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 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 18-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 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 which were used to analyze various block cipher primitives[16,15,14,4,23]. Another type of differential attack is the modular differential attack which is based on modular differences instead of XOR differences, and it is widely used to attack or evaluate the 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 specifically optimized differential path. Then he determines a set of sufficient bit conditions to result in 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 the satisfaction of more bit conditions. 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 recalling the previous work on SIMON family, we briefly give some explanations about the versions of SIMON. SIMON$2n/l_k$ denotes a SIMON version with block size $2n$ and key length l_k. SIMON$2n$ means 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 the impossible differential attacks on 14, 15, 16, 19, and 22 rounds of the corresponding versions for 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^{32}, 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 with 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 enlarged differential paths by investigating the bitwise behavior of differences in the paths. All the bit conditions can be divided into two types. The first type of conditions 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.

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^{32}	2^{31}	[6]
			21	$2^{52.25}$	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	$2^{119.25}$	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	$2^{135.25}$	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

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 guessing 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 $2^{22.28}$ solutions of 51-bit subkey for a filtered palintext pair. It implies that, for the collected pair, we need to guess $2^{22.28}$ subkey space instead of 2^{51} 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 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 $2^{52.25}$, $2^{63.25}$, $2^{87.25}$, $2^{84.25}$, $2^{119.25}$, 2^{95}, $2^{135.25}$, 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, give a brief description of block cipher SIMON family and some observations. Section 3 describes the details of our differential attacks on 21-round SIMON32. 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 the 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 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 left-most bit of L_i, $X_i[2n-1]$ is the right-most bit of L_i, $X_i[0]$ is the left-most bit of R_i, and $X_i[n-1]$ 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, we refer to [3]. In fact, the key schedules are linear, the master key can be deduced to any mn independent bits of subkeys.

2.3 Some Observations

Observation 1 ([12]) *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 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 key bit guessing , and obtain a subkey bit according to the following four cases.*

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 $\Delta X_{i+1}[j+n](j < n)$.*
2. *When $(\Delta X_i[(j+1)\%n+n], \Delta X_i[(j+8)\%n+n]) = (0,1)$, we can compute $K_{i-1}[(j+1)\%n]$ by the value of $\Delta X_{i+1}[j+n](j < n)$.*
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 $\Delta X_{i+1}[j+n](j < n)$.*
4. *When $(\Delta X_i[(j+1)\%n+n], \Delta X_i[(j+8)\%n+n]) = (1,1)$, one equivalent key bit $K_{i-1}[(j+8)\%n] \oplus K_{i-1}[(j+1)\%n]$ 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.

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

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

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

It is obviously that Observation 2 is obtained from equations (1)-(3). By Observation 2, we easily get the following observation.

Observation 3 *Given an equation* $\Delta X_{i+1}[j+n] = b$*, where* $b = 0$ *or* 1*, we can find all the solutions of the 2-bit subkey* $(K_{i-1}[(j+1)\%n], K_{i-1}[(j+8)\%n])$ *which satisfies the equation by the following 5 cases.*

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* $(K_{i-1}[(j+1)\%n], K_{i-1}[(j+8)\%n])$.

Observation 3 can be directly verified by Observation 2. From Observation 3, 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 the 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 a 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. 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 Sufficient Conditions for Differential Path of 21-round SIMON32

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

$$D : (2000, 8000) \rightarrow (2000, 0000).$$

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 to ensure the middle differential path from round 4 to round 17 hold (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 17 conditions in bold from round 1 and round 19 are independent of subkey bits, 33 conditions in bold from rounds 2-4 and 17-19 are related to subkey bits. If all the 50 conditions (17+33) hold, the other conditions in the extended path hold with probability 1. So these 50 conditions are sufficient to lead to the input and output differences of the 13-round differential D, 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, *, *, *, 0, *, *, 1, *
1	*, *, **0**, **0**, **0**, **0**, *, *, **0**, **0**, *, **0**, **1**, *, *, **0**, *, 0, *, 0, *, *, *, 0, *, *, 1, *, *, *, *, *
2	**0**, 0, **1**, 0, **0**, **0**, **0**, 0, *, **0**, 0, **0**, **0**, **0**, **1**, *, *, *, 0, 0, 0, 0, *, *, 0, 0, *, 0, 1, *, *, 0
3	**1**, **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, 1, *
4	0, 0, 1, 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
4 → 17	13-round differential D
17	0, 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, 0
18	1, *, 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**
19	*, 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**
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 17 conditions which are independent of the secret key in Table 3, and the 33 conditions related to the secret key in the 2rd column of Table 6 in Appendix. The clue of our attack is to build the structures in the data collection phase to get 17 conditions independent of the secret key, get 33 equations on key bits from the other 33 conditions, then find the possible solutions of these equations to reduce the key space searched. Table 6 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 of the equation to hold, and P_r^F means that a wrong bit condition occurs which results in the dissatisfaction of the differential path.

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	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	$\Delta X_{20}[4] = 0$, $\Delta X_{20}[5] = 0$, $\Delta X_{20}[6] = 0$, $\Delta X_{20}[7] = 0$, $\Delta X_{20}[11] = 0$, $\Delta X_{20}[12] = 0$, $\Delta X_{20}[13] = 0$, $\Delta X_{20}[14] = 1$

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 9 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 Observation 2 to reduce the key space greatly.

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

1. There are 4 conditions on the input difference of plaintexts, 9 conditions in the 2nd round. We divide the plaintexts into 2^{13} structures including $2^{32-13} = 2^{19}$ plaintexts for each. By Observation 2, $K_0[j]$ is independent of $\Delta X_1[j]$, which does not impact the structure. According to the round function definition, we build 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 fix 4 bits of $X_0[i] (i = 17, 19, 23, 26)$, and 9 bits of $X_1[j]$ to be constants, and obtain each structure by solving the above equations system.
2. For structures A and A' with 2 different bits ($X_0[26]$, $X_1[28]$), we find the corresponding ciphertexts, and save them to a table indexed by $X_{21}[t]$, where $\Delta X_{21}[t] = 0$. There are about $2^{19\times 2-8} = 2^{30}$ remaining pairs for each structure.
3. We build 2^{12} structures, and filter out the remaining pairs by decrypting one round according to the conditions in Table 3. Then there are $2^{12-1+30-10} = 2^{31}$ pairs left. Store the pairs in table T.

For the $2^{12+19} = 2^{31}$ collected plaintexts, we get $2^{12-1+38-19} = 2^{30}$ pairs satisfying the input difference. Hence, there are about $2^{30-28.11} = 3.7$

right pairs occurred on average.

