Improved Differential Attacks on Reduced SIMON Versions ⋆

Ning Wang[1,2], Xiaoyun Wang[1,2,3⋆⋆], Keting Jia[4], and Jingyuan Zhao[1,2]

[1] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
[2] School of Mathematics, Shandong University, Jinan 250100, China
[3] Institute for Advanced Study, Tsinghua University, Beijing 100084, China
xiaoyunwang@mail.tsinghua.edu.cn
[4] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

Abstract. SIMON is a family of lightweight block ciphers which are designed by the U.S National Security Agency in 2013. In this paper, we improve the previous differential attacks on SIMON family of block ciphers by considering some bit-difference equations. Combining with some new observations on key guess policies of SIMON family, we mount differential attacks on 21-round SIMON32/64, 22-round SIMON48/72, 22-round SIMON48/96, 28-round SIMON64/96 and SIMON64/128 with time complexity about 2^{46}, 2^{63}, 2^{71}, 2^{60} and 2^{60} encryptions respectively. As far as we know, these results are the best attacks on reduced-round SIMON versions.

Keywords: SIMON, lightweight block cipher, differential attack

1 Introduction

Today, lightweight block ciphers for resource-constrained applications such as RFID tags and sensor networks have received much attention. During the last decade, many lightweight ciphers have been proposed, such as PRESENT[9], LED[12], PRINCE[10], KANTAN[11] and CLEFIA[18] etc.

In 2013, NSA published the specifications of lightweight block cipher families SIMON and SPECK. Compared to the other existing lightweight block ciphers, these two families have the competitive performance for both hardware and software implementations which can be used to the extremely resource-constrained devices.

Differential cryptanalysis[6] firstly introduced by Biham et al is a popular attack on block ciphers. Over the years, differential cryptanalysis has been developed numerous variants that were used to analyze many primitives of block ciphers. Higher order differential cryptanalysis was introduced by Lai in 1994. In the same year, Knudsen introduced truncated differentials[16] to analyze the block cipher DES. In 1998, Knudsen[15] and Biham et al.[4] independently proposed the idea of impossible-differential attacks, which allow the adversary to filter out wrong keys by distinguishing the impossible differential characteristics. To construct a long distinguisher by connecting two short differential characteristic, Wagner proposed the boomerang attack in 1999 [19], which was extended by Kelsey et al. as amplified boomerang attack[13], and independently introduced by Biham et al. as rectangle attack[5]. Lately, Blondeau et al. introduced multiple differential cryptanalysis with multiple input differences and multiple output differences to attack reduced PRESENT [8].

Related Works In this paper, we only focus on the differential attacks on SIMON family. SIMON family has 10 versions depending on the state size (block size) $2n$ and key length l_k, named as SIMON$2n/l_k$. There is only an instance for 32-bit state size, i.e. SIMON32/64, two instances for 48-, 64-, 96-bit state sizes, and 3 instances for 128-bit state size. After its announcement, SIMON family attracts a lot attention of cryptanlists soon. Alkhzaimi and Lauridsen[2]

⋆ Supported by National Key Basic Research Program of China (Grant No. 2013CB834205), and the National Natural Science Foundation of China (Grant No. 61133013).
⋆⋆ Corresponding author.

gave the differential attacks on five reduced versions of SIMON with 16, 18, 24, 29, and 40 rounds corresponding to five state sizes respectively. They also showed the impossible-differential attacks on 14, 15, 16, 19, and 22 rounds of the corresponding versions. Biryukov and Velichkov [7] found the differential characteristics up to 13, 15 and 21 rounds of SIMON which can be used to attack the corresponding reduced versions of 32-, 48- and 64-bit state sizes. As a result, 19-round SIMON32/64, 20-round SIMON48/72, 20-round SIMON48/96, 26-round SIMON64/96 and 26-round SIMON64/128 can be attacked with about 2^{32}, 2^{52}, 2^{75}, 2^{89} and 2^{121} encryptions, respectively. In addition, Farzaneh Abed and Eik List[1] presented differential attacks up to 18, 19, 26, 35 and 46 rounds for SIMON with 5 versions, respectively.

Our Contribution In this paper, we investigate some important bitwise behavior of the existing differentials of SIMON versions, and obtain many bit conditions available to enlarge the differentials path with 3 or 4 rounds on the top. Especially, some bit conditions are dependent on secret key bits, which motivate us to explore new key bits guess strategies. Based on these bit conditions and key bits guess policies, we fulfill the differential attack on the reduced SIMON with 32, 48, and 64 state size versions. Our attacks work on these reduced versions with 1 to 2 more rounds than the previous attacks. Because the main part of our attack reveals how to control bit equations relating to key bits, we call our attack as bit differential attack. As a result, we present several differential attacks on 20-round SIMON32/64, 21-round SIMON32/64, 21-round SIMON48, 22-round SIMON48/72, 22-round SIMON48/96 and 28-round SIMON64 with the time complexity of 2^{31}, 2^{46}, 2^{50}, 2^{63}, 2^{71} and 2^{60} encryptions, respectively. Our results are summarized and compared to the previous results in Table 1.

The rest of this paper is organized as follows. We list some notations, give a brief description of block cipher SIMON and show some observations available in the differential attack in section 2. Section 3 presents the differential attacks on 20 and 21-round SIMON32. The differential cryptanalysis of 21 and 22-round SIMON48 are described in section 4. We introduced the differential attack on 28-round SIMON64 in section 5. Finally, we conclude this paper in section 6.

Table 1. Summary of Attacks on SIMON

Cipher	Key Size	Total Rounds	Attacked Rounds	Time	Data	Reference
SIMON32	64	32	18	2^{46}	$2^{31.2}$	[1]
			19	2^{32}	2^{31}	[7]
			20	2^{31}	2^{31}	Section 3
			21	2^{46}	2^{31}	Section 3
SIMON48	72	36	19	2^{52}	2^{46}	[1]
			20	2^{52}	2^{46}	[7]
			21	2^{50}	2^{45}	Section 4
			22	2^{63}	2^{45}	Section 4
SIMON48	96	36	19	2^{76}	2^{46}	[1]
			20	2^{75}	2^{46}	[7]
			21	2^{50}	2^{45}	Section 4
			22	2^{71}	2^{45}	Section 4
SIMON64	96	42	26	2^{94}	2^{63}	[1]
			26	2^{89}	2^{63}	[7]
			28	2^{60}	2^{59}	Section 5
SIMON64	128	44	26	2^{126}	2^{63}	[1]
			26	2^{121}	2^{63}	[7]
			28	2^{60}	2^{59}	Section 5

2 Brief Description of SIMON

2.1 Notations

The following notations are used in this paper:

X_r	the input of r-th round
L_{r-1}	the left half of the r-th round input
R_{r-1}	the right half of the r-th round input
K_r	the subkey used in the r-th round
$X[i]$	the i-th bit of X, the index of bits is from left to right
$X \lll r$	the left rotation of the bits of X by r positions
$X \ggg r$	the right rotation of the bits of X by r positions
$\oplus$	bitwise exclusive OR (XOR)
$\cap$	bitwise AND
ΔX	the XOR difference of X and X'
$+$	addition
$\%$	modular operation

2.2 Brief Description of Block Cipher SIMON

The SIMON block cipher is a Feistel structure with an $2n$-bit state, where n is required to be 16, 24, 32, 48, or 64. SIMON2n with an mn-bit key is referred to as SIMON2n/mn, where $m = 2, 3, 4$. There are 10 suggested versions with different numbers of rounds n_r. The round numbers of 6 versions of SIMON are listed in the third column of Table 1. All versions of SIMON use the similar round function.

Round Functions For high performance on both hardware and software platforms, SIMON utilizes an extremely simple round function which is iterated over many rounds. The function $F(x) = (x \lll 1) \cap (x \lll 8) \oplus (x \lll 2)$ is non-linear transformation from $\{0,1\}^n$ to $\{0,1\}^n$, which is built by 3 bitwise operations $\oplus$, $\cap$ and $\lll$. Let the plaintext be $P = (L_0, R_0)$, and the i-th round function is described in the following.

$$\begin{aligned} L_i &= R_{i-1} \oplus F(L_{i-1}) \oplus K_{i-1}, \\ R_i &= L_{i-1}, \end{aligned}$$

where $i = 1, ..., n_r$. The ciphertext C is selected as (R_{n_r}, L_{n_r}).

In this paper, for convenience to describe our bit differential attack, we give a bitwise round function description. Let $L_i = \{X_i[n], X_i[n-1], \ldots, X_i[2n-1]\}$, $R_i = \{X_i[0], X_i[1], \ldots, X_i[n-1]\}$, and then the i-th round function is denoted as:

$$\begin{aligned} X_i[j+n] = X_{i-1}[(j+1)\%n+n] \cap X_{i-1}[(j+8)\%n+n]) \\ \oplus X_{i-1}[(j+2)\%n+n] \oplus X_{i-1}[j] \oplus K_{i-1}[j], \\ X_i[j] = X_{i-1}[j+n], \end{aligned}$$

where $j = 0, 1, \ldots, n-1$, and $X_i[n]$ is the most significant bit of L_i, $X_i[2n-1]$ is the least significant bit of L_i, $X_i[0]$ is the most significant bit of R_i, and $X_i[n-1]$ is the least significant bit of R_i.

Key Schedules The key schedules generate a sequence of n_r round subkeys $\{K_0, ..., K_{n_r-1}\}$ from master key $\{k_0, k_1, ..., k_{m-1}\}$. For different key length mn, the the key schedules are given

as follows. when $i = 1, \ldots, m-1$, $K_i = k_i$; and when $i = m, m+1, \ldots, n_r$,

$$\begin{aligned}
&\text{if } m = 2, K_i = c \oplus (z_j)_{i-m} \oplus K_{i-m} \oplus K_{i-m+1} \oplus (K_{i-m+1} \ggg 4),\\
&\text{if } m = 3, K_i = c \oplus (z_j)_{i-m} \oplus K_{i-m} \oplus K_{i-m+2} \oplus (K_{i-m+2} \ggg 4),\\
&\text{if } m = 4, K_i = c \oplus (z_j)_{i-m} \oplus K_{i-m} \oplus (K_{i-m+1} \oplus (K_{i-m+1} \ggg 1)\\
&\qquad\qquad \oplus (K_{i-m+3} \ggg 3) \oplus (K_{i-m+3} \ggg 4).
\end{aligned}$$

Here $c = 2^n - 4$, z_j is the version-dependent choice of constant sequence. For more details, refer to [3]. In fact, the key schedule is linear, the master key can be deduced any mn independent bits of subkeys.

2.3 Some Observations

Observation 1 (from [14]) *Let $\Delta x = x \oplus x'$, $\Delta y = y \oplus y'$, and then*

$$\begin{aligned}
(x \cap y) \oplus (x' \cap y) &= \Delta x \cap y,\\
(x \cap y) \oplus (x \cap y') &= x \cap \Delta y,\\
(x \cap y) \oplus (x' \cap y') &= (x \cap \Delta y) \oplus (\Delta x \cap y) \oplus (\Delta x \cap \Delta y).
\end{aligned}$$

Observation 2 *Given two inputs X_{i-1} and X'_{i-1} of i-th round, where $\Delta X_{i-1} = X_{i-1} \oplus X'_{i-1}$. Then the output difference ΔX_i is computed without the round subkey of K_i. $\Delta X_{i+1}[j+n](j < n)$ is computed by one of 4 cases in the following.*

1. $(\Delta X_i[(j+1)\%n + n], \Delta X_i[(j+8)\%n + n]) = (0,0)$, $\Delta X_{i+1}[j+n](j < n)$ *can be computed without any key bit guess.*
2. $(\Delta X_i[(j+1)\%n + n], \Delta X_i[(j+8)\%n + n]) = (0,1)$, $\Delta X_{i+1}[j+n](j < n)$ *can be computed by guessing $K_{i-1}[(j+1)\%n]$.*
3. $(\Delta X_i[(j+1)\%n + n], \Delta X_i[(j+8)\%n + n]) = (1,0)$, $\Delta X_{i+1}[j+n](j < n)$ *can be computed by guessing $K_{i-1}[(j+8)\%n]$.*
4. $(\Delta X_i[(j+1)\%n + n], \Delta X_i[(j+8)\%n + n]) = (1,1)$, $\Delta X_{i+1}[j+n](j < n)$ *can be computed by guessing $K_{i-1}[(j+8)\%n] \oplus K_{i-1}[(j+1)\%n]$.*

Since the subkey K_i is linear with the output of X_i, it is obviously ΔX_i is independent with K_i.

By partial encryption and Observation 1, we know the following equations hold.

$$\begin{aligned}
\Delta X_{i+1}[j+n] &= (\Delta X_i[(j+1)\%n + n] \cap X_i[(j+8)\%n + n])\\
&\quad \oplus (X_i[(j+1)\%n + n] \cap \Delta X_i[(j+8)\%n + n])\\
&\quad \oplus (\Delta X_i[(j+1)\%n + n] \cap \Delta X_i[(j+8)\%n + n])\\
&\quad \oplus \Delta X_i[(j+2)\%n + n] \oplus \Delta X_i[j],\\
X_i[(j+1)\%n + n] &= (X_{i-1}[(j+2)\%n + n] \cap X_{i-1}[(j+9)\%n + n])\\
&\quad \oplus X_{i-1}[(j+3)\%n + n] \oplus X_{i-1}[(j+1)\%n] \oplus K_{i-1}[(j+1)\%n],\\
X_i[(j+8)\%n + n] &= (X_{i-1}[(j+9)\%n + n] \cap X_{i-1}[(j+16)\%n + n])\\
&\quad \oplus X_{i-1}[(j+10)\%n + n] \oplus X_{i-1}[(j+8)\%n] \oplus K_{i-1}[(j+8)\%n].
\end{aligned} \tag{1}$$

It is obviously that Observation 2 is obtained by equation (1). When $(\Delta X_i[(j+1)\%n + n], \Delta X_i[(j+8)\%n + n]) = (0,0)$, no key bit guessed is necessary to compute ΔX_{i+1}. However, there is only one equivalent key bit needed to guess when $(\Delta X_i[(j+1)\%n + n], \Delta X_i[(j+8)\%n + n]) \neq (0,0)$. This phenomenon is useful to reduce the time complexity of our differential cryptanalysis.

3 Differential Attack on SIMON32

In this section, we describe a bit differential attack on round-reduced SIMON32/64. We utilize a 13-round differential path in [7] to attack 20-round SIMON32 by adding 3 rounds on the top and 4 rounds at the bottom, and attack 21-rounds of SIMON32 by adding 4 rounds on the top and 4 rounds at the bottom. For simplicity, let $C = \{L_{n_r}, R_{n_r}\}$ replace $C = \{R_{n_r}, L_{n_r}\}$ in the remaining of this paper.

