Automatic Search for Related-Key Differential Trails in SIMON-like Block Ciphers Based on MILP

Xuzi Wang[1,2], Baofeng Wu[1,2], Lin Hou[1,2(✉)], and Dongdai Lin[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
{wangxuzi,wubaofeng,houlin,ddlin}@iie.ac.cn
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

Abstract. In this paper, we revisit the relationship between the probability of differential trails and the input difference of each round for SIMON-like block ciphers. The key observation is that not only the Hamming weight but also the positions of active bits of the input difference have effect on the probability. Based on this, our contributions are mainly twofold. Firstly, we rebuild the MILP model for SIMON-like block ciphers without quadratic constraints. Accordingly, we give the accurate objective function and reduce its degree to one by adding auxiliary variants to make the model easy to solve. Secondly, we search for optimal differential trails for SIMON and SIMECK based on this model. To the best of our knowledge, this is the first time that related-key differential trails have been obtained. Besides, we not only recover the single-key results in [11], but also obtain impossible differentials through this method.

Keywords: SIMON · SIMECK · Related-key differential trails
Impossible differentials · MILP

1 Introduction

Devices of small size, such as smart cards and sensor networks, are increasingly involved in our life. Despite of the convenience, a major concern is that these highly constrained devices cannot afford the computational cost of traditional block ciphers such as DES and AES. To this end, the notion of *lightweight block cipher* was raised, and has seen a flourish of research works in recent years.

Specifically, SIMON and SPECK families of block ciphers [4] proposed by the NSA are amongst the most promising candidates. The distinguishing feature of SIMON (SPECK) is that AND operations (modular additions) serve as non-linear components instead of S-boxes, and this directly yields an implementation advantage on both hardware and software platforms. Later on, Yang *et al.* proposed a variant of SIMON, namely SIMECK [22] which adopts the rotational constants and key schedules of SPECK within the framework of SIMON.

L. Chen et al. (Eds.): ISC 2018, LNCS 11060, pp. 116–131, 2018.
https://doi.org/10.1007/978-3-319-99136-8_7

We refer to both SIMON and SIMECK as SIMON-like block ciphers, as introduced in [11].

Related Work. For SIMON, no designing rationale or security analysis was explicitly given in the original paper [4]. Lots of subsequent researches have been done for evaluating its security, and a majority of these works are also applicable to the SIMECK case due to their great similarities [22].

There have been many results for SIMON by differential cryptanalysis [2,3,6–11,20] and linear cryptanalysis [1,12,14]. To our interest, Kölbl *et al.* [9] gave an exact closed form expression for the differential probability, and obtained single-key differential characteristics through SAT/SMT solvers; in 2017, Liu *et al.* [11] further investigated the relationship between Hamming weight of input difference and differential probability, and proposed an automatic searching algorithm by adapting Matsui's algorithm [13], and obtained optimal single-key differential trails for SIMON-like block ciphers.

On the other hand, Todo introduced the notion of *division property*, and used it in finding integral distinguishers for SIMON [18]; later on, Todo and Morii proposed a fine-grained variant called *bit-based division property* [19], and thus gave integral distinguisher for SIMON32 with one more round.

Besides, the method of Mixed-Integer Linear Programming (MILP) is widely used in automatic searching recently [15,17]. Specifically for SIMON, Sun *et al.* modified the original model [15,17] into an MIP (Mixed-Integer Programming) one by adding quadratic constraints [16], to remove invalid characteristics out of the feasible region. Although they made it theoretically solvable by adding auxiliary variants, it still seems rather sophisticated to make practical use of this model. It is worth noting that based on division property, Xiang *et al.* [21] applied MILP to *automatically* searching integral distinguishers for six lightweight block ciphers including SIMON and SIMECK.

Throughout, no cryptanalysis work has been done for SIMON-like block ciphers in related-key setting, and this issue is also mentioned by the designers of SIMON [5] and SIMECK [22] independently. In fact, the behavior of certain block cipher under related-key differential cryptanalysis is an important criterion for its security, since the secret keys are often updated in security protocols or differences can be incorporated using fault attacks. Meanwhile, avoiding high-probability related-key differential characteristics is one of the goal of the key schedule.

Our Contributions. In this paper, we make a fine-grained analysis of the ROTATION-AND operations and construct proper MILP models for SIMON-like block ciphers. As a result, we give related-key differential trails for SIMON-like block ciphers for the first time.

Specifically, we revisit the relationship between the input difference and the probability of differential trails, and reveal that *the active bits' positions* of the input difference will not only determine which bits of the output difference are likely to be active, but also affect the probability of differential characteristics.

From this we can get all possible output differences of the ROTATION-AND operation and their accurate probabilities *directly from input difference*, rather than using a DDTA (Difference Distribution Table of AND) accompanied with some checking conditions as done in [6,9,11]. As a result, we can construct proper MILP models with linear objective function while without quadratic constraints, and search related-key differential trails for SIMON and SIMECK automatically, as well as impossible differentials.

Our main results are listed in the following:

1. We find 10, 9, 9 rounds optimal related-key differential trails for SIMON32/64, SIMON48/96 and SIMON64/128 with probability 2^{-16}, 2^{-18} and 2^{-18} respectively, costing about 15 days, 6 days and 7 days respectively.[1] Moreover, we find that there is an 8-round period trail with probability 2^{-n} for SIMON2n/4n, and thus all trails can be extended to 19 rounds with probability 2^{-2n}.
2. We find two 11 rounds optimal related-key differential trails for SIMON48/72 and SIMON64/96 with probability 2^{-22} and 2^{-22} respectively, costing about 7 days and 7 days respectively. The extension for SIMON48 reaches 16 rounds with probability 2^{-50}, and the extension for SIMON64 reaches 18 rounds with probability 2^{-64}.
3. We find 15, 16, 16 rounds optimal related-key differential trails for SIMECK32/64, SIMECK48/96, and SIMECK64/128 with probability 2^{-34}, 2^{-40}, and 2^{-40} respectively, costing about 9.6 h, 3.8 days and 4 days respectively. The extension of SIMECK48/96 reaches 19 rounds with probability 2^{-48}, and the extension for SIMECK64/128 reaches 23 rounds with probability 2^{-66}.

