Improved Zero-Correlation Cryptanalysis on SIMON

Ling Sun[1], Kai Fu[1], and Meiqin Wang[1,2](✉)

[1] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, Jinan 250100, China
{lingsun,fukai6}@mail.sdu.edu.cn

[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
mqwang@sdu.edu.cn

Abstract. SIMON is a family of lightweight block ciphers publicly released by the NSA. Up to now, there have been many cryptanalytic results on it by means of differential, linear, impossible differential, integral, zero-correlation linear cryptanalysis and so forth. At INDOCRYPT 2014, Wang *et al.* gave zero-correlation attacks for 20-round SIMON32, 20-round SIMON48/72 and 21-round SIMON48/96. We investigate the security of whole family of SIMON by using zero-correlation linear cryptanalysis in this paper. For SIMON32 and SIMON48, we can attack one more round than the previous zero-correlation attacks given by Wang *et al.* We are the first one to give zero-correlation linear approximations of SIMON64, SIMON96 and SIMON128. These approximations are also utilized to attack the corresponding ciphers.

Keywords: SIMON · Zero-correlation linear approximation · Cryptanalysis

1 Introduction

Lightweight primitives aim at finding an optimal compromise between efficiency, security and hardware performance. Lightweight ciphers have been used in many fields, such as RFID tags, smartcards, and FPGAs. The impact of lightweight cipher is likely to continue increasing in the future. In recent years, many lightweight ciphers have been developed, including KATAN [10], KLEIN [11], LED [12], Piccolo [15], PRESENT [8] and TWINE [17].

SIMON [6] is a family of lightweight block ciphers publicly released by the National Security Agency (NSA) in June 2013. NSA has developed three ciphers to date, including SIMON, SPECK and Skipjack. SIMON has been optimized for performance in hardware implementations, while its sister algorithm, SPECK [6], has been optimized for software implementations. SIMON and SPECK offer users a variety of block sizes and key sizes for different implementations.

Many cryptanalytic results have been published on SIMON. The first differential cryptanalysis on SIMON was presented by Abed *et al.* in [1].

D. Lin et al. (Eds.): Inscrypt 2015, LNCS 9589, pp. 125–143, 2016.
DOI: 10.1007/978-3-319-38898-4_8

Then, Biryukov *et al.* improved the differential cryptanalysis of SIMON32, SIMON48 and SIMON64 by searching better differential characteristics in [7]. Based on the differential distinguisher shown by Biryukov *et al.*, Wang *et al.* improved the key recovery attacks on SIMON32, SIMON48 and SIMON64 [18]. In [18], Wang *et al.* gave the attack on 21-round SIMON32, which is still the best attack up to now. In addition, Sun *et al.* identified better differential distinguisher for SIMON with MILP models in [16]. Impossible differential attack against SIMON was firstly presented in [2], then the improved impossible differential attacks on SIMON32 and SIMON48 were given in [19], which had been further improved by Boura *et al.* in [9].

For the integral attack, Wang *et al.* proposed the attack on 21-round SIMON32 in [19] based on a zero-sum integral distinguisher for 15-round SIMON32, which was obtained experimentally.

Zero-correlation linear attack is one of the recent cryptanalytic methods introduced by Bogdanov and Rijmen in [3]. This kind of attack is based on the linear approximation with correlation zero (*i.e.* the linear approximation with probability exactly $\frac{1}{2}$). The idea of multiple zero-correlation cryptanalysis was developed in recent years in [4] by Bogdanov and Wang. They proposed a new distinguisher by using the fact that there are numerous zero-correlation approximations in susceptible ciphers. In [5], a more powerful distinguisher called multidimensional zero-correlation distinguisher was introduced. Wang *et al.* also gave the zero correlation linear approximations for SIMON32 and SIMON48 in [19]. They employed these approximations to attack 20-round SIMON32, 20-round SIMON48/72 and 21-round SIMON48/96.

In this paper, we investigate the security of whole family of SIMON by using zero-correlation linear cryptanalysis. For SIMON32 and SIMON48, by using the technique of equivalent-key, our cryptanalysis can attack one more round than the previous zero-correlation attacks in [19]. We are the first ones to give zero-correlation linear approximations of SIMON64, SIMON96 and SIMON128. These approximations are also utilized to attack the corresponding ciphers.

Our Contributions. In this paper, we investigate the security of whole family of SIMON by using zero-correlation linear cryptanalysis. Our contributions can be summarized as follows:

- Based on the 11-round zero-correlation distinguisher for SIMON32 and 12-round zero-correlation distinguisher for SIMON48, we use the equivalent-key technique (*i.e.* by moving the subkey into the left-side of round function) to improve the key recovery attack on SIMON32 and SIMON48. Finally, we can attack 21-round SIMON32, 21-round SIMON48/72 and 22-round SIMON48/96. The equivalent-key technique has been widely used in various key-recovery attacks. This technique aims at reducing the number of guessed subkey by using equivalent subkeys to replace the original subkeys used in the cipher. This technique had been used in [13] by Isobe. But there exists a little difference. Because the subkey is XORed after non-linear function, the condition in [13] that some parts of plaintext should be fixed can be canceled.

– We provide 13-, 16- and 19- round zero-correlation linear approximations of SIMON64, SIMON96 and SIMON128, respectively. We also use them to analysis the security of the corresponding ciphers. We are the first one to give the zero-correlation linear cryptanalysis for SIMON64, SIMON96 and SIMON128.

Our results along with the previous zero-correlation attacks on SIMON32 and SIMON48 are listed in Table 1.

Table 1. Summary of zero-correlation attacks on SIMON

Cipher	Rounds	Time (ENs)	Data (KPs)	Memory (Bytes)	Ref.
SIMON32	20	$2^{59.9}$	2^{32}	$2^{41.4}$	[19]
SIMON32	**21**	$2^{59.4}$	2^{32}	$2^{31.0}$	**Sect.** 4.1
SIMON48/72	20	$2^{59.7}$	2^{48}	$2^{43.0}$	[19]
SIMON48/72	**21**	$2^{61.9}$	2^{48}	$2^{43.0}$	**Sect.** 4.2
SIMON48/96	21	$2^{72.6}$	2^{48}	$2^{46.7}$	[19]
SIMON48/96	**22**	$2^{80.5}$	2^{48}	$2^{43.0}$	**Sect.** 4.2
SIMON64/96	**23**	$2^{90.4}$	2^{64}	$2^{54.0}$	**Sect.** 4.3
SIMON64/128	**24**	$2^{116.8}$	2^{64}	$2^{54.0}$	**Sect.** 4.3
SIMON96/144	**28**	$2^{141.0}$	2^{96}	$2^{85.0}$	**Sect.** 4.3
SIMON128/192	**32**	$2^{156.8}$	2^{128}	$2^{117.0}$	**Sect.** 4.3
SIMON128/256	**34**	$2^{255.6}$	2^{128}	$2^{117.0}$	**Sect.** 4.3

KP: Known Plaintext; EN: Encryption.

Outline. The remainder of this paper is organized as follows. Section 2 gives a brief description of SIMON and a general introduction of zero-correlation linear cryptanalysis. Section 3 presents the zero-correlation linear distinguishers used in the following attacks. Section 4 covers the zero-correlation attacks on the whole family of SIMON. Finally, we conclude the paper in Sect. 5.

2 Preliminaries

2.1 Brief Description of SIMON

SIMON [6] is a family of lightweight block ciphers publicly released by the National Security Agency (NSA) in June 2013. SIMON offers users a variety of block sizes and key sizes for different implementations. Table 2 lists the different block and key sizes, in bits, for SIMON.

SIMON is a two-branch balanced Feistel network which consists of three operations: AND (&), XOR ($\oplus$) and rotation ($\lll$). We denote the input of the i-th round by $(L_i, R_i), i = 0, 1, \ldots, r-1$. In round i, (L_i, R_i) is updated to (L_{i+1}, R_{i+1}) by using a function $F(x) = (x \lll 1) \,\&\, (x \lll 8) \oplus (x \lll 2)$ as follows:

Table 2. SIMON parameters

Block size	Key size
32	64
48	72, 96
64	96, 128
96	96, 144
128	128, 192, 256

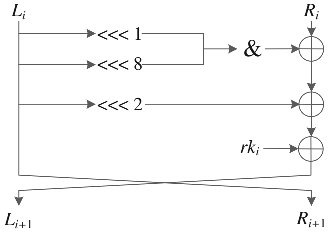


Fig. 1. Round function of SIMON

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

The output of the last round (L_r, R_r) is the ciphertext. An illustration of the round function is depicted in Fig. 1.

