Linear Cryptanalysis of Reduced-Round SIMECK Variants

Nasour Bagheri[1]

E.E. Department, Shahid Rajaee Teacher Training University, Iran, NBagheri@srttu.edu

Abstract. SIMECK is a family of 3 lightweight block ciphers designed by Yang *et al.* They follow the framework used by Beaulieu *et al.* from the United States National Security Agency (NSA) to design SIMON and SPECK. A cipher in this family with K-bit key and N-bit block is called SIMECKN/K. We show that the security of this block cipher against linear cryptanalysis is not as good as its predecessors SIMON. More precisely, while the best known linear attack for SIMON32/64, using algorithm 1 of Matsui, covers 13 rounds we present a linear attack in this senario which covers 14 rounds of SIMECK32/64. Similarly, using algorithm 1 of Matsui, we present attacks on 19 and 22 rounds of SIMECK48/96 and SIMECK64/128 respectively, compare them with known attacks on 16 and 19 rounds SIMON48/96 and SIMON64/128 respectively. In addition, we use algorithm 2 of Matsui to attack 18, 23 and 27 rounds of SIMECK32/64, SIMECK48/96 and SIMECK64/128 respectively, compare them with known attacks on 18, 19 and 21 rounds SIMON32/64, SIMON48/96 and SIMON64/128 respectively.

Keywords: SIMECK, SIMON, SPECK, Linear Cryptanalysis.

1 Introduction

SIMECK [26] is a new family of lightweight block ciphers designed by Yang *et al.* and inspired by SIMON and SPECK, designed by the NSA [8]. The round function of SIMECK is similar to the round function of SIMON while its key schedule is more similar to the key schedule of SPECK. The aim of SIMECK is to provide optimal hardware and software performance for low-power limited gate devices such as RFID devices by combing good components from both SIMON and SPECK. Variants of this block cipher support plaintext block sizes of 32, 48, 64 and 96 and 128 bits. The key size of those variants are 64, 96 and 128 bits respectively. SIMECKN/K denotes a variant of SIMECK that has a block size of N bits and a key size of K bits.

Although, several works investigated the security of SIMON and SPECK against differential attack [2, 3, 6, 9, 22, 24], its variants such as impossible differential attack [2–4, 6, 10, 12, 14, 15, 21, 25] and linear attack [1, 4, 5, 7, 11, 20]. However, we are not aware of any third party security analysis of SIMECK. In this paper, we present linear cryptanalysis against reduced variants of SIMECK.

Contributions. In this paper, we analyze the security of SIMECK against linear cryptanalytic techniques. In this direction, we present linear characteristics for different variants of SIMECK, that can be used for key recovery attacks on SIMECK reduced to 14, 19 and 22 rounds for the respective block sizes of 32, 48 and 64 bits using Matsui's algorithm 1. Furthermore, we extend this linear characteristics to attack more rounds using Matsui's algorithm 2. These attacks covers 18, 23 and 26 rounds for the respective block sizes of 32, 48 and 64. A brief summary of our results on SIMECK and the best known results on the equivalent versions of SIMON are presented in Table 1. It must be noted that designers' security analysis against linear cryptanalysis covers 12, 15 and 19 rounds of SIMECK32/64, SIMECK48/96 and SIMECK64/128 respectively [26, §5].

Table 1: Linear cryptanalysis of SIMECK, using the Matsui's Algorithm 1 and 2, and comparison with the best known results on the equivalent versions of SIMON.

	Variant	# Attacked Rounds	Data	Time	Success Probability	Reference
Matsui's Algorithm 1	SIMON32/64	13	2^{32}	2^{32}	0.997	[4]
	SIMECK32/64	13	2^{30}	2^{30}	0.997	Section 3
	SIMECK32/64	14	2^{32}	2^{32}	0.841	Section 3
	SIMON48/96	16	2^{46}	2^{46}	0.997	[4]
	SIMECK48/96	18	2^{48}	2^{48}	0.997	Section 3
	SIMECK48/96	19	2^{46}	2^{46}	0.841	Section 3
	SIMON64/128	19	2^{58}	2^{58}	0.997	[4]
	SIMECK64/128	22	2^{60}	2^{60}	0.997	Section 3
	SIMECK64/128	23	2^{64}	2^{64}	0.841	Section 3
Matsui's Algorithm 2	SIMON32/64	18	2^{32}	$2^{61.5}$	¡ 0.477	[1]
	SIMECK32/64	18	2^{31}	$2^{63.5}$	0.477	Section 4
	SIMON48/96	19	2^{47}	2^{82}	0.477	[1]
	SIMECK48/96	24	2^{45}	2^{94}	0.477	Section 4
	SIMON64/128	21	2^{59}	2^{123}	0.477	[1]
	SIMECK64/128	27	2^{61}	$2^{120.5}$	0.477	Section 4

Organization. The paper is structured as follows. In §2 we present a brief description of SIMECK. In section §3 we present the idea of linear attacks on SIMON and apply linear attacks to variants of SIMECK using Matsui's algorithm 1. In §3 we extend our attacks on variants of SIMECK using Matsui's algorithm 2. Finally, we conclude the paper in §5 and propose possible future directions of research.

