625	−0.0	0.25	−1.0	−1.0

Table 18: Continued.

	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.875
	−1.0	−1.0	−1.0	−1.0	−0.75	−1.0	−0.75	−1.0
	−0.25	−0.4688	−0.25	−0.4688	−0.0	−0.0625	−0.0	−0.0625
	−0.0	−0.0	−0.25	−0.0	0.25	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
12	−0.6426	−0.77	−0.2637	−0.2727	−0.1510	−0.2727	−0.0385	−0.0445
	−0.0033	−0.0192	−0.0	−0.0018	−0.0	−0.00006	−0.0	−0.0
	−0.0	−0.0	−0.0078	−0.0	−0.0313	−0.0	−1.0	−1.0
	−1.0	−1.0	−0.9375	−1.0	−0.9375	−1.0	−0.6426	−0.77
	−1.0	−0.875	−1.0	−0.4688	−0.6426	−0.4688	−0.6426	−0.125
	−0.1556	−0.0459	−0.1556	−0.0	−0.0156	−0.0	−0.0039	−0.0
	−0.0	0.125	−0.0	−0.0625	−0.0	0.25	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.875
13	−0.4024	−0.1060	−0.09	−0.0226	−0.0514	−0.0057	−0.0074	−0.0001
	−0.00075	−0.0	−0.00007	−0.0	-2.38×2^{-7}	−0.0	−0.0	−0.0
	−0.0	0.0005	−0.0	−0.00098	−0.0	0.1211	−1.0	−0.9688
	−1.0	−0.77	−0.8573	−0.77	−0.8573	−0.4060	−0.4024	−0.2864
	−0.6426	−0.77	−0.2637	−0.2727	−0.1510	−0.2727	−0.0385	−0.0445
	−0.0033	−0.0192	−0.0	−0.0018	−0.0	−0.00006	−0.0	−0.0
	−0.0	−0.0	−0.0078	−0.0	−0.0313	−0.0	−1.0	−1.0
	−1.0	−1.0	−0.9375	−1.0	−0.9375	−1.0	−0.6426	−0.77
14	−0.0240	−0.0193	−0.0016	−0.0036	−0.0002	−0.0005	−0.000001	−0.000008
	−0.0	-3.41×2^{-7}	−0.0	-1.09×2^{-10}	−0.0	−0.0	−0.0	−0.0
	−0.0	−0.0	−0.000003	−0.0	0.0017	−0.0	−0.8573	−0.9142
	−0.5413	−0.5320	−0.4311	−0.5320	−0.1955	−0.1542	−0.0660	−0.1048
	−0.4024	−0.1060	−0.09	−0.0226	−0.0514	−0.0057	−0.0074	−0.0001
	−0.0007	−0.0	−0.00007	−0.0	-2.38×2^{-7}	−0.0	−0.0	−0.0
	−0.0	0.0005	−0.0	−0.00098	−0.0	0.1211	−1.0	−0.96875
	−1.0	−0.77	−0.8573	−0.77	−0.8573	−0.4060	−0.4024	−0.2864
	Linear part							
	0000000000000000000000010000000000000000000000000000000000000000							
15	0000000000000000000000000000000000000000000000000000000100000000							
16	0000000000000000000000010000000000000000000000000000000010000000							
17	0000000000000000000000001000000000000000000000000000000101000000							
18	0000000000000000000000010100000000000000000000000000000000100000							
19	0000000000000000000000000010000000000000000000000000000101010000							
20	0000000000000000000000010101000000000000000000000000000010000000							
21	0000000000000000000000001000000000000000000000000000000100010000							
22	0000000000000000000000010001000000000000000000000000000000000000							
23	0000000000000000000000000000000000000000000000000000000100010000							

Note: The experimental correlation of the first 14 $(7+7)$ rounds is $2^{-6.77}$ under 2^{32} sample sizes and 100 random keys, and the experimental correlation of the 9 rounds at the bottom is $2^{-9.34}$ under 2^{28} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-6.77}\times(2^{-9.34})^2 = 2^{-25.45}$.

Table 19: Twenty-four-round DL distinguisher for SIMECK64 with theoretical correlation $2^{-38.13}$ and experimental correlation $2^{-27.17}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are $2^{-14}, 0.91(=2^{-0.13})$, and 2^{-12}, respectively.