3.1 Conditions in the Differential Cryptanalysis of 20-round SIMON32

For this attack, we consider the following 13-round differential whose probability is $2^{-28.11}$.

$$D_1 : (2000, 8000) \rightarrow (2000, 0000)$$

After prefixing 3 rounds on the top, it is easy to prove that the input difference is

$$\Delta P_1 : (**00, 00**, 00*0, 1**0, \quad *0*0, ***0, **1*, ****)$$

After appending 4 rounds at the bottom, the output difference of 20-round SIMON is

$$\Delta C_1 : (*0*0, ****, **1*, ****, \quad **00, 00**, *0*0, 1***)$$

For the differential D_1, decrypting the first 3 rounds and encrypting the last 4 rounds, we obtain 41 conditions which are independent of the secret key in Table 2, and 23 conditions relating to the secret key in Table 3. These 32 conditions in plaintexts and the first three round are sufficient and necessary to ensure the output difference of the third round to be $(2000, 8000)$. It is easy to guarantee the conditions hold in Table 2 by choosing the plaintexts. However, for the conditions in Table 3, we guess some subkey bits to make them hold, the numbers of corresponding key values is listed in the 6th column of Table 3, depending on the conditions for key guess seen the 5th column of Table 3. The core of our attack is how to ensure all the conditions in Table 3 hold by guessing some secret key bits as few as possible.

We give following two examples to explain the computations of the last column of Table 3.

1. $\Delta X_2[16] = 1$. By partial encryption, we know

$$\begin{aligned} \Delta X_2[16] &= X_1[17] \cap \Delta X_1[24] \oplus \Delta X_1[18] \oplus \Delta X_1[0] \\ X_1[17] &= (X_0[18] \cap X_0[25]) \oplus X_0[19] \oplus X_0[1] \oplus K_0[1] \end{aligned}$$

   If $\Delta X_1[24] = 0$, $\Delta X_2[16] = 1$ holds with probability $1/2$, $K_0[1]$ can take 2 values. Otherwise, $K_0[1]$ has one value to make $\Delta X_2[16] = 1$ hold. Therefore, there are one value for $K_0[1]$ on average.
2. $\Delta X_2[23] = 0$. By partial encryption, the following equations are deduced.

$$\begin{aligned} \Delta X_2[23] &= X_1[24] \cap \Delta X_1[31] \oplus X_1[31] \cap \Delta X_1[24] \oplus \Delta X_1[25] \oplus \Delta X_1[7], \\ X_1[24] &= (X_0[25] \cap X_0[16]) \oplus X_0[26] \oplus X_0[8] \oplus K_0[8], \\ X_1[31] &= (X_0[16] \cap X_0[23]) \oplus X_0[17] \oplus X_0[15] \oplus K_0[15]. \end{aligned}$$

   There are 4 cases depending on the values of ($\Delta X_1[24]$, $\Delta X_1[31]$).
   - (0,0): $\Delta X_2[23] = 0$ holds with probability $1/2$, $(K_0[8], K_0[15])$ can take 4 values.
   - (0,1): $K_0[1]$ has one values to make $\Delta X_2[16] = 1$ hold, $K_0[15]$ can take 2 values.
   - (1,0): $K_0[15]$ has one values to make $\Delta X_2[16] = 1$ hold, $K_0[1]$ can take 2 values.
   - (1,1): $K_0[15] \oplus K_0[1]$ has one values to make $\Delta X_2[16] = 1$ hold, ($K_0[1]$, $K_0[15]$) can take 2 values.

   Hence, there are about two values for ($K_0[1]$, $K_0[15]$) to make $\Delta X_2[23] = 0$ hold.

3.2 Key-Recovey Attack on 20-round SIMON32

In this subsection, we describe a key recovery attack on 20-round SIMON32/64. Since there are many conditions in the plaintext and the output of the 1st round, which are independent of secret key, we make use of these conditions to construct structures, and reduce the time complexity for collecting plaintext pairs. In the process of key recovery attack, we use Observation 2 to reduce the key bits guessed.

Data Collection In order to reduce the time complexity for data collection, we propose the following method to reduce time complexity of collecting the pairs.

1. There are 13 necessary conditions on plaintexts, 10 necessary conditions on the first three rounds. We divided the plaintexts into 2^{23} structures, which has $2^{32-23} = 2^9$ plaintexts (equivalent to traverse 9 positions). By Observation 2, $K_0[j]$ is independent with $\Delta X_1[j]$, which do not impact the structure. By round function definition, we built the following 10 equations

$$X_1[j] = X_0[(j+1-n)\%n+n] \cap X_0[(j+8)\%n+n] \oplus X_0[(j+2)\%n+n] \oplus X_0[j-n],$$

   where $j = 16, 18, 20, 21, 22, 25, 27, 28, 29, 30$. Because there are 13 conditions on plaintexts, we fixed 13 bit $X_0[i]$ as constants, where $i = 1, 3, 7, 10, 18, 19, 20, 21, 24, 25, 27, 28, 31$, and obtained each structure by traversing left 19 bits of plaintexts and solving the above equations system.
2. For structures A and A' with 4 different bits ($X_0[10]$, $X_0[28]$, $X_1[18]$, $X_1[30]$), find the corresponding ciphertexts, and inset a table indexed by $X_{20}[t]$, where $\Delta X_{20}[t] = 0$. There are about $2^{9\times 2-8} = 2^{10}$ pairs remaining for each structure.
3. We build 2^{22} structures, and filter out the remaining pairs according to the conditions in Table 2, there are $2^{22-1+10-10} = 2^{21}$ pairs left. Store the pairs in table T_1.

In the data collection phase, choosing $2^{22+9} = 2^{31}$ plaintexts, we get $2^{22-1+18-9} = 2^{30}$ pairs satisfying the input difference of the differential. Hence, there are about $2^{30-28.11} = 3.7$ right pairs.

Key Guessing There are 36 bits of subkey or equivalent subkey required to guess for differential D_1. By key schedules, we know that these 36 bits are linearly independent. To detect the correct key, we maintain a set of counters of size 2^{36}, named as S_1, initialized with 0. Then for the pairs in T_1, guess subkey in the following procedure.

1. Guess some subkey bits of the 2nd round listed in Table 3 to compute $\Delta X_2[17, 22, 26, 29, 16, 30, 23]$ one by one, and eliminate the pairs which do not satisfy the conditions. There are about $2^{21-7} = 2^{14}$ remaining pairs.
2. Guess some subkey bits of the 18th round listed in Table 3 to obtain $\Delta X_{18}[6, 15, 0, 13, 14, 7, 8]$ one by one, and keep the pairs which fulfill the conditions. There are $2^{14-7} = 2^7$ pairs left on average.
3. Guess $K_1[7]$ to calculate $\Delta X_3[31]$, and discard the pairs, if $\Delta X_3[31] \neq 0$. Then guess $K_1[9]$, $K_0[10]$ to deduce $\Delta X_3[24]$, and keep the pairs when $\Delta X_3[24] = 0$. There are about $2^{7-2} = 2^5$ remaining pairs on average.
4. Guess some subkey bits the 17th round listed in the 4th column of Table 3 to compute $\Delta X_{17}[2, 8, 0, 9, 15]$ one by one, and eliminate the pairs which are not content with the conditions. There are about $2^{5-5} = 1$ pairs left.
5. For the 16th round, compute $\Delta X_{18}[3]$ and $\Delta X_{19}[5]$. There are 4 types of subkey which should be guessed to compute $\Delta X_{16}[10]$ by the values of ($\Delta X_{18}[3]$, $\Delta X_{19}[5]$).
   - (0,0): Guessing $K_{17}[11] \oplus K_{18}[13]$ is enough.

– (0,1): We need to guess $K_{17}[11] \oplus K_{18}[13] \oplus K_{19}[14]$.
– (1,0): Since $\Delta X_{18}[3] = 1$, the value of $X_{18}[12]$ is necessary to compute. Then compute $\Delta X_{19}[4]$. When $\Delta X_{19}[4] = 0$, we need to guess $K_{18}[12]$; otherwise, guess $K_{18}[12] \oplus K_{19}[13]$.
– (1,1): The values of $X_{18}[12]$, $X_{19}[14]$ are needed. When $\Delta X_{19}[4] = 0$, we need to guess $K_{18}[12] \oplus K_{17}[11] \oplus K_{18}[13] \oplus K_{19}[14]$; otherwise, guess $K_{18}[12] \oplus K_{19}[13] \oplus K_{17}[11] \oplus K_{18}[13] \oplus K_{19}[14]$.

Keep the pairs if $\Delta X_{16}[10] = 0$. Then guess $K_{19}[3]$ to get $X_{19}[3]$. If $X_{19}[3] = 0$, guess $K_{17}[9] \oplus K_{18}[11]$; otherwise, guess $K_{17}[9] \oplus K_{18}[11] \oplus K_{19}[12]$. Then calculate $\Delta X_{16}[1] = 0$. Discard the pairs when $\Delta X_{16}[1] = 1$. There are about 2^{-2} pairs left.

6. Increase the counters corresponding to the guessed subkeys by the number of the remaining pairs.
7. We compute the master key by the key schedule with the known 36-bit subkey. Then exhaustive the remaining bits of master key.

Complexity Cryptanalysis For data collection, we need 2^{31} encryptions for chosen plaintexts, the time complexity is dominated by Step 2, which is about $2^{21} \times 2^{10} = 2^{31}$ one round encryption to save the pairs which fulfill the conditions.

In the key guessing procedure, the complexity is dominated by Step 6. Since there are about 2^{12} 36-bit subkeys for a pair which conform the input difference of the differential D_1, it is about $2^{21} \times 2^{13} = 2^{34}$ increment. Therefore the time complexity is about 2^{31} encryptions, and the data complexity about 2^{31} chosen plaintexts.

It is expected to have 3.7 pairs left for the right key. However, the counter is about $2^{21} \times 2^{13}/2^{36} = 2^{-2}$ for a wrong key. The signal-to-noise ratio is $Sn = \frac{2^{-28.11}}{2^{-32}} = 14.83$.

According to [17], the success probability is

$$Ps = \int_{-\frac{\sqrt{\mu S/N} - \Phi^{-1}(1-2^{-a})}{\sqrt{S/N+1}}}^{\infty} \Phi(x)dx = 0.576, \tag{2}$$

where $a = 36$ is the number of subkey bits guessed, μ is the number of right pairs and $\mu = 3.7$.

3.3 Conditions in the Differential Cryptanalysis of 21-round SIMON32

For this attack, we consider the above 13-round differential again.

After prefixing 4 rounds on the top, it is easy to prove that the input difference is

$$\Delta P_1 : (*0*0, ***0, **1*, ****, \quad ****, ****, ****, ****)$$

After appending 4 rounds at the bottom, the output difference of 21-round SIMON is

$$\Delta C_1 : (*0*0, ****, **1*, ****, \quad **00, 00**, *0*0, 1***)$$

For the differential D_1, decrypting the first 4 rounds and encrypting the last 4 rounds, we deduce 31 conditions independent of the secret key in Table 4, and 33 conditions relating to the secret key in Table 5. There are 28 conditions in the plaintexts and the rounds 1-4, which are sufficient and necessary to ensure the output difference of the third round to be $(2000, 8000)$. We make the 31 conditions independent of the secret key hold by choosing the plaintexts, and give a method to ensure all the conditions in Table 5 hold by guessing some secret key bits as few as possible.

3.4 Key-Recovey Attack on 21-round SIMON32

In this subsection, we describe a key recovery attack on 21-round SIMON32. We make use of these conditions independent of secret key to construct the structure, and reduce the time complexity for collecting plaintext pairs. In the process of key recovery attack, we use Observation 2 to reduce the key bits guessed.

Data Collection In order to reduce the time complexity for data collection, We use the above method in Section 3.2 to collect pairs..

1. There are 4 necessary conditions on plaintexts, 9 necessary conditions on the first three rounds. We divided the plaintexts into 2^{13} structures, which has $2^{32-13} = 2^{19}$ plaintexts (equivalent to traverse 19 positions). By Observation 2, $K_0[j]$ is independent with $\Delta X_1[j]$, which do not impact the structure. By round function definition, we built the following 9 equations

$$X_1[j] = X_0[(j+1-n)\%n+n] \cap X_0[(j+8)\%n+n] \oplus X_0[(j+2)\%n+n] \oplus X_0[j+-n],$$

   where $j = 18, 19, 20, 21, 24, 25, 27, 28, 31$. Because there are 4 conditions on plaintexts, we fixed 4 bit $X_0[i]$ as constants, where i=17, 19, 23, 26, and obtained each structure by traversing left 28 bits of plaintexts and solving the above equations system.
2. For structures A and A' with 2 different bits ($X_0[26]$, $X_1[28]$), find the corresponding ciphertexts, and inset a table indexed by $X_{21}[t]$, where $\Delta X_{21}[t] = 0$. There are about $2^{19\times 2-8} = 2^{30}$ pairs remaining for each structure.
3. We build 2^{12} structure, and filter out the remaining pairs according the conditions, there are $2^{12-1+30-10} = 2^{31}$ pairs left. Store the pairs in table T_1.

In the data collection phase, choosing $2^{12+19} = 2^{31}$ plaintexts, we get $2^{12+19+18-19} = 2^{30}$ pairs satisfying the input difference of the differential. Hence, there are about $2^{30-28.11} = 3.7$ right pairs.

Key Guessing There are 52-bit of subkey or equivalent subkey required to guess for differential D_1. By key schedules, we know that these 52 bits are linearly dependent. Further, we can verify that $K_{20}[13]$ can be computed from the first-three subkeys included in Table 5. So, to detect the correct key, we maintain a set of counters of size 2^{51}, initialized with 0. Then for the pairs in T_1, subkey guessing phase is similar to the attack on 20-round SIMON32.

Complexity Cryptanalysis For data collection, we need 2^{31} encryptions for chosen plaintexts, the time complexity is dominated by Step 2, which is about $2^{11} \times 2^{30} = 2^{41}$ one round encryption to save the pairs which fulfill the conditions.

In the key guessing procedure, Since there are about 2^{19} 51-bit subkeys for a pair which conform the input difference of the differential D_1, it is about $2^{31} \times 2^{19} = 2^{50}$ increments. Therefore the time complexity is about 2^{46} encryptions, and the data complexity about 2^{31} chosen plaintexts.

It is expected to have 3.7 pairs left for the right key. However, the counter is about $2^{31} \times 2^{19}/2^{51} = 2^{-1}$ for a wrong key. The signal-to-noise ratio is $Sn = \frac{2^{-28.11}}{2^{-32}} = 14.83$.

The success probability is increased to 0.4367 computed by equation (2), where $a = 51$, $\mu = 3.7$.

Therefore, the differential attacks on 21-round SIMON32/64 needs 2^{46} encryptions with 2^{31} chosen plaintexts, and the success probability is 0.4367.

4 Differential Attack on SIMON48

In this section, we describe a differential attack on round-reduced SIMON48. We utilize a 15-round differential[7] to attack 21 rounds of SIMON48 by adding 3 rounds on the top and 3 rounds at the bottom, and attack 22-round of SIMON48 by adding one more round at the bottom.