The key schedule of SIMON uses an LFSR-like procedure to generate r subkeys $rk_0, rk_1, \ldots, rk_{r-1}$. SIMON processes three slightly different key schedule procedures, depending on the number of word (ω) included in the master key. The first ω subkeys $rk_0, rk_1, \ldots, rk_{\omega-1}$ are initialized by the master key. The remaining subkeys are generated as follows:

$$rk_{i+m} = c \oplus (z_j)_i \oplus rk_i \oplus Y_m \oplus (Y_m \ggg 1),$$
$$Y_m = \begin{cases} rk_{i+1} \ggg 3 & \text{if } \omega = 2 \\ rk_{i+1} \oplus (rk_{i+2} \ggg 3) & \text{if } \omega = 3 \\ rk_{i+1} \oplus (rk_{i+3} \ggg 3) & \text{if } \omega = 4. \end{cases}$$

Here, the value c is constant `0xff...fc`, and $(z_j)_i$ denotes the i-th bit from one of the five constant sequences z_0, z_1, z_2, z_3 and z_4. The master key can be derived if any sequence of ω consecutive subkeys is known. For more information, please refer to [6].

2.2 Zero-Correlation Linear Cryptanalysis

Zero-correlation linear attack is one of the recent cryptanalytic methods introduced by Bogdanov and Rijmen in [3]. This kind of attack is based on the linear approximation with correlation zero (*i.e.* the linear approximation with probability exactly $\frac{1}{2}$). The idea of multiple zero-correlation cryptanalysis was developed in recent years in [4] by Bogdanov and Wang. They proposed a new distinguisher by using the fact that there are numerous zero-correlation approximations in susceptible ciphers. In [5], a more powerful distinguisher called multidimensional zero-correlation distinguisher was introduced.

Even though multiple zero-correlation cryptanalysis and multidimensional zero-correlation cryptanalysis perform better than zero-correlation linear cryptanalysis for various ciphers, we have to claim that they are not appropriate for SIMON. Multiple zero-correlation cryptanalysis and multidimensional zero-correlation cryptanalysis are more appropriate for word-level ciphers, such as AES, Skipjack and CAST-256.

The following Theorem is useful for computing the success probability of zero-correlation linear cryptanalysis.

Theorem 1 **([3, Proposition 3]).** *The probability that the correlation value is* 0 *for a non-trivial linear approximation of a randomly drawn n-bit permutation can be approximated by* $\frac{1}{\sqrt{2\pi}}2^{\frac{4-n}{2}}$ *for* $n \geq 5$.

Based on the linear approximation of correlation zero, a technique similar to Matsui's Algorithm 2 [14] can be used for key recovery. Let the adversary have 2^n plaintext-ciphertext pairs and a zero-correlation linear approximation $\alpha \rightarrow \beta$ for a part of the cipher. The linear approximation is placed in the middle of the attacked cipher. Let E and D be the partial intermediate states of the data transform at the boundaries of the linear approximations (See Fig. 2). Then the key can be recovered using the following approach:

1. Guess the bits of the key needed to compute E and D. For each guess:
   (a) Partially encrypt the plaintexts and partially decrypt the ciphertexts up to the boundaries of the zero-correlation linear approximation $\alpha \rightarrow \beta$.
   (b) Estimate the correlation c of the linear approximation $\alpha \rightarrow \beta$ for the key guess using the partially encrypted and decrypted value E and D by counting how many times $\langle \alpha, E \rangle + \langle \beta, D \rangle$ is zero over 2^n plaintext-ciphertext pairs.
   (c) Perform a test on the estimated correlation c to tell of the estimated values of c is compatible with the hypothesis that the actual value of c is zero.

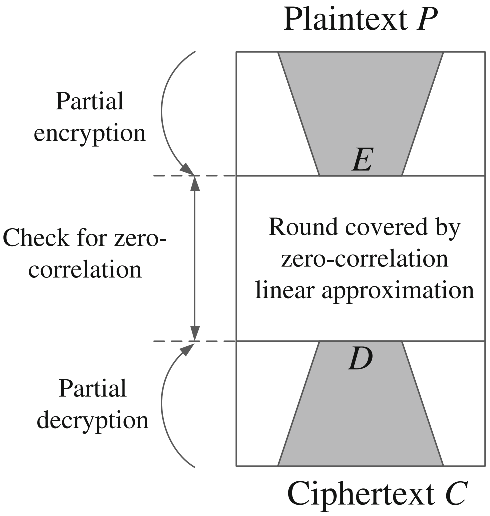

Plaintext P
Partial encryption
E
Check for zero-correlation
Round covered by zero-correlation linear approximation
D
Partial decryption
Ciphertext C

Fig. 2. Key recovery in zero-correlation linear cryptanalysis

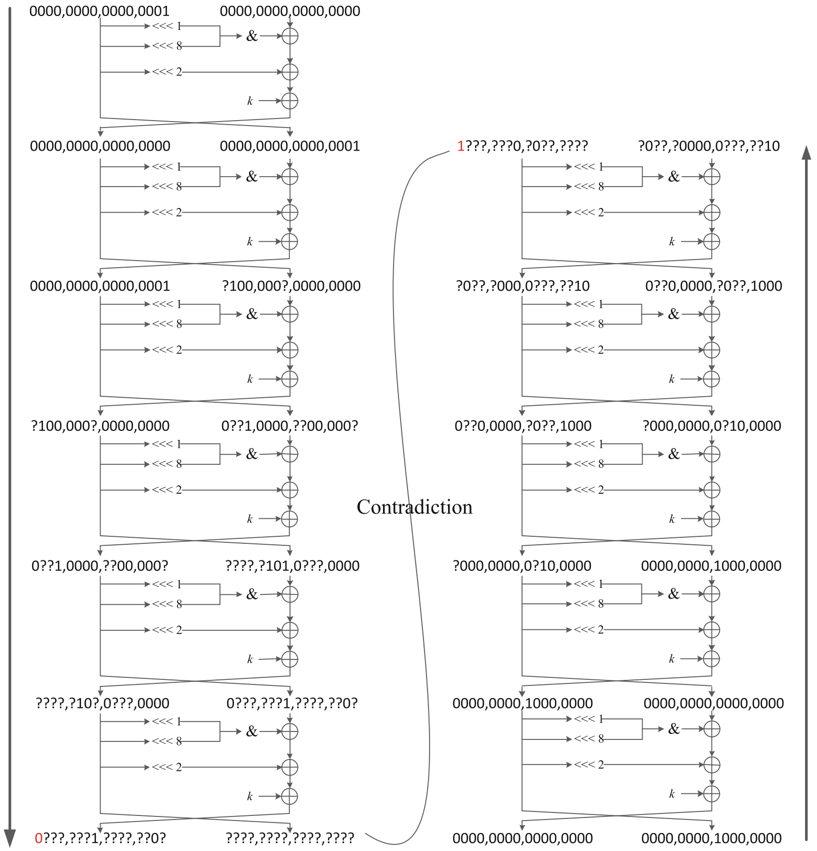


Fig. 3. Zero-correlation linear approximation of 11-round SIMON32. (Color figure online)

2. Test the surviving key candidates against a necessary number of plaintext-ciphertext pairs.

3 Zero-Correlation Linear Distinguishers of SIMON

3.1 Zero-Correlation Linear Distinguisher of SIMON32

For SIMON32, we use the 11-round zero-correlation linear distinguisher in [19], which is shown in Fig. 3. The input mask is (0x0001,0x0000) and the output mask is (0x0000,0x0080). The '0' at bottom left and the '1' at top right (in red) constitute the contradiction that ensures zero correlation.

3.2 Zero-Correlation Linear Distinguisher of SIMON48

Similarly, by using the 12-round zero-correlation linear distinguisher in [19], we can mount the key recovery attacks on 21-round SIMON48/72 and

