Differential Attacks on Reduced SIMON Versions with Dynamic Key-guessing Techniques

No Author Given

No Institute Given

Abstract. SIMON is a family of lightweight block ciphers which are designed by the U.S National Security Agency in 2013. It has totally 10 versions corresponding to different block size $2n$ and key length l_k, named as SIMON$2n/l_k$. In this paper, we present a new differential attack by considering the sufficient bit conditions of the previous differential paths. Based on the bit conditions, we successfully propose a new type of dynamic key-guessing technique which greatly reduces the key space guessed. Our attacks work on the reduced SIMON of all 10 suggested versions, which improve the best previous results by 2 to 4 rounds. For verification, we implemented a practical attack on 19-round SIMON32 in a PC, and the experimental data confirm the correctness of the attack, which also fit the theoretical complexity and success rate very well. It is remarked that, our cryptanalysis only provides a more accurate security evaluation, and it does not mean the security problem of the whole SIMON family.

Keywords: SIMON, lightweight block cipher, bit condition, differential attack, dynamic key-guessing

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[7], LED[11], PRINCE[8], KANTAN[9] and CLEFIA[19] etc.

In 2013, NSA published the specifications of two lightweight block cipher families SIMON and SPECK[3] which can perform well both in hardware and software. Especially, compared with the other lightweight block cipher primitives, SIMON and SPECK perform competitively in hardware and software platforms respectively.

In this paper, we only focus on the differential attacks on reduced versions of SIMON family. Differential attack [5] was firstly introduced by Biham and Shamir which becomes a powerful tool in cryptanalysis of block ciphers today. Differential cryptanalysis aims to analyze how particular XOR differences in plaintext pairs affect the XOR differences of the resultant ciphertext pairs. In the past 25 years, it has been developed into many variants used to analyze various block cipher primitives[16,15,14,4,23]. Another type of differential attack is modular differential attack which is based on modular differences

instead of XOR differences, and it is widely used to attack or evaluate hash functions[24,22,10,21,18,17]. The core of modular differential attack can be regarded as three steps: Firstly the adversary cancels the unwanted avalanche arisen from a given input difference by various complex bit-carry control techniques and finds a specifical optimized differential path. Then he determines a set of sufficient bit conditions to obtain the specific differential path. Finally the adversary fulfills various techniques including message modifications to guarantee more bit conditions hold, and this improves the success rate of the attack. The basic idea of our attack is to merge two types of differential attacks. Specifically, we get the sufficient bit conditions using similar techniques as that of the modular differential attack, and then apply some new techniques especially dynamic key-guessing technique to ensure more bit conditions are satisfied. In addition, cryptanalysis based on bit conditions are also used in condition differential cryptanalysis which was introduced by Knellwolf et al. in [13] to analyze the stream cipher.

Related Works Since the SIMON family was announced, it has attracted a lot of attention of the cryptographers. Before previewing the previous works on SIMON family, we briefly give some explanations about the versions of SIMON. SIMON2n/l_k denotes a SIMON version with block size $2n$ and key length l_k. SIMON2n stands for the SIMON versions with block size $2n$. For example, SIMON48 has two versions SIMON48/72 and SIMON48/96 corresponding to key length 72 and 96 respectively. Alkhzaimi and Lauridsen[2] presented the first security analysis of all the versions. They gave differential attacks on 16-round SIMON32, 18-round SIMON48, 24-round SIMON64, 29-round SIMON96 and 40-round SIMON128, as well as impossible differential attacks on 14, 15, 16, 19, and 22 rounds of the corresponding versions of SIMON. At FSE 2014, Biryukov and Velichkov [6] found new differentials up to 13, 15 and 21 rounds for SIMON32, SIMON48, SIMON64 respectively. As a result, 19-round SIMON32/64, 20-round SIMON48/72, 20-round SIMON48/96, 26-round SIMON64/96 and 26-round SIMON64/128 were attacked with about 2^{34}, 2^{52}, 2^{75}, 2^{89} and 2^{121} encryptions, respectively. In addition, at the same workshop, Abed and List [1] independently used another differential to attack 18, 19, 26, 35 and 46 rounds of SIMON versions of 5 different block sizes, respectively.

Our Contributions In this paper, we use the existing differentials in [6,20,1] to analyze the reduced SIMON versions. The sketch of our attack is as follows.

Firstly, we extend several rounds on the top and the bottom of the previous differentials, and get the target differential path to attack. We obtain the sufficient bit conditions of the extended differential paths by investigating bitwise behavior of differences in the paths. All the bit conditions can be categorized into two types. The first type only depends on plaintexts or ciphertexts, which can be handled by choosing plaintexs, ciphertexts and building the data structures. The other type of conditions is related to the secret key.

Secondly, we observe that, there exists some information redundancy in the second type of conditions (equations) which comes from the single non-linearity in the round function of SIMON. Based on the observation, we can avoid guess-

Table 1. Summary of Differential Attacks on SIMONs

Cipher	Key Size	Total Rounds	Attacked Rounds	Time	Data	Reference
SIMON32	64	32	18	2^{46}	$2^{31.2}$	[1]
			19	2^{34}	2^{31}	[6]
			21	$2^{55.25}$	2^{31}	Section 3
SIMON48	72	36	19	2^{52}	2^{46}	[1]
			20	2^{52}	2^{46}	[6]
			23	$2^{63.25}$	2^{47}	Section 4.1
	96	36	19	2^{76}	2^{46}	[1]
			20	2^{75}	2^{46}	[6]
			24	$2^{87.25}$	2^{47}	Section 4.2
SIMON64	96	42	26	2^{94}	2^{63}	[1]
			26	2^{89}	2^{63}	[6]
			28	$2^{84.25}$	2^{63}	Section 4.2
	128	44	26	2^{126}	2^{63}	[1]
			26	2^{121}	2^{63}	[6]
			29	$2^{116.25}$	2^{63}	Section 4.2
SIMON96	96	52	35	$2^{93.3}$	$2^{93.2}$	[1]
			37	2^{95}	2^{95}	Section 4.2
	144	54	35	$2^{101.1}$	$2^{93.2}$	[1]
			37	$2^{132.25}$	2^{95}	Section 4.2
SIMON128	128	68	46	$2^{125.7}$	$2^{125.6}$	[1]
			49	2^{127}	2^{127}	Section 4.2
	192	69	46	$2^{142.0}$	$2^{125.6}$	[1]
			49	$2^{183.25}$	2^{127}	Section 4.2
	256	72	46	$2^{206.0}$	$2^{125.6}$	[1]
			50	$2^{247.25}$	2^{127}	Section 4.2

ing some subkey bits (or equivalent key bits) involved in these conditions, which depend on the specific bits or the bit differences of intermediate variables. Consequently, we propose a dynamic key-guessing technique which reduces the number of secret key bits guessed greatly. For example, in the attack on 21-round SIMON32, we find $2^{23.9}$ solutions of 49-bit subkey for a filtered palintext pair. It implies that, for the collected pair, we need to guess $2^{23.9}$ subkey space instead of 2^{49} in the conventional differential attack.

As a result, our attacks work on these reduced versions with 2 to 4 rounds more than the previous attacks. The time complexities of our attacks on the 21-round SIMON32/64, 23-round SIMON48/72, 24-round SIMON48/96, 28-round SIMON64/96, 29-round SIMON64/128, 37-round SIMON96/96, 37-round SIMON96/144, 49-round SIMON128/128, 49-round SIMON128/192 and 50-round SIMON128/256 are $2^{55.25}$, $2^{63.25}$, $2^{87.25}$, $2^{84.25}$, $2^{116.25}$, 2^{95}, $2^{132.25}$, 2^{127}, $2^{183.25}$ and $2^{247.25}$ encryptions, respectively. Our results are summarized in Table 1.

The rest of this paper is organized as follows. In Section 2, we list some notations, and give a brief description of the block cipher SIMON family and some observations. Section 3 describes the details of our differential attacks on

21-round SIMON32, and implements a practical attack expriment on 19-round SIMON32 in a PC. The attacks on the other versions of SIMON are given in Section 4. Finally, we conclude this paper in Section 5.

2 Brief Description of SIMON

2.1 Notations

The following notations are used in this paper:

X^{r-1}	the input of the 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-1}	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 X by r bits
$X \ggg r$	the right rotation of X by r bits
$\oplus$	bitwise exclusive OR (XOR)
$\cap$	bitwise AND
ΔX	the XOR difference of X and X'
$+$	addition operation
$\%$	modular operation

2.2 Brief Description of Block Cipher SIMON

The SIMON block cipher is a Feistel structure with a $2n$-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. All versions of SIMON use similar round function.

Round Functions For high performance on both hardware and software platforms, SIMON utilizes an extremely simple round function which iterates many rounds. The function $F(x) = ((x \lll 1) \cap (x \lll 8)) \oplus (x \lll 2)$ is a 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 $P = (L^0, R^0)$, 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 $i = 1, ..., n_r$. (R^{n_r}, L^{n_r}) is the ciphertext C.

