On the Design Rationale of SIMON Block Cipher: Integral Attacks and Impossible Differential Attacks against SIMON Variants

Kota Kondo[1], Yu Sasaki[2], and Tetsu Iwata[1(✉)]

[1] Nagoya University, Nagoya, Japan
k_kondo@echo.nuee.nagoya-u.ac.jp, iwata@cse.nagoya-u.ac.jp
[2] NTT Secure Platform Laboratories, Tokyo, Japan
sasaki.yu@lab.ntt.co.jp

Abstract. SIMON is a lightweight block cipher designed by NSA in 2013. NSA presented the specification and the implementation efficiency, but they did not provide detailed security analysis nor the design rationale. The original SIMON has rotation constants of $(1, 8, 2)$, and Kölbl *et al.* regarded the constants as a parameter (a, b, c), and analyzed the security of SIMON block cipher variants against differential and linear attacks for all the choices of (a, b, c). This paper complements the result of Kölbl *et al.* by considering integral and impossible differential attacks. First, we search the number of rounds of integral distinguishers by using a supercomputer. Our search algorithm follows the previous approach by Wang *et al.*, however, we introduce a new choice of the set of plaintexts satisfying the integral property. We show that the new choice indeed extends the number of rounds for several parameters. We also search the number of rounds of impossible differential characteristics based on the miss-in-the-middle approach. Finally, we make a comparison of all parameters from our results and the observations by Kölbl *et al.* Interesting observations are obtained, for instance we find that the optimal parameters with respect to the resistance against differential attacks are not stronger than the original parameter with respect to integral and impossible differential attacks. We also obtain a parameter that is better than the original parameter with respect to security against these four attacks.

Keywords: SIMON · Lightweight block cipher · Integral attack · Impossible differential attack · Design rationale · Rotation constant

1 Introduction

Lightweight cryptography has been discussed actively to provide secure communication for various communication devices with constraint resources, such as RFID tags and sensor network. In fact, quite a few lightweight ciphers, hash functions, message authentication codes (MACs) etc. have been designed recently.

© Springer International Publishing Switzerland 2016
M. Manulis et al. (Eds.): ACNS 2016, LNCS 9696, pp. 518–536, 2016.
DOI: 10.1007/978-3-319-39555-5_28

Among a large variety of lightweight block ciphers, Simon and Speck [6], which were designed by NSA in 2013, achieve overwhelming performance and thus attract a lot of attention. Meanwhile, the designers of Simon and Speck do not provide any security discussion and design rationale. Thus it is necessary to carry out security analysis and to study design rationale so that the community can have more confidence on those designs.

Yang *et al.* investigated a performance aspect of Simon, and proposed another block cipher Simeck which optimizes the performance of Simon by slightly modifying its round function and key schedule [27]. As a drawback, security of Simeck is known to be weaker than Simon, thus evaluating security of Simeck is also important.

In general, security of block ciphers is evaluated by deriving lowerbounds and upperbounds of the cipher's security against particular cryptanalysis. Here, lowerbounds are derived by applying cryptanalysis. Regarding Simon, a large number of attacks have been applied since its proposal including differential cryptanalysis [2,8,17,22,23,25], linear cryptanalysis [1,4,5,10,11,20,22], algebraic analysis [3,19], integral attack [24,26], impossible differential attack [9,12,26], zero-correlation attack [26], known-key attack [13] and so on.

Design rationale of block cipher is often provided by the designers. If it is not the case, there still exists an approach for the third party to study the design rationale. For example, an evaluator parameterizes some part of the target cipher, e.g. rotation constants, and evaluates the security for all parameter choices. If the original parameter shows the highest security, it can be said that the original parameters have been chosen in good rationale. For example, Pramstaller *et al.* evaluated the design rationale of SHA-1 by evaluating all the rotation constants [18]. Regarding Simon, Kölbl *et al.* regarded three rotation constants $(1, 8, 2)$ of Simon as a parameter (a, b, c), and evaluated security of Simon variants denoted by $\text{Simon}_{a,b,c}$ against differential and linear cryptanalysis for all choices of (a, b, c) [16]. As a result, it turned out that the original rotation constants in Simon are not one of the strongest. Kölbl *et al.* concluded that considering only differential and linear cryptanalysis is not sufficient to explain the design rationale, and further security evaluation with other cryptanalysis approach were left open.

Our Contributions. In this paper, we study design rationale of Simon32; a member of the Simon family whose block size is 32 bits. We extend the analysis by Kölbl *et al.* [16] to integral attack and impossible differential attack. Namely, we apply those attacks to $\text{Simon}_{a,b,c}$ for all the choices of rotation constants (a, b, c).

Regarding integral attacks on Simon, Wang *et al.* experimentally evaluated the number of rounds covered by integral distinguishers [26]. In more details, Wang *et al.* choose 2^{31} plaintexts and encrypt them with several keys to check if the sum of the corresponding internal states after some rounds is always zero in some bits. In this paper, we use the same approach to evaluate all the choices of rotation constants. Here, the difficulty is expensive computational cost of

this experiment. To overcome this problem, we introduce equivalence classes for rotation constants and sets of 2^{31} plaintexts, which make the experiment feasible for a supercomputer. Moreover, we point out that the method of choosing 2^{31} plaintexts by Wang *et al.* [26] does not cover all the cases, thus may miss an optimal attack. In this paper, we enlarge the search space so that wider classes of 2^{31} plaintext sets are examined. The obtained results contain many interesting features. Several parameters can be distinguished even after 32 rounds, which is the default number of rounds for SIMON32. We show that original rotation constants in SIMON have reasonably good resistance against the integral attack, while several other choices have stronger resistance.

Regarding impossible differential attacks, we derive the number of rounds for impossible differential characteristics with the miss-in-the-middle approach. Many round constant choices lead to impossible differential characteristics of length between 9 rounds to 17 rounds, while the original SIMON parameter allows 11-round distinguishers.

At the last part of this paper, we compare strength of rotation constants by considering integral attacks and impossible differential attacks from our paper and differential cryptanalysis and linear cryptanalysis by Kölbl *et al.* [16]. We classify strength of each parameter with respect to the number of rounds covered by distinguishers. This identifies several interesting properties, for example, any rotation constant having better resistance against integral and impossible differential attacks than original SIMON is not as strong as original SIMON with respect to differential and linear cryptanalysis. It turns out that original rotation constants in SIMON are fairly well by taking into account four kinds of cryptanalysis, yet we find that rotation constant $(5, 12, 3)$ is better than original SIMON, and thus interesting to investigate more details in future.

Paper Outline. The rest of this paper is organized as follows. We describe notations used in this paper, specification of SIMON and basic concepts of integral and impossible differential attacks in Sect. 2. Integral attacks on $\text{SIMON}_{a,b,c}$ are shown in Sect. 3. Impossible differential attacks on $\text{SIMON}_{a,b,c}$ are shown in Sect. 4. We then compare strength of parameters to study the design rationale of SIMON in Sect. 5. Finally, we conclude this paper in Sect. 6.