Filtering the Plaintext Pairs Because the conditions in round 2 and 19 are unrelated to the secret key, for each pair in T, we first filter those pairs who have failure events in round 2 and 19. For $\Delta X_2[16] = 0$. By equation (1), we know that,

$$\Delta X_2[16] = (\Delta X_1[17] \cap X_1[24]) \oplus (X_1[17] \cap \Delta X_1[24]) \oplus (\Delta X_1[17] \cap \Delta X_1[24]) \oplus \Delta X_1[18] \oplus \Delta X_0[16].$$

From Table 2, we know that, $X_1[24] = 0$, $X_1[18] = 0$. We simplify the equation as $\Delta X_2[16] = \Delta X_1[17] \cap X_1[24] \oplus \Delta X_0[16] = 0$. Therefore, when $\Delta X_1[17] = 0$ and $\Delta X_0[16] = 1$, there is no solution to the equation. Thus we can discard this plaintext pair, and the probability for this situation (we call it a failure event) is $P_r^F = \frac{1}{4}$.

Consider the condition $\Delta X_2[22] = 0$, by the same method, when $\Delta X_1[23] = 0$, $\Delta X_1[30] = 0$ and $\Delta X_0[22] = 1$, there is no solution to the equation, and the probability for the failure event is $P_r^F = \frac{1}{8}$.

Applying similar method to conditions on $\Delta X_2[18, 29, 30, 28, 21, 25]$ of the 2nd round and conditions on $\Delta X_{19}[15, 0, 14, 7, 8]$ of the 19-th round. We totally have $2^{31} \times (1 - \frac{1}{4})^8 \times (1 - \frac{1}{8})^5 \approx 2^{26.72}$ pairs left. We store $2^{26.72}$ plaintext pairs in T_1.

Computing Subkey Candidates By partial encryptions and decryptions, we know that, there are totally 52 bits of subkey involved in 33 conditions, and 51 bits are independent according to key schedules. Given a plaintext pair in T_1, we obtain 33 equations of 51-bit subkey 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 can compute all the solutions to 33 equations, every solution is a possible candidate of 51-bit subkey. We collect all the solutions of corresponding $2^{26.72}$ 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 results in the same differential path, we deduce the solutions of different subkey. The subkey solved is decided by the specific differences in the differential path. To detect the correct key, we maintain a lot of counters of size 2^{51}, initialized with 0. Given a plaintext pair in T_1, the computation details of 33 equations about 51-bit subkey is as follows.

1. Select a new pair in T_1
2. We get 10 equations by partially encrypting round 2, see Table 6 in Appendix.

– By condition $\Delta X_2[16] = 0$, we partially encrypt round 2, and obtain that,

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

Because the pair is filtered by removing all the failure events in round 2 and round 19 corresponding to the specific path, so the failure event $\Delta X_1[17] = 0$ and $\Delta X_0[16] = 1$ dose not occur. So $\Delta X_2[16] = 0$ has solutions about subkey bit $K_0[8]$ only with following 3 cases.

- When $\Delta X_1[17] = 0$ and $\Delta X_0[16] = 0$, there are two solutions to equation $\Delta X_2[16] = 0$ by the similar method in Observation 3, i.e, $K_0[8]$ can be taken as 0 or 1.
- When $\Delta X_1[17] = 1$, both for $\Delta X_0[16] = 0$ and 1, we deduce one solution of the subkey bit $K_0[8]$.

Clearly, we get 4 solutions for these 3 cases, and there are about $\frac{4}{3}$ solutions of $K_0[8]$ for each one of pairs in T_1 on average.

– Similarly, solving the equation $\Delta X_2[18] = 0$, we get about $\frac{4}{3}$ solutions of subkey bit $K_0[3]$ on average.
– From condition $\Delta X_2[22] = 0$, partially encrypting round 2, we get the following equations.

$$\begin{aligned}\Delta X_2[22] &= (X_1[23] \cap \Delta X_1[30]) \oplus (\Delta X_1[23] \cap X_1[30])\\ &\quad \oplus (\Delta X_1[23] \cap \Delta X_1[30]) \oplus \Delta X_0[22],\\ X_1[23] &= (X_0[24] \cap X_0[31]) \oplus X_0[25] \oplus X_0[7] \oplus K_0[7],\\ X_1[30] &= (X_0[31] \cap X_0[22]) \oplus X_0[16] \oplus X_0[14] \oplus K_0[14].\end{aligned}$$

By Observation 3, there are only 7 cases happened, and each case has the solutions of 2-bit subkey $(K_0[7], K_0[14])$. We find these solutions according to the values of ($\Delta X_1[23]$, $\Delta X_1[30]$, $\Delta X_2[22] = 0$).

- (0,0,0): there is no subkey bit involved in $\Delta X_2[22]$, and there are 4 solutions of $(K_0[7], K_0[14])$.
- (0,1,0) or (0,1,1): we have one solution of $K_0[7]$, so, there are two solutions of $(K_0[7], K_0[14])$.
- (1,0,0) or (1,0,1): we have one solution of $K_0[14]$, two solutions of $(K_0[7], K_0[14])$
- (1,1,0) or (1,1,1): we have one solution of $K_0[7] \oplus K_0[14]$, two solutions of $(K_0[7], K_0[14])$.

For each pair in T_1, we obtain about $\frac{16}{7}$ values of $(K_0[7], K_0[14])$ on average.

– Using the above similar techniques, solve 7 equations on corresponding 7 bits in $\Delta X_2[21, 27, 20, 29, 30, 28, 25]$ of the 2nd round listed in Table 6 in Appendix.
  - Two equations corresponding to $\Delta X_2[21, 25]$ has $\frac{16}{7}$ values of($K_0[6]$,$K_0[13]$), ($K_0[10]$,$K_0[1]$) respectively.
  - Three equations with $X_2[29, 30, 28]$ has $\frac{4}{3}$ values of $K_0[5]$, $K_0[15]$, $K_0[4]$ respectively.
  - For equation of condition $\Delta X_2[27]$, we obtain one solution on $K_0[3]$, because $K_0[3]$ has occurred in the previous equation corresponding to $\Delta X_2[18]$. If two solutions are different, this is a failure event which happens with probability $P_r^F = \frac{1}{2}$.
  - Similar to $K_0[3]$, the equation on $\Delta X_2[20]$ has one solution of $K_0[5]$ with probability $P_r = 1$, it is a failure event with $P_r^F = \frac{1}{2}$.

