Linear Cryptanalysis of Round Reduced Variants of SIMON

Javad Alizadeh[1], Nasour Bagheri[2], Praveen Gauravaram[3], Abhishek Kumar[4], and Somitra Kumar Sanadhya[4]

[1] Information Systems and Security Lab. (ISSL), Electrical Eng. Department, Sharif University of Technology, Iran, alizadja@gmail.com
[2] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Iran, NBagheri@srttu.edu
[3] Innovation Labs Hyderabad, Tata Consultancy Services Limited, India, P.Gauravaram@tcs.com
[4] Indraprastha Institute of Information Technology, Delhi, India, abhishek1101,Somitra@iiitd.ac.in

Abstract. SIMON [3] is a family of lightweight block ciphers which has been recently proposed by U.S National Security Agency (NSA). Round reduced versions of SIMON has undergone interesting analysis recently [1,2]. In this paper we investigate the security of this family of block ciphers against linear cryptanalysis. We present several linear characteristics for all variants of SIMON. Our best linear characteristic covers SIMON 32/64 reduced to 13 rounds out of 32 rounds with the bias 2^{-16}. In addition we present attacks for the round reduced variants of SIMON48/96, SIMON64/128, SIMON96/144 and SIMON128/256. Our results are the best known results on linear cryptanalysis for any variant of SIMON.

keywords: SIMON, Linear Characteristic, Linear Cryptanalysis.

1 Introduction

SIMON is a family of lightweight block ciphers designed by the NSA to provide an optimal hardware performance [3]. In order to meet hardware implementation flexibility (efficient implementations across wide variety of platforms as well as several implementations on a single platform), SIMON was designed to support block sizes of 32, 48, 64, 96 and 128 bits, with up to three key sizes for each block size. SIMON $|P|/|K|$ denotes a variant of SIMON that has the plaintext block length of size P and the key size of length K. For example, SIMON 32/64 refers to one variant of SIMON with 32-bit plaintext block and 64-bit key. Like this there are overall 10 variants of SIMON forming a family of lightweight block ciphers (see Table 2).

In this paper we investigate the security of SIMON family against linear cryptanalysis. We present linear characteristics for different variants of SIMON that can be used to attack reduced round versions of these ciphers. Our results cover more rounds, for any variant of the cipher, compared to the known results on the linear cryptanalysis of SIMON [1]. The summary of the results and the comparison with the results of Abed *et. al.* [1] are given in Table 1. The comparison shows that our results covers more number of rounds for the same success probability and also comparable data complexity.

The paper is structured as follows: In section 2 we present a brief description of SIMON family. In section 3 we present the idea of linear attack on SIMON and apply it to the SIMON32/64. Section 4 extends the attack to the other variants of SIMON. Finally, we conclude the paper in section 5

Table 1. Comparison of our results with the previous results when the success probability of key recovery attack is 0.997.

	Variant of SIMON	32/64	48/96	64/128	96/144	128/256
This work	# rounds with $\epsilon \geq 2^{-\frac{\lfloor p \rfloor}{2}+2}$	10	13	17	26	33
	# rounds attacked	12	15	19	28	35
	# approximation	13	19	28	44	59
	Data Complexity	2^{31}	2^{43}	2^{61}	2^{93}	2^{123}
Abed *et. al.* [1]	# rounds with $\epsilon \geq 2^{-\frac{\lfloor p \rfloor}{2}+2}$	9	12	14	18	21
	# rounds attacked	11	14	16	20	23
	# approximation	10	21	28	45	60
	Data Complexity	2^{25}	2^{47}	2^{61}	2^{95}	2^{125}

2 SIMON family

SIMON has a classical Feistel structure (see Figure 1) with the round block size of $2n$ bits, where n word size. The number of rounds of cipher is denoted by r and depends on the variant. In addition, we denote the right part and the left part of the plaintext P by P_R and P_L respectively. Similarly, we denote the right part and the left part of the ciphertext C by C_R and C_L respectively. The output of round r is denoted by $X^r = X_R^r \| X_L^r$ and the subkey used in round r is denoted by K^r. Given an string X, $(X)_i$ denotes the i-th bit of X.

Each round of SIMON includes a non-linear and non-invertible function F (see Figure 2). The F function is an n-bit to n-bit function. Given $X \in \{0,1\}^n$, $F(X)$ is calculated as follows:

$$F(X) = (X \lll 2) \oplus ((X \lll 1) \& (X \lll 8))$$

where "$a \lll b$" denotes the bitwise rotation of string b to the left a times and "&" denotes bitwise AND operation. Given an $2n$-bit internal state, the input of the F-function is the left half of the internal state and its output is directly exored by the right half of the internal state and a subkey. The subkeys are driven from an master key. Depending on the size of the master key, the key schedule of SIMON operates on two, three or four n-bit word registers. Assuming that the number of words for the master key K is m (see Table 2), the first m subkeys are directly driven from K, i.e., $K^0, \ldots, K^{m-1}$. The subkey for round i, for $m \leq i \leq r-1$, is calculated as follows:

$$\left.\begin{array}{ll} m=2: & K^i = K^{i-2} \oplus (K^{i-1} \ggg 3) \oplus (K^{i-1} \ggg 4) \oplus c \oplus (Z_j)_{i-m}, \\ m=3: & K^i = K^{i-3} \oplus (K^{i-1} \ggg 3) \oplus (K^{i-1} \ggg 4) \oplus c \oplus (Z_j)_{i-m}, \\ m=4: & K^i = K^{i-4} \oplus K^{i-3} \oplus (K^{i-1} \ggg 3) \oplus ((K^{i-3} \oplus (K^{i-1} \ggg 3)) \ggg 1) \oplus c \oplus (Z_j)_{i-m}. \end{array}\right\} \quad (1)$$

where, "$a \ggg b$" denotes the bitwise rotation of string a to the right b times, $c = (2^n - 1) \oplus 3 = 0xFF \ldots FFC$ is a constant value, $(Z_j)_{i-m}$ denotes the i^{th} bit of Z_j and $i-m$ is taken module 62. Z_j are five constant sequence $Z_0, \ldots, Z_4$ depicted in Table 3 and j is a parameter of the cipher (see Table 2).

Table 2. Detailes of variants of SIMON

Variant	Block size	Key size	Number of rounds	n	m	j
SIMON32/64	32	64	32	16	4	0
SIMON48/72	48	72	36	24	3	0
SIMON48/96	48	96	36	24	4	1
SIMON64/96	64	96	42	32	3	2
SIMON64/128	64	128	44	32	4	3
SIMON96/92	96	92	52	48	2	2
SIMON96/144	96	144	54	48	3	3
SIMON128/128	128	128	68	64	2	2
SIMON128/192	128	192	69	64	3	3
SIMON128/256	128	256	72	64	4	4

Table 3. Five constant sequence of Z_j

j	Z_j
0	11111010001001010110000111001101111101000100101011000011100110
1	10001110111110010011000010110101000111011111001001100001011010
2	10101111011100000011010010011000101000010001111110010110110011
3	11011011101011000110010111100000010010001010011100110100001111
4	11010001111001101011011000100000010111000011001010010011101111

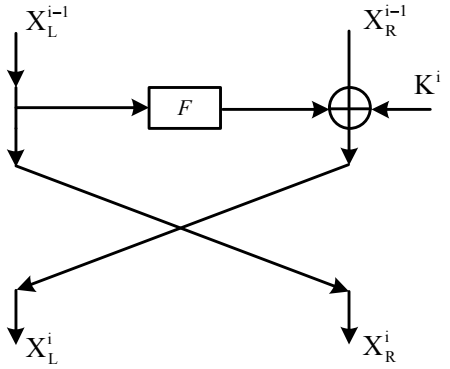

Fig. 1. A round function of SIMON.