4.1 Conditions in the Differential Cryptanalysis of 21-round SIMON48

The following 15-round differential with probability $2^{-42.11}$ is applied in our differential cryptanalysis.

$$D_1 : (200020, 800800) \rightarrow (080888, 000200)$$

After prefixing 3 rounds on the top, it is easy to prove that the difference of the input of 21-round SIMON48 for the differential path is

$$\Delta P_1 : (***0, *0**, 00**, ***0, 1***, 1000, \quad ****, ***0, ****, **0*, ****, *0**)$$

The output difference of 21-round SIMON48 is given in the following by appending 3 rounds at the bottom of our differential.

$$\Delta C_1 : (****, ****, ****, **0*, ****, *0**, \quad ****, *0**, 1***, ***0, 0***, *000)$$

For the differential D_1, decrypting the first 3 rounds and encrypting the last 3 rounds, we deduce 56 conditions independent of the secret key in Table 6, and 40 conditions relating to the secret key in Table 7. There are 48 conditions in the plaintexts and the rounds 1-3, which are sufficient and necessary to ensure the output difference of the third round to be $(200020, 800800)$. We make the conditions in Table 6 hold by choosing the plaintexts, and give a method to ensure all the conditions in Table 7 hold by guessing some secret key bits as few as possible.

4.2 Key-Recovey Attack on 21-round SIMON48

In this subsection, we describe a key recovery attack on 21-round SIMON48. We make use of these conditions independent of secret key to construct structures, and reduce the time complexity for collecting plaintext pairs. In the process of key recovery attack, we use Observation 2 to reduce the key bits guessed.

Data Collection We also apply the above method in Section 3.2 to collect pairs.

1. There are 13 necessary conditions on plaintexts, and 18 necessary conditions in the first three rounds independent with secret key, i.e. $\Delta X_1[i] = 0 (i =$24, 25, 26, 28, 29, 30, 33, 34, 35, 37, 40, 41, 42, 46, 47$)$, $\Delta X_2[j] = 0 (j = 25, 34, 41)$ in Table 6. Hence, let K_0 and K_1 be fixed constants. For each fixed 13-bit X_0[7, 14, 21, 27, 29, 32, 33, 39, 40, 44, 45, 46, 47], traverse the left bits of X_0 to compute $X_1[i] = 0 (i =$24, 25, 26, 28, 29, 30, 33, 34, 35, 37, 40, 41, 42, 46, 47$)$, $X_2[j] = 0 (j = 25, 34, 41)$, and divide the plaintexts into 2^{18} sets indexed the corresponding $X_1[i]$ and $X_2[j]$. Each set is a structure with $2^{48-13-18} = 2^{17}$ plaintexts.
2. For structure A and A' with different 40th and 44th bit of plaintexts, query the corresponding ciphertexts, and inset a table indexed by $X_{20}[t]$, where $\Delta X_{20}[t] = 0$. There are about $2^{17\times 2-7} = 2^{27}$ pairs between A and A' remaining.
3. We built 2^{28} structure, and filter out the obtained pairs according to the conditions in Table 6, there are $2^{28-1+27-18} = 2^{36}$ pairs left. Store the pairs in table T_1.

In the data collection phase, we get $2^{28-1+34-17} = 2^{44}$ pairs which satisfying the input difference of D_1. Hence, there are about 3.7 right pairs.

Key Guessing There are 55-bit of subkey or equivalent subkey required to guess for differential D_1. By key schedules, we know that these 55 bits are linearly independent. To detect the correct key, we maintain a set of counters of size 2^{55}, initialized with 0. Then for the pairs in T_1, guess subkey in the following procedure.

1. Guess some subkey bits of the 2nd round listed in Table 7 to compute ΔX_2[24, 26, 28, 36, 38, 42, 31, 35, 43, 37, 30] one by one, and eliminate the pairs which do not satisfy the conditions. There are about $2^{36-11} = 2^{25}$ remaining pairs.

2. Guess some subkey bits of the 19th round listed in Table 7 to obtain ΔX_{19}[0, 17, 4, 14, 12, 20, 1, 2, 3, 7, 9, 10, 11, 18, 19] one by one, and keep the pairs which fulfill the conditions. There are $2^{25-15} = 2^{10}$ pairs left on average.
3. Guess some subkey bits of the 3rd round listed in Table 7 to compute ΔX_3[27, 44, 32, 36, 39, 43] one by one, and remain the pairs which are in accordance with the conditions. There are about $2^{10-6} = 2^4$ remaining pairs.
4. Guess some subkey bits the 18th round listed in the 4th column of Table 7 to compute $\Delta X_{17}[2, 8, 0, 9, 15]$ one by one, and eliminate the pairs which are not content with the conditions. There are about $2^{4-8} = 2^{-4}$ pairs left.
5. Increase the counters corresponding to the guessed subkeys by the number of the remaining pairs.
6. We compute the master key by the key schedule with the known 55-bit subkey. Then exhaustive the remaining bits of master key.

Complexity Cryptanalysis For data collection, we need about 2^{45} encryptions for the chosen plaintexts, and about 2^{54} one round computations to decide the conditions equivalent to 2^{50} encryptions. The data complexity is about 2^{45} chosen plaintexts.

In the key guessing procedure, the complexity is dominated by Step 6. Since there are about 2^{15} 55-bit subkeys for a pair which fulfill the input difference of the differential D_1, it is about $2^{36} \times 2^{15} = 2^{51}$ increments equivalent to 2^{47} encryptions.

It is expected to have 3.7 pairs left for the right key. However, the counter is about $2^{36} \times 2^{15}/2^{55} = 2^{-4}$ for a wrong key. The signal-to-noise ratio is $Sn = \frac{2^{-42.11}}{2^{-48}} = 2^{5.89}$.

The success probability is increased to 0.79 computed by equation (2), where $a = 55$, $\mu = 3.7$.

Therefore, the differential attacks on SIMON48 needs 2^{50} encryptions with 2^{45} chosen plaintexts, and the success probability is 0.79.

4.3 Conditions in the Differential Cryptanalysis of 22-round SIMON48

For this attack, we consider the above 15-round differential for SIMON48 again.

After prefixing 3 rounds on the top, it is easy to prove that the difference of the input of 21-round SIMON48 for our differential path is

$$\Delta P_1 : (***0, *0**, 00**, ***0, 1***, 1000, \quad ****, ***0, ****, **0*, ****, *0**)$$

The the output difference of 22-round SIMON48 is given in the following by appending 4 rounds at the bottom of our differential.

$$\Delta C_1 : (****, ****, ****, ****, ****, ****, \quad ****, ****, ****, **0*, ****, *0**)$$

For the differential D_1, decrypting the first 3 rounds and encrypting the last 4 rounds, we deduce 41 conditions independent of the secret key in Table 8, and 55 conditions relating to the secret key in Table 9. There are 48 conditions in the plaintexts and the rounds 1-3, which are sufficient and necessary to ensure the output difference of the third round to be $(200020, 800800)$. We make the conditions independent of the secret key hold by choosing the plaintexts, and give a method to ensure all the conditions in Table 9 hold by guessing some secret key bits as few as possible.

4.4 Key-Recovey Attack on 22-round SIMON48

In this subsection, we describe a key recovery attack on 22-round SIMON48. We make use of these conditions independent of secret key to construct the structure, and reduce the time complexity

for collecting plaintext pairs. In the process of key recovery attack, we use Observation 2 to reduce the key bits guessed. The bit differential cryptanalysis includes data collection and key guess two phases, which are demonstrated in the following.

Data Collection We also apply the above method in Section 3.2 to collect pairs.

1. This phase is the same as data collection phase of 21-round SIMON48, Each set is a structure with $2^{48-13-18} = 2^{17}$ plaintexts.
2. For structure A and A' with different 40th and 44th bit of plaintexts, query the corresponding ciphertexts, and inset a table indexed by $X_{20}[t]$, where $\Delta X_{20}[t] = 0$. There are about $2^{17\times 2-2} = 2^{32}$ pairs between A and A' remaining.
3. We built 2^{28} structure, and filter out the obtained pairs according to the conditions independent of secret key, there are $2^{28-1+32-8} = 2^{51}$ pairs left. Store the pairs in table T_1.

In the data collection phase, we get $2^{28-1+34-17} = 2^{44}$ pairs which satisfying the input difference of D_1. Hence, there are about 3.7 right pairs.

Key Guessing There are 79-bit of subkey or equivalent subkey required to guess for differential D_1.

According to the key schedule of SIMON48/72 version, we know that these 79 bits are linearly dependent, further we can verify that $K_{20}[23] \oplus K_{19}[21]$, $K_0[0, 3, 11, 14, 17]$, $K_1[13, 23]$, $K_{19}[13, 23]$ can be computed from other 69 bit subkeys. To detect the correct key, we maintain a set of counters of size 2^{69}, initialized with 0. Then for the pairs in T_1, guess subkey phase is the same as attack on 21-round SIMON48, but above 10 bit subkeys be guessed in the end, thus we can reduce time complexity of compution.

According to the key schedules of SIMON48/96 version, we know that these 79 bits are linearly independent. To detect the correct key, we maintain a set of counters of size 2^{79}, initialized with 0. Then for the pairs in T_1, subkey guessing phase is the same as attack on 21-round SIMON48.

Complexity Cryptanalysis For data collection, we need about 2^{45} encryptions for the chosen plaintexts, and about 2^{59} one round computations to decide the conditions equivalent to 2^{55} encryptions. The data complexity is about 2^{45} chosen plaintexts.

In the key guessing procedure, for SIMON48/72 version, since there are about 2^{16} 69-bit subkeys for a pair which fulfill the input difference of the differential D_1, it is about $2^{51}\times 2^{16} = 2^{67}$ increments equivalent to 2^{63} encryptions.

There is expected to have 3.7 pairs left for the right key. However, the counter is about $2^{51} \times 2^{16}/2^{69} = 2^2$ for a wrong key. The signal-to-noise ratio is $Sn = \frac{2^{-42.11}}{2^{-48}} = 2^{5.89}$.

The success probability is increased to 0.755 computed by equation (2), where $a = 69$, $\mu = 3.7$.

Therefore, the differential attacks on 22-round SIMON48/72 needs 2^{69} encryptions with 2^{45} chosen plaintexts, and the success probability is 0.755.

For SIMON48/96 version, Since there are about 2^{24} 79-bit subkeys for a pair which fulfill the input difference of the differential D_1, it is about $2^{51} \times 2^{24} = 2^{75}$ increments equivalent to 2^{71} encryptions.

It is expected to have 3.7 pairs left for the right key. However, the counter is about $2^{51} \times 2^{24}/2^{79} = 2^{-4}$ for a wrong key. The signal-to-noise ratio is $Sn = \frac{2^{-42.11}}{2^{-48}} = 2^{5.89}$.

The success probability is increased to 0.726 computed by equation (2), where $a = 79$, $\mu = 3.7$.

Therefore, the differential attacks on 22-round SIMON48/96 needs 2^{71} encryptions with 2^{45} chosen plaintexts, and the success probability is 0.726.

5 Differential attack on SIMON64

In this section we describe a differential attack on round-reduced SIMON64 with key size 96 and 128. In this attack, we use a 21-round differential path in[7]. We mount a 28-round attack on SIMON64 by adding 4 rounds on the top and 3 rounds at the bottom.

5.1 Conditions in the Differential Cryptanalysis of SIMON64

The following 21-round differential with probability $2^{-60.53}$ is applied in our differential cryptanalysis.

$$D_1 : (04000000, 11000000) \rightarrow (00080888, 00000200)$$

After prefixing 4 rounds on the top, it is easy to prove that the input differences of 28-round SIMON64 is

$$\Delta P_1 : (*0**, *0*0, 000*, 000*, 0**0, 0***, **0*, ****, \quad ****, **0*, 0**0, 0***, **0*, ****, ****, ****)$$

The output difference of 28-round SIMON64 is given in the following by appending 3 rounds at the bottom.

$$\Delta C_1 : (*0**, *0*0, 000*, 000*, 0**0, 0***, **0*, ****, \quad **00, **01, 0000, 0000, 000*, 000*, 0**0, 0**0)$$

For the differential D_1, decrypting the first 4 rounds and encrypting last 3 rounds, we deduce 91 conditions independent of the secret key in Table 10, and 31 conditions relating to the secret key in Table 11. There are 58 conditions in the plaintexts and the rounds 1-4, which are sufficient and necessary to ensure the output difference of the 4th round to be (04000000, 11000000). We make the conditions in Table 10 hold by choosing the plaintexts, and give a method to ensure all the conditions in Table 11 hold by guessing some secret key bits as few as possible.

5.2 Key-Recovey Attack on SIMON64

In this subsection, we describe a key recovery attack on 28-round SIMON64. We make use of these conditions independent of secret key to construct the structure, and reduce the time complexity for collecting plaintext-ciphertext pairs. In the process of key recovery attack, we use Observation 2 to reduce the key bits guessed. The bit differential cryptanalysis includes data collection and key guess two phases, which are demonstrated in the following.
Data Collection We apply the above method in Section 3.2 to collect pairs.

1. There are 18 necessary conditions on plaintexts, and 21 necessary conditions in the first three rounds independent of secret key seen in Table 10. Hence let K_0 and K_1 and K_2 be fixed constants. For a fixed 18-bit value X_0[1, 6, 8, 11, 12, 18, 33, 37, 39, 40, 41, 42, 44, 45, 46, 48, 51, 52, 58], traverse the left 46 bits of X_0 to compute $X_1[i](i$ =34, 35, 39, 41, 42, 45, 46, 47, 48, 49, 52, 53, 54, 56, 59, 60, 63), X_2[55], X_2[62], X_3[32], X_3[57], and divide the plaintexts into 2^{18} sets indexed the corresponding $X_1[i]$ and X_2[55], X_2[62], X_3[32], X_3[57]. Each set is a structure with $2^{46-21} = 2^{25}$ plaintexts.
2. For structures A and A' with different bit, i.e. (X_0[11], X_0[42], X_0[52], X_1[39], X_1[63]), find the corresponding ciphertexts, and inset a table indexed by $X_{28}[t]$, where $\Delta X_{28}[t] = 0$. There are about $2^{25\times2-34} = 2^{16}$ pairs between A and A' remaining.
3. We built 2^{34} structures, and filter out the obtained pairs according to the conditions in Table 6, there are $2^{34-1+16-18} = 2^{31}$ pairs left. Store the pairs in table T_1.

In the data collection phase, we choose $2^{34+25} = 2^{59}$ plaintexts, and get $2^{34-1+50-19} = 2^{64}$ pairs which satisfying the input difference of D_1. Hence, there are about 11.08 right pairs.

Key Guessing There are 74-bit of subkey or equivalent subkey required to guess for differential D_1. By key schedules, we know that these 74 bits are linearly independent. To detect the correct key, we maintain a set of counters of size 2^{74}, named as S_1, initialized with 0. Then for the pairs in T_1, guess subkey in the following procedure.

