Optimal Differential Trails in SIMON-like Ciphers

Zhengbin Liu[1,2], Yongqiang Li[1,2,3*], 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, Beijing, China
[3] Science and Technology on Communication Security Laboratory, Chengdu, China
yongq.lee@gmail.com
{liuzhengbing,wangmingsheng}@iie.ac.cn

Abstract. In the present paper, we propose an automatic search algorithm for optimal differential trails in SIMON-like ciphers. First, we give a more accurate upper bound on the differential probability of SIMON-like round function. It is shown that when the Hamming weight of the input difference α, which is denoted by $wt(\alpha)$, is less than one half of the input size, the corresponding maximum differential probability of SIMON-like round function is less than or equal to $2^{-wt(\alpha)-1}$. Based on this, we adapt Matsui's algorithm and propose an efficient algorithm for searching for optimal differential trails. With the proposed algorithm, we find the provably optimal differential 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 differential trails for SIMON64, SIMON96 and SIMON128 are reported. The provably optimal differential trails for 13, 19 and 25 rounds of SIMECK32/48/64 are also found respectively, which confirm the results given by Kölbl et al. [KR15]. Besides the optimal differential trails, we also find the 14, 17, 23, 31 and 41-round differentials for SIMON32/48/64/96/128, and 14, 21 and 27-round differentials for SIMECK32/48/64, respectively. As far as we know, these are the best differential distinguishers for SIMON and SIMECK so far. Compared with the approach based on SAT/SMT solvers used by Kölbl et al., our algorithm is more efficient and more practical to evaluate the security against differential cryptanalysis in the design of SIMON-like ciphers.

Keywords: automatic search, differential trail, SIMON, SIMECK

1 Introduction

Lightweight ciphers are driven by the need of resource-constrained applications such as RFID tags, smart cards and sensor networks. During the last decade, many lightweight ciphers have been proposed. Here are some notable examples: mCrypton [LK05], SEA [SPGQ06], HIGHT [HSH+06], DESL [PLSP07], DESXL [LPPS07], PRESENT [BKL+07], CLEFIA [SSA+07], MIBS [ISSK09], TWIS [OKJL09], KATAN and KTANTAN [CDK09], KLEIN [GNL11], LED [GPPR11], Piccolo [SIH+11], LBlock [WZ11], PRINCE [BCG+12], TWINE [SMMK12].

In 2013, the NSA published two novel lightweight cipher families SIMON and SPECK [BSS+13]. Compared with other existing ciphers, these families have a better performance in both hardware and software platforms. Afterwards, a family of lightweight block ciphers called SIMECK was proposed at CHES'15 by Yang et al. [YZS+15]. The designers combined the good components of SIMON and SPECK and gave a more compact and efficient cipher in hardware. SIMON and SIMECK are both based on Feistel construction

[*] Corresponding author

and their round functions are the same except using 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.

However, the designers of SIMON and SPECK neither provided the design rationale, nor gave any security evaluation or cryptanalytic results. This inspired the cryptographic community to take further investigations for a deeper understanding of these ciphers. So far, a large variety of papers evaluating the security of SIMON have been published [ALLW14, AAA+14, AL13, BRV14, CW16, CWW15, CMS+14, KSI16, TM16, WWJZ14, WLV+14]. And among these cryptanalytic results, differential and linear cryptanalysis are the most promising attacks.

Differential cryptanalysis is one of the most powerful techniques in the cryptanalysis of symmetric-key cryptographic primitives. Therefore, security against differential cryptanalysis is becoming a major security metrics for the design of block ciphers. As for S-box based ciphers, a variety of automatic search algorithms have been proposed for evaluating the security against differential cryptanalysis [BBF15, BZL14, BN10, BN11, BDF11, Mat94, MWGP11, SHW+14]. Because the S-boxes used in S-box based ciphers usually operate on 8 or 4-bit words, and it is easy to construct their difference distribution tables (DDT). However, SIMON-like ciphers use AND operation as the source of nonlinearity. Constructing a DDT for SIMON-like round function of n-bit input requires 2^{2n} bytes of memory. This is infeasible for a typical word size of 32 bits.

Biryukov et al. introduced the concept of partial difference distribution table (pDDT) and proposed an automatic search algorithm for differential trails in ARX ciphers [BV14]. The pDDT contains only a fraction of differences whose probabilities are above a fixed threshold. With the pDDT, they extended Matsui's algorithm [Mat94] to ARX ciphers for the first time. Due to the generalization of pDDT, their algorithm can also be used to search for differential trails in SIMON-like ciphers. With the proposed algorithm, they found some improved differential trails for SIMON and SPECK [BRV14, BV14]. However, their algorithm uses heuristics to find high-probability differential trails and may not obtain the optimal differential trail.

At CRYPTO 2015, Kölbl et al. gave an explicit formula for the differential probability of SIMON-like round function [KLT15]. Based on this, they applied an approach based on SAT/SMT solvers to find optimal differential trails for SIMON, and reported the provably optimal differential trails for SIMON32, SIMON48, and a 16-round optimal differential trail with probability 2^{-54} for SIMON64. Due to the similarity of SIMON and SIMECK, Kölbl et al. also found the provably optimal differential trails for SIMECK [KR15]. However, they didn't report the provably optimal differential trails for SIMON64, SIMON96 and SIMON128. Also, it takes much time for the SAT/SMT solver to find optimal differential trails in SIMON-like ciphers, which may limit its application to SIMON-like ciphers with large block sizes, such as 96 and 128 bits.

At SCN 2016, Beierle gave an upper bound on the probability of differential trails in SIMON-like ciphers and presented the first non-experimental security argument for several SIMON-like instances [Bei16]. Although these bounds are worse than the bounds obtained by other automatic search algorithms, the argument gives more insights into the design of SIMON-like ciphers.

Our Contributions. This paper investigates the problem of automatic searching for optimal differential trails in SIMON-like ciphers, and our main contributions are summarized as follows.

1. Based on the observations given by Kölbl et al. [KLT15] and Beierle's arguments [Bei16], we give a more accurate upper bound on the differential probability of SIMON-like round function. According to the theorem given by Kölbl et al., the maximum differential probability of SIMON-like round function decreases as the

Hamming weight of input difference increases. Beierle derived an accurate upper bound for the case when the Hamming weight of input difference equals 2. We extend the accurate upper bound to the case when the Hamming weight is less than one half of the input size.

2. We propose an efficient automatic search algorithm for optimal differential trails in SIMON-like ciphers. Our algorithm is based on Matsui's branch-and-bound algorithm [Mat94]. Since the maximum differential probability of round function depends on the Hamming weight of input difference, we can always search for differential trails by traversing input differences from low Hamming weight. Once we find some difference whose probability does not satisfy the search condition, we can break the unnecessary branches as soon as possible, that is, we needn't traverse the input differences with higher Hamming weight. With the upper bound given in this paper, we can improve the efficiency of the search algorithm greatly.