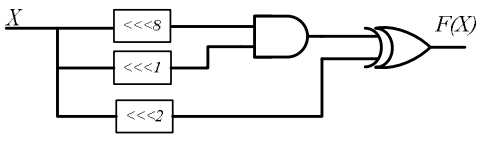

Fig. 2. A round function of SIMON.

3 Linear Cryptanalysis of SIMON 32/64

Linear cryptanalysis [4] is a known plaintext attack that tries to find a high probable linear expressions involving "plaintext" bits, "ciphertext" bits and the "subkey" bits as follows:

$$\oplus_{i=1}^{m} P_{pi} \oplus_{i=1}^{m} C_{ci} = \oplus_{i=1}^{m} K_{ki}$$

for $0 \leq pi \leq |P| - 1$, $0 \leq ci \leq |C| - 1$ and $0 \leq ki \leq |K| - 1$, and P, C and K represents plaintext, ciphertext and key respectively. In this attack, the attacker has no way to select which plaintexts (and corresponding ciphertexts) are available, which is a reasonable assumption in many applications and scenarios. In this paper we use this technique to analyze SIMON family of block ciphers. So far the only result on linear cryptanalysis of SIMON is results published by [1], which for SIMON 32/64 they have attack on 11-rounds for which the bias is 2^{-11}.

The round function of SIMON can be represented as follows:

$$\left.\begin{array}{ll} X_L^r = F(X_L^{r-1}) \oplus X_R^{r-1} \oplus K^r \\ X_R^r = \qquad\qquad X_L^{r-1} \end{array}\right\} \tag{2}$$

where $(F(X))_i = (X)_{i-2} \oplus ((X)_{i-1} \& (X)_{i-8})$ and addition calculations perform mode n. On the other hand, given single bits A and B, the output of $A \& B$ would be "0" with the probability of 0.75. Hence, we can extract the following highly biased linear expressions for F-function:

$$\left.\begin{array}{ll} \textit{Approximation } 1: & Pr[(F(X))_i = (X)_{i-2}] = \frac{3}{4} \\ \textit{Approximation } 2: & Pr[(F(X))_i = (X)_{i-2} \oplus (X)_{i-1}] = \frac{3}{4} \\ \textit{Approximation } 3: & Pr[(F(X))_i = (X)_{i-2} \oplus (X)_{i-8}] = \frac{3}{4} \\ \textit{Approximation } 4: & Pr[(F(X))_i = (X)_{i-2} \oplus ((X)_{i-1} \oplus (X)_{i-8})] = \frac{1}{4} \end{array}\right\} \tag{3}$$

Given Equations 2 and 3 we can extract the following linear expression for the first round of the SIMON:

$$(P_R)_2 \oplus (K^1)_2 \oplus (X_L^1)_2 = (P_L)_0 \tag{4}$$

which holds with the probability of $\frac{3}{4}$. Given the above expression, we can extract a 3-round linear expression as follows (see Fig. 3):

$$(X_R^{i-1})_2 \oplus (K^i)_2 \oplus (X_L^{i-1})_0 = (X_R^{i+2})_0 \oplus (K^{i+2})_2 \oplus (X_L^{i+2})_2 \tag{5}$$

It is possible to use Equation 5 to produce a 7-round linear expression as follows (see Fig. 4):

$$\begin{array}{c} (X_R^{i-1})_2 \oplus (K^i)_2 \oplus (X_L^{i-1})_0 \oplus (X_R^{i+2})_0 \oplus (K^{i+2})_2 \oplus (X_L^{i+2})_2 \ = \\ (X_R^{i+3})_2 \oplus (K^{i+4})_2 \oplus (X_L^{i+3})_0 \oplus (X_R^{i+6})_0 \oplus (K^{i+6})_2 \oplus (X_L^{i+6})_2 \end{array} \tag{6}$$

which can be simplified as follows:

$$\begin{array}{c} (X_R^{i-1})_2 \oplus (K^i)_2 \oplus (X_L^{i-1})_0 \oplus (K^{i+2})_2 \oplus F(X_L^{i+2})_0 \oplus (K^{i+3})_0 = \\ (K^{i+4})_2 \oplus (X_R^{i+6})_0 \oplus (K^{i+6})_2 \oplus (X_L^{i+6})_2 \end{array} \tag{7}$$

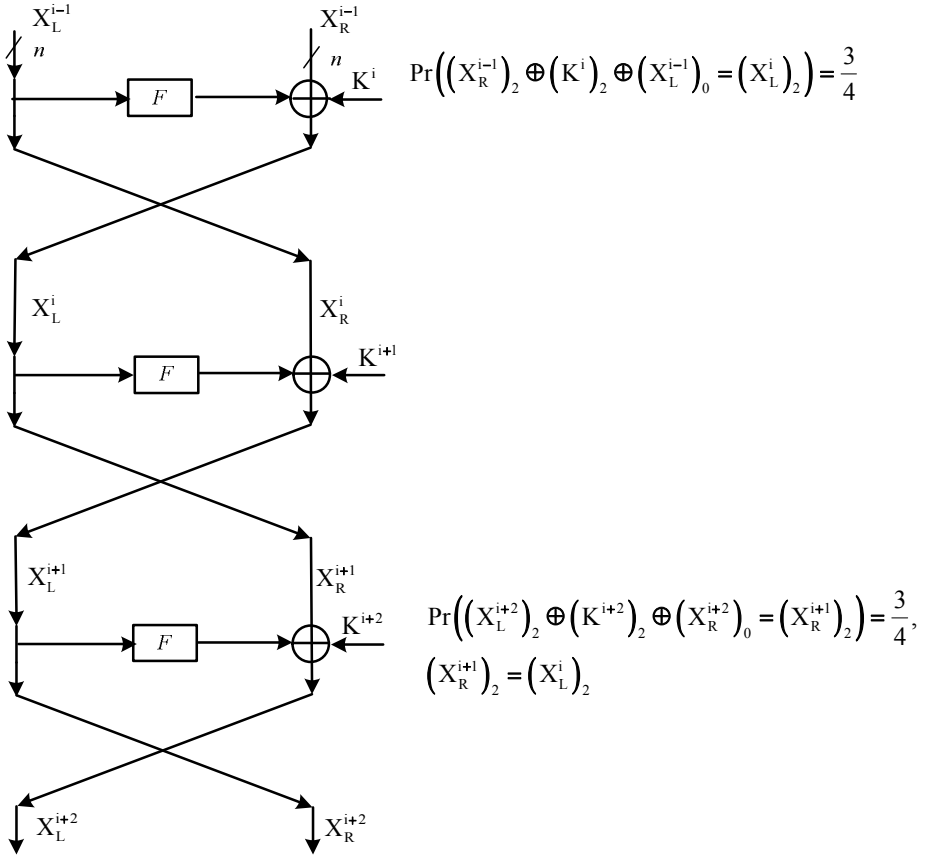

Fig. 3. A 3-round linear characteristic for SIMON.