To describe our differential attack with bit conditions conveniently, we give a bitwise description of the round function. 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 $K^i = \{K^i_0, K^i_1, \ldots, K^i_{n-1}\}$, 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_n^i is the left-most bit of L^i, X_{2n-1}^i is the right-most bit of L^i, X_0^i is the left-most bit of R^i, and X_{n-1}^i is the right-most bit of R^i.

Key Schedules The key schedules generate a sequence of n_r round subkeys $\{K^0, ..., K^{n_r-1}\}$ from the master key $\{k_0, k_1, ..., k_{m-1}\}$. For different key lengths mn, the key schedules are given as follows, when $i = 0, 1, \ldots, m-1$, $K^i = k_i$; and when $i = m, m+1, \ldots, n_r$,

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

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

2.3 Some Observations

Observation 1 ([12]) *Let $\Delta x = x \oplus x'$, $\Delta y = y \oplus y'$, 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 the i-th round, where $\Delta X^{i-1} = X^{i-1} \oplus (X^{i-1})'$. Then we can compute the output difference ΔX^i of the i-th round function without any key bit guessing , and obtain a subkey bit according to the following four cases(for $j = 0, 1, \ldots, n-1$).*

1. *When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (0, 0)$, there is no key bit involved in ΔX^{i+1}_{j+n}.*
2. *When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (0, 1)$, $K^{i-1}_{(j+1)\%n}$ is computed from the value of ΔX^{i+1}_{j+n}.*
3. *When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (1, 0)$, $K^{i-1}_{(j+8)\%n}$ is computed from the value of ΔX^{i+1}_{j+n}.*
4. *When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (1, 1)$, one equivalent key bit $K^{i-1}_{(j+1)\%n} \oplus K^{i-1}_{(j+8)\%n}$ is computed from $\Delta X^{i+1}_{j+n} (j < n)$.*

Since the subkey K^{i-1} is linear with the output of X^i, it is obvious that ΔX^i is independent with K^{i-1}.

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

$$\begin{aligned}
\Delta X^{i+1}_{j+n} = &(\Delta X^i_{(j+1)\%n+n} \cap X^i_{(j+8)\%n+n}) \oplus (X^i_{(j+1)\%n+n} \cap \Delta X^i_{(j+8)\%n+n})\\
&\oplus (\Delta X^i_{(j+1)\%n+n} \cap \Delta X^i_{(j+8)\%n+n}) \oplus \Delta X^i_{(j+2)\%n+n} \oplus \Delta X^i j,
\end{aligned} \tag{1}$$

$$X^i_{(j+1)\%n+n} = (X^{i-1}_{(j+2)\%n+n} \cap X^{i-1}_{(j+9)\%n+n}) \oplus X^{i-1}_{(j+3)\%n+n} \oplus X^{i-1}_{(j+1)\%n} \oplus K^{i-1}_{(j+1)\%n}, \quad (2)$$

$$X^i_{(j+8)\%n+n} = (X^{i-1}_{(j+9)\%n+n} \cap X^{i-1}_{(j+16)\%n+n}) \oplus X^{i-1}_{(j+10)\%n+n} \oplus X^{i-1}_{(j+8)\%n} \oplus K^{i-1}(j+8)\%n. \quad (3)$$

It is obvious that Observation 2 is obtained from equations (1)-(3). In other word, given a equation $\Delta X^{i+1}_{j+n} = b$, where $b = 0$ or 1, Observation 2 implies that,

1. When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (0,0)$ and $\Delta X^i_{(j+2)\%n+n} \oplus \Delta X^i_j = b \oplus 1$, there is no solution of the subkey $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$.
2. When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (0,0)$ and $\Delta X^i_{(j+2)\%n+n} \oplus \Delta X^i_j = b$, there are 4 solutions of $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$.
3. When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (0,1)$, there are two solutions of $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$.
4. When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (1,0)$, there are two solutions of $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$.
5. When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (1,1)$, there are two solutions of $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$.

From Observation 2, we know that, the equation $\Delta X^{i+1}_{j+n} = b$ has all the 4 solutions only with probability $\frac{1}{8}$. It has 2 solutions with probability $\frac{3}{4}$ and no solution with probability $\frac{1}{8}$. This is an example of the dynamic key bit guessing. In our attacks, we can explore more strategies of the dynamic key bit guessing according to different bit conditions. It is obvious that, we can greatly reduce the key space to be guessed by solving enough bit equations.

3 Differential Attack on SIMON32

In this section, we describe the details of differential attack on round-reduced SIMON32/64. We utilize the recent 13-round differential in [6] to attack 21-round SIMON32 by adding 4 rounds on the top and 4 rounds at the bottom. We first find a set of sufficient bit-difference conditions to make 21-round differential path hold, then deduce the equations related to subkey bits for a chosen plaintext-ciphertext pair, and finally calculate the subkey solutions to the equations. Based on the number of subkeys counted, we can distinguish the right subkey fast. Here, we also implement a attack expriment on 19-round SIMON32 in a PC in order to verify the correctness of our attack. For simplicity, we replace $C = \{R^{n_r}, L^{n_r}\}$ by $C = \{L^{n_r}, R^{n_r}\}$ in the rest of this paper.

3.1 Sufficient Conditions for Differential Path of 21-round SIMON32

For this attack, we consider the following 13-round differential with probability $2^{-28.56}$,

$$D_1 : (0000, 0040) \rightarrow (4000, 0000).$$

After prefixing 4 rounds on the top and appending 4 rounds at the bottom, we extend the 13-round differential path to 21 rounds. It is easy to obtain a set of sufficient bit conditions thar lead to the input and output differences of the 13-round differential D_1 (see Table 2). We select a plaintext pair to make the input difference in the first row of Table 2 and the output difference in the last row hold. It is easy to verify that 16 conditions in bold from round 1 and round 20 are independent of subkey bits, 28 conditions in bold from rounds 2-4 and 17-19 are related to subkey bits. If all the 44 conditions (16+28) hold, the other conditions in the extended path hold with probability 1. So these 44 conditions are sufficient to lead to the input and output differences of the 13-round differential D_1, and we call them a set of sufficient conditions of the differential path.

Table 2: Sufficient Conditions of Extended Differential Path of 21-round SIMON32

Rounds	Input Differences of Each Round
0	0, *, 0, 1, *, *, *, *, *, 0, 0, 0, 0, *, *, *, *, 1, *, *, *, *, *, *, *, 0, *, 0, *, *, *, *, *
1	*, 0, **0**, **0**, **0**, **1**, *, *, 0, *, 0, **0**, **0**, **0**, **0**, *, 0, *, 0, 1, *, *, *, *, *, 0, 0, 0, 0, *, *, *
2	0, *, 0, 0, **0**, **0**, **0**, **1**, *, 0, 0, 0, 0, **0**, **0**, **0**, *, 0, 0, 0, 0, 1, *, *, 0, *, 0, 0, 0, 0, 0, *
3	**0**, 0, 0, 0, 0, 0, **0**, **0**, 0, **1**, 0, 0, 0, 0, 0, **0**, 0, *, 0, 0, 0, 0, 0, 1, *, 0, 0, 0, 0, 0, 0, 0
4	0, **0**, 0, 0, 0, 0, 0, 0, **0**, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0
4 $\rightarrow$ 17	13-round differential D_1
17	0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, **0**, 0, 0, 0, 0, 0, 0, 0, 0, **0**, 0, 0, 0, 0, 0, 0
18	*, 0, 0, 0, 0, 0, 0, 0, 0, *, 0, 0, 0, 0, 0, 1, 0, **1**, 0, 0, 0, 0, 0, **0**, **0**, 0, 0, 0, 0, 0, **0**, **0**
19	0, *, 0, 0, 0, 0, 0, *, *, 0, 0, 0, 0, 1, *, *, *, 0, 0, 0, 0, **0**, **0**, **0**, 0, *, 0, 0, **0**, **0**, **0**, **1**
20	*, 0, 0, 0, 0, *, *, *, 0, *, 0, 1, *, *, *, *, 0, *, 0, **0**, **0**, **0**, **0**, *, *, 0, **0**, **0**, **0**, **1**, *, *
21	0, *, 0, *, *, *, *, *, *, 1, *, *, *, *, *, *, *, *, **0**, **0**, **0**, **0**, *, *, *, **0**, *, **0**, **1**, *, *, *, *

We put the 16 conditions which are independent of the secret key in Table 3, and the 28 conditions related to the secret key in the 2rd column of Table 4 in Appendix. The clue of our attack is to build the structures in the data collection phase to get 16 conditions independent of the secret key, and get 28 equations on key bits from the other 28 conditions, then find the possible solutions of these equations to reduce the key space searched. Table 4 gives solutions of the key bits in the 3rd column, the 4th column is the conditions for the equation to have the solutions in 3rd column, and the P_r in the 5th column denotes the probability that the equations hold, and P_r^F means the probability that a wrong bit condition occurs which results in the dissatisfaction of the differential path(we call it a failure event).