3. With our algorithm, it is able to find the provably optimal differential trails for SIMON and SIMECK. For SIMON with block size 32, 48, 64, 96 and 128 bits, we find the optimal differential trails on 12, 16, 19, 28 and 37 rounds with probability 2^{-34}, 2^{-50}, 2^{-64}, 2^{-96} and 2^{-128} respectively. Meanwhile we report the provably optimal differential 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 differential trails on 13, 19 and 25 rounds respectively, which confirm the optimal differential trails given by Kölbl et al. [KR15]. Besides, we find the 14, 17, 23, 31 and 41-round differentials for SIMON32/48/64/96/128, with probabilities $2^{-30.76}$, $2^{-46.38}$, $2^{-61.93}$, $2^{-95.34}$ and $2^{-123.74}$ respectively. The 14, 21 and 27-round differentials with probabilities $2^{-31.64}$, $2^{-45.28}$ and $2^{-61.49}$ are also found for SIMECK32/48/64, respectively.

Outline. The paper is organized as follows. Section 2 gives a brief description of the block ciphers SIMON and SIMECK. In Section 3, we give a more accurate upper bound on the differential probability of SIMON-like round function. In Section 4, an automatic search algorithm is proposed for optimal differential trails in SIMON-like ciphers. In Section 5, we apply the proposed algorithm to block ciphers SIMON and SIMECK, and show the experimental results. A short conclusion is given in Section 6.

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
$x \lll r$	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
Δx	XOR difference of x and x' : $\Delta x = x \oplus x'$
x_i	the i-th bit of the n-bit word x
0_n	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 [BSS+13]. It has a Feistel structure and operates on $2n$-bit state, where n is the word size and $n = 16, 24, 32, 48$ and 64. The key size composes of m n-bit words, where $m = 2, 3, 4$. SIMON with block size $2n$ bits and key size mn bits is referred to as SIMON$2n/mn$.

SIMON utilizes an extremely simple round function consisting of three operations: AND ($\wedge$) , XOR ($\oplus$) and rotation ($\lll$). The round function 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 of SIMON. The output of i-th round is (L_{i+1}, R_{i+1}), and (L_{i+1}, R_{i+1}) is computed as follows:

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

In 2015, Yang et al. proposed a family of lightweight block ciphers SIMECK [YZS+15]. Their design combines the good components of SIMON and SPECK which leads to a more compact and efficient implementation in hardware. SIMECK has only three variants: SIMECK32/64, SIMECK48/96 and SIMECK64/128. SIMECK is also based on Feistel construction and its round function is the same as SIMON's apart from using $(0, 5, 1)$ as the rotational constants.

The subkeys are derived from a master key by key scheduling. As the key schedule is not relevant to the search algorithm, we omit its description and refer the reader to [BSS+13] and [YZS+15] for the detail description of SIMON and SIMECK.

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

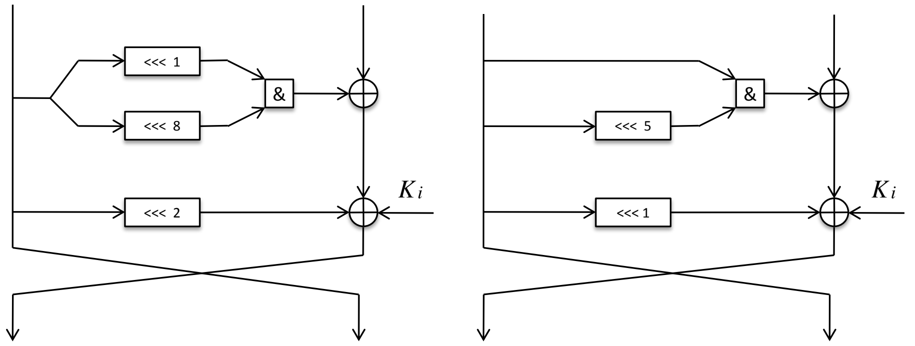

Figure 1: The round functions of SIMON and SIMECK

3 Upper Bound on the Differential Probability of SIMON-like Round Function

In this section, we derive a more accurate upper round on the differential probability of SIMON-like round function, which is based on the observations given by Kölbl et al. [KLT15] and Beierle's arguments [Bei16].

Definition 1 (SIMON-like Round Function[KLT15]). 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 are two particular cases of SIMON-like cipher, which use $(1, 8, 2)$ and $(0, 5, 1)$ as a choice for the rotational constants (a, b, c) respectively.

Note that the SIMON-like round function defined above is a particular case of Beierle's definition [Bei16], where a quadratic, rotational invariant function is used 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 differential probability of SIMON-like round function, and their results are as follows.

Theorem 1 (Differential probability of SIMON-like round function [KLT15])**.** *Let $F(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$, where n is even, $a > b$ and $\gcd(n, a-b) = 1$. Let α and β be an input and an output difference. Then with*

$$varibits = (\alpha \lll a) \vee (\alpha \lll b)$$

and

$$doublebits = (\alpha \lll b) \wedge \overline{(\alpha \lll a)} \wedge (\alpha \lll (2a - b))$$

and

$$\gamma = \beta \oplus (\alpha \lll c),$$

the probability that difference α goes to difference β is

$$P(\alpha \mapsto \beta) = \begin{cases} 2^{-n+1} & if\ \alpha = 2^n - 1\ and\ wt(\gamma) \equiv 0\ mod\ 2 \\ 2^{-wt(varibits \oplus doublebits)} & if\ \alpha \neq 2^n - 1\ and\ \gamma \wedge \overline{varibits} = 0_n \\ & and\ (\gamma \oplus (\gamma \lll (a-b))) \wedge doublebits \\ & = 0_n \\ 0 & else. \end{cases}$$

From Theorem 1, the differential probability $P(\alpha \mapsto \beta)$ is the same for all possible output differences β, and we use P_α instead of $P(\alpha \mapsto \beta)$. Beierle obtains an upper bound on the differential probability of SIMON-like function depending on the Hamming weight of input difference. We list the result in the following.

Theorem 2 (Upper bound on the differential probability [Bei16])**.** *Let $F(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$. Assume that $n \geq 6$ is even, $a > b$ and $\gcd(n, a-b) = 1$. Let α be an input difference of $F(x)$. Then for the differential probability, it holds that*

(1) If $wt(\alpha) = 1$, then $P_\alpha \leq 2^{-2}$;

(2) If $wt(\alpha) = 2$, then $P_\alpha \leq 2^{-3}$;

(3) If $wt(\alpha) \neq n$, then $P_\alpha \leq 2^{-wt(\alpha)}$;

(4) If $wt(\alpha) = n$, then $P_\alpha \leq 2^{-n+1}$.