1. Guess some subkey bits of the 2nd round listed in Table 11 to compute ΔX_2[32, 35, 36, 43, 47, 49, 53, 50, 54, 56, 57, 61, 60] one by one, and eliminate the pairs which do not satisfy the conditions. There are about $2^{31-7} = 2^{24}$ remaining pairs.
2. Guess some subkey bits of the 26th round listed in Table 11 to obtain ΔX_{26}[4, 29, 1, 5, 19, 23, 26, 30] one by one, and keep the pairs which fulfill the conditions. There are $2^{24-8} = 2^{16}$ pairs left on average.
3. Guess some subkey bits of the 3rd round listed in Table 11 to compute ΔX_3[33, 36, 37, 51, 55, 58, 61, 62] one by one, and remain the pairs which are in accordance with the conditions. There are about $2^{16-8} = 2^8$ remaining pairs.
4. Guess some subkey bits of the 25th round listed in the 4th column of Table 3 to compute $\Delta X_{25}[2, 6, 27, 31]$ one by one, and eliminate the pairs which are not content with the conditions. There are about $2^{8-4} = 2^4$ pairs left.
5. Guess some subkey bits of the 4nd round listed in Table 11 to compute ΔX_4[34, 38, 59, 63] one by one, and eliminate the pairs which do not satisfy the conditions. There are about $2^{4-4} = 1$ remaining pairs.
6. Increase the counters corresponding to the guessed subkeys by the number of the remaining pairs.
7. We compute the master key by the key schedule with the known 74-bit subkey. Then exhaustive the remaining bits of master key.

Complexity Cryptanalysis For data collection, we need about 2^{59} encryptions for the chosen plaintexts, and about 2^{49} one round computations to decide the conditions. The data complexity about 2^{59} chosen plaintexts.

In the key guessing procedure, the complexity is dominated by Step 7. Since there are about 2^{33} 74-bit subkeys for a pair which fulfill the input difference of the differential D_1, it is about $2^{31} \times 2^{33} = 2^{64}$ increments equivalent to 2^{60} encryptions. For SIMON64/128, the exhaustive searching cost $2^{128-74} = 2^{54}$ encryptions.

It is expected to have 11.08 pairs left for the right key. However, the counter is about $2^{31} \times 2^{33}/2^{74} = 2^{-10}$ for a wrong key. The signal-to-noise ratio is $Sn = \frac{2^{-60.53}}{2^{-64}} = 11.08$. The success probability is increased to 0.628 computed by equation (2), where $a = 74$, $\mu = 11.08$.

Therefore, the differential attacks on SIMON64 needs 2^{61} encryptions with 2^{59} chosen plaintexts, and the success probability is 0.628.

6 Conclusion

In this paper, we present improved differential attacks on SIMON32, SIMON48 and SIMON64 with one or two rounds more than previous attacks. The core of our method is the bit differential cryptanalysis. we present the round function with bitwise expression, and give some bit-difference equations corresponding to subkey or equivalent subkey bit. Based on this, an optimal key guess policy is proposed, which reduces the time complexity of the differential cryptanalysis. Besides, a new method constructing structure for plaintexts is given to decrease the complexity of collecting pairs. Our technique is not only available to differential attacks, but also is helpful to impossible differential attacks, boomerang attacks etc.

References

1. Abed, F., List, E., Lucks, S., b Wenzel: Differential Cryptanalysis of Round-Reduced SIMON and SPECK. In: FSE (2014)
2. AlKhzaimi, H., Lauridsen, M.M.: Cryptanalysis of the SIMON Family of Block Ciphers. IACR Cryptology ePrint Archive 2013, 543 (2013)
3. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK Families of Lightweight Block Ciphers. IACR Cryptology ePrint Archive 2013, 404 (2013)
4. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. pp. 12–23. Springer-Verlag (1999)
5. Biham, E., Dunkelman, O., Keller, N.: The Rectangle Attack - Rectangling the Serpent. In: Pfitzmann, B. (ed.) Advances in Cryptology – EUROCRYPT 2001. Lecture Notes in Computer Science, vol. 2045, pp. 340–357. Springer (May 2001)
6. Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer (1993)
7. Biryukov, A., Roy, A., vesselin Velichkov: Differential Analysis of Block Ciphers SIMON and SPECK. In: FSE (2014)
8. Blondeau, C., Gérard, B.: Multiple Differential Cryptanalysis: Theory and Practice. In: Fast Software Encryption. pp. 35–54. Springer (2011)
9. Bogdanov, A., Knudsen, L., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., Vikkelsoe, C.: Present: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems-CHES 2007 pp. 450–466 (2007)
10. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçin, T.: PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract. In: ASIACRYPT. pp. 208–225 (2012)
11. Cannière, C.D., Dunkelman, O., Knezevic, M.: KATAN and KTANTAN - A Family of Small and Efficient Hardware-Oriented block ciphers. In: CHES. pp. 272–288 (2009)
12. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED Block Cipher. In: Cryptographic Hardware and Embedded Systems–CHES 2011, pp. 326–341. Springer (2011)
13. Kelsey, J., Kohno, T., Schneier, B.: Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent. In: FSE. pp. 75–93 (2000)
14. Khn, U., Ag, D.B.: Improved Cryptanalysis of MISTY1. In: In: Fast Software Encryption, 9th International Workshop, FSE 2002. Volume 2365 of LNCS., Springer-Verlag. pp. 61–75. Springer-Verlag (2002)
15. Knudsen, L.: DEAL-a 128-bit Block Cipher. complexity 258(2) (1998)
16. Knudsen, L.R.: Truncated and Higher Order Differentials. In: Preneel, B. (ed.) Fast Software Encryption – FSE'94. Lecture Notes in Computer Science, vol. 1008, pp. 196–211. Springer (Dec 1994)
17. Selçuk, A.A., Biçak, A.: On Probability of Success in Linear and Differential Cryptanalysis. In: Cimato, S., Galdi, C., Persiano, G. (eds.) SCN 02: 3rd International Conference on Security in Communication Networks. Lecture Notes in Computer Science, vol. 2576, pp. 174–185. Springer (Sep 2002)
18. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-Bit Blockcipher CLEFIA (Extended Abstract). In: FSE. pp. 181–195 (2007)
19. Wagner, D.: The Boomerang Attack. In: Knudsen, L.R. (ed.) Fast Software Encryption – FSE'99. Lecture Notes in Computer Science, vol. 1636, pp. 156–170. Springer (Mar 1999)

Table 2: Conditions of Differential Path of 20-round SIMON32 are Independent of Subkeys

Rounds	Number of Conditions	Difference Conditions of i-th Round
input	13	$\Delta X_0[1] = 0$, $\Delta X_0[3] = 0$, $\Delta X_0[7] = 0$, $\Delta X_0[10] = 1$, $\Delta X_0[18] = 0$, $\Delta X_0[19] = 0$, $\Delta X_0[20] = 0$, $\Delta X_0[21] = 0$, $\Delta X_0[24] = 0$, $\Delta X_0[25] = 0$, $\Delta X_0[27] = 0$, $\Delta X_0[28] = 1$, $\Delta X_0[31] = 0$
1	10	$\Delta X_1[16] = 0, \Delta X_1[16] = X_0[24] \cap \Delta X_0[17] + \Delta X_0[18] + \Delta X_0[0]$, $\Delta X_1[18] = 1, \Delta X_1[18] = X_0[19] \cap \Delta X_0[26] + \Delta X_0[20] + \Delta X_0[2]$, $\Delta X_1[20] = 0, \Delta X_1[20] = X_0[21] + \Delta X_0[22] + \Delta X_0[4]$, $\Delta X_1[21] = 0, \Delta X_1[21] = X_0[22] \cap \Delta X_0[29] + X_0[29] \cap \Delta X_0[22] + \Delta X_0[23] + \Delta X_0[5]$, $\Delta X_1[22] = 0, \Delta X_1[22] = X_0[23] \cap \Delta X_0[30] + X_0[30] \cap \Delta X_0[23] + \Delta X_0[24] + \Delta X_0[6]$, $\Delta X_1[25] = 0, \Delta X_1[25] = X_0[26] \cap \Delta X_0[17] + X_0[17] \cap \Delta X_0[26] + \Delta X_0[27] + \Delta X_0[9]$, $\Delta X_1[27] = 0, \Delta X_1[27] = X_0[19] + \Delta X_0[29] + \Delta X_0[11]$, $\Delta X_1[28] = 0, \Delta X_1[28] = X_0[20] \cap \Delta X_0[29] + \Delta X_0[30] + \Delta X_0[12]$, $\Delta X_1[29] = 0, \Delta X_1[29] = X_0[21] \cap \Delta X_0[30] + \Delta X_0[31] + \Delta X_0[13]$, $\Delta X_1[30] = 1, \Delta X_1[30] = X_0[31] \cap \Delta X_0[22] + \Delta X_0[16] + \Delta X_0[14]$

19	8	$\Delta X_{19}[4] = 0$, $\Delta X_{19}[4] = X_{20}[5] + \Delta X_{20}[6] + \Delta X_0[4]$, $\Delta X_{19}[5] = 0$, $\Delta X_{19}[5] = X_{20}[6] \cap \Delta X_{20}[13] + X_{20}[13] \cap \Delta X_{20}[6] + \Delta X_{20}[7] + \Delta X_0[5]$, $\Delta X_{19}[6] = 0$, $\Delta X_{19}[6] = X_{20}[7] \cap \Delta X_{20}[14] + X_{20}[14] \cap \Delta X_{20}[7] + \Delta X_{20}[8] + \Delta X_0[6]$, $\Delta X_{19}[7] = 0$, $\Delta X_{19}[7] = 0 = X_{20}[8] \cap \Delta X_{20}[15] + X_{20}[15] \cap \Delta X_{20}[8] + \Delta X_{20}[9] + \Delta X_0[7]$, $\Delta X_{19}[11] = 0$, $\Delta X_{19}[11] = 0 = X_{20}[3] + \Delta X_{20}[13] + \Delta X_0[11]$, $\Delta X_{19}[12] = 0$, $\Delta X_{19}[12] = 0 = X_{20}[4] \cap \Delta X_{20}[13] + \Delta X_{20}[14] + \Delta X_0[12]$, $\Delta X_{19}[13] = 0$, $\Delta X_{19}[13] = 0 = X_{20}[5] \cap \Delta X_{20}[14] + \Delta X_{20}[15] + \Delta X_0[13]$, $\Delta X_{19}[14] = 1$, $\Delta X_{19}[14] = X_{20}[15] \cap \Delta X_{20}[6] + X_{20}[6] \cap \Delta X_{20}[15] + \Delta X_{20}[0] + \Delta X_0[14]$
20	10	$\Delta X_{20}[2] = 0$, $\Delta X_{20}[3] = 0$, $\Delta X_{20}[4] = 0$, $\Delta X_{20}[5] = 0$, $\Delta X_{20}[9] = 0$, $\Delta X_{20}[11] = 0$, $\Delta X_{20}[12] = 1$, $\Delta X_{20}[17] = 0$, $\Delta X_{20}[19] = 0$, $\Delta X_{20}[26] = 1$

Table 3: Conditions of Differential Path of 20-round SIMON32 Relating to the Secret Key

Rounds	Number of Conditions	Difference Conditions of i-th Round	Possible Guessed Subkeys	Conditions for Key Guess	Number of Key Values
2	7	$\Delta X_2[17] = 0$	$K_0[9]$		1
		$\Delta X_2[22] = 0$	$K_0[7]$		1
		$\Delta X_2[26] = 0$	$K_0[11]$		1
		$\Delta X_2[29] = 0$	$K_0[5]$		1
		$\Delta X_2[16] = 1$		$\Delta X_1[24] = 0$	1
			$K_0[1]$	$\Delta X_1[24] = 1$	
		$\Delta X_2[30] = 0$		$\Delta X_1[31] = 0$	1
			$K_0[6]$	$\Delta X_1[31] = 1$	
		$\Delta X_2[23] = 0$		$\Delta X_1[24] = 0$ and $\Delta X_1[31] = 0$	2
			$K_0[8]$	$\Delta X_1[24] = 0$ and $\Delta X_1[31] = 1$	
			$K_0[15]$	$\Delta X_1[24] = 1$ and $\Delta X_1[31] = 0$	
			$K_0[8] \oplus K_0[15]$	$\Delta X_1[24] = 1$ and $\Delta X_1[31] = 1$	
3	2	$\Delta X_3[31] = 0$	$K_1[7]$		1
		$\Delta X_3[24] = 0$	$K_1[9]$	$X_1[17] = 0$	2
			$K_1[9] \oplus K_0[10]$	$X_1[17] = 1$	
16	2	$\Delta X_{16}[10] = 0$	$K_{17}[11] \oplus K_{18}[13]$	$\Delta X_{18}[3] = 0$ and $\Delta X_{19}[5] = 0$	8
			$K_{19}[14] \oplus K_{17}[11] \oplus K_{18}[13]$	$\Delta X_{18}[3] = 0$ and $\Delta X_{19}[5] = 1$	
			$K_{18}[12] \oplus K_{17}[11] \oplus K_{18}[13]$	$\Delta X_{18}[3] = 1$ and $\Delta X_{19}[5] = 0$ and $\Delta X_{19}[4] = 0$	
			$K_{18}[12] \oplus K_{19}[13] \oplus K_{17}[11] \oplus K_{18}[13]$	$\Delta X_{18}[3] = 1$ and $\Delta X_{19}[5] = 0$ and $\Delta X_{19}[4] = 1$	
			$K_{18}[12] \oplus K_{19}[14] \oplus K_{17}[11] \oplus K_{18}[13]$	$\Delta X_{18}[3] = 1$ and $\Delta X_{19}[5] = 1$ and $\Delta X_{19}[4] = 0$	
			$K_{18}[12] \oplus K_{19}[13] \oplus K_{19}[14] \oplus K_{17}[11] \oplus K_{18}[13]$	$\Delta X_{18}[3] = 1$ and $\Delta X_{19}[5] = 1$ and $\Delta X_{19}[4] = 1$	
		$\Delta X_{16}[1] = 0$	$K_{19}[3]$, $K_{17}[9] \oplus K_{18}[11]$	$X_{19}[3] = 0$	2
			$K_{19}[3]$, $K_{17}[9] \oplus K_{18}[11] \oplus K_{19}[12]$	$X_{19}[3] = 1$	
17	5	$\Delta X_{17}[2] = 1$	$K_{19}[11]$	$\Delta X_{18}[10] = 0$	4
			$K_{19}[11]$, $K_{18}[3]$	$\Delta X_{18}[10] = 1$ and $\Delta X_{19}[11] = 0$	
			$K_{19}[11]$, $K_{18}[3] \oplus K_{19}[4]$	$\Delta X_{18}[10] = 1$ and $\Delta X_{19}[11] = 1$	
		$\Delta X_{17}[8] = 0$	$K_{18}[9]$	$X_{19}[1] = 0$	2
			$K_{18}[9] \oplus K_{19}[10]$	$X_{19}[1] = 1$	
		$\Delta X_{17}[0] = 0$	$K_{19}[2]$	$\Delta X_{18}[1] = 0$	2
			$K_{19}[2]$, $K_{18}[8]$	$\Delta X_{18}[1] = 1$	
		$\Delta X_{17}[9] = 0$		$\Delta X_{18}[1] = 0$ and $\Delta X_{18}[10] = 0$	2
			$K_{18}[1] \oplus K_{19}[3]$	$\Delta X_{18}[1] = 0$ and $\Delta X_{18}[10] = 1$	
			$K_{19}[12] \oplus K_{18}[10]$	$\Delta X_{18}[1] = 1$ and $\Delta X_{18}[10] = 0$	
			$K_{18}[1] \oplus K_{19}[3] \oplus K_{19}[12] \oplus K_{18}[10]$	$\Delta X_{18}[1] = 1$ and $\Delta X_{18}[10] = 1$	
		$\Delta X_{17}[15] = 0$	$K_{18}[7]$		1
		$\Delta X_{18}[6] = 0$	$K_{19}[7]$		1
18	7				