2 Preliminaries

2.1 Notation

The set $\{0, 1, \ldots, n-1\}$ is written as Z_n, and the set $\{n' \mid 1 \leq n' \leq n, \gcd(n', n) = 1\}$ is written as Z_n^*. The d-bit circular rotation of a bit string x to the left is written as $S^d(x)$.

2.2 Specification of SIMON

SIMON is a lightweight block cipher suitable for hardware implementation that was designed by NSA in 2013 [6]. The SIMON block cipher with a $2n$-bit block is

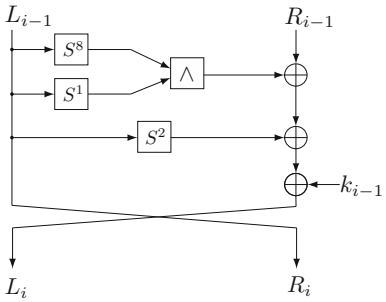

Fig. 1. The $(i-1)$-st round function of Simon

denoted Simon$2n$, where $n \in \{16, 24, 32, 48, 64\}$. Simon$2n$ with an m-word key (mn bits) is denoted Simon$2n/mn$. In this paper, we are only concerned with the case $n = 16$ and $m = 4$.

The round function of Simon is composed of three operations: AND ($\wedge$), rotation (S) and XOR ($\oplus$). Let v denote the n-bit input word of the round function F, where F is defined as

$$F(v) = (S^1(v) \wedge S^8(v)) \oplus S^2(v).$$

Let (L_{i-1}, R_{i-1}) denote the $2n$-bit input state of the $(i-1)$-st round, which is encrypted into (L_i, R_i) as:

$$L_i = F(L_{i-1}) \oplus R_{i-1} \oplus k_{i-1},$$
$$R_i = L_{i-1},$$

where k_{i-1} is the subkey of the $(i-1)$-st round. The plaintext is (L_0, R_0), and if the number of rounds is r, then (L_r, R_r) is the ciphertext. We note that the index of the round starts with 0 and the last round is the $(r-1)$-st round. Figure 1 shows the round function of Simon. The key schedule is irrelevant in our analysis and we omit the details, which can be found in [6].

2.3 Simon Block Cipher Variants

In [16], Kölbl *et al.* introduced Simon block cipher variants by regarding the three rotation constants $(1, 8, 2)$ of Simon as a parameter (a, b, c). Then they proved a structural equivalence among the round functions with different parameters. Furthermore, they showed the detailed security analysis of Simon block cipher variants against differential attacks for a large set of parameters.

The round function of Simon block cipher variants is defined as:

$$F_{a,b,c}(v) = (S^a(v) \wedge S^b(v)) \oplus S^c(v),$$

where $a, b, c \in Z_n$. We exclude the case $a = b$ since the encryption algorithm becomes a linear transformation. We also assume that $a < b$ from the symmetry

of AND operation. The size of parameter space is $\binom{16}{2} \times 16 = 1920$, where $\binom{16}{2}$ is the number of combinations of a and b, and 16 is the number of choices of c.

The structural equivalence is formalized as follows.

Proposition 1 ([16]). *Let T be a permutation of the bits of an n-bit word that corresponds to an affine transformation of the bit-indices. Thus there are $s \in Z_n$ and $t \in Z_n$ such that bit i is translated to $s \cdot i + t$. Then*

$$T(F_{a,b,c}(v)) = F_{sa,sb,sc}(T(v)).$$

The equivalence relation of Proposition 1 is written with $\Leftrightarrow$, and the set of all distinct equivalence classes is written as $\mathcal{SV}$. In Sects. 3.3 and 4.1, we will point out that if the round functions are equivalent, attack characteristics we consider are also equivalent. Therefore we can reduce the size of parameter space that we must search by computers. The size of parameter space after the reduction is 509 ($= |\mathcal{SV}|$).

As the results of the analyses by Kölbl *et al.*, the following 20 parameters are optimal with respect to 10 rounds differential characteristics.

$$\begin{array}{lllll} (0,1,2) & (0,1,3) & (1,2,3) & (3,4,5) & (0,5,10) \\ (0,5,15) & (4,5,3) & (0,7,14) & (6,7,5) & (1,8,3) \\ (3,8,14) & (7,8,5) & (5,10,15) & (6,11,1) & (1,12,7) \\ (5,12,3) & (7,12,1) & (0,13,10) & (0,13,7) & (8,13,2) \end{array}$$

Among these parameters, $(0,1,2)$ and $(5,12,3)$ are also optimal with respect to linear characteristics for 10 rounds. SIMECK, a variant of SIMON block cipher proposed by Yang *et al.* [27], has the equivalent structure as SIMON and its parameter corresponds to $(a,b,c) = (0,5,1)$. As a result, Kölbl *et al.* found that SIMON and SIMECK are not optimal with respect to differential characteristics.

2.4 Basic Consepts of Integral and Impossible Differential Attacks

The integral attack [15] is a chosen-plaintext attack against block ciphers. It is composed of *integral distinguishers* and the *key recovery* step. Suppose that a set of plaintexts is encrypted. An integral distinguisher refers to an event where certain bits of the XOR of all ciphertexts is always 0. Integral distinguishers are often constructed by evaluating the propagation characteristic of the integral property, which is the property for a multiset of the internal state. The integral property is classified as follows:

- All ($\mathcal{A}$): Every value appears the same number of times in the multiset.
- Balance ($\mathcal{B}$): The XOR of all texts in the multiset is 0.
- Const ($\mathcal{C}$): The value is fixed to a constant for all texts in the multiset.
- Unknown (*): The multiset is indistinguishable from one of random values.

In this paper, we focus on the search of integral distinguishers for all the SIMON block cipher variants.

Table 1. Computation environment

Computation node - processor - the memory capacity	Fujitsu PRIMEHPC FX100 - Fujitsu SPARC64 XIfx (2.2 GHz) 32 cores - 32 GiB
The total number of nodes (cores)	2880 nodes (92160 cores)
The total computing performance	3.2 PFlop/s
The total memory capacity	90 TiB
Programming language	C
MPI library	Fujitsu MPI

The impossible differential attack [7] is a chosen-plaintext attack against block ciphers. An adversary attempts to recover the right key by using impossible differential characteristics, which are the differential characteristics where an input difference can never result in an output difference. In this paper, we focus on the search of impossible differential characteristics for all the Simon block cipher variants.

3 Integral Attacks

In general, the propagation of integral properties cannot be evaluated efficiently in Simon because of its computational structure in which the round function is computed without S-box. Wang *et al.* [26] addressed the issue by experimentally searching the number of rounds of integral distinguishers of Simon32. The algorithm they used is shown in Sect. 3.1. However, it is computationally difficult to apply it to all parameters (Sect. 3.2). Therefore we introduce equivalence classes for rotation constants and sets of 2^{31} plaintexts (Sect. 3.3). The search result is shown in Sect. 3.4.

In Table 1, we show the computing environment we used to carry out the experiments in this section.