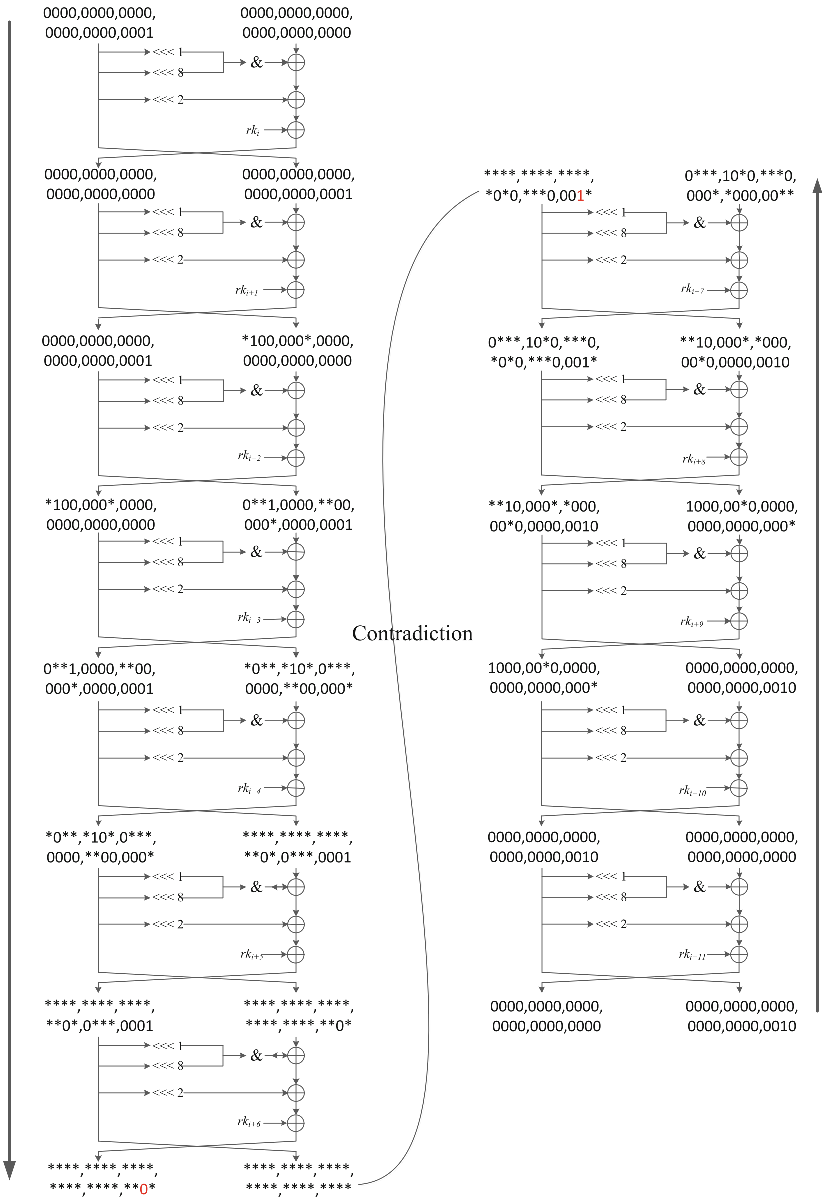


Fig. 4. Zero-correlation linear approximation of 12-round SIMON48. (Color figure online)

22-round SIMON48/96. The distinguisher used in the following attacks is shown in Fig. 4. The input mask is (0x000001,0x000000) and the output mask is (0x000000,0x000002). The '0' at bottom left and the '1' at top right (in red) constitute the contradiction that ensures zero correlation.

3.3 Zero-Correlation Linear Distinguishers of SIMON64, SIMON96 and SIMON128

In order to attack SIMON64/96/128, we first construct 13-, 16- and 19-round zero-correlation linear approximations for SIMON64, SIMON96 and SIMON128 by applying miss-in-the middle technique, which are shown in Figs. 5, 6 and 7, respectively.

	ROUND	LEFT	RIGHT
FORWARD	0	00000000000000000000000000000001	00000000000000000000000000000000
	1	00000000000000000000000000000000	00000000000000000000000000000001
	2	00000000000000000000000000000001	*100000*000000000000000000000000
	3	*100000*000000000000000000000000	0**10000**00000*0000000000000001
	4	0**10000**00000*0000000000000001	*0***10*0***0000**00000*00000000
	5	*0***10*0***0000**00000*00000000	0******1******0*0***0000**00000*
	6	0******1******0*0***0000**00000*	**********************0*0***0000
	7	**********************0*0***0000	0*****************************0*
	8	0*****************************0*	********************************
BACKWARD	8	1******0*0***0000**00000*0******	*0***0000**00000*00000000*0***10
	9	*0***0000**00000*00000000*0***10	0**00000*00000000000000010**1000
	10	0**00000*00000000000000010**1000	*000000000000000000000000*100000
	11	*000000000000000000000000*100000	00000000000000000000000010000000
	12	00000000000000000000000010000000	00000000000000000000000000000000
	13	00000000000000000000000000000000	00000000000000000000000010000000

Fig. 5. Zero-correlation linear approximation of 13-round SIMON64.

	ROUND	LEFT	RIGHT
FORWARD	0	000000000000000000000000000000000000000000000001	000000000000000000000000000000000000000000000000
	1	000000000000000000000000000000000000000000000000	000000000000000000000000000000000000000000000001
	2	000000000000000000000000000000000000000000000001	*100000*0000000000000000000000000000000000000000
	3	*100000*0000000000000000000000000000000000000000	0**10000**00000*00000000000000000000000000000001
	4	0**10000**00000*00000000000000000000000000000001	*0***10*0***0000**00000*000000000000000000000000
	5	*0***10*0***0000**00000*000000000000000000000000	0******1******0*0***0000**00000*0000000000000001
	6	0******1******0*0***0000**00000*0000000000000001	*1********************0*0***0000**00000*00000000
	7	*1********************0*0***0000**00000*00000000	0*****************************0*0***0000**00000*
	8	0*****************************0*0***0000**00000*	**************************************0*0***0000
	9	**************************************0*0***0000	0***0*
	10	0***0*	**
BACKWARD	6	*******************0*0***0000**00000*00000000*1*	****1******0*0***0000**00000*00000000000000010**
	5	****1******0*0***0000**00000*00000000000000010**	**10*0***0000**00000*000000000000000000000000*0*
	4	**10*0***0000**00000*000000000000000000000000*0*	10000**00000*000000000000000000000000000000010**
	3	10000**00000*000000000000000000000000000000010**	0000*0000000000000000000000000000000000000000*10
	2	0000*0000000000000000000000000000000000000000*10	000000000000000000000000000000000000000000001000
	1	000000000000000000000000000000000000000000001000	000000000000000000000000000000000000000000000000
	0	000000000000000000000000000000000000000000000000	000000000000000000000000000000000000000000001000

Fig. 6. Zero-correlation linear approximation of 16-round SIMON96.

	ROUND	LEFT	RIGHT
FORWARD	0	000000000000000000000000000000000000000000000000000000000000001	0000000000000000000000000000000000000000000000000000000000000000
	1	0000000000000000000000000000000000000000000000000000000000000000	000000000000000000000000000000000000000000000000000000000000001
	2	000000000000000000000000000000000000000000000000000000000000001	*100000*00000000000000000000000000000000000000000000000000000000
	3	*100000*00000000000000000000000000000000000000000000000000000000	0**10000**00000*000000000000000000000000000000000000000000000001
	4	0**10000**00000*000000000000000000000000000000000000000000000001	*0***10*0***0000**00000*0000000000000000000000000000000000000000
	5	*0***10*0***0000**00000*0000000000000000000000000000000000000000	0******1******0*0***0000**00000*00000000000000000000000000000001
	6	0******1******0*0***0000**00000*00000000000000000000000000000001	*1********************0*0***0000**00000*000000000000000000000000
	7	*1********************0*0***0000**00000*000000000000000000000000	0*****************************0*0***0000**00000*0000000000000001
	8	0*****************************0*0***0000**00000*0000000000000001	*0************************************0*0***0000**00000*00000000
	9	*0************************************0*0***0000**00000*00000000	0***0*0***0000**00000*
	10	0***0*0***0000**00000*	**0*0***0000
	11	**0*0***0000	0***0*
	12	0***0*	**
BACKWARD	7	*****************************0*0***0000**00000*00000000000000010	1********************0*0***0000**00000*000000000000000000000000*
	6	1********************0*0***0000**00000*000000000000000000000000*	******1******0*0***0000**00000*0000000000000000000000000000000010
	5	******1******0*0***0000**00000*0000000000000000000000000000000010	0***10*0***0000**00000*0000000000000000000000000000000000000000*
	4	0***10*0***0000**00000*0000000000000000000000000000000000000000*	**10000**00000*0000000000000000000000000000000000000000000000010
	3	**10000**00000*0000000000000000000000000000000000000000000000010	100000*00000000000000000000000000000000000000000000000000000000*
	2	100000*00000000000000000000000000000000000000000000000000000000*	0000000000000000000000000000000000000000000000000000000000000010
	1	0000000000000000000000000000000000000000000000000000000000000010	0000000000000000000000000000000000000000000000000000000000000000
	0	0000000000000000000000000000000000000000000000000000000000000000	0000000000000000000000000000000000000000000000000000000000000010

Fig. 7. Zero-correlation linear approximation of 19-round SIMON128.