For searching single-key differential trails, without of generality, we assume that there must exist certain round with input difference of Hamming weight one when considering the diffusion of block ciphers. Then by our method, we can recover the results in [11]. In addition, we also get 11, 12 and 13 rounds impossible differentials for SIMON32, SIMON48 and SIMON64 respectively, and get 11, 15 and 17 rounds impossible differentials for SIMECK32, SIMECK48 and SIMECK64 respectively, all in the single-key setting.

Organization of the Paper. We introduce notations and recall the constructions of SIMON-like block ciphers in Sect. 2. In Sect. 3, we present the main theorem on relationship between the input difference and the differential probability, and construct proper MILP models for SIMON-like block ciphers. Our results are presented in Sect. 4. Section 5 is a conclusion of this paper.

[1] All experiments are performed on a PC with 2.5 GHz Intel Core i7 and 16GB 1600 MHz DDR3.

2 Preliminaries

2.1 Notations

We say a bit is *active* if it is one. For the left half input difference in SIMON2n, each bit has a subscript denoting its position, with that of the most significant bit being 0; all subscripts are in the sense modulo n. We list main notations in Table 1.

Table 1. Notations.

Notation	Description
$\odot, \&$	AND operation
$\oplus$	XOR operation
S^i	left circular shift by i bits
S^{-i}	right circular shift by i bits
Δx_i^r	the i-th bit of left half input difference of the r-th round
Δd_i^r	the i-th bit of output difference of AND operation of the r-th round
(a, b, c)	the rotation parameters for SIMON-like block ciphers

2.2 A Brief Description of SIMON and SIMECK

The round function of SIMON-like block ciphers is shown in Fig. 1, with the value of (a, b, c) being (8, 1, 2) and (0, 5, 1) for SIMON and SIMECK respectively.

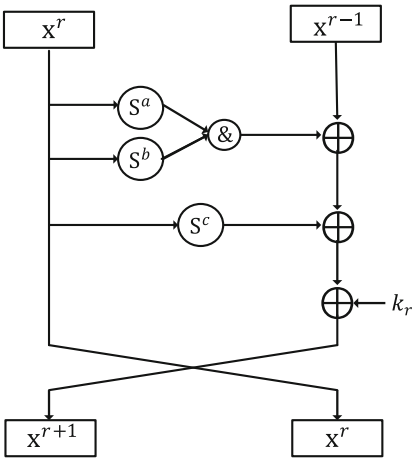

Fig. 1. The round function of SIMON-like block ciphers.

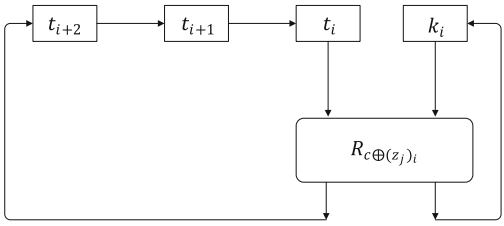

Fig. 2. The key expansion of SIMECK.

The key schedules of SIMON and SIMECK are totally different. The constant $C = 2^n - 4 = 0xff\cdots fc$, and the generation of constant sequence $\{z_j\}$ is referred to [4] (for SIMON) and [22] (for SIMECK). The key of the i-th round is denoted by k_i, and the identical permutation is denoted by I. For SIMON2n/mn, round keys are generated by

$$k_{i+m} = \begin{cases} C \oplus (z_j)_i \oplus k_i \oplus (I \oplus S^{-1})S^{-3}k_{i+1}, \; if \; m = 2, \\ C \oplus (z_j)_i \oplus k_i \oplus (I \oplus S^{-1})S^{-3}k_{i+2}, \; if \; m = 3, \\ C \oplus (z_j)_i \oplus k_i \oplus (I \oplus S^{-1})(S^{-3}k_{i+3} \oplus k_{i+1}), \; if \; m = 4. \end{cases}$$

For SIMECK2n/4n, the key schedules are shown in Fig. 2. The updating function is expressed as

$$\begin{cases} k_{i+1} = t_i, \\ t_{i+3} = k_i \oplus f(t_i) \oplus C \oplus (z_j)_i. \end{cases}$$

where $f(x) = x \odot S^5(x) \oplus S^1(x)$ is part of the round function.

3 Constructing MILP Models for SIMON-like Block Ciphers

In this section, we make a fine-grained analysis of the relationship between input and output difference of the ROTATION-AND operations. We prove that not only the Hamming weight but also the active bits' positions of the input difference can affect the probability of differential characteristics. The former has been proved by Liu *et al.* [11], and we highlight the latter's importance in constructing proper MILP models for SIMON-like block ciphers. Specifically, we give the following theorem:

Theorem 1. *Let $f(x) = S^a(x) \odot S^b(x)$ be a Boolean function from $\mathbb{F}_2^n$ to itself, and $gcd(n, a - b) = 1$. Let Δx, $\Delta d \in \mathbb{F}_2^n$ be the input and output difference of f respectively, with $wt(\Delta x) = m$, $m < n$, and $R = \{\Delta x_{i_0}, \Delta x_{i_1}, \ldots, \Delta x_{i_{m-1}}\}$ be the set of all active bits in Δx. If there exist*

1. *p_1 pairs of $\{i_j, i_k\}$ such that $|i_j - i_k| \equiv |a - b| \bmod n$; and*
2. *p_2 pairs of $\{i_j, i_k\}$ such that $|i_j - i_k| \equiv 2|a - b| \bmod n$ and there exists some h such that $|h - i_j| \equiv |a - b| \bmod n$, $|h - i_k| \equiv |a - b| \bmod n$, $\Delta x_h \notin R$;*

then there will be $2^{2m-p_1-p_2}$ possible values for Δd, and each has the same probability $2^{-2m+p_1+p_2}$.