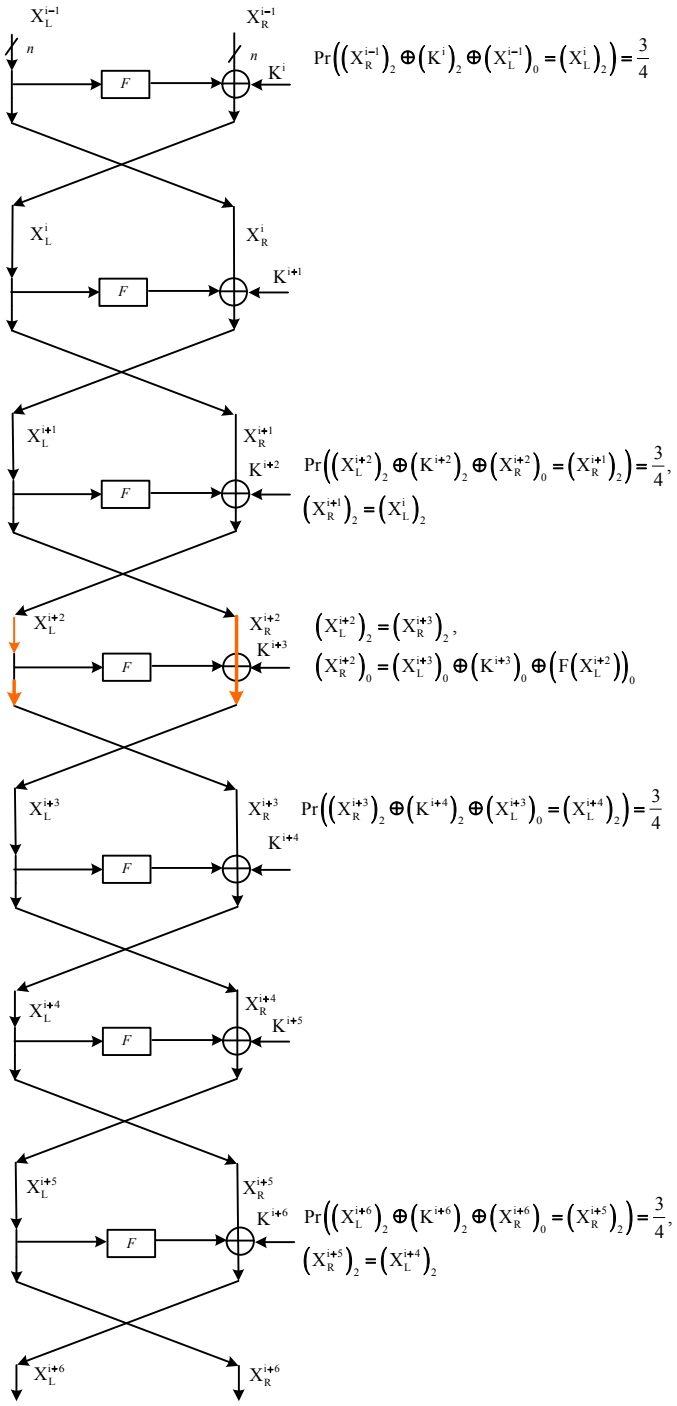

Fig. 4. A 7-round linear characteristic for SIMON.

Table 4. The biases for a 11-round linear characteristic

Bias of 7 round linear expression	2^{-10}
Bias of $F(X_L^{i+6})_0$ approximate	2^{-6}
Bias of approximate 7-11	2^{-3}

In Equation 7, the only intermediate value is the term $F(X_L^{i+2})_0$. We can approximate $F(X_L^{i+2})_0$ with some bits of plaintext (Considering Fig. 4):

$$\left.\begin{array}{l} Pr[F(X_L^{i+2})_0 = (X_L^{i+2})_{14})] = \frac{3}{4} \\ Pr[(X_L^{i+2})_{14} = (X_R^{i+1})_{14} \oplus (K^{i+2})_{14} \oplus (X_L^{i+1})_{12})] = \frac{3}{4} \\ Pr[(X_R^{i+1})_{14} = (X_R^{i-1})_{14} \oplus (K^{i})_{14} \oplus (X_L^{i-1})_{12}] = \frac{3}{4} \\ Pr[(X_L^{i+1})_{12} = (X_L^{i-1})_{12} \oplus (K^{i+1})_{12} \oplus (X_L^{i})_{10}] = \frac{3}{4} \\ Pr[(X_L^{i})_{10} = (X_R^{i-1})_{10} \oplus (K^{i})_{10} \oplus (X_L^{i-1})_{8}] = \frac{3}{4} \end{array}\right\}. \tag{8}$$

Then

$$F(X_L^{i+2})_0 = (X_R^{i-1})_{14} \oplus (K^i)_{14} \oplus (X_L^{i-1})_{12} \oplus (K^{i+2})_{14} \oplus (X_R^i)_{12} \oplus (K^{i+1})_{12} \oplus (X_R^{i-1})_{10} \oplus (K^i)_{10} \oplus (X_L^{i-1})_8 \tag{9}$$

with probability $(3/4)^5$ and bias 2^{-6}. Using Equation 9 in Equation 7, we can extract a 7 round linear expression with bias 2^{-10}. It is possible to use Equation 7 and produce a 11-round linear expression as follows (see Fig. 5):

$$\begin{array}{c} (X_R^{i-1})_2 \oplus (K^i)_2 \oplus (X_L^{i-1})_0 \oplus (K^{i+2})_2 \oplus F(X_L^{i+2})_0 \oplus (K^{i+3})_0 = \\ (K^{i+4})_2 \oplus (X_R^{i+6})_0 \oplus (K^{i+6})_2 \oplus (X_L^{i+6})_2 \end{array} \tag{10}$$

where,

$$\left.\begin{array}{l} (X_L^{i+6})_2 = (X_R^{i+7})_2 \\ (X_R^{i+6})_0 = (X_L^{i+7})_0 \oplus (K^{i+7})_0 \oplus F(X_L^{i+6})_0 \\ Pr[(X_L^{i+8})_2 = (X_R^{i+7})_2 \oplus (K^{i+8})_2 \oplus (X_L^{i+7})_0] = \frac{3}{4} \\ Pr[(X_R^{i+9})_2 = (X_L^{i+10})_2 \oplus (K^{i+10})_2 \oplus (X_R^{i+10})_0] = \frac{3}{4} \end{array}\right\}. \tag{11}$$