Differential part (optimal differential trail)								
0	0000000000000000001000000000000000000000000000000101010000000000							
7	0000000000000000000101000000000000000000000000000000100000000000							
DL part								
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.0	−1.0
	−0.0	−1.0	1.0	−0.0	−1.0	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
9	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.5	−1.0	−0.5	−1.0	−0.0	−0.25	−0.0
	−0.25	1.0	−0.0	0.5	−0.0	0.5	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.0	−1.0
	−0.0	−1.0	1.0	−0.0	−1.0	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
10	−1.0	−1.0	−1.0	−1.0	−0.75	−1.0	−0.75	−1.0
	−0.25	−0.4688	−0.25	−0.4688	−0.0	−0.0625	−0.0	−0.0625
	−0.0	−0.0	−0.25	−0.0	0.25	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.5	−1.0	−0.5	−1.0	−0.0	−0.25	−0.0
	−0.25	1.0	−0.0	0.5	−0.0	0.5	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
11	−1.0	−0.875	−1.0	−0.4688	−0.6426	−0.4688	−0.6426	−0.125
	−0.1556	−0.0459	−0.1556	−0.0	−0.0156	−0.0	−0.0039	−0.0
	−0.0	0.125	−0.0	−0.0625	−0.0	0.25	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.875
	−1.0	−1.0	−1.0	−1.0	−0.75	−1.0	−0.75	−1.0
	−0.25	−0.4688	−0.25	−0.4688	−0.0	−0.0625	−0.0	−0.0625
	−0.0	−0.0	−0.25	−0.0	0.25	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
12	−0.6426	−0.77	−0.2637	−0.2727	−0.1510	−0.2727	−0.0385	−0.0445
	−0.0033	−0.0192	−0.0	−0.0018	−0.0	−0.00006	−0.0	−0.0
	−0.0	−0.0	−0.0078	−0.0	−0.03125	−0.0	−1.0	−1.0
	−1.0	−1.0	−0.9375	−1.0	−0.9375	−1.0	−0.6426	−0.77
	−1.0	−0.875	−1.0	−0.4688	−0.6426	−0.4688	−0.6426	−0.125
	−0.1556	−0.0459	−0.1556	−0.0	−0.0156	−0.0	−0.0039	−0.0

Table 19: Continued.

	−0.0	0.125	−0.0	−0.0625	−0.0	0.25	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.875
13	−0.4024	−0.1060	−0.09	−0.0226	−0.0514	−0.0057	−0.0074	−0.0001
	−0.0007	−0.0	−0.00007	−0.0	-2.38×2^{-7}	−0.0	−0.0	−0.0
	−0.0	0.0004	−0.0	−0.00098	−0.0	0.1211	−1.0	−0.9688
	−1.0	−0.77	−0.8573	−0.77	−0.8573	−0.4060	−0.4024	−0.2864
	−0.6426	−0.77	−0.2637	−0.2727	−0.1510	−0.2727	−0.0385	−0.0445
	−0.0033	−0.0192	−0.0	−0.0018	−0.0	−0.00006	−0.0	−0.0
	−0.0	−0.0	−0.0078	−0.0	−0.0313	−0.0	−1.0	−1.0
	−1.0	−1.0	−0.9375	−1.0	−0.9375	−1.0	−0.6426	−0.77
14	−0.0240	−0.0193	−0.0016	−0.0036	−0.0002	−0.0005	−0.000001	−0.000008
	−0.0	-3.41×2^{-7}	−0.0	-1.09×2^{-10}	−0.0	−0.0	−0.0	−0.0
	−0.0	−0.0	−0.000003	−0.0	0.0017	−0.0	−0.8573	−0.9142
	−0.5413	−0.5320	−0.4311	−0.5320	−0.1955	−0.1542	−0.0660	−0.1048
	−0.4024	−0.1060	−0.09	−0.0226	−0.0514	−0.0057	−0.0074	−0.0001
	−0.0007	−0.0	−0.00007	−0.0	-2.38×2^{-7}	−0.0	−0.0	−0.0
	−0.0	0.0005	−0.0	−0.00098	−0.0	0.1211	−1.0	−0.9688
	−1.0	−0.77	−0.8573	−0.77	−0.8573	−0.4060	−0.4024	−0.2864
	Linear part							
	0000000000000000000000010000000000000000000000000000001000000000							
15	0000000000000000000000100000000000000000000000000000000000000000							
16	0000000000000000000000100000000000000000000000000000001000000000							
17	0000000000000000000000100000000000000000000000000000000100000000							
18	0000000000000000000000010000000000000000000000000000001010000000							
19	0000000000000000000000101000000000000000000000000000000001000000							
20	0000000000000000000000000100000000000000000000000000001010100000							
21	0000000000000000000000101010000000000000000000000000000100000000							
22	0000000000000000000000010000000000000000000000000000001000100000							
23	0000000000000000000000100010000000000000000000000000000000000000							
24	0000000000000000000000000000000000000000000000000000001000100000							

