The Security of SIMON-like Ciphers Against Linear Cryptanalysis

Zhengbin Liu[1,2], Yongqiang Li[1,2], Mingsheng Wang[1,2]

1. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
2. School of Cyber Security, University of Chinese Academy of Sciences
yongq.lee@gmail.com
{liuzhengbin,wangmingsheng}@iie.ac.cn

Abstract. In the present paper, we analyze the security of SIMON-like ciphers against linear cryptanalysis. First, an upper bound is derived on the squared correlation of SIMON-like round function. It is shown that the upper bound on the squared correlation of SIMON-like round function decreases with the Hamming weight of output mask increasing. Based on this, we derive an upper bound on the squared correlation of linear trails for SIMON and SIMECK, which is 2^{-2R+2} for any R-round linear trail. We also extend this upper bound to SIMON-like ciphers. Meanwhile, an automatic search algorithm is proposed, which can find the optimal linear trails in SIMON-like ciphers under the Markov assumption. With the proposed algorithm, we find the provably optimal linear trails for 12, 16, 19, 28 and 37 rounds of SIMON32/48/64/96/128. To the best of our knowledge, it is the first time that the provably optimal linear trails for SIMON64, SIMON96 and SIMON128 are reported. The provably optimal linear trails for 13, 19 and 25 rounds of SIMECK32/48/64 are also found respectively. Besides the optimal linear trails, we also find the 23, 31 and 41-round linear hulls for SIMON64/96/128, and 13, 21 and 27-round linear hulls for SIMECK32/48/64. As far as we know, these are the best linear hull distinguishers for SIMON and SIMECK so far. Compared with the approach based on SAT/SMT solvers in [25], our search algorithm is more efficient and practical to evaluate the security against linear cryptanalysis in the design of SIMON-like ciphers.

Keywords: automatic search, linear trail, linear hull, SIMON, SIMECK

1 Introduction

With the increasingly ubiquitous use of smart devices such as RFID tags, smart cards and mobile phones, lightweight ciphers will gain more and more wide application. During the last decade, many lightweight ciphers have been proposed, including but not limited to mCrypton [27], SEA [35], HIGHT [22], PRESENT [13], CLEFIA [34], MIBS [23], KATAN and KTANTAN [15], KLEIN [20], LED [21], Piccolo [33], LBlock [39], PRINCE [14], TWINE [36], PRIDE [3], Midori [7], RECTANGLE [41], SKINNY [10], SPARX [19].

In 2013, the NSA published two novel families of lightweight block cipher called SIMON and SPECK [8]. In comparison to their predecessors, these families have a more competitive performance in both hardware and software platforms. Afterwards, Yang et al. proposed the SIMECK family of lightweight block ciphers at CHES 2015 [40], which is a more compact and efficient cipher in hardware. SIMON and SIMECK both have a Feistel structure and use the same round function but with different rotational constants (rotational constants $(1, 8, 2)$ for SIMON and $(0, 5, 1)$ for SIMECK). The SIMON design can be generalized to SIMON-like ciphers, which use the same structure and round function but different rotational constants.

The lack of design rationale and security evaluation for SIMON and SPECK inspired the cryptanalysts' curiosity, and they took a lot of investigations for a deeper understanding of these ciphers. Since the publication of SIMON and SPECK, there have been a large variety of papers evaluating the security of SIMON [2,4,5,6,11,16,17,18,37,38]. And among these cryptanalytic results, linear and differential cryptanalysis are the most promising attacks.

Linear cryptanalysis is one of the most important and powerful techniques in the cryptanalysis of symmetric-key cryptographic primitives. For the design of block ciphers, security against linear cryptanalysis is a major security criterion. As for S-box based ciphers, Matsui's branch-and-bound algorithm was widely used to evaluate the security against linear cryptanalysis [29]. Because S-box based ciphers usually use S-boxes operated on 8 or 4-bit words, it is easy to construct their linear approximation tables (LAT). However, the nonlinear component used in SIMON-like ciphers is the AND operation, and it requires 2^{2n} bytes of memory to construct a LAT for SIMON-like round function with n-bit input, which is infeasible for a typical word size of 32 bits.

At CRYPTO 2015, Kölbl et al. derived an explicit formula for the squared correlation of SIMON-like round function [25]. Based on this, they applied an approach based on SAT/SMT solvers to find the optimal linear trails for SIMON, and reported the provably optimal linear trails for SIMON32, SIMON48, and a 16-round optimal linear trail with squared correlation 2^{-54} for SIMON64. Because SIMON and SIMECK use the same structure and round function except different rotational constants, the SAT/SMT solver approach can also be used to find the optimal linear trails for SIMECK. In [26], Kölbl et al. also reported the provably optimal linear trails for SIMECK.

However, Kölbl et al. didn't report the provably optimal linear trails for SIMON with block size 64, 96 and 128 bits. Also, it takes much time for the SAT/SMT solver to find the optimal linear trails in SIMON-like ciphers, which may limit its application to SIMON-like ciphers with large block sizes, such as 96 and 128 bits.

Recently, Liu et al. proposed an automatic search algorithm for the optimal differential trails in SIMON-like ciphers at FSE 2017, and they found the provably optimal differential trails for all versions of SIMON and SIMECK [28]. However, the optimal linear trails is absent in that paper. To fill this gap, we

investigate the security of SIMON-like ciphers against linear cryptanalysis in the present paper.

Our Contributions. Our main contributions are summarized as follows.

1. Based on the theorems given by Kölbl et al. [25], we derive an upper bound on the squared correlation of SIMON-like round function. It is shown that the upper bound on the squared correlation of SIMON-like round function decreases as the Hamming weight of output mask increases.
2. We derive an upper bound on the squared correlation of linear trails for SIMON and SIMECK, which can be extended to SIMON-like ciphers. It is shown that the squared correlation is upper bounded by 2^{-2R+2} for any R-round linear trail.
3. An efficient automatic search algorithm, which is an extension of Matsui's algorithm, is proposed for the optimal linear trails in SIMON-like ciphers. Because the upper bound on the squared correlation of round function decreases with the Hamming weight of output mask increasing, it can always search for linear trails by traversing output masks from low Hamming weight. Once some output mask whose squared correlation does not satisfy the search condition is found, it can break the unnecessary branches as soon as possible, that is, it needn't traverse the output masks with higher Hamming weight.
4. With the proposed algorithm, it is able to find the provably optimal linear trails for SIMON and SIMECK. For SIMON with block size 32, 48, 64, 96 and 128 bits, we find the optimal linear trails on 12, 16, 19, 28 and 37 rounds with squared correlation 2^{-34}, 2^{-50}, 2^{-64}, 2^{-96} and 2^{-128} respectively. Meanwhile we report the provably optimal linear trails for SIMON64, SIMON96 and SIMON128 for the first time. As for SIMECK with block size 32, 48 and 64 bits, we find the provably optimal linear trails on 13, 19 and 25 rounds respectively. Besides, we find the 23, 31 and 41-round linear hulls for SIMON64/96/128, with potential $2^{-62.84}$, $2^{-93.8}$ and $2^{-123.15}$ respectively. The 13, 21 and 27-round linear hulls with potential $2^{-29.43}$, $2^{-46.3}$ and $2^{-61.14}$ are also found for SIMECK32/48/64. Compared with the approach based on SAT/SMT solvers in [25], our search algorithm is more efficient.

Outline. The paper is organized as follows. In Section 2, we give a brief description of the block ciphers SIMON and SIMECK. In Section 3, an upper bound is given on the squared correlation of SIMON-like round function. In Section 4, we derive an upper bound on the squared correlation of linear trails for SIMON and SIMECK. In Section 5, a generic and efficient automatic search algorithm is proposed for the optimal linear trails in SIMON-like ciphers. Section 6 gives the optimal linear trails and linear hulls found for block ciphers SIMON and SIMECK. A short conclusion is given in Section 7.

Notations used in the present paper are defined in Table 1.

Table 1. Notation

Notation	Description
$\overline{x}$	bitwise NOT of x
$x \oplus y$	bitwise exclusive OR (XOR) of x and y
$x \wedge y$	bitwise AND of x and y
$x \vee y$	bitwise OR of x and y
$x \ll r$	shift of x to the left by r positions
$x \gg r$	shift of x to the right by r positions
$x \lll r$	rotation of x to the left by r positions
$x \ggg r$	rotation of x to the right by r positions
$x \| y$	concatenation of bit strings x and y
$wt(x)$	the hamming weight of x
$x \cdot y$	dot product of x and $y : x \cdot y = \bigoplus_{i=0}^{n-1} x_i y_i$
x_i	the i-th bit of the n-bit word x
$\mathbf{0}$	an n-bit vector with all entries equal 0

2 Description of SIMON and SIMECK

SIMON is a family of lightweight block ciphers published by the NSA in 2013. It is based on Feistel construction and operates on $2n$-bit state for $n = 16, 24, 32, 48$ and 64. The key size is composed of m n-bit words, where $m = 2, 3$ and 4 depending on the block size. SIMON with block size $2n$ bits and key size mn bits is referred to as SIMON$2n/mn$.