3.1 Integral Distinguisher Searching Algorithm

We use the following algorithm by Wang *et al.* [26] to search the number of rounds of integral distinguishers of a Simon block cipher variant.

1. Generate 2^t plaintexts ($t \geq 16$) by setting all (16) bits of the right half and $(t-16)$ bits of the left half of the input in round 1 to be property $\mathcal{A}$ (each bit is called active), while keeping the remaining bits as constant.
2. (a) Choose the private key randomly. Encrypt 2^t plaintexts by r rounds and check whether certain bits of the output are balanced (i.e., for each of these bits, the XOR sum of the bit over 2^t output states is 0). If yes, keep this as an integral candidate.

(b) Repeat (a) for K times and verify if the integral candidate always holds. If not, discard it. Here, K is the number of random keys.

3. If there is an integral candidate for all the structures with the same pattern (i.e., with the same t active bits), regard this as an r-round integral distinguisher of SIMON32.

Straightforward implementation of the above algorithm executes Step 3 after iterating Steps 2 (a) and (b) for K times. However, we see that Steps 2 (b) and 3 can be merged into a single step by fixing the constant bit of round 1 to an arbitrary value and randomly choosing the private key, and our implementation takes this approach. We note that $K = 2^{13}$ was used in [26], and it is argued that if the 2^{31} plaintexts yield the same balanced bits for all the K random keys, then with a high probability, we obtain an integral distinguisher. From the results, we observe that for large t (i.e., if the number of active bits is large), the number of rounds of integral distinguishers becomes large.

This is also the case for SIMON block cipher variants. Therefore we use this algorithm in which t is fixed to 31 because we are interested in maximizing the number of rounds of integral distinguishers.

In [14], the same experimental search was performed for SIMON48/96 with $K = 96$, where the rationale here is that it is sufficient if K is at least the key length of the block cipher. In this paper, we follow the approach in [14] and use $K = 64$. An example of an integral distinguisher against $\text{SIMON}_{5,12,3}$ that we obtain by applying this algorithm with $r = 15$ is shown in Fig. 2. In Step 1, we prepare plaintexts that have the integral property of $(\mathcal{C}, \mathcal{A}, \ldots, \mathcal{A})$ as the input of round 1, and this means that the number of rounds can be extended by one round compared to the case where we use $(\mathcal{C}, \mathcal{A}, \ldots, \mathcal{A})$ as the integral property of round 0.

3.2 Necessity for Reducing the Search Space

We first estimate the time complexity for the search of all parameters by using the algorithm in Sect. 3.1. We first observe that even if the round functions $F_{a,b,c}$ are equivalent, this may not guarantee that we have the equivalence between the corresponding integral distinguishers, and we thus need to consider 1920 parameters. From Sect. 3.1, there are 16 choices for the sets of chosen plaintexts. Then the time complexity of the algorithm is 64×2^{31} r-round $\text{SIMON}_{a,b,c}$ encryptions, implying that the time complexity for the search of all parameters and plaintext sets is estimated as $1920 \times 16 \times 64 \times 2^{31} \simeq 2^{51.91}$ r-round $\text{SIMON}_{a,b,c}$ encryptions.

We implement the algorithm in Sect. 3.1 on a computer system shown in Table 1, and we estimate the number of necessary cores to search over all parameter choices, assuming that one core carries out the algorithm in Sect. 3.1. Then one node has 32 cores under our environment. Now we observe that we need to consider 1920 parameters and 16 choices for the sets of chosen plaintexts. Thus naive implementation requires $1920 \times 16 = 30{,}720$ cores, and this corresponds to 960 nodes.

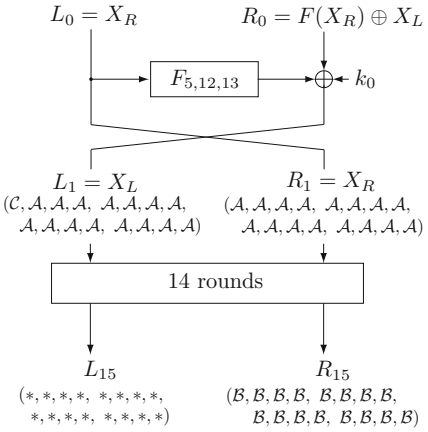

Fig. 2. 15-round integral distinguisher of SIMON$_{5,12,3}$

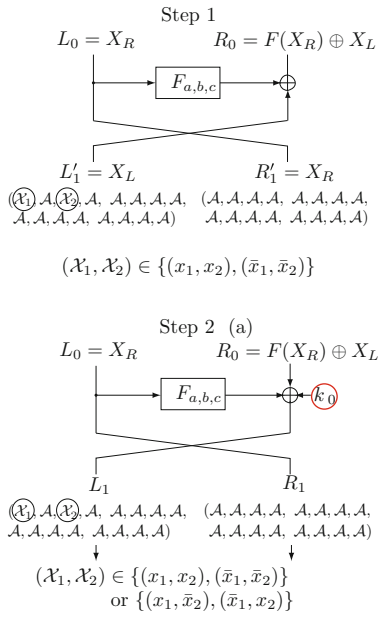

Fig. 3. Applying the algorithm in Sect. 3.1 to the new set with 2^{31} plaintexts

3.3 Finding Equivalent Parameters

We present the following property regarding the equivalence.

Property 1. Let T be a permutation of the bits of an n-bit word that corresponds to an affine transformation of the bit-indices. Thus there are $s \in Z_n$ and $t \in Z_n$ such that bit i is translated to $s \cdot i + t$. Let

$$(\mathcal{L}_0, \mathcal{R}_0) \rightarrow (\mathcal{L}_r, \mathcal{R}_r)$$

be an r-round integral distinguisher against SIMON$_{a,b,c}$. Then

$$(T(\mathcal{L}_0), T(\mathcal{R}_0)) \rightarrow (T(\mathcal{L}_r), T(\mathcal{R}_r))$$

is an r-round integral distinguisher against SIMON$_{sa,sb,sc}$.

The proof is not obvious but elementary and omitted. From Property 1, the number of parameters to consider is reduced to 509. By letting $s = 1$ in Property 1, we observe that we only have to consider an integral distinguisher with the input of round 1 of the form

$$(\mathcal{C}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}, \mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}).$$

This means that we only have to consider one set of plaintexts, and hence the time complexity is estimated $509 \times 1 \times 64 \times 2^{31} \simeq 2^{45.99}$ r-round SIMON$_{a,b,c}$ encryptions. Then the number of necessary cores in the implementation is 509, which amounts to 16 nodes.