Note: The experimental correlation of the first 14 (7 + 7) rounds is $2^{-7.05}$ under 2^{32} sample sizes and 100 random keys, and the experimental correlation of the 10 rounds at the bottom is $2^{-10.06}$ under 2^{28} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-7.05}\times(2^{-10.06})^2=2^{-27.17}$.

Table 20: Twenty-five-round DL distinguisher for SIMECK64 with theoretical correlation $2^{-41.04}$ and experimental correlation $2^{-29.65}$, where the theoretical probability of the differential part, the theoretical correlation of the DL part, and the theoretical correlation of the linear part are 2^{-14}, $0.486(=2^{-1.04})$, and 2^{-13}, respectively.

	Differential part (optimal differential trail)							
0	0000000000000000001000000000000000000000000000000101010000000000							
7	0000000000000000001010000000000000000000000000000001000000000000							
	DL part							
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
8	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.0	−1.0
	−0.0	−1.0	1.0	−0.0	−1.0	−0.0	−1.0	−1.0

Table 20: Continued.

	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	1.0	−1.0	1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
9	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.5	−1.0	−0.5	−1.0	−0.0	−0.25	−0.0
	−0.25	1.0	−0.0	0.5	−0.0	0.5	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.0	−1.0
	−0.0	−1.0	1.0	−0.0	−1.0	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
10	−1.0	−1.0	−1.0	−1.0	−0.75	−1.0	−0.75	−1.0
	−0.25	−0.4688	−0.25	−0.4688	−0.0	−0.0625	−0.0	−0.0625
	−0.0	−0.0	−0.25	−0.0	0.25	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
	−1.0	−0.5	−1.0	−0.5	−1.0	−0.0	−0.25	−0.0
	−0.25	1.0	−0.0	0.5	−0.0	0.5	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
11	−1.0	−0.875	−1.0	−0.4688	−0.6426	−0.4688	−0.6426	−0.125
	−0.1556	−0.0459	−0.1556	−0.0	−0.0156	−0.0	−0.0039	−0.0
	−0.0	0.125	−0.0	−0.0625	−0.0	0.25	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.875
	−1.0	−1.0	−1.0	−1.0	−0.75	−1.0	−0.75	−1.0
	−0.25	−0.4688	−0.25	−0.4688	−0.0	−0.0625	−0.0	−0.0625
	−0.0	−0.0	−0.25	−0.0	0.25	−0.0	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0
12	−0.6426	−0.77	−0.2637	−0.2727	−0.1510	−0.2727	−0.0385	−0.0445
	−0.0033	−0.0192	−0.0	−0.0018	−0.0	−0.00006	−0.0	−0.0
	−0.0	−0.0	−0.0078	−0.0	−0.03125	−0.0	−1.0	−1.0
	−1.0	−1.0	−0.9375	−1.0	−0.9375	−1.0	−0.6426	−0.77
	−1.0	−0.875	−1.0	−0.4688	−0.6426	−0.4688	−0.6426	−0.125
	−0.1556	−0.0459	−0.1556	−0.0	−0.0156	−0.0	−0.0039	−0.0
	−0.0	0.125	−0.0	−0.0625	−0.0	0.25	−1.0	−1.0
	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−1.0	−0.875
13	−0.4024	−0.1060	−0.09	−0.0226	−0.0514	−0.0057	−0.0074	−0.0001
	−0.0007	−0.0	−0.00007	−0.0	-2.38×2^{-7}	−0.0	−0.0	−0.0
	−0.0	0.0004	−0.0	−0.00098	−0.0	0.1211	−1.0	−0.9688
	−1.0	−0.77	−0.8573	−0.77	−0.8573	−0.4060	−0.4024	−0.2864
	−0.6426	−0.77	−0.2637	−0.2727	−0.1510	−0.2727	−0.0385	−0.0445
	−0.0033	−0.0192	−0.0	−0.0018	−0.0	−0.00006	−0.0	−0.0
	−0.0	−0.0	−0.0078	−0.0	−0.03125	−0.0	−1.0	−1.0
	−1.0	−1.0	−0.9375	−1.0	−0.9375	−1.0	−0.6426	−0.77
14	−0.0240	−0.0193	−0.0016	−0.0036	−0.0002	−0.0005	−0.000001	−0.000008
	−0.0	-3.41×2^{-7}	−0.0	-1.09×2^{-10}	−0.0	−0.0	−0.0	−0.0
	−0.0	−0.0	−0.000003	−0.0	0.0017	−0.0	−0.8573	−0.9142
	−0.5413	−0.5320	−0.4311	−0.5320	−0.1955	−0.1542	−0.0660	−0.1048
	−0.4024	−0.1060	−0.09	−0.0226	−0.0514	−0.0057	−0.0074	−0.0001
	−0.0007	−0.0	−0.00007	−0.0	-2.38×2^{-7}	−0.0	−0.0	−0.0
	−0.0	0.0005	−0.0	−0.00098	−0.0	0.1211	−1.0	−0.96875