The round function of SIMON consists of only three bitwise operations: AND ($\wedge$) , XOR ($\oplus$) and rotation ($\lll$), and it is defined as

$$f(x) = ((x \lll 1) \wedge (x \lll 8)) \oplus (x \lll 2).$$

Let (L_i, R_i) be the input of i-th round, and (L_{i+1}, R_{i+1}) be the output of i-th round, then (L_{i+1}, R_{i+1}) is computed as follows:

$$L_{i+1} = f(L_i) \oplus R_i \oplus K_i, R_{i+1} = L_i.$$

The SIMECK family of lightweight block ciphers was proposed by Yang et al. at CHES 2015 [40]. Its design combines the good components of SIMON and SPECK in order to get a more efficient hardware implementation. More specifically, SIMECK uses a slightly modified version of SIMON's round function, and reuses the round function to update the keys in the key schedule just as SPECK does. The SIMECK family includes three variants: SIMECK32/64, SIMECK48/96 and SIMECK64/128. The round function of SIMECK is defined as

$$f(x) = (x \wedge (x \lll 5)) \oplus (x \lll 1).$$

The subkeys are derived from a master key by key scheduling. As the key schedule is irrelevant to the search algorithm, we omit its description and refer the reader to [8] and [40] for the detail description of SIMON and SIMECK.

The round functions of SIMON and SIMECK are shown in Fig 1.

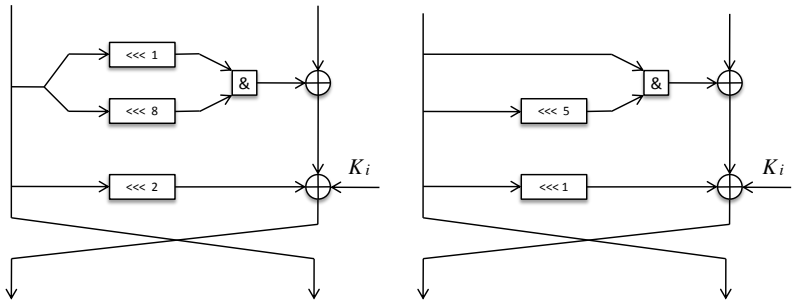

Fig. 1. The round functions of SIMON and SIMECK

3 Upper Bound on the Squared Correlation of SIMON-like Round Function

In this section, we derive an upper bound on the squared correlation of SIMON-like round function, which is based on the theorems given by Kölbl et al. [25].

Definition 1 (SIMON-like Round Function[25]). *Let $x \in \mathbb{F}_2^n$, $a, b, c \in N$, and $a, b, c \geq 0$. Then the SIMON-like function is defined as:*

$$f(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c),$$

where a, b, c are the rotational constants.

In the context, a **SIMON-like cipher** is defined as an iterated cipher using the SIMON-like round function in a Feistel construction. The block ciphers SIMON and SIMECK, whose rotational constants are $(1, 8, 2)$ and $(0, 5, 1)$ respectively, are two particular cases of SIMON-like cipher.

In [9], Beierle gave a more generic definition of SIMON-like round function, which uses a quadratic, rotational invariant function as the non-linear component and an $\mathbb{F}_2$-linear function as the linear component. In this paper, we only focus on the SIMON-like cipher with $f(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$ as the round function.

Kölbl et al. derived a closed expression for the squared correlation of SIMON-like round function, and their results are as follows.

Theorem 1 (Squared Correlation of SIMON-like round function [25]). *Let $f(x) = x \wedge (x \lll (a-b))$, where $x \in \mathbb{F}_2^n$, n is even, $a > b$ and $gcd(n, a-b) = 1$. Let α and β be an input and an output mask, U_β is defined as*

$$U_\beta = \{x \mid (\beta \wedge (x \lll (a-b))) \oplus ((\beta \wedge x) \ggg (a-b)) = \mathbf{0}\}$$

and $d = dim\ U_\beta$. Then the squared correlation that α goes to β can be calculated as

$$C^2(\alpha,\beta) = \begin{cases} 2^{-n+2} & if\ \beta = 2^n - 1\ and\ \alpha \in U_\beta^\perp \\ 2^{-n+d} & if\ \beta \neq 2^n - 1\ and\ \alpha \in U_\beta^\perp \\ 0 & else. \end{cases}$$

Note that $f(x)$ is the only nonlinear component of SIMON-like round function, so $C^2(\alpha,\beta)$ is the squared correlation of SIMON-like round function. From Theorem 1, the squared correlation $C^2(\alpha,\beta)$ is the same for all possible input masks $\alpha \in U_\beta^\perp$, and we use C_β^2 instead of $C^2(\alpha,\beta)$. In the following, we derive an upper bound on the squared correlation of SIMON-like round function.

Theorem 2. *Let $f(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$, where $x \in \mathbb{F}_2^n$, n is even, $a > b$ and $gcd(n, a-b) = 1$. Let β be an output mask of $f(x)$. Then for the squared correlation, it holds that*

(1) If $\beta \neq 2^n - 1$ and $wt(\beta)\ mod\ 2 = 0$, then $C_\beta^2 \leq 2^{-wt(\beta)}$;
(2) If $\beta \neq 2^n - 1$ and $wt(\beta)\ mod\ 2 = 1$, then $C_\beta^2 \leq 2^{-wt(\beta)-1}$;
(3) If $\beta = 2^n - 1$, then $C_\beta^2 \leq 2^{-n+2}$.

Proof. Appendix A.

4 Upper bound on the Squared Correlation of Linear Trails for SIMON and SIMECK

In [9], Beierle gave an upper bound on the probability of differential trails for SIMON and SIMECK. Inspired by this, we derive the upper bound on the squared correlation of linear trails.

In this section, x_i represents the i-th bit of an n-bit vector $x = (x_{n-1}, \ldots, x_1, x_0) \in \mathbb{F}_2^n$. For a vectorial function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $k \in \mathbb{F}_2^n$, the *Feistel round function* is defined as

$$\begin{aligned} F_k : \mathbb{F}_2^n \times \mathbb{F}_2^n &\to \mathbb{F}_2^n \times \mathbb{F}_2^n \\ (x, y) &\mapsto (f(x) \oplus y \oplus k, x). \end{aligned}$$

Within a Feistel cipher, the input mask of one round is denoted as (γ, δ), where γ and δ represent the left and right halves respectively.

Lemma 1. *For $r \geq 1$ and for all non-zero masks α and β, let the squared correlation of any r-round linear trail starting with $(\alpha, \mathbf{0})$ and ending with $(\beta, \mathbf{0})$ be upper bounded by $p(r)$. Let further $p(0) = 1$ and $q = \max_{\beta \neq 0,\alpha} C^2(\alpha,\beta)$. Then for any non-trivial R-round linear trail Ω, it holds that*

$$C^2(\Omega) \leq \max_{k \leq R} p(k) q^{R-k-1}.$$

Proof. For an R-round linear trail $\Omega = (\gamma_0, \delta_0) \to \cdots \to (\gamma_R, \delta_R)$, it holds that $C^2(\Omega) = \prod_{i=0}^{R-1} C^2(\delta_i, \delta_{i+1})$, where $C^2(\delta_i, \delta_{i+1})$ represents the squared correlation of the $(i+1)$-th round. Next we spilt the proof into two cases.

(1) Assume there exist distinct i and j such that $\delta_i = \delta_j = \mathbf{0}$. Without loss of generality, let $\delta_i = \delta_j = \mathbf{0}$ and $\delta_k \neq \mathbf{0}$ for all $k < i$ and all $k > j$. Then, according to the definition,

$$C^2((\gamma_i, \delta_i) \to \cdots \to (\gamma_j, \delta_j)) \leq p(j-i).$$

Since $\delta_i = \delta_j = \mathbf{0}$ and $\delta_k \neq \mathbf{0}$ for $k < i$ and $k > j$, then

$$\begin{aligned} C^2(\Omega) &\leq p(j-i) \prod_{k=0}^{i-1} C^2(\delta_k, \delta_{k+1}) \prod_{k=j+1}^{R-1} C^2(\delta_k, \delta_{k+1}) \\ &\leq p(j-i) q^i q^{R-(j+1)} = p(j-i) q^{R-(j-i)-1}. \end{aligned}$$

(2) If $\delta_i = \mathbf{0}$ for at most one i, then

$$\prod_{k<R} C^2(\delta_k, \delta_{k+1}) \leq \prod_{k \neq i} C^2(\delta_k, \delta_{k+1}) \leq q^{R-1} = p(0) q^{R-1}.$$

□

Lemma 1 is a general statement for all Feistel ciphers. According to it, we can bound the squared correlation of any linear trail, from upper bounds on the squared correlation of all linear trails starting with $(\alpha, \mathbf{0})$ and ending with $(\beta, \mathbf{0})$. As for SIMON-like ciphers, we have the following results.