2 Description of the SIMECK Family

SIMECK is a classical Feistel block cipher with the round block size of $2n$ bits and the key size of $4n$, where n is the word size. The number of rounds of cipher is denoted by r and depends on the variant of SIMON which are 32, 36 and 44 rounds for SIMECK32/64, SIMECK48/96 and SIMECK64/128 respectively. For a $2n$-bit string X, we use X_L and X_R to denote the left and right halves of the string respectively. The output of round r is denoted by $X^r = (X_R^r \parallel X_L^r)$ and the subkey used in the round r is denoted by K^r. Given a string X, $(X)_i$ denotes the i-th bit of X. Bitwise circular rotation of string a by b position to the left is denoted by $a \lll b$. Further, $\oplus$ and & denote bitwise XOR and AND operations respectively. We use P and C to denote a plaintext and a ciphertext respectively.

The function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ used in each round of SIMECK is non-linear and non-invertible, and is applied to the left half of the state, so the state is updated as:

$$X^{r+1} = (F(X_L^r) \oplus X_R^r \oplus K^r \parallel X_L^r). \tag{1}$$

The F function is defined as:

$$F(X) = (X \lll 1) \oplus ((X) \ \& \ (X \lll 5)).$$

The subkeys are derived from a master key. Depending on the size of the master key, the key schedule of SIMECK operates on four n-bit word registers. Detailed description of SIMECK variants structure and key scheduling can be found in [26] but it has no affect on our analysis.

3 Linear Cryptanalysis of SIMECK using the Matsui's Algorithm 1

Linear cryptanalysis [17] is a classical known-plaintext attack cryptanalytic technique that was employed on several block ciphers such as FEAL-4, DES, Serpent and SAFER [13, 16, 17, 23]. In this section, we present linear characteristics for variants of SIMECK using the Matsui's algorithm 1 [17].

In the round function of SIMECK, similar to SIMON, the only non-linear operation is the bitwise AND. Note that, given single bits A and B, then $\Pr(A \,\&\, B = 0) = \frac{3}{4}$. Hence, we can extract the following highly biased linear expressions for the F function of SIMECK (there are equivalent linear expressions for the F function of SIMON [4]):

$$\begin{array}{l} \text{Approximation 1}: \ \Pr\left((F(X))_i = (X)_{i-1}\right) = \frac{3}{4}, \\ \text{Approximation 2}: \ \Pr\left((F(X))_i = (X)_{i-1} \oplus (X)_i\right) = \frac{3}{4}, \\ \text{Approximation 3}: \ \Pr\left((F(X))_i = (X)_{i-1} \oplus (X)_{i-5}\right) = \frac{3}{4}, \\ \text{Approximation 4}: \ \Pr\left((F(X))_i = (X)_{i-1} \oplus (X)_i \oplus (X)_{i-5}\right) = \frac{1}{4}. \end{array} \tag{2}$$

Given the round function (1) of SIMECK and these linear approximations, we can extract the following linear expressions for the i^{th} round of the SIMECK:

$$(X_L^i)_9 \oplus (X_R^i)_{10} \oplus (K^i)_{10} = (X_L^{i+1})_{10} \tag{3}$$

$$(X_L^{i+3})_{10} \oplus (X_R^{i+3})_9 \oplus (K^{i+2})_{10} = (X_R^{i+2})_{10} \tag{4}$$

Each equality in Equation (3) holds with probability $\frac{3}{4}$. Given that $(X_L^{i+1})_{10} = (X_R^{i+2})_{10}$, we can use Equation (3) in a meet in the middle approach to extract a 3-round linear approximation as follows, for which the bias is $\frac{1}{8}$ (the bias of a linear approximation which is hold with the probability of p is defined as $\left|p - \frac{1}{2}\right|$):

$$(X_L^i)_9 \oplus (X_R^i)_{10} \oplus (X_L^{i+3})_{10} \oplus (X_R^{i+3})_9 = (K^i)_{10} \oplus (K^{i+2})_{10}. \tag{5}$$