Note that the cases (1), (3) and (4) in Theorem 2 follow directly from Theorem 1, and Beierle derived an accurate upper bound for the case $wt(\alpha) = 2$. We extend the accurate upper bound to the case $1 \leq wt(\alpha) < n/2$, which can be used to further improve the efficiency of the search algorithm. Our result is as follows.

Theorem 3. *Let $F(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$, where n is even, $a > b$ and* $\gcd(n, a-b) = 1$. *Let α be an input difference of $F(x)$. Then for the differential probability, it holds that*

(1) If $1 \leq wt(\alpha) < n/2$*, then* $P_\alpha \leq 2^{-wt(\alpha)-1}$;

(2) If $n/2 \leq wt(\alpha) < n$*, then* $P_\alpha \leq 2^{-wt(\alpha)}$;

(3) If $wt(\alpha) = n$*, then* $P_\alpha \leq 2^{-n+1}$.

Proof. Appendix A.

4 Automatic Search Algorithm for Optimal Differential Trails

In 1994, Matsui proposed a practical automatic search algorithm for the optimal differential trail of DES [Mat94]. The algorithm performs a recursive search for differential trails over a given number of rounds n ($n \geq 1$). It derives the best n-round differential probability B_n from the knowledge of the best i-round probability B_i ($1 \leq i \leq n-1$) and the initial estimate $\overline{B_n}$ for B_n. However, Matsui's algorithm is only applicable to S-box based ciphers. Recently Biryukov et al. proposed a threshold search algorithm and obtained some improved differential trails for SIMON [BRV14, BV14]. They introduced the concept of pDDT and adapted Matsui's algorithm for finding differential trails in SIMON. But their algorithm can't always find the optimal differential trail since it uses heuristics to find high-probability differential trails.

In this section, an adapted Matsui's algorithm is introduced, which can find optimal differential trails in SIMON-like ciphers under the Markov assumption. Because our algorithm doesn't introduce any heuristics, it can obtain the optimal differential trail. The propagation of differences in SIMON-like round function is depicted in Fig 2.

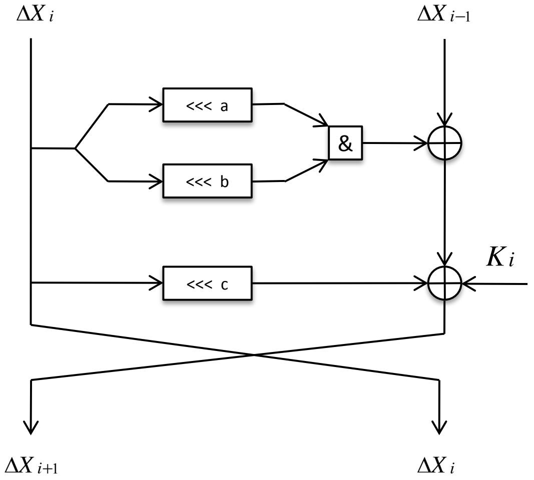

Figure 2: Propagation of differences in SIMON-like round function

SIMON-like ciphers use bitwise AND operation as the nonlinear component. If the inputs of AND operation are independent, we can break the computation of differential probability into portions. After computing the probability of every component, we obtain the differential probability by multiplying them. However, the inputs of AND operation in SIMON-like ciphers are dependent on each other because they are both from the same input by rotation.

From the theorem given by Kölbl et al., the differential probability of SIMON-like round function $P(\alpha \mapsto \beta)$ depends only on the input difference α and the rotational constants a

and b, if $\alpha \mapsto \beta$ is a possible differential. So in our search algorithm, we can firstly compute the differential probability of one round. If the probability satisfies the search condition, then we go on finding all possible output differences and searching the next round.

As for searching for output differences, we firstly consider the differential property of AND operation with independent inputs. Inspired by the idea of S-box, we can break an n-bit AND operation into m t-bit AND operations (assume $n = mt$) and build the difference distribution table (DDT) of t-bit AND operation, which is defined as DDTA (difference distribution table of AND). In contrast to the DDT of S-box, the DDTA only stores the possible output differences whose probability aren't zero, because we only need output differences and don't care their probabilities − the probability of SIMON-like round function has been computed according to Theorem 1. Then, we turn the problem of searching for differential trails in SIMON-like ciphers into that in S-box based ciphers.

Next, we give the construction of DDTA and the method to compute the output difference of SIMON-like round function with DDTAs. The DDTA can be constructed with Algorithm 1.

Algorithm 1 Constructing t-bit DDTA

```
for $A,\ B = 0\ to\ 2^t - 1$ do
    $\Delta I = A||B$;
    $Num = 0$;
    for $\Gamma = 0\ to\ 2^t - 1$ do
        $\Delta O = \Gamma$;
        $flag = wt(\overline{A} \wedge \overline{B} \wedge \Gamma)$;
        if $flag = 0$ then
            $DDTA[\Delta I][Num] = \Delta O$;
            $Num = Num + 1$;
        end if
    end for
end for
```

Given an n-bit input difference α, we firstly compute $\alpha \lll a$ and $\alpha \lll b$, and then look up the m DDTAs to obtain the corresponding output differences. Concatenating the partial output differences, we get the output difference γ of AND operation. After that, we need to check whether α and γ satisfy the condition in Theorem 1. If so, we obtain an possible output difference $\beta = \gamma \oplus (\alpha \lll c)$ of SIMON-like round function.

To improve the efficiency, we apply Theorem 3 in the search algorithm. More specifically, we traverse plaintext differences from the difference with low Hamming weight, because the maximum differential probability of SIMON-like round function decreases as the Hamming weight of input difference increases. Once we find some plaintext difference whose maximum differential probability doesn't satisfy the search condition, that is $P_{max}B_{n-1} < \overline{B_n}$, we break the branch and needn't traverse the plaintext differences with higher Hamming weight.

Theorem 2 improved the bound from Theorem 1 for the case when the Hamming weight of input difference equals 2. Compared with Theorem 1, it can break the branch in advance in some cases. For example, when $\overline{B}_n = 2^{-2} \times B_{n-1}$, it needn't traverse input differences with Hamming weight of 2 for the first round, since the maximum probability is 2^{-3} according to Theorem 2. There is a similar case for the second round. Theorem 3 has a more practical application than Theorem 2 in the search algorithm. Because Theorem 3 improved the upper bound for the case when the Hamming weight is less than $n/2$, it can break the branch in advance in most cases, which improves the efficiency of the search algorithm significantly. The pseudo-code of our algorithm is listed in Algorithm 2.

In the following, we give a rough estimation of the complexity of the search algorithm.