4 Zero-Correlation Linear Cryptanalysis of SIMON

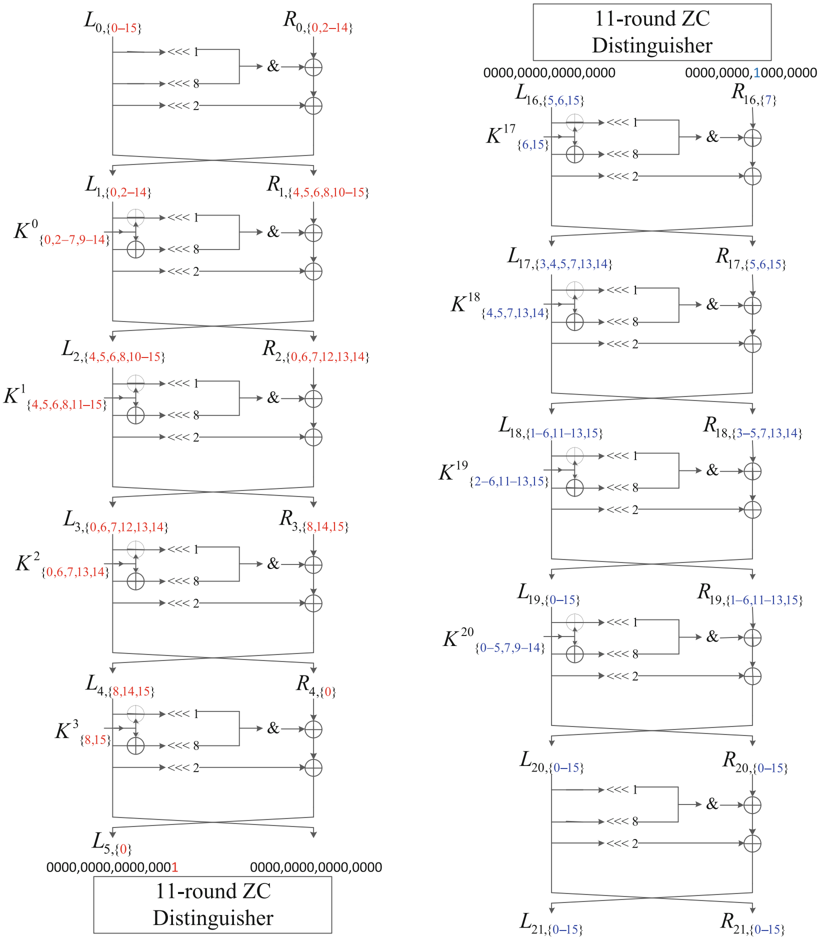
In this section, we investigate the security of whole family of SIMON by using zero-correlation linear cryptanalysis. We use 11- and 12-round zero-correlation linear approximations of SIMON32 and SIMON48 in [19] to present the key recovery attacks on 21-round SIMON32, 21-round SIMON48/72 and 22-round SIMON48/96. We also utilize the distinguishers presented in Sect. 3.3 to attack SIMON64, SIMON96 and SIMON128.

4.1 Zero-Correlation Linear Cryptanalysis of SIMON32

In this section, we use the 11-round zero-correlation linear distinguisher (See Fig. 3) in [19] to attack 21-round SIMON32. As shown in Fig. 8, we can add five rounds before the distinguisher and append five rounds after the distinguisher (*i.e.* the zero-correlation distinguisher starts from the 5-th round and ends at the 15-th round, with round number starting from 0). In this way, we can attack 21-round SIMON32.

Equivalent-Subkey Technique. The equivalent-subkey technique has been widely used in various key-recovery attacks. This technique aims at reducing the number of guessed subkey bits by replacing the equivalent subkeys with the original subkeys. This technique had been used in [13] by Isobe. But there exists a little difference. Because the subkey is XORed after non-linear function, the condition in [13] that some parts of plaintext should be fixed can be canceled.

In order to reduce the number of guessed subkey bits in the key recovery process, we move the subkey rk_i of the i-th round to the $(i+1)$-th round, $(i = 0, 1, 2, 3, 4)$, to get the equivalent subkey K^i, see Fig. 8 (a). For example, K^0 in Fig. 8 (a) is equal to rk_0, and K^1 is equal to $(rk_0 \lll 2) \oplus rk_1$ and so forth. Note that K^4 is located in the distinguisher and doesn't need to be guessed. In Fig. 8 (a), we only list the guessed bits for K^i, $0 \leq i \leq 3$. Similarly, we can move the subkey rk_i of the i-th round to the $(i-1)$-th round, $(i = 16, 17, 18, 19, 20)$, to get the equivalent subkey K^i, see Fig. 8 (b). Again, K^{16} is located in the distinguisher and doesn't need to be guessed. In Fig. 8 (b), we only list the guessed bits for K^i, $17 \leq i \leq 20$.



(a) five rounds before the distinguisher

(b) five rounds after the distinguisher

Fig. 8. Key recovery attack on 21-round SIMON32.

Key Recovery Process for SIMON32. In the following, R_i denotes the output of the i-th round. $R_{i,\{j\}}$ denotes the j-th bit of the R_i. $L_{i,\{j\}}$ is defined in a similar way. Note the bit position starts from '0'.

Firstly, we guess a part of the equivalent subkeys K^{17}, K^{18}, K^{19} and K^{20} (the concrete guessed key bits are shown in Fig. 8 (b)) and partially decrypt the ciphertext up to the state $R_{16,\{7\}}$. Next, we guess a part of the equivalent subkeys K^0, K^1, K^2, K^3 (the concrete guessed key bits are shown in Fig. 8 (a)) and partially encrypt the plaintext to the state $L_{5,\{0\}}$. We count the number of occurrences of the event that $L_{5,\{0\}} \| R_{16,\{7\}}$ is equal to "00" or "11". If the occurrence number is exactly equal to 2^{31}, we can keep the guessed 58-bit subkey as a possible subkey candidate, and discard it otherwise. To this end, 58-bit subkey is already guessed, which includes $K^0_{\{0,2-7,9-14\}}$, $K^2_{\{4-6,8,11-15\}}$, $K^3_{\{0,6,7,13,14\}}$, $K^4_{\{8,15\}}$, $K^{17}_{\{6,15\}}$, $K^{18}_{\{4,5,7,13,14\}}$, $K^{19}_{\{2-6,11-13,15\}}$ and $K^{20}_{\{0-5,7,9-14\}}$.

From Theorem 1, the probability that a wrong subkey guess is kept after the above procedure can be approximated by $\frac{1}{\sqrt{2\pi}}2^{\frac{4-32}{2}} \approx 2^{-15.33}$. Thus, $2^{58} \times 2^{-15.33} = 2^{42.67}$ subkey candidates will be left. After that, we guess 6-bit subkey $K^0_{\{1,8,15\}} \| K^1_{\{0,1,2\}}$ and obtain 29 remaining bits of $K^1_{\{3,7,9,10\}} \parallel K^2_{\{1-5,8-12,15\}} \parallel K^3_{\{0-7,9-14\}}$ by solving the linear equations with Gaussian elimination. At last, we can compute all bits of the master key by inverting the key schedule, and check the correctness by using at most two plaintext-ciphertext pairs. We express this procedure in Algorithm 1.

Algorithm 1. Key Recovery Attack of SIMON32

```
Represent $K^{20}_{\{0-5,7,9-14\}} \| K^{19}_{\{2-6,11-13,15\}} \| K^{18}_{\{4,5,7,13,14\}} \| K^{17}_{\{6,15\}}$ by
  $K^0 \| K^1 \| K^2 \| K^3$, and get 29 linear equations
for all $2^{42.67}$ subkey candidates getting from the subkey recovery procedure (See
  Table 3) do
    for all values of $K^0_{\{1,8,15\}} \| K^1_{\{0,1,2\}}$ do
        Get 29 linear equations with respect to
          $K^1_{\{3,7,9,10\}} \| K^2_{\{1-5,8-12,15\}} \| K^3_{\{0-7,9-14\}}$
        Solve the linear equations by means of Gaussian elimination
        if solvable then
            Compute all bits of the master key according to the key schedule.
            Verify the master key by using two plaintext-ciphertext pairs.
```

Complexity of Attack. The data complexity for the attack on SIMON32 is 2^{32} known plaintexts.

In this attack, the dominant term for the memory complexity is the term used to store 2^{31} 8-bit counters $T_0[\boldsymbol{X_1^{32}}]$, which makes the memory complexity be 2^{31} bytes.