Corollary 1. *For $r \geq 1$ and for all non-zero masks α and β, let the squared correlation of any r-round linear trail starting with $(\alpha, \mathbf{0})$ and ending with $(\beta, \mathbf{0})$ be upper bounded by 2^{-2r}. Let further $C_\beta^2 \leq 2^{-2}$. Then for any non-trivial R-round linear trail Ω, it holds that*

$$C^2(\Omega) \leq 2^{-2R+2}.$$

Proof. With the notations in Lemma 1, we have $p(r) = 2^{-2r}$ and $q = 2^{-2}$. Therefore,

$$C^2(\Omega) \leq \max_{k \leq R} p(k) q^{R-k-1} = \max_{k \leq R} 2^{-2k} 2^{-2R+2k+2} = 2^{-2R+2}.$$

□

According to Corollary 1, in order to prove the upper bound 2^{-2R+2} on the squared correlation of linear trails, we only need to focus on r-round linear trails of the form $(\alpha, \mathbf{0}) \to \cdots \to (\beta, \mathbf{0})$, and prove the upper bound is 2^{-2r}. For an r-round linear trail of the form $(\alpha, \mathbf{0}) \to \cdots \to (\beta, \mathbf{0})$, we implicitly assume $\delta_i \neq \mathbf{0}$ for all intermediate δ_i, because it is easy to concatenate the short trails to longer ones if $\delta_i = \mathbf{0}$ for some δ_i.

In the following, we derive the upper bound on the squared correlation of linear trails for SIMON and SIMECK.

Theorem 3 (Upper Bounds for SIMON). *Let* $n \in \{16, 24, 32, 48, 64\}$, $x \in \mathbb{F}_2^n$ *and* $f(x) = ((x \lll 1) \wedge (x \lll 8)) \oplus (x \lll 2)$. *The squared correlation of any* R*-round linear trail is upper bounded by* 2^{-2R+2}.

Proof. Fix an r-round linear trail of the form

$$(\mu, \mathbf{0}) \to (\mathbf{0}, \delta_1 = \mu) \to (\gamma_2, \delta_2) \to \cdots \to (\gamma_{r-1}, \delta_{r-1}) \to (\nu, \mathbf{0})$$

with $\delta_i \neq \mathbf{0}$ for all $i \in \{1, \ldots, r-1\}$. According to Corollary 1, we only need to prove that $C_{\delta_i}^2 \leq 2^{-4}$ for at least one i. The proof is split into two cases, and the symbol $*$ indicates an unknown bit.

(1) $wt(\mu) = 1$
Considering the rotational equivalence, let w.l.o.g. $\mu = (1, 0, \ldots, 0)$. Then we have

$$\delta_2 = (0, *_1, 1, 0, \quad 0, 0, 0, 0, \quad *_2, 0, 0, 0, \quad 0, 0, 0, 0, \quad \ldots).$$

If at least one of $*_1$ and $*_2$ equal to one, then $C_{\delta_2}^2 \leq 2^{-4}$. Because according to Theorem 1, when $wt(\beta) = 2$, $C_\beta^2 = 2^{-2}$ if and only if β satisfies $\beta_i = 1$ and $\beta_{i-7 \ mod \ n} = 1$.
Next, we consider the case that both $*_1$ and $*_2$ equal to zero, then

$$\delta_2 = (0, 0, 1, 0, \quad 0, 0, 0, 0, \quad 0, 0, 0, 0, \quad 0, 0, 0, 0, \quad \ldots)$$

and

$$\delta_3 = (1, 0, 0, *_1, \quad 1, 0, 0, 0, \quad 0, 0, *_2, 0, \quad 0, 0, 0, 0, \quad \ldots).$$

It is obviously that $C_{\delta_3}^2 \leq 2^{-4}$.

(2) $wt(\mu) = 2$
Considering the rotational equivalence, let w.l.o.g.

$$\mu = (1, 0, 0, 0, \quad 0, 0, 0, 1, \quad 0, 0, 0, 0, \quad 0, 0, 0, 0, \quad \ldots).$$

Then we have

$$\delta_2 = (0, *_1, 1, 0, \quad 0, 0, 0, 0, \quad *_2, 1, 0, 0, \quad 0, 0, 0, *_1, \quad \ldots).$$

If at least one of $*_1$ and $*_2$ equal to one, then $C_{\delta_2}^2 \leq 2^{-4}$ according to Theorem 1. Next, we consider the case that both $*_1$ and $*_2$ equal to zero, then

$$\delta_2 = (0, 0, 1, 0, \quad 0, 0, 0, 0, \quad 0, 1, 0, 0, \quad 0, 0, 0, 0, \quad \ldots)$$

and

$$\delta_3 = (1, 0, 0, *_1, \quad 1, 0, 0, 1, \quad 0, 0, *_2, 1, \quad 0, 0, 0, 0, \quad 0, *_1, 0, 0, \quad \ldots).$$

It is obviously that $C_{\delta_3}^2 \leq 2^{-4}$.

□

With a similar argument, we can obtain the upper bound on the squared correlation of linear trails for SIMECK. Our results are list as follows.

Theorem 4 (Upper Bounds for SIMECK). *Let $n \in \{16, 24, 32\}$, $x \in \mathbb{F}_2^n$ and $f(x) = (x \wedge (x \lll 5)) \oplus (x \lll 1)$. The squared correlation of any R-round linear trail is upper bounded by 2^{-2R+2}.*

The upper bounds for SIMON and SIMECK can be extended to a more generic SIMON-like design, which can be proven in a similar way. With the SIMON-like cipher defined in this paper, we have the following upper bounds on the squared correlation of linear trails.

Theorem 5 (Upper Bounds for SIMON-like Ciphers). *Let $a, b, c \in N$, $a > b$, $c \neq a$ and $c \neq b$. Let $f(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$, where $x \in \mathbb{F}_2^n$, n is even and $gcd(n, a - b) = 1$. The squared correlation of any R-round linear trail is upper bounded by 2^{-2R+2}.*

These upper bounds give a rough estimation of the security of SIMON-like ciphers against linear cryptanalysis. As for SIMON and SIMECK, it turns out that they are sufficient in order to bound the squared correlation of linear trails below 2^{-2n}, where $2n$ is the block size. We give a comparison of the rounds needed for bounding the squared correlation and the security margin for every instance of SIMON and SIMECK in Table 2.

Table 2. Number of rounds needed for bounding the squared correlation of linear trails by 2^{-2n} for SIMON and SIMECK.

ciphers	block size	key size	rounds	rounds needed	security margin
SIMON	32	64	32	17	15
	48	72	36	25	11
		96	36	25	11
	64	96	42	33	9
		128	44	33	11
	96	96	52	49	3
		144	54	49	5
	128	128	68	65	3
		192	69	65	4
		256	72	65	7
SIMECK	32	64	32	17	15
	48	96	36	25	11
	64	128	44	33	11

From Table 2, the security margin of SIMECK and SIMON with block size less than or equal to 64 bits is reasonable. However, as for SIMON with block size 96 and 128 bits, the security margin is too small, and it may not guarantee the security against linear cryptanalysis with these upper bounds.

In the following, we give an automatic search algorithm, which can find the provably optimal linear trails in SIMON-like ciphers under the Markov assumption. The results found by the search algorithm show that SIMON and SIMECK can be considered resistant against linear cryptanalysis.

5 Automatic Search Algorithm for Optimal Linear Trails

At EUROCRYPT' 94, Matsui proposed a practical automatic search algorithm for the optimal linear trail of DES [29]. The algorithm performs a recursive search for linear trails over a given number of rounds n ($n \geq 1$). It derives the best n-round squared correlation B_n from the knowledge of the best i-round squared correlation B_i ($1 \leq i \leq n-1$) and the initial estimate $\overline{B_n}$ for B_n.

However, Matsui's algorithm can't be applicable to SIMON-like ciphers, since it is infeasible to construct the linear approximation table of SIMON-like round function. Although Biryukov et al. adapted Matsui's algorithm for finding differential trails for SIMON with pDDT (partial difference distribution table) [12], their algorithm may not obtain the optimal differential trail since it uses heuristics so as to find high probability trails. Meanwhile, they didn't report the linear trails for SIMON. Even if partial linear approximation table of SIMON's round function is constructed and used in the search algorithm, it can't make sure to find the optimal linear trail.

In this section, we propose an automatic search algorithm for the optimal linear trails in SIMON-like ciphers, which is also based on Matsui's algorithm. Because our algorithm doesn't introduce any heuristics, it can find the optimal linear trail. The propagation of linear masks in SIMON-like round function is depicted in Fig 2.

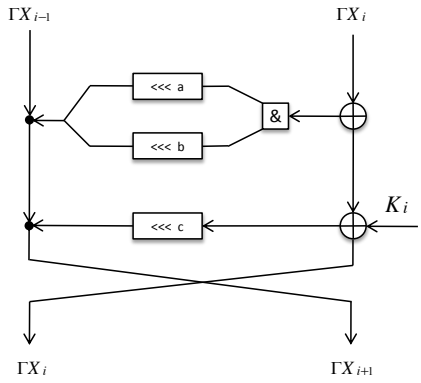

Fig. 2. Propagation of linear masks in SIMON-like round function. The sign "•" denotes "three-forked branch" and acts as XOR on the linear masks.

From the theorem given by Kölbl et al., the squared correlation of SIMON-like round function $C^2(\alpha, \beta)$ is only related to the output mask β and rotational constants a and b, if $\alpha \mapsto \beta$ isn't zero correlation. So in the search algorithm, we can firstly compute the squared correlation of one round. If the squared correlation satisfies the search condition, then we continue finding all possible input masks and searching the next round.