To prove this theorem, we use the following lemma, which can be regarded as a generalization of Observation 2 in [8]. All proofs can be found in the Appendix.

Lemma 1. *Let $f(x) = S^a(x) \odot S^b(x)$ be a Boolean function from $\mathbb{F}_2^n$ to itself. Let Δx, $\Delta d \in \mathbb{F}_2^n$ be the input and output difference of f respectively, and $x \in \mathbb{F}_2^n$ be an input of f. Then,*

1. *In Δx, only two bits, namely Δx_{i+a} and Δx_{i+b} can affect the value of Δd_i, which is an arbitrary bit in Δd;*
2. *An arbitrary bit Δx_i in Δx, can affect only two bits Δd_{i-a} and Δd_{i-b} in Δd;*
3. *An arbitrary bit x_i in x can affect at most two bits Δd_{i-a} and Δd_{i-b} in Δd. Specifically, Δd_{i-a} is affected by x_i, iff. $\Delta x_{i-a+b} = 1$; Δd_{i-b} is affected by x_i, iff. $\Delta x_{i-b+a} = 1$.*

Based on Theorem 1, we can construct proper MILP models for SIMON-like block ciphers in the following.

Constraints Imposed by XOR Operations. There are lots of XOR operations in either round functions or key schedules of SIMON-like block ciphers. This turns out be a bottleneck in constructing efficient models if we follow the XOR constraints given in [15,17], since there will be too many auxiliary variants. However, we note that all possible points can be figured out easily and linear constraints without auxiliary variants can then be obtained using the SageMath code in [17]. We demonstrate this by the following example.

Let $x \oplus y \oplus z = w$, where x, y, z, $w \in \mathbb{F}_2$. All possible points for (x, y, z, w) are (0, 0, 0, 0), (0, 0, 1, 1), (0, 1, 0, 1), (0, 1, 1, 0), (1, 0, 0, 1), (1, 0, 1, 0), (1, 1, 0, 0) and (1, 1, 1, 1). We can easily get the linear constraints as follows:

$$\begin{cases} x + y - z + w \geq 0 \\ x + y + z - w \geq 0 \\ -x + y + z + w \geq 0 \\ x - y + z + w \geq 0 \\ -x - y + z - w \geq -2 \\ x - y - z - w \geq -2 \\ -x + y - z - w \geq -2 \\ -x - y - z + w \geq -2 \end{cases}$$

Constraints Imposed by ROTATION-AND Operations. Based on Theorem 1, we divide the n bits input difference and n bits output difference of ROTATION-AND operations into n groups. Specifically, group i ($0 \leq i \leq n-1$) consists of three input difference bits at positions $(i, i+t, i+2t)$ and two output difference bits at positions $(i-b, i+t-b)$, where $t = |a-b|$.

Taking SIMON32 as an example, we list all 16 groups in Table 2, and all possible points with respect to each group in Table 3. Then we can get the following linear constraints by running the SageMath code [17] on input of all possible points, where there is no auxiliary variants and the feasible region of which contains no invalid characteristics.

$$\begin{cases} \Delta x_{i+t}^r - \Delta x_{i+2t}^r - \Delta d_{i-b}^r + \Delta d_{i+t-b}^r \geq -1 \\ \Delta x_i^r + \Delta x_{i+t}^r - \Delta d_{i-b}^r \geq 0 \\ -\Delta x_i^r + \Delta x_{i+t}^r + \Delta d_{i-b}^r - \Delta d_{i+t-b}^r \geq -1 \\ \Delta x_{i+t}^r + \Delta x_{i+2t}^r - \Delta d_{i+t-b}^r \geq 0 \end{cases}$$

Table 2. The 16 groups for SIMON32.

Input Bits	0,7,14	7,14,5	14,5,12	5,12,3	12,3,10	3,10,1	10,1,8	1,8,15
Output Bits	15,6	6,13	13,4	4,11	11,2	2,9	9,0	0,7
Input Bits	8,15,6	15,6,13	6,13,4	13,4,11	4,11,2	11,2,9	2,9,0	9,0,7
Output Bits	7,14	14,5	5,12	12,3	3,10	10,1	1,8	8,15

Objective Functions. Let the probability of the differential characteristic be 2^{-w}. Then we have the following objective function from Theorem 1:

$$w = \sum_{r=0}^{R}(2\sum_{i=0}^{n-1}\Delta x_i^r - \sum_{i=0}^{n-1}\Delta x_i^r \Delta x_{i+t}^r - \sum_{i=0}^{n-1}\Delta x_i^r \Delta x_{i+2t}^r + \sum_{i=0}^{n-1}\Delta x_i^r \Delta x_{i+t}^r \Delta x_{i+2t}^r). \tag{1}$$

However, this objective function of degree three makes it hard to solve the model. To solve this issue, we form n groups with group i consisting of three bits input difference $(\Delta x_i^r, \Delta x_{i+t}^r, \Delta x_{i+2t}^r)$ as well as an auxiliary variants p_i^r, in order to reduce the degree of the objective function to one.