The time complexity of each step in subkey recovery procedure is listed in Table 3. Overall, the time complexity in subkey recovery procedure is $2^{59.42}$ 21-round SIMON32 encryptions. In master key recovery phase, solving 29 linear equations with 29 variables by using Gaussian elimination needs about $\frac{1}{3} \cdot 29^3 \approx 8130$ bit-XOR operations, which can be measured by $\frac{8130}{16 \cdot 4 \cdot 21} \approx 2^{2.60}$ 21-round SIMON32 encryptions (Note that there are three XOR operations and

Table 3. Procedure of subkey recovery for SIMON32

Step	Input state	Guessed subkey (♯Bits)	Computing (♯Bits)	Counter (size)	Time complexity
0	$\boldsymbol{X_0^{32}}$	$K^{20}_{\{0-5,7,9-14\}}$ $K^{19}_{\{2-6,11-13,15\}}$ $K^{18}_{\{4,5,7,13,14\}}$ $K^{17}_{\{6,15\}}(29)$	$R_{16,\{7\}}$ (36)*	$T_0[\boldsymbol{X_1^{32}}](31)$	$2^{32}\cdot 2^{29}\cdot\frac{1+3+6+10+16}{16\times 21}$ $\approx 2^{55.78}$
1	$\boldsymbol{X_1^{32}}$	None(0)	$L_{1,\{0,2-14\}}$ (14)	$T_1[\boldsymbol{X_2^{32}}](25)$	$2^{31}\cdot 2^{29}\cdot\frac{14}{16\times 21}\approx 2^{55.41}$
2	$\boldsymbol{X_2^{32}}$	$K^0_{\{0,3,5,7,10,12,14\}}(7)$	$L_{2,\{4,6,8,11,13,15\}}$ (6)	$T_2[\boldsymbol{X_3^{32}}](24)$	$2^{25}\cdot 2^{36}\cdot\frac{6}{16\times 21}\approx 2^{55.19}$
3	$\boldsymbol{X_3^{32}}$	$K^0_{\{4,6,11,13\}}(4)$	$L_{2,\{5,12,14\}}$ (3)	$T_3[\boldsymbol{X_4^{32}}](20)$	$2^{24}\cdot 2^{40}\cdot\frac{3}{16\times 21}\approx 2^{57.19}$
4	$\boldsymbol{X_4^{32}}$	$K^0_{\{2,9\}}(2)$	$L_{2,\{10\}}$ (1)	$T_4[\boldsymbol{X_5^{32}}](17)$	$2^{20}\cdot 2^{42}\cdot\frac{1}{16\times 21}\approx 2^{53.61}$
5	$\boldsymbol{X_5^{32}}$	$K^1_{\{6,8,13,15\}}(4)$	$L_{3,\{0,7,14\}}$ (3)	$T_5[\boldsymbol{X_6^{32}}](15)$	$2^{17}\cdot 2^{46}\cdot\frac{3}{16\times 21}\approx 2^{56.19}$
6	$\boldsymbol{X_6^{32}}$	$K^1_{\{5,12,14\}}(3)$	$L_{3,\{6,13\}}$ (2)	$T_6[\boldsymbol{X_7^{32}}](13)$	$2^{15}\cdot 2^{49}\cdot\frac{2}{16\times 21}\approx 2^{56.61}$
7	$\boldsymbol{X_7^{32}}$	$K^1_{\{4,11\}}(2)$	$L_{3,\{12\}}$ (1)	$T_7[\boldsymbol{X_8^{32}}](10)$	$2^{13}\cdot 2^{51}\cdot\frac{1}{16\times 21}\approx 2^{55.61}$
8	$\boldsymbol{X_8^{32}}$	$K^2_{\{0,7,14\}}(3)$	$L_{4,\{8,15\}}$ (2)	$T_8[\boldsymbol{X_9^{32}}](8)$	$2^{10}\cdot 2^{54}\cdot\frac{2}{16\times 21}\approx 2^{56.61}$
9	$\boldsymbol{X_9^{32}}$	$K^2_{\{6,13\}}(2)$	$L_{4,\{14\}}$ (1)	$T_9[\boldsymbol{X_{10}^{32}}](5)$	$2^{8}\cdot 2^{56}\cdot\frac{1}{16\times 21}\approx 2^{55.61}$
10	$\boldsymbol{X_{10}^{32}}$	$K^3_{\{8,15\}}(2)$	$L_{5,\{0\}}$ (1)	$T_{10}[\boldsymbol{X_{11}^{32}}](2)$	$2^{5}\cdot 2^{58}\cdot\frac{1}{16\times 21}\approx 2^{54.61}$

Input State: input state of each step (See Table 4 for its concrete meaning);
Guessed Subkey: guessed subkey bits in each step;
Computing: state bits to be computed in each step;
Counter: counters to be constructed in each step;
Time Complexity: measured in 21-round SIMON32 encryption.
*: To compute $R_{16,\{7\}}$, we also need to compute $R_{17,\{5,6,15\}}$, $R_{18,\{3-5,7,13,14\}}$, $R_{19,\{1-6,11-13,15\}}$ and $R_{20,\{0-15\}}$, which are in total 36 bits.

Table 4. Explanation of symbols used in subkey recovery of SIMON32

Symbol	Meaning
$\boldsymbol{X_0^{32}}$	$L_{0,\{0-15\}}\Vert R_{0,\{0,2-14\}}\Vert L_{21,\{0-15\}}\Vert R_{21,\{0-15\}}$
$\boldsymbol{X_1^{32}}$	$L_{0,\{0-15\}}\ \Vert\ R_{0,\{0,2-14\}}\ \Vert\ R_{16,\{7\}}$
$\boldsymbol{X_2^{32}}$	$L_{1,\{0,2-14\}}\Vert R_{1,\{4-6,8,10-15\}}\Vert R_{16,\{7\}}$
$\boldsymbol{X_3^{32}}$	$L_{2,\{4,6,8,11,13,15\}}\Vert L_{1,\{0,2-4,6-14\}}\Vert R_{1,\{5,10,12,14\}}\Vert R_{16,\{7\}}$
$\boldsymbol{X_4^{32}}$	$L_{2,\{4-6,8,11-15\}}\Vert L_{1,\{0,2,6-9,12-14\}}\Vert R_{1,\{10\}}\Vert R_{16,\{7\}}$
$\boldsymbol{X_5^{32}}$	$L_{2,\{4-6,8,10-15\}}\Vert R_{2,\{0,6,7,12-14\}}\Vert R_{16,\{7\}}$
$\boldsymbol{X_6^{32}}$	$L_{3,\{0,7,14\}}\Vert L_{2,\{4,5,8,10-12,14,15\}}\Vert R_{2,\{6,12,13\}}\Vert R_{16,\{7\}}$
$\boldsymbol{X_7^{32}}$	$L_{3,\{0,6,7,13,14\}}\Vert L_{2,\{4,8,10,11,14,15\}}\Vert R_{2,\{12\}}\Vert R_{16,\{7\}}$
$\boldsymbol{X_8^{32}}$	$L_{3,\{0,6,7,12-14\}}\Vert R_{3,\{8,14,15\}}\Vert R_{16,\{7\}}$
$\boldsymbol{X_9^{32}}$	$L_{4,\{8,15\}}\Vert L_{3,\{0,6,12,13\}}\Vert R_{3,\{14\}}\Vert R_{16,\{7\}}$
$\boldsymbol{X_{10}^{32}}$	$L_{4,\{8,14,15\}}\Vert R_{4,\{0\}}\Vert R_{16,\{7\}}$
$\boldsymbol{X_{11}^{32}}$	$L_{5,\{0\}}\Vert R_{16,\{7\}}$

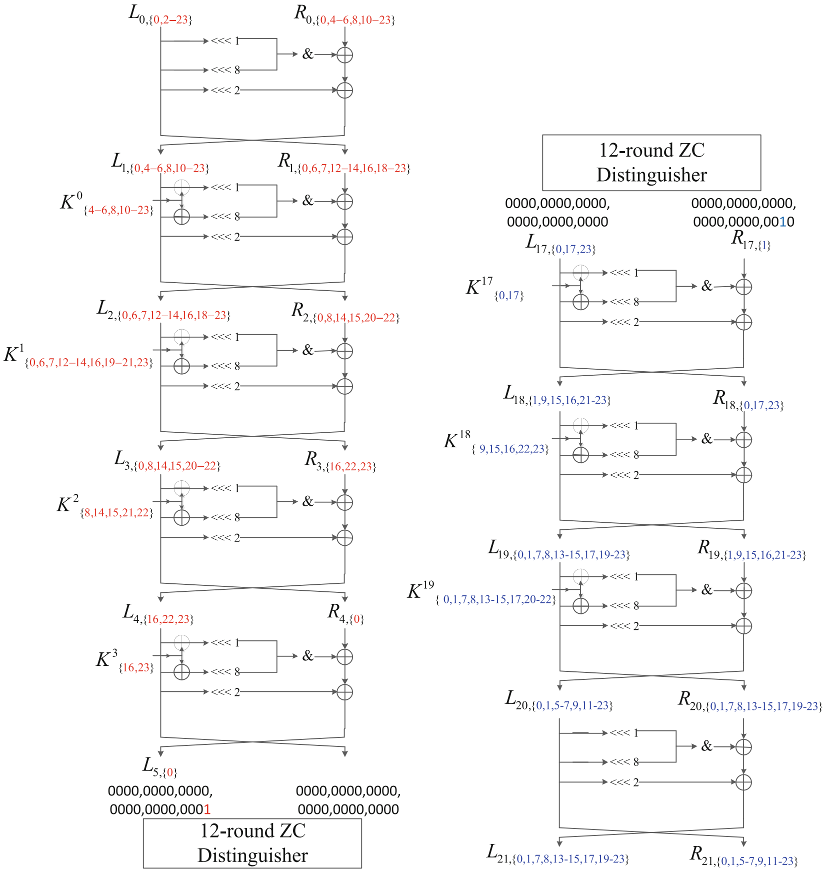
one AND operation in the round function of SIMON. For simplicity, we approximate them as four XOR operations in our analysis), thus the time complexity of master key recovery phase can be approximated as $2^{42.67}\times 2^5\times 2^{2.60}+2^{42.67}\times 2^5\times(1+2^{-32})\approx 2^{50.49}$ 21-round SIMON32 encryptions. Thus, the total time complexity of this attack is about $2^{59.42}$ 21-round SIMON32 encryptions.