  In Step 2, by solving 10 equations, we obtain $(\frac{4}{3})^5 \times (\frac{16}{7})^3 \times 2^{-2}$ solutions of the following subkey

$$K_0[8, 3, 7, 14, 6, 13, 5, 15, 4, 10, 1],$$

  which is involved in 2nd round conditions .

3. For the subkeys obtained in Step 2, partially encrypting round 3, we get total 7 equations. Each of three equations from $\Delta X_3[17, 22, 29]$ has one solution. The equation from $\Delta X_3[26]$ has 2 solutions. The equation from $\Delta X_3[30]$ has $\frac{4}{3}$ solutions, and failure events happen with $P_r^F = \frac{1}{4}$, totally it has $\frac{4}{3} \times (1 - \frac{1}{4}) = 1$ solution on average. The equation $\Delta X_3[16]$ has $\frac{16}{7}$ solutions, and a failure event happen with $P_r^F = \frac{1}{8}$, so the equation has $\frac{16}{7} \times (1 - \frac{1}{8}) = 2$ solutions. The equation of $\Delta X_3[23]$ has $\frac{16}{7}$ solutions, and a failure event happens with $P_r^F = \frac{1}{8}$, so the equation has $(2^2 \times \frac{16}{7} \times (1 - \frac{1}{8}) = 2^3$ solutions. More details about solutions of equations are referred to Table 6 in Appendix. We can find 2^5 values of subkey involved in the conditions of 3rd round.
4. For the subkeys computed in Step 3, we get 2 corresponding equations about subkey bits depending on conditions of $\Delta X_4[31, 24]$ with probability 1. By the end of this step, we will get $(\frac{4}{3})^5 \times (\frac{16}{7})^3 \times 2^5$ values of subkey bits involved in first 4 rounds conditions for every pairs in $T1$.
5. Similar to the above method, we decrypt round 19, and get 7 equations corresponding to conditions of $\Delta X_{19}[6, 15, 0, 13, 14, 7, 8]$. Three equations corresponding to $\Delta X_{19}[15, 0, 14]$ have $\frac{4}{3}$ values of ($K_{20}[7]$, $K_{20}[1]$,$K_{20}[6]$), two equations corresponding to $\Delta X_{19}[7, 8]$ has $\frac{16}{7}$ values of($K_{20}[8], K_{20}[15]$), ($K_{20}[9]$,$K_{20}[0]$). Two equations corresponding

to $\Delta X_{19}[6,13]$ have 1 value of$(K_{20}[7], K_{20}[5])$ respectively, where there is a failure event about $K_{20}[5]$ with probability $P_r^F = \frac{1}{2}$. We get $(\frac{4}{3})^3 \times (\frac{16}{7})^2 \times 2^{-1}$ values of subkey $K_{20}[7,1,5,6,8,15,9,0]$ involved in conditions of round 19.

6. For the subkeys solved in Step 5, we decrypt round 18, and have 5 equations corresponding to conditions $\Delta X_{18}[15,2,8,10,9]$. The equation $\Delta X_{18}[15]$ has one solution, the equation $\Delta X_{18}[8]$ has 2 solutions. Two equations from $\Delta X_{18}[0,9]$ have $\frac{16}{7}$ solutions, and failure events happen with $P_r^F = \frac{1}{8}$, totally have $\frac{16}{7} \times (1 - \frac{1}{8}) = 2$ solutions respectively, the equation $\Delta X_{18}[2]$ has 2^2 solutions. We can find 2^5 values of subkey involved in 18th round conditions under each one of subkeys involved in 19th round.
7. For the subkeys obtained in Step 6, we decrypt round 17, and have 2 equations corresponding to conditions of $\Delta X_{17}[10,1]$. By the end of this step, we get $(\frac{4}{3})^3 \times (\frac{16}{7})^2 \times 2^9$ values of subkey bits of last 4 rounds for every pairs in T_1.
8. Combining all the subkeys computed from Step 4 to Step 7, because 51 bits are independent in 52-bit keybits, we can obtain $(\frac{4}{3})^8 \times (\frac{16}{7})^5 \times 2^{13} \approx 2^{22.28}$ solutions to the 51-bit subkey for every chosen pair in T_1. Renew the counter by these solutions.
9. Go to Step 1 until no pair in T_1 left.

Complexity Evaluation For remaining $2^{31} \times (1 - \frac{1}{4})^8 \times (1 - \frac{1}{8})^5$ valid pairs in T_1, we totally get $2^{31} \times (1 - \frac{1}{4})^8 \times (1 - \frac{1}{8})^5 \times (\frac{4}{3})^8 \times (\frac{16}{7})^5 \times 2^{13} \approx 2^{49}$ solutions to 51-bit subkey. It is obviously that the time complexity of Computing Subkey Candidates denoted as T_{csc} is dominated by updating subkey counter in the Step 8. Hence, the time complexity of this attack can be computed by the formula (4).

$$T_{csc} = 2^{|sk|} \times N \times 2^{-n_c}/(16 \times n_r), \tag{4}$$

where $|sk|$ is the number of independent subkeys in the extended rounds which is used to deduce the input and output differences of the differential path. N is the pairs left in the data collection which are used to sieve the right key, n_c is the number of conditions related with subkeys sk, and n_r is the rounds of the attack. We assume that the counter updating is equivalent to $\frac{1}{16}$-round computations. Therefore, the complexity of Computing Subkey Candidates is about $2^{51} \times 2^{31} \times 2^{-33}/(16 \times 21) \approx 2^{40.6}$ encryptions.

Since we know the expected count of the right key is 3.7 in the data collection, we choose the subkeys whose counts are greater than or

equal to 4, and exhaustively search them by trail encryption. We apply the Poisson distribution in the following 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. Because a wrong subkey occurs with probability $p_e = \frac{2^{22.28}}{2^{51}}$, the expected count of a wrong subkey for all $2^{26.72}$ pairs is $\lambda_e = 2^{26.72} \times p_e = 2^{-2}$. In fact the expected count of a wrong subkey for all remaining pairs in data collection can be also computed by the equation

$$\lambda_e = N \times 2^{-n_c}. \tag{5}$$

Therefore, the number of the remaining subkeys which should be searched is

$$2^{51}(1 - \Pr[\xi_e = 0] - \Pr[\xi_e = 1] - \Pr[\xi_e = 2] - \Pr[\xi_e = 3]) = 2^{39.25}.$$

So, we search $2^{39.25}$ 51-bit subkeys and the rest 13-bit subkey, which needs $2^{52.25}$ encryptions. We denote the exhaustive search complexity as T_{es}. Thus the total time complexity is about $2^{52.25} + 2^{40.6} = 2^{52.25}$ encryptions.