$$w = 2\sum_{r=0}^{R}\sum_{i=0}^{n-1}\Delta x_i^r - \sum_{r=0}^{R}\sum_{i=0}^{n-1} p_i^r. \tag{2}$$

Then we can obtain the following linear constraints, taking the relationships between $(\Delta x_i^r, \Delta x_{i+t}^r, \Delta x_{i+2t}^r)$ and p_i^r as shown in Table 4.

$$\begin{cases} \Delta x_{i+2t}^r - p_i^r \geq 0 \\ -\Delta x_i^r - \Delta x_{i+2t}^r + p_i^r \geq -1 \\ -\Delta x_{i+t}^r - \Delta x_{i+2t}^r + p_i^r \geq -1 \\ \Delta x_i^r + \Delta x_{i+t}^r - p_i^r \geq 0 \end{cases}$$

Since the non-linear key schedules of SIMECK essentially reuse its round function, the objective function of SIMECK turns out to

$$w = 2\sum_{r=0}^{R}\sum_{i=0}^{n-1}\Delta x_i^r - \sum_{r=0}^{R}\sum_{i=0}^{n-1} p_i^r + 2\sum_{r=1}^{R-3}\sum_{i=0}^{n-1}\Delta k_i^r - \sum_{r=1}^{R-3}\sum_{i=0}^{n-1} p_{ki}^r. \tag{3}$$

4 (Related-Key) Differential Trails for SIMON and SIMECK

In this section, we show the (related-key) differential trails for SIMON and SIMECK, which are automatically searched by solving the MILP models in Sect. 3 using Gurobi. Our results are twofold: first and foremost, we give (long) related-key differential trails for SIMON-like block ciphers for the first time; second, using the same method, we give impossible differentials for SIMON-like block ciphers and recover the trails given by Liu *et al.* [11], both in the single-key setting.

Table 3. All possible points for each group.

$(\Delta x_i^r, \Delta x_{i+t}^r, \Delta x_{i+2t}^r)$	$(\Delta d_{i-b}^r, \Delta d_{i+t-b}^r)$
(0, 0, 0)	(0, 0)
(0, 0, 1)	(0, 0), (0,1)
(0, 1, 0)	(0, 0), (0,1), (1,0), (1,1)
(0, 1, 1)	(0, 0), (0,1), (1,0), (1,1)
(1, 0, 0)	(0, 0), (1,0)
(1, 0, 1)	(0, 0), (1,1)
(1, 1, 0)	(0, 0), (0,1), (1,0), (1,1)
(1, 1, 1)	(0, 0), (0,1), (1,0), (1,1)

Table 4. The value of auxiliary variant p_i^r.

$(\Delta x_i^r, \Delta x_{i+t}^r, \Delta x_{i+2t}^r)$	p_i^r
(0, 0, 0)	0
(0, 0, 1)	0
(0, 1, 0)	0
(0, 1, 1)	1
(1, 0, 0)	0
(1, 0, 1)	1
(1, 1, 0)	0
(1, 1, 1)	1

4.1 Related-Key Differential Trails

We present optimal related-key differential trails for SIMON32/64 in Table 6, SIMON48/72 and SIMON48/96 in Table 7, SIMECK32/64 and SIMECK48/96 in Table 8. The optimal trails for SIMON64 and SIMECK64 are identical to those for SIMON48 and SIMECK48 respectively.

Except for SIMECK32/64, constrained by the limited computational resources, it is still difficult to obtain longer optimal related-key differential trails for other parameters, whose probabilities may hopefully reach the security margin. To solve this issue, putting some optimal trail in the middle, we search both forwards and backwards until it reaches the security margin. In addition, we observe that there exists an 8-round period for SIMON32/64 in the related-key setting, which yields a 19-round related-key differential trail with probability 2^{-32}. These results are summarized in Table 5.

4.2 Single-Key Differential Trails

For obtaining single-key trails, it indeed costs more time by *directly* solving the MILP models in Sect. 3 than using the method in [11]. However, a key observation is that in optimal single-key differential trails, there is always some round's input difference with Hamming weight one. This can explained from the following two perspectives: on the one hand, the upper-bound of probability of each round is negatively related to the Hamming weight of its input difference, as proved in [11]; on the other hand, considering the diffusion property, an active input difference bit of some round can make many forward and backward bits active; thus, it is intuitive to require the hamming weight of some round's input difference to be the least (namely one), for obtaining long trails.

Keeping these in mind, we can recover the results in [11] (R-round optimal single-key differential trails) using much less time, by solving the MILP models with the precondition that there exists some $r \in \{0, \cdots, R-1\}$ such that the Hamming weight of the r-th round's input difference is one.

Table 5. The probabilities of optimal and best related-key differential trails for variants of SIMON and SIMECK. To distinguish from optimal trails, best trails are labeled with *. For simplicity, all probabilities p are given as $(-\log_2 p)$ in the table.