Table 20: Continued.

	−1.0	−0.77	−0.8573	−0.77	−0.8573	−0.4060	−0.4024	−0.2864
	Linear part							
	0000000000000000000000010001000000000000000000000000000000000000							
15	0000000000000000000000000000000000000000000000000000000100010000							
16	0000000000000000000000010001000000000000000000000000000010000000							
17	0000000000000000000000001000000000000000000000000000000101010000							
18	0000000000000000000000010101000000000000000000000000000000100000							
19	0000000000000000000000000010000000000000000000000000000101000000							
20	0000000000000000000000010100000000000000000000000000000010000000							
21	0000000000000000000000001000000000000000000000000000000100000000							
22	0000000000000000000000010000000000000000000000000000000000000000							
23	0000000000000000000000000000000000000000000000000000000100000000							
24	0000000000000000000000010000000000000000000000000000000010000000							
25	0000000000000000000000001000000000000000000000000000000101000000							

Note: The experimental correlation of the first 14 (7 + 7) rounds is $2^{-8.25}$ under 2^{32} sample sizes and 100 random keys, and the experimental correlation of the 11 rounds at the bottom is $2^{-10.70}$ under 2^{28} sample sizes and 100 random keys. According to piling-up lemma, the experimental correlation is $2^{-8.25} \times (2^{-10.70})^2 = 2^{-29.65}$.

Data Availability

No underlying data were collected or produced in this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was sponsored by the National Natural Science Foundation of China (grant nos. 62102448, 62202493, and 62372463).

References

[1] S. K. Langford and M. E. Hellman, "Differential-linear cryptanalysis," in *Advances in Cryptology–CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21–25, 1994, Proceedings*, vol. 836 of *Lecture Notes in Computer Science*, pp. 17–25, Springer, Santa Barbara, California, USA, 1994.

[2] E. Biham and A. S., *Differential Cryptanalysis of the Data Encryption Standard*, Springer, Berlin, Germany, 1993.

[3] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT '93. EUROCRYPT 1993*, T. Helleseth, Ed., vol. 765 of *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 1994.

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

[5] E. Biham, O. Dunkelman, and N. Keller, "Enhancing differential-linear cryptanalysis," in *Advances in Cryptology —ASIACRYPT 2002*, Y. Zheng, Ed., vol. 2501 of *ASIACRYPT 2002. Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 2002.

[6] A. Bar-On, O. Dunkelman, N. Keller, and A. Weizman, "DLCT: A new tool for differential-linear cryptanalysis," in *Proceedings of Advances in Cryptology — EUROCRYPT. 2019–38th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Lecture Notes in Computer Science, pp. 313–342, 2019.

[7] Y. Liu, S. Sun, and C. Li, "Rotational cryptanalysis from a differential-linear perspective - practical distinguishers for round-reduced friet, xoodoo, and alzette," in *Proceedings of Advances in Cryptology EUROCRYPT. 2021 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Lecture Notes in Computer Science, pp. 741–770, 2021.

[8] P. Morawiecki, J. Pieprzyk, and M. Srebrny, "Rotational cryptanalysis of round-reduced keccak," in *Proceedings of Fast Software Encryption–20th International Workshop*, Lecture Notes in Computer Science, pp. 241–262, 2013.

[9] Z. Niu, S. Sun, Y. Liu, and C. Li, "Rotational differential-linear distinguishers of ARX ciphers with arbitrary output linear masks," in *Proceedings of Advances in Cryptology–CRYPTO. 2022–42nd Annual International Cryptology Conference*, Lecture Notes in Computer Science, pp. 3–32, 2022.