Algorithm 2 Search for Optimal Differential 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 $\Delta X_1$ with $wt(\Delta X_1)$ from 0 to $n$, do the following:
    If $P_{max} \times B_{n-1} < \overline{B}_n$, then //$P_{max}$ is precomputed according to Theorem 3.
      Return to the upper procedure;
    Else
      Let $\alpha = \Delta X_1$ and $P_\alpha$ is computed according to Theorem 1;
      If $P_\alpha \times B_{n-1} \geq \overline{B}_n$, then
      Let $\mu = \alpha \lll a$, $\nu = \alpha \lll b$, $p_1 = P_\alpha$, and $\gamma$ is computed with DDTAs;
      $flag$ = Judge-Diff($\alpha, \gamma$);
      If $flag = true$, then
      Let $\beta = F(\alpha) = \gamma \oplus (\alpha \lll c)$, and Call Procedure Round-2;
  Return to the upper procedure;

Procedure Round-2:
  For each candidate for $\Delta X_2$ with $wt(\Delta X_2)$ from 0 to $n$, do the following:
    If $p_1 \times P_{max} \times B_{n-2} < \overline{B}_n$, then
      Return to the upper procedure;
    Else
      Let $\alpha = \Delta X_2$, and $P_\alpha$ is computed according to Theorem 1;
      If $p_1 \times P_\alpha \times B_{n-2} \geq \overline{B}_n$, then
      Let $\mu = \alpha \lll a$, $\nu = \alpha \lll b$, $p_2 = P_\alpha$, and $\gamma$ is computed with DDTAs;
      $flag$ = Judge-Diff($\alpha, \gamma$);
      If $flag = true$, then
      Let $\beta = F(\alpha) = \gamma \oplus (\alpha \lll c)$, and Call Procedure Round-3;
  Return to the upper procedure;

Procedure Round-$i$ ($3 \leq i \leq n-1$):
  Let $\Delta X_i = \Delta X_{i-2} \oplus F(\Delta X_{i-1})$;
  Let $\alpha = \Delta X_i$, and $P_\alpha$ is computed according to Theorem 1;
  If $p_1 \times \cdots \times p_{i-1} \times P_\alpha \times B_{n-i} \geq \overline{B}_n$, then
  Let $\mu = \alpha \lll a$, $\nu = \alpha \lll b$, $p_i = P_\alpha$, and $\gamma$ is computed with DDTAs;
  $flag$ = Judge-Diff($\alpha, \gamma$);
  If $flag = true$, then
  Let $\beta = F(\alpha) = \gamma \oplus (\alpha \lll c)$, and Call Procedure Round-($i+1$);
  Return to the upper procedure;

Procedure Round-$n$:
  Let $\Delta X_n = \Delta X_{n-2} \oplus F(\Delta X_{n-1})$;
  Let $\alpha = \Delta X_n$, and $P_\alpha$ is computed according to Theorem 1;
  If $p_1 \times \cdots \times p_{n-1} \times P_\alpha = \overline{B}_n$, then $B_n = \overline{B}_n$;
  Return to the upper procedure;