Rounds	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
SIMON32/64	0	2	4	8	11	16	16*	24*	24*	24*	24*	32*	32*	32*	32*	-	-	-	-
SIMON48/72	2	4	6	12	14	18	22	30*	33*	40*	42*	50*	-	-	-	-	-	-	-
SIMON48/96	0	2	4	8	12	18	24*	35*	36*	36*	36*	48*	48*	48*	48*	-	-	-	-
SIMON64/96	2	4	6	12	14	18	22	30*	34*	42*	46*	54*	55*	64*	70*	-	-	-	-
SIMON64/128	0	2	4	8	12	18	26*	36*	41*	48*	48*	64*	64*	64*	64*	-	-	-	-
SIMECK32/64	0	2	4	8	10	14	18	22	26	30	34	-	-	-	-	-	-	-	-
SIMECK48/96	0	2	4	8	10	14	18	22	26	30	34	40	42*	46*	48*	-	-	-	-
SIMECK64/128	0	2	4	8	10	14	18	22	26	30	34	40	42*	46*	48*	54*	56*	62*	66*

4.3 Impossible Differentials

Considering the *miss-in-the-middle* approach and the diffusion property, we search impossible differentials for SIMON-like block ciphers in single-key setting, under that there is only one active bit in either the input difference or the

Table 6. 10 rounds optimal related-key differential trails for SIMON32/64, where the numbers represent the positions of active bits of input difference of each round while '-' represents that there is no active bits.

R	SIMON32/64		
	Δx^l	Δx^r	Δk
0	-	1,3,5,7,9,11,13,15	1,3,5,7,9,11,13,15
1	-	-	-
2	-	-	0,2,4,6,8,10,12,14
3	0,2,4,6,8,10,12,14	-	1,3,5,7,9,11,13,15
4	-	0,2,4,6,8,10,12,14	0,2,4,6,8,10,12,14
5	-	-	-
6	-	-	1,3,5,7,9,11,13,15
7	1,3,5,7,9,11,13,15	-	1,3,5,7,9,11,13,15
8	-	1,3,5,7,9,11,13,15	1,3,5,7,9,11,13,15
9	-	-	-
10	-	-	0,2,4,6,8,10,12,14
11	0,2,4,6,8,10,12,14	-	1,3,5,7,9,11,13,15

Table 7. Optimal related-key differential trails for SIMON48.

R	SIMON48/72			SIMON48/96		
	Δx^l	Δx^r	Δk	Δx^l	Δx^r	Δk
0	-	7,8,9,10,22	4,6,7,8,9,10,22	-	9,11,12,13,16,17,19	9,11,12,13,16,17,19
1	4,6	-	2,4,22	-	-	11,12,14,15
2	22	4,6	1,2,4,6,20	11,12,14,15	-	9,12,14
3	1,2	22	0,22,23	11	11,12,14,15	9,10,14,15
4	-	1,2	1,2,22	11,12	11	9
5	22	-	20	11	11,12	9,10,11,12
6	-	22	22	-	11	11
7	-	-	22	-	-	-
8	22	-	1,2,20	-	-	13
9	1,2	22	0,4,6,22,23	13	-	9,10,16,17
10	4,6	1,2	1,4,7,8,9,10,22	9,10,11,16,17	-	
11	7,8,9,10,22	4,6				

output difference. Then if the MILP models are infeasible under this condition, we get impossible differentials.

Taking the rotational invariance property of SIMON-like block ciphers [20], for each variant of SIMON2n and SIMECK2n, an impossible differential additionally yields $(n-1)$ impossible differentials by rotation. Our main results are listed in Table 9.

Table 8. Optimal related-key differential trails for SIMECK32 and SIMECK48.

R	SIMECK32/64			SIMECK48/96		
	Δx^l	Δx^r	Δk	Δx^l	Δx^r	Δk
0	-	4,8,9,10	4,8,9	-	18	18
1	10	-	9	-	-	-
2	-	10	10	-	-	20
3	-	-	-	20	-	-
4	-	-	-	19	20	18
5	-	-	-	20	19	19
6	-	-	10	19	20	20
7	10	-	-	18,19	19	17
8	9	10	-	-	18,19	-
9	4,8,9,10	9	9	18,19	-	-
10	5,7	4,8,9,10	10	17,19	18,19	16,20
11	6,8,9	5,7	-	20	17,19	17
12	-	6,8,9	8,9	-	20	-
13	6	-	5	20	-	19
14	-	6	10	-	20	20
15	6,10	-		-	-	17
16				17	-	

Table 9. Impossible differentials for SIMON and SIMECK in single-key.

	ROUNDS	Trails
SIMON32	11	(0,4000)$\nrightarrow$(80,0); (0,4000)$\nrightarrow$(20,0)
SIMON48	12	(0,400000)$\nrightarrow$(800000,0); (0,400000)$\nrightarrow$(200000,0)
SIMON64	13	(0,40000000)$\nrightarrow$(8000000,0); (0,40000000)$\nrightarrow$(800000,0); (0,40000000)$\nrightarrow$(200000,0); (0,40000000)$\nrightarrow$(80,0); (0,40000000)$\nrightarrow$(20,0); (0,40000000)$\nrightarrow$(2,0)
SIMECK32	11	(0,4000)$\nrightarrow$(200,0); (0,4000)$\nrightarrow$(8,0)
SIMECK48	15	(0,400000)$\nrightarrow$(800000,0); (0,400000)$\nrightarrow$(200000,0); (0,400000)$\nrightarrow$(20000,0); (0,400000)$\nrightarrow$(8,0)
SIMECK64	17	(0,40000000)$\nrightarrow$(8000000,0); (0,40000000)$\nrightarrow$(2,0)

5 Summary

In this paper, we mainly studied the security of SIMON-like block ciphers in the related-key setting, by a fine-grained analysis of the ROTATION-AND operations. We hope our work helpful in designing key schedules for SIMON-like block ciphers. For future works, it is desirable to obtain longer optimal differ-

ential trails in related-key setting, maybe by combining our work with other automatic searching algorithm, e.g., SAT/SMT solver.

Acknowledgement. The authors thank the anonymous reviewers of ISC2018 for useful comments. This work was supported by the NSFC under grant #61379139.