As for searching for input masks, we don't traverse every input mask α and check whether it satisfies the condition $\alpha \in U_\beta^\perp$. On the contrary, we give an algorithm which can find all possible input masks $\alpha \in U_\beta^\perp$. Then we use it to obtain all the possible input masks in the search algorithm directly. The algorithm is based on the algorithm given by Kölbl et al. [25], and the pseudo-code is listed in Algorithm 1.

Algorithm 1 Squared correlation of SIMON-like round function

$//f(x) = x \wedge (x \lll d)$;
$//U_\beta = \{x \mid (\beta \wedge (x \lll d)) \oplus ((\beta \wedge x) \ggg d) = \mathbf{0}\}$;
$tmp = \beta$;
$abits = \beta$;
while tmp ! $= \mathbf{0}$ **do**
    $tmp = \beta \wedge (tmp \ggg d)$;
    $abits = abits \oplus tmp$;
end while
$\mu = abits \ggg 2d$;
$\nu = \beta \ggg d$;
$\omega = \mu \wedge \nu$;
$\gamma = abits \oplus (abits \ggg d)$;
$//x[i]$ and $y[i]$ are n-bit vectors for $i = 1, \cdots, n$
for $i = 1$ *to* n **do**
    $x[i] = \gamma \wedge (1 \ll i)$;
    $y[i] = x[i] \oplus (\omega \wedge (1 \ll (i - 2d)))$;
end for
$C_\beta^2 = 2^{-2 * wt(abits)}$;
Nonzero vectors of $y[i]$ $(i = 1, \cdots, n)$ construct the bases of $U_\beta^\perp$

Note: The arithmetic of bit indices is always done modulo the word size n.

Besides, we apply Theorem 2, which can be used to break the unnecessary branches as soon as possible, to improve the efficiency of the search algorithm. More specifically, we traverse output masks from low Hamming weight for the first and second round, because the upper bound on the squared correlation of SIMON-like round function decreases as the Hamming weight of output mask increases. Once we find some output mask whose maximum squared correlation doesn't satisfy the search condition, that is $C_{max}^2 B_{n-1} < \overline{B_n}$, we break the branch and needn't traverse the output masks with higher Hamming weight. The pseudo-code of our algorithm is listed in Algorithm 2.

Algorithm 2 Search for optimal linear trails in SIMON-like ciphers

Procedure Main:
  Begin the program
  Let $\overline{B}_n = 2 \times B_{n-1}$, and $B_n = 1$.
  Do
    Let $\overline{B}_n = 2^{-1} \times \overline{B}_n$;
    Call Procedure Round-1;
  while $\overline{B}_n \neq B_n$.
  Exit the program

Procedure Round-1:
  For each candidate for ΓX_1 with $wt(\Gamma X_1)$ from 0 to n, do the following:
    If $C^2_{max} \times B_{n-1} < \overline{B}_n$, then //$C^2_{max}$ is precomputed according to Theorem 2.
      Return to the upper procedure;
    Else
      Let $\beta = \Gamma X_1$ and C^2_β is computed according to Theorem 1;
      If $C^2_\beta \times B_{n-1} \geq \overline{B}_n$, then
      Let $c^2_1 = C^2_\beta$;
      For each candidate of $\alpha \in U^\perp_\beta$ //$U^\perp_\beta$ is computed with Algorithm 1.
        Let $f(\beta) = (\alpha \ggg b) \oplus (\beta \ggg c)$, and Call Procedure Round-2;
  Return to the upper procedure;

Procedure Round-2:
  For each candidate for ΓX_2 with $wt(\Gamma X_2)$ from 0 to n, do the following:
    If $c^2_1 \times C^2_{max} \times B_{n-2} < \overline{B}_n$, then
      Return to the upper procedure;
    Else
      Let $\beta = \Gamma X_2$, and C^2_β is computed according to Theorem 1;
      If $c^2_1 \times C^2_\beta \times B_{n-2} \geq \overline{B}_n$, then
      Let $c^2_2 = C^2_\beta$;
      For each candidate of $\alpha \in U^\perp_\beta$
        Let $f(\beta) = (\alpha \ggg b) \oplus (\beta \ggg c)$, and Call Procedure Round-3;
  Return to the upper procedure;

Procedure Round-i ($3 \leq i \leq n-1$):
  Let $\Gamma X_i = \Gamma X_{i-2} \oplus f(\Gamma X_{i-1})$;
  Let $\beta = \Gamma X_i$, and C^2_β is computed according to Theorem 1;
  If $c^2_1 \times \cdots \times c^2_{i-1} \times C^2_\beta \times B_{n-i} \geq \overline{B}_n$, then
  Let $c^2_i = C^2_\beta$;
  For each candidate of $\alpha \in U^\perp_\beta$
    Let $f(\beta) = (\alpha \ggg b) \oplus (\beta \ggg c)$, and Call Procedure Round-$(i+1)$;
  Return to the upper procedure;

Procedure Round-n:
  Let $\Gamma X_n = \Gamma X_{n-2} \oplus f(\Gamma X_{n-1})$;
  Let $\beta = \Gamma X_n$, and C^2_β is computed according to Theorem 1;
  If $c^2_1 \times \cdots \times c^2_{n-1} \times C^2_\beta = \overline{B}_n$, then $B_n = \overline{B}_n$;
  Return to the upper procedure;

In the following, we give a rough estimation of the complexity of the search algorithm. Let m_1 be the number of masks α_1 and β_1 in the first round, for which the maximum squared correlation $C^2_{max}(\alpha_1, \beta_1)$ is greater than or equal to $\overline{B}_n/B_{n-1} : m_1 = \#\{(\alpha_1, \beta_1) \mid C^2_{max}(\alpha_1, \beta_1) \geq \overline{B}_n/B_{n-1}\}$. Analogously, let m_2 be the number of masks α_2 and β_2 in the second round, for which the maximum squared correlation $C^2_{max}(\alpha_2, \beta_2)$ is greater than or equal to $\overline{B}_n/(c_1^2 B_{n-2})$ $: m_2 = \#\{(\alpha_2, \beta_2) \mid C^2_{max}(\alpha_2, \beta_2) \geq \overline{B}_n/(c_1^2 B_{n-2})\}$. As the complexity of the search is dominated by the number of candidates in the first two rounds, the complexity of Algorithm 2 has the form $\mathcal{O}(m_1 m_2)$. Because the maximum squared correlation C^2_{max} decreases with the Hamming weight of output masks increasing, it only searches a very small fraction of all the possible plaintext masks, which makes $\mathcal{O}(m_1 m_2)$ be significantly lower than the complexity of full search 2^{2n}. However, it is difficult to get the precise values of m_1 and m_2, since they change dynamically in the search.

Note that in Theorem 1 and Theorem 2, n and $a-b$ must satisfy the condition $\gcd(n, a-b) = 1$. It is implicitly assumed to be satisfied in SIMON-like ciphers, and therefore Theorem 1 and Theorem 2 can be applied in the search algorithm to find the optimal linear trails efficiently. Our algorithm can also be applied to other SIMON-like designs with $f(x) = x \wedge (x \lll a)$ as the only nonlinear component, because the squared correlation is computed according to Theorem 1 in our search algorithm.

6 Linear Trails and Linear Hulls for SIMON and SIMECK

In this section, Algorithm 2 is applied to search for the optimal linear trails for block ciphers SIMON and SIMECK [1]. The linear trails found are the provably optimal under the Markov assumption. Besides the optimal linear trails, we also find the linear hulls for SIMON and SIMECK with Algorithm 2.

6.1 Linear Trails for SIMON and SIMECK

For SIMON with block size 32, 48, 64, 96 and 128 bits, the optimal linear trails found cover 12, 16, 19, 28 and 37 rounds with squared correlation 2^{-34}, 2^{-50}, 2^{-64}, 2^{-96} and 2^{-128} respectively. The provably optimal linear trails are reported for the first time for SIMON64, SIMON96 and SIMON128. As for SIMON32 and SIMON48, our results are the same as those of Kölbl et al. [25]. The squared correlations of the optimal linear trails for SIMON are shown in Table 3. And the optimal linear trails found for SIMON are shown in Table 7 and Table 8 in Appendix B.

For SIMECK with block size 32, 48 and 64 bits, we find the provably optimal linear trails for up to 13, 19 and 25 rounds with squared correlation 2^{-32}, 2^{-48}

[1] All experiments are performed on a PC with a single core (Intel® Core™ i7 − 6700 CPU 3.4GHz).

Table 3. Squared correlation of the optimal linear trails for SIMON. The squared correlation are given as $log_2 c^2$. The column "times" provides the time needed to find a single optimal linear trail in seconds or hours ("s" and "h" for short).