bool Judge-Diff($\alpha$, $\gamma$) //A function to judge the differential condition in Theorem 1.
  If $\alpha = 2^n - 1$ then
    If $wt(\gamma) \equiv 0 \; mod \; 2$, then return true;
  Else
    Let $varibits = (\alpha \lll a) \vee (\alpha \lll b)$;
    Let $doublebits = (\alpha \lll b) \wedge \overline{(\alpha \lll a)} \wedge (\alpha \lll (2a - b))$;
    If $\gamma \wedge \overline{varibits} = 0_n$ and $(\gamma \oplus (\gamma \lll (a-b))) \wedge doublebits = 0_n$, then return true;
  Return false;
```

Let m_1 be the number of differences α_1 and β_1 in the first round, where $m_1 = \#\{(\alpha_1, \beta_1) \mid P_{max}(\alpha_1 \mapsto \beta_1) \geq \overline{B}_n/B_{n-1}\}$. Analogously, let m_2 be the number of differences α_2 and β_2 in the second round, where $m_2 = \#\{(\alpha_2, \beta_2) \mid P_{max}(\alpha_2 \mapsto \beta_2) \geq \overline{B}_n/(p_1 B_{n-2})\}$. 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 differential probability P_{max} decreases with the Hamming weight of input differences increasing, it only searches a very small fraction of all the possible plaintext differences, 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 3, n and $a - b$ must satisfy $\gcd(n, a - b) = 1$. We implicitly assume this condition is satisfied in SIMON-like ciphers, and therefore we can apply Theorem 1 and Theorem 3 in the search algorithm and find optimal differential trails in SIMON-like ciphers efficiently. Our algorithm can also be extended to other constructions which use $f(x) = x \wedge (x \lll a)$ as the only nonlinear component, because the differential probability is computed according to Theorem 1 in our search algorithm.As for the size of the DDTA, it can be any number only if it can divide the word size n. In our experiments, we use 8-bit DDTA tables (taking tradeoff of time and memory).

Remark 1. Traversing the plaintext differences from low to high Hamming weight is the main reason that our algorithm can be applicable to SIMON-like ciphers with large block size such as 96 and 128 bits. This observation can also be applied to other ciphers when the differential probability of round function and the Hamming weight of its input differences have monotonic relationship. However, as for ciphers with block size larger than 128 bits, our algorithm can find optimal differential trails on round-reduced variants, but may not obtain the trail reaching the security bound. Because it need traverse more candidates of the plaintext difference. Furthermore, the differential probability reaching the security bound becomes smaller and the corresponding trail covers more rounds, then it needs more time to find the optimal trail. In such cases, one possible solution is to perform a parallel version of the algorithm. Another possible solution is to restrict the Hamming weight of the plaintext differences. It can find a longer differential trail, but may not obtain the optimal differential trail.

5 Differential Trails and Differentials for SIMON and SIMECK

In this section, we apply Algorithm 2 to search for optimal differential trails for block ciphers SIMON and SIMECK [1]. The differential trails found by our algorithm are optimal under the Markov assumption. Besides the optimal differential trails, we also find the differentials for SIMON and SIMECK.

5.1 Differential Trails for SIMON and SIMECK

For SIMON with block size 32, 48, 64, 96 and 128 bits, the optimal differential trails found cover 12, 16, 19, 28 and 37 rounds with probability 2^{-34}, 2^{-50}, 2^{-64}, 2^{-96} and 2^{-128} respectively. We find the provably optimal differential trails for all versions of SIMON, which 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. [KLT15]. The probabilities of optimal differential trails for SIMON are shown in Table 2, and the optimal differential trails found are shown in Table 6 and Table 7 in Appendix B.

[1] All experiments are performed on a PC with a single core (Intel® Core$^{\text{TM}}$ i5 – 4570 CPU 3.2GHz).

Table 2: Probabilities of the optimal differential trails for SIMON. The probabilities are given as log_2p. The column "time" provides the time needed to find a single optimal differential trail in seconds or hours ("s" and "h" for short).

	SIMON32		SIMON48		SIMON64		SIMON96		SIMON128	
R	*Prob*	*time*	*Prob*	*time*	*Prob*	*time*	*Prob*	*time*	*Prob*	*time*
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	0.00s	−4	0.00s	−4	0.00s	−4	0.00s	−4	0.00s
4	−6	0.00s	−6	0.00s	−6	0.00s	−6	0.02s	−6	0.02s
5	−8	0.00s	−8	0.01s	−8	0.01s	−8	0.02s	−8	80.02s
6	−12	0.02s	−12	0.13s	−12	0.09s	−12	1.48s	−12	2.46s
7	−14	0.01s	−14	0.10s	−14	0.07s	−14	1.30s	−14	2.24s
8	−18	0.04s	−18	0.29s	−18	0.16s	−18	1.98s	−18	3.02s
9	−20	0.01s	−20	0.12s	−20	0.08s	−20	1.23s	−20	2.29s
10	−25	0.54s	−26	17.03s	−26	8.84s	−26	172.99s	−26	302.58s
11	−30	17.31s	−30	238.73s	−30	103.72s	−30	2.04h	−30	4.32h
12	−34	24.57s	−35	513.99s	−36	0.28h	−36	6.01h	−36	9.16h
13			−38	139.28s	−38	6.90s	−38	111.13s	−38	211.23s
14			−44	4.25h	−44	0.64h	−44	3.92h	−44	3.50h
15			−46	97.64s	−48	0.69h	−48	6.43h	−48	7.78h
16			−50	0.60h	−54	44.44h	−54	288.95h	−54	242.34h
17					−56	341.90s	−56	0.49h	−56	0.44h
18					−62	105.23h	−62	528.38h	−62	550.73h
19					−64	25.92s	−64	145.78s	−64	128.50s
20							−66	33.91s	−66	27.09s
21							−68	1.56s	−68	1.19s
22							−72	365.75s	−72	298.55s
23							−74	1.06s	−74	2.05s
24							−78	12.04s	−78	11.40s
25							−80	1.15s	−80	2.15s
26							−86	312.4s	−86	442.92s
27							−90	1.93h	−90	5.68h
28							−96	5.90h	−96	11.37h
29									−98	221.93s
30									−104	3.02h
31									−108	8.64h
32									−114	221.91h
33									−116	0.64h
34									−122	516.32h
35									−124	160.95s
36									−126	35.13s
37									−128	2.08s

For SIMECK with block size 32, 48 and 64 bits, we find the provably optimal differential trails for up to 13, 19 and 25 rounds with probability 2^{-32}, 2^{-48} and 2^{-64} respectively. We confirm the optimal differential trails given by Kölbl et al. [KR15], but our algorithm is more efficient than their algorithm. The probabilities of optimal differential trails for SIMECK are shown in Table 3, and the optimal differential trails found are shown in Table 8 in Appendix C.

Table 3: Probabilities of the optimal differential trails for SIMECK. The probabilities are given as $log_2 p$. The column "time" provides the time needed to find a single optimal differential trail in seconds ("s" for short).

	SIMECK32		SIMECK48		SIMECK64	