Thus, Equation 12 will be a 11-round linear expression with bias 2^{-17} (We note that similar to $F(X_L^{i+2})_0$, we can approximate $F(X_L^{i+6})_0$ with some bits of X^{i+10} with probability $(3/4)^5$ and bias 2^{-6}). The bias is calculated using biases given in Table 4 and the pilling up lemma.

$$\begin{array}{c} (X_R^{i-1})_2 \oplus (K^i)_2 \oplus (X_L^{i-1})_0 \oplus (K^{i+2})_2 \oplus F(X_L^{i+2})_0 \oplus (K^{i+3})_0 = \\ (K^{i+4})_2 \oplus (K^{i+7})_0 \oplus (K^{i+6})_2 \oplus F(X_L^{i+6})_0 \oplus (K^{i+8})_2 \oplus (X_L^{i+10})_2 \oplus (K^{i+10})_2 \oplus (X_R^{i+10})_0 \end{array} \tag{12}$$

Unfortunately this linear expression can't yield a successful linear attack because the required number of data exceeds the possible values, i.e. 2^{32}. Although we will introduce a

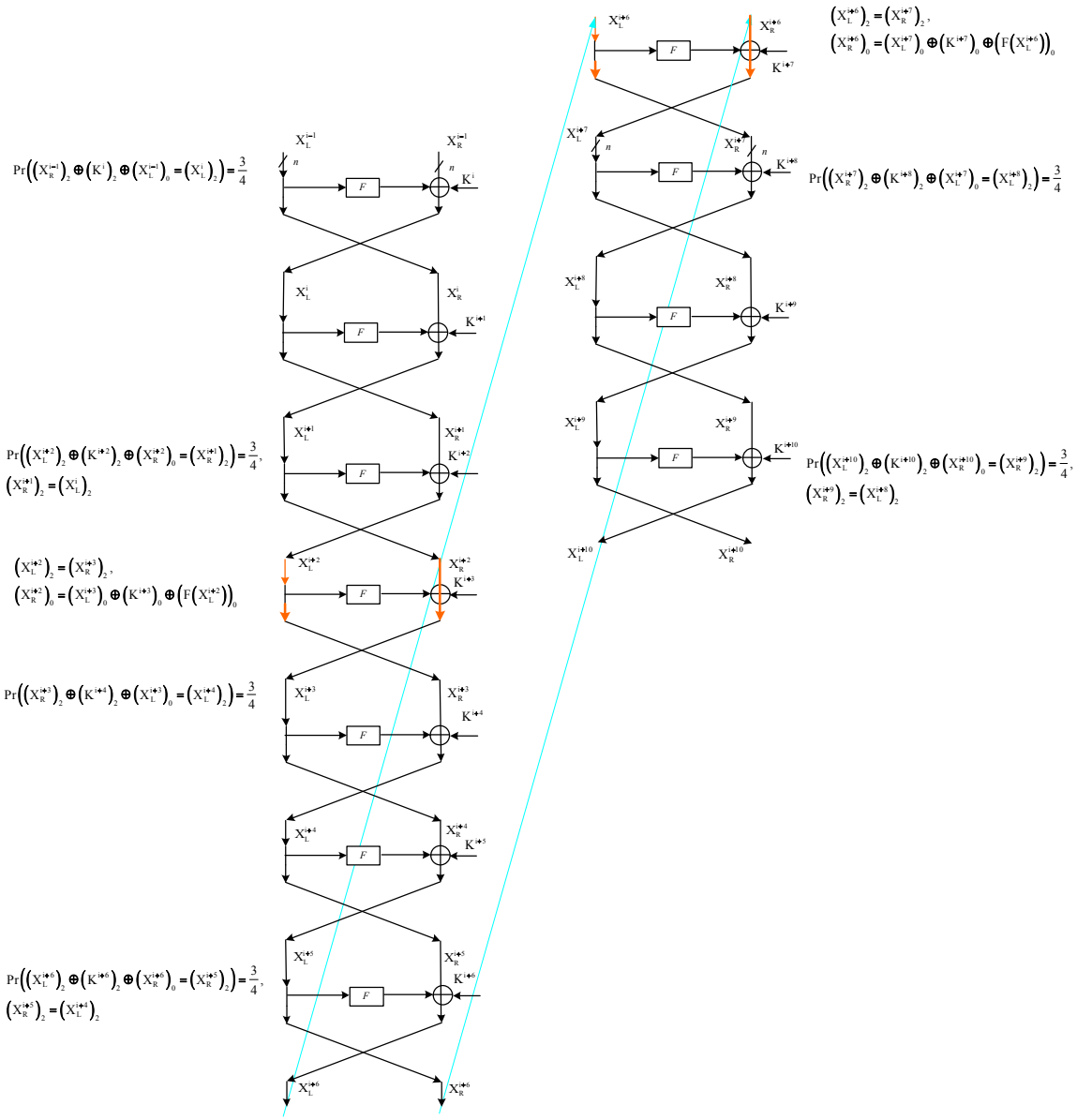

Fig. 5. A 11-round linear characteristic for SIMON.

Table 5. The biases for a 10-round linear characteristic

Bias of 7 round linear expression	2^{-10}
Bias of $F(X_L^{i+6})_0$ approximate	2^{-4}
Bias of approximate 7-10	2^{-2}

11-round linear expression with bias 2^{-16} later, but in this section we use the above method and calculate a 10-round linear expression. The biases of the 10-round linear characteristic is given in Table 5 and the expression is as follows:

$$\begin{array}{r} (X_R^{i-1})_2 \oplus (K^i)_2 \oplus (X_L^{i-1})_0 \oplus (K^{i+2})_2 \oplus F(X_L^{i+2})_0 \oplus (K^{i+3})_0 \quad = \\ (K^{i+4})_2 \oplus (K^{i+7})_0 \oplus (K^{i+6})_2 \oplus F(X_L^{i+6})_0 \oplus (K^{i+8})_2 \oplus (X_R^{i+9})_2, \end{array} \tag{13}$$

where approximate of $F(X_L^{i+6})_0$ is as follows:

$$\left.\begin{array}{l} Pr[F(X_L^{i+6})_0 = (X_L^{i+6})_{14}] = \frac{3}{4} \\ Pr[(X_L^{i+6})_{14} = (K^{i+8})_{14} \oplus (X_R^{i+8})_{12} \oplus (X_R^{i+9})_{14}] = \frac{3}{4} \\ Pr[(X_R^{i+8})_{12} = (X_L^{i+9})_{12} \oplus (K^{i+9})_{12} \oplus (X_L^{i+8})_{10} = \\ \qquad\qquad (X_L^{i+9})_{12} \oplus (K^{i+9})_{12} \oplus (X_R^{i+9})_{10}] = \frac{3}{4} \end{array}\right\}. \tag{14}$$