3.4 Experiments and Search Results

We searched the number of rounds of integral distinguishers of $\text{SIMON}_{a,b,c}$ for all $(a,b,c) \in \mathcal{SV}$, where we consider two types of the sets of the input of round 1 in the algorithm in Sect. 3.1. In what follows, we show the two types of the sets. The first type is the set

$$(\mathcal{C}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}, \mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}), \tag{1}$$

mentioned in Sect. 3.1, which was searched by Wang *et al.*

The second type is the new sets we introduce in this paper, which are defined as 15 sets of the form:

$$\begin{gathered}(\mathcal{X}_1\mathcal{A}\mathcal{X}_2\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}, \mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}) \\ (\mathcal{X}_1\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{X}_2\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}, \mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}) \\ \vdots \\ (\mathcal{X}_1\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}, \mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{A}\mathcal{X}_2\mathcal{A})\end{gathered} \tag{2}$$

each of which contains 2^{31} states, which will be used as the input of round 1. Here each set contains one bit $\mathcal{X}_1$, one bit $\mathcal{X}_2$, and 30 active bits. We first fix the two bits indicated with $\mathcal{X}_1$ and $\mathcal{X}_2$ to any value $(x_1, x_2) \in \{(0,0),(0,1),(1,0),(1,1)\}$, and this yields 2^{30} states from the 30 active bits. We then consider another set of 2^{30} states by fixing the two bits to $(\bar{x}_1, \bar{x}_2)$, and the actual set of 2^{31} states consists of the whole above mentioned states. Here, we let $\bar{x} = x \oplus 1$ for a bit x. In Fig. 3, we show how the algorithm in Sect. 3.1 is applied to (2). In Step 1, we obtain 2^{31} plaintexts by decrypting the set of the input of round 1 satisfying property (2) without the subkey (or equivalently, by assuming that the subkey is zero). In Step 2 (a), we encrypt the obtained plaintexts in Step 1. Here, if the corresponding bits of subkey in round 0 have value $(0,0)$ or $(1,1)$, the corresponding bits of the input of round 1 have values of the form (x_1, x_2) and $(\bar{x}_1, \bar{x}_2)$. If the corresponding bits of subkey in round 0 have value $(0,1)$ or $(1,0)$, they have the value of the form $(x_1, \bar{x}_2)$ and $(\bar{x}_1, x_2)$. However, we observe that both cases still have the property indicated in (2).

Since we consider two types, namely the 16 sets in total with 2^{31} chosen plaintexts, the time complexity is estimated as $509 \times 16 \times 64 \times 2^{31} \simeq 2^{49.99}$ r-round $\text{SIMON}_{a,b,c}$ encryptions from Sect. 3.3.

We show the number of rounds of integral distinguishers and the number of corresponding parameters as the result of the experiment in Table 2 and Fig. 4. Note that small number of rounds implies the stronger resistance against integral attack.

In our implementation of this experiments, we set r to $r_{\max}$ which is a sufficiently large number in the algorithm in Sect. 3.1. In Step 2 (a) we check if certain bits are balanced for $r_{\max}$ rounds, and save all the intermediate states so that we obtain the number of rounds of integral distinguishers. With respect to the running time, when the number of cores is 509, $r_{\max} = 26$, and with (1), it

Table 2. Search result of integral distinguishers

The number of rounds	14	15	16	18	19	20	22	33	≥ 53	∞	Sum
The number of parameters	97	112	62	4	15	18	16	6	15	164	509

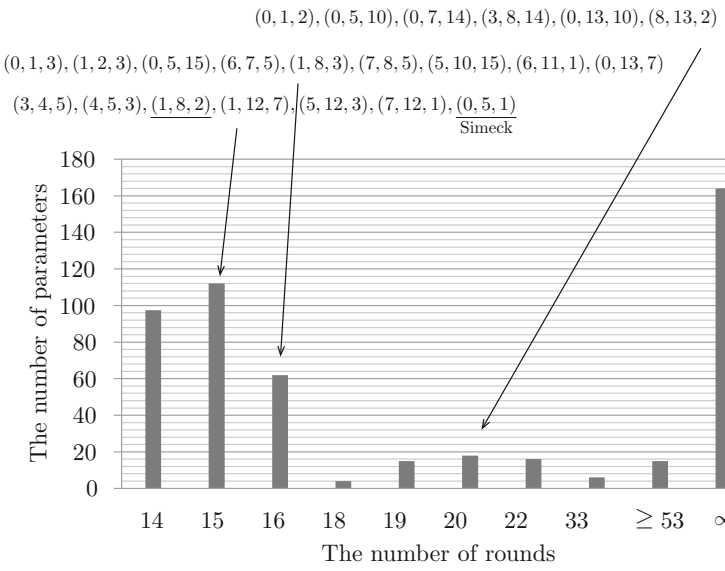

Fig. 4. Search result of integral distinguishers and comparison with parameter in [16]. The listed parameters are 20 parameters from [16] and the parameters for Simon and Simeck, and the 20 parameters are optimal with respect to 10 rounds differential characteristics.

took 18 h 8 m 31 s. When the number of cores is 345 and $r_{\max} = 36$, each of (2) took about a day, and for instance the first case of (2) took 25 h 5 m 52 s.

We also note that "≥ 53" means that the maximum value of $r_{\max}$ was set to 53, as we stopped the program due to the time constraint. Thus parameters in this class have integral distinguishers with the number of rounds that is larger than 53, but the precise value is unknown at this moment. Moreover, we observe that when a, b, and c are all odd or all even, then the cipher has integral distinguisher of infinite number of rounds.

A detailed result shows an interesting fact. Most of the results are obtained by using (1). However, it turns out that there are cases where (2) outperforms (1). In more detail, for parameters $(1, 6, 4), (1, 14, 12), (2, 3, 12)$ and $(2, 7, 4)$, we obtain larger number of rounds with (2) than (1), and this was obtained when both $\mathcal{X}_1$ and $\mathcal{X}_2$ belong to the left half of the input of round 1.

In Sect. 5, we use the result to make a comparison of the strength of Simon block cipher variants.

4 Impossible Differential Attacks

4.1 Impossible Differential Characteristic (IDC) of SIMON$_{a,b,c}$

In this paper, we use the *miss-in-the-middle approach* [26] to search impossible differential characteristics (IDCs) of SIMON block cipher variants. First, we extend two differential paths forward/backward from fixed input/output difference by using differential propagation through one round repeatedly. Next, we check if the corresponding bits are different in the outputs of these paths. If this is the case, we obtain IDC by connecting these paths.

Differential Propagation through One Round. Let $L_r[i]$ and $R_r[i]$ denote the i-th bit of L_r and R_r, and ΔL_r and ΔR_r denote the difference of L_r and R_r, respectively. From the definition of the round function, we obtain the following bitwise equation.

$$\begin{aligned}\Delta L_{r+1}[i] =&(\Delta L_r[i+a] \wedge L_r[i+b]) \oplus (L_r[i+a] \wedge \Delta L_r[i+b]) \\ &\oplus (\Delta L_r[i+a] \wedge \Delta L_r[i+b]) \oplus \Delta L_r[i+c] \oplus \Delta R_r[i] \end{aligned} \tag{3}$$

Therefore the one round differential propagation can be described without any information of subkeys as follows:

$$\begin{aligned}\Delta L_{r+1}[i] &= \begin{cases} \Delta L_r[i+c] \oplus \Delta R_r[i] & \text{if } (\Delta L_r[i+a], \Delta L_r[i+b]) = (0,0) \\ ?\ \text{(Unknown)} & \text{otherwise} \end{cases} \\ \Delta R_{r+1}[i] &= \Delta L_r[i] \end{aligned} \tag{4}$$

We extend the differential path by using (4) along the encryption direction. We call it a forward differential path.