4.2 Zero-Correlation Linear Cryptanalysis of SIMON48

Similarly, by using the 12-round zero-correlation linear distinguisher (See Fig. 4) in [19], we can mount key recovery attacks on 21-round SIMON48/72 and 22-round SIMON48/96.

Key Recovery Attack on 21-Round SIMON48/72. As shown in Fig. 9, we can add five rounds before the distinguisher and append four rounds after the distinguisher. In this way, we can attack 21-round SIMON48/72. We only list the guessed subkey bits in Fig. 9. The detailed attack procedure is proceeded in Algorithm 2.

The data complexity for the attack on SIMON48/72 is 2^{48} known plaintexts.


$L_{0,\{0,2-23\}}$
$R_{0,\{0,4-6,8,10-23\}}$
<<< 1
<<< 8
<<< 2
&
$L_{1,\{0,4-6,8,10-23\}}$
$R_{1,\{0,6,7,12-14,16,18-23\}}$
$K^0_{\{4-6,8,10-23\}}$
$L_{2,\{0,6,7,12-14,16,18-23\}}$
$R_{2,\{0,8,14,15,20-22\}}$
$K^1_{\{0,6,7,12-14,16,19-21,23\}}$
$L_{3,\{0,8,14,15,20-22\}}$
$R_{3,\{16,22,23\}}$
$K^2_{\{8,14,15,21,22\}}$
$L_{4,\{16,22,23\}}$
$R_{4,\{0\}}$
$K^3_{\{16,23\}}$
$L_{5,\{0\}}$
0000,0000,0000,
0000,0000,0001
0000,0000,0000,
0000,0000,0000
12-round ZC Distinguisher
12-round ZC Distinguisher
0000,0000,0000,
0000,0000,0000
0000,0000,0000,
0000,0000,0010
$L_{17,\{0,17,23\}}$
$R_{17,\{1\}}$
$K^{17}_{\{0,17\}}$
$L_{18,\{1,9,15,16,21-23\}}$
$R_{18,\{0,17,23\}}$
$K^{18}_{\{9,15,16,22,23\}}$
$L_{19,\{0,1,7,8,13-15,17,19-23\}}$
$R_{19,\{1,9,15,16,21-23\}}$
$K^{19}_{\{0,1,7,8,13-15,17,20-22\}}$
$L_{20,\{0,1,5-7,9,11-23\}}$
$R_{20,\{0,1,7,8,13-15,17,19-23\}}$
$L_{21,\{0,1,7,8,13-15,17,19-23\}}$
$R_{21,\{0,1,5-7,9,11-23\}}$

(a) five rounds before the distinguisher

(b) four rounds after the distinguisher

Fig. 9. Key recovery attack on 21-round SIMON48/72.

Algorithm 2. Key Recovery Attack of SIMON48/72

```
Represent $K^3_{\{16,23\}}\|K^{18}_{\{0,17\}}\|K^{19}_{\{9,15,16,22,23\}}\|K^{20}_{\{0,1,7,8,13-15,17,20-22\}}$ by
  $K^0\|K^1\|K^2$, and get 20 linear equations.
for all $2^{30.67}$ subkey candidates getting from the subkey recovery procedure (the
  concrete subkey recovery procedure is listed in Table 5) do
    for all values of $K^0_{\{0-3,7,9\}}\|K^1_{\{1-5,8-11,15,17,18\}}$ do
        Get 20 linear equations with respect to $K^1_{\{22\}}\|K^2_{\{0-7,9-13,16-20,23\}}$.
        Solve the linear equations by means of Gaussian elimination
        if solvable then
            Compute all bits of the master key according to the key schedule.
            Verify the master key by using two plaintext-ciphertext pairs.
```

Table 5. Procedure of subkey recovery for SIMON48/72[†]

Step	Input State	Guessed Subkey(♯Bits)	Computing(♯Bits)	Counter(Size)	Time Complexity
0	$\boldsymbol{X_0^{48,72}}$	$K^{18}_{\{0,17\}}\|K^{19}_{\{9,15,16,22,23\}}$ $K^{20}_{\{0,1,7,8,13-15,17,20-22\}}(18)$	$R_{17,\{1\}}$ (24)*	$T_0[\boldsymbol{X_1^{48,72}}](43)$	$2^{48}\cdot 2^{18}\cdot\frac{1+3+7+13}{24\times 21}\approx 2^{61.61}$
1	$\boldsymbol{X_1^{48,72}}$	None(0)	$L_{1,\{0,4-6,8,10-23\}}$ (19)	$T_1[\boldsymbol{X_2^{48,72}}](33)$	$2^{43}\cdot 2^{18}\cdot\frac{19}{24\times 21}\approx 2^{56.27}$
2	$\boldsymbol{X_2^{48,72}}$	$K^0_{\{5,6,8,10,12,13,15-17,19,20,22,23\}}(13)$	$L_{2,\{0,6,7,13,14,16,18,20,21,23\}}$ (10)	$T_2[\boldsymbol{X_3^{48,72}}](26)$	$2^{33}\cdot 2^{31}\cdot\frac{10}{24\times 21}\approx 2^{58.34}$
3	$\boldsymbol{X_3^{48,72}}$	$K^0_{\{4,11,14,18,21\}}(5)$	$L_{2,\{12,19,22\}}$ (3)	$T_3[\boldsymbol{X_4^{48,72}}](21)$	$2^{26}\cdot 2^{36}\cdot\frac{3}{24\times 21}\approx 2^{54.61}$
4	$\boldsymbol{X_4^{48,72}}$	$K^1_{\{0,7,14,21\}}(4)$	$L_{3,\{8,15,22\}}$ (3)	$T_4[\boldsymbol{X_5^{48,72}}](17)$	$2^{21}\cdot 2^{40}\cdot\frac{3}{24\times 21}\approx 2^{53.61}$
5	$\boldsymbol{X_5^{48,72}}$	$K^1_{\{6,12,13,16,19,20,23\}}(7)$	$L_{3,\{0,20-22\}}$ (4)	$T_5[\boldsymbol{X_6^{48,72}}](11)$	$2^{17}\cdot 2^{47}\cdot\frac{4}{24\times 21}\approx 2^{57.02}$
6	$\boldsymbol{X_6^{48,72}}$	$K^2_{\{8,14,15,21,22\}}(5)$	$L_{4,\{16,22,23\}}$ (3)	$T_6[\boldsymbol{X_7^{48,72}}](5)$	$2^{11}\cdot 2^{52}\cdot\frac{3}{24\times 21}\approx 2^{55.61}$
7	$\boldsymbol{X_7^{48,72}}$	$K^3_{\{16,23\}}(2)$	$L_{5,\{0\}}$ (1)	$T_7[\boldsymbol{X_8^{48,72}}](2)$	$2^{5}\cdot 2^{54}\cdot\frac{1}{24\times 21}\approx 2^{50.02}$

Input State: input state of each step (See Table 6 for its concrete meaning);
Guessed Subkey: guessed subkey bits in each step;
Computing: state bits to be computed in each step;
Counter: counters to be constructed in each step;
Time Complexity: measured in 21-round SIMON48 encryption.

* : To compute $R_{17,\{1\}}$, we also need to compute$R_{18,\{0,17,23\}}$, $R_{19,\{1,9,15,16,21-23\}}$ and $R_{20,\{0,1,7,8,13-15,17,19-23\}}$, which are in total 24 bits.