Hence, the approximation of $F(X_L^{i+6})_0$ can be simplified as follows, with bias 2^{-4}:

$$F(X_L^{i+6})_0 = (K^{i+8})_{14} \oplus (X_L^{i+9})_{12} \oplus (K^{i+9})_{12} \oplus (X_R^{i+9})_{10} \oplus (X_R^{i+9})_{14} \tag{15}$$

Then the 10-round linear expression simplified as follows:

$$\begin{array}{l} (X_R^{i-1})_2 \oplus (K^i)_2 \oplus (X_L^{i-1})_0 \oplus (K^{i+2})_2 \oplus (X_R^{i-1})_{14} \oplus (K^i)_{14} \oplus \\ (K^{i+2})_{14} \oplus (K^{i+1})_{12} \oplus (X_R^{i-1})_{10} \oplus (K^i)_{10} \oplus (X_L^{i-1})_8 \oplus (K^{i+3})_0 = \\ (K^{i+4})_2 \oplus (K^{i+7})_0 \oplus (K^{i+6})_2 \oplus (K^{i+8})_{14} \oplus (X_L^{i+9})_{12} \oplus (K^{i+9})_{12} \\ \oplus (X_R^{i+9})_{10} \oplus (X_R^{i+9})_{14} \oplus (K^{i+8})_2 \oplus (X_R^{i+9})_2 \end{array} \tag{16}$$

3.1 13-Round Linear Characteristic

In this section we get some 11-round linear expressions for SIMON 32/64. In addition we can add another round to the beginning and a round to the end of each characteristic, that are related to plaintext and ciphertext free of any approximation, because we know the input of F function for this rounds. In this way we receive a 13-round linear characteristic for SIMON 32/64.

METHOD 1: We can consider the 10-round linear expression in previous section and add a single round at its beginning to achieve a 11-round characteristic. In this case we have

these changes:

$$\left.\begin{array}{l}(X_R^{i-1})_2 = (X_L^{i-2})_2 \\ Pr[(X_L^{i-1})_0 = (X_R^{i-2})_0 \oplus (K^{i-1})_0 \oplus (X_L^{i-2})_{14}] = \frac{3}{4} \\ (X_R^{i-1})_{14} = (X_L^{i-2})_{14} \\ (X_R^{i-1})_{10} = (X_L^{i-2})_{10} \\ Pr[(X_L^{i-1})_8 = (X_R^{i-2})_8 \oplus (K^{i-1})_8 \oplus (X_L^{i-2})_6] = \frac{3}{4}\end{array}\right\}. \tag{17}$$

Hence bias of added round is 2^{-3} and the bias of the 11-round linear expression is 2^{-16}.

METHOD 2: In this method we begin of X_R^{i+3} and X_L^{i+3} and backward to X_R^{i-1} and X_L^{i-1}:

$$\left.\begin{array}{l}(X_R^{i+3})_2 = (X_L^{i+2})_2 \\ Pr[(X_L^{i+3})_0 = (X_R^{i+2})_0 \oplus (K^{i+3})_0 \oplus (X_L^{i+2})_{14}] = \frac{3}{4} \\ Pr[(X_L^{i+2})_2 = (X_R^{i+1})_2 \oplus (K^{i+2})_2 \oplus (X_L^{i+1})_0] = \frac{3}{4} \\ (X_R^{i+2})_0 = (X_L^{i+1})_0 \\ Pr[(X_L^{i+2})_{14} = (X_R^{i+1})_{14} \oplus (K^{i+2})_{14} \oplus (X_L^{i+1})_{12}] = \frac{3}{4} \\ (X_R^{i+1})_2 = (X_L^{i})_2 \\ Pr[(X_L^{i+1})_0 = (X_R^{i})_0 \oplus (K^{i+1})_0 \oplus (X_L^{i})_{14}] = \frac{3}{4} \\ (X_R^{i+1})_{14} = (X_L^{i})_{14} \\ Pr[(X_L^{i+1})_{12} = (X_R^{i})_{12} \oplus (K^{i+1})_{12} \oplus (X_L^{i})_{10}] = \frac{3}{4} \\ Pr[(X_L^{i})_2 = (X_R^{i-1})_2 \oplus (K^{i})_2 \oplus (X_L^{i-1})_0] = \frac{3}{4}\ (*) \\ (X_R^{i})_0 = (X_L^{i-1})_0 \\ Pr[(X_L^{i})_{14} = (X_R^{i-1})_{14} \oplus (K^{i})_{14} \oplus (X_L^{i-1})_{12}] = \frac{3}{4}\ (**) \\ (X_R^{i})_{12} = (X_L^{i-1})_{12} \\ Pr[(X_L^{i})_{10} = (X_R^{i-1})_{10} \oplus (K^{i})_{10} \oplus (X_L^{i-1})_8] = \frac{3}{4}\ (***)\end{array}\right\}. \tag{18}$$

If we assume that with control of plaintext bits, we can establish 3 relations *, **, and ***, the 4-round linear expression will have bias 2^{-6}.

Now we can attach the 3-round linear expression $(X_R^{i+3})_2 \oplus (K^{i+4})_2 \oplus (X_L^{i+3})_0 = (X_R^{i+6})_0 \oplus (K^{i+6})_2 \oplus (X_L^{i+6})_2$ with bias 2^{-3} to the 4-round linear expression and get a 7-round linear expression with bias 2^{-8} . Then we add another 4-round linear expression that begin of

$(X_R^{i+6})_0$ and $(X_L^{i+6})_2$ to the 7-round linear expression. This new 4-round linear expression is:

$$\left.\begin{array}{l}(X_L^{i+6})_2 = (X_R^{i+7})_2\\ Pr[(X_R^{i+6})_0 = (X_L^{i+7})_0 \oplus (K^{i+7})_0 \oplus (X_L^{i+6})_{14}] = \frac{3}{4}\\ Pr[(X_R^{i+7})_2 = (X_L^{i+8})_2 \oplus (K^{i+8})_2 \oplus (X_L^{i+7})_0] = \frac{3}{4}\\ (X_L^{i+7})_0 = (X_R^{i+8})_0\\ Pr[(X_L^{i+6})_{14} = (X_L^{i+8})_{14} \oplus (K^{i+8})_{14} \oplus (X_L^{i+7})_{12}] = \frac{3}{4}\\ (X_L^{i+8})_2 = (X_R^{i+9})_2\\ Pr[(X_R^{i+8})_0 = (X_L^{i+9})_0 \oplus (K^{i+9})_0 \oplus (X_R^{i+9})_{14}] = \frac{3}{4}\\ (X_L^{i+8})_{14} = (X_R^{i+9})_{14}\\ Pr[(X_L^{i+7})_{12} = ((X_L^{i+9})_{12} \oplus (K^{i+9})_{12} \oplus (X_R^{i+9})_{10}] = \frac{3}{4}\\ Pr[(X_R^{i+9})_2 = (X_L^{i+10})_2 \oplus (K^{i+10})_2 \oplus (X_R^{i+10})_0] = \frac{3}{4}\\ (X_L^{i+9})_0 = (X_R^{i+10})_0\\ Pr[(X_R^{i+9})_{14} = (X_L^{i+10})_{14} \oplus (K^{i+10})_{14} \oplus (X_R^{i+10})_{12}] = \frac{3}{4}\\ (X_L^{i+9})_{12} = (X_R^{i+10})_{12}\\ Pr[(X_R^{i+9})_{10} = (X_L^{i+10})_{10} \oplus (K^{i+10})_{10} \oplus (X_R^{i+10})_8] = \frac{3}{4}\end{array}\right\}. \quad (19)$$

This expression has bias 2^{-9}. So we have a 11-round linear expression of bias 2^{-16}.