As to the decryption direction, we use the following equation.

$$\begin{aligned}\Delta L_{r-1}[i] &= \Delta R_r[i] \\ \Delta R_{r-1}[i] &= \begin{cases} \Delta R_r[i+c] \oplus \Delta L_r[i] & \text{if } (\Delta R_r[i+a], \Delta R_r[i+b]) = (0,0) \\ ?\ \text{(Unknown)} & \text{otherwise} \end{cases} \end{aligned} \tag{5}$$

We call paths extended by using (5) backward differential paths.

Furthermore, it is obvious that if the round functions have equivalent parameters, there is a corresponding equivalent differential path, and hence we also have the IDC.

IDC Search Algorithm. We use the following algorithm to search the number of rounds of IDCs of a SIMON block cipher variant. We denote a $2n$-bit input difference to the input/output differential paths by $\Delta\text{input}_0/\Delta\text{output}_0$. Then, $2n$-bit difference after r rounds of input/output differential paths are denoted by $\Delta\text{input}_r/\Delta\text{output}_r$. In the following algorithm, we obtain the number of rounds of IDCs by updating a temporal variable $r_{\max}$, which is initialized to 0.

R	Left	Right
0	0000, 0000, 0000,0000	1000, 0000, 0000, 0000
1	1000, 0000, 0000, 0000	0000, 0000, 0000, 0000
2	0000, ?000, 000?, 0100	1000, 0000, 0000, 0000
3	1?00, 00?0, ?010, 000?	0000, ?000, 000?, 0100
4	0?0?, ??01, 00??, ?0?0	1?00, 00?0, ?010, 000?
5	???0, 1???, ??1?, ?0??	0?0?, ??01, 00??, ?0?0
6	????, ????, ????, ????	???0, **1**???, ??1?, ?0??
5	00?0, ???0, 100?, ??0?	????, **01**??, ???1, ??0?
4	?1?0, 000?, 0?01, 0000	00?0, ???0, 100?, ??0?
3	0000, 0?00, 0000, ?010	?1?0, 000?, 0?01, 0000
2	0100, 0000, 0000, 0000	0000, 0?00, 0000, ?010
1	0000, 0000, 0000, 0000	0100, 0000, 0000, 0000
0	0100, 0000, 0000, 0000	0000, 0000, 0000, 0000

Fig. 5. 11-round IDC of $\text{SIMON}_{5,12,3}$ (R is the number of extended rounds)

1. Extend a forward differential path for given Δinput_0 by using (4) until all the bits of the state become unknown. Let r_{in} be the number obtained by subtracting 1 from the number of extended rounds. The subtraction is to consider a path whose bits are not all unknown.
2. Extend a backward differential path for given Δoutput_0 by using (5) until all the bits of the state become unknown. Let r_{out} be the number obtained by subtracting 1 from the number of extended rounds. Let $r_{\text{tmp}} \leftarrow r_{\text{in}} + r_{\text{out}}$.
3. Check if there are different values between the corresponding bits in $\Delta\text{input}_{r'_{\text{in}}}$ and $\Delta\text{output}_{r'_{\text{out}}}$ for all $(r'_{\text{in}}, r'_{\text{out}})$ satisfying $r'_{\text{in}} + r'_{\text{out}} = r_{\text{tmp}}$. If not, update r_{tmp} to $r_{\text{tmp}} - 1$ and iterate this step.
4. If $r_{\text{tmp}} > r_{\text{max}}$, update r_{max} to r_{tmp}.
5. Apply Steps 1 to 4 to all $(\Delta\text{input}_0, \Delta\text{output}_0) = (S^l(0\ldots01), S^m(0\ldots01))$ satisfying $l, m \in Z_{2n}$.

We then obtain the number of rounds of IDC as r_{max}. We note the reason why it is sufficient to consider the differences of the form $(\Delta\text{input}_0, \Delta\text{output}_0) = (S^l(0\ldots01), S^m(0\ldots01))$ only. Notice that if we have more bits with 1 or unknown in a certain state, then we have more bits with unknown in the next state. Thus the number of extended rounds of each differential path is reduced. Therefore it is sufficient that we search paths starting with input and output differences of low Hamming weight. An example of IDC that we obtain by applying this algorithm is shown in Fig. 5. Notice that bold bits are always different, which indicates that the differential propagation is impossible.

4.2 Experiments and Search Results

We searched the number of rounds of IDCs of $\text{SIMON}_{a,b,c}$ for all $(a, b, c) \in \mathcal{SV}$. We show the maximum number of rounds of IDCs and the number of corresponding parameters in Table 3 and Fig. 6. Smaller number of rounds that corresponds to

Table 3. IDC search result

The number of rounds	9	10	11	12	13	17	∞	Sum
The number of parameters	42	85	111	28	48	31	164	509

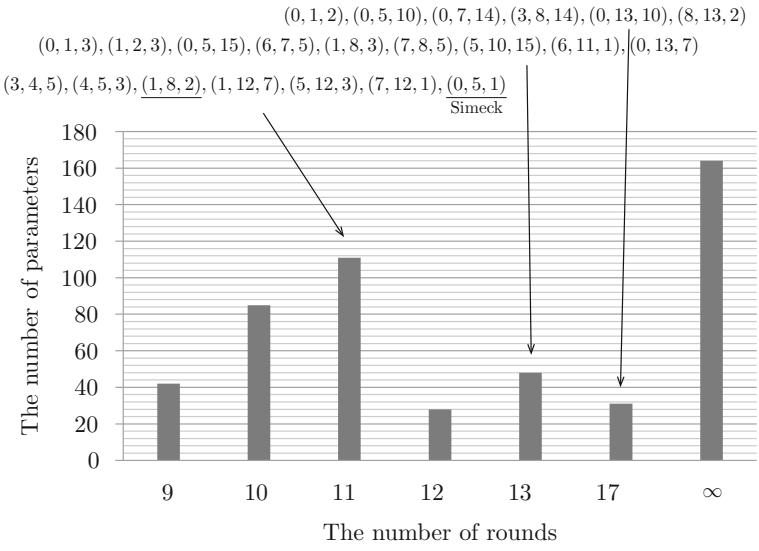

Fig. 6. IDC search result

the parameters in the left part of Fig. 6 implies the stronger resistance against impossible differential attack. We note that the same observation as the integral distinguisher here, that is, when a, b, and c are all odd or all even, then the cipher has IDC of infinite number of rounds.

In this experiment, we use a computer of which CPU is Core i5-4210M, capacity of mounted memory (RAM) is 8 GB and OS is Windows 7.

In Sect. 5, we use the result to make a comparison of the strength of SIMON block cipher variants.