R	$Prob$	$time$	$Prob$	$time$	$Prob$	$time$
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	$0.01s$
4	-6	$0.01s$	-6	$0.02s$	-6	$0.02s$
5	-8	$0.01s$	-8	$0.02s$	-8	$0.02s$
6	-12	$0.08s$	-12	$0.58s$	-12	$0.40s$
7	-14	$0.05s$	-14	$0.44s$	-14	$0.40s$
8	-18	$0.21s$	-18	$1.46s$	-18	$0.86s$
9	-20	$0.08s$	-20	$0.60s$	-20	$0.38s$
10	-24	$0.44s$	-24	$1.76s$	-24	$0.83s$
11	-26	$0.07s$	-26	$0.25s$	-26	$0.11s$
12	-30	$0.83s$	-30	$3.89s$	-30	$1.92s$
13	-32	$0.05s$	-32	$0.21s$	-32	$0.12s$
14			-36	$5.33s$	-36	$2.84s$
15			-38	$0.59s$	-38	$0.47s$
16			-44	$223.07s$	-44	$117.22s$
17			-44	$0.01s$	-44	$0.00s$
18			-46	$0.00s$	-46	$0.00s$
19			-48	$0.01s$	-48	$0.00s$
20					-50	$0.02s$
21					-52	$0.01s$
22					-56	$0.40s$
23					-58	$0.32s$
24					-62	$0.70s$
25					-64	$0.34s$

Compared with the approach based on SAT/SMT solvers in [KLT15] and [KR15], our algorithm is a more efficient algorithm. It is efficient to find optimal differential trails for SIMON-like ciphers with block size less than or equal to 64 bits. As for SIMON-like ciphers with large block size such as 96 and 128 bits, our algorithm can also find the optimal differential trails. To the best of our knowledge, it is the first algorithm that finds the optimal differential trails for SIMON96 and SIMON128 in the public literature. Besides evaluating the security of SIMON-like ciphers against differential cryptanalysis, our algorithm has a more practical use in the design of SIMON-like ciphers.

5.2 Differentials for SIMON and SIMECK

Besides the optimal differential trails, we also find the differentials for SIMON and SIMECK. Firstly, we apply Algorithm 2 to find some differential trails. Secondly, we start from the input difference of the differential trail and search for the possible differential trails leading to the same output difference. Then, we add their probabilities to obtain the probability of the differential.

For SIMON with block size 32, 48, 64, 96 and 128 bits, we find the 14, 17, 23, 31 and 41-round differentials with probabilities $2^{-30.76}$, $2^{-46.38}$, $2^{-61.93}$, $2^{-95.34}$ and $2^{-123.74}$ respectively. As for SIMECK with block size 32, 48 and 64 bits, the 14, 21 and 27-round differentials are found, with probabilities $2^{-31.64}$, $2^{-45.28}$ and $2^{-61.49}$ respectively. To the best of our knowledge, these are the best differential distinguishers for SIMON and SIMECK so far. The differentials for SIMON and SIMECK are shown in Table 4 and Table 5. In these tables, (X_L, X_R) and (Y_L, Y_R) represent the input difference and output difference respectively, where X_L and X_R are the left and right half of the input difference respectively.

Table 4: The differentials for SIMON.

Block Size	Round	Input active bits	Output active bits	Probability	Reference
32	14	$X_{R,3}$	$Y_{L,11}$	$2^{-30.81}$	[KLT15]
	14	$X_{R,0}$	$Y_{L,10}, Y_{R,8}$	$2^{-30.76}$	this paper
48	17	$X_{L,7}, X_{R,1}, X_{R,5}, X_{R,9}$	$Y_{L,1}, Y_{L,5}, Y_{L,9}, Y_{R,7}$	$2^{-46.32}$	[KLT15]
	17	$X_{L,0}, X_{R,2}, X_{R,18}, X_{R,22}$	$Y_{L,2}, Y_{L,18}, Y_{L,22}, Y_{R,0}$	$2^{-46.38}$	this paper
64	22	$X_{L,6}, X_{L,10}, X_{R,7}, X_{R,11}, X_{R,12}$	$Y_{L,6}, Y_{L,10}, Y_{R,8}$	$2^{-61.32}$	[KLT15]
	23	$X_{L,0}, X_{R,2}, X_{R,30}$	$Y_{L,2}, Y_{L,6}, Y_{L,30}, Y_{R,4}$	$2^{-61.93}$	this paper
96	30	$X_{L,20}, X_{R,6}, X_{R,14}, X_{R,18}, X_{R,22}$	$Y_{L,8}, Y_{L,16}, Y_{R,6}, Y_{R,10}, Y_{R,14}$	$2^{-92.2}$	[ALLW14]
	31	$X_{L,14}, X_{R,0}, X_{R,8}, X_{R,12}, X_{R,16}$	$Y_{L,0}, Y_{L,8}, Y_{L,12}, Y_{R,2}, Y_{R,10}$	$2^{-95.34}$	this paper
128	41	$X_{L,12}, X_{R,6}, X_{R,10}, X_{R,14}$	$Y_{L,6}, Y_{L,10}, Y_{L,14}, Y_{R,12}$	$2^{-124.6}$	[ALLW14]
	41	$X_{L,6}, X_{R,0}, X_{R,4}, X_{R,8}$	$Y_{L,0}, Y_{L,4}, Y_{L,8}, Y_{R,6}$	$2^{-123.74}$	this paper

Table 5: The differentials for SIMECK.

Block Size	Round	Input active bits	Output active bits	Probability	Reference
32	13	$X_{L,15}, X_{R,0}, X_{R,4}, X_{R,14}$	$Y_{L,14}$	$2^{-27.28}$	[KR15]
	14	$X_{L,0}, X_{R,1}, X_{R,3}, X_{R,15}$	$Y_{L,2}, Y_{R,1}, Y_{R,15}$	$2^{-31.64}$	this paper
48	21	$X_{L,17}, X_{R,16}, X_{R,17}, X_{R,18}, X_{R,22}$	$Y_{L,16}, Y_{L,18}, Y_{R,17}$	$2^{-45.65}$	[KR15]
	21	$X_{L,0}, X_{R,1}, X_{R,23}$	$Y_{L,1}, Y_{L,23}, Y_{R,0}$	$2^{-45.28}$	this paper
64	26	$X_{R,22}, X_{R,26}$	$Y_{L,23}, Y_{L,27}, Y_{R,22}$	$2^{-60.02}$	[KR15]
	27	$X_{R,0}, X_{R,4}$	$Y_{L,0}, Y_{L,2}, Y_{R,1}$	$2^{-61.49}$	this paper

6 Conclusion

In this paper, we derive a more accurate upper bound on the differential probability of SIMON-like round function. Based on this, we adapt Matsui's algorithm and propose an efficient automatic search algorithm for optimal differential trails in SIMON-like ciphers. We use the block ciphers SIMON and SIMECK as a test platform for demonstrating the practical application of our algorithm. With the proposed algorithm, we find the provably optimal differential trails for all versions of block ciphers SIMON and SIMECK, and report the optimal differential trails for SIMON64, SIMON96 and SIMON128 for the first time. Besides the optimal differential trails, we also find the best differentials for SIMON and SIMECK so far.

We hope that the algorithm proposed in this paper is helpful for evaluating the security of SIMON-like ciphers against differential cryptanalysis, and also useful in the design of SIMON-like ciphers.

Acknowledgements

The authors are very grateful to Dr. Jian Guo and the anonymous reviewers for their valuable comments. This work was supported by the 973 project under Grant (2013CB834203), by the National Science Foundation of China (No.61379142).

References

[AAA+14] Javad Alizadeh, Hoda AlKhzaimi, Mohammad Reza Aref, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar, Martin M. Lauridsen, and Somitra Kumar 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.

[AL13] Hoda AlKhzaimi and Martin M. Lauridsen. Cryptanalysis of the SIMON family of block ciphers. *IACR Cryptology ePrint Archive*, 2013:543, 2013.

[ALLW14] Farzaneh Abed, Eik List, Stefan Lucks, and Jakob 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.

[BBF15] Arnaud Bannier, Nicolas Bodin, and Eric Filiol. Automatic search for a maximum probability differential characteristic in a substitution-permutation network. In *48th Hawaii International Conference on System Sciences, HICSS 2015, Kauai, Hawaii, USA, January 5-8, 2015*, pages 5165–5174, 2015.

[BCG+12] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga 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.