Table 3: Conditions of Differential of 21-round SIMON32 that are Independent of Subkeys

Rounds i	Number of Conditions	Bit Conditions of the i-th Round

1	8	$\Delta X_1[18] = 0,\ \Delta X_1[19] = 0,\ \Delta X_1[20] = 0,\ \Delta X_1[21] = 1,$ $\Delta X_1[27] = 0,\ \Delta X_1[28] = 0,\ \Delta X_1[29] = 0,\ \Delta X_1[30] = 0$
20	8	$\Delta X_{20}[3] = 0,\ \Delta X_{20}[4] = 0,\ \Delta X_{20}[5] = 0,\ \Delta X_{20}[6] = 0,$ $\Delta X_{20}[10] = 0,\ \Delta X_{20}[11] = 0,\ \Delta X_{20}[12] = 0,\ \Delta X_{20}[13] = 1$

Table 4: Solutions of Subkey Bits Corresponding to Differential Path of 21-round SIMON32

Rounds	Bit Conditions	Solutions of Key Bits to Equations	Conditions Leading to Solutions	P_r	P_r^F
2(7)	$\Delta X^2_{20} = 0 \Leftrightarrow$ $X^1_{28} \oplus \Delta X^1_{22} \oplus \Delta X^0_{20} = 0$	K^0_{12}		1	
	$\Delta X^2_{29} = 0 \Leftrightarrow$ $X^1_{30} \oplus \Delta X^1_{31} \oplus \Delta X^0_{29} = 0$	K^0_{14}		1	
	$\Delta X^2_{30} = 0 \Leftrightarrow$ $\Delta(X^1_{31} \cap X^1_{22}) \oplus \Delta X^1_{16}$ $\oplus \Delta X^0_{30} = 0$	Discard the pair	$(\Delta X^1_{31},\ \Delta X^1_{22},\ \Delta X^1_{16} \oplus \Delta X^0_{30}) = (0,0,1)$		$\frac{1}{8}$
		$K^0_{15} = 0, 1,\ K^0_6 = 0, 1$	$(\Delta X^1_{31},\ \Delta X^1_{22},\ \Delta X^1_{16} \oplus \Delta X^0_{30}) = (0,0,0)$	$\frac{1}{8}$	
		$K^0_6 = 0, 1,\ K^0_{15}$	$(\Delta X^1_{31},\ \Delta X^1_{22}) = (0,1)$	$\frac{1}{4}$	
		$K^0_{15} = 0, 1,\ K^0_6$	$(\Delta X^1_{31},\ \Delta X^1_{22}) = (1,0)$	$\frac{1}{4}$	
		$K^0_{15} \oplus K^0_6$	$(\Delta X^1_{31},\ \Delta X^1_{22}) = (1,1)$	$\frac{1}{4}$	
	$\Delta X^2_{21} = 0 \Leftrightarrow$ $(\Delta X^1_{22} \cap X^1_{29}) \oplus \Delta X^1_{23}$ $\oplus \Delta X^0_{21} = 0$	Discard the pair	$(\Delta X^1_{22},\ \Delta X^1_{23} \oplus \Delta X^0_{21}) = (0,1)$		$\frac{1}{4}$
		$K^0_{13} = 0, 1$	$(\Delta X^1_{22},\ \Delta X^1_{23} \oplus \Delta X^0_{21}) = (0,0)$	$\frac{1}{4}$	
		K^0_{13}	$\Delta X^1_{22} = 1$	$\frac{1}{2}$	
	$\Delta X^2_{23} = 1 \Leftrightarrow$ $(\Delta X^1_{31} \cap X^1_{24}) \oplus \Delta X^1_{25}$ $\oplus \Delta X^0_{23} \oplus 1 = 0$	Discard the pair	$(\Delta X^1_{31},\ \Delta X^1_{25} \oplus \Delta X^0_{23} \oplus 1) = (0,1)$		$\frac{1}{4}$
		$K^0_8 = 0, 1$	$(\Delta X^1_{31},\ \Delta X^1_{25} \oplus \Delta X^0_{23} \oplus 1) = (0,0)$	$\frac{1}{4}$	
		K^0_8	$\Delta X^1_{31} = 1$	$\frac{1}{2}$	
	$\Delta X^2_{31} = 0 \Leftrightarrow$ $\Delta(X^1_{16} \cap X^1_{23}) \oplus \Delta X^0_{31} = 0$	Discard the pair	$(\Delta X^1_{16},\ \Delta X^1_{23},\ \Delta X^0_{31}) = (0,0,1)$		$\frac{1}{8}$
		$K^0_0 = 0, 1,\ K^0_7 = 0, 1$	$(\Delta X^1_{16},\ \Delta X^1_{23},\ \Delta X^0_{31}) = (0,0,0)$	$\frac{1}{8}$	
		$K^0_7 = 0, 1,\ K^0_0$	$(\Delta X^1_{16},\ \Delta X^1_{23}) = (0,1)$	$\frac{1}{4}$	
		$K^0_0 = 0, 1,\ K^0_7$	$(\Delta X^1_{16},\ \Delta X^1_{23}) = (1,0)$	$\frac{1}{4}$	
		$K^0_0 \oplus K^0_7$	$(\Delta X^1_{16},\ \Delta X^1_{23}) = (1,1)$	$\frac{1}{4}$	
	$\Delta X^2_{22} = 0 \Leftrightarrow$ $(\Delta X^1_{23} \cap X^1_{30}) \oplus \Delta X^0_{22} = 0$	Discard the pair	$(\Delta X^1_{23},\ \Delta X^0_{22}) = (0,1)$		$\frac{1}{4}$
		$K^0_{14} = 0, 1$	$(\Delta X^1_{23},\ \Delta X^0_{22}) = (0,0)$	$\frac{1}{4}$	
		K^0_{14}	$\Delta X^1_{23} = 1$	$\frac{1}{2}$	
3(5)	$\Delta X^3_{16} = 0 \Leftrightarrow$ $\Delta(X^2_{17} \cap X^2_{24}) \oplus \Delta X^1_{16} = 0$ (guess $K^0_9,\ K^0_2$)	No solution	$(\Delta X^2_{17},\ \Delta X^2_{24},\ \Delta X^1_{16}) = (0,0,1)$		$\frac{1}{8}$
		$K^1_1 \oplus K^0_3 = 0, 1,\ K^1_8 \oplus K^0_{10} = 0, 1$	$(\Delta X^2_{17},\ \Delta X^2_{24},\ \Delta X^1_{16}) = (0,0,0)$	$\frac{1}{8}$	
		$K^1_8 \oplus K^0_{10} = 0, 1,\ K^1_1 \oplus K^0_3$	$(\Delta X^2_{17},\ \Delta X^2_{24}) = (0,1)$	$\frac{1}{4}$	
		$K^1_1 \oplus K^0_3 = 0, 1,\ K^1_8 \oplus K^0_{10}$	$(\Delta X^2_{17},\ \Delta X^2_{24}) = (1,0)$	$\frac{1}{4}$	
		$K^1_1 \oplus K^0_3 \oplus K^1_8 \oplus K^0_{10}$	$(\Delta X^2_{17},\ \Delta X^2_{24}) = (1,1)$	$\frac{1}{4}$	
	$\Delta X^3_{22} = 0 \Leftrightarrow$ $X^2_{30} \oplus \Delta X^2_{24} \oplus \Delta X^1_{22} = 0$	K^1_{14}		1	
	$\Delta X^3_{23} = 0 \Leftrightarrow$ $(\Delta X^2_{24} \cap X^2_{31}) \oplus \Delta X^1_{23} = 0$	No solution	$(\Delta X^2_{24},\ \Delta X^1_{23}) = (0,1)$		$\frac{1}{4}$
		$K^1_{15} \oplus K^0_1 = 0, 1$	$(\Delta X^2_{24},\ \Delta X^1_{23}) = (0,0)$	$\frac{1}{4}$	
		$K^1_{15} \oplus K^0_1$	$\Delta X^2_{24} = 1$	$\frac{1}{2}$	
	$\Delta X^3_{25} = 1 \Leftrightarrow$ $(\Delta X^2_{17} \cap X^2_{26}) \oplus \Delta X^1_{25}$ $\oplus 1 = 0$ (guess K^0_{11})	No solution	$(\Delta X^2_{17},\ \Delta X^1_{25} \oplus 1) = (0,1)$		$\frac{1}{4}$
		$K^1_{10} = 0, 1$	$(\Delta X^2_{17},\ \Delta X^1_{25} \oplus 1) = (0,0)$	$\frac{1}{4}$	
		K^1_{10}	$\Delta X^2_{17} = 1$	$\frac{1}{2}$	
	$\Delta X^3_{31} = 0 \Leftrightarrow X^2_{16} \oplus \Delta X^2_{17} \oplus$ $\Delta X^1_{31} = 0$ (guess K^0_1)	K^1_0		1	
4(2)	$\Delta X^4_{17} = 0 \Leftrightarrow X^3_{18} \oplus \Delta X^2_{17} =$ 0 (guess $K^0_4,\ K^0_5,\ K^1_3$)	$K^2_2 \oplus K^1_4$		1	
	$\Delta X^4_{24} = 0 \Leftrightarrow X^3_{16} \oplus \Delta X^2_{24} =$ 0 (guess $K^0_3,\ K^0_{10}$)	$K^2_0 \oplus K^1_2$		1	
19(7)	$\Delta X^{19}_5 = 0 \Leftrightarrow$ $X^{20}_6 \oplus \Delta X^{20}_7 \oplus \Delta X^{21}_5 = 0$	K^{20}_6		1	
	$\Delta X^{19}_{12} = 0 \Leftrightarrow$ $X^{20}_4 \oplus \Delta X^{20}_{14} \oplus \Delta X^{21}_{12} = 0$	K^{20}_4		1	