		$\Delta X_{18}[15] = 0$	$K_{19}[7]$		1/2
		$\Delta X_{18}[0] = 1$		$\Delta X_{19}[8] = 0$	1
			$K_{19}[1]$	$\Delta X_{19}[8] = 1$	
		$\Delta X_{18}[13] = 0$	$K_{19}[5]$		1
		$\Delta X_{18}[14] = 0$		$\Delta X_{19}[15] = 0$	1
			$K_{19}[6]$	$\Delta X_{19}[15] = 1$	
		$\Delta X_{18}[7] = 0$		$\Delta X_{19}[15] = 0$ and $\Delta X_{19}[8] = 0$	2
			$K_{19}[8]$	$\Delta X_{19}[15] = 1$ and $\Delta X_{19}[8] = 0$	
			$K_{19}[15]$	$\Delta X_{19}[15] = 0$ and $\Delta X_{19}[8] = 1$	
			$K_{19}[8] \oplus K_{19}[15]$	$\Delta X_{19}[15] = 1$ and $\Delta X_{19}[8] = 1$	
		$\Delta X_{18}[8] = 0$		$\Delta X_{19}[0] = 0$ and $\Delta X_{19}[9] = 0$	2
			$K_{19}[9]$	$\Delta X_{19}[0] = 1$ and $\Delta X_{19}[9] = 0$	
			$K_{19}[0]$	$\Delta X_{19}[0] = 0$ and $\Delta X_{19}[9] = 1$	
			$K_{19}[0] \oplus K_{19}[9]$	$\Delta X_{19}[0] = 1$ and $\Delta X_{19}[0] = 1$	

Table 4: Conditions of Differential Path of 21-round SIMON32 are Independent of Subkeys

Rounds	Number of Conditions	Difference Conditions of i-th Round
input	4	$\Delta X_0[17] = 0$, $\Delta X_0[19] = 0$, $\Delta X_0[23] = 0$, $\Delta X_0[26] = 1$
1	9	$\Delta X_1[18] = 0$, $\Delta X_1[19] = 0$, $\Delta X_1[20] = 0$, $\Delta X_1[21] = 0$, $\Delta X_1[24] = 0$, $\Delta X_1[25] = 0$, $\Delta X_1[27] = 0$, $\Delta X_1[28] = 1$, $\Delta X_1[31] = 0$
20	8	$\Delta X_{20}[4] = 0$, $\Delta X_{20}[5] = 0$, $\Delta X_{20}[6] = 0$, $\Delta X_{20}[7] = 0$, $\Delta X_{20}[11] = 0$, $\Delta X_{20}[12] = 0$, $\Delta X_{20}[13] = 0$, $\Delta X_{20}[14] = 1$
21	10	$\Delta X_{21}[2] = 0$, $\Delta X_{21}[3] = 0$, $\Delta X_{21}[4] = 0$, $\Delta X_{21}[5] = 0$, $\Delta X_{21}[9] = 0$, $\Delta X_{21}[11] = 0$, $\Delta X_{21}[12] = 1$, $\Delta X_{21}[17] = 0$, $\Delta X_{21}[19] = 0$, $\Delta X_{21}[26] = 1$

Table 5: Conditions of Differential Path of 21-round SIMON32 Relating to the Secret Key

Rounds	Number of Conditions	Difference Conditions of i-th Round	Possible Guessed Subkeys	Conditions for Key Guess	Number of Key Values
2	10	$\Delta X_2[16] = 0$		$\Delta X_1[17] = 0$	1
			$K_0[8]$	$\Delta X_1[17] = 1$	
		$\Delta X_2[18] = 0$		$\Delta X_1[26] = 0$	1
			$K_0[3]$	$\Delta X_1[26] = 1$	
		$\Delta X_2[22] = 0$		$\Delta X_1[23] = 0$ and $\Delta X_1[30] = 0$	2
			$K_0[7]$	$\Delta X_1[23] = 0$ and $\Delta X_1[30] = 1$	
			$K_0[14]$	$\Delta X_1[23] = 1$ and $\Delta X_1[30] = 0$	
			$K_0[7] \oplus K_0[14]$	$\Delta X_1[23] = 1$ and $\Delta X_1[30] = 1$	
		$\Delta X_2[21] = 0$		$\Delta X_1[22] = 0$ and $\Delta X_1[29] = 0$	2
			$K_0[6]$	$\Delta X_1[22] = 0$ and $\Delta X_1[29] = 1$	
			$K_0[13]$	$\Delta X_1[22] = 1$ and $\Delta X_1[29] = 0$	
			$K_0[6] \oplus K_0[13]$	$\Delta X_1[22] = 1$ and $\Delta X_1[29] = 1$	
		$\Delta X_2[27] = 0$	$K_0[3]$		1/2
		$\Delta X_2[20] = 0$	$K_0[5]$		1
		$\Delta X_2[29] = 0$		$\Delta X_1[30] = 0$	1/2
			$K_0[5]$	$\Delta X_1[30] = 1$	
		$\Delta X_2[30] = 0$		$\Delta X_1[22] = 0$	1
			$K_0[15]$	$\Delta X_1[22] = 1$	
		$\Delta X_2[28] = 0$		$\Delta X_1[29] = 0$	1
			$K_0[4]$	$\Delta X_1[29] = 1$	
		$\Delta X_2[25] = 0$		$\Delta X_1[26] = 0$ and $\Delta X_1[17] = 0$	2
			$K_0[10]$	$\Delta X_1[26] = 0$ and $\Delta X_1[17] = 1$	

			$K_0[1]$	$\Delta X_1[26] = 1$ and $\Delta X_1[17] = 0$	
			$K_0[10] \oplus K_0[1]$	$\Delta X_1[26] = 1$ and $\Delta X_1[17] = 1$	
		$\Delta X_3[17] = 0$	$K_0[11] \oplus K_1[9]$		1
		$\Delta X_3[23] = 0$	$K_0[9]$,$K_0[0]$	$\Delta X_2[24] = 0$ and $\Delta X_2[31] = 0$	
			$K_0[9]$,$K_0[0]$,$K_1[8]$	$\Delta X_2[24] = 0$ and $\Delta X_2[31] = 1$	8
			$K_0[9]$,$K_0[0]$,$K_1[15]$	$\Delta X_2[24] = 1$ and $\Delta X_2[31] = 0$	
3	7		$K_0[9]$, $K_0[0]$,$K_1[8] \oplus K_1[15]$	$\Delta X_2[24] = 1$ and $\Delta X_2[31] = 1$	
		$\Delta X_3[22] = 0$	$K_1[7]$		1
		$\Delta X_3[29] = 0$	$K_1[5]$		1
		$\Delta X_3[30] = 0$		$\Delta X_2[31] = 0$	1
			$K_1[6]$	$\Delta X_2[31] = 1$	
		$\Delta X_3[26] = 1$	$K_1[11]$	$X_1[19] = 0$	2
			$K_1[11] \oplus K_0[12]$	$X_1[19] = 1$	
		$\Delta X_3[16] = 0$		$\Delta X_2[24] = 0$	2
			$K_1[1]$	$\Delta X_2[24] = 1$ and $X_1[25] = 0$	
			$K_1[1] \oplus K_0[2]$	$\Delta X_2[24] = 1$ and $X_1[25] = 1$	
		$\Delta X_4[31] = 0$	$K_2[7]$		1
4	2	$\Delta X_4[24] = 0$	$K_2[9]$	$X_2[17] = 0$	4
			$K_2[9] \oplus K_1[10]$	$X_2[17] = 1$ and $X_1[18] = 0$	
			$K_2[9] \oplus K_1[10] \oplus K_0[11]$	$X_2[17] = 1$ and $X_1[18] = 1$	
		$\Delta X_{18}[15] = 0$	$K_{19}[7]$		1
		$\Delta X_{17}[10] = 0$	$K_{18}[11] \oplus K_{19}[13]$	$\Delta X_{19}[3] = 0$ and $\Delta X_{20}[5] = 0$	
			$K_{20}[14] \oplus K_{18}[11] \oplus K_{19}[13]$	$\Delta X_{19}[3] = 0$ and $\Delta X_{20}[5] = 1$	
17	2		$K_{19}[12] \oplus K_{18}[11] \oplus K_{19}[13]$	$\Delta X_{19}[3] = 1$ and $\Delta X_{20}[5] = 0$ and $\Delta X_{19}[4] = 0$	
			$K_{19}[12] \oplus K_{20}[13] \oplus K_{18}[11] \oplus K_{19}[13]$	$\Delta X_{19}[3] = 1$ and $\Delta X_{20}[5] = 0$ and $\Delta X_{20}[4] = 1$	8
			$K_{19}[12] \oplus K_{20}[14] \oplus K_{18}[11] \oplus K_{19}[13]$	$\Delta X_{19}[3] = 1$ and $\Delta X_{20}[5] = 1$ and $\Delta X_{20}[4] = 0$	
			$K_{19}[12] \oplus K_{20}[13] \oplus K_{20}[14] \oplus K_{18}[11] \oplus K_{19}[13]$	$\Delta X_{19}[3] = 1$ and $\Delta X_{20}[5] = 1$ and $\Delta X_{20}[4] = 1$	
		$\Delta X_{17}[1] = 0$	$K_{20}[3]$, $K_{18}[9] \oplus K_{19}[11]$	$X_{20}[3] = 0$	4
			$K_{20}[3]$, $K_{18}[9] \oplus K_{19}[11] \oplus K_{20}[12]$	$X_{20}[3] = 1$	
		$\Delta X_{18}[2] = 1$	$K_{20}[11]$	$\Delta X_{19}[10] = 0$	
			$K_{20}[11]$, $K_{19}[3]$	$\Delta X_{19}[10] = 1$ and $\Delta X_{20}[11] = 0$	4
			$K_{20}[11]$, $K_{19}[3] \oplus K_{20}[4]$	$\Delta X_{19}[10] = 1$ and $\Delta X_{20}[11] = 1$	
18	5	$\Delta X_{18}[8] = 0$	$K_{19}[9]$	$X_{20}[1] = 0$	2
			$K_{19}[9] \oplus K_{20}[10]$	$X_{20}[1] = 1$	
		$\Delta X_{18}[0] = 0$	$K_{20}[2]$	$\Delta X_{19}[1] = 0$	2
			$K_{20}[2]$, $K_{19}[8]$	$\Delta X_{19}[1] = 1$	
		$\Delta X_{18}[9] = 0$		$\Delta X_{18}[1] = 0$ and $\Delta X_{19}[10] = 0$	
			$K_{19}[1] \oplus K_{20}[3]$	$\Delta X_{19}[1] = 0$ and $\Delta X_{19}[10] = 1$	2
			$K_{20}[12] \oplus K_{19}[10]$	$\Delta X_{19}[1] = 1$ and $\Delta X_{19}[10] = 0$	
			$K_{19}[1] \oplus K_{20}[3] \oplus K_{20}[12] \oplus K_{19}[10]$	$\Delta X_{19}[1] = 1$ and $\Delta X_{19}[10] = 1$	
		$\Delta X_{19}[6] = 0$	$K_{20}[7]$		1
		$\Delta X_{19}[15] = 0$	$K_{20}[7]$		1/2
		$\Delta X_{19}[0] = 1$		$\Delta X_{20}[8] = 0$	1
19	7		$K_{20}[1]$	$\Delta X_{20}[8] = 1$	
		$\Delta X_{19}[13] = 0$	$K_{20}[5]$		1
		$\Delta X_{19}[14] = 0$		$\Delta X_{20}[15] = 0$	1
			$K_{20}[6]$	$\Delta X_{20}[15] = 1$	
		$\Delta X_{19}[7] = 0$		$\Delta X_{20}[15] = 0$ and $\Delta X_{20}[8] = 0$	
			$K_{20}[8]$	$\Delta X_{20}[15] = 1$ and $\Delta X_{20}[8] = 0$	2
			$K_{20}[15]$	$\Delta X_{20}[15] = 0$ and $\Delta X_{20}[8] = 1$	
			$K_{20}[8] \oplus K_{20}[15]$	$\Delta X_{20}[15] = 1$ and $\Delta X_{20}[8] = 1$	
		$\Delta X_{19}[8] = 0$		$\Delta X_{20}[0] = 0$ and $\Delta X_{20}[9] = 0$	
			$K_{20}[9]$	$\Delta X_{20}[0] = 1$ and $\Delta X_{20}[9] = 0$	2
			$K_{20}[0]$	$\Delta X_{20}[0] = 0$ and $\Delta X_{20}[9] = 1$	
			$K_{20}[0] \oplus K_{20}[9]$	$\Delta X_{20}[0] = 1$ and $\Delta X_{20}[0] = 1$	

Table 6: Conditions of Differential Path of 21-round SIMON48 are Independent of Subkeys