Since $(X_R^i)_{10} = (X_L^{i-1})_{10}$ and with the probability of $\frac{3}{4}$, we have $(X_L^i)_9 = (X_L^{i-1})_8 \oplus (X_R^{i-1})_9 \oplus (K^{i-1})_9$, we can add a round to the top of the current 3-round approximation and produce a 4-round linear expression, with the bias of $\frac{1}{16}$, as follows:

$$(X_L^{i-1})[8,10] \oplus (X_R^{i-1})_9 \oplus (X_L^{i+3})_{10} \oplus (X_R^{i+3})_9 = (K^{i-1})_9 \oplus (K^i)_{10} \oplus (K^{i+2})_{10}. \tag{6}$$

where $(X)[i_1, ..., i_m] = (X)_{i_1} \oplus \ldots \oplus (X)_{i_m}$. Similarly, since $(X_L^{i+3})_{10} = (X_R^{i+4})_{10}$ and with the probability of $\frac{3}{4}$ we have $(X_R^{i+3})_9 = (X_R^{i+4})_8 \oplus (X_L^{i+4})_9 \oplus (K^{i+4})_9$, we can add a round to the bottom of the current 4-round approximation and produce a 5-round linear expression, with the bias of $\frac{1}{16}$, as follows:

$$(X_L^{i-1})[8,10] \oplus (X_R^{i-1})_9 \oplus (X_R^{i+4})[8,10] \oplus (X_L^{i+4})_9 = (K^{i-1})_9 \oplus (K^i)_{10} \oplus (K^{i+2})_{10} \oplus (K^{i+4})_9. \tag{7}$$

Following this approach we can extend this linear approximation by adding extra rounds to top and bottom and drive a linear approximation for more rounds of SIMECK. In Table 2, Table 3 and Table 4 sequences of approximation to produce linear characteristics for SIMECK32/64, SIMECK48/96 and SIMECK64/128 are presented. In the last column of each table, number of approximation in each round is presented. Given that for any used approximation in these tables bias is $\frac{1}{4}$, based on the piling-up lemma [17] the bias of a linear characteristic with N approximation would be $2^{N-1} \times (\frac{1}{4})^N = 2^{-(N+1)}$.

It is clear from Table 2 that we can produce a 11-round linear characteristic for SIMECK32/64 with bias 2^{-15} as follows:

$$\begin{pmatrix} (X_R^1)_7 \oplus (X_L^1)[6,8,10] \\ \oplus (X_L^{12})_9 \oplus (X_R^{12})[6,10] \end{pmatrix} = \begin{pmatrix} (K^1)_7 \oplus (K^2)[8,10] \oplus (K^3)_9 \oplus (K^4)_{10} \\ \oplus (K^6)_{10} \oplus (K^7)_9 \oplus (K^8)[8,10] \\ \oplus (K^9)_7 \oplus (K^{10})[6,8,10] \oplus (K^{11})_9 \end{pmatrix}, \tag{8}$$

Given this 11-round linear characteristic, we can add another round to its top and a round to its bottom to extend the attack up to 13 rounds. The added rounds are related to the plaintext and

ciphertext and free of any approximation, because we know the input of F functions for these rounds and key does not affect approximation. In this way we have a 13-round linear characteristic between plaintext and ciphertext of SIMECK32/64 for which the bias is 2^{-15}. Given this linear characteristic, using Matsui's Algorithm 1 with the data complexity of $(2^{-15})^2 = 2^{30}$, an adversary can retrieve 1 bit of the key with the success probability of 0.997 [17, Table 2.].

The adversary can use Table 2 to produce a 12-round linear characteristic for SIMECK32/32 with bias of 2^{-17} as follows:

$$\begin{pmatrix} (X_R^1)_7 \oplus (X_L^1)[6,8,10] \\ \oplus (X_L^{13})[6,10] \oplus (X_R^{13})_5 \end{pmatrix} = \begin{pmatrix} (K^1)_7 \oplus (K^2)[8,10] \oplus (K^3)_9 \oplus (K^4)_{10} \\ \oplus (K^6)_{10} \oplus (K^7)_9 \oplus (K^8)[8,10] \oplus (K^9)_7 \\ \oplus (K^{10})[6,8,10] \oplus (K^{11})_9 \oplus (K^{12})[6,10] \end{pmatrix}, \tag{9}$$

Given this 12-round linear characteristic, we can add another round to its top and a round to its bottom to extend the attack up to 14 rounds. Hence, using Matsui's Algorithm 1 with the data complexity of $\frac{1}{4}(2^{-17})^2 = 2^{32}$, the adversary can retrieves 1 bit of the key with the success probability of 0.841 [17, Table 2.].

Similarly, it is clear from Table 3 that we can produce a 16-round linear characteristic (Equation 10) with bias 2^{-24} and a 17-round linear characteristic (Equation 11) with bias 2^{-25} for SIMECK48/96.

$$\begin{pmatrix} (X_R^1)_5 \oplus (X_L^1)[4,6,10] \\ \oplus (X_L^{17})[6,10] \oplus (X_R^{17})_5 \end{pmatrix} = \begin{pmatrix} (K^1)_5 \oplus (K^2)[6,10] \oplus (K^3)_9 \oplus (K^4)[6,8,10] \\ \oplus (K^5)_7 \oplus (K^6)[8,10] \oplus (K^7)_9 \oplus (K^8)_{10} \\ \oplus (K^{10})_{10} \oplus (K^{11})_9 \oplus (K^{12})[8,10] \oplus (K^{13})_7 \\ \oplus (K^{14})[6,8,10] \oplus (K^{15})_9 \oplus (K^{16})[6,10] \end{pmatrix}, \tag{10}$$