5 Discussions

From the results presented in Fig. 4, Table 2, Fig. 6, and Table 3, in Table 4, we list all 345 parameters that have integral distinguishers and IDCs of finite number rounds and write in boldface the parameters that are optimal with respect to differential attacks. We classify the parameters into Groups A, B, ..., T according to the number of rounds of integral distinguishers and IDCs, and they are summarized in Fig. 7.

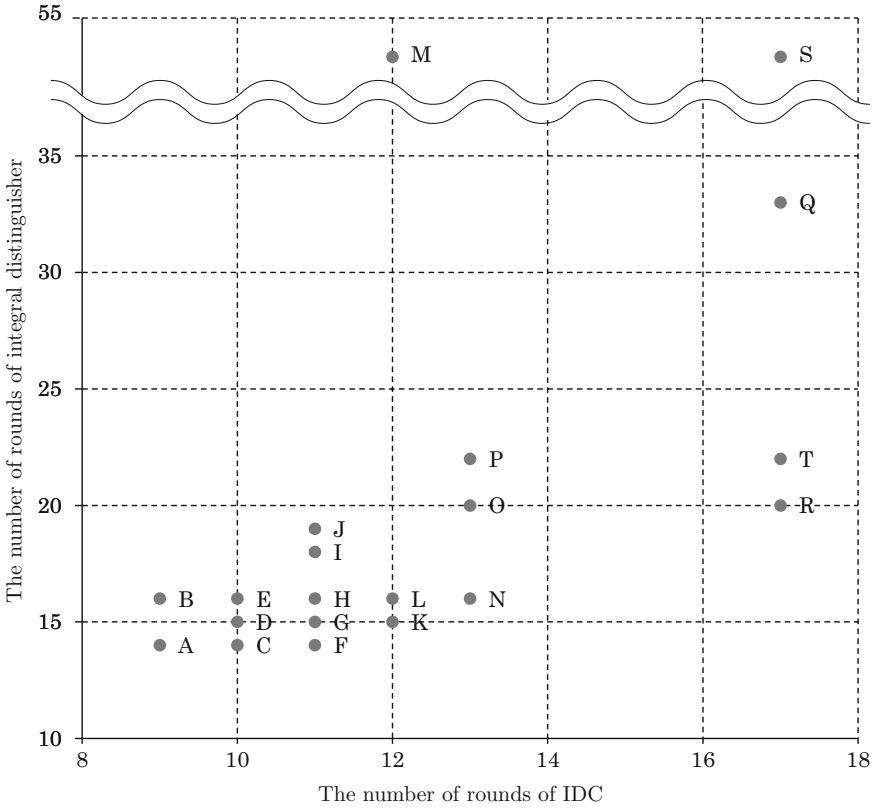

Fig. 7. Comparison of the strength against impossible differential and integral distinguisher among all parameters

We describe some observations and the notable parameters as follows:

- Note that there are many parameters in the lower left of Fig. 7.
- We observe that Group G that contains Simon and Simeck is not placed in the bottom left part of the figure, implying that the resistance against integral and impossible differential attacks was not given the highest priority when defining the rotation constants of these block ciphers.
- The number of parameters equivalent to original Simon and Simeck in resistance against these attacks is larger than any other parameters of which distinguishers have finite round.
- The default number of rounds of Simon32 is 32, and we see that all Simon block cipher variants in Groups M, S, and Q are distinguishable with the integral distinguishers even if they have the default number of rounds. They are also less resistant against impossible differential attacks.
- Parameters in Groups N and R have the highest resistance against differential attacks but low resistance against integral and impossible differential attacks.

Table 4. Comparison of the strength against impossible differential and integral distinguisher among all parameters