Rounds	Number of Conditions	Difference Conditions of i-th Round
input	13	$\Delta X_0[7] = 0$, $\Delta X_0[14] = 0$, $\Delta X_0[21] = 0$, $\Delta X_0[27] = 0$, $\Delta X_0[29] = 0$, $\Delta X_0[32] = 0$, $\Delta X_0[33] = 0$, $\Delta X_0[39] = 0$, $\Delta X_0[40] = 1$, $\Delta X_0[44] = 1$, $\Delta X_0[45] = 0$ $\Delta X_0[46] = 0$, $\Delta X_0[47] = 0$
1	15	$\Delta X_1[24] = 0, \Delta X_1[24] = X_0[25] \cap \Delta X_0[32] \oplus \Delta X_0[25] \cap X_0[32] \oplus \Delta X_0[26] \oplus \Delta X_0[0]$ $\Delta X_1[25] = 0, \Delta X_1[25] = X_0[26] \cap \Delta X_0[33] \oplus \Delta X_0[26] \cap X_0[33] \oplus \Delta X_0[27] \oplus \Delta X_0[1]$ $\Delta X_1[26] = 0, \Delta X_1[26] = X_0[27] \cap \Delta X_0[34] \oplus \Delta X_0[27] \cap X_0[34] \oplus \Delta X_0[28] \oplus \Delta X_0[2]$ $\Delta X_1[28] = 0, \Delta X_1[28] = X_0[29] \cap \Delta X_0[36] \oplus \Delta X_0[29] \cap X_0[36] \oplus \Delta X_0[30] \oplus \Delta X_0[4]$ $\Delta X_1[29] = 0, \Delta X_1[29] = X_0[30] \cap \Delta X_0[37] \oplus \Delta X_0[30] \cap X_0[37]$ $\Delta X_1[30] = 0, \Delta X_1[30] = \Delta X_0[32] \oplus \Delta X_0[6]$ $\Delta X_1[33] = 0, \Delta X_1[33] = X_0[34] \cap \Delta X_0[41] \oplus \Delta X_0[34] \cap X_0[41] \oplus \Delta X_0[35]$ $\Delta X_1[34] = 0, \Delta X_1[34] = X_0[35] \cap \Delta X_0[42] \oplus \Delta X_0[35] \cap X_0[42] \oplus \Delta X_0[36] \oplus \Delta X_0[10]$ $\Delta X_1[35] = 0, \Delta X_1[35] = X_0[36] \cap \Delta X_0[43] \oplus \Delta X_0[36] \cap X_0[43] \oplus \Delta X_0[37] \oplus \Delta X_0[11]$ $\Delta X_1[37] = 0, \Delta X_1[37] = \Delta X_0[39] \oplus \Delta X_0[13]$ $\Delta X_1[40] = 0, \Delta X_1[40] = X_0[41] \cap \Delta X_0[24]$ $\Delta X_1[41] = 0, \Delta X_1[41] = X_0[42] \cap \Delta X_0[25] \oplus \Delta X_0[42] \cap X_0[25] \oplus \Delta X_0[43] \oplus \Delta X_0[17]$ $\Delta X_1[42] = 0, \Delta X_1[42] = X_0[43] \cap \Delta X_0[26] \oplus \Delta X_0[43] \cap X_0[26] \oplus \Delta X_0[44] \oplus \Delta X_0[18]$ $\Delta X_1[46] = 0, \Delta X_1[46] = X_0[47] \cap \Delta X_0[30] \oplus \Delta X_0[47] \cap X_0[30] \oplus \Delta X_0[24]$ $\Delta X_1[47] = 0, \Delta X_1[47] = \Delta X_0[24] \cap X_0[31] \oplus \Delta X_0[25]$
2	3	$\Delta X_2[25] = 0, \Delta X_2[25] = \Delta X_1[27] \oplus \Delta X_0[25]$ $\Delta X_2[34] = 0, \Delta X_2[34] = \Delta X_1[36] \oplus \Delta X_0[34]$ $\Delta X_2[41] = 0, \Delta X_2[41] = \Delta X_1[43] \oplus \Delta X_0[41]$
18	2	$\Delta X_{19}[6] = 0, \Delta X_{19}[6] = \Delta X_{20}[8] \oplus \Delta X_{21}[6]$ $\Delta X_{19}[13] = 0, \Delta X_{19}[13] = \Delta X_{20}[15] \oplus \Delta X_{21}[13]$
19	14	$\Delta X_{19}[0] = 0$, $\Delta X_{19}[0] = \Delta X_{19}[1] \cap X_{19}[8] \oplus \Delta X_{19}[2] \oplus \Delta X_0[24]$ $\Delta X_{19}[1] = 0$, $\Delta X_{19}[1] = X_{19}[2] \cap \Delta X_{19}[9] \oplus \Delta X_{19}[2] \cap X_{19}[9] \oplus \Delta X_{19}[3] \oplus \Delta X_0[25]$ $\Delta X_{19}[2] = 1$, $\Delta X_{19}[2] = X_{19}[3] \cap \Delta X_{19}[10] \oplus \Delta X_{19}[3] \cap X_{19}[10] \oplus \Delta X_{19}[4] \oplus \Delta X_0[26]$ $\Delta X_{19}[5] = 0$, $\Delta X_{19}[5] = X_{19}[6] \cap \Delta X_{19}[13] \oplus \Delta X_{19}[6] \cap X_{19}[13] \oplus \Delta X_{19}[7] \oplus \Delta X_0[29]$ $\Delta X_{19}[6] = 0$, $\Delta X_{19}[6] = X_{19}[7] \cap \Delta X_{19}[14] \oplus \Delta X_{19}[7] \cap X_{19}[14] \oplus \Delta X_{19}[8] \oplus \Delta X_0[30]$ $\Delta X_{19}[7] = 0$, $\Delta X_{19}[7] = \Delta X_{19}[8] \cap X_{19}[15] \oplus \Delta X_{19}[9] \oplus \Delta X_0[31]$ $\Delta X_{19}[9] = 0$, $\Delta X_{19}[9] = X_{19}[10] \cap \Delta X_{19}[17] \oplus \Delta X_{19}[10] \cap X_{19}[17] \oplus \Delta X_{19}[11] \oplus \Delta X_0[33]$ $\Delta X_{19}[10] = 1$, $\Delta X_{19}[10] = X_{19}[11] \cap \Delta X_{19}[18] \oplus \Delta X_{19}[11] \cap X_{19}[18] \oplus \Delta X_{19}[12] \oplus \Delta X_0[34]$ $\Delta X_{19}[13] = 0$,$\Delta X_{19}[13] = \Delta X_{19}[14] \cap X_{19}[21] \oplus \Delta X_{19}[15] \oplus \Delta X_0[37]$ $\Delta X_{19}[16] = 0$, $\Delta X_{19}[16] = X_{19}[17] \cap \Delta X_{19}[24] \oplus \Delta X_{19}[17] \cap X_{19}[24] \oplus \Delta X_{19}[18] \oplus \Delta X_0[40]$ $\Delta X_{19}[17] = 0$, $\Delta X_{19}[17] = X_{19}[18] \cap \Delta X_{19}[25] \oplus \Delta X_{19}[18] \cap X_{19}[25] \oplus \Delta X_{19}[19] \oplus \Delta X_0[41]$ $\Delta X_{19}[18] = 1$, $\Delta X_{19}[18] = X_{19}[19] \cap \Delta X_{19}[26] \oplus \Delta X_{19}[19] \cap X_{19}[26] \oplus \Delta X_{19}[20] \oplus \Delta X_0[42]$ $\Delta X_{19}[22] = 0$, $\Delta X_{19}[22] = X_{19}[23] \cap \Delta X_{19}[30] \oplus \Delta X_{19}[24] \oplus \Delta X_0[46]$ $\Delta X_{19}[23] = 0$,$\Delta X_{19}[23] = X_{19}[24] \cap \Delta X_{19}[31] \oplus \Delta X_{19}[24] \cap X_{19}[31] \oplus \Delta X_{19}[25] \oplus \Delta X_0[47]$
20	9	$\Delta X_{20}[5] = 0$, $\Delta X_{20}[8] = 1$, $\Delta X_{20}[15] = 0$, $\Delta X_{20}[16] = 0$, $\Delta X_{20}[21] = 0$, $\Delta X_{20}[22] = 0$, $\Delta X_{20}[23] = 1$, $\Delta X_{20}[38] = 0$, $\Delta X_{20}[45] = 0$

Table 7: Conditions of Differential Path of 21-round SIMON48 Relating to the Secret Key

Rounds	Number of Conditions	Difference Conditions of i-th Round	Possible Guessed Subkeys	Conditions for Key Guess	Number of Key Values

2	11	$\Delta X_2[24] = 1$		$\Delta X_1[32] = 0$	1
			$K_0[1]$	$\Delta X_1[32] = 1$	
		$\Delta X_2[26] = 0$		$\Delta X_1[27] = 0$	1
			$K_0[10]$	$\Delta X_1[27] = 1$	
		$\Delta X_2[28] = 0$		$\Delta X_1[36] = 0$	1
			$K_0[5]$	$\Delta X_1[36] = 1$	
		$\Delta X_2[36] = 0$		$\Delta X_1[44] = 0$	1
			$K_0[13]$	$\Delta X_1[44] = 1$	
		$\Delta X_2[38] = 0$		$\Delta X_1[39] = 0$	1
			$K_0[22]$	$\Delta X_1[39] = 1$	
		$\Delta X_2[42] = 0$		$\Delta X_1[43] = 0$	1
			$K_0[2]$	$\Delta X_1[43] = 1$	
		$\Delta X_2[30] = 0$	$K_0[7]$		1
		$\Delta X_2[31] = 0$		$\Delta X_1[32]$=0 and $\Delta X_1[39]$=0	2
			$K_0[8]$	$\Delta X_1[32]$=0 and $\Delta X_1[39]$=1	
			$K_0[15]$	$\Delta X_1[32]$=1 and $\Delta X_1[39]$=0	
			$K_0[8] \oplus K_0[15]$	$\Delta X_1[32]$=1 and $\Delta X_1[39]$=1	
		$\Delta X_2[35] = 0$		$\Delta X_1[36]$=0 and $\Delta X_1[43]$=0	2
			$K_0[19]$	$\Delta X_1[36]$=1 and $\Delta X_1[43]$=0	
			$K_0[12]$	$\Delta X_1[36]$=0 and $\Delta X_1[43]$=1	
			$K_0[12] \oplus K_0[19]$	$\Delta X_1[36]$=1 and $\Delta X_1[43]$=1	
		$\Delta X_2[37] = 0$	$K_0[21]$		1
		$\Delta X_2[43] = 0$		$\Delta X_1[44]$=0 and $\Delta X_1[27]$=0	2
			$K_0[3]$	$\Delta X_1[44]$=1 and $\Delta X_1[27]$=0	
			$K_0[20]$	$\Delta X_1[44]$=0 and $\Delta X_1[27]$=1	
			$K_0[3] \oplus K_0[20]$	$\Delta X_1[44]$=1 and $\Delta X_1[27]$=1	
3	6	$\Delta X_3[27] = 0$	$K_1[11]$		1
		$\Delta X_3[44] = 0$	$K_1[21] \oplus K_0[23]$		1
		$\Delta X_3[32] = 0$	$K_1[9]$	$X_1[34] = 0$	2
			$K_1[9] \oplus K_0[17]$	$X_1[34] = 1$	
		$\Delta X_3[36] = 0$	$K_1[13]$	$X_1[45] = 0$	2
			$K_1[13] \oplus K_0[14]$	$X_1[45] = 1$	
		$\Delta X_3[39] = 0$	$K_1[23]$	$X_1[31] = 0$	2
			$K_1[23] \oplus K_0[0]$	$X_1[31] = 1$	
		$\Delta X_3[43] = 0$	$K_0[4]$, $K_1[3]$	$X_1[28] = 0$	4
			$K_0[4]$, $K_1[3] \oplus K_0[11]$	$X_1[28] = 1$	
18	8	$\Delta X_{18}[3] = 0$	$K_{19}[11]$		1
		$\Delta X_{18}[8] = 0$	$K_{19}[9]$		1
		$\Delta X_{18}[11] = 0$	$K_{19}[19]$		1
		$\Delta X_{18}[12] = 0$	$K_{19}[13]$	$X_{20}[21] = 0$	2
			$K_{19}[13] \oplus K_{20}[14]$	$X_{20}[21] = 1$	
		$\Delta X_{18}[4] = 0$	$K_{19}[5]$	$X_{20}[13] = 0$	2
			$K_{19}[5] \oplus K_{20}[6]$	$X_{20}[13] = 1$	
		$\Delta X_{18}[19] = 0$	$K_{19}[3]$		1
		$\Delta X_{18}[20] = 0$	$K_{19}[21] \oplus K_{20}[23]$		1
		$\Delta X_{18}[15] = 0$	$K_{20}[0], K_{19}[23]$	$X_{20}[0] = 0$	4
			$K_{20}[0], K_{19}[23] \oplus K_{20}[7]$	$X_{20}[0] = 1$	
19	15	$\Delta X_{19}[0] = 0$		$\Delta X_{20}[8]$=0	1
			$K_{20}[1]$	$\Delta X_{20}[8]$=1	
		$\Delta X_{19}[17] = 0$	$K_{20}[1]$		1/2
		$\Delta X_{19}[4] = 1$		$\Delta X_{20}[12]$=0	1
			$K_{20}[5]$	$\Delta X_{20}[12]$=1	
		$\Delta X_{19}[14] = 0$		$\Delta X_{20}[15] = 0$	1
			$K_{20}[22]$	$\Delta X_{20}[15] = 1$	
		$\Delta X_{19}[12] = 1$		$\Delta X_{20}[20]$=0	1
			$K_{20}[13]$	$\Delta X_{20}[20]$=1	
		$\Delta X_{19}[20] = 1$		$\Delta X_{20}[4]$=0	1
			$K_{20}[21]$	$\Delta X_{20}[4]$=1	
		$\Delta X_{19}[1] = 0$	$K_{20}[9]$		1
		$\Delta X_{19}[2] = 0$		$\Delta X_{20}[3]$=0 and $\Delta X_{20}[10]$=0	2

			$K_{20}[3]$	$\Delta X_{20}[3]$=0 and $\Delta X_{20}[10]$=1	
			$K_{20}[10]$	$\Delta X_{20}[3]$=1 and $\Delta X_{20}[10]$=0	
			$K_{20}[3] \oplus K_{20}[10]$	$\Delta X_{20}[3]$=1 and $\Delta X_{20}[10]$=1	
		$\Delta X_{19}[3] = 0$		$\Delta X_{20}[4]$=0 and $\Delta X_{20}[11]$=0	2
			$K_{20}[4]$	$\Delta X_{20}[4]$=0 and $\Delta X_{20}[11]$=1	
			$K_{20}[11]$	$\Delta X_{20}[4]$=1 and $\Delta X_{20}[11]$=0	
			$K_{20}[4] \oplus K_{20}[11]$	$\Delta X_{20}[4]$=1 and $\Delta X_{20}[11]$=1	
		$\Delta X_{19}[7] = 0$		$\Delta X_{20}[8]$=0 and $\Delta X_{20}[15]$=0	2
			$K_{20}[8]$	$\Delta X_{20}[8]$=0 and $\Delta X_{20}[15]$=1	
			$K_{20}[15]$	$\Delta X_{20}[8]$=1 and $\Delta X_{20}[15]$=0	
			$K_{20}[8] \oplus K_{20}[15]$	$\Delta X_{20}[8]$=1 and $\Delta X_{20}[15]$=1	
		$\Delta X_{19}[9] = 0$	$K_{20}[17]$		1
		$\Delta X_{19}[10] = 0$		$\Delta X_{20}[11]$=0	1
			$K_{20}[18]$	$\Delta X_{20}[11]$=1	
		$\Delta X_{19}[11] = 0$		$\Delta X_{20}[12]$=0 and $\Delta X_{20}[19]$=0	2
			$K_{20}[12]$	$\Delta X_{20}[12]$=0 and $\Delta X_{20}[19]$=1	
			$K_{20}[19]$	$\Delta X_{20}[12]$=1 and $\Delta X_{20}[19]$=0	
			$K_{20}[12] \oplus K_{20}[19]$	$\Delta X_{20}[12]$=1 and $\Delta X_{20}[19]$=1	
		$\Delta X_{19}[18] = 0$		$\Delta X_{20}[19]$=0	1
			$K_{20}[2]$	$\Delta X_{20}[19]$=1	
		$\Delta X_{19}[19] = 0$		$\Delta X_{20}[3]$=0	1
			$K_{20}[20]$	$\Delta X_{20}[3]$=1	