	SIMON32		SIMON48		SIMON64		SIMON96		SIMON128	
R	$log_2 c^2$	$times$	$log_2 c^2$	$times$	$log_2 c^2$	$times$	$log_2 c^2$	$times$	$log_2 c^2$	$times$
1	-0	$0.00s$	-0	$0.00s$	-0	$0.00s$	-0	$0.00s$	-0	$0.00s$
2	-2	$0.00s$	-2	$0.00s$	-2	$0.00s$	-2	$0.00s$	-2	$0.00s$
3	-4	$0.01s$	-4	$0.00s$	-4	$0.00s$	-4	$0.00s$	-4	$0.00s$
4	-6	$0.02s$	-6	$0.01s$	-6	$0.02s$	-6	$0.05s$	-6	$0.14s$
5	-8	$0.02s$	-8	$0.01s$	-8	$0.02s$	-8	$0.03s$	-8	$0.09s$
6	-12	$0.13s$	-12	$0.23s$	-12	$0.70s$	-12	$2.98s$	-12	$11.97s$
7	-14	$0.13s$	-14	$0.21s$	-14	$0.47s$	-14	$2.89s$	-14	$11.98s$
8	-18	$0.39s$	-18	$0.43s$	-18	$1.09s$	-18	$3.46s$	-18	$12.49s$
9	-20	$0.16s$	-20	$0.23s$	-20	$0.75s$	-20	$2.92s$	-20	$11.84s$
10	-26	$13.03s$	-26	$16.62s$	-26	$32.52s$	-26	$195.55s$	-26	$0.27h$
11	-30	$31.60s$	-30	$169.74s$	-30	$0.17h$	-30	$2.40h$	-30	$15.47h$
12	-34	$72.31s$	-36	$0.48h$	-36	$0.76h$	-36	$4.78h$	-36	$22.22h$
13			-38	$27.46s$	-38	$35.15s$	-38	$197.67s$	-38	$0.30h$
14			-44	$1.27h$	-44	$1.04h$	-44	$1.89h$	-44	$2.55h$
15			-46	$93.11s$	-48	$1.41h$	-48	$4.46h$	-48	$18.48h$
16			-50	$0.32h$	-54	$84.16h$	-54	$136.43h$	-54	$165.34h$
17					-56	$0.32h$	-56	$0.72h$	-56	$0.95h$
18					-62	$126.76h$	-62	$343.88h$	-62	$367.37h$
19					-64	$33.27s$	-64	$90.05s$	-64	$104.12s$
20							-66	$63.07s$	-66	$63.52s$
21							-68	$3.74s$	-68	$3.73s$
22							-72	$242.79s$	-72	$264.31s$
23							-74	$3.52s$	-74	$14.02s$
24							-78	$12.42s$	-78	$23.20s$
25							-80	$3.54s$	-80	$13.86s$
26							-86	$349.58s$	-86	$0.36h$
27							-90	$2.76h$	-90	$17.56h$
28							-96	$5.54h$	-96	$24.85h$
29									-98	$0.31h$
30									-104	$2.82h$
31									-108	$21.12h$
32									-114	$194.86h$
33									-116	$2.96h$
34									-122	$375.46h$
35									-124	$112.37s$
36									-126	$66.27s$
37									-128	$4.37s$

and 2^{-64} respectively. The squared correlations of the optimal linear trails for SIMECK are shown in Table 4. And the optimal linear trails found for SIMECK are shown in Table 9 in Appendix C.

Table 4. Squared correlation of the optimal linear trails for SIMECK. The squared correlation are given as $log_2 c^2$. The column "times" provides the time needed to find a single optimal linear trail in seconds ("s" for short).

	SIMECK32		SIMECK48		SIMECK64	
R	$log_2 c^2$	$times$	$log_2 c^2$	$times$	$log_2 c^2$	$times$
1	-0	$0.00s$	-0	$0.00s$	-0	$0.00s$
2	-2	$0.00s$	-2	$0.00s$	-2	$0.00s$
3	-4	$0.00s$	-4	$0.00s$	-4	$0.00s$
4	-6	$0.00s$	-6	$0.01s$	-6	$0.01s$
5	-8	$0.00s$	-8	$0.01s$	-8	$0.02s$
6	-12	$0.03s$	-12	$0.18s$	-12	$0.50s$
7	-14	$0.02s$	-14	$0.16s$	-14	$0.35s$
8	-18	$0.08s$	-18	$0.32s$	-18	$0.54s$
9	-20	$0.03s$	-20	$0.18s$	-20	$0.38s$
10	-24	$0.12s$	-24	$0.37s$	-24	$0.32s$
11	-26	$0.01s$	-26	$0.03s$	-26	$0.04s$
12	-30	$0.24s$	-30	$0.58s$	-30	$0.60s$
13	-32	$0.02s$	-32	$0.04s$	-32	$0.04s$
14			-36	$1.04s$	-36	$1.28s$
15			-38	$0.24s$	-38	$0.46s$
16			-44	$27.59s$	-44	$30.73s$
17			-44	$0.00s$	-44	$0.00s$
18			-46	$0.00s$	-46	$0.00s$
19			-48	$0.00s$	-48	$0.00s$
20					-50	$0.01s$
21					-52	$0.01s$
22					-56	$0.37s$
23					-58	$0.35s$
24					-62	$0.57s$
25					-64	$0.37s$

Compared with the approach based on SAT/SMT solvers in [25], our algorithm is more efficient. For SIMON-like ciphers with block size less than or equal to 64 bits, our algorithm is able to find the optimal linear trails efficiently. As for SIMON-like ciphers with large block size such as 96 and 128 bits, it can also find the optimal linear trails. To the best of our knowledge, it is the first algorithm that finds the provably optimal linear trails for SIMON96 and SIMON128 in the public literature. Besides evaluating the security of SIMON and SIMECK against linear cryptanalysis, our algorithm has a more practical use in the design of SIMON-like ciphers.

Remark 1. In [26], there is something wrong with the squared correlation of the best linear trails for SIMON48. For example, the squared correlations of 19 and 20-round optimal linear trails are not 2^{-62} and 2^{-66}, and we find the optimal linear trails with squared correlation 2^{-60} and 2^{-64}. We list the 19 and 20-round optimal linear trails for SIMON48 in Table 10 in Appendix D. Analysing the code of CryptoSMT given by Kölbl [24], we find it is a little different from the python code in [25] for the computation of squared correlation (page 21, line 5, "beta" is replaced by "sbits" in the code of CryptoSMT), and we confirm that it is right for the code in [25].

6.2 Linear Hulls for SIMON and SIMECK

The linear hull, which was proposed by Nyberg [30], is a set of linear approximations with the same input mask and output mask. For a block cipher $C = F(P, K)$, the potential of a linear hull with input mask α and output mask β is defined as:

$$ALH(\alpha, \beta) = \sum_{\gamma} (Pr(\alpha \cdot P \oplus \beta \cdot C \oplus \gamma \cdot K = 0) - 1/2)^2.$$

The effect of linear hull is that the bias of linear approximation is much higher than that of an individual linear trail. With linear hull, the linear cryptanalysis requires less known plaintexts.

Table 5. The linear hulls of SIMON.

Block Size	Round	Input active bits	Output active bits	Potential	Reference
64	22	$X_{L,3}, X_{L,27}, X_{L,31}, X_{R,29}$	$Y_{L,3}, Y_{R,1}, Y_{R,2}$	$2^{-63.83}$	[32]
	23	$X_{L,2}, X_{L,30}, X_{R,0}$	$Y_{L,28}, Y_{R,2}, Y_{R,26}, Y_{R,30}$	$2^{-62.84}$	this paper
96	30	$X_{L,2}, X_{L,34}, X_{L,38}, X_{L,42}, X_{R,36}$	$Y_{L,2}, Y_{L,42}, Y_{L,46}, Y_{R,0}, Y_{R,40}$	$2^{-94.2}$	[1]
	30	$X_{L,2}, X_{L,6}, X_{L,14}, X_{L,46}, X_{R,0}$	$Y_{L,6}, Y_{L,10}, Y_{L,14}, Y_{R,4}, Y_{R,12}$	$2^{-91.22}$	this paper
	31	$X_{L,2}, X_{L,6}, X_{L,14}, X_{L,46}, X_{R,0}$	$Y_{L,4}, Y_{L,12}, Y_{R,2}, Y_{R,6}, Y_{R,14}$	$2^{-93.8}$	this paper
128	41	$X_{L,2}, X_{L,58}, X_{L,62}, X_{R,60}$	$Y_{L,60}, Y_{R,0}, Y_{R,2}, Y_{R,58}, Y_{R,62}$	$2^{-126.6}$	[1]
	41	$X_{L,2}, X_{L,6}, X_{L,62}, X_{R,0}$	$Y_{L,0}, Y_{R,2}, Y_{R,6}, Y_{R,62}$	$2^{-123.15}$	this paper

Besides the optimal linear trails, we also investigate the linear hulls of SIMON and SIMECK. With the input and output masks of the optimal linear trail, we extend Algorithm 2 to find the linear hulls of SIMON and SIMECK. More specifically, after finding the optimal linear trail, we fix the input and output masks and search for linear trails with the same input and output masks of the optimal linear trail. We obtain as many linear trails as possible and add their squared correlations to get the potential.