	*	&	parameter (a, b, c)
A	9	14	$(1,2,6)$, $(1,2,11)$, $(1,2,12)$, $(1,4,2)$, $(1,4,3)$, $(1,4,5)$, $(1,4,13)$, $(1,5,4)$, $(1,5,12)$, $(1,6,2)$, $(1,7,4)$, $(1,7,12)$, $(1,10,4)$, $(1,10,11)$, $(1,10,14)$, $(1,12,3)$, $(1,12,5)$, $(1,12,10)$, $(1,12,13)$, $(1,13,4)$, $(1,13,12)$, $(1,14,10)$, $(2,3,6)$, $(2,5,4)$, $(2,5,6)$, $(2,5,7)$, $(2,7,6)$, $(2,9,3)$, $(2,9,6)$, $(2,9,12)$, $(4,5,1)$, $(4,5,9)$, $(4,5,10)$, $(4,5,15)$, $(4,7,3)$, $(4,7,5)$, $(4,7,6)$, $(4,7,11)$
B	9	16	$(1,6,8)$, $(1,14,0)$, $(2,3,8)$, $(2,7,0)$
C	10	14	$(0,2,5)$, $(1,2,5)$, $(1,3,6)$, $(1,3,14)$, $(1,4,6)$, $(1,4,10)$, $(1,5,2)$, $(1,5,6)$, $(1,5,10)$, $(1,5,14)$, $(1,6,3)$, $(1,6,7)$, $(1,6,13)$, $(1,7,0)$, $(1,7,2)$, $(1,7,6)$, $(1,7,8)$, $(1,7,10)$, $(1,7,14)$, $(1,10,5)$, $(1,11,2)$, $(1,11,10)$, $(1,12,2)$, $(1,12,14)$, $(1,13,2)$, $(1,13,6)$, $(1,13,10)$, $(1,13,14)$, $(1,14,3)$, $(1,14,7)$, $(1,14,13)$, $(1,15,4)$, $(1,15,12)$, $(2,3,5)$, $(2,3,7)$, $(2,3,9)$,$(2,4,5)$, $(2,4,7)$, $(2,5,9)$, $(2,7,1)$, $(2,7,5)$, $(2,7,11)$, $(2,8,1)$, $(2,9,13)$, $(2,12,1)$, $(2,12,3)$, $(4,5,2)$, $(4,5,14)$, $(4,6,1)$, $(4,6,3)$, $(4,7,2)$, $(4,7,14)$, $(4,10,1)$, $(4,10,3)$, $(8,10,5)$
D	10	15	$(1,2,4)$, $(1,2,10)$, $(1,6,4)$, $(1,6,14)$, $(1,10,2)$, $(1,10,12)$, $(1,14,6)$, $(1,14,12)$, $(2,3,10)$, $(2,3,12)$, $(2,4,3)$, $(2,5,10)$, $(2,5,12)$, $(2,7,4)$, $(2,7,10)$, $(2,9,4)$, $(2,9,10)$, $(2,12,7)$, $(4,6,5)$, $(4,10,7)$
E	10	16	$(0,1,6)$, $(0,1,11)$, $(1,6,15)$, $(1,8,11)$, $(1,8,14)$, $(1,14,15)$, $(2,3,13)$, $(2,7,9)$, $(8,9,3)$, $(8,9,14)$
F	11	14	$(1,2,7)$, $(1,10,7)$, $(2,5,3)$, $(2,9,15)$
G	11	15	$(0,1,4)$, $(0,1,5)$, $(0,1,7)$, $(0,1,10)$, $(0,1,12)$, **$(0, 1, 13)$**(Simeck), $(0,4,1)$, $(0,4,3)$, $(1,2,8)$, $(1,2,9)$, $(1,2,13)$, $(1,2,14)$, $(1,3,4)$, $(1,3,12)$, $(1,4,0)$, **$(1, 4, 7)$**, $(1,4,8)$, $(1,4,11)$, $(1,4,15)$, $(1,5,0)$, $(1,5,8)$, $(1,6,5)$, $(1,6,9)$, $(1,6,10)$, $(1,8,2)$, $(1,8,4)$, $(1,8,5)$, $(1,8,7)$, $(1,8,12)$, $(1,8,13)$, $(1,10,0)$, $(1,10,6)$, $(1,10,9)$, $(1,10,13)$, $(1,11,4)$, $(1,11,12)$, $(1,12,0)$, **$(1, 12, 7)$**, $(1,12,8)$, $(1,12,11)$, $(1,12,15)$, $(1,13,0)$, $(1,13,8)$, $(1,14,2)$, $(1,14,5)$, $(1,14,9)$, $(2,3,11)$, $(2,3,14)$, $(2,3,15)$, $(2,5,0)$, $(2,5,1)$, $(2,5,13)$, $(2,5,14)$, $(2,7,3)$, $(2,7,14)$, $(2,7,15)$, $(2,9,1)$, $(2,9,5)$, $(2,9,8)$, $(2,9,14)$, $(2,14,1)$, $(2,14,3)$, $(2,14,5)$, $(2,14,7)$, $(4,5,0)$, $(4,5,3)$, $(4,5,7)$, $(4,5,8)$, $(4,5,11)$, $(4,7,0)$, $(4,7,1)$, $(4,7,8)$, $(4,7,9)$, $(4,7,13)$, $(4,8,1)$, $(4,8,3)$, $(8,9,2)$, $(8,9,4)$, $(8,9,5)$, $(8,9,12)$, $(8,9,13)$, $(8,9,15)$, $(8,12,1)$, $(8,12,3)$
H	11	16	$(1,6,12)$, $(1,14,4)$, $(2,3,4)$, $(2,7,12)$
I	11	18	$(1,4,9)$, $(1,12,9)$, $(4,5,13)$, $(4,7,15)$
J	11	19	$(0,1,8)$, $(0,1,9)$, $(0,2,1)$, $(1,4,12)$, $(1,8,0)$, $(1,8,9)$, $(1,12,4)$, $(1,15,0)$, $(1,15,8)$, $(2,8,5)$, $(4,5,12)$, $(4,7,12)$, $(8,9,0)$, $(8,9,1)$, $(8,10,1)$
K	12	15	$(2,4,1)$, $(2,6,1)$, $(2,6,3)$, $(2,6,5)$, $(2,6,7)$, $(2,12,5)$, $(4,6,7)$, $(4,10,5)$
L	12	16	$(1,3,0)$, $(1,3,8)$, $(1,4,14)$, $(1,6,0)$, $(1,11,0)$, $(1,11,8)$, $(1,12,6)$, $(1,14,8)$, $(2,3,0)$, $(2,7,8)$, $(4,5,6)$, $(4,7,10)$
M	12	53	$(1,9,2)$, $(1,9,6)$, $(1,9,10)$, $(1,9,14)$, $(2,10,1)$, $(2,10,3)$, $(2,10,5)$, $(2,10,7)$

(Continued)

Table 4. *(Continued)*

	*	&	parameter (a, b, c)
N	13	16	**(0, 1, 3)**, **(0, 1, 14)**, $(0,2,3)$, $(0,2,7)$, **(1, 2, 3)**, $(1,2,15)$, $(1,3,2)$, $(1,3,10)$, $(1,6,11)$, **(1, 8, 3)**, $(1,8,6)$, **(1, 10, 3)**, $(1,10,15)$, $(1,11,6)$, $(1,11,14)$, $(1,14,11)$, $(1,15,2)$, $(1,15,6)$, $(1,15,10)$, $(1,15,14)$, $(2,3,1)$, $(2,5,11)$, $(2,5,15)$, $(2,7,13)$, $(2,8,3)$, $(2,8,7)$, $(2,9,7)$, $(2,9,11)$, $(8,9,6)$, $(8,9,11)$, $(8,10,3)$, $(8,10,7)$
O	13	20	$(1,6,1)$, $(1,6,6)$, $(1,14,1)$, $(1,14,14)$, $(2,3,2)$, $(2,3,3)$, $(2,7,2)$, $(2,7,7)$
P	13	22	$(1,4,1)$, $(1,4,4)$, $(1,12,1)$, $(1,12,12)$, $(4,5,4)$, $(4,5,5)$, $(4,7,4)$, $(4,7,7)$
Q	17	33	$(0,1,0)$, $(0,1,1)$, $(1,8,1)$, $(1,8,8)$, $(8,9,8)$, $(8,9,9)$
R	17	20	**(0, 1, 2)**, $(0,1,15)$, $(1,2,0)$, **(1, 8, 10)**, $(1,8,15)$, $(1,10,8)$, $(2,5,8)$, $(2,9,0)$, $(8,9,7)$, $(8,9,10)$
S	17	53	$(0,8,1)$, $(1,9,0)$, $(1,9,4)$, $(1,9,8)$, $(1,9,12)$, $(4,12,1)$, $(4,12,3)$
T	17	22	$(1,2,1)$, $(1,2,2)$, $(1,10,1)$, $(1,10,10)$, $(2,5,2)$, $(2,5,5)$, $(2,9,2)$, $(2,9,9)$

*: The number of rounds of impossible differential characteristic
&: The number of rounds of integral distinguisher

Interestingly, we find that two parameters $(1,4,7)$ and $(5,12,3) \Leftrightarrow (1,12,7)$ (both in Group G) are better than original SIMON from the following reasons.

- $(1,4,7)$ and $(5,12,3)$ belong to the 20 parameters with optimal security against differential attack, while SIMON or SIMECK are not optimal.
- $(1,4,7)$ and $(5,12,3)$ have the same level of security against integral and impossible differential attacks as the original SIMON.

Additionally, $(5,12,3)$ is optimal with respect to linear attacks, and hence this can be an alternative parameter to the original one. However, it should be noted that we only focus on the security aspect against the four attacks only, and the implementation characteristic is not considered here.

Links Between Impossible Differential and Integral Attacks. In 2015, Sun *et al.* [21] showed that impossible differential characteristics lead to integral distinguishers for any Feistel cipher adopting an SP-round function. Actually, for all parameters from Fig. 7, we observe that integral distinguishers cover more rounds than impossible differential characteristics, which agrees with the observation by Sun *et al.* Thus we are interested in if we can view our results with the context of the link.