	$\Delta X_6^{19}=0 \Leftrightarrow \Delta(X_7^{20} \cap X_{14}^{20}) \oplus \Delta X_8^{20} \oplus \Delta X_6^{21}=0$	Discard the pair	$(\Delta X_7^{20}, \Delta X_{14}^{20}, \Delta X_8^{20} \oplus \Delta X_6^{21})=(0,0,1)$		$\frac{1}{8}$
		$K_7^{20}=0,1,\ K_{14}^{20}=0,1$	$(\Delta X_7^{20}, \Delta X_{14}^{20}, \Delta X_8^{20} \oplus \Delta X_6^{21})=(0,0,0)$	$\frac{1}{8}$	
		$K_{14}^{20}=0,1,\ K_7^{20}$	$(\Delta X_7^{20}, \Delta X_{14}^{20})=(0,1)$	$\frac{1}{4}$	
		$K_7^{20}=0,1,\ K_{14}^{20}$	$(\Delta X_7^{20}, \Delta X_{14}^{20})=(1,0)$	$\frac{1}{4}$	
		$K_7^{20} \oplus K_{14}^{20}$	$(\Delta X_7^{20}, \Delta X_{14}^{20})=(1,1)$	$\frac{1}{4}$	
	$\Delta X_{15}^{19}=1 \Leftrightarrow (\Delta X_7^{20} \cap X_0^{20}) \oplus \Delta X_1^{20} \oplus \Delta X_{15}^{21} \oplus 1=0$	Discard the pair	$(\Delta X_7^{20}, \Delta X_1^{20} \oplus \Delta X_{15}^{21} \oplus 1)=(0,1)$		$\frac{1}{4}$
		$K_0^{20}=0,1$	$(\Delta X_7^{20}, \Delta X_1^{20} \oplus \Delta X_{15}^{21} \oplus 1)=(0,0)$	$\frac{1}{4}$	
		K_0^{20}	$\Delta X_7^{20}=1$	$\frac{1}{2}$	
	$\Delta X_{13}^{19}=0 \Leftrightarrow (\Delta X_{14}^{20} \cap X_5^{20}) \oplus \Delta X_{15}^{20} \oplus \Delta X_{13}^{21}=0$	Discard the pair	$(\Delta X_{14}^{20}, \Delta X_{15}^{20} \oplus \Delta X_{13}^{21})=(0,1)$		$\frac{1}{4}$
		$K_5^{20}=0,1$	$(\Delta X_{14}^{20}, \Delta X_{15}^{20} \oplus \Delta X_{13}^{21})=(0,0)$	$\frac{1}{4}$	
		K_5^{20}	$\Delta X_{14}^{20}=1$	$\frac{1}{2}$	
	$\Delta X_7^{19}=0 \Leftrightarrow \Delta(X_8^{20} \cap X_{15}^{20}) \oplus \Delta X_7^{21}=0$	Discard the pair	$(\Delta X_8^{20}, \Delta X_{15}^{20}, \Delta X_7^{21})=(0,0,1)$		$\frac{1}{8}$
		$K_8^{20}=0,1,\ K_{15}^{20}=0,1$	$(\Delta X_8^{20}, \Delta X_{15}^{20}, \Delta X_7^{21})=(0,0,0)$	$\frac{1}{8}$	
		$K_{15}^{20}=0,1,\ K_8^{20}$	$(\Delta X_8^{20}, \Delta X_{15}^{20})=(0,1)$	$\frac{1}{4}$	
		$K_8^{20}=0,1,\ K_{15}^{20}$	$(\Delta X_8^{20}, \Delta X_{15}^{20})=(1,0)$	$\frac{1}{4}$	
		$K_8^{20} \oplus K_{15}^{20}$	$(\Delta X_8^{20}, \Delta X_{15}^{20})=(1,1)$	$\frac{1}{4}$	
	$\Delta X_{14}^{19}=0 \Leftrightarrow (\Delta X_{15}^{20} \cap X_6^{20}) \oplus \Delta X_{14}^{21}=0$	Discard the pair	$(\Delta X_{15}^{20}, \Delta X_{14}^{21})=(0,1)$		$\frac{1}{4}$
		$K_6^{20}=0,1$	$(\Delta X_{15}^{20}, \Delta X_{14}^{21})=(0,0)$	$\frac{1}{4}$	
		K_6^{20}	$\Delta X_{15}^{20}=1$	$\frac{1}{2}$	
18(5)	$\Delta X_8^{18}=0 \Leftrightarrow \Delta(X_9^{19} \cap X_0^{19}) \oplus \Delta X_8^{20}=0]$ (guess K_1^{20}, K_{10}^{20})	No solution	$(\Delta X_9^{19}, \Delta X_0^{19}, \Delta X_8^{20})=(0,0,1)$		$\frac{1}{8}$
		$K_0^{19} \oplus K_2^{20}=0,1,\ K_9^{19} \oplus K_{11}^{20}=0,1$	$(\Delta X_9^{19}, \Delta X_0^{19}, \Delta X_8^{20})=(0,0,0)$	$\frac{1}{8}$	
		$K_0^{19} \oplus K_2^{20}=0,1,\ K_9^{19} \oplus K_{11}^{20}$	$(\Delta X_9^{19}, \Delta X_0^{19})=(0,1)$	$\frac{1}{4}$	
		$K_9^{19} \oplus K_{11}^{20}=0,1,\ K_0^{19} \oplus K_2^{20}$	$(\Delta X_9^{19}, \Delta X_0^{19})=(1,0)$	$\frac{1}{4}$	
		$K_9^{19} \oplus K_{11}^{20} \oplus K_0^{19} \oplus K_2^{20}$	$(\Delta X_9^{19}, \Delta X_0^{19})=(1,1)$	$\frac{1}{4}$	
	$\Delta X_7^{18}=0 \Leftrightarrow X_8^{19} \oplus \Delta X_9^{19} \oplus \Delta X_7^{20}=0$ (guess K_9^{20})	K_8^{19}		1	
	$\Delta X_1^{18}=1 \Leftrightarrow (\Delta X_9^{19} \cap X_2^{19}) \oplus \Delta X_1^{20} \oplus 1=0$ (guess K_3^{20})	No solution	$(\Delta X_9^{19}, \Delta X_1^{20} \oplus 1)=(0,1)$		$\frac{1}{4}$
		$K_2^{19}=0,1$	$(\Delta X_9^{19}, \Delta X_1^{20} \oplus 1)=(0,0)$	$\frac{1}{4}$	
		K_2^{19}	$\Delta X_9^{19}=1$	$\frac{1}{2}$	
	$\Delta X_{14}^{18}=0 \Leftrightarrow X_6^{19} \oplus \Delta X_0^{19} \oplus \Delta X_{14}^{20}=0$	K_6^{19}		1	
	$\Delta X_{15}^{18}=0 \Leftrightarrow (\Delta X_0^{19} \cap X_7^{19}) \oplus \Delta X_{15}^{20}=0$	No solution	$(\Delta X_0^{19}, \Delta X_{15}^{20})=(0,1)$		$\frac{1}{4}$
		$K_7^{19}=0,1$	$(\Delta X_0^{19}, \Delta X_{15}^{20})=(0,0)$	$\frac{1}{4}$	
		K_7^{19}	$\Delta X_0^{19}=1$	$\frac{1}{2}$	
17(2)	$\Delta X_9^{17}=0 \Leftrightarrow X_{10}^{18} \oplus \Delta X_9^{19}=0$ (guess K_{12}^{20}, K_{13}^{20}, K_{11}^{19})	$K_{10}^{18} \oplus K_{12}^{19}$		1	
	$\Delta X_0^{17}=0 \Leftrightarrow X_8^{18} \oplus \Delta X_0^{19}=0$ (guess K_2^{20}, K_{11}^{20})	$K_8^{18} \oplus K_{10}^{19}$		1	

In the 3rd column of Table 4, for example, K_{12}^0 means that there are 1 solution to the corresponding equation, $K_6^0=0,1$ means that 0 and 1 are all solutions to the corresponding equation.

3.2 Key-Recovey Attack on 21-round SIMON32

In this subsection, we describe a key recovery attack on 21-round SIMON32/64. Since there are 8 conditions in the input of the 2nd round, which are independent of the secret key, we make use of these conditions to construct structures, so as to reduce the time complexity of collecting plaintext-ciphertext pairs. In the process of key recovery attack, we use the above observations to reduce the guessed key space greatly.