Since the expected count of the right key is $\lambda_r = 3.7$, the probability that the right key count is greater than or equal to 4 is

$$1 - \Pr[\xi_r = 0] - \Pr[\xi_r = 1] - \Pr[\xi_r = 2] - \Pr[\xi_r = 3] = 0.51.$$

Therefore, our attacks on 21-round SIMON32/64 needs $2^{52.25}$ encryptions with 2^{31} chosen plaintexts, and the success probability is about 51%.

Experimental Data for the Attack on 18-round SIMON32 In order to verify the correctness of our attack, we give a key recovery experimental test on 18-round SIMON32/64. We consider the following 13-round differential with probability $2^{-28.11}$.

$$D : (2000, 8000) \rightarrow (2000, 0000).$$

After prefixing 2 rounds on the top and appending 3 rounds at the bottom, we extend the 13-round differential to 18 rounds. There are totally 11 bits of subkey involved in conditions of differential path. By using above method to evaluate complexity with 2^{31} chosen plaintexts, we have tested that, there are about $2^7 \times (1 - \frac{1}{4})^2 \times (1 - \frac{1}{8}) \approx 2^6$ pairs left after data collection and filtering, and there are about 2^9 values of subkeys. We perform 100 experimental test for different masterkeys, 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 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 7 in Appendix).

There are 11 conditions on plaintexts and 16 conditions without subkey bits in rounds 1-2 (see Table 4). We divide the plaintexts into 2^{27} sets indexed by these 27 bits. Each set is a structure with $2^{48-27} = 2^{21}$ plaintexts. For structure A and A' with different bits ($X_0[42]$, $X_0[46]$, $X_1[28]$, $X_1[44]$, $X_2[40]$), query the corresponding ciphertexts, and inset a table indexed by $X_{23}[t]$, where $\Delta X_{23}[t] = 0$. There are about $2^{21\times 2-9} = 2^{33}$ pairs between A and A' remained. 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. In data collection, we need about $2^{26+21} = 2^{47}$ encryptions for the chosen plaintexts, and about 2^{59} one round computations to decide the conditions equivalent to 2^{55} encryptions. We get $2^{26-1+42-21} = 2^{46}$ pairs satisfying the input difference of the differential. Hence, there are about $2^{46-44.65} = 2.6$ right pairs. It means the expected count of the right key is $\lambda_r = 2.6$.

Table 4: Conditions of Differential of 23-round SIMON48 are Independent of Subkeys

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

By 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 with 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 is computed by equation (4) equals to $2^{64} \times 2^{42} \times 2^{-44}/(16 \times 23) = 2^{53.48}$ encryptions. By equation (5), 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. Therefore, 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 attacks 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 36 bit conditions independent of the secret key and $n_c = 60$ bit conditions relating to $|sk| = 88$ the secret key.

According to 11 conditions without any key bit in the input difference of plaintexts and the first two rounds, we divide the plaintexts into 2^{11} sets. Each set is a structure with $2^{48-11} = 2^{37}$ plaintexts. We build 2^{10} structure, and filter out the chosen pairs according to the conditions independent of secret key, there are $N = 2^{10-1+37\times2-25} = 2^{58}$ pairs left. In data collection, we need about $2^{10+37} = 2^{47}$ encryptions for the chosen plaintexts, and about $2^{10+37\times2-9} = 2^{75}$ one round computations to decide the conditions equivalent to 2^{71} encryptions. We get $2^{10-1+74-37} = 2^{46}$ pairs satisfying the input difference 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 the dynamic key-guessing method to compute the subkey candidates which lead to the input and output differences of the differential D for a pair, and update the corresponding subkey counter. The time

complexity is computed by equation (4) equals to $2^{88} \times 2^{58} \times 2^{-60}/(16 \times 24) = 2^{77.4}$ 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 still 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

In this section, we give a brief description of the differential attacks on SIMON64/96/128 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 without secret key, and 34 conditions relating to 68 bit equivalent subkeys (see Table 9 in Appendix).

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 53 conditions related to 99 bit equivalent subkeys (see Table 10 in Appendix).

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 11 in Appendix). There are 49 conditions on plaintexts, 22 conditions in the first two rounds without secret key. For the 101-bit subkey from the 52 sufficient conditions, we show that the 101-bit subkey can be computed from a 88-bit subkey for SIMON96/96.

Attack on SIMON128 Versions From 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 12 in Appendix). There are 69 conditions on plaintexts, and 20 conditions in the first round without secret key bits. We decide a 158-bit subkey involved in the 78 sufficient conditions. By key schedules, we know that these 158 bits are linearly independent for SIMON128/192 but linearly dependent for SIMON128/128, further we show that these 158-bits of subkey can be computed from 122 bit subkeys for SIMON128/128.

We prefix one round on the top of the 49-round attack to launch the 50-round attack on SIMON128/256 (see Table 13 in Appendix). We have 69 conditions on plaintexts, and 20 conditions in the first round without secret key bits. For the 219-bit subkey from the 98 sufficient conditions.

We choose plaintexts to construct structures with 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 (4). 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 $T_{es} + T_{csc}$	Success Rate
SIMON64/96	28	68	2^{-2}	3.46	4	2^{63}	$2^{84.25} + 2^{59.19}$	0.67
SIMON64/128	29	99	2^{-2}	3.46	4	2^{63}	$2^{119.25} + 2^{90.19}$	0.67
SIMON96/96	37	88	2^{-2}	3.48	4	2^{95}	$2^{87.25} + 2^{77.09}$	0.68
SIMON96/144	37	101	2^{-2}	3.48	4	2^{95}	$2^{135.25} + 2^{90.9}$	0.68
SIMON128/128	49	122	2^{-2}	2.6	3	2^{127}	$2^{119.25} + 2^{110.39}$	0.48
SIMON128/192	49	158	2^{-2}	2.6	3	2^{127}	$2^{183.25} + 2^{146.39}$	0.48
SIMON128/256	50	219	2^{-2}	2.6	3	2^{127}	$2^{247.25} + 2^{207.36}$	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 Suffiicient Conditions of Extended Differential Paths for SIMON

Table 6: Solutions of Subkey Bits Corresponding to Differential Path of 21-round SIMON32