[10] M. Liu, X. Lu, and D. Lin, "Differential-linear cryptanalysis from an algebraic perspective," in *Proceedings of Advances in Cryptology–CRYPTO. 2021–41st Annual International Cryptology Conference*, Lecture Notes in Computer Science, pp. 247–277, 2021.

[11] G. Beierle, Christofand Leander, and Y. Todo, "Improved differential-linear attacks with applications to ARX ciphers," in *Proceedings of Advances in Cryptology — CRYPTO. 2020–40th Annual International Cryptology Conference*, Lecture Notes in Computer Science, pp. 329–358, 2020.

[12] H. Wu and B. Preneel, "Differential-linear attacks against the stream cipher phelix," in *Proceedings of Fast Software Encryption–14th International Workshop*, Lecture Notes in Computer Science, pp. 87–100, 2007.

[13] G. Leurent, "Improved differential-linear cryptanalysis of 7-round chaskey with partitioning," in *Proceedings of Advances*

in Cryptology –EUROCRYPT. 2016 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lecture Notes in Computer Science, pp. 344–371, 2016.

[14] T. Huang, I. Tjuawinata, and H. Wu, "Differential-linear cryptanalysis of ICEPOLE," in *Proceedings of Fast Software Encryption–22nd International Workshop*, Lecture Notes in Computer Science, pp. 243–263, 2015.

[15] E. Bellini, D. Gérault, J. Grados, R. H. Makarim, and T. Peyrin, "Fully automated differential-linear attacks against ARX ciphers," in *Proceedings of Topics in Cryptology–CT-RSA. 2023–Cryptographers' Crack at the RSA Conference*, Lecture Notes in Computer Science, pp. 252–276, 2023.

[16] F. Abed, E. List, S. Lucks, and J. Wenzel, "Differential cryptanalysis of round-reduced simon and speck," in *Proceedings of Fast Software Encryption–21st International Workshop*, Lecture Notes in Computer Science, pp. 525–545, 2014.

[17] J. Alizadeh, H. AlKhzaimi, M. R. Aref et al., "Cryptanalysis of SIMON variants with connections," in *Proceedings of Radio Frequency Identification: Security and Privacy Issues–10th International Workshop*, Lecture Notes in Computer Science, pp. 90–107, 2014.

[18] S. Sun, L. Hu, M. Wang et al., "Constructing mixed-integer programming models whose feasible region is exactly the set of all valid differential characteristics of SIMON," *Cryptology ePrint Archive, Paper 2015/122*, 2015.

[19] Q. Wang, Z. Liu, K. Varici, Y. Sasaki, V. Rijmen, and Y. Todo, "Cryptanalysis of reduced-round SIMON32 and SIMON48," in *Proceedings of Progress in Cryptology–INDOCRYPT. 2014–15th International Conference on Cryptology*, Lecture Notes in Computer Science, pp. 143–160, 2014.

[20] S. Kölbl, G. Leander, and T. Tiessen, "Observations on the SIMON block cipher family," in *Proceedings of Advances in Cryptology –CRYPTO–35th Annual Cryptology Conference*, Lecture Notes in Computer Science, pp. 161–185, 2015.

[21] K. Qiao, L. Hu, and S. Sun, "Differential analysis on simeck and SIMON with dynamic key-guessing techniques," in *Proceedings of Information Systems Security and Privacy–Second International Conference*, Communications in Computer and Information Science, pp. 64–85, 2016.

[22] L. Sun, W. Wang, and M. Wang, "Accelerating the search of differential and linear characteristics with the SAT method," *IACR Transactions on Symmetric Cryptology*, vol. 2021, no. 1, pp. 269–315, 2021.

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

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

[25] R. Beaulieu, D. Shors, J. Smith, S. Clark, B. Weeks, and L. W., "The SIMON and SPECK families of lightweight block ciphers," *IACR Cryptology ePrint Archive*, Article ID 404, 2013.

[26] G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong, "The simeck family of lightweight block ciphers," in *Proceedings of Cryptographic Hardware And Embedded Systems–CHES–17th International Workshop*, Lecture Notes in Computer Science, pp. 307–329, 2015.

[27] M. Coutinho, R. de Sousa Júnior, and F. Borges, "Continuous diffusion analysis," *IEEE Access*, vol. 8, pp. 123 735–123 745, 2020.