METHOD 3: In this method we begin of $(X_R^{i+3})_2$ and $(X_L^{i+3})_0$ and use a 7-round linear expression (see equation 6):

$$\begin{array}{c}(X_R^{i+3})_2 \oplus (K^{i+4})_2 \oplus (X_L^{i+3})_0 \oplus (K^{i+6})_2 \oplus F(X_L^{i+6})_0 \oplus (K^{i+7})_0 =\\ (K^{i+8})_2 \oplus (X_R^{i+10})_0 \oplus (K^{i+10})_2 \oplus (X_L^{i+10})_2.\end{array} \quad (20)$$

Then we add the 4-round linear expression that we get in method 2 at first of the 7-round linear expression and provide a 11-round linear expression with bias 2^{-15} (2^{-6} of first 4-round linear expression and 2^{-10} of second 7-round linear expression). Note that we can approximate $F(X_L^{i+6})_0$ with some bits of X^{i+10} with bias 2^{-6}:

$$\left.\begin{array}{l}Pr[F(X_L^{i+6})_0 = (X_L^{i+6})_{14}] = \frac{3}{4}\\ Pr[(X_L^{i+6})_{14} = (K^{i+8})_{14} \oplus (X_R^{i+8})_{12} \oplus (X_R^{i+9})_{14}] = \frac{3}{4}\\ Pr[(X_R^{i+8})_{12} = (X_R^{i+10})_{12} \oplus (K^{i+9})_{12} \oplus (X_R^{i+9})_{10}] = \frac{3}{4}\\ Pr[(X_R^{i+9})_{14} = (X_L^{i+10})_{14} \oplus (K^{i+10})_{14} \oplus (X_R^{i+10})_{12}] = \frac{3}{4}\\ Pr[(X_R^{i+9})_{10} = (X_L^{i+10})_{10} \oplus (K^{i+10})_{10} \oplus (X_R^{i+10})_8] = \frac{3}{4}\end{array}\right\} \quad (21)$$

It is possible to use equation 7 to produce a 15-round linear expression as follows (see Fig. 6):

$$\begin{array}{c}(X_R^{i-1})_2 \oplus (K^i)_2 \oplus (X_L^{i-1})_0 \oplus (K^{i+2})_2 \oplus\\ F(X_L^{i+2})_0 \oplus (K^{i+3})_0 \oplus (K^{i+4})_2 \oplus (X_R^{i+6})_0 \oplus (K^{i+6})_2 \oplus (X_L^{i+6})_2 =\\ (X_R^{i+7})_2 \oplus (K^{i+8})_2 \oplus (X_L^{i+7})_0 \oplus (K^{i+10})_2 \oplus F(X_L^{i+10})_0 \oplus\\ (K^{i+11})_0 \oplus (K^{i+12})_2 \oplus (X_R^{i+14})_0 \oplus (K^{i+14})_2 \oplus (X_L^{i+14})_2\end{array} \quad (22)$$

which can be simplified as follows:

$$\begin{gathered}(X_R^{i-1})_2 \oplus (K^i)_2 \oplus (X_L^{i-1})_0 \oplus (K^{i+2})_2 \oplus F(X_L^{i+2})_0 \oplus (K^{i+3})_0 \oplus (K^{i+4})_2 \oplus (K^{i+6})_2 = \\ F(X_L^{i+6})_0 \oplus (K^{i+7})_0 \oplus (K^{i+8})_2 \oplus (K^{i+10})_2 \oplus \\ F(X_L^{i+10})_0 \oplus (K^{i+11})_0 \oplus (K^{i+12})_2 \oplus (X_R^{i+14})_0 \oplus (K^{i+14})_2 \oplus (X_L^{i+14})_2\end{gathered} \tag{23}$$

In Equation 23, the only intermediate values are the term $F(X_L^{i+2})_0, F(X_L^{i+6})_0$ and $F(X_L^{i+10})_0$. This approach can repeated to extend the number of rounds of the linear characteristic.

3.2 Other Linear Characteristics for SIMON

In Fig. 7 and Fig. 8 two distinct 3-round linear characteristic are depicted. The interesting point of these characteristic is that they can be combined to receive a characteristic for extra rounds which does not include any intermediate value. For example concatenating these figs gives a 6-round characteristic that includes the input, output and several sub-keys bits. However, the probability of such characteristic is expected to be $\frac{1}{2} + 2^{-17}$. If we extend the number of rounds to 9-rounds then the probability of such characteristic is expected to be $\frac{1}{2} + 2^{-25}$. Although such characteristic can not be used to recover the key but maybe considered as a distinguisher for the reduced cipher. It must be noted that this distinguisher is expendable to any variant of SIMON.

4 Linear attack on the other variants of SIMON

In this section we investigate the strength of different variants of SIMON against linear attack. We use the simple approximation of AND operation through this section also. In Tables 8, 9, 10, 11 and 12 the propagation of our linear characteristics for SIMON32/64, SIMON48/96, SIMON64/128, SIMON96/192 and SIMON128/256 are presented respectively (for the detaile of each used approximation see equation 3). In Tables 11 and 12 we used the approach of Abed *et. al.* [1, Table 5] for producing their differential characteristic as the main core of the presented paths. The significant of this approach is that any progress on providing a better differential characteristic may be directly used to provide a better linear characteristic. It is clear from these Tables that the propagation of number of required approximation in our characteristics are far better than the pattern presented by Abed *et. al.* [1], which is as follows, exclude for SIMON32/64 that we have a same pattern as theirs (as far as they have included in the paper):

$$\ldots; 3; 1; 2; 1; 1; 0; 1; 1; 2; 1; 3; \ldots$$

On the other hand, for SIMON32/64 reduce to 11 rounds a linear characteristics based on the Abed *et. al.* [1] approach will have bias of 2^{-17}. However, we considered the propagation of number of approximations for this variant of SIMON on more rounds and received the following pattern, see Table 8:

$$\ldots; 1; 2; 1; 3; 2; 3; 1; 2; 1; 1; 0; 1; 1; 2; 1; 3; 2; 3; 1; 2; 1; 1; 0; 1; 1; 2; 1; 3; 2; 3 \ldots$$