[BDF11] Charles Bouillaguet, Patrick Derbez, and Pierre-Alain Fouque. Automatic search of attacks on round-reduced AES and applications. In *Advances in*

Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings, pages 169–187, 2011.

[Bei16] Christof 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.

[BKL$^+$07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick 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.

[BN10] Alex Biryukov and Ivica Nikolic. Automatic search for related-key differential characteristics in byte-oriented block ciphers: Application to AES, camellia, khazad and others. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, pages 322–344, 2010.

[BN11] Alex Biryukov and Ivica Nikolic. Search for related-key differential characteristics in DES-like ciphers. In *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, pages 18–34, 2011.

[BRV14] Alex Biryukov, Arnab Roy, and Vesselin 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.

[BSS$^+$13] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. *IACR Cryptology ePrint Archive*, 2013:404, 2013.

[BV14] Alex Biryukov and Vesselin 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.

[BZL14] Zhenzhen Bao, Wentao Zhang, and Dongdai Lin. Speeding up the search algorithm for the best differential and best linear trails. In *Information Security and Cryptology - 10th International Conference, Inscrypt 2014, Beijing, China, December 13-15, 2014, Revised Selected Papers*, pages 259–285, 2014.

[CDK09] Christophe De Cannière, Orr Dunkelman, and Miroslav 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.

[CMS$^+$14] Nicolas Courtois, Theodosis Mourouzis, Guangyan Song, Pouyan Sepehrdad, and Petr 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.

[CW16] Huaifeng Chen and Xiaoyun 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.

[CWW15] Zhan Chen, Ning Wang, and Xiaoyun Wang. Impossible differential cryptanalysis of reduced round SIMON. *IACR Cryptology ePrint Archive*, 2015:286, 2015.

[GNL11] Zheng Gong, Svetla Nikova, and Yee Wei 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.

[GPPR11] Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew 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.

[HSH$^+$06] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, Donghoon Chang, Jaesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek 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.

[ISSK09] Maryam Izadi, Babak Sadeghiyan, Seyed Saeed Sadeghian, and Hossein Arabnezhad 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.

[KLT15] Stefan Kölbl, Gregor Leander, and Tyge 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.

[KR15] Stefan Kölbl and Arnab Roy. A brief comparison of Simon and Simeck. *IACR Cryptology ePrint Archive*, 2015:706, 2015.

[KSI16] Kota Kondo, Yu Sasaki, and Tetsu Iwata. On the design rationale of simon block cipher: Integral attacks and impossible differential attacks against simon variants. In *Applied Cryptography and Network Security - 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings*, pages 518–536, 2016.

[LK05] Chae Hoon Lim and Tymur 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.

[LPPS07] Gregor Leander, Christof Paar, Axel Poschmann, and Kai Schramm. New lightweight DES variants. In *Fast Software Encryption, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers*, pages 196–210, 2007.

[Mat94] Mitsuru 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.

[MWGP11] Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In *Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers*, pages 57–76, 2011.

[OKJL09] Shrikant Ojha, Naveen Kumar, Kritika Jain, and Sangeeta Lal. TWIS - A lightweight block cipher. In *Information Systems Security, 5th International Conference, ICISS 2009, Kolkata, India, December 14-18, 2009, Proceedings*, pages 280–291, 2009.

[PLSP07] Axel Poschmann, Gregor Leander, Kai Schramm, and Christof Paar. New lightweight crypto algorithms for RFID. In *International Symposium on Circuits and Systems (ISCAS 2007), 27-20 May 2007, New Orleans, Louisiana, USA*, pages 1843–1846, 2007.

[SHW+14] Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song. Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, pages 158–178, 2014.

[SIH+11] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo 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.

[SMMK12] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita 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.

[SPGQ06] François-Xavier Standaert, Gilles Piret, Neil Gershenfeld, and Jean-Jacques 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.

[SSA+07] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu 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.

[TM16] Yosuke Todo and Masakatu Morii. Bit-based division property and application to simon family. In *Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*, pages 357–377, 2016.

[WLV+14] Qingju Wang, Zhiqiang Liu, Kerem Varici, Yu Sasaki, Vincent Rijmen, and Yosuke 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.

[WWJZ14] Ning Wang, Xiaoyun Wang, Keting Jia, and Jingyuan Zhao. Differential attacks on reduced SIMON versions with dynamic key-guessing techniques. *IACR Cryptology ePrint Archive*, 2014:448, 2014.

[WZ11] Wenling Wu and Lei 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.

[YZS+15] Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, and Guang 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.

A Proof of Theorem 3

Proof. The case of $wt(\alpha) = n$ is obvious according to Theorem 1, and the case of $n/2 \leq wt(\alpha) < n$ can also be obtained easily from Theorem 1. To make it clear, we give a proof as follows.

Suppose $wt(\alpha) < n$. Let vt and dt be the *varibits* and *doublebits* that are defined in Theorem 1. For an n-bit vector $v := [v_{n-1}, v_{n-2}, \ldots, v_0] \in \mathbb{F}_2^n$, and $c \in \mathbb{F}_2$, let

$$S(v, c) = \{i \mid v_i = c, 0 \leq i \leq n-1\}.$$

Note that $S(dt, 1) \subseteq S(\alpha \lll b, 1) \subseteq S(vt, 1)$, then $wt(vt \oplus dt) = |S(vt, 1)| - |S(dt, 1)|$. Therefore, according to Theorem 1, we have

$$P_\alpha = 2^{-wt(dt \oplus vt)} = 2^{|S(dt,1)| - |S(vt,1)|}.$$

Note that $S(\alpha \lll a, 1) \subseteq S(vt, 1)$, and $S(\alpha \lll a, 1) \subseteq S(dt, 0)$, then

$$S(\alpha \lll a, 1) \subseteq (S(vt, 1) \setminus S(dt, 1)),$$