A Proof of Lemma 1

Proof. Let x and $(x \oplus \Delta x)$ be two inputs of the function f. We have

$$\begin{aligned} \Delta d &= f(x) \oplus f(x \oplus \Delta x) \\ &= (S^a(x) \odot S^b(x)) \oplus (S^a(x \oplus \Delta x) \odot S^b(x \oplus \Delta x)) \\ &= S^a(x) \odot S^b(\Delta x) \oplus S^a(\Delta x) \odot S^b(x) \oplus S^a(\Delta x) \odot S^b(\Delta x) \end{aligned} \tag{4}$$

Then for any bit Δd_i in Δd $(i = 0, \cdots, n-1)$, we have

$$\Delta d_i = x_{i+a} \odot \Delta x_{i+b} \oplus \Delta x_{i+a} \odot x_{i+b} \oplus \Delta x_{i+a} \odot \Delta x_{i+b} \tag{5}$$

Obviously, only two bits in Δx, namely Δx_{i+a} and Δx_{i+b} can affect the value of Δd_i.

Fix an arbitrary i, assume that Δd_k is affected by Δx_i. First, we have

$$\Delta d_k = x_{k+a} \odot \Delta x_{k+b} \oplus \Delta x_{k+a} \odot x_{k+b} \oplus \Delta x_{k+a} \odot \Delta x_{k+b}, \tag{6}$$

from Eq. (5). If Δd_k is affected by Δx_i, then we have

$$i \equiv k + a \mod n \tag{7}$$

or

$$i \equiv k + b \mod n \tag{8}$$

Put it in another form, we have

$$k \equiv i - a \mod n \tag{9}$$

or

$$k \equiv i - b \mod n \tag{10}$$

So proved that an arbitrary bit Δx_i can affect only two bits Δd_{i-a} and Δd_{i-b}.

From Eq. (5), we have that

(1) if $\Delta x_{i+a} = 0, \Delta x_{i+b} = 0$, then $\Delta d_i = 0$;
(2) if $\Delta x_{i+a} = 1, \Delta x_{i+b} = 1$, then $\Delta d_i = (x_{i+a} \oplus x_{i+b}) \odot 1 \oplus 1$;
(3) if $\Delta x_{i+a} = 1$, $\Delta x_{i+b} = 0$, then $\Delta d_i = \Delta x_{i+a} \odot x_{i+b} = x_{i+b}$;
(4) if $\Delta x_{i+a} = 0$, $\Delta x_{i+b} = 1$, then $\Delta d_i = x_{i+a} \odot \Delta x_{i+b} = x_{i+a}$.

Let x_i denote an arbitrary bit in x. Δd_k is affected by x_i, iff. $k \equiv i-a \mod n$ and $\Delta x_{k+b} = \Delta x_{i-a+b} = 1$, or $k \equiv i - b \mod n$ and $\Delta x_{k+a} = \Delta x_{i-b+a} = 1$. □

B Proof of Theorem 1

Proof. Let R_d be the collection of bits in Δd which are affected by bits in R. From Lemma 1,

$$R_d = \{\Delta d_{i_0-a}, \Delta d_{i_0-b}, \Delta d_{i_1-a}, \Delta d_{i_1-b}, \ldots, \Delta d_{i_{m-1}-a}, \Delta d_{i_{m-1}-b}\}$$

There may be duplicate elements in the collection R_d.

1. Since $a \neq b$, then $i_\ell - a \not\equiv i_\ell - b \mod n$, for $\ell = 0, \cdots, m-1$;
2. For $0 \leq j \neq k \leq m-1$, $i_j - a \not\equiv i_k - a \mod n$, since $i_j \neq i_k$;
3. For $0 \leq j \neq k \leq m-1$, if $i_j - a \equiv i_k - b \mod n$, then $i_j - i_k \equiv a - b \mod n$;
4. For $0 \leq j \neq k \leq m-1$, if $i_j - b \equiv i_k - a \mod n$, then $i_j - i_k \equiv b - a \mod n$;

If there exist p_1 pairs of $\{i_j, i_k\}$ such that $|i_j - i_k| \equiv |a - b| \mod n$, we have

$$i_j - i_k \equiv a - b \mod n \tag{11}$$

or

$$i_j - i_k \equiv b - a \mod n \tag{12}$$

we claim that Eqs. (11) and (12) cannot hold true simultaneously, otherwise it contradicts with $gcd(n, a-b) = 1$. Let R'_d denote the set obtained by removing duplicate elements from the collection R_d. Then if there exist p_1 pairs of $\{i_j, i_k\}$ such that $|i_j - i_k| \equiv |a - b| \mod n$, $|R_d| - |R'_d| = p_1$.

Now we turn to discuss the relationships amongst bits in Δd. First, for $\Delta d_k \notin R'_d$, we have $\Delta x_{k+a} = 0$ and $\Delta x_{k+b} = 0$ from Lemma 1; specifically, $\Delta d_k = 0$ holds with probability 1, regardless of the values of x_{k+a} and x_{k+b}. Thus, we need only to discuss the relationships amongst bits in R'_d. For $\Delta d_k \in R'_d$, it has been proved by Lemma 1 that at least one of Δx_{k+a} and Δx_{k+b} is active. Specifically,

1. $\Delta x_{k+a} = 1$, $\Delta x_{k+b} = 0$. In this case, $\Delta d_k = x_{k+b}$. If there exists some other bit $\Delta d'_k \in R'_d$ such that $\Delta d'_k$ is dependent of Δd_k, then $k' \equiv k + b - a \mod n$, since Δd_{k+b-a} is the only bit which *may be* affected by x_{k+b} except for Δd_k from Lemma 1.