For SIMON with block size 64, 96 and 128 bits, we find the 23, 31 and 41-round linear hulls with potential $2^{-62.84}$, $2^{-93.8}$ and $2^{-123.15}$ respectively. As for SIMECK with block size 32, 48 and 64 bits, the 13, 21 and 27-round linear hulls are found, with potential $2^{-29.43}$, $2^{-46.3}$ and $2^{-61.14}$ respectively. As far as we know, these are the best linear hull distinguishers for SIMON and SIMECK so far. The linear hulls of SIMON and SIMECK are shown in Table 5 and Table 6. In these tables, (X_L, X_R) and (Y_L, Y_R) represent the input mask and output mask respectively, where X_L is the left half of the input mask and X_R is the right half.

Table 6. The linear hulls of SIMECK.

Block Size	Round	Input active bits	Output active bits	Potential	Reference
32	13	$X_{L,1}$	$Y_{R,1}$	$2^{-30.91}$	[31]
	13	$X_{L,0}, X_{L,4}$	$Y_{L,1}, Y_{R,0}, Y_{R,2}, Y_{R,4}$	$2^{-29.43}$	this paper
48	20	$X_{L,19}, X_{L,21}, X_{R,20}$	$Y_{L,21}, Y_{R,20}$	$2^{-45.66}$	[31]
	21	$X_{L,1}, X_{L,23}, X_{R,0}$	$Y_{L,0}, Y_{R,1}, Y_{R,23}$	$2^{-46.3}$	this paper
64	26	$X_{L,18}, X_{L,22}$	$Y_{L,22}, Y_{R,21}$	$2^{-62.09}$	[31]
	27	$X_{L,0}, X_{L,4}$	$Y_{L,3}, Y_{R,2}, Y_{R,4}$	$2^{-61.14}$	this paper

7 Conclusion

In this paper, we derive an upper bound on the squared correlation of SIMON-like round function. Based on this, we proved the upper bounds on the squared correlation of linear trails for SIMON and SIMECK. Meanwhile, we propose an automatic search algorithm for the optimal linear trails in SIMON-like ciphers. The block ciphers SIMON and SIMECK are used as a test platform for demonstrating the practical application of our algorithm. With the proposed algorithm, we find the provably optimal linear trails for all versions of block ciphers SIMON and SIMECK, and report the provably optimal linear trails for SIMON64, SIMON96 and SIMON128 for the first time. Besides the optimal linear trails, we also find the best linear hulls for SIMON and SIMECK so far.

The proposed algorithm is not only helpful for evaluating the security of SIMON-like ciphers against linear cryptanalysis, but also useful in the design of SIMON-like ciphers.

References

1. M. A. Abdelraheem, J. Alizadeh, H. A. Alkhzaimi, M. R. Aref, N. Bagheri, P. Gauravaram, and M. M. Lauridsen. Improved linear cryptanalysis of reduced-round simon. 2014. http://eprint.iacr.org/2014/681.
2. F. Abed, E. List, S. Lucks, and J. Wenzel. Differential cryptanalysis of round-reduced Simon and Speck. In *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, pages 525–545, 2014.
3. M. R. Albrecht, B. Driessen, E. B. Kavun, G. Leander, C. Paar, and T. Yalçin. Block ciphers - focus on the linear layer (feat. PRIDE). In *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, pages 57–76, 2014.
4. J. Alizadeh, H. AlKhzaimi, M. R. Aref, N. Bagheri, P. Gauravaram, A. Kumar, M. M. Lauridsen, and S. K. Sanadhya. Cryptanalysis of SIMON variants with connections. In *Radio Frequency Identification: Security and Privacy Issues - 10th International Workshop, RFIDSec 2014, Oxford, UK, July 21-23, 2014, Revised Selected Papers*, pages 90–107, 2014.
5. J. Alizadeh, H. AlKhzaimi, M. R. Aref, N. Bagheri, P. Gauravaram, and M. M. Lauridsen. Improved linear cryptanalysis of round reduced SIMON. *IACR Cryptology ePrint Archive*, 2014:681, 2014.
6. H. AlKhzaimi and M. M. Lauridsen. Cryptanalysis of the SIMON family of block ciphers. *IACR Cryptology ePrint Archive*, 2013:543, 2013.
7. S. Banik, A. Bogdanov, T. Isobe, K. Shibutani, H. Hiwatari, T. Akishita, and F. Regazzoni. Midori: A block cipher for low energy. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, pages 411–436, 2015.
8. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. The SIMON and SPECK families of lightweight block ciphers. *IACR Cryptology ePrint Archive*, 2013:404, 2013.
9. C. Beierle. Pen and paper arguments for SIMON and simon-like designs. In *Security and Cryptography for Networks - 10th International Conference, SCN 2016, Amalfi, Italy, August 31 - September 2, 2016, Proceedings*, pages 431–446, 2016.
10. C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, pages 123–153, 2016.
11. A. Biryukov, A. Roy, and V. Velichkov. Differential analysis of block ciphers SIMON and SPECK. In *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, pages 546–570, 2014.
12. A. Biryukov and V. Velichkov. Automatic search for differential trails in ARX ciphers. In *Topics in Cryptology - CT-RSA 2014 - The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February 25-28, 2014. Proceedings*, pages 227–250, 2014.
13. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher.

In *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, pages 450–466, 2007.

14. J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, pages 208–225, 2012.
15. C. D. Cannière, O. Dunkelman, and M. Knezevic. KATAN and KTANTAN - A family of small and efficient hardware-oriented block ciphers. In *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings*, pages 272–288, 2009.
16. H. Chen and X. Wang. Improved linear hull attack on round-reduced simon with dynamic key-guessing techniques. In *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 428–449, 2016.
17. Z. Chen, N. Wang, and X. Wang. Impossible differential cryptanalysis of reduced round SIMON. *IACR Cryptology ePrint Archive*, 2015:286, 2015.
18. N. Courtois, T. Mourouzis, G. Song, P. Sepehrdad, and P. Susil. Combined algebraic and truncated differential cryptanalysis on reduced-round simon. In *SECRYPT 2014 - Proceedings of the 11th International Conference on Security and Cryptography, Vienna, Austria, 28-30 August, 2014*, pages 399–404, 2014.
19. D. Dinu, L. Perrin, A. Udovenko, V. Velichkov, J. Großschädl, and A. Biryukov. Design strategies for ARX with provable bounds: Sparx and LAX. In *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, pages 484–513, 2016.
20. Z. Gong, S. Nikova, and Y. W. Law. KLEIN: A new family of lightweight block ciphers. In *RFID. Security and Privacy - 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26-28, 2011, Revised Selected Papers*, pages 1–18, 2011.
21. J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw. The LED block cipher. In *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, pages 326–341, 2011.
22. D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee. HIGHT: A new block cipher suitable for low-resource device. In *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop, Yokohama, Japan, October 10-13, 2006, Proceedings*, pages 46–59, 2006.
23. M. Izadi, B. Sadeghiyan, S. S. Sadeghian, and H. A. Khanooki. MIBS: A new lightweight block cipher. In *Cryptology and Network Security, 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009. Proceedings*, pages 334–348, 2009.
24. S. Kölbl. CryptoSMT: An easy to use tool for cryptanalysis of symmetric primitives. https://github.com/kste/cryptosmt.
25. S. Kölbl, G. Leander, and T. Tiessen. Observations on the SIMON block cipher family. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 161–185, 2015.

26. S. Kölbl and A. Roy. A brief comparison of Simon and Simeck. *IACR Cryptology ePrint Archive*, 2015:706, 2015.
27. C. H. Lim and T. Korkishko. mCrypton - A lightweight block cipher for security of low-cost RFID tags and sensors. In *Information Security Applications, 6th International Workshop, WISA 2005, Jeju Island, Korea, August 22-24, 2005, Revised Selected Papers*, pages 243–258, 2005.
28. Z. Liu, Y. Li, and M. Wang. Optimal differential trails in simon-like ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(1):358–379, 2017.
29. M. Matsui. On correlation between the order of s-boxes and the strength of DES. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, pages 366–375, 1994.
30. K. Nyberg. Linear approximation of block ciphers. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, pages 439–444, 1994.
31. L. Qin, H. Chen, and X. Wang. Linear hull attack on round-reduced simeck with dynamic key-guessing techniques. In *Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II*, pages 409–424, 2016.
32. D. Shi, L. Hu, S. Sun, L. Song, K. Qiao, and X. Ma. Improved linear (hull) cryptanalysis of round-reduced versions of SIMON. *SCIENCE CHINA Information Sciences*, 60(3):39101:1–39101:3, 2017.
33. K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai. Piccolo: An ultra-lightweight blockcipher. In *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, pages 342–357, 2011.
34. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-bit blockcipher CLEFIA (extended abstract). In *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, pages 181–195, 2007.
35. F. Standaert, G. Piret, N. Gershenfeld, and J. Quisquater. SEA: A scalable encryption algorithm for small embedded applications. In *Smart Card Research and Advanced Applications, 7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006, Tarragona, Spain, April 19-21, 2006, Proceedings*, pages 222–236, 2006.
36. T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi. TWINE : A lightweight block cipher for multiple platforms. In *Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers*, pages 339–354, 2012.
37. N. Wang, X. Wang, K. Jia, and J. Zhao. Differential attacks on reduced SIMON versions with dynamic key-guessing techniques. *IACR Cryptology ePrint Archive*, 2014:448, 2014.
38. Q. Wang, Z. Liu, K. Varici, Y. Sasaki, V. Rijmen, and Y. Todo. Cryptanalysis of reduced-round SIMON32 and SIMON48. In *Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings*, pages 143–160, 2014.
39. W. Wu and L. Zhang. Lblock: A lightweight block cipher. In *Applied Cryptography and Network Security - 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011. Proceedings*, pages 327–344, 2011.
40. G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong. The simeck family of lightweight block ciphers. In *Cryptographic Hardware and Embedded Systems -*

CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings, pages 307–329, 2015.