$$\begin{pmatrix} (X_R^1)_5 \oplus (X_L^1)[4,6,10] \\ \oplus (X_L^{18})_5 \oplus (X_R^{18})[4,6,10] \end{pmatrix} = \begin{pmatrix} (K^1)_5 \oplus (K^2)[6,10] \oplus (K^3)_9 \oplus (K^4)[6,8,10] \\ \oplus (K^5)_7 \oplus (K^6)[8,10] \oplus (K^7)_9 \oplus (K^8)_{10} \\ \oplus (K^{10})_{10} \oplus (K^{11})_9 \oplus (K^{12})[8,10] \oplus (K^{13})_7 \\ \oplus (K^{14})[6,8,10] \oplus (K^{15})_9 \oplus (K^{16})[6,10] \oplus (K^{17})_5 \end{pmatrix}, \tag{11}$$

Given these linear characteristics, we can add another round to their top and a round to their bottom to extend the attack up to 18 and 19 rounds respectively, free of extra approximation. Hence, using these linear characteristics and Matsui's Algorithm 1 with the data complexity of 2^{48}, the adversary can retrieves 1 bit of the key with the success probability of 0.997 and 0.841 respectively.

Table 4 shows the sequence of approximations to produce a 19-round linear characteristic (Equation 12) with bias 2^{-30} and a 20-round linear characteristic (Equation 13) with bias 2^{-33} for SIMECK64/128, which can be extended to attack to 21 and 22 rounds of algorithm respectively. Given those linear characteristics, using Matsui's Algorithm 1, with the data complexity of 2^{60} and 2^{64}, the adversary can retrieve 1 bit of the key with the success probability of 0.997 and 0.841 respectively.

$$\begin{pmatrix} (X_R^2)_5 \oplus (X_L^2)[4,6,10] \\ \oplus (X_L^{20})[3,9] \oplus (X_R^{20})[2,6,8,10] \end{pmatrix} = \begin{pmatrix} (K^2)_5 \oplus (K^3)[6,10] \oplus (K^4)_9 \oplus (K^5)[6,8,10] \\ \oplus (K^6)_7 \oplus (K^7)[8,10] \oplus (K^8)_9 \oplus (K^9)_{10} \\ \oplus (K^{11})_{10} \oplus (K^{12})_9 \oplus (K^{13})[8,10] \oplus (K^{14})_7 \\ \oplus (K^{15})[6,8,10] \oplus (K^{16})_9 \oplus (K^{17})[6,10] \\ \oplus (K^{18})_5 \oplus (K^{19})[4,6,10] \oplus (K^{20})[3,9] \end{pmatrix}, \tag{12}$$

$$\begin{pmatrix} (X_R^1)[4,6,10] \oplus (X_L^1)[3,9] \\ \oplus (X_L^{21})[3,9] \oplus (X_R^{21})[2,6,8,10] \end{pmatrix} = \begin{pmatrix} (K^1)[4,6,10] \oplus (K^2)_5 \oplus (K^3)[6,10] \oplus (K^4)_9 \oplus \\ (K^5)[6,8,10] \oplus (K^6)_7 \oplus (K^7)[8,10] \oplus (K^8)_9 \\ \oplus (K^9)_{10} \oplus (K^{11})_{10} \oplus (K^{12})_9 \oplus (K^{13})[8,10] \oplus \\ (K^{14})_7 \oplus (K^{15})[6,8,10] \oplus (K^{16})_9 \oplus (K^{17})[6,10] \\ \oplus (K^{18})_5 \oplus (K^{19})[4,6,10] \oplus (K^{20})[3,9] \end{pmatrix}, \tag{13}$$

Table 2: Sequences of approximation of a 12 round linear characteristic for SIMECK32/64. $\mathcal{A}_L$ and $\mathcal{A}_R$ denote the active bits in the left and right side respectively and App. denotes the approximation used for the corresponding bit(s) of $\mathcal{A}_R$.

	$\mathcal{A}_L$	$\mathcal{A}_R$	Used App.	# App.
1	10, 8, 6	7	1	1
2	9, 9, 7	10, 8	1; 1	2
3	10, 8	9	1	1
4	9	10	1	1
5	10	–	–	0
6	9	10	1	1
7	10,8	9	1	1
8	9, 9, 7	10, 8	1; 1	2
9	10, 8, 6	7	1	1
10	7, 9,5, 7, 5	10, 8, 6	2; 1; 1	3
11	10, 8, 6, 8	9	1	1
12	9, 9, 5	10,6	1; 1	2

Table 3: Sequences of approximation of a 17 round linear characteristic for SIMECK48/96. Notations are similar to the notations used in Table 3.