Rounds (Number of Conditions)	Bit Conditions	Solutions of Key Bits to Equations	Conditions Leading to Solutions	P_r	P_r^F
2(10)	$\Delta X_2[16]=0$	Discard the pair	$\Delta X_1[17]=0$ and $\Delta X_0[16]=1$		1/4
		$K_0[8]=0,1$	$\Delta X_1[17]=0$ and $\Delta X_0[16]=0$	1/4	
		$K_0[8]$	$\Delta X_1[17]=1$	1/2	
	$\Delta X_2[18]=1$	Discard the pair	$\Delta X_1[26]=0$ and $\Delta X_0[18]=0$		1/4
		$K_0[3]=0,1$	$\Delta X_1[26]=0$ and $\Delta X_0[18]=1$	1/4	
		$K_0[3]$	$\Delta X_1[26]=1$	1/2	
	$\Delta X_2[22]=0$	Discard the pair	$\Delta X_1[23]=0$ and $\Delta X_1[30]=0$ and $\Delta X_0[22]=1$		1/8
		$K_0[7]=0,1$, $K_0[14]=0,1$	$\Delta X_1[23]=0$ and $\Delta X_1[30]=0$ and $\Delta X_0[22]=0$	1/8	
		$K_0[7]$, $K_0[14]=0,1$	$\Delta X_1[23]=0$ and $\Delta X_1[30]=1$	1/4	
		$K_0[14]$, $K_0[7]=0,1$	$\Delta X_1[23]=1$ and $\Delta X_1[30]=0$	1/4	
		$K_0[7]\oplus K_0[14]$, $K_0[7]=0,1$	$\Delta X_1[23]=1$ and $\Delta X_1[30]=1$	1/4	
	$\Delta X_2[21]=0$	Discard the pair	$\Delta X_1[22]=0$ and $\Delta X_1[29]=0$ and $\Delta X_1[23]\oplus\Delta X_0[21]=1$		1/8
		$K_0[6]=0,1$, $K_0[13]=0,1$	$\Delta X_1[22]=0$ and $\Delta X_1[29]=1$ and $\Delta X_1[23]\oplus\Delta X_0[21]=0$	1/4	
		$K_0[6]$, $K_0[13]=0,1$	$\Delta X_1[22]=0$ and $\Delta X_1[29]=1$	1/4	
		$K_0[13]$,$K_0[6]=0,1$	$\Delta X_1[22]=1$ and $\Delta X_1[29]=0$	1/4	
		$K_0[6]\oplus K_0[13]$, $K_0[6]=0,1$	$\Delta X_1[22]=1$ and $\Delta X_1[29]=1$	1/4	
	$\Delta X_2[27]=0$	$K_0[3]$	contradiction to above $K_0[3]$		1/2(*)
		$K_0[3]$		1/2	
	$\Delta X_2[29]=0$	Discard the pair	$\Delta X_1[30]=0$ and $\Delta X_0[29]=1$		1/4
		$K_0[5]=0,1$	$\Delta X_1[30]=0$ and $\Delta X_0[29]=0$	1/4	
		$K_0[5]$	$\Delta X_1[30]=1$	1/2	
	$\Delta X_2[20]=0$	No solution	contradiction to above $K_0[5]$		1/2(*)
		$K_0[5]$		1/2	
	$\Delta X_2[30]=1$	Discard the pair	$\Delta X_1[22]=0$ and $\Delta X_1[16]\oplus\Delta X_0[30]=0$		1/4
		$K_0[15]=0,1$	$\Delta X_1[22]=0$ and $\Delta X_1[16]\oplus\Delta X_0[30]=1$	1/4	
		$K_0[15]$	$\Delta X_1[22]=1$	1/2	
	$\Delta X_2[28]=0$	Discard the pair	$\Delta X_1[29]=0$ and $\Delta X_1[30]\oplus\Delta X_0[28]=1$		1/4
		$K_0[4]=0,1$	$\Delta X_1[29]=0$ and $\Delta X_1[30]\oplus\Delta X_0[28]=0$	1/4	