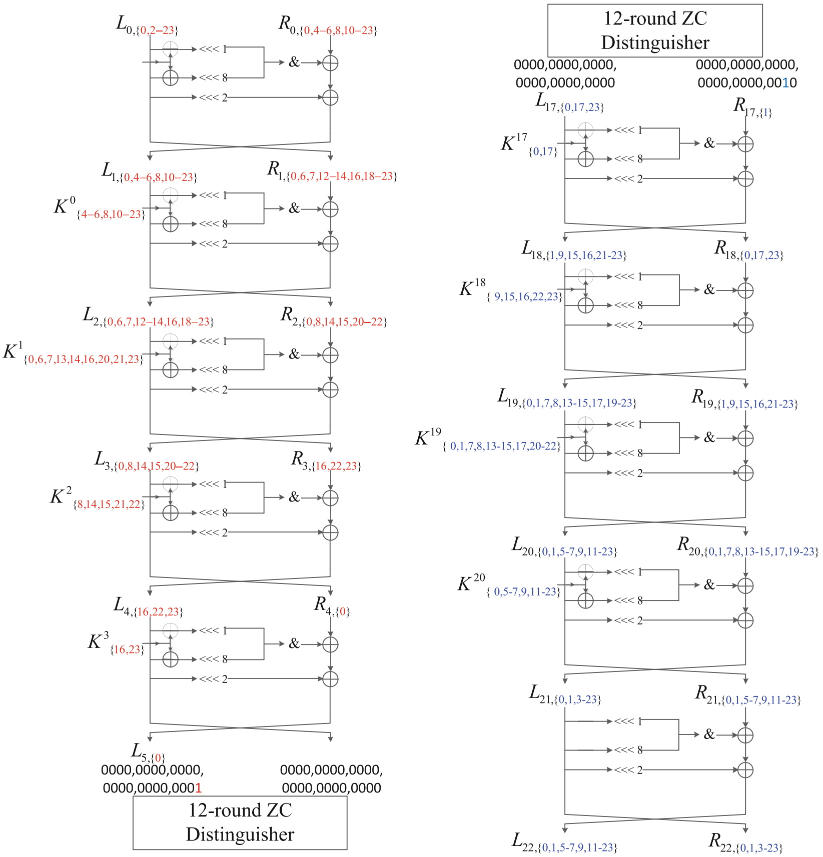
[†] : The false positive probability of this attack is $\frac{1}{\sqrt{2\pi}}2^{\frac{4-48}{2}}\approx 2^{-23.33}$ from Theorem 1. The number of remaining subkey candidates is $2^{54}\cdot 2^{-23.33}\approx 2^{30.67}$ as we guess 54 subkey bits in total.

In this attack, the dominant term for the memory complexity is the term used to store 2^{43} 8-bit counters $T_0[\boldsymbol{X_1^{48,72}}]$, which makes the memory complexity be 2^{43} bytes.

From Table 5, the time complexity for subkey recovery is about $2^{61.87}$ 21-round SIMON48/72 encryptions. In Algorithm 2, it will proceed Gaussian elimination process for $2^{30.67}\cdot 2^{18}=2^{48.67}$ times, which can be ignored compared to $2^{61.87}$ 21-round encryptions. After that, the time complexity of checking the correctness of guess using two plaintext-ciphertext pairs also can be ignored compared to $2^{61.87}$ 21-round encryptions. Thus, the total time complexity is about $2^{61.87}$ 21-round SIMON48/72 encryptions.

Table 6. Explanation of symbols used in subkey recovery of SIMON48/72

Symbol	Meaning
$\boldsymbol{X_0^{48,72}}$	$L_{0,\{0-23\}} \| R_{0,\{0-23\}} \| L_{21,\{0-23\}} \| R_{21,\{0-23\}}$
$\boldsymbol{X_1^{48,72}}$	$L_{0,\{0,2-23\}} \| R_{0,\{0,4-6,8,10-23\}} \| R_{17,\{1\}}$
$\boldsymbol{X_2^{48,72}}$	$L_{1,\{0,4-6,8,10-23\}} \| R_{1,\{0,6,7,12-14,16,18-23\}} \| R_{17,\{1\}}$
$\boldsymbol{X_3^{48,72}}$	$L_{2,\{0,6,7,13,14,16,18,20,21,23\}} \| L_{1,\{0,4,8,10,11,14,15,17,18,20-22\}} \| R_{1,\{12,19,22\}} \| R_{17,\{1\}}$
$\boldsymbol{X_4^{48,72}}$	$L_{2,\{0,6,7,12-14,16,18-23\}} \| R_{2,\{0,8,14,15,20-22\}} \| R_{17,\{1\}}$
$\boldsymbol{X_5^{48,72}}$	$L_{3,\{8,15,22\}} \| L_{2,\{6,12,13,16,18-20,22,23\}} \| R_{2,\{0,14,20,21\}} \| R_{17,\{1\}}$
$\boldsymbol{X_6^{48,72}}$	$L_{3,\{0,8,14,15,20-22\}} \| R_{3,\{16,22,23\}} \| R_{17,\{1\}}$
$\boldsymbol{X_7^{48,72}}$	$L_{4,\{16,22,23\}} \| R_{4,\{0\}} \| R_{17,\{1\}}$
$\boldsymbol{X_8^{48,72}}$	$L_{5,\{0\}} \| R_{17,\{1\}}$



(a) five rounds before the distinguisher

(b) five rounds after the distinguisher

Fig. 10. Key recovery attack on 22-round SIMON48/96.

Algorithm 3. Key Recovery Attack of SIMON48/96

```
Represent $K^{17}_{\{0,17\}}\|K^{18}_{\{9,15,16,22,23\}}\|K^{19}_{\{0,1,7,8,13-15,17,20-22\}}\|K^{20}_{\{0,5-7,9,11-23\}}$ by
  $K^0\|K^1\|K^2\|K^3$, and get 36 linear equations.
for all $2^{48.67}$ subkey candidates getting from the subkey recovery procedure (the
  concrete subkey recovery procedure is listed in Table 7) do
    for all values of $K^0_{\{0-3,7,9\}}\|K^1_{\{1-5,8-11,15,17,18,22\}}\|K^2_{\{0-4\}}$ do
        Get 36 linear equations with respect to
          $K^2_{\{5-7,9-13,16-20,23\}}\|K^3_{\{0-15,17-22\}}$.
        Solve the linear equations by means of Gaussian elimination
        if solvable then
            Compute all bits of the master key according to the key schedule.
            Verify the master key by using two plaintext-ciphertext pairs.
```

Table 7. Procedure of subkey recovery for SIMON48/96†

Step	Input State	Guessed Subkey(♯Bits)	Computing(♯Bits)	Counter(Size)	Time Complexity
0	$\boldsymbol{X_0^{48,96}}$	$K^{17}_{\{0,17\}}\|K^{18}_{\{9,15,16,22,23\}}$ $K^{19}_{\{0,1,7,8,13-15,17,20-22\}}$ $K^{20}_{\{0,5-7,9,11-23\}}(36)$	$R_{17,\{1\}}$ (43)*	$T_0[\boldsymbol{X_1^{48,96}}](43)$	$2^{48}\cdot 2^{36}\cdot\frac{43}{24\times 22}\approx 2^{80.38}$
1	$\boldsymbol{X_1^{48,96}}$	None(0)	$L_{1,\{0,4-6,8,10-23\}}$ (19)	$T_1[\boldsymbol{X_2^{48,96}}](33)$	$2^{43}\cdot 2^{36}\cdot\frac{19}{24\times 22}\approx 2^{74.20}$
2	$\boldsymbol{X_2^{48,96}}$	$K^0_{\{5,6,8,10,12,13,15-17,19,20,22,23\}}(13)$	$L_{2,\{0,6,7,13,14,16,18,20,21,23\}}$ (10)	$T_2[\boldsymbol{X_3^{48,96}}](26)$	$2^{33}\cdot 2^{49}\cdot\frac{10}{24\times 22}\approx 2^{76.28}$
3	$\boldsymbol{X_3^{48,96}}$	$K^0_{\{4,11,14,18,21\}}(5)$	$L_{2,\{12,19,22\}}$ (3)	$T_3[\boldsymbol{X_4^{48,96}}](21)$	$2^{26}\cdot 2^{54}\cdot\frac{3}{24\times 22}\approx 2^{72.54}$
4	$\boldsymbol{X_4^{48,96}}$	$K^1_{\{0,6,7,13,14,20,21\}}(7)$	$L_{3,\{8,14,15,21,22\}}$ (5)	$T_4[\boldsymbol{X_5^{48,96}}](14)$	$2^{21}\cdot 2^{61}\cdot\frac{5}{24\times 22}\approx 2^{75.28}$
5	$\boldsymbol{X_5^{48,96}}$	$K^1_{\{12,16,19,23\}}(4)$	$L_{3,\{0,20\}}$ (2)	$T_5[\boldsymbol{X_6^{48,96}}](11)$	$2^{14}\cdot 2^{65}\cdot\frac{2}{24\times 22}\approx 2^{70.96}$
6	$\boldsymbol{X_6^{48,96}}$	$K^2_{\{8,14,15,21,22\}}(5)$	$L_{4,\{16,22,23\}}$ (3)	$T_6[\boldsymbol{X_7^{48,96}}](5)$	$2^{11}\cdot 2^{70}\cdot\frac{3}{24\times 22}\approx 2^{73.54}$
7	$\boldsymbol{X_7^{48,96}}$	$K^3_{\{16,23\}}(2)$	$L_{5,\{0\}}$ (1)	$T_7[\boldsymbol{X_8^{48,96}}](2)$	$2^{5}\cdot 2^{72}\cdot\frac{1}{24\times 22}\approx 2^{67.96}$

Input State: input state of each step (See Table 8 for its concrete meaning);
Guessed Subkey: guessed subkey bits in each step;
Computing: state bits to be computed in each step;
Counter: counters to be constructed in each step;
Time Complexity: measured in 22-round SIMON48 encryption.