	$\mathcal{A}_L$	$\mathcal{A}_R$	Used App.	# App.
1	10, 6,4	5	1	1
2	9, 9, 5	10,6	1; 1	2
3	10, 8, 6, 8	9	1	1
4	7, 9,5, 7, 5	10, 8, 6	2; 1; 1	3
5	10, 8, 6	7	1	1
6	9, 9, 7	10, 8	1; 1	2
7	10, 8	9	1	1
8	9	10	1	1
9	10	–	–	0
10	9	10	1	1
11	10,8	9	1	1
12	9, 9, 7	10, 8	1; 1	2
13	10, 8, 6	7	1	1
14	7, 9,5, 7, 5	10, 8, 6	2; 1; 1	3
15	10, 8, 6, 8	9	1	1
16	9, 9, 5	10,6	1; 1	2
17	10, 6,4	5	1	1

Table 4: Sequences of approximation of a 20 round linear characteristic for SIMECK64/128. Notations are similar to the notations used in Table 3.

	$\mathcal{A}_L$	$\mathcal{A}_R$	Used App.	# App.
1	5,9,5,3	10, 6,4	1;1; 1	3
2	10, 6,4	5	1	1
3	9, 9, 5	10,6	1; 1	2
4	10, 8, 6, 8	9	1	1
5	7, 9,5, 7, 5	10, 8, 6	2; 1; 1	3
6	10, 8, 6	7	1	1
7	9, 9, 7	10, 8	1; 1	2
8	10, 8	9	1	1
9	9	10	1	1
10	10	–	–	0
11	9	10	1	1
12	10,8	9	1	1
13	9, 9, 7	10, 8	1; 1	2
14	10, 8, 6	7	1	1
15	7, 9,5, 7, 5	10, 8, 6	2; 1; 1	3
16	10, 8, 6, 8	9	1	1
17	9, 9, 5	10,6	1; 1	2
18	10, 6,4	5	1	1
19	5,9,5,3	10, 6,4	1;1; 1	3
20	10, 6,4,8,4,2	9,3	2,1	2

4 Linear Cryptanalysis of SIMECK using the Matsui's Algorithm 2

In this section, we use Matsui's algorithm 2 to recover the key of more rounds of variants of SIMECK. For example, in the case of SIMECK 32/64, given the linear characteristic represented in Equation 8 with bias 2^{-15}, we guess subkyes of rounds at the beginning and the end of the cipher and determine the correlation of the following linear relation to filter the wrong subkeys:

$$(X_R^i)_7 \oplus (X_L^i)[6,8,10] \oplus (X_L^{i+11})_9 \oplus (X_R^{i+11})[6,10] \tag{14}$$

With respect to Table 5, we can append a round to the beginning of the cipher to find a new 12-round linear characteristic. Since SIMECK injects the subkey at the end of its round function, then this work does not add any computational complexity. More precisely, for the current 11-round linear characteristic, we evaluate $(X_R^i)_7 \oplus (X_L^i)[6,8,10] \oplus (X_L^{i+11})_9 \oplus (X_R^{i+11})[6,10]$. When we add a round in the backwards direction, i.e. round $i-1$, we can determine $(X_L^i)[6,8,10]$ as a function of $F(X_L^{i-1})[6,8,10] \oplus (K^{i-1})[6,8,10] \oplus X_R^{i-1})[6,8,10]$, where we know X_R^{i-1} and X_L^{i-1}. On the other hand, $(X_R^i)_7 = (X_L^{i-1})_7$. Hence, it is possible to use the correlation of the following linear relation to filter the wrong subkeys:

$$(X_L^{i-1})_7 \oplus F(X_L^{i-1})[6,8,10] \oplus X_R^{i-1})[6,8,10] \oplus (X_L^{i+11})_9 \oplus (X_R^{i+11})[6,10].$$

It means that we do not need to know the value of $(K^{i-1})[6,8,10]$ (in Table 5 such bits of key are indicated in red). We can continue our method to add more rounds to the beginning of linear characteristic in the cost of guessing some bits of subkeys. To add more rounds in backward, for example we must guess the bit $(F(X_L^{i-1}))_6 = (X_L^{i-1})_5 \oplus ((X_L^{i-1})_6 \& (X_L^{i-1})_1)$. Given that for any 2-bit AND gate if an input is 0 then the output would be 0, to determine $(F(X_L^{i-1}))_6$ one should guess

$(X_L^{i-1})_1$ only if the guessed value for $(X_L^{i-1})_6$ is 1, but it always should guess the value of $(X_L^{i-1})_5$ (this observation originally has been used in [1] to attack SIMON). So, in average we need one bit guess for $(X_L^{i-1})_6$ and $(X_L^{i-1})_1$ (in Table 5 such bits are indicated inblue).

Following this approach, Table 5 shows the bits of subkeys that should be guessed (31 bits of subkey in average) when we add 3 rounds at the top and 4 rounds at the bottom of the 11-round characteristic of Equation 8. Hence, we can attack 18 rounds of SIMMECK32/64 using Algorithm 2 of Matsui to recover bits of subkeys. For the data complexity of 2^{31} and the time complexity of $2^{63.5}$ the attack success probability would be 0.477 [19].