Table 8: Conditions of Differential Path of 22-round SIMON48 are Independent of Subkeys

Rounds	Number of Conditions	Difference Conditions of i-th Round
input	13	$\Delta X_0[7] = 0$, $\Delta X_0[14] = 0$, $\Delta X_0[21] = 0$, $\Delta X_0[27] = 0$, $\Delta X_0[29] = 0$, $\Delta X_0[32] = 0$, $\Delta X_0[33] = 0$, $\Delta X_0[39] = 0$, $\Delta X_0[40] = 1$, $\Delta X_0[44] = 1$, $\Delta X_0[45] = 0$, $\Delta X_0[46] = 0$, $\Delta X_0[47] = 0$
1	15	$\Delta X_1[24] = 0$, $\Delta X_1[25] = 0$, $\Delta X_1[26] = 0$, $\Delta X_1[28] = 0$, $\Delta X_1[29] = 0$, $\Delta X_1[30] = 0$, $\Delta X_1[33] = 0$, $\Delta X_1[34] = 0$, $\Delta X_1[35] = 0$, $\Delta X_1[37] = 0$, $\Delta X_1[40] = 0$, $\Delta X_1[41] = 0$, $\Delta X_1[42] = 0$, $\Delta X_1[46] = 0$, $\Delta X_1[47] = 0$
2	3	$\Delta X_2[25] = 0, \Delta X_2[25] = \Delta X_1[27] \oplus \Delta X_0[25]$ $\Delta X_2[34] = 0, \Delta X_2[34] = \Delta X_1[36] \oplus \Delta X_0[34]$ $\Delta X_2[41] = 0, \Delta X_2[41] = \Delta X_1[43] \oplus \Delta X_0[41]$
19	1	$\Delta X_{19}[13] = 0, \Delta X_{19}[13] = \Delta X_{21}[17] \oplus \Delta X_{22}[15] \oplus \Delta X_{21}[13]$
20	7	$\Delta X_{20}[5] = 0$, $\Delta X_{20}[8] = 1$, $\Delta X_{20}[15] = 0$, $\Delta X_{20}[16] = 0$, $\Delta X_{20}[21] = 0$, $\Delta X_{20}[22] = 0$, $\Delta X_{20}[23] = 0$
21	2	$\Delta X_{21}[14] = 0$, $\Delta X_{21}[21] = 0$

Table 9: Conditions of Differential Path of 22-round SIMON48 Relating to the Secret Key

Rounds	Number of Conditions	Difference Conditions of i-th Round	Possible Guessed Subkeys	Conditions for Key Guess	Number of Key Values
2	11	$\Delta X_2[24] = 1$		$\Delta X_1[32] = 0$	1
			$K_0[1]$	$\Delta X_1[32] = 1$	
		$\Delta X_2[26] = 0$		$\Delta X_1[27] = 0$	1
			$K_0[10]$	$\Delta X_1[27] = 1$	
		$\Delta X_2[28] = 0$		$\Delta X_1[36] = 0$	1
			$K_0[5]$	$\Delta X_1[36] = 1$	
		$\Delta X_2[36] = 0$		$\Delta X_1[44] = 0$	1
			$K_0[13]$	$\Delta X_1[44] = 1$	
		$\Delta X_2[38] = 0$		$\Delta X_1[39] = 0$	1

			$K_0[22]$	$\Delta X_1[39] = 1$	
		$\Delta X_2[42] = 0$		$\Delta X_1[43] = 0$	1
			$K_0[2]$	$\Delta X_1[43] = 1$	
		$\Delta X_2[31] = 0$		$\Delta X_1[32]$=0 and $\Delta X_1[39]$=0	2
			$K_0[8]$	$\Delta X_1[32]$=0 and $\Delta X_1[39]$=1	
			$K_0[15]$	$\Delta X_1[32]$=1 and $\Delta X_1[39]$=0	
			$K_0[8] \oplus K_0[15]$	$\Delta X_1[32]$=1 and $\Delta X_1[39]$=1	
		$\Delta X_2[35] = 0$		$\Delta X_1[36]$=0 and $\Delta X_1[43]$=0	2
			$K_0[19]$	$\Delta X_1[36]$=1 and $\Delta X_1[43]$=0	
			$K_0[12]$	$\Delta X_1[36]$=0 and $\Delta X_1[43]$=1	
			$K_0[12] \oplus K_0[19]$	$\Delta X_1[36]$=1 and $\Delta X_1[43]$=1	
		$\Delta X_2[37] = 0$	$K_0[21]$		1
		$\Delta X_2[30] = 0$	$K_0[7]$		1
		$\Delta X_2[43] = 0$		$\Delta X_1[44]$=0 and $\Delta X_1[27]$=0	2∗
			$K_0[3]$	$\Delta X_1[44]$=1 and $\Delta X_1[27]$=0	
			$K_0[20]$	$\Delta X_1[44]$=0 and $\Delta X_1[27]$=1	
			$K_0[3] \oplus K_0[20]$	$\Delta X_1[44]$=1 and $\Delta X_1[27]$=1	
3	6	$\Delta X_3[27] = 0$	$K_1[11]$		1
		$\Delta X_3[44] = 0$	$K_1[21] \oplus K_0[23]$		1
		$\Delta X_3[32] = 0$	$K_1[9]$	$X_1[34] = 0$	2∗
			$K_1[9] \oplus K_0[17]$	$X_1[34] = 1$	
		$\Delta X_3[36] = 0$	$K_1[13]$	$X_1[45] = 0$	2∗
			$K_1[13] \oplus K_0[14]$	$X_1[45] = 1$	
		$\Delta X_3[39] = 0$	$K_1[23]$	$X_1[31] = 0$	2∗
			$K_1[23] \oplus K_0[0]$	$X_1[31] = 1$	
		$\Delta X_3[43] = 0$	$K_0[4],\ K_1[3]$	$X_1[28] = 0$	4∗
			$K_0[4],\ K_1[3] \oplus K_0[11]$	$X_1[28] = 1$	
18	8	$\Delta X_{18}[3] = 0$	$K_{19}[11]$		1
		$\Delta X_{18}[8] = 0$	$K_{19}[9]$		1
		$\Delta X_{18}[11] = 0$	$K_{19}[19]$		1
		$\Delta X_{18}[12] = 0$	$K_{19}[13]$	$X_{20}[21] = 0$	2∗
			$K_{19}[13] \oplus K_{20}[14]$	$X_{20}[21] = 1$	
		$\Delta X_{18}[4] = 0$	$K_{19}[5]$	$X_{20}[13] = 0$	2
			$K_{19}[5] \oplus K_{20}[6]$	$X_{20}[13] = 1$	
		$\Delta X_{18}[19] = 0$	$K_{19}[3]$		1
		$\Delta X_{18}[20] = 0$	$K_{19}[21] \oplus K_{20}[23]$		1∗
		$\Delta X_{18}[15] = 0$	$K_{20}[0], K_{19}[23]$	$X_{20}[0] = 0$	4∗
			$K_{20}[0], K_{19}[23] \oplus K_{20}[7]$	$X_{20}[0] = 1$	
19	16	$\Delta X_{19}[6] = 0$	$K_{21}[16]$		1
		$\Delta X_{19}[0] = 0$	$K_{20}[1]$		1
		$\Delta X_{19}[17] = 0$	$K_{21}[20]$		1
		$\Delta X_{19}[1] = 0$	$K_{20}[9]$		1
		$\Delta X_{19}[2] = 0$	$K_{21}[5],\ K_{21}[4]$	$\Delta X_{20}[3]$=0 and $\Delta X_{20}[10]$=0	8
			$K_{21}[5],\ K_{21}[4],\ K_{20}[3]$	$\Delta X_{20}[3]$=0 and $\Delta X_{20}[10]$=1	
			$K_{21}[5],\ K_{21}[4],\ K_{20}[10]$	$\Delta X_{20}[3]$=1 and $\Delta X_{20}[10]$=0	
			$K_{21}[5], K_{21}[4], K_{20}[3] \oplus K_{20}[10]$	$\Delta X_{20}[3]$=1 and $\Delta X_{20}[10]$=1	
		$\Delta X_{19}[3] = 0$	$K_{21}[12]$	$\Delta X_{20}[4]$=0 and $\Delta X_{20}[11]$=0	4
			$K_{21}[12], K_{20}[4]$	$\Delta X_{20}[4]$=0 and $\Delta X_{20}[11]$=1	
			$K_{21}[12], K_{20}[11]$	$\Delta X_{20}[4]$=1 and $\Delta X_{20}[11]$=0	
			$K_{21}[12], K_{20}[4] \oplus K_{20}[11]$	$\Delta X_{20}[4]$=1 and $\Delta X_{20}[11]$=1	
		$\Delta X_{19}[4] = 1$		$\Delta X_{20}[12]$=0	1
			$K_{20}[5]$	$\Delta X_{20}[12]$=1	
		$\Delta X_{19}[7] = 0$		$\Delta X_{20}[8]$=0 and $\Delta X_{20}[15]$=0	2
			$K_{20}[8]$	$\Delta X_{20}[8]$=0 and $\Delta X_{20}[15]$=1	
			$K_{20}[15]$	$\Delta X_{20}[8]$=1 and $\Delta X_{20}[15]$=0	
			$K_{20}[8] \oplus K_{20}[15]$	$\Delta X_{20}[8]$=1 and $\Delta X_{20}[15]$=1	
		$\Delta X_{19}[9] = 0$	$K_{20}[17]$		1
		$\Delta X_{19}[10] = 0$		$\Delta X_{20}[11]$=0	1
			$K_{20}[18]$	$\Delta X_{20}[11]$=1	

		$\Delta X_{19}[11] = 0$		$\Delta X_{20}[12]$=0 and $\Delta X_{20}[19]$=0	2
			$K_{20}[12]$	$\Delta X_{20}[12]$=0 and $\Delta X_{20}[19]$=1	
			$K_{20}[19]$	$\Delta X_{20}[12]$=1 and $\Delta X_{20}[19]$=0	
			$K_{20}[12] \oplus K_{20}[19]$	$\Delta X_{20}[12]$=1 and $\Delta X_{20}[19]$=1	
		$\Delta X_{19}[12] = 1$		$\Delta X_{20}[20]$=0	1
			$K_{20}[13]$	$\Delta X_{20}[20]$=1	
		$\Delta X_{19}[14] = 0$		$\Delta X_{20}[15] = 0$	1
			$K_{20}[22]$	$\Delta X_{20}[15] = 1$	
		$\Delta X_{19}[18] = 0$		$\Delta X_{20}[19]$=0	1
		$\Delta X_{19}[19] = 0$	$K_{21}[22]$	$\Delta X_{20}[3]$=0	2
			$K_{21}[22]K_{20}[20]$	$\Delta X_{20}[3]$=1	
		$\Delta X_{19}[20] = 1$		$\Delta X_{20}[4]$=0	1
			$K_{20}[21]$	$\Delta X_{20}[4]$=1	
20	14	$\Delta X_{20}[0] = 0$		$\Delta X_{21}[1]$=0 and $\Delta X_{21}[8] = 0$	2
			$K_{21}[1]$	$\Delta X_{21}[1]$=0 and $\Delta X_{21}[8] = 1$	
			$K_{21}[8]$	$\Delta X_{21}[1]$=1 and $\Delta X_{21}[8] = 0$	
			$K_{21}[1] \oplus K_{21}[8]$	$\Delta X_{21}[1]$=1 and $\Delta X_{21}[8] = 1$	
		$\Delta X_{20}[1] = 0$		$\Delta X_{21}[2]$=0 and $\Delta X_{21}[9] = 0$	2
			$K_{21}[2]$	$\Delta X_{21}[2]$=0 and $\Delta X_{21}[9] = 1$	
			$K_{21}[9]$	$\Delta X_{21}[2]$=0 and $\Delta X_{21}[9] = 0$	
			$K_{21}[2] \oplus K_{21}[9]$	$\Delta X_{21}[2]$=1 and $\Delta X_{21}[9] = 1$	
		$\Delta X_{20}[2] = 0$		$\Delta X_{21}[3]$=0 and $\Delta X_{21}[10] = 0$	2
			$K_{21}[3]$	$\Delta X_{21}[3]$=0 and $\Delta X_{21}[10] = 1$	
			$K_{21}[10]$	$\Delta X_{21}[3]$=0 and $\Delta X_{21}[10] = 0$	
			$K_{21}[3] \oplus K_{21}[10]$	$\Delta X_{21}[3]$=0 and $\Delta X_{21}[10] = 1$	
		$\Delta X_{20}[5] = 0$		$\Delta X_{21}[6]$=0 and $\Delta X_{21}[13] = 0$	2
			$K_{21}[6]$	$\Delta X_{21}[6]$=0 and $\Delta X_{21}[13] = 1$	
			$K_{21}[13]$	$\Delta X_{21}[6]$=1 and $\Delta X_{21}[13] = 0$	
			$K_{21}[6] \oplus K_{21}[13]$	$\Delta X_{21}[6]$=1 and $\Delta X_{21}[13] = 1$	
		$\Delta X_{20}[6] = 0$		$\Delta X_{21}[7]$=0 and $\Delta X_{21}[14] = 0$	2
			$K_{21}[7]$	$\Delta X_{21}[7]$=0 and $\Delta X_{21}[14] = 1$	
			$K_{21}[14]$	$\Delta X_{21}[7]$=1 and $\Delta X_{21}[14] = 0$	
			$K_{21}[7] \oplus K_{21}[14]$	$\Delta X_{21}[7]$=1 and $\Delta X_{21}[14] = 1$	
		$\Delta X_{20}[7] = 0$	$K_{21}[15]$		1
		$\Delta X_{20}[9] = 0$	$K_{21}[17]$		1
		$\Delta X_{20}[10] = 0$		$\Delta X_{21}[11]$=0 and $\Delta X_{21}[18] = 0$	2
			$K_{21}[11]$	$\Delta X_{21}[11]$=0 and $\Delta X_{21}[18] = 1$	
			$K_{21}[18]$	$\Delta X_{21}[11]$=1 and $\Delta X_{21}[18] = 0$	
			$K_{21}[11] \oplus K_{21}[18]$	$\Delta X_{21}[11]$=1 and $\Delta X_{21}[18] = 1$	
		$\Delta X_{20}[13] = 0$	$K_{21}[21]$		1
		$\Delta X_{20}[16] = 0$	$K_{21}[0]$		1
		$\Delta X_{20}[17] = 0$	$K_{21}[18]$,$K_{21}[1]$		1/2
		$\Delta X_{20}[18] = 0$	$K_{21}[19]$		1
		$\Delta X_{20}[22] = 0$	$K_{21}[23]$		1
		$\Delta X_{20}[23] = 0$	$K_{21}[0]$,$K_{21}[7]$		1/2