* : To compute $R_{17,\{1\}}$, we also need to compute$R_{18,\{0,17,23\}}$, $R_{19,\{1,9,15,16,21-23\}}$, $R_{20,\{0,1,7,8,13-15,17,19-23\}}$ and $R_{21,\{0,1,5-7,9,11-23\}}$, which are in total 43 bits.

† : The false positive probability of this attack is $\frac{1}{\sqrt{2\pi}}2^{\frac{4-48}{2}} \approx 2^{-23.33}$ from Theorem 1.
The number of remaining subkey candidates is $2^{72}\cdot 2^{-23.33}\approx 2^{48.67}$ for we guess 72 subkey bits in total.

Key Recovery Attack on 22-Round SIMON48/96. As shown in Fig. 10, we can add five rounds before the distinguisher and append five rounds after the distinguisher. In this way, we can attack 22-round SIMON48/96. We only list the guessed subkey bits in Fig. 10. The detailed attack procedure is proceeded in Algorithm 3.

The data complexity for the attack on SIMON48/96 is 2^{48} known plaintexts.

In this attack, the dominant term for the memory complexity is the term used to store 2^{43} 8-bit counters $T_0[\boldsymbol{X_1^{48,96}}]$, which makes the memory complexity to be 2^{43} bytes.

Table 8. Explanation of symbols used in subkey recovery of SIMON48/96

Symbol	Meaning
$\boldsymbol{X_0^{48,96}}$	$L_{0,\{0-23\}} \Vert R_{0,\{0-23\}} \Vert L_{22,\{0-23\}} \Vert R_{22,\{0-23\}}$
$\boldsymbol{X_1^{48,96}}$	$L_{0,\{0,2-23\}} \Vert R_{0,\{0,4-6,8,10-23\}} \Vert R_{17,\{1\}}$
$\boldsymbol{X_2^{48,96}}$	$L_{1,\{0,4-6,8,10-23\}} \Vert R_{1,\{0,6,7,12-14,16,18-23\}} \Vert R_{17,\{1\}}$
$\boldsymbol{X_3^{48,96}}$	$L_{2,\{0,6,7,13,14,16,18,20,21,23\}} \Vert L_{1,\{0,4,8,10,11,14,15,17,18,20-22\}} \Vert R_{1,\{12,19,22\}} \Vert R_{17,\{1\}}$
$\boldsymbol{X_4^{48,96}}$	$L_{2,\{0,6,7,12-14,16,18-23\}} \Vert R_{2,\{0,8,14,15,20-22\}} \Vert R_{17,\{1\}}$
$\boldsymbol{X_5^{48,96}}$	$L_{3,\{8,14,15,21,22\}} \Vert R_{2,\{0,20\}} \Vert L_{2,\{12,16,18,19,22,23\}} \Vert R_{17,\{1\}}$
$\boldsymbol{X_6^{48,96}}$	$L_{3,\{0,8,14,15,20-22\}} \Vert R_{3,\{16,22,23\}} \Vert R_{17,\{1\}}$
$\boldsymbol{X_7^{48,96}}$	$L_{4,\{16,22,23\}} \Vert R_{4,\{0\}} \Vert R_{17,\{1\}}$
$\boldsymbol{X_8^{48,96}}$	$L_{5,\{0\}} \Vert R_{17,\{1\}}$

From Table 7, the time complexity for subkey recovery is about $2^{80.54}$ 22-round SIMON48/96 encryptions. In Algorithm 3, it will proceed Gaussian elimination process for $2^{48.67} \cdot 2^{24} = 2^{72.67}$ times, which can be ignored compared to $2^{80.54}$ 22-round encryptions. After that, the time complexity of checking the correctness of guess using two plaintext-ciphertext pairs also can be ignored compared to $2^{80.54}$ 22-round encryptions. Thus, the total time complexity is about $2^{80.54}$ 22-round SIMON48/96 encryptions.

4.3 Zero-Correlation Linear Cryptanalysis of SIMON64, SIMON96 and SIMON128

We can use the zero-correlation linear approximations showed in Figs. 5, 6 and 7 to attack SIMON64, SIMON96 and SIMON128, respectively. Since the attack procedures for them are similar, we only list the attack results in Table 9.

Table 9. Summary of ZC linear attack results on SIMON

Cipher	ZC linear distinguisher	Attacked rounds	Total rounds	Time (ENs)	Data (KPs)	Memory
SIMON64/96	13	23(5+13+5)*	42	$2^{90.4}$	2^{64}	2^{54} bytes
SIMON64/128	13	24(6+13+5)	44	$2^{116.8}$	2^{64}	2^{54} bytes
SIMON96/144	16	28(6+16+6)	54	$2^{141.0}$	2^{96}	2^{85} bytes
SIMON128/192	19	32(7+19+6)	69	$2^{156.8}$	2^{128}	2^{117} bytes
SIMON128/256	19	34(8+19+7)	72	$2^{255.6}$	2^{128}	2^{117} bytes

KP: Known Plaintext; EN: Encryption.

*: For $(a + b + c)$, a is the number of rounds before the distinguisher, b is the length of the distinguisher and c is the number of rounds after the distinguisher.

5 Conclusion

In this paper, we study the security of whole family of SIMON by using zero-correlation linear cryptanalysis. We improved the previous zero-correlation attacks for SIMON32 and SIMON48. Moreover, we present the 13-, 16- and 19-round zero correlation linear approximations of SIMON64, SIMON96 and SIMON128, respectively, and use them to attack the corresponding ciphers. We are the first one to give the zero-correlation linear cryptanalysis for SIMON 64, SIMON96 and SIMON128.

Acknowledgements. This work has been supported by 973 program (No. 2013CB834205), NSFC Projects (No. 61133013 and No. 61572293), Program for New Century Excellent Talents in University of China (No. NCET-13-0350), as well as Outstanding Young Scientists Foundation Grant of Shandong Province (No. BS2012DX018).

References

1. Abed, F., List, E., Lucks, S., Wenzel, J.: Differential cryptanalysis of round-reduced SIMON and SPECK. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 525–545. Springer, Heidelberg (2015)
2. Alkhzaimi, H., Lauridsen, M.: Cryptanalysis of the SIMON family of block ciphers. IACR Cryptology ePrint Archive, 2013/543 (2013)
3. Bogdanov, A., Rijmen, V.: Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Designs, Codes and Cryptography **70**, 369–383 (2014). Springer, Heidelberg
4. Bogdanov, A., Wang, M.: Zero correlation linear cryptanalysis with reduced data complexity. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 29–48. Springer, Heidelberg (2012)
5. Bogdanov, A., Leander, G., Nyberg, K., Wang, M.: Integral and multidimensional linear distinguishers with correlation zero. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 244–261. Springer, Heidelberg (2012)
6. 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, Report 2013/404 (2013)
7. Biryukov, A., Roy, A., Velichkov, V.: Differential analysis of block ciphers SIMON and SPECK. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 546–570. Springer, Heidelberg (2015)
8. Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
9. Boura, C., Naya-Plasencia, M., Suder, V.: Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and Simon. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 179–199. Springer, Heidelberg (2014)
10. Cannière, C., Dunkelman, O., Kneževiá, M.: KATAN and KTANTAN-a family of small and efficient hardware-oriented block ciphers. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 272–288. Springer, Heidelberg (2009)

11. Gong, Z., Nikova, S., Law, Y.W.: KLEIN: a new family of lightweight block ciphers. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 1–18. Springer, Heidelberg (2012)
12. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)
13. Isobe, T., Shibutani, K.: Generic key recovery attack on feistel scheme. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 464–485. Springer, Heidelberg (2013)
14. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
15. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: *Piccolo*: an ultra-lightweight blockcipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 342–357. Springer, Heidelberg (2011)
16. Sun, S., Hu, L., Wang, M., Wang, P., Qiao, K., Ma, X., et al.: Constructing mixed-integer programming models whose feasible region is exactly the set of all valid differential characteristics of SIMON. IACR Cryptology ePrint Archive, 2015/122 (2015)
17. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: a lightweight block cipher for multiple platforms. In: Knudsen, L.R., Wu, H. (eds.) SAC 2013. LNCS, vol. 7707, pp. 339–354. Springer, Heidelberg (2013)
18. Wang, N., Wang, X., Jia, K., Zhao, J.: Improved differential attacks on reduced SIMON versions. IACR Cryptology ePrint Archive, 2014/448 (2014)
19. Wang, Q., Liu, Z., Varici, K., Sasaki, Y., Rijmen, V., Todo, Y.: Cryptanalysis of reduced-round SIMON32 and SIMON48. In: Meier, W., Mukhopadhyay, D. (eds.) Progress in Cryptology – INDOCRYPT 2014. LNCS, vol. 8885, pp. 143–160. Springer, Heidelberg (2014)