41. W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede. RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. *SCIENCE CHINA Information Sciences*, 58(12):1–15, 2015.

A Proof of Theorem 2

Proof. Let $k = a - b$, $L_\beta(x) = \beta \wedge S^k(x) \oplus S^{n-k}(\beta \wedge x)$, and $U = \ker(L_\beta(x))$, where $S^i(x) = (x \lll i)$ for $0 \le i \le n-1$. Then as shown in [25], it holds

$$\lambda_f^2(\alpha,\beta) = (\sum_{x\in\mathbb{F}_2^n} (-1)^{\beta\cdot f(x)\oplus\alpha\cdot x})^2 \le |\ker(L_\beta(x))|2^n.$$

Let

$$M_\beta = \begin{pmatrix} \beta_{n-1} & \dots & \dots & 0 \\ \vdots & \beta_{n-2} & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & \dots & \beta_0 \end{pmatrix}, M_{S^i} = \begin{pmatrix} 0_{n-i,i} & I_{n-i,n-i} \\ I_{i,i} & 0_{i,n-i} \end{pmatrix}.$$

Then

$$L_\beta(x) = (M_\beta M_{S^k} \oplus M_{S^{n-k}} M_\beta) \cdot x^t = L_\beta \cdot x^t,$$

where $x = (x_{n-1}, \dots, x_0) \in \mathbb{F}_2^n$ and x^t means the transpose of x. Thus we get

$$C^2(\alpha,\beta) = \frac{\lambda_f(\alpha,\beta)}{2^{2n}} \le \frac{2^{n-\mathrm{rank}(L_\beta)}}{2^n} = 2^{-\mathrm{rank}(L_\beta)}.$$

Then we only need to investigate the rank of $L_\beta = M_\beta M_{S^k} \oplus M_{S^{n-k}} M_\beta$. In the following, for a matrix M and $0 \le i, j \le n-1$, $M[i]$ means the i-th row of M, and $M[i,j]$ means the j-th entry in i-th row of M. For example, $M_\beta[0] = [\beta_{n-1}, 0, \dots, 0]$.

Let $L = M_\beta M_{S^k}$. Then $M_{S^{n-k}} M_\beta = L^t$ and $L_\beta = L \oplus L^t$. For $0 \le i, j \le n-1$, it is easy to see that

$$L[i,j] = \begin{cases} \beta_{n-1-i} & if\ j = i + k \mod n \\ 0 & else \end{cases}$$

and

$$L^t[i,j] = \begin{cases} \beta_{k-1-i} & if\ j = i - k \mod n \\ 0 & else, \end{cases}$$

where $k-1-i$ is computed in $\mathbb{Z}_n$. Therefore

$$L_\beta = \begin{bmatrix} & & & & \beta_{n-1} & & \beta_{k-1} & & \\ & & & & \ddots & & \ddots & & \\ & & & & & \ddots & & & \\ & & & & & & & \beta_0 & \\ & & & & & & & \ddots & \\ \beta_{n-1} & & & & & & & & \\ & \ddots & & & & & & & \\ & & & & & & & \beta_k & \\ \beta_{k-1} & & \ddots & & & & & & \\ & \ddots & & & \ddots & & & & \\ & & \beta_0 & & & \beta_k & & & \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \} n-k \\ , \\ \} k \end{matrix}$$

which means L_β is a symmetric matrix. Furthermore, there are only two entries which can be nonzero in the i-th row of L_β, which are

$$L_\beta[i, i+k] \text{ and } L_\beta[i, i-k]$$

respectively for $0 \leq i \leq n-1$, and there are also only two entries which can be nonzero in the i-th column of L_β, which are

$$L_\beta[i-k, i] \text{ and } L_\beta[i+k, i]$$

respectively for $0 \leq i \leq n-1$. Note that $i \pm k$ means $(i \pm k) \mod n$ in the proof.

First, we prove that

$$\text{rank}(L_\beta) \geq \text{wt}(\beta).$$

Let $S = \{i \mid L_\beta[i, i+k] = 1, 0 \leq i \leq n-1\}$. Then $|S| = \text{wt}(\beta)$. We are going to show that $\{L_\beta[i] \mid i \in S\}$ are linear independent. Suppose there exists $S_1 \subseteq S$ such that

$$\sum_{i \in S_1} L_\beta[i] = \mathbf{0}. \tag{1}$$

For $i \in S_1 \subseteq S$, we have $L_\beta[i, i+k] = 1$. Note that the only two entries in the $(i+k)$-th column of L_β that can be nonzero are $L_\beta[i, i+k]$ and $L_\beta[i+2k, i+k]$. Then equality (1) means for $i \in S_1$, it holds

$$L_\beta[i+2k, i+k] = 1 = L_\beta[i+k, i+2k],$$

from which we get $i+2k \in S_1 \subseteq S$ and $i+k \in S$. Choosing $i \in S_1$ and using the above fact recursively, we can get that there exists l, such that

$$i + 2lk = i \mod n.$$

Then we have $l = \frac{n}{2}$ since $\gcd(k, n) = 1$. This means equality (1) holds if and only if $S_1 = \{i + 2jk \mid 0 \leq j \leq \frac{n}{2} - 1\}$ for some $0 \leq i \leq n-1$, which is equivalent to that $S_1 = \{1 + 2jk \mid 0 \leq j \leq \frac{n}{2} - 1\}$ or $S_1 = \{2jk \mid 0 \leq j \leq \frac{n}{2} - 1\}$. For

the two cases, we can get that $S = \{i \mid 0 \leq i \leq n-1\}$, which is equivalent to $\mathrm{wt}(\beta) = n$.

Therefore, when $\mathrm{wt}(\beta) = n$, $\mathrm{rank}(L_\beta) = n-2$ since both the odd rows and even rows of L_β are linear dependent. When $\mathrm{wt}(\beta) < n$,

$$\mathrm{rank}(L_\beta) \geq \mathrm{wt}(\beta)$$

since $\sum_{i \in S_1} L_\beta[i] \neq \mathbf{0}$ for any subset $S_1 \subseteq S$. This means $\{L_\beta[i] \mid i \in S\}$ are linear independent. This has proved the items (1) and (3).

Next, we prove that when $\mathrm{wt}(\beta) < n$ and $\mathrm{wt}(\beta)$ is odd, it holds

$$\mathrm{rank}(L_\beta) \geq \mathrm{wt}(\beta) + 1.$$

Let $S = \{i \mid L_\beta[i, i+k] = 1, 0 \leq i \leq n-1\}$, and $\bar{S} = \{i \mid L_\beta[i, i-k] = 1, L_\beta[i, i+k] = 0, 0 \leq i \leq n-1\}$. It is easy to see that $S \cap \bar{S} = \emptyset$ and $\bar{S} = \{i+k \mid i \in S, i+k \notin S\}$. Therefore, $\bar{S} \neq \emptyset$. Otherwise, $\{i+k \mid i \in S\} = S$, which means there exists $1 \leq l \leq n$, such that $i + lk = i \mod n$ for $i \in S$. This implies $l = n$ and hence $\mathrm{wt}(\beta) = n$, which is a contradiction.

We define the function $EL(i, j)$ as follows:

$$EL(i,j) = \begin{cases} (i-2k, j) & if\ j = i-k \\ (i, j-2k) & if\ j = i+k, \end{cases}$$

where $0 \leq i, j \leq n-1$, and the computation is in $\mathbb{Z}_n$. We also define

$$EL^k(i,j) = \begin{cases} (i,j) & if\ k = 0 \\ EL(EL^{k-1}(i,j)) & if\ k \geq 1. \end{cases}$$

Note that for $i \in \bar{S}$ it holds $L_\beta[i, i-k] = 1$ and $L_\beta(i, i+k) = 1$. Suppose $i_0 \in \bar{S}$. Then there exists $r \geq 1$ such that $L_\beta(EL^r(i_0, i_0-k)) = 0$. Let r_{i_0} be the smallest number such that $L_\beta(EL^{r_{i_0}}(i_0, i_0-k)) = 0$. Then $L_\beta[EL^k(i_0, i_0-k)] = 1$ for $0 \leq k \leq r_{i_0}-1$. We call $[EL^k(i_0, i_0-k), 0 \leq k \leq r_{i_0}-1]$ be the elimination chain of (i_0, i_0-k) and r_{i_0} is called the length of the elimination chain of (i_0, i_0-k).