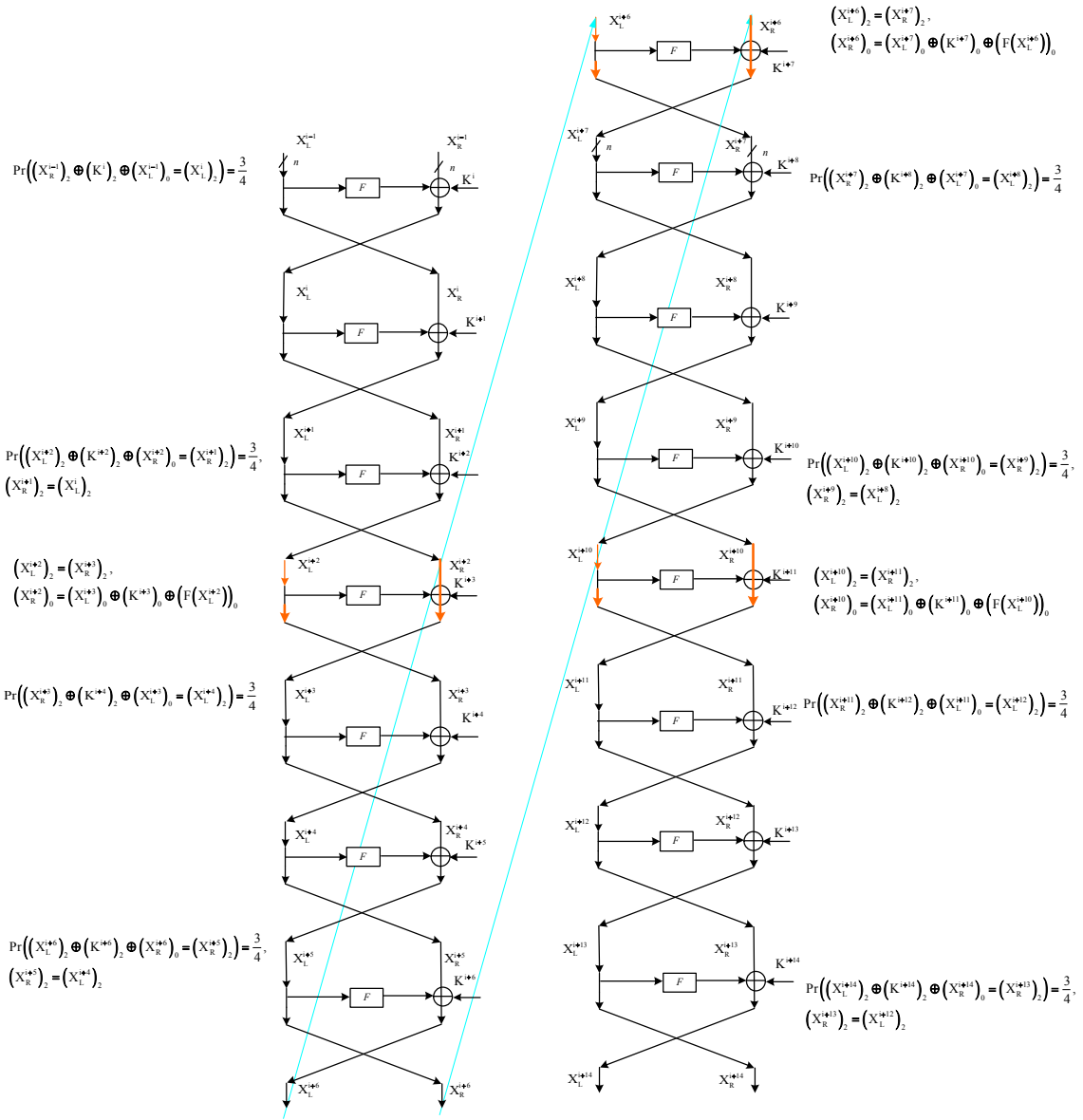

Fig. 6. A 15-round linear characteristic for SIMON.

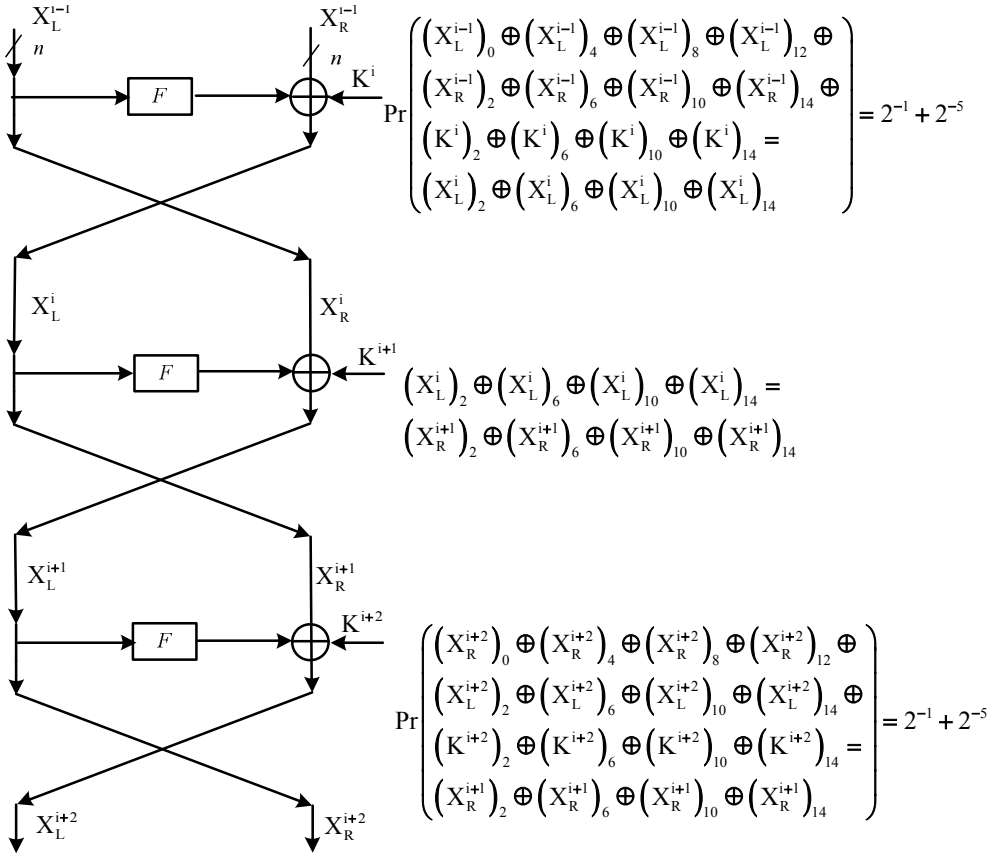

Fig. 7. A 3-round linear characteristic for SIMON include 4 active bits.