		$K_0[4]$	$\Delta X_1[29] = 1$	1/2	
	$\Delta X_2[25] = 0$	Discard the pair	$\Delta X_1[26] = 0$ and $\Delta X_1[17] = 0$ and $\Delta X_0[25] = 1$		1/8
		$K_0[10] = 0, 1$, $K_0[1] = 0, 1$	$\Delta X_1[26] = 0$ and $\Delta X_1[17] = 0$ and $\Delta X_0[25] = 1$	1/8	
		$K_0[10]$, $K_0[1] = 0, 1$	$\Delta X_1[26] = 0$ and $\Delta X_1[17] = 1$	1/4	
		$K_0[1]$, $K_0[10] = 0, 1$	$\Delta X_1[26] = 1$ and $\Delta X_1[17] = 0$	1/4	
		$K_0[10] \oplus K_0[1]$, $K_0[10] = 0, 1$	$\Delta X_1[26] = 1$ and $\Delta X_1[17] = 1$	1/4	
3(7)	$\Delta X_3[17] = 0$	$K_0[11] \oplus K_1[9]$		1	
	$\Delta X_3[23] = 0$(guess $K_0[9]$,$K_0[0]$)	No solution	$\Delta X_2[24] = 0$ and $\Delta X_2[31] = 0$ and $\Delta X_1[23] = 1$		1/8(*)
		$K_1[8] = 0, 1$, $K_1[15] = 0, 1$	$\Delta X_2[24] = 0$ and $\Delta X_2[31] = 0$ and $\Delta X_1[23] = 0$	1/8	
		$K_1[8]$, $K_1[15] = 0, 1$	$\Delta X_2[24] = 0$ and $\Delta X_2[31] = 1$	1/4	
		$K_1[15]$, $K_1[8] = 0, 1$	$\Delta X_2[24] = 1$ and $\Delta X_2[31] = 0$	1/4	
		$K_1[8] \oplus K_1[15]$, $K_1[8] = 0, 1$	$\Delta X_2[24] = 1$ and $\Delta X_2[31] = 1$	1/4	
	$\Delta X_3[22] = 0$	$K_1[7]$		1	
	$\Delta X_3[29] = 0$	$K_1[5]$		1	
	$\Delta X_3[30] = 0$	No solution	$\Delta X_2[31] = 0$ and $\Delta X_1[29] = 1$		1/4(*)
		$K_1[6] = 0, 1$	$\Delta X_2[31] = 0$ and $\Delta X_1[29] = 0$	1/4	
		$K_1[6]$	$\Delta X_2[31] = 1$	1/2	
	$\Delta X_3[26] = 0$	$K_1[11]$, $K_0[12] = 0, 1$	$X_1[19] = 0$	1/2	
		$K_1[11] \oplus K_0[12]$, $K_1[11] = 0, 1$	$X_1[19] = 1$	1/2	
	$\Delta X_3[16] = 1$	No solution	$\Delta X_2[24] = 0$ and $\Delta X_1[16] = 1$		1/4(*)
		$K_1[1] = 0, 1$, $K_0[2] = 0, 1$	$\Delta X_2[24] = 0$ and $\Delta X_1[16] = 0$	1/4	
		$K_1[1]$, $K_0[2] = 0, 1$	$\Delta X_2[24] = 1$ and $X_1[25] = 0$	1/4	
		$K_1[1] \oplus K_0[2]$, $K_0[2] = 0, 1$	$\Delta X_2[24] = 1$ and $X_1[25] = 1$	1/4	
4(2)	$\Delta X_4[31] = 0$	$K_2[7]$		1	
	$\Delta X_4[24] = 0$	$K_2[9]$, $K_1[10] = 0, 1$, $K_0[11] = 0, 1$	$X_2[17] = 0$	1/2	
		$K_2[9] \oplus K_1[10]$, $K_1[10] = 0, 1$, $K_0[11] = 0, 1$	$X_2[17] = 1$ and $X_1[18] = 0$	1/4	
		$K_2[9] \oplus K_1[10] \oplus K_0[11]$, $K_1[10] = 0, 1$, $K_0[11] = 0, 1$	$X_2[17] = 1$ and $X_1[18] = 1$	1/4	
19(7)	$\Delta X_{19}[15] = 0$	Discard the pair	$\Delta X_{20}[0] = 0$ and $\Delta X_{21}[15] = 1$		1/4
		$K_{20}[7] = 0, 1$	$\Delta X_{20}[0] = 0$ and $\Delta X_{21}[15] = 0$	1/4	
		$K_{20}[7]$	$\Delta X_{20}[0] = 1$	1/2	
	$\Delta X_{19}[6] = 0$	Discard key $K_{20}[7]$	contradiction to above $K_{20}[7]$		1/2(*)
	$\Delta X_{19}[0] = 1$	Discard the pair	$\Delta X_{20}[8] = 0$ and $\Delta X_{20}[2] \oplus \Delta X_{21}[0] = 0$		1/4
		$K_{20}[1]$=0,1	$\Delta X_{20}[8] = 0$ and $\Delta X_{20}[2] \oplus \Delta X_{21}[0] = 1$	1/4	
		$K_{20}[1]$	$\Delta X_{20}[8] = 1$	1/2	
	$\Delta X_{19}[13] = 0$	$K_{20}[5]$		1	
	$\Delta X_{19}[14] = 0$	Discard the pair	$\Delta X_{20}[15] = 0$ and $\Delta X_{20}[0] \oplus \Delta X_{21}[14] = 1$		1/4
		$K_{20}[6] = 0, 1$	$\Delta X_{20}[15] = 0$ and $\Delta X_{20}[0] \oplus \Delta X_{21}[14] = 0$	1/4	
		$K_{20}[6]$	$\Delta X_{20}[15] = 1$	1/2	
	$\Delta X_{19}[7] = 0$	Discard the pair	$\Delta X_{20}[15] = 0$ and $\Delta X_{20}[8] = 0$ and $\Delta X_{20}[9] \oplus \Delta X_{21}[7] = 1$		1/8
		$K_{20}[8] = 0, 1$, $K_{20}[15] = 0, 1$	$\Delta X_{20}[15] = 0$ and $\Delta X_{20}[8] = 0$ and $\Delta X_{20}[9] \oplus \Delta X_{21}[7] = 0$	1/8	
		$K_{20}[8]$, $K_{20}[15] = 0, 1$	$\Delta X_{20}[15] = 1$ and $\Delta X_{20}[8] = 0$	1/4	
		$K_{20}[15]$, $K_{20}[8] = 0, 1$	$\Delta X_{20}[15] = 0$ and $\Delta X_{20}[8] = 1$	1/4	
		$K_{20}[8] \oplus K_{20}[15]$, $K_{20}[8] = 0, 1$	$\Delta X_{20}[15] = 1$ and $\Delta X_{20}[8] = 1$	1/4	
	$\Delta X_{19}[8] = 0$	Discard the pair	$\Delta X_{20}[0] = 0$ and $\Delta X_{20}[9] = 0$ and $\Delta X_{21}[8] = 1$		1/8
		$K_{20}[9] = 0, 1$, $K_{20}[0] = 0, 1$	$\Delta X_{20}[0] = 0$ and $\Delta X_{20}[9] = 0$ and $\Delta X_{21}[8] = 0$	1/8	
		$K_{20}[9]$, $K_{20}[0] = 0, 1$	$\Delta X_{20}[0] = 1$ and $\Delta X_{20}[9] = 0$	1/4	
		$K_{20}[0]$, $K_{20}[9] = 0, 1$	$\Delta X_{20}[0] = 0$ and $\Delta X_{20}[9] = 1$	1/4	
		$K_{20}[0] \oplus K_{20}[9]$, $K_{20}[9] = 0, 1$	$\Delta X_{20}[0] = 1$ and $\Delta X_{20}[0] = 1$	1/4	
18(5)	$\Delta X_{18}[2] = 1$(guess $K_{20}[11]$)	No solution	$\Delta X_{19}[10] = 0$ and $\Delta X_{20}[2] = 0$		1/4(*)
		$K_{19}[3] = 0, 1$, $K_{20}[4] = 0, 1$	$\Delta X_{19}[10] = 0$ and $\Delta X_{20}[2] = 1$	1/4	
		$K_{19}[3]$, $K_{20}[4] = 0, 1$	$\Delta X_{19}[10] = 1$ and $X_{20}[11] = 0$	1/4	
		$K_{19}[3] \oplus K_{20}[4]$, $K_{20}[4] = 0, 1$	$\Delta X_{19}[10] = 1$ and $X_{20}[11] = 1$	1/4	