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

1. There are 10 conditions on the plaintext differences, 8 conditions in the input of the 2nd round. We divide the plaintexts into 2^{18} structures with $2^{32-18} = 2^{14}$ plaintexts. By Observation 2, K_j^0 is independent of ΔX_j^1, which does not impact the structure. According to the round function definition and conditions on Table 3, we build the following 8 equations $X_j^1 = (X^0_{(j+1-n)\%n+n} \cap X^0_{(j+8)\%n+n}) \oplus X^0_{(j+2)\%n+n} \oplus X^0_{j-n}$, where $j = 18, 19, 20, 21, 27, 28, 29, 30$. Because there are 10 conditions on plaintexts, we fix 10 bits of $X_i^0 (i = 16, 18, 19, 25, 26, 27, 28, 1, 8, 10)$, and 8 bits of X_j^1 to be constants, and obtain each structure by solving the above equations system.
2. For structures A and A' with 3 different bits (X^0_{19}, X^0_1, X^1_{21}), we find the corresponding ciphertexts, and save them into a table indexed by $X_t^{21} (t = 1, 2, 3, 4, 8, 10, 16, 18)$ with $\Delta X_t^{21} = 0$. There are about $2^{14\times 2-8} = 2^{20}$ remaining pairs for each structure.
3. We build 2^{17} structures, and filter out the remaining pairs by decrypting one round according to the conditions in Table 2. Then there are $2^{17-1+20-10} = 2^{26}$ pairs left. Store the pairs in table T.

In data collection phase, we need about $2^{17+14} = 2^{31}$ encryptions for the chosen plaintexts, and about $2^{17+20} = 2^{37}$ one round computations to decide the conditions which is equivalent to 2^{33} encryptions. For the 2^{31} collected plaintexts, we get about $2^{17-1+28-14} = 2^{30}$ pairs satisfying the input difference of the 13-round differential D_1. Hence, there are about $2^{30-28.56} = 2.7$ right pairs occurred on average.

Filtering the Wrong Plaintext Pairs Because the conditions leading to necessary solutions in round 2 and 19 are independent of the secret key, for each pair in T, we first discard those wrong pairs which are not consistent with the conditions in rounds 2 and 19. For conditions ($\Delta X^2_{30} = 0$, $\Delta X^2_{21} = 0$, $\Delta X^2_{23} = 1$). we get the probability that all the three equations have solutions is $\frac{17}{32}$ from Table 4, In other words, the probability of no solution for the three equations is $P_r^F = \frac{15}{32}$ which is called failure event.

Applying similar method to conditions ($\Delta X^2_{31} = 0$, $\Delta X^2_{22} = 0$), ($\Delta X^{19}_6 = 0$, $\Delta X^{19}_{15} = 1$, $\Delta X^{19}_{13} = 0$), ($\Delta X^{19}_7 = 0$, $\Delta X^{19}_{14} = 1$), we get the probabilities that equations have solutions are $\frac{11}{16}$, $\frac{17}{32}$, $\frac{11}{16}$ respectively. There are $2^{26} \times (\frac{17}{32})^2 \times (\frac{11}{16})^2 \approx 2^{23.1}$ pairs remaining after discarding false pairs, which are stored in T_1 .

Computing Subkey Candidates By partial encryptions and decryptions, there are totally 50 bits of subkeys involved in the 28 conditions, of which 49 bits are independent according to key schedules(K_1^{20} can be deduced from the other 49-bit subkeys). Given a plaintext pair in T_1, we obtain 28 equations of 49-bit independent subkeys by partially encrypting the first 4 rounds, and decrypting the last 4 rounds. According to the specific bit-differences in the corresponding 21-round differential path, we compute all the solutions to the 28 equations, and every solution is a possible candidate for 49-bit subkeys. We collect all the solutions of corresponding $2^{23.1}$ pairs, and the right subkey will occur with an obvious probability advantage. It is mentioned that, the key-guessing technique

is dynamic. For the different pairs which result in the same differential path, we deduce the solutions of different subkeys. The subkeys solved are determined by specific differences in the differential path. To detect the correct key, we maintain lots of counters of size 2^{49}, initialized with 0. Given a plaintext pair in T_1, the computation details of 28 equations of 49-bit subkeys are as follows.

1. Choose a new pair in T_1
2. There are 7 equations obtained by partially encrypting round 2 (see Table 4).
   - For conditions ($\Delta X^2_{30} = 0$, $\Delta X^2_{21} = 0$, $\Delta X^2_{23} = 1$), we partially encrypt round 2, and deduce that

$$\Delta(X^1_{31} \cap X^1_{22}) \oplus \Delta X^1_{16} \oplus \Delta X^0_{30} = 0, \quad (4)$$
$$(\Delta X^1_{22} \cap X^1_{29}) \oplus \Delta X^1_{23} \oplus \Delta X^0_{21} = 0, \quad (5)$$
$$(\Delta X^1_{31} \cap X^1_{24}) \oplus \Delta X^1_{25} \oplus \Delta X^0_{23} \oplus 1 = 0. \quad (6)$$

     Because the pairs which are inconsistent with conditions in round 2 and round 19 have been discarded corresponding to the specific path, so the failure event dose not occur.
     From

$$X^1_{31} = (X^0_{16} \cap X^0_{23}) \oplus X^0_{17} \oplus X^0_{15} \oplus K^0_{15},$$
$$X^1_{22} = (X^0_{23} \cap X^0_{30}) \oplus X^0_{24} \oplus X^0_{6} \oplus K^0_{6},$$
$$X^1_{29} = (X^0_{30} \cap X^0_{21}) \oplus X^0_{31} \oplus X^0_{13} \oplus K^0_{13},$$
$$X^1_{24} = (X^0_{25} \cap X^0_{16}) \oplus X^0_{26} \oplus X^0_{8} \oplus K^0_{8},$$

     equations (4)-(6) should have solutions about subkey (K^0_{15}, K^0_6, K^0_{13}, K^0_8) with the following cases depending on the values of (ΔX^1_{22}, ΔX^1_{31}, $\Delta X^1_{16} \oplus \Delta X^0_{30}$, $\Delta X^1_{23} \oplus \Delta X^0_{21}$, $\Delta X^1_{25} \oplus \Delta X^0_{23} \oplus 1$).
     - $(0, 0, 0, 0, 0)$: there are 16 solutions to the above the three equations.
     - $(0, 1, *, 0, *)$: there are 4 solutions to the three equations for each of 4 the cases.
     - $(1, 0, *, *, 0)$: there are 4 solutions to the three equations for each of 4 the cases.
     - $(1, 1, *, *, *)$: there are 2 solutions to the three equations for each of 8 the cases.

     Clearly, we get in total 64 solutions for 17 cases, thus there are $\frac{64}{17}$ values of subkeys (K^0_{15}, K^0_6, K^0_{13}, K^0_8) for each pair in T_1 on average.
   - Similarly, solving the equations ($\Delta X^2_{31} = 0$, $\Delta X^2_{22} = 0$), we get about $\frac{32}{11}$ values of subkeys (K^0_0, K^0_7, K^0_{14}).
   - For the equations ($\Delta X^2_{20} = 0$, $\Delta X^2_{29} = 0$), we get a solution of subkeys (K^0_{12}, K^0_{14}).

     In Step 2, by solving 7 equations and combining these obtained subkeys, we get $\frac{64}{17} \times \frac{32}{11} \times 2^{-1}$ values of subkeys (K^0_0, K^0_6, K^0_7, K^0_8, K^0_{12}, K^0_{13}, K^0_{14}, K^0_{15}) which are involved in the 2nd round conditions .

3. For every subkey obtained in Step 2, by partially encrypting round 3, we get 5 equations. Guessing all subkeys (K_9^0, K_2^0, K_{11}^0, K_1^0), we use similar method above to solve the 5 equations, and get about 2 values of subkeys ($K_3^0 \oplus K_1^1$, $K_{10}^0 \oplus K_8^1$, K_{14}^1, $K_1^0 \oplus K_{15}^1$, K_{10}^1, K_0^1) for each guess. By the end of this step, we will get $\frac{64}{17} \times \frac{32}{11} \times 2^4$ values of subkeys involved in the first 3 rounds for each pair in $T1$.
4. Under the above computed subkeys, we get 2 corresponding equations about subkey bits depending on conditions of $\Delta X_{17}^4 = 0$, $\Delta X_{24}^4 = 0$ with probability 1. We can get one value of subkey bit ($K_2^2 \oplus K_4^1$, $K_0^2 \oplus K_2^1$) for every guessed subkey (K_4^0, K_5^0, K_3^1, K_3^0, K_{10}^0). By the end of this step, we will get $\frac{64}{17} \times \frac{32}{11} \times 2^9$ values of subkey bits involved in first 4 rounds conditions for every pairs in $T1$.
5. Applying the above similar method to the last 4 rounds, we also get $\frac{64}{17} \times \frac{32}{11} \times 2^9$ values of subkeys involved in the 4 rounds conditions for every pair in $T1$.
6. Combining all the subkeys computed from Step 4 to Step 5, we deduce $(\frac{64}{17})^2 \times (\frac{32}{11})^2 \times 2^{17} \approx 2^{23.9}$ solutions of the 49-bit subkeys for every chosen pair in T_1. Renew the corresponding counter by these solutions.
7. Go to Step 1 until no pairs in T_1 left.