Table 5: The keys (in *black*) that should be guessed to attack 18 rounds of SIMECK32/64. The red bits are not required to be guessed and the blue bits cost guessing a half bit on average. Here $i \sim j$ denotes the sequence of numbers $i, i-1, \ldots, j+1, j$, LC is the core linear characteristic, BW is the rounds added at the top and FW is the rounds added at the bottom of the core linear characteristic and AGK denotes average guessed subkey-bits.

		$\mathcal{A}_L$	$\mathcal{A}_R$	active subkeys' bits	AGK.
BW	-2	15∼0	14,12,10∼0	14,12,10,8,6,3,1,9,7,5,4,2,0	$2^{9.5}$
	-1	14,12,10∼0	10∼5,3,1	9,7,10,8,5,6,3,1	2^3
	0	10∼5, 3,1	10, 8, 6	10, 8, 6	0
LC	1	10, 8, 6	7	-	-
	2	9, 9, 7	10, 8	-	-
	3	10, 8	9	-	-
	4	9	10	-	-
	5	10	–	-	-
	6	9	10	-	-
	7	10,8	9	-	-
	8	9, 9, 7	10, 8	-	-
	9	10, 8, 6	7	-	-
	10	7, 9,5, 7, 5	10, 8, 6	-	-
	11	10, 8, 6, 8	9	-	-
FW	13	10,9,6,5,1	10,6	10,6	0
	14	12,10∼8,6∼4,1,0	10,9,6,5,1	9,10,6,5,1	2^2
	15	15,12∼3,1,0	12,10∼8,6∼4,1,0	8,12,10,6,1,9,5,4,0	2^6
	16	15,14,12∼0	15,12∼3,1,0	12,7,15,11∼8,6∼3,1,0	2^{12}

Given Equation 10, as a linear characteristic for SIMECK48/96, is possible to apply the above technique to extend the linear characteristics over more number of rounds. However, the bias of that linear characteristic is 2^{-24}, which means that we can not use it to mount an attack with high success probability [17, 19]. Hence, we use Equation 15 which covers 15 rounds. Table 6 shows the bits of subkeys that should be guessed (49 bits of subkey in average) when we add 4 rounds at the top and 4 rounds at the bottom of the 15-round characteristic of Equation 15. Hence, we can attack 23 rounds

of SIMECK48/96 using Algorithm 2 of Matsui to recover bits of subkeys. For the data complexity of 2^{45} and the time complexity of 2^{94} the attack success probability would be 0.477 [19].

$$\begin{pmatrix} (X_R^1)_5 \oplus (X_L^1)[4,6,10] \\ \oplus (X_L^{16})_9 \oplus (X_R^{16})[6,10] \end{pmatrix} = \begin{pmatrix} (K^1)_5 \oplus (K^2)[6,10] \oplus (K^3)_9 \oplus (K^4)[6,8,10] \\ \oplus (K^5)_7 \oplus (K^6)[8,10] \oplus (K^7)_9 \oplus (K^8)_{10} \\ \oplus (K^{10})_{10} \oplus (K^{11})_9 \oplus (K^{12})[8,10] \oplus (K^{13})_7 \\ \oplus (K^{14})[6,8,10] \oplus (K^{15})_9 \end{pmatrix}, \tag{15}$$

Table 6: The keys (in *black*) that should be guessed to attack 23 rounds of SIMECK48/96. Notations are similar to the notations used in Table 5.

		$\mathcal{A}_L$	$\mathcal{A}_R$	active subkeys' bits	AGK.
BW	-3	23∼12,10∼0	23∼17,15,13,10∼0	7,20,18,15,13,23∼21,19,17,10∼8,6∼0	2^{17}
	-2	23∼17,15,13,10∼0	23,22,20,18,10∼8,6∼0	8,2,23,20,18,10,6,1,22,9,5,4,3,0	2^{9}
	-1	23,22,20,18,10∼8,6∼0	23,10,9,6∼3,1	9,3,23,10,6∼4,1	2^{3}
	0	23,10,9,6∼3,1	10,6,4	10,6,4	0
LC	1	10, 6,4	5	-	-
	2	9, 9, 5	10,6	-	-
	3	10, 8, 6, 8	9	-	-
	4	7, 9,5, 7, 5	10, 8, 6	-	-
	5	10, 8, 6	7	-	-
	6	9, 9, 7	10, 8	-	-
	7	10, 8	9	-	-
	8	9	10	-	-
	9	10	–	-	-
	10	9	10	-	-
	11	10,8	9	-	-
	12	9, 9, 7	10, 8	-	-
	13	10, 8, 6	7	-	-
	14	7, 9,5, 7, 5	10, 8, 6	-	-
	15	10, 8, 6, 8	9	-	-
FW	16	10,9,6,5,1	10,6	10,6	0
	17	20,10∼8,6∼4,1,0	10,9,6,5,1	9,10,6,5,1	2^{2}
	18	23,20,19,15,10∼3,1,0	20,10∼8,6∼4,1,0	8,20,10,6,1,9,5,4,0	2^{6}
	19	23,22,20∼18,15,14,10∼0	23,20,19,15,10∼3,1,0	7,20,15,23,19,10∼8,6∼3,1,0	2^{12}

Similarly, given Equation 12 with bias 2^{-30}, it is possible to apply this technique to extend the linear characteristics to 27 rounds of SIMECK64/128 (Table 7). To attack 27 rounds of SIMECK64/128, the data complexity is 2^{61}, the time complexity is $2^{120.5}$ and the attack success probability would be 0.477 [19].