	$\Delta X_{18}[8] = 0$	$K_{19}[9]$, $K_{20}[10] = 0, 1$	$X_{20}[1] = 0$	1/2	
		$K_{19}[9] \oplus K_{20}[10]$, $K_{20}[10] = 0, 1$	$X_{20}[1] = 1$	1/2	
	$\Delta X_{18}[0] = 0$(guess $K_{20}[2]$)	No solution	$\Delta X_{19}[1] = 0$ and $\Delta X_{20}[0] = 1$		1/4(*)
		$K_{19}[8] = 0, 1$	$\Delta X_{19}[1] = 0$ and $\Delta X_{20}[0] = 0$	1/4	
		$K_{19}[8]$	$\Delta X_{19}[1] = 1$	1/2	
	$\Delta X_{18}[9] = 0$	No solution	$\Delta X_{19}[1] = 0$ and $\Delta X_{19}[10] = 0$ and $\Delta X_{20}[9] = 1$		1/8(*)
		$K_{19}[1] \oplus K_{20}[3] = 0, 1$, $K_{20}[12] \oplus K_{19}[10] = 0, 1$	$\Delta X_{19}[1] = 0$ and $\Delta X_{19}[10] = 1$ and $\Delta X_{20}[9] = 1$	1/8	
		$K_{19}[1] \oplus K_{20}[3]$, $K_{20}[12] \oplus K_{19}[10] = 0, 1$	$\Delta X_{19}[1] = 0$ and $\Delta X_{19}[10] = 1$	1/4	
		$K_{20}[12] \oplus K_{19}[10]$, $K_{19}[1] \oplus K_{20}[3] = 0, 1$	$\Delta X_{19}[1] = 1$ and $\Delta X_{19}[10] = 0$	1/4	
		$K_{19}[1] \oplus K_{20}[3] \oplus K_{20}[12] \oplus K_{19}[10]$, $K_{19}[1] \oplus K_{20}[3] = 0, 1$	$\Delta X_{19}[1] = 1$ and $\Delta X_{19}[10] = 1$	1/4	
	$\Delta X_{18}[15] = 0$	$K_{19}[7]$		1	
17(2)	$\Delta X_{17}[10] = 0$	$K_{18}[11] \oplus K_{19}[13]$	guess $K_{20}[14]$,$K_{20}[13]$,$K_{19}[12]$	1	
	$\Delta X_{17}[1] = 0$	$K_{18}[9] \oplus K_{19}[11]$	guess $K_{20}[3]$,$K_{20}[12]$	1	

Table 7: Sufficient Conditions of Differential Path of 23-round SIMON48

Rounds	Input Differences of Each Round
0	*,0,0,*,*,0,*,*,0,0,*,0,*,*,*,0,*,*,1,*,*,*,1,*,0,*,*,*,*,*,*,0,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*
1	0,*,**0,0,1**,*,**0,0,*,**0,0,0,0,0,0**,*,*,**0,0,*,**0,0,1**,*,*,**0,*,0,0,*,*,0,*,*,0,0,*,0,*,*,*,0,*,*,1,*,*,*,1,*
2	0,*,**0,0,1**,*,**0,0,*,**0,0,0,0,0,0**,*,*,**0,0,*,**0,0,1**,*,*,**0,*,0,0,*,*,0,*,*,0,0,*,0,*,*,*,0,*,*,1,*,*,*,1,*
3	1,**0**,0,0,0,**0**,0,0,**0**,0,0,0,0,0,0,**0,0**,0,0,**0**,0,0,**0,0**,0,0,0,1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0
3 → 19	16-round differential D
19	1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,0,0,0,**0**
20	0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,*,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**,0,0,0,**0,0**,0
21	0,*,0,0,1,*,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**,**0**,0,*,**0**,0,**0,0**,**0**,1,*
22	*,0,0,*,*,0,*,*,0,0,*,0,*,*,*,0,*,*,1,*,*,*,1,*,0,*,**0,0,1**,*,**0**,0,*,**0,0,0,0,0,0**,*,*,**0,0**,*,**0,1**,*,*,**0**
23	0,*,*,*,*,*,*,0,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,0,0,0,*,*,0,*,*,0,0,*,0,*,*,*,0,*,*,1,*,*,*,1,*

Table 8: Sufficient Conditions of Extended Differential Path of 24-round SIMON48

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

Table 9: Sufficient Conditions of Extended Differential Path of 28-round SIMON64

Rounds	Input Differences of Each Round
0(left)	*,*,*,0,*,*,1,*,*,*,1,*,*,0,0,*,*,0,1,0,0,0,0,0,0,0,*,0,0,0,*,0
0(right)	*,*,*,*,*,*,*,*,*,*,*,0,*,*,*,0,*,*,0,0,0,*,0,*,*,*,0,*,*,*,*
1(left)	**0,0,***,**0,0,0,***,**0,1,***,**0**,0,*,**0,0**,1,*,**0**,0,0,0,**0,0**,0,**0,0,0**,0,**0,0,0,0**
1(right)	*,*,*,0,*,*,1,*,*,*,1,*,*,0,0,*,*,0,1,0,0,0,0,0,0,0,*,0,0,0,*,0
2(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
2(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
3(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
3(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

3 → 24	21-round differential D
24(left)	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
24(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
25(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
25(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
26(left)	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
26(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
27(left)	*,*,0,0,0,0,*,*,*,0,*,0,1,*,*,*,0,*,0,0,0,0,0,0,0,0,*,0,0,0,0,0
27(right)	**0**,0,*,0,**0**,**0**,**0**,**0**,*,*,0,**0**,**0**,**0**,**1**,*,*,0,**1**,0,0,0,0,0,**0**,**0**,0,0,0,0,**0**,**0**
28(left)	*,0,*,0,*,*,*,*,*,*,1,*,*,*,*,*,*,0,*,0,0,0,0,0,*,*,0,0,0,0,*,*
28(right)	*,*,0,0,0,0,*,*,*,0,*,0,1,*,*,*,0,*,0,0,0,0,0,0,0,0,*,0,0,0,0,0

Table 10: Sufficient Conditions of Extended Differential Path of 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)	0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0
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,*,*,0,0,0,0,1,*,*,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0
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 11: Sufficient Conditions of Extended Differential Path of 37-round SIMON96