Complexity Evaluation Let N_r be the number of plaintext pairs in T_1, C_s be the number of solutions to subkey for every pair in T_1, and C_{key} be the number of candidate subkeys obtained by Computing Subkey Candidates. Then $C_{key} = N_r \times C_s$. It is obviously that the time complexity of Computing Subkey Candidates (denoted as T_{csc}) is dominated by updating subkey counter in Step 6. Hence, the time complexity of Computing Subkey Candidates is estimated by the formula (4)

$$T_{csc} = C_{key}/(n \times n_r), \tag{4}$$

where we assume that the counter updating is equivalent to $\frac{1}{n}$ time-round computations, and n_r is the attack rounds. Therefore, the complexity of Computing Subkey Candidates is about $T_{csc} = C_{key}/(n \times n_r) = (N_r \times C_s)/(n \times n_r) = 2^{23.1} \times 2^{23.9} \approx 2^{38.6}$ encryptions.

Since the expected count of the right key is 2.7, we choose the subkeys whose counts are greater than or equal to 3, and exhaustively search them by trail encryptions. We apply the Poisson distribution in as follows to compute the number of the remaining subkeys. The probability that the event ξ occurs k times is

$$\Pr[\xi = k] = \frac{\lambda^k}{k!} \times e^{-\lambda},$$

where λ is the expectation of ξ.

Let $|sk|$ be the number of independent subkeys in the extended rounds which is used to deduce the input and output differences for a pair to satisfy the differential path. Because a wrong subkey occurs with probability $p_e = \frac{C_s}{2^{|sk|}}$, the expected count of a wrong subkey for all pairs in T_1 is $\lambda_e = N_r \times p_e = 2^{23.1} \times \frac{2^{23.9}}{2^{49}} = 2^{-2}$. Therefore, the number of the remaining subkeys that need

to be searched is

$$2^{49}(1 - \Pr[\xi_e = 0] - \Pr[\xi_e = 1] - \Pr[\xi_e = 2]) = 2^{40.25}.$$

So, we search $2^{40.25}$ 49-bit subkeys, and tranverse 15-bit subkey, which needs $2^{55.25}$ encryptions. We denote the exhaustive search complexity as T_{es}, and the total time complexity is obviously dominated by T_{es}.

Since the expected count of the right key is $\lambda_r = 2.7$, the probability that the right key count is greater than or equal to 4 is

$$1 - \Pr[\xi_r = 0] - \Pr[\xi_r = 1] - \Pr[\xi_r = 2] = 0.51.$$

Therefore, our attack on 21-round SIMON32/64 needs $2^{55.25}$ encryptions with 2^{31} chosen plaintexts, and the success probability is about 51%.

General Formula of Complexity Evaluation Let N be the pairs left in the data collection which are used to sieve the right key, n_c be the number of conditions related to subkeys sk in the extended rounds for differential attack. It is easy to prove that $C_{key} = 2^{|sk|} \times N \times 2^{-n_c}$ without consideration of filtering the wrong plaintext pairs.

Hence, the time complexity of Computing Subkey Candidates is computed by formula (5).

$$T_{csc} = 2^{|sk|} \times N \times 2^{-n_c}/(n \times n_r) \tag{5}$$

The expected count of a wrong subkey for all remaining pairs in data collection is obtained by formula (6)

$$\lambda_e = N \times 2^{-n_c} \tag{6}$$

3.3 Experimental Results of the Attack on 19-round SIMON32

In order to verify the correctness of our attacks, with the above 13-round differential mounted rounds 3-16, we first statistics the number of right pairs for all 2^{32} plaintexts with 100 random masterkeys respectively, there are about 4.95 right pairs satisfying a 13-round differential.

Furthermore, by prefixing 3 rounds on the top and appending 3 rounds at the bottom, we use the 13-round differential D_1 to attack 19 rounds, and expiriment a key recovery on 19-round SIMON32/64 with 2^{31} chosen plaintexts. There are totally 18 bits of subkey involved in 14 conditions of the extended differential path. By using the above attack method, there are about $2^{12} \times (\frac{17}{32})^2 \approx 2^{10.17}$ pairs left for 2^{31} chosen plaintexts after data collection and filtering, and there are about 2^{16} possible subkeys, those whose count is greater than or equal to 3 is about:

$$2^{18}(1 - \Pr[\xi_e = 0] - \Pr[\xi_e = 1] - \Pr[\xi_e = 2]) = 2^{9.25}.$$

We perform experiment for 100 random masterkeys, there are 22 subkeys which are obtained successfully. Hence, the experimental results are consistent with the complexity and success rate.

4 Differential Attack on Other SIMON versions

In this section, we describe the differential attacks on round-reduced SIMON48, SIMON64, SIMON96 and SIMON128 respectively.

4.1 Differential Attack on SIMON48

We utilize a 16-round differential $D : (800000, 220082) \rightarrow (800000, 220000)$ in [20] with probability $2^{-44.65}$ to mount 23-round attack on SIMON48/72 by adding 3 rounds on the top and 4 rounds at the bottom, and 24-round attack on SIMON48/96 by adding one more round on the top.

Attack on 23-round SIMON48/72 For the differential D, decrypt the first 3 rounds and encrypt the last 4 rounds. It is easy to obtain a set of sufficient bit conditions (see Table 6).

There are 11 conditions on plaintexts and 16 conditions not related subkey bits in rounds 1-2 ($\Delta X^2_{40} = \Delta X^1_{42} \oplus \Delta X^0_{40} = 1$, $\Delta X^2_{47} = \Delta X^1_{25} \oplus \Delta X^0_{47} = 0$). We build 2^{26} structures, and filter out the chosen pairs according to the conditions independent of secret key, there are $N = 2^{26-1+33-16} = 2^{42}$ pairs left. We get $2^{26-1+42-21} = 2^{46}$ pairs satisfying the input difference of the differential. Hence, the expected count of the right key is $\lambda_r = 2^{46-44.65} \approx 2.6$.

According to the key schedule, we find there are 64-bit independent subkey required to guess in order to conform the path D, i.e, $|sk| = 64$. To distinguish the correct key, we maintain a counter of size 2^{64}, which is the memory complexity. There are $n_c = 44$ bit conditions relating to the subkey bits in the 7 extended rounds. We apply the dynamic key-guessing method to compute the subkey candidates which may lead to the input and output differences of the high probability differential D for a pair, and update the corresponding subkey counter. The time complexity of Computing Subkey Candidates is computed by equation (5) which equals to $2^{64} \times 2^{42} \times 2^{-44}/(24 \times 23) = 2^{52.9}$ encryptions. By equation (6), the expected count of a wrong subkey for all remain pairs in data collection is $\lambda_e = N \times 2^{-n_c} = 2^{-2}$. Since the expected count of the right key $\lambda_r = 2.6$, we choose the subkeys whose count is greater than 2, and exhaustively search them by trail encryption. Then, the number of the remaining subkeys which should be searched is $2^{64}(1 - \Pr[\xi_e = 0] - \Pr[\xi_e = 1] - \Pr[\xi_e = 2]) = 2^{55.25}$. Therefore, the exhaustive search complexity is $2^8 \times 2^{55.25} = 2^{63.25}$ encryptions, which demonstrates the time complexity.

Since the expected count of the right key is $\lambda_r = 2.6$, the probability that the right key count is greater than or equal to 3 is $1 - \Pr[\xi_r = 0] - \Pr[\xi_r = 1] - \Pr[\xi_r = 2] = 0.48$. Therefore, our attack on 23-round SIMON48/72 needs $2^{63.25}$ encryptions with 2^{47} chosen plaintexts, and the success probability is about 48%.

Attack on 24-round SIMON48/96 We extend one more round on the top of the above 23-round differential path, and deduce 37 bit conditions independent of the secret key and $n_c = 59$ bit conditions relating to $|sk| = 88$ secret key.

According to 12 conditions not related to any key bit in the input differences of plaintexts and the first three rounds, we divide the plaintexts into 2^{12} sets. Each set is a structure with $2^{48-12} = 2^{36}$ plaintexts. We build 2^{11} structures, and get $2^{11-1+72-36} = 2^{46}$ pairs satisfying the input differences of the differential. Hence, there are about $2^{46-44.65} = 2.6$ right pairs. It means that the expected count of the right key is $\lambda_r = 2.6$.

We apply th method above, the time complexity of Computing Subkey Candidates is computed by equation (5) which equals to $2^{88} \times 2^{57} \times 2^{-59}/(24 \times 24) = 2^{76.8}$ encryptions. The expected count of a wrong subkey for all 2^{47} chosen plaintexts is still $\lambda_e = 2^{-2}$. Therefore, the exhaustive search complexity is $2^8 \times 2^{88}(1 - \Pr[\xi_e = 0] - \Pr[\xi_e = 1] - \Pr[\xi_e = 2]) = 2^{87.25}$. Since the expected count of the right key is $\lambda_r = 2.6$, the success rate is also 0.48. Consequently, our attacks on 24-round SIMON48/96 needs $2^{87.25}$ encryptions with 2^{47} chosen plaintexts, and the success probability is about 48%.