$$\begin{aligned} \Delta d_{k+b-a} = &\Delta x_{k+b} \odot x_{k+2b-a} \oplus x_{k+b} \odot \Delta x_{k+2b-a} \\ &\oplus \Delta x_{k+b} \odot \Delta x_{k+2b-a} \end{aligned} \tag{13}$$

   If $\Delta x_{k+2b-a} \in R$, then $\Delta d_{k+b-a} = x_{k+b} = \Delta d_k$; otherwise, $\Delta d_{k+b-a} = 0$ holds with probability 1 (independent of Δd_k).
2. $\Delta x_{k+a} = 0$, $\Delta x_{k+b} = 1$. In this case, $\Delta d_k = x_{k+a}$. If there exists some other bit $\Delta d'_k \in R'_d$ such that $\Delta d'_k$ is dependent of Δd_k, then $k' \equiv k + a - b \mod n$, since Δd_{k+a-b} is the only bit which *may be* affected by x_{k+a} except for Δd_k from Lemma 1.

$$\begin{aligned} \Delta d_{k+a-b} = &\Delta x_{k+a} \odot x_{k+2a-b} \oplus x_{k+a} \odot \Delta x_{k+2a-b} \\ &\oplus \Delta x_{k+a} \odot \Delta x_{k+2a-b} \end{aligned} \tag{14}$$

   If $\Delta x_{k+2a-b} \in R$, then $\Delta d_{k+a-b} = x_{k+a} = \Delta d_k$; otherwise, $\Delta d_{k+a-b} = 0$ holds with probability 1 (independent of Δd_k).

3. $\Delta x_{k+a} = 1$, $\Delta x_{k+b} = 1$. In this case, $\Delta d_k = (x_{k+a} \oplus x_{k+b}) \odot 1 \oplus 1$. From Lemma 1, the only other bit which may be affected by x_{k+a} is Δd_{k+a-b}. Specifically, the following equation holds if $\Delta x_{k+2a-b} \in R$.

$$\Delta d_{k+a-b} = (x_{k+2a-b} \oplus x_{k+a}) \odot 1 \oplus 1 \tag{15}$$

From Lemma 1, the only other bit which may be affected by x_{k+b} is Δd_{k+b-a}. Specifically, the following equation holds if $\Delta x_{k+2b-a} \in R$.

$$\Delta d_{k+b-a} = (x_{k+b} \oplus x_{k+2b-a}) \odot 1 \oplus 1 \tag{16}$$

It is obvious that Δd_k can be dependent of other bit(s) in R'_d, only in the case that $\Delta x_{k+2a-b}, \Delta x_{k+2b-a} \in R$. However, since Δd_{k+b-a} and Δd_{k+a-b} introduce the new bits (variants) of x_{k+2a-b} and x_{k+2b-a} respectively, we should involve more elements in R'_d to reduce the effects of x_{k+2a-b} and x_{k+2b-a}. Again from Lemma 1, the only other bit affected by x_{k+2a-b} (x_{k+2b-a}) is $\Delta d_{k+2a-2b} = (x_{k+3a-2b} \oplus x_{k+2a-b}) \odot 1 \oplus 1$ ($\Delta d_{k+2b-2a} = (x_{k+2b-a} \oplus x_{k+3b-2a}) \odot 1 \oplus 1$) on condition that $\Delta x_{k+3a-2b} \in R$ ($\Delta x_{k+3b-2a} \in R$).
Thus, in order to eliminate the effects of x_{k+2a-b} and x_{k+2b-a}, the *only* choice (from Lemma 1) is involving the new bits of $\Delta d_{k+2a-2b}$ and $\Delta d_{k+2b-2a}$, which can indeed eliminate x_{k+2a-b} and x_{k+2b-a} however introduce two new variants of $x_{k+3a-2b}$ and $x_{k+3b-2a}$. Under the condition $gcd(n, a-b) = 1$, this *eliminating-while-introducing* process will succeed iff. $|R| = n$, and the probability of each possible value of Δd is $2^{-(n-1)}$ which coincides with the result in [11]. On the other hand, $\Delta d_k = (x_{k+a} \oplus x_{k+b}) \odot 1 \oplus 1$ is independent of other bits in R'_d when $|R| < n$.

□

For a better understanding, we give an example with (n, a, b)=(8, 0, 3) as shown in Fig. 3. Assume that $\Delta x_0 = 1$, $\Delta x_3 = 1$. Only in the case where all input difference bits are active, can Δd_0 be dependent of other bits in Δd, namely $\Delta d_0 = \Delta d_1 \oplus \cdots \oplus \Delta d_7$.

1. $\Delta d_0 = (x_0 \oplus x_3) \odot 1 \oplus 1$
2. $\Delta d_5 = (x_0 \oplus x_5) \odot 1 \oplus 1$, when $\Delta x_5 = 1$; $\Delta d_3 = (x_6 \oplus x_3) \odot 1 \oplus 1$, when $\Delta x_6 = 1$
3. $\Delta d_2 = (x_2 \oplus x_5) \odot 1 \oplus 1$, when $\Delta x_2 = 1$; $\Delta d_6 = (x_6 \oplus x_1) \odot 1 \oplus 1$, when $\Delta x_1 = 1$
4. $\Delta d_7 = (x_2 \oplus x_7) \odot 1 \oplus 1$, when $\Delta x_7 = 1$; $\Delta d_1 = (x_1 \oplus x_4) \odot 1 \oplus 1$, when $\Delta x_4 = 1$
5. $\Delta d_4 = (x_4 \oplus x_7) \odot 1 \oplus 1$

Essentially, given $gcd(n, a-b) = 1$, there is only one cycle ($\begin{pmatrix} 3\,6\,1\,4\,7\,2\,5\,0 \\ 6\,1\,4\,7\,2\,5\,0\,3 \end{pmatrix}$ in this example). More generally, when $gcd(n, a-b) = t$, there will be t cycles, and this in some way explains the rationalities of such requirement $gcd(n, a-b) = 1$.