Rounds	Input Differences of Each Round
0(left)	0,0,*,*,*,*,*,0,*,*,1,*,*,*,0,*,*,0,1,*,*,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,0,0,0,*,*,*,0
0(right)	*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,0,*,*,*,1,*,0,0,0,0,0,0,0,0,*,0,0,0,0,0,*,*,*,0,0,0,*,*,*,*,*,0
1(left)	**0**,**0**,**0**,**0**,**1**,*,*,**0**,**0**,**0**,*,**0**,**1**,*,*,**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
1(right)	0,0,*,*,*,*,*,0,*,*,1,*,*,*,0,*,*,0,1,*,*,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,0,0,0,*,*,*,0
2(left)	0,0,**0**,**0**,**0**,**0**,**1**,0,**0**,**0**,0,**0**,**0**,**0**,1,**0**,**0**,0,1,**0**,**0**,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,0,**0**,**0**,**0**,0
2(right)	0,0,0,0,1,*,*,0,0,0,*,0,1,*,*,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
3(left)	0,0,0,0,0,**0**,**0**,0,0,0,**0**,0,0,**0**,**0**,0,0,**0**,0,0,1,**0**,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0
3(right)	0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
3 → 33	30-round differential D
33(left)	0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
33(right)	**0**,0,0,0,0,0,1,**0**,**0**,0,1,0,0,0,1,**0**,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
34(left)	*,0,0,0,0,0,0,0,*,*,0,1,0,0,0,0,0,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
34(right)	**0**,0,**0**,0,0,**0**,**0**,**0**,1,**0**,0,0,0,0,**0**,**0**,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,0,0,0,**0**,**0**
35(left)	*,0,*,0,0,*,*,*,0,*,0,0,0,*,*,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,0,0,0,*,*
35(right)	*,**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**,0,0,0,0,0,0,**0**,**0**,**0**,0,**0**,0,**0**,**0**,**0**,**0**,
36(left)	*,*,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,*,*,*,*
36(right)	*,**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,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,**0**,**0**,*,*,
37(left)	*,*,*,*,*,*,*,*,1,*,*,*,*,*,*,0,1,0,0,0,0,0,0,0,*,0,0,0,0,0,0,*,*,*,0,*,0,*,*,*,*,*,*,*,*,*,*,*
37(right)	*,*,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,*,*,*,*

Table 12: Sufficient Conditions of Extended Differential Path of 49-round SIMON128

Rounds	Input Differences of Each Round
0(L)	*,*,*,*,*,*,*,*,0,*,*,*,1,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*
0(R)	*,*,*,*,*,*,*,*,*,*,*,*,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,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*
1(L)	*,*,**1**,*,*,*,**0**,*,*,**0**,**1**,*,*,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**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,*,*,*,**0**,*
1(R)	*,*,*,*,*,*,*,0,*,*,*,1,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*
2(L)	**0**,**0**,*,**0**,**1**,*,*,**0**,1,*,**0**,**0**,0,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,*
2(R)	*,1,*,*,*,0,*,*,0,1,*,*,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0
3(L)	**0**,**0**,0,**0**,**0**,**0**,1,**0**,**0**,0,1,**0**,**0**,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,0
3(R)	0,*,0,1,*,*,0,1,*,0,0,0,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0
4(L)	0,0,**0**,0,0,**0**,**0**,0,0,**0**,0,0,1,**0**,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0
4(R)	0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
$4 \rightarrow 45$	41-round differential D
45(L)	0,0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
45(R)	0,0,**0**,0,0,**0**,**0**,0,0,**0**,0,0,1,**0**,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,
46(L)	0,0,*,0,1,*,*,0,1,*,0,0,0,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0
46(R)	**0**,**0**,0,**0**,**0**,**0**,1,**0**,**0**,0,1,**0**,**0**,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,
47(L)	*,*,1,*,*,*,0,*,*,0,1,*,*,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0
47(R)	**0**,**0**,*,**0**,**1**,*,*,**0**,1,*,**0**,**0**,0,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,
48(leLft)	*,*,*,*,*,*,*,*,0,*,*,*,1,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*
48(R)	*,*,**1**,*,*,*,**0**,*,*,**0**,**1**,*,*,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**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,*,*,*,**0**,
49(L)	*,*,*,*,*,*,*,*,*,*,*,*,*,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,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*
49(R)	*,*,*,*,*,*,*,*,0,*,*,*,1,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*

Table 13: Sufficient Conditions of Extended Differential Path of 50-round SIMON128

Rounds	Input Differences of Each Round
0(L)	*,*,*,*,*,*,*,*,0,*,*,*,1,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*
0(R)	*,*,*,*,*,*,*,*,*,*,*,*,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,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*
1(L)	*,*,**1**,*,*,*,**0**,*,*,**0**,**1**,*,*,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**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,*,*,*,**0**,*
1(R)	*,*,*,*,*,*,*,0,*,*,*,1,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*
2(L)	**0**,**0**,*,**0**,**1**,*,*,**0**,1,*,**0**,**0**,0,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,*
2(R)	*,1,*,*,*,0,*,*,0,1,*,*,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0
3(L)	**0**,**0**,0,**0**,**0**,**0**,1,**0**,**0**,0,1,**0**,**0**,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,0
3(R)	0,*,0,1,*,*,0,1,*,0,0,0,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0
4(L)	0,0,**0**,0,0,**0**,**0**,0,0,**0**,0,0,1,**0**,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0
4(R)	0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
$4 \rightarrow 45$	41-round differential D
45(L)	0,0,0,0,0,0,1,0,0,0,1,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
45(R)	0,0,**0**,0,0,**0**,**0**,0,0,**0**,0,0,1,**0**,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,
46(L)	0,0,*,0,1,*,*,0,1,*,0,0,0,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0
46(R)	**0**,**0**,0,**0**,**0**,**0**,1,**0**,**0**,0,1,**0**,**0**,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,
47(L)	*,*,1,*,*,*,0,*,*,0,1,*,*,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0
47(R)	**0**,**0**,*,**0**,**1**,*,*,**0**,1,*,**0**,**0**,0,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,**0**,0,0,0,**0**,0,**0**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,
48(L)	*,*,*,*,*,*,*,*,0,*,*,*,1,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*,*,*,*,*,*,*,*
48(R)	*,*,**1**,*,*,*,**0**,*,*,**0**,**1**,*,*,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**,**0**,**0**,0,**0**,**0**,**0**,**0**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,*,*,*,**0**,
49(L)	*,*,*,*,*,*,*,*,*,*,*,*,*,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,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*
49(R)	*,*,*,*,*,*,*,*,**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**,**0**,**0**,*,**0**,**0**,**0**,*,**0**,*,*,*,**0**,*,*,*,*,*,*,*,*,
50(L)	*,*,*,*,*,*,*,*,*,*,*,*,0,*,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,*,0,0,0,*,0,*,*,*,0,*
50(R)	*,*,*,*,*,*,*,*,*,*,*,*,*,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,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*