Table 10: Conditions of Differential Path of SIMON64 are Independent of Subkeys

Rounds	Number of Conditions	Difference Conditions of i-th Round
input	18	$\Delta X_0[1] = 0$, $\Delta X_0[6] = 0$, $\Delta X_0[8] = 0$, $\Delta X_0[11] = 1$, $\Delta X_0[12] = 0$, $\Delta X_0[18] = 0$, $\Delta X_0[33] = 0$, $\Delta X_0[37] = 0$, $\Delta X_0[39] = 0$, $\Delta X_0[40] = 0$, $\Delta X_0[41] = 0$, $\Delta X_0[42] = 1$, $\Delta X_0[44] = 0$, $\Delta X_0[45] = 0$, $\Delta X_0[46] = 0$, $\Delta X_0[48] = 0$, $\Delta X_0[51] = 0$, $\Delta X_0[52] = 1$, $\Delta X_0[58] = 0$
1	17	$\Delta X_1[34] = 0$ $\Delta X_1[35] = 0$, $\Delta X_1[39] = 1$, $\Delta X_1[41] = 0$, $\Delta X_1[42] = 0$, $\Delta X_1[45] = 0$, $\Delta X_1[46] = 0$, $\Delta X_1[47] = 0$, $\Delta X_1[48] = 0$, $\Delta X_1[49] = 0$, $\Delta X_1[52] = 0$, $\Delta X_1[53] = 0$, $\Delta X_1[54] = 0$, $\Delta X_1[56] = 0$, $\Delta X_1[59] = 0$, $\Delta X_1[60] = 0$, $\Delta X_1[63] = 1$

2	2	$\Delta X_2[55] = 0$, $\Delta X_2[55] = \Delta X_1[57] + \Delta X_0[55]$, $\Delta X_2[62] = 0$, $\Delta X_2[62] = \Delta X_1[32] + \Delta X_0[62]$
3	2	$\Delta X_3[32] = 0$, $\Delta X_3[32] = \Delta X_1[36] + \Delta X_1[32] + \Delta X_0[34]$, $\Delta X_3[57] = 0$, $\Delta X_3[57] = \Delta X_1[61] + \Delta X_1[57] + \Delta X_0[59]$
26	2	$\Delta X_{26}[0] = 0$, $\Delta X_{26}[0] = \Delta X_{27}[2] + \Delta X_{28}[0]]$, $\Delta X_{26}[25] = 0$, $\Delta X_{26}[25] = \Delta X_{27}[27] + \Delta X_{28}[25]$
27	15	$\Delta X_{27}[1] = 0$, $\Delta X_{27}[3] = 0$, $\Delta X_{27}[4] = 0$, $\Delta X_{27}[11] = 0$, $\Delta X_{27}[15] = 0$, $\Delta X_{27}[17] = 0$, $\Delta X_{27}[18] = 0$, $\Delta X_{27}[21] = 0$, $\Delta X_{27}[22] = 0$, $\Delta X_{27}[23] = 0$, $\Delta X_{27}[24] = 0$, $\Delta X_{27}[25] = 0$, $\Delta X_{27}[28] = 0$, $\Delta X_{27}[29] = 0$, $\Delta X_{27}[30] = 0$
28	35	$\Delta X_{28}[2] = 0$, $\Delta X_{28}[3] = 0$, $\Delta X_{28}[6] = 0$, $\Delta X_{28}[7] = 1$, $\Delta X_{28}[8] = 0$, $\Delta X_{28}[9] = 0$, $\Delta X_{28}[10] = 0$, $\Delta X_{28}[11] = 0$, $\Delta X_{28}[12] = 0$, $\Delta X_{28}[13] = 0$, $\Delta X_{28}[14] = 0$, $\Delta X_{28}[15] = 0$, $\Delta X_{28}[16] = 0$, $\Delta X_{28}[17] = 0$, $\Delta X_{28}[18] = 0$, $\Delta X_{28}[20] = 0$, $\Delta X_{28}[21] = 0$, $\Delta X_{28}[22] = 0$, $\Delta X_{28}[24] = 0$, $\Delta X_{28}[27] = 0$, $\Delta X_{28}[28] = 0$, $\Delta X_{28}[31] = 0$, $\Delta X_{28}[33] = 0$, $\Delta X_{28}[37] = 0$, $\Delta X_{28}[39] = 0$, $\Delta X_{28}[40] = 0$, $\Delta X_{28}[41] = 0$, $\Delta X_{28}[42] = 0$, $\Delta X_{28}[44] = 0$, $\Delta X_{28}[45] = 0$, $\Delta X_{28}[46] = 0$, $\Delta X_{28}[48] = 0$, $\Delta X_{28}[51] = 0$, $\Delta X_{28}[52] = 0$, $\Delta X_{28}[58] = 0$

Table 11: Conditions of Differential Path of 28-round SIMON64 Relating to the Secret Key

Rounds	Number of Conditions	Difference Conditions of i-th Round	Possible Guessed Subkeys	Conditions for Key Guess	Number of Key Values
2	7	$\Delta X_2[32] = 0$		$\Delta X_1[33] = 0$	1
			$K_0[8]$	$\Delta X_1[33] = 1$	
		$\Delta X_2[35] = 0$		$\Delta X_1[36] = 0$	1
			$K_0[11]$	$\Delta X_1[36] = 1$	
		$\Delta X_2[36] = 0$		$\Delta X_1[37] = 0$	1
			$K_0[12]$	$\Delta X_1[37] = 1$	
		$\Delta X_2[43] = 0$		$\Delta X_1[37] = 1$	1/2
			$K_0[12]$	$\Delta X_1[37] = 0$	
		$\Delta X_2[47] = 0$		$\Delta X_1[55] = 0$	1
			$K_0[16]$	$\Delta X_1[55] = 1$	
		$\Delta X_2[49] = 0$		$\Delta X_1[57] = 0$	1
			$K_0[18]$	$\Delta X_1[57] = 1$	
		$\Delta X_2[53] = 0$		$\Delta X_1[61] = 0$	1
			$K_0[22]$	$\Delta X_1[61] = 1$	
		$\Delta X_2[50] = 0$		$\Delta X_1[51] = 0$ and $\Delta X_1[58] = 0$	2
			$K_0[19]$	$\Delta X_1[51] = 0$ and $\Delta X_1[58] = 1$	
			$K_0[26]$	$\Delta X_1[51] = 1$ and $\Delta X_1[58] = 0$	
			$K_0[19] \oplus K_0[26]$	$\Delta X_1[51] = 1$ and $\Delta X_1[58] = 1$	
		$\Delta X_2[54] = 0$		$\Delta X_1[55] = 0$ and $\Delta X_1[62] = 0$	2
			$K_0[23]$	$\Delta X_1[55] = 0$ and $\Delta X_1[62] = 1$	
			$K_0[30]$	$\Delta X_1[55] = 1$ and $\Delta X_1[62] = 0$	
			$K_0[23] \oplus K_0[30]$	$\Delta X_1[55] = 1$ and $\Delta X_1[62] = 1$	
		$\Delta X_2[56] = 0$		$\Delta X_1[57] = 0$ and $\Delta X_1[32] = 0$	2
			$K_0[25]$	$\Delta X_1[57] = 0$ and $\Delta X_1[32] = 1$	
			$K_0[0]$	$\Delta X_1[57] = 1$ and $\Delta X_1[32] = 0$	
			$K_0[25] \oplus K_0[0]$	$\Delta X_1[57] = 1$ and $\Delta X_1[32] = 1$	
		$\Delta X_2[57] = 0$		$\Delta X_1[58] = 0$	1
			$K_0[1]$	$\Delta X_1[58] = 1$	
		$\Delta X_2[61] = 0$		$\Delta X_1[62] = 0$	1
			$K_0[5]$	$\Delta X_1[62] = 1$	
		$\Delta X_2[60] = 0$		$\Delta X_1[61] = 0$ and $\Delta X_1[36] = 0$	2
			$K_0[29]$	$\Delta X_1[61] = 0$ and $\Delta X_1[36] = 1$	
			$K_0[4]$	$\Delta X_1[61] = 1$ and $\Delta X_1[36] = 0$	
			$K_0[29] \oplus K_0[4]$	$\Delta X_1[61] = 1$ and $\Delta X_1[36] = 1$	
3	8	$\Delta X_3[33] = 0$		$\Delta X_2[34] = 0$	4

			$K_0[10], K_1[9]$	$\Delta X_2[34] = 1$ and $X_1[42] = 0$	
			$K_0[10],\ K_1[9] \oplus K_0[17]$	$\Delta X_2[34] = 1$ and $X_1[42] = 1$	
		$\Delta X_3[36] = 0$	$K_0[13],\ K_1[12]$	$X_1[45] = 0$	4
			$K_0[13],\ K_1[12] \oplus K_0[20]$	$X_1[45] = 1$	
		$\Delta X_3[37] = 0$	$K_0[14]$	$\Delta X_2[38] = 0$	
			$K_0[14],\ K_0[15] \oplus K_1[13]$	$\Delta X_2[38] = 1$ and $\Delta X_1[46] = 0$	4
			$K_0[14],\ K_0[15] \oplus K_1[13] \oplus K_0[21]$	$\Delta X_2[38] = 1$ and $\Delta X_1[46] = 1$	
		$\Delta X_3[51] = 0$		$\Delta X_2[59] = 0$	
			$K_1[20]$	$\Delta X_2[59] = 1$ and $X_1[53] = 0$	4
			$K_1[20] \oplus K_0[28]$	$\Delta X_2[59] = 1$ and $X_1[53] = 1$	
		$\Delta X_3[55] = 0$	$K_0[7]$	$\Delta X_2[63] = 0$	2
			$K_0[7], K_1[24]$	$\Delta X_2[63] = 1$	
		$\Delta X_3[58] = 0$	$K_0[3]$	$\Delta X_2[59] = 0$ and $\Delta X_2[34] = 0$	
			$K_0[3], K_1[27]$	$\Delta X_2[59] = 0$ and $\Delta X_2[34] = 1$	4
			$K_0[3], K_1[2]$	$\Delta X_2[59] = 1$ and $\Delta X_2[34] = 0$	
			$K_0[3], K_1[2] \oplus K_1[27]$	$\Delta X_2[59] = 1$ and $\Delta X_2[34] = 1$	
		$\Delta X_3[61] = 0$	$K_0[6], K_1[30]$	$X_1[38] = 0$	2
			$K_0[6], K_1[30] \oplus K_1[31]$	$X_1[38] = 1$	
		$\Delta X_3[62] = 0$		$\Delta X_2[63] = 0$ and $\Delta X_2[38] = 0$	
			$K_1[31]$	$\Delta X_2[63] = 0$ and $\Delta X_2[38] = 1$	2
			$K_1[6]$	$\Delta X_2[63] = 1$ and $\Delta X_2[38] = 0$	
			$K_1[31] \oplus K_1[6]$	$\Delta X_2[63] = 0$ and $\Delta X_2[38] = 1$	
4	4	$\Delta X_4[34] = 0$	$K_1[11], K_1[12] \oplus K_2[10]$	$X_2[43] = 0$	2
			$K_1[11], K_1[12] \oplus K_2[10] \oplus K_1[18]$	$X_2[43] = 1$	
		$\Delta X_4[38] = 0$	$K_1[15], K_1[16] \oplus K_2[14]$	$X_2[47] = 0$	2
			$K_1[15], K_1[16] \oplus K_2[14] \oplus K_1[22] \oplus K_0[24]$	$X_2[47] = 1$	
		$\Delta X_4[59] = 0$	$K_1[29], K_2[28]$	$X_2[61] = 0$	2
			$K_1[29], K_1[4] \oplus K_2[28]$	$X_2[61] = 1$	
		$\Delta X_4[63] = 0$	$K_0[2],\ K_0[9], K_1[8], K_2[0]$	$X_2[40] = 0$	16
			$K_0[2], K_0[9], K_1[8], K_1[1] \oplus K_2[0]$	$X_2[40] = 1$	
25	4	$\Delta X_{25}[2] = 0$	$K_{27}[11], K_{26}[10]$	$X_{27}[11] = 0$	4
			$K_{27}[11], K_{26}[10] \oplus K_{27}[18]$	$X_{27}[11] = 1$	
		$\Delta X_{25}[6] = 0$	$K_{27}[15], K_{27}[16] \oplus K_{26}[14]$	$X_{27}[15] = 0$	4
			$K_{27}[15], K_{27}[16] \oplus K_{26}[14] \oplus K_{27}[22]$	$X_{27}[15] = 1$	
		$\Delta X_{25}[27] = 0$	$K_{27}[29], K_{26}[28]$	$X_{27}[29] = 0$	4
			$K_{27}[29], K_{27}[4] \oplus K_{26}[28]$	$X_{27}[29] = 1$	
		$\Delta X_{25}[31] = 0$	$K_{27}[1], K_{26}[0]$	$X_{27}[1] = 0$	4
			$K_{27}[1], K_{27}[8] \oplus K_{26}[0]$	$X_{27}[1] = 1$	
26	8	$\Delta X_{26}[4] = 0$	$K_{27}[12]$		1
		$\Delta X_{26}[29] = 0$	$K_{27}[30]$		1
		$\Delta X_{26}[1] = 0$		$\Delta X_{27}[2] = 0$	1
			$K_{27}[9]$	$\Delta X_{27}[2] = 1$	
		$\Delta X_{26}[5] = 0$		$\Delta X_{27}[6] = 0$	1
			$K_{27}[13]$	$\Delta X_{27}[6] = 1$	
		$\Delta X_{26}[19] = 0$		$\Delta X_{27}[27] = 0$	1
			$K_{27}[20]$	$\Delta X_{27}[27] = 1$	
		$\Delta X_{26}[23] = 0$		$\Delta X_{27}[31] = 0$	1
			$K_{27}[24]$	$\Delta X_{27}[31] = 1$	
		$\Delta X_{26}[26] = 0$		$\Delta X_{27}[27] = 0$ and $\Delta X_{27}[2] = 0$	
			$K_{27}[27]$	$\Delta X_{27}[27] = 0$ and $\Delta X_{27}[2] = 1$	2
			$K_{27}[2]$	$\Delta X_{27}[27] = 1$ and $\Delta X_{27}[2] = 0$	
			$K_{27}[27] \oplus K_{27}[2]$	$\Delta X_{27}[27] = 1$ and $\Delta X_{27}[2] = 1$	
		$\Delta X_{26}[30] = 0$		$\Delta X_{27}[31] = 0$ and $\Delta X_{27}[6] = 0$	
			$K_{27}[31]$	$\Delta X_{27}[31] = 0$ and $\Delta X_{27}[6] = 1$	2
			$K_{27}[6]$	$\Delta X_{27}[31] = 1$ and $\Delta X_{27}[6] = 0$	
			$K_{27}[31] \oplus K_{27}[6]$	$\Delta X_{27}[31] = 1$ and $\Delta X_{27}[6] = 1$	