4.2 Differential Attacks on SIMON64/96/128

Here, we give a brief description of the differential attacks on SIMON64, SIMON96 and SIMON128 with the similar method mentioned in the Section 3.

Attack on SIMON64 Versions We invoke a 21-round differential with probability $2^{-60.21}$ in [20] to mount a 28-round attack on SIMON64/96 by adding 3 rounds on the top and 4 rounds at the bottom. We deduce 25 conditions on plaintexts, and 21 conditions in the first two rounds not relating to secret key, and 34 conditions relating to 69 bit equivalent subkeys (see Table 7).

We prefix one round on the top of the 28-round attack to launch the 29-round attack on SIMON64/128. There are 8 conditions on plaintexts, and 18 conditions in the first three rounds independent of secret key, and 54 conditions related to 101 bit equivalent subkeys (see Table 7).

Attack on SIMON96 Versions Applying a 30-round differential with probability $2^{-92.2}$ in [1], we mount a 37-round attack on SIMON96 with 3 rounds on the top and 4 rounds in the tail (see Table 8). There are 47 conditions on plaintexts, 25 conditions in the first two rounds not relating to secret key. For the 103-bit subkey from the 59 sufficient conditions, we show that the 103-bit subkey can be computed from a 88-bit subkey for SIMON96/96.

Attack on SIMON128 Versions From a 41-round differential with probability $2^{-124.6}$ in [1], we mount a 49-round attack on SIMON128/128 and SIMON128/192 by adding 4 rounds on the top and 4 rounds in the tail (see Table 9). There are 69 conditions on plaintexts, and 21 conditions in the first three rounds not relating to secret key bits. There are 168-bit subkeys involved in the 76 sufficient conditions. By key schedules, we know that 168-bits of subkey can be obtained from 164 bit subkeys for SIMON128/192, and obtained from 122 bit subkeys for SIMON128/128 respectively.

We prefix one round at the bottom of the 49-round attack to launch the 50-round attack on SIMON128/256 (see Table 9). We have 69 conditions on plaintexts, 21 conditions in the first three rounds not related secret key bits, and the 220-bit subkey from the 96 sufficient conditions.

We choose plaintexts to construct structures using the similar techniques as described in Section 3, and apply the dynamic key-guessing method to compute the subkey candidates which lead to the input and output differences of the differential for a pair, and update the corresponding subkey counter. The time complexity is computed by equation (5). The time complexities and success rates are summarized in Table 5.

Table 5. Differential Attacks for Reduced SIMONs

Cipher	Attacked Rounds	$\|sk\|$	λ_e	λ_r	Chosen Count	Data Complexity	Time Complexity T_{es}	Success Rate
SIMON64/96	28	69	2^{-2}	3.46	4	2^{63}	$2^{84.25}$	0.46
SIMON64/128	29	101	2^{-2}	3.46	4	2^{63}	$2^{116.25}$	0.46
SIMON96/96	37	88	2^{-2}	3.48	2	2^{95}	2^{95}	0.86
SIMON96/144	37	103	2^{-2}	3.48	4	2^{95}	$2^{132.25}$	0.46
SIMON128/128	49	122	2^{-2}	2.6	2	2^{127}	2^{127}	0.73
SIMON128/192	49	164	2^{-2}	2.6	3	2^{127}	$2^{183.25}$	0.48
SIMON128/256	50	220	2^{-2}	2.6	3	2^{127}	$2^{247.25}$	0.48

5 Conclusion

In this paper, we present the improved differential attacks on SIMON32, SIMON48, SIMON64, SIMON96, and SIMON128 with 2 to 4 more rounds than previous attacks. The main contribution of our work is to compute sufficient conditions to ensure the differential path hold, and obtain the corresponding subkey bits equations. Based on the equations, we reduce the key space searched greatly. Furthermore, we present a new method to build structures in data collection phase, and decrease the time complexity of sieving the collected pairs. Our technique can be applied to other lightweight block ciphers depending on the bitwise operations.

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., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer (1993)

6. Biryukov, A., Roy, A., vesselin Velichkov: Differential Analysis of Block Ciphers SIMON and SPECK. In: FSE (2014)
7. 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)
8. 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)
9. 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)
10. De Cannière, C., Rechberger, C.: Finding SHA-1 characteristics: General results and applications. In: Lai, X., Chen, K. (eds.) Advances in Cryptology – ASIACRYPT 2006. Lecture Notes in Computer Science, vol. 4284, pp. 1–20. Springer (Dec 2006)
11. 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)
12. 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)
13. Knellwolf, S., Meier, W., Naya-Plasencia, M.: Conditional differential cryptanalysis of nlfsr-based cryptosystems. In: Abe, M. (ed.) ASIACRYPT. Lecture Notes in Computer Science, vol. 6477, pp. 130–145. Springer (2010), http://dblp.uni-trier.de/db/conf/asiacrypt/asiacrypt2010.html#KnellwolfMN10
14. Knudsen, L.: DEAL-a 128-bit Block Cipher. complexity 258(2) (1998)
15. 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)
16. xuejia lai: Higher Order Derivatives and Differential Cryptanalysis. communications and cryptography (1994)
17. Leurent, G.: Construction of differential characteristics in ARX designs application to skein. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I. Lecture Notes in Computer Science, vol. 8042, pp. 241–258. Springer (2013), http://dx.doi.org/10.1007/978-3-642-40041-4_14
18. Mendel, F., Nad, T., Schläffer, M.: Finding SHA-2 characteristics: Searching through a minefield of contradictions. In: Lee, D.H., Wang, X. (eds.) Advances in Cryptology – ASIACRYPT 2011. Lecture Notes in Computer Science, vol. 7073, pp. 288–307. Springer (Dec 2011)
19. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-Bit Blockcipher CLEFIA (Extended Abstract). In: FSE. pp. 181–195 (2007)
20. Siwei Sun, Lei Hu, M.W.P.W.K.Q.X.M.D.S.L.S.: Automatic enumeration of (related-key) differential and linear characteristics with predefined properties and its applications. Cryptology ePrint Archive, Report 2014/747 (2014), http://eprint.iacr.org/
21. Stevens, M., Lenstra, A.K., de Weger, B.: Chosen-prefix collisions for MD5 and colliding X.509 certificates for different identities. In: Naor, M. (ed.) Advances in Cryptology – EUROCRYPT 2007. Lecture Notes in Computer Science, vol. 4515, pp. 1–22. Springer (May 2007)

22. Theobald, T.: How to break Shamir's asymmetric basis. In: Coppersmith, D. (ed.) Advances in Cryptology – CRYPTO'95. Lecture Notes in Computer Science, vol. 963, pp. 136–147. Springer (Aug 1995)
23. 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)
24. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full SHA-1. In: Shoup, V. (ed.) Advances in Cryptology – CRYPTO 2005. Lecture Notes in Computer Science, vol. 3621, pp. 17–36. Springer (Aug 2005)

A Differential Conditions

Here, we list some differential conditions used in our cryptanalysis.

Table 6: Sufficient Conditions of Extended Differential Path of 23/24-round SIMON48

Rounds	Input Differences of Each Round
0	0,*,*,*,*,*,*,0,*
1	*,**0**,**0**,*,*,**0**,*,*,**0**,**0**,*,**0**,*,*,*,**0**,*,*,**1**,*,*,*,**1**,*,0,*,*,*,*,*,*,0,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*
2	0,*,**0**,**0**,**1**,*,**0**,0,*,**0**,**0**,**0**,**0**,**0**,*,*,**0**,**0**,*,**0**,**1**,*,*,**0**,*,0,0,*,*,0,*,*,0,0,*,0,*,*,*,0,*,*,1,*,*,*,1,*
3	**0**,0,1,**0**,**0**,0,**1**,**0**,0,0,**0**,0,**0**,**0**,**0**,0,**1**,**0**,0,**0**,**0**,**0**,1,**0**,0,*,0,0,1,*,0,0,*,0,0,0,0,0,*,*,0,0,*,0,1,*,*,0
4	1,**0**,0,0,0,**0**,0,0,**0**,0,0,0,0,0,**0**,**0**,0,0,**0**,0,0,**0**,**0**,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,1,0
4 → 20	16-round differential D
20	1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,0,0,**0**
21	0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,*,0,0,0,0,0,1,*,1,**0**,0,0,0,**0**,0,0,**0**,0,0,0,0,0,**0**,**0**,0,0,**0**,0,0,**0**,**0**,0
22	0,*,0,0,1,*,0,0,*,0,0,0,0,0,*,*,0,0,*,0,1,*,*,0,**0**,0,1,**0**,**0**,0,**1**,**0**,0,0,**0**,0,**0**,**0**,**0**,0,*,**0**,0,**0**,**0**,**0**,1,*
23	*,0,0,*,*,0,*,*,0,0,*,0,*,*,*,0,*,*,1,*,*,*,1,*,0,*,**0**,**0**,**1**,*,**0**,0,*,**0**,**0**,**0**,**0**,**0**,*,*,**0**,**0**,*,**0**,**1**,*,*,**0**
24	0,*,*,*,*,*,*,0,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,0,0,*,*,0,*,*,0,0,*,0,*,*,*,0,*,*,1,*,*,*,1,*