Note that $\mathrm{wt}(\beta)$ is odd, then there exists $i_0 \in \bar{S}$, such that the elimination chain of (i_0, i_0-k) has odd length. Otherwise, assume the elimination chain of $(i, i-k)$, which is denoted by r_i, has even length for all $i \in \bar{S}$. Then

$$\{EL^l(i_1, i_1-k) \mid 0 \leq l \leq r_{i_1}\} \cap \{EL^l(i_2, i_2-k) \mid 0 \leq l \leq r_{i_2}\} = \emptyset$$

for $i_1 \neq i_2 \in \bar{S}$ and

$$\sum_{i \in \bar{S}} r_i = |S| = \mathrm{wt}(\beta).$$

This means $\mathrm{wt}(\beta)$ is even, which contradicts with the supposition that $\mathrm{wt}(\beta)$ is odd.

At last, we prove that $\{L_\beta[i_0]\} \cup \{L_\beta[i] \mid i \in S\}$ is linear independent, where $i_0 \in \bar{S}$ such that the elimination chain of (i_0, i_0-k) has odd length. Let r be the length, and let $S_2 = \{i_0 - 2lk \mid 1 \leq l \leq \frac{r-1}{2}\}$.

Note that $L_\beta[i, i_0-k] = 0$ for all $i \in S\backslash S_2$, and $L_\beta[i, i_1-k] = 0 = L_\beta[i, i_1+k]$ for all $i \in S\backslash S_2$ and $i_1 \in S_2$. Furthermore, since $\mathrm{wt}(L_\beta[i_0]) = 1$ and $\mathrm{wt}(L_\beta[i]) = 2$ for $i \in S_2$, then $L_\beta[i, j] = 0$ for all $i \in S_2 \cup \{i_0\}$ and $j \in \{k \mid L_\beta[t, k] = 1 \text{ for some } t \in S \setminus (S_2 \cup \{i_0\}), 0 \le k \le n-1\}$. Thus, it only need to prove that

$$\{L_\beta[i_0]\} \cup \{L_\beta[i] \mid i \in S_2\}$$

is linear independent. This is easy to prove since for any subset $S_3 \subset S_2$, $\mathrm{wt}(L_\beta[i_0] + \sum_{i \in S_3} L_\beta[i]) \ge 1$. Therefore, $\{L_\beta[i_0]\} \cup \{L_\beta[i] \mid i \in S\}$ is linear independent and hence

$$\mathrm{rank}(L_\beta) \ge |S| + 1 = \mathrm{wt}(\beta) + 1.$$

Then we complete the proof. □

B Linear trails for SIMON

Table 7. Linear trails for SIMON32, SIMON48 and SIMON64

	SIMON32			SIMON48			SIMON64		
R	ΓL	ΓR	$log_2 c^2$	ΓL	ΓR	$log_2 c^2$	ΓL	ΓR	$log_2 c^2$
0	447	0	-0	400004	1	-0	1	0	-0
1	0	447	-0	1	4	-2	0	1	-0
2	447	14	-8	4	0	-2	1	40000000	-2
3	14	440	-4	0	4	-0	40000000	10000001	-2
4	440	100	-4	4	40001	-2	10000001	4000000	-4
5	100	400	-2	40001	400404	-4	4000000	11000001	-2
6	400	0	-2	400404	104104	-6	11000001	40400000	-6
7	0	400	-0	104104	400404	-8	40400000	1100001	-4
8	400	100	-2	400404	40001	-6	1100001	1840000	-6
9	100	440	-2	40001	4	-4	1840000	1300001	-6
10	440	10	-4	4	0	-2	1300001	40c00000	-8
11	10	444	-2	0	4	-0	40c00000	11000001	-4
12				4	1	-2	11000001	4000000	-6
13				1	400004	-2	4000000	10000001	-2
14				400004	100000	-4	10000001	40000000	-4
15				100000	440004	-2	40000000	1	-2
16							1	0	-2
17							0	1	-0
18							1	40000000	-2
19							40000000	10000001	-2
$\sum_r log_2 c_r^2$	-30			-46			-64		

Table 8. Linear trails for SIMON96 and SIMON128

	SIMON96			SIMON128		
R	ΓL	ΓR	$log_2 c^2$	ΓL	ΓR	$log_2 c^2$
0	400000000044	1	-0	4000000000000004	1	-0
1	1	44	-2	1	4	-2
2	44	10	-4	4	0	-2
3	10	40	-2	0	4	-0
4	40	0	-2	4	1	-2
5	0	40	-0	1	4000000000000004	-2
6	40	10	-2	4000000000000004	1000000000000000	-4
7	10	44	-2	1000000000000000	4000000000000004	-2
8	44	1	-4	4000000000000004	100000000000001	-6
9	1	400000000044	-2	100000000000001	440000000000004	-4
10	400000000044	100000000010	-6	440000000000004	610000000000000	-6
11	100000000010	440000000040	-4	610000000000000	4c0000000000004	-6
12	440000000040	610000000000	-6	4c0000000000004	300000000000001	-8
13	610000000000	4c0000000040	-6	300000000000001	4000000000000004	-4
14	4c0000000040	300000000010	-8	4000000000000004	1000000000000000	-6
15	300000000010	400000000044	-4	1000000000000000	4000000000000004	-2
16	400000000044	1	-6	4000000000000004	1	-4
17	1	44	-2	1	4	-2
18	44	10	-4	4	0	-2
19	10	40	-2	0	4	-0
20	40	0	-2	4	1	-2
21	0	40	-0	1	4000000000000004	-2
22	40	10	-2	4000000000000004	1000000000000000	-4
23	10	44	-2	1000000000000000	4000000000000004	-2
24	44	1	-4	4000000000000004	100000000000001	-6
25	1	400000000044	-2	100000000000001	440000000000004	-4
26	400000000044	100000000010	-6	440000000000004	610000000000000	-6
27	100000000010	440000000040	-4	610000000000000	4c0000000000004	-6
28	440000000040	10000000000	-6	4c0000000000004	300000000000001	-8
29				300000000000001	4000000000000004	-4
30				4000000000000004	1000000000000000	-6
31				1000000000000000	4000000000000004	-2
32				4000000000000004	1	-4
33				1	4	-2
34				4	0	-2
35				0	4	-0
36				4	1	-2
37				1	4000000000000004	-2
$\sum_r log_2 c_r^2$		-96			-128	

C Linear trails for SIMECK

Table 9. Linear trails for SIMECK32, SIMECK48 and SIMECK64

	SIMECK32			SIMECK48			SIMECK64		
R	ΓL	ΓR	$log_2 c^2$	ΓL	ΓR	$log_2 c^2$	ΓL	ΓR	$log_2 c^2$
0	11	0	-0	1	0	-0	$8000000a$	1	-0
1	0	11	-0	0	1	-0	1	a	-2
2	11	8	-4	1	800000	-2	a	4	-4
3	8	15	-2	800000	400001	-2	4	8	-2
4	15	2	-6	400001	200000	-4	8	0	-2
5	2	14	-2	200000	500001	-2	0	8	-0
6	14	8	-4	500001	800000	-6	8	4	-2
7	8	10	-2	800000	100001	-2	4	a	-2
8	10	0	-2	100001	0	-4	a	1	-4
9	0	10	-0	0	100001	-0	1	$8000000a$	-2
10	10	8	-2	100001	800000	-4	$8000000a$	4	-6
11	8	14	-2	800000	500001	-2	4	80000008	-2
12	14	2	-4	500001	200000	-6	80000008	0	-4
13	2	15	-2	200000	400001	-2	0	80000008	-0
14				400001	800000	-4	80000008	4	-4
15				800000	1	-2	4	$8000000a$	-2
16				1	0	-2	$8000000a$	1	-6
17				0	1	-0	1	a	-2
18				1	800000	-2	a	4	-4
19				800000	400001	-2	4	8	-2
20							8	0	-2
21							0	8	-0
22							8	4	-2
23							4	a	-2
24							a	1	-4
25							1	$8000000a$	-2
$\sum_r log_2 c_r^2$		-32			-48			-64	

D The 19 and 20-round optimal linear trails for SIMON48

Table 10. The 19 and 20-round optimal linear trails for SIMON48

	19-round linear trail			20-round linear trail		
R	ΓL	ΓR	$log_2 c^2$	ΓL	ΓR	$log_2 c^2$
0	400004	1	-0	400044	1	-0
1	1	4	-2	1	44	-2
2	4	0	-2	44	10	-4
3	0	4	-0	10	40	-2
4	4	1	-2	40	0	-2
5	1	400004	-2	0	40	-0
6	400004	100000	-4	40	10	-2
7	100000	440004	-2	10	44	-2
8	440004	50401	-6	44	1	-4
9	50401	44704	-8	1	400044	-2
10	44704	1400	-10	400044	504010	-6
11	1400	44000	-4	504010	447040	-8
12	44000	10000	-4	447040	14000	-10
13	10000	40000	-2	14000	440000	-4
14	40000	0	-2	440000	100000	-4
15	0	40000	-0	100000	400000	-2
16	40000	10000	-2	400000	0	-2
17	10000	44000	-2	0	400000	-0
18	44000	1000	-4	400000	100000	-2
19	1000	44400	-2	100000	440000	-2
20				440000	10000	-4
$\sum_r log_2 c_r^2$	-60			-64		