5 Conclusion and Open Problems

In this paper, we analyzed the security of SIMECK family against linear cryptanalysis techniques. Our results show that each variant of SIMON provides better security against linear cryptanalysis compared to equivalent SIMECK variant. More precisely, the best known attack on SIMON32/64,

Table 7: The keys (in *black*) that should be guessed to attack 27 rounds of SIMECK64/128. Notations are similar to the notations used in Table 5.

		$\mathcal{A}_L$	$\mathcal{A}_R$	active subkeys' bits	AGK.
BW	-3	31∼20,18,16,10∼0	31∼25,23,21,10∼0	7,28,26,23,21,31∼29,27,25,10∼8,6∼0	2^{17}
	-2	31∼25,23,21,10∼0	31,30,28,26,10∼8,6∼0	8,2,31,28,26,10,6,1,30,9,5,4,3,0	2^{9}
	-1	31,30,28,26,10∼8,6∼0	31,10,9,6∼3,1	9,3,31,10,6∼4,1	2^{3}
	0	31,10,9,6∼3,1	10,6,4	10,6,4	0
LC	1	10, 6,4	5	-	-
	2	9, 9, 5	10,6	-	-
	3	10, 8, 6, 8	9	-	-
	4	7, 9,5, 7, 5	10, 8, 6	-	-
	5	10, 8, 6	7	-	-
	6	9, 9, 7	10, 8	-	-
	7	10, 8	9	-	-
	8	9	10	-	-
	9	10	–	-	-
	10	9	10	-	-
	11	10,8	9	-	-
	12	9, 9, 7	10, 8	-	-
	13	10, 8, 6	7	-	-
	14	7, 9,5, 7, 5	10, 8, 6	-	-
	15	10, 8, 6, 8	9	-	-
	16	9, 9, 5	10,6	-	-
	17	10, 6,4	5	-	-
	18	5,9,5,3	10, 6,4	-	-
	19	10, 6,4,8,4,2	9,3	-	-
FW	20	29,10∼5,3∼1	10,8,6,2	10,8,6,2	0
	21	30∼28,24,10∼0	29,10∼5,3∼1	9,7,3,29,10,8,6,5,2,1	$2^{3.5}$
	22	31∼27,24,23,19,10∼0	30∼28,24,10∼0	8,6,30,29,24,10,3,2,28,9,7,5,4,1,0	2^{10}
	23	31∼22,19,18,14,10∼0	31∼27,24,23,19,10∼0	30,24,19,7,31,29∼27,23,10∼8,6∼0	2^{17}

SIMON48/96 and SIMON64/128 using Mastui's algorithm 1 covers 13, 16 and 19 rounds respectively while our result on SIMECK32/64, SIMECK48/96, SIMECK64/128 covers 14, 19 and 22 rounds. Moreover, the best known attack on SIMON32/64, SIMON48/96 and SIMON64/128 using Mastui's algorithm 2 covers 18, 19 and 21 rounds respectively while our result on SIMECK32/64, SIMECK48/96, SIMECK64/128 covers 18, 23 and 27 rounds. Hence, in the perspective of linear cryptanalysis, SIMON provides better security margin compared to SIMECK.

On the other hand, from the point of number of rounds attacked, linear hull [18] shows to be a more promising approach to analyze the security of SIMON [1, 11, 20] compared to other attacks. Hence, as a future work, we aim to investigate the security of SIMECK variants against this attack.

References

1. M. A. Abdelraheem, J. Alizadeh, H. AlKhzaimi, M. R. Aref, N. Bagheri, P. Gauravaram, and M. M. Lauridsen. Improved linear cryptanalysis of round reduced SIMON. *IACR Cryptology ePrint Archive*, 2014:681, 2014.
2. F. Abed, E. List, S. Lucks, and J. Wenzel. Differential Cryptanalysis of Reduced-Round Simon. Cryptology ePrint Archive, Report 2013/526, 2013. `http://eprint.iacr.org/`.