Sun *et al.* assumes that the domain and range sizes of the S-layer is a word size, n. To fit the round function of $\text{SIMON}_{a,b,c}$ into this framework, we have to regard the entire round function as S and then P is an identity transformation. Otherwise, concatenation of bit-wise AND is the only possible candidate as S, leading to $2n$-bit to n-bit S-layer which does not match the framework. By regarding the entire round function as S, we can only examine a set of 2^n plaintexts, in which $n = 16$ for SIMON32. At this level, the link in [21] can be applied

to SIMON. However, we carried out our experiments, considering the details of $F_{a,b,c}$. At this level, any links between integral distinguishers and impossible differential characteristics has not been discovered.

6 Conclusions

In this paper, we searched the number of rounds of integral distinguishers and impossible differential characteristic for all parameters $(a, b, c) \in \mathcal{SV}$. As a result, we clarified that original rotation constants $(1, 8, 2)$ are not chosen to optimize resistance against integral and impossible differential attacks. Furthermore, from our experiments and investigations by Kölbl *et al.*, we found that $(a, b, c) = (5, 12, 3)$ is a possible alternative parameter to the original parameter.

Acknowledgments. The authors thank the anonymous ACNS 2016 reviewers for helpful comments. The work was partially carried out during ASK 2015 (Asian-workshop on Symmetric Key Cryptography) and Dagstuhl seminar 16021. The work by Tetsu Iwata was supported in part by JSPS KAKENHI, Grant-in-Aid for Scientific Research (B), Grant Number 26280045. The experiment in Sect. 3 was conducted using a supercomputer system at Information Technology Center of Nagoya University.

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.) Progress in Cryptology – INDOCRYPT 2015. LNCS, vol. 9462, pp. 153–179. Springer, Heidelberg (2015)
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)
3. Ahmadian, Z., Rasoolzadeh, S., Salmasizadeh, M., Aref, M.R.: Automated Dynamic Cube Attack on Block Ciphers: Cryptanalysis of SIMON and KATAN. Cryptology ePrint Archive, Report 2015/040 (2015). http://eprint.iacr.org/
4. Alizadeh, J., Alkhzaimi, H.A., Aref, M.R., Bagheri, N., Gauravaram, P., Kumar, A., Lauridsen, M.M., Sanadhya, S.K.: Cryptanalysis of SIMON variants with connections. In: Sadeghi, A.-R., Saxena, N. (eds.) RFIDSec 2014. LNCS, vol. 8651, pp. 90–107. Springer, Heidelberg (2014)
5. Ashur, T.: Improved Linear Trails for the Block Cipher Simon. Cryptology ePrint Archive, Report 2015/285 (2015). http://eprint.iacr.org/
6. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404 (2013). http://eprint.iacr.org/
7. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. J. Crypt. **18**(4), 291–311 (2005)
8. Biryukov, A., Roy, A., Velichkov, V.: Differential analysis of block ciphers SIMON and SPECK. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 546–570. Springer, Heidelberg (2015)

9. Boura, C., Naya-Plasencia, M., Suder, V.: Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 179–199. Springer, Heidelberg (2014)
10. Chen, H., Wang, X.: Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-guessing Techniques. Cryptology ePrint Archive, Report 2015/666 (2015). http://eprint.iacr.org/
11. Chen, H., Wang, X.: Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-guessing Techniques. In: Pre-Proceedings of FSE 2016 (2016). https://fse.rub.de/index.html
12. Chen, Z., Wang, N., Wang, X.: Impossible Differential Cryptanalysis of Reduced Round SIMON. Cryptology ePrint Archive, Report 2015/286 (2015). http://eprint.iacr.org/
13. Hao, Y., Meier, W.: Truncated Differential Based Known-Key Attacks on Round-Reduced Simon. Cryptology ePrint Archive, Report 2016/020 (2016). http://eprint.iacr.org/
14. Iizuka, H., Todo, Y., Morii, M.: Integral Attack against Simon48. In: SCIS 2015 2E1-3 (2015) (in Japanese)
15. Knudsen, L.R., Wagner, D.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
16. Kölbl, S., Leander, G., Tiessen, T.: Observations on the SIMON block cipher family. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology – CRYPTO 2015. LNCS, vol. 9215, pp. 161–185. Springer, Heidelberg (2015)
17. Mourouzis, T., Song, G., Courtois, N., Christofii, M.: Advanced Differential Cryptanalysis of Reduced-Round SIMON64/128 Using Large-Round Statistical Distinguishers. Cryptology ePrint Archive, Report 2015/481 (2015). http://eprint.iacr.org/
18. Pramstaller, N., Rechberger, C., Rijmen, V.: Impact of rotations in SHA-1 and related hash functions. In: Preneel, B., Tavares, S.E. (eds.) SAC 2005. LNCS, vol. 3897, pp. 261–275. Springer, Heidelberg (2006)
19. Raddum, H.: Algebraic analysis of the simon block cipher family. In: Lauter, K., Rodríguez-Henríquez, F. (eds.) LatinCrypt 2015. LNCS, vol. 9230, pp. 157–169. Springer, Heidelberg (2015)
20. Shi, D., Hu, L., Sun, S., Song, L., Qiao, K., Ma, X.: Improved Linear (hull) Cryptanalysis of Round-reduced Versions of SIMON. Cryptology ePrint Archive, Report 2014/973 (2014). http://eprint.iacr.org/
21. Sun, B., Liu, Z., Rijmen, V., Li, R., Cheng, L., Wang, Q., AlKhzaimi, H., Li, C.: Links among impossible differential, integral and zero correlation linear cryptanalysis. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology – CRYPTO 2015. LNCS, vol. 9215, pp. 95–115. Springer, Heidelberg (2015)
22. Sun, S., Hu, L., Wang, M., Wang, P., Qiao, K., Ma, X., Shi, D., Song, L., Fu, K.: Constructing Mixed-integer Programming Models whose Feasible Region is Exactly the Set of All Valid Differential Characteristics of SIMON. Cryptology ePrint Archive, Report 2015/122 (2015). http://eprint.iacr.org/
23. 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.) Advances in Cryptology – ASIACRYPT 2014. LNCS, vol. 8873, pp. 158–178. Springer, Heidelberg (2014)
24. Todo, Y., Morii, M.: Bit-Based Division Property and Application to Simon Family. In: Pre-Proceedings of FSE 2016 (2016). https://fse.rub.de/index.html

25. Wang, N., Wang, X., Jia, K., Zhao, J.: Differential Attacks on Reduced SIMON Versions with Dynamic Key-guessing Techniques. Cryptology ePrint Archive, Report 2014/448 (2014). http://eprint.iacr.org/
26. Wang, Q., Liu, Z., Varici, K., Sasaki, Y., Rijmen, V., Todo, Y.: Cryptanalysis of reduced-round SIMON32 and SIMON48. In: Meier, W., Mukhopadhyay, D. (eds.) Progress in Cryptology – INDOCRYPT 2014. LNCS, vol. 8885, pp. 143–160. Springer, Heidelberg (2014)
27. 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)