Table 7: Sufficient Conditions of Extended Differential Path of 28/29-round SIMON64

Rounds	Input Differences of Each Round
0(left)	*,*,*,*,*,*,*,*,*,*,*,*,0,*,*,*,0,*,*,0,0,0,*,0,*,*,*,0,*,*,*,*
0(right)	*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,0,*,*,*,*,*,*,*,*,*,*,*,*
1(left)	*,*,*,**0**,*,*,**1**,*,*,*,**1**,*,*,**0**,**0**,*,*,**0**,**1**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**
1(right)	*,*,*,*,*,*,*,*,*,*,*,*,0,*,*,*,0,*,*,0,0,0,*,0,*,*,*,0,*,*,*,*
2(left)	**0**,**0**,*,**0**,**0**,**0**,*,**0**,**1**,*,*,**0**,0,*,**0**,**0**,1,*,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**
2(right)	*,*,*,0,*,*,1,*,*,*,1,*,*,0,0,*,*,0,1,0,0,0,0,0,0,0,*,0,0,0,*,0
3(left)	**0**,**0**,**0**,0,**0**,**0**,0,**0**,**0**,**0**,1,**0**,**0**,0,1,**0**,**0**,0,1,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0
3(right)	0,0,*,0,0,0,*,0,1,*,*,0,0,*,0,0,1,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0
4(left)	0,0,**0**,0,0,0,**0**,0,0,**0**,**0**,0,1,**0**,0,0,0,**0**,0,0,0,0,0,0,0,0,0,0,0,0,0,0
4(right)	0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0
4 → 25	21-round differential D
25(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0
25(right)	0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,0,0,**0**,0,0,0,0,0,0,0,0,0,0,0,0,0,0
26(left)	0,0,0,0,0,0,0,0,0,0,*,0,0,0,0,0,1,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0
26(right)	0,0,**0**,0,0,0,0,0,0,**0**,**0**,0,0,0,0,0,0,**0**,**0**,0,1,0,0,0,0,0,0,0,0,0,0,0
27(left)	0,0,*,0,0,0,0,0,0,*,*,0,0,0,0,1,*,*,0,1,0,0,0,0,0,0,0,0,0,0,0,0
27(right)	**0**,**0**,0,0,0,0,**0**,**0**,**0**,0,*,0,0,**0**,**0**,**0**,1,*,0,0,0,0,0,0,0,0,**0**,0,0,0,0,0
28(left)	*,*,0,0,0,0,*,*,*,0,*,0,1,*,*,*,0,*,0,0,0,0,0,0,0,0,*,0,0,0,0,0
28(right)	**0**,0,*,0,**0**,**0**,**0**,**0**,*,*,0,**0**,**0**,**0**,**1**,*,*,0,**1**,0,0,0,0,0,**0**,**0**,0,0,0,0,**0**,**0**
29(left)	*,0,*,0,*,*,*,*,*,*,1,*,*,*,*,*,*,0,*,0,0,0,0,0,*,*,0,0,0,0,*,*
29(right)	*,*,0,0,0,0,*,*,*,0,*,0,1,*,*,*,0,*,0,0,0,0,0,0,0,0,*,0,0,0,0,0

Table 8: Sufficient Conditions of Extended Differential Path of 37-round SIMON96

Rounds	Input Differences of Each Round
0(left)	0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,1,*,*,*,*,*,*,0,0,*,*,*,1,0,0,0,1,*,*,0,1,0,0,0,0,0,0
0(right)	0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,0,*,*,*,*,*,*,0,1,*,*,*,0,*,0,0,0,0,0,0,0
1(left)	0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,**1**,*,*,**0**,0,*,**0**,**0**,**1**,*,*,0,0,**0**,**0**,**0**,1,*,0,0,0,0,0,0,0
1(right)	0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,1,*,*,*,*,*,*,0,0,*,*,*,1,0,0,0,1,*,*,0,1,0,0,0,0,0,0
2(left)	0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,0,**0**,**0**,**0**,**1**,**0**,**0**,0,1,**0**,**0**,**0**,1,0,0,0,0,**0**,**0**,0,1,0,0,0,0,0,0

2(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,1,*,*,0,0,*,0,0,1,*,*,0,0,0,0,0,1,*,0,0,0,0,0,0,0
3(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,0,**0**,**0**,0,1,**0**,0,0,0,**0**,**0**,0,0,0,0,0,0,**0**,0,0,0,0,0,0,0
3(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0
3 → 33	30-round differential D
33(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0
33(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,0,0,0,**0**,**0**,0,1,0,0,0,1,**0**,0,0,1,0,0,0,0,0,0
34(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,0,0,1,*,*,0,1,0,0,0,0,*,0,0,1,0,0,0,0,0,0
34(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,0,**0**,**0**,**0**,0,**0**,0,0,**0**,**0**,**0**,1,**0**,**0**,0,0,**0**,**0**,0,1,**0**,0,0,0,0,0,0,0
35(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,0,0,*,*,*,0,*,0,1,*,*,*,0,*,*,0,0,*,*,0,0,*,0,0,0,0,0,0,0
35(right)	0,0,0,0,0,0,0,**0**,0,0,0,0,0,**0**,**0**,**0**,0,**0**,0,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,**0**,**0**,**1**,*,*,**0**,1,**0**,**0**,**0**,0,*,**0**,0,1,0,0,0,0,0,0
36(left)	0,0,0,0,0,0,0,*,0,0,0,0,0,*,*,*,0,*,0,*,*,*,*,*,*,*,*,*,*,*,*,*,*,1,*,*,*,0,*,*,0,1,0,0,0,0,0,0
36(right)	0,0,0,0,0,**0**,**0**,**0**,0,**0**,0,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,**0**,**0**,*,*,*,**0**,*,**0**,**1**,*,*,*,**0**,*,*,**0**,**0**,*,*,**0**,0,*,0,0,0,0,0,0,**0**
37(left)	0,0,0,0,0,*,*,*,0,*,0,*,1,*,0,0,0,0,0,0,*
37(right)	0,0,0,0,0,0,0,*,0,0,0,0,0,*,*,*,0,*,0,*,*,*,*,*,*,*,*,*,*,*,*,*,*,1,*,*,*,0,*,*,0,1,0,0,0,0,0,0

Table 9: Sufficient Conditions of Extended Differential Path of 49/50-round SIMON128

Rounds	Input Differences of Each Round
0(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,0,*,*,*,0,*,0,0,0,0,0,0,0
0(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,0,1,0,0,0,0,0,0,0
1(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,*,*,*,**0**,*,*,**1**,*,*,*,**1**,*,*,**0**,**0**,*,*,0,1,0,0,0,0,0,0
1(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,0,*,*,*,0,*,0,0,0,0,0,0,0
2(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,**1**,*,*,**0**,0,*,**0**,**0**,1,*,0,0,0,0,0,0,0
2(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,1,*,*,*,1,*,*,0,0,*,*,0,1,0,0,0,0,0,0
3(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,**0**,0,0,**0**,**0**,**0**,0,**0**,**0**,0,**0**,**0**,**0**,1,**0**,**0**,0,1,**0**,**0**,0,1,0,0,0,0,0,0,0
3(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,1,*,*,0,0,*,0,0,1,*,0,0,0,0,0,0,0
4(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,**0**,0,0,0,**0**,**0**,0,1,**0**,0,0,0,0,**0**,0,0,0,0,0,0,0
4(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0
4 → 45	41-round differential D
45(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0
45(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,**0**,0,0,0,**0**,**0**,0,1,**0**,0,0,0,0,**0**,0,0,0,0,0,0,0
46(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,1,*,*,0,0,*,0,0,1,*,0,0,0,0,0,0,0
46(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,**0**,0,0,**0**,**0**,**0**,0,**0**,**0**,0,**0**,**0**,**0**,1,**0**,**0**,0,1,**0**,**0**,0,1,0,0,0,0,0,0,0
47(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,1,*,*,*,1,*,*,0,0,*,*,0,1,0,0,0,0,0,0
47(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,**1**,*,*,**0**,0,*,**0**,**0**,1,*,0,0,0,0,0,0,0
48(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,0,*,*,*,0,*,0,0,0,0,0,0,0
48(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,*,*,*,**0**,*,*,**1**,*,*,*,**1**,*,*,**0**,**0**,*,*,0,1,0,0,0,0,0,0
49(left)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,0,1,0,0,0,0,0,0,0
49(right)	0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,*,*,*,**0**,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,**0**,*,*,*,0,*,0,0,0,0,0,0,0
50(left)	0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,1,*,0,0,0,0,0,0,0
50(right)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,0,1,0,0,0,0,0,0,0