3. F. Abed, E. List, S. Lucks, and J. Wenzel. Differential cryptanalysis of round-reduced simon and speck. In C. Cid and C. Rechberger, editors, *FSE 2014*, volume 8540 of *Lecture Notes in Computer Science*, pages 525–545. Springer, 2014.
4. J. Alizadeh, H. AlKhzaimi, M. R. Aref, N. Bagheri, P. Gauravaram, A. Kumar, M. M. Lauridsen, and S. K. Sanadhya. Cryptanalysis of SIMON variants with connections. In N. Saxena and A. Sadeghi, editors, *RFIDSec 2014*, volume 8651 of *Lecture Notes in Computer Science*, pages 90–107. Springer, 2014.
5. J. Alizadeh, N. Bagheri, P. Gauravaram, A. Kumar, and S. K. Sanadhya. Linear Cryptanalysis of Round Reduced SIMON. Cryptology ePrint Archive, Report 2013/663, 2013. `http://eprint.iacr.org/`.
6. H. AlKhzaimi and M. M. Lauridsen. Cryptanalysis of the SIMON Family of Block Ciphers. *IACR Cryptology ePrint Archive*, 2013:543, 2013.
7. T. Ashur. Improved linear trails for the block cipher simon. *IACR Cryptology ePrint Archive*, 2015:285, 2015.
8. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. `http://eprint.iacr.org/2013/404`.
9. A. Biryukov, A. Roy, and V. Velichkov. Differential analysis of block ciphers SIMON and SPECK. In C. Cid and C. Rechberger, editors, *FSE 2014*, volume 8540 of *Lecture Notes in Computer Science*, pages 546–570. Springer, 2014.
10. C. Boura, M. Naya-Plasencia, and V. Suder. Scrutinizing and improving impossible differential attacks: Applications to clefia, camellia, lblock and simon. In P. Sarkar and T. Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014*, volume 8873 of *Lecture Notes in Computer Science*, pages 179–199. Springer, 2014.
11. H. Chen and X. Wang. Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-guessing Techniques, 2015.
12. Z. Chen, N. Wang, and X. Wang. Impossible differential cryptanalysis of reduced round SIMON. *IACR Cryptology ePrint Archive*, 2015:286, 2015.
13. J. Y. Cho, M. Hermelin, and K. Nyberg. A New Technique for Multidimensional Linear Cryptanalysis with Applications on Reduced Round Serpent. In *ICISC*, pages 383–398, 2008.
14. N. Courtois, T. Mourouzis, G. Song, P. Sepehrdad, and P. Susil. Combined algebraic and truncated differential cryptanalysis on reduced-round simon. In M. S. Obaidat, A. Holzinger, and P. Samarati, editors, *SECRYPT 2014*, pages 399–404. SciTePress, 2014.
15. I. Dinur. Improved differential cryptanalysis of round-reduced speck. In A. Joux and A. M. Youssef, editors, *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, volume 8781 of *Lecture Notes in Computer Science*, pages 147–164. Springer, 2014.
16. J. N. Jr., B. Preneel, and J. Vandewalle. Linear Cryptanalysis of Reduced-Round Versions of the SAFER Block Cipher Family. In B. Schneier, editor, *FSE*, volume 1978 of *Lecture Notes in Computer Science*, pages 244–261. Springer, 2000.
17. M. Matsui. Linear Cryptoanalysis Method for DES Cipher. In T. Helleseth, editor, *EUROCRYPT*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1994.
18. K. Nyberg. Linear Approximation of Block Ciphers. In A. D. Santis, editor, *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 439–444. Springer, 1994.
19. A. A. Selçuk. On probability of success in linear and differential cryptanalysis. *J. Cryptology*, 21(1):131–147, 2008.
20. D. Shi, L. Hu, S. Sun, L. Song, K. Qiao, and X. Ma. Improved Linear (hull) Cryptanalysis of Round-reduced Versions of SIMON. *IACR Cryptology ePrint Archive*, 2014:973, 2014.
21. S. Sun, L. Hu, M. Wang, P. Wang, K. Qiao, X. Ma, D. Shi, L. Song, and K. Fu. Towards Finding the Best Characteristics of Some Bit-oriented Block Ciphers and Automatic Enumeration of (Related-key) Differential and Linear Characteristics with Predefined Properties. *IACR Cryptology ePrint Archive*, 2014:747, 2014.

22. S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song. Automatic security evaluation and (related-key) differential characteristic search: Application to simon, present, lblock, DES(L) and other bit-oriented block ciphers. In P. Sarkar and T. Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014*, volume 8873 of *Lecture Notes in Computer Science*, pages 158–178. Springer, 2014.
23. A. Tardy-Corfdir and H. Gilbert. A known plaintext attack of feal-4 and feal-6. In *CRYPTO*, pages 172–181, 1991.
24. N. Wang, X. Wang, K. Jia, and J. Zhao. Improved Differential Attacks on Reduced SIMON Versions. *IACR Cryptology ePrint Archive*, 2014:448, 2014.
25. Q. Wang, Z. Liu, K. Varici, Y. Sasaki, V. Rijmen, and Y. Todo. Cryptanalysis of Reduced-Round SIMON32 and SIMON48. In *Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings*, pages 143–160, 2014.
26. G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong. The Simeck family of lightweight block ciphers, 2015. To appear in the proceeding of the Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2015.