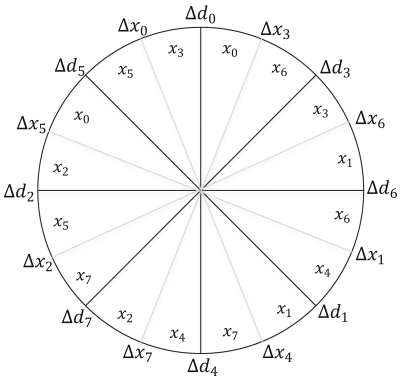

Fig. 3. The affected relationship between input and output difference bits of ROTATION-AND.

References

1. Abdelraheem, M.A., Alizadeh, J., Alkhzaimi, H.A., Aref, M.R., Bagheri, N., Gauravaram, P.: Improved linear cryptanalysis of reduced-round SIMON-32 and SIMON-48. In: Biryukov, A., Goyal, V. (eds.) INDOCRYPT 2015. LNCS, vol. 9462, pp. 153–179. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-26617-6_9
2. Abed, F., List, E., Lucks, S., Wenzel, J.: Differential cryptanalysis of round-reduced Simon and Speck. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 525–545. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46706-0_27
3. Alkhzaimi, H.A., Lauridsen, M.M.: Cryptanalysis of the SIMON Family of Block Ciphers. Cryptology ePrint Archive, Report 2013/543 (2013). https://eprint.iacr.org/2013/543
4. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The Simon and Speck Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404 (2013). https://eprint.iacr.org/2013/404
5. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: Notes on the design and analysis of SIMON and SPECK. Cryptology ePrint Archive, Report 2017/560 (2017). https://eprint.iacr.org/2017/560
6. Biryukov, A., Roy, A., Velichkov, V.: Differential analysis of block ciphers SIMON and SPECK. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 546–570. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46706-0_28
7. Biryukov, A., Velichkov, V.: Automatic search for differential trails in ARX ciphers. In: Benaloh, J. (ed.) CT-RSA 2014. LNCS, vol. 8366, pp. 227–250. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-04852-9_12
8. Chen, Z., Wang, N., Wang, X.: Impossible Differential Cryptanalysis of Reduced Round SIMON. Cryptology ePrint Archive, Report 2015/286 (2015). https://eprint.iacr.org/2015/286
9. Kölbl, S., Leander, G., Tiessen, T.: Observations on the SIMON block cipher family. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 161–185. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_8

10. Kondo, K., Sasaki, Y., Iwata, T.: On the design rationale of Simon block cipher: integral attacks and impossible differential attacks against Simon variants. In: Manulis, M., Sadeghi, A.-R., Schneider, S. (eds.) ACNS 2016. LNCS, vol. 9696, pp. 518–536. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39555-5_28
11. Liu, Z., Li, Y., Wang, M.: Optimal differential trails in SIMON-like ciphers. IACR Trans. Symmetric Cryptol. **2017**, 358–379 (2017). https://doi.org/10.13154/tosc.v2017.i1.358-379
12. Liu, Z., Li, Y., Wang, M.: The Security of SIMON-like Ciphers Against Linear Cryptanalysis. Cryptology ePrint Archive, Report 2017/576 (2017). https://eprint.iacr.org/2017/576
13. Matsui, M.: On correlation between the order of S-boxes and the strength of DES. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 366–375. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0053451
14. Shi, D., Hu, L., Sun, S., Song, L., Qiao, K., Ma, X.: Improved linear (hull) cryptanalysis of round-reduced versions of SIMON. **60**, 39101, May 2016.https://doi.org/10.1007/s11432-015-0007-1
15. Sun, S., et al.: Towards Finding the Best Characteristics of Some Bit-oriented Block Ciphers and Automatic Enumeration of (Related-key) Differential and Linear Characteristics with Predefined Properties. Cryptology ePrint Archive, Report 2014/747 (2014). https://eprint.iacr.org/2014/747
16. Sun, S., et al.: Constructing Mixed-integer Programming Models whose Feasible Region is Exactly the Set of All Valid Differential Characteristics of SIMON (2015). https://eprint.iacr.org/2015/122
17. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 158–178. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_9
18. Todo, Y.: Division property: efficient method to estimate upper bound of algebraic degree. In: Phan, R.C.-W., Yung, M. (eds.) Mycrypt 2016. LNCS, vol. 10311, pp. 553–571. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-61273-7_30
19. Todo, Y., Morii, M.: Bit-based division property and application to Simon family. In: Peyrin, T. (ed.) FSE 2016. LNCS, vol. 9783, pp. 357–377. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-52993-5_18
20. Wang, Q., Liu, Z., Varıcı, K., Sasaki, Y., Rijmen, V., Todo, Y.: Cryptanalysis of reduced-round SIMON32 and SIMON48. In: Meier, W., Mukhopadhyay, D. (eds.) INDOCRYPT 2014. LNCS, vol. 8885, pp. 143–160. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-13039-2_9
21. Xiang, Z., Zhang, W., Bao, Z., Lin, D.: Applying MILP method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 648–678. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_24
22. Yang, G., Zhu, B., Suder, V., Aagaard, M.D., Gong, G.: The Simeck family of lightweight block ciphers. In: Güneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 307–329. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48324-4_16