from which we get $|S(dt, 1)| - |S(vt, 1)| \leq -|S(\alpha \lll a, 1)| = -wt(\alpha)$. Then

$$P_\alpha \leq 2^{-wt(\alpha)}$$

when $wt(\alpha) < n$. This proves the case (2).

Next, we claim that when $1 \leq wt(\alpha) < \frac{n}{2}$, it always holds that

$$\mathcal{X} := S(\alpha \lll b, 1) \cap S(\alpha \lll a, 0) \cap S(\alpha \lll (2a-b), 0) \neq \emptyset.$$

Note that

$$\begin{aligned} S(\alpha \lll a, 0) &= \{i \mid 0 \leq i \leq n-1\} \setminus \{(i + (a-b)) \mod n \mid i \in S(\alpha \lll b, 1)\}, \\ S(\alpha \lll 2a-b, 0) &= \{i \mid 0 \leq i \leq n-1\} \setminus \{(i + 2(a-b)) \mod n \mid i \in S(\alpha \lll b, 1)\}, \end{aligned}$$

then it is equivalent to prove that there exists $e \in S(\alpha \lll b, 1)$, such that

$$(e-k) \mod n \notin S(\alpha \lll b, 1) \text{ and } (e-2k) \mod n \notin S(\alpha \lll b, 1),$$

where $k = a - b$.

Let $\mathcal{S} = S(\alpha \lll b, 1)$, $w = |\mathcal{S}| = wt(\alpha)$. Assume the claim does not hold, then for any $e \in \mathcal{S}$, there exists $d \in \{1, 2\}$, such that

$$e - dk \in \mathcal{S},$$

where $e - dk$ denotes $(e - dk) \mod n$ for simplicity. Suppose $e_0 \in \mathcal{S}$. Using the above statement recursively, we get that there exists $d_i \in \{1, 2\}, 1 \le i \le w - 1$, such that

$$\{e_0, e_0 - d_1k, e_0 - (d_1 + d_2)k, \cdots, e_0 - (d_1 + \cdots + d_{w-1})k\} \subseteq \mathcal{S}.$$

Note that $\gcd(k, n) = 1$, then $j_1k = j_2k \mod n$ if and only if $j_1 = j_2 \mod n$. Since $0 < d_1 < d_1 + d_2 < \cdots < d_1 + \cdots + d_{w-1} \le 2(w - 1) < n - 2$, we get that

$$e_0, e_0 - d_1k, e_0 - (d_1 + d_2)k, \cdots, e_0 - (d_1 + \cdots + d_{w-1})k$$

are pairwise different. Because of $|\mathcal{S}| = w$, it holds

$$\mathcal{S} = \{e_0, e_0 - d_1k, e_0 - (d_1 + d_2)k, \cdots, e_0 - (d_1 + \cdots + d_{w-1})k\}.$$

Then from $e_0 - \sum_{i=1}^{w-1} d_ik \in \mathcal{S}$, we deduce that there exists $d_w \in \{1, 2\}$, such that

$$e_0 - (d_1 + \cdots + d_{w-1})k - d_wk \in \mathcal{S}.$$

This means $\sum_{i=1}^{w} d_ik = \sum_{i=1}^{j} d_ik \mod n$ for some $0 \le j \le w - 1$, where $\sum_{i=1}^{0} d_i$ is defined as 0. Hence $\sum_{i=1}^{w} d_i = \sum_{i=1}^{j} d_i \mod n$ since $\gcd(n, k) = 1$. However, note that

$$0 < d_1 < d_1 + d_2 < \cdots < \sum_{i=1}^{w-1} d_i < \sum_{i=1}^{w} d_i \le 2w < n.$$

Thus we have $\sum_{i=1}^{w} d_i \ne \sum_{i=1}^{j} d_i \mod n$ for any $0 \le j \le w - 1$, and hence the claim holds.

Therefore, we have $|\mathcal{X}| \ge 1$. Note that $\mathcal{X} \cap S(\alpha \lll a, 1) = \emptyset$ and

$$\mathcal{X} \cup S(\alpha \lll a, 1) \subseteq (S(vt, 1) \setminus S(dt, 1)),$$

then it holds

$$|S(dt, 1)| - |S(vt, 1)| \le -(|S(\alpha \lll a, 1)| + |\mathcal{X}|) \le -wt(\alpha) - 1,$$

and we complete the proof. □

B Differential Trails for SIMON

Table 6: Differential trails for SIMON32, SIMON48 and SIMON64

	SIMON32			SIMON48			SIMON64		
R	ΔL	ΔR	$log_2 p$	ΔL	ΔR	$log_2 p$	ΔL	ΔR	$log_2 p$
0	1	4404	−0	1	400004	−0	0	1	−0
1	4400	1	−2	400000	1	−2	1	0	−0
2	1000	4400	−4	0	400000	−2	4	1	−2
3	400	1000	−2	400000	0	−0	11	4	−2
4	0	400	−2	41	400000	−2	40	11	−4
5	400	0	−0	404004	41	−4	111	40	−2
6	1000	400	−2	410410	404004	−6	404	111	−6
7	4400	1000	−2	404004	410410	−8	1101	404	−4
8	1	4400	−4	41	404004	−6	4300	1101	−6
9	4404	1	−2	400000	41	−4	1901	4300	−6
10	1010	4404	−6	0	400000	−2	404	1901	−8
11	444	1010	−4	400000	0	−0	111	404	−4
12				1	400000	−2	40	111	−6
13				400004	1	−2	11	40	−2
14				10	400004	−4	4	11	−4
15				400044	10	−2	1	4	−2
16							0	1	−2
17							1	0	−0
18							4	1	−2
19							11	4	−2
$\sum_r log_2 p_r$	−30			−46			−64		

Table 7: Differential trails for SIMON96 and SIMON128

	SIMON96			SIMON128		
R	ΔL	ΔR	log_2p	ΔL	ΔR	log_2p
0	1	440000000004	−0	1	4000000000000004	−0
1	440000000000	1	−2	4000000000000000	1	−2
2	100000000000	440000000000	−4	0	4000000000000000	−2
3	40000000000	100000000000	−2	4000000000000000	0	−0
4	0	40000000000	−2	1	4000000000000000	−2
5	40000000000	0	−0	4000000000000004	1	−2
6	100000000000	40000000000	−2	10	4000000000000004	−4
7	440000000000	100000000000	−2	4000000000000044	10	−2
8	1	440000000000	−4	101	4000000000000044	−6
9	440000000004	1	−2	4000000000000440	101	−4
10	100000000010	440000000004	−6	10c0	4000000000000440	−6
11	40000000044	100000000010	−4	4000000000000640	10c0	−6
12	10c	40000000044	−6	101	4000000000000640	−8
13	40000000064	10c	−6	4000000000000044	101	−4
14	100000000010	40000000064	−8	10	4000000000000044	−6
15	440000000004	100000000010	−4	4000000000000004	10	−2
16	1	440000000004	−6	1	4000000000000004	−4
17	440000000000	1	−2	4000000000000000	1	−2
18	100000000000	440000000000	−4	0	4000000000000000	−2
19	40000000000	100000000000	−2	4000000000000000	0	−0
20	0	40000000000	−2	1	4000000000000000	−2
21	40000000000	0	−0	4000000000000004	1	−2
22	100000000000	40000000000	−2	10	4000000000000004	−4
23	440000000000	100000000000	−2	4000000000000044	10	−2
24	1	440000000000	−4	101	4000000000000044	−6
25	440000000004	1	−2	4000000000000440	101	−4
26	100000000010	440000000004	−6	10c0	4000000000000440	−6
27	40000000044	100000000010	−4	4000000000000640	10c0	−6
28	100	40000000044	−6	101	4000000000000640	−8
29				4000000000000044	101	−4
30				10	4000000000000044	−6
31				4000000000000004	10	−2
32				1	4000000000000004	−4
33				4000000000000000	1	−2
34				0	4000000000000000	−2
35				4000000000000000	0	−0
36				1	4000000000000000	−2
37				4000000000000004	1	−2
$\sum_r log_2p_r$	−96			−128		

C Differential Trails for SIMECK

Table 8: Differential trails for SIMECK32, SIMECK48 and SIMECK64

	SIMECK32			SIMECK48			SIMECK64		
R	ΔL	ΔR	log_2p	ΔL	ΔR	log_2p	ΔL	ΔR	log_2p
0	0	11	−0	0	1	−0	1	a0000002	−0
1	11	0	−0	1	0	−0	a0000000	1	−2
2	2	11	−4	2	1	−2	40000000	a0000000	−4
3	15	2	−2	5	2	−2	20000000	40000000	−2
4	8	15	−6	8	5	−4	0	20000000	−2
5	5	8	−2	15	8	−2	20000000	0	−0
6	2	5	−4	2	15	−6	40000000	20000000	−2
7	1	2	−2	11	2	−2	a0000000	40000000	−2
8	0	1	−2	0	11	−4	1	a0000000	−4
9	1	0	−0	11	0	−0	a0000002	1	−2
10	2	1	−2	2	11	−4	40000000	a0000002	−6
11	5	2	−2	15	2	−2	20000002	40000000	−2
12	8	5	−4	8	15	−6	0	20000002	−4
13	15	8	−2	5	8	−2	20000002	0	−0
14				2	5	−4	40000000	20000002	−4
15				1	2	−2	a0000002	40000000	−2
16				0	1	−2	1	a0000002	−6
17				1	0	−0	a0000000	1	−2
18				2	1	−2	40000000	a0000000	−4
19				5	2	−2	20000000	40000000	−2
20							0	20000000	−2
21							20000000	0	−0
22							40000000	20000000	−2
23							a0000000	40000000	−2
24							1	a0000000	−4
25							a0000002	1	−2
$\sum_r log_2p_r$	−32			−48			−64		