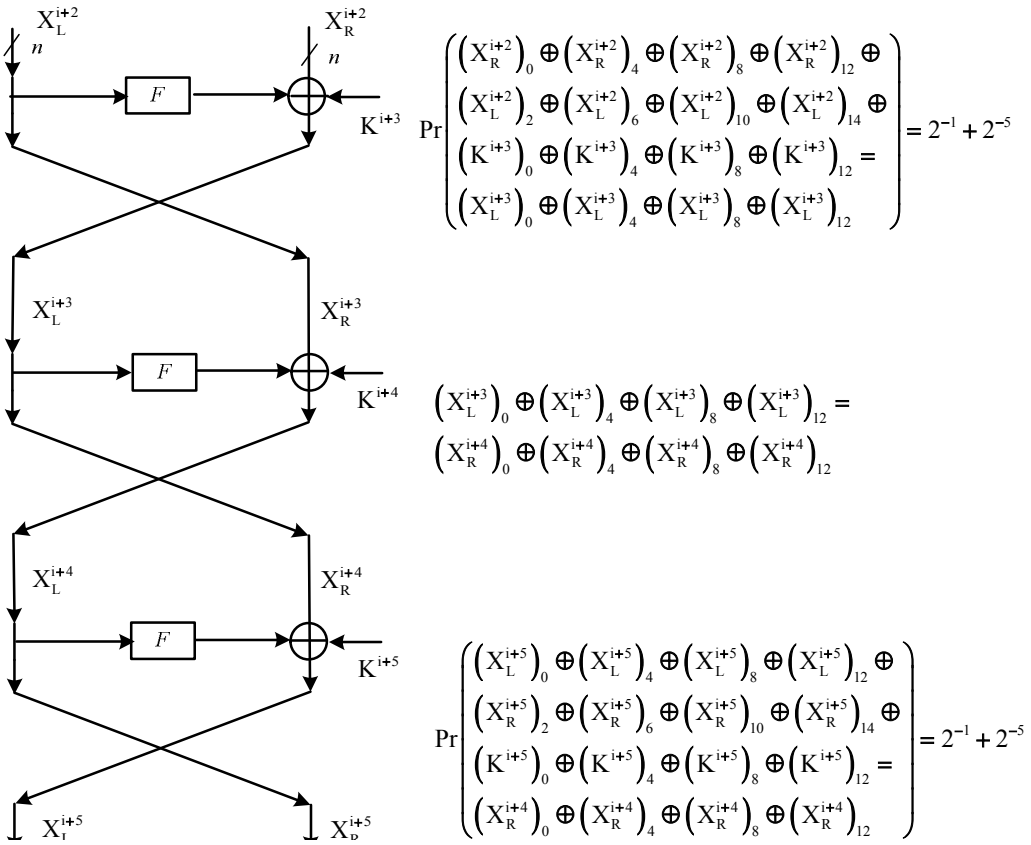

Fig. 8. Another 3-round linear characteristic for SIMON include 4 active bits.

Based on tis pattern, it is possible to generate a pattern that has bias of 2^{-16} for 11-round, as follows:

$$2; 3; 1; 2; 1; 1; 0; 1; 1; 2; 1;$$

This is actually the pattern that we used in previous section to provide a 13-round linear characteristic for SIMON32/64. Based on a similar strategy, it is possible to present linear characteristics for other variants of SIMON. We summarizes the parameters of our linear attacks for the different variants of SIMON in Table 6. On the other hand to use an approximation with the bias of 'ϵ' to mount a linear attack the expected complexity is $O(\epsilon^{-2})$ [4]. Hence, we consider a case where $\epsilon \geq 2^{-n+2}$, where $|P| = 2n$ and for the complexity of $8 \times \epsilon^{-2}$ the success probability of key recovery attack would be '0.997' [1,4]. Our results for different variants of SIMON when $\epsilon \geq 2^{-n+2}$ have been represented in Table 7.

Table 6. Summary of our linear analysis for the different variants of SIMON. In this table **KR** denotes a linear characteristic that can be used trough a key recovery attack and **Dis** denotes a linear characteristic that can be used trough a distinguishing attack.

SIMON	Linear Expression				# Rounds	# Approximations	Bias	Attack
	Start		End					
	Active bits in the left side	Active bits in the right side	Active bits in the left side	Active bits in the right side				
32/64	10,6,2,6,14	8,0	2,10,6,2	4	11	15	2^{-16}	KR
32/64	4,8,4,0	10,6,2	2,14,10	12	22	31	2^{-32}	Dis
48/96	2,18,14,10	12	20,0,20,16	2,22,18	14	22	2^{-23}	KR
48/96	2,18,14,10	12	10,22,6,6	8	23	46	2^{-47}	Dis
64/128	2,26,22,18	20	2,26,22,18	20	17	28	2^{-29}	KR
64/128	2,26,18,28,14 ,28,62,24,10	30,0,26,12	2,26,18,28,14 ,28,62,24,10	30,0,26,12	25	60	2^{-61}	Dis
96/144	2,46,42,46,38	0,40	2,46,42	44	27	46	2^{-47}	KR
96/144	2,42,38,34 ,46,38,30	0,40,32	36,0,40,36,32	2,42,38,34	36	70	2^{-71}	Dis
128/256	52,0,56,52,48	2,58,54,50	2,58,54,50	52	34	63	2^{-64}	KR
128/256	36,0,48,40,36,32	2,50,42,38,34	2,50,42,38,34 ,62,46,38,30	0,48,40,32	52	127	2^{-128}	Dis

Assuming that $(X)_{i_1,\ldots,i_m} = (X)_{i_1} \oplus \ldots \oplus (X)_{i_m}$ and given Tables 8, 9, 10, 11 and 12 it is possible to extract the linear expression related to each variant of SIMON that include only input, output and key bits as follows:

11-Round Linear Expression for SIMON 32/64:

$$\begin{aligned}(P_L)_{10,2,14} \oplus (P_R)_{8,0} \oplus (C_L)_4 \oplus (C_R)_{10,6} = (K^1)_{8,0} \oplus (K^2)_{10,6,2} \oplus (K^3)_4 \\ \oplus (K^4)_{10,6} \oplus (K^5)_8 \oplus (K^6)_{10} \oplus (K^8)_{10} \oplus (K^9)_8 \oplus (K^{10})_{10,6} \oplus (K^{11})_4\end{aligned} \tag{24}$$

14-Round Linear Expression for SIMON 48/96:

$$\begin{aligned}(P_L)_{2,18,14,10} \oplus (P_R)_{12} \oplus (C_L)_{2,22,18} \oplus (C_R)_{0,16} = (K^1)_{12} \oplus (K^2)_{2,18,14} \oplus (K^3)_{0,16} \\ \oplus (K^4)_{2,22,18} \oplus (K^5)_{20} \oplus (K^6)_{2,22} \oplus (K^7)_0 \oplus (K^8)_2 \oplus (K^{10})_2 \oplus (K^{11})_0 \\ \oplus (K^{12})_{2,22} \oplus (K^{13})_{20} \oplus (K^{14})_{2,22,18}\end{aligned} \tag{25}$$

Table 7. Summary of our linear analysis for the different variants of SIMON such that we can mount a linear attack with the success probability of '0.997'.

SIMON	Linear Expression				# Rounds	# Approximations	Bias
	Start		End				
	Active bits in the left side	Active bits in the right side	Active bits in the left side	Active bits in the right side			
32/64	10,6,2	4	0,8,0,8,4	2,10,6	10	13	2^{-14}
48/96	2,18,14,10	12	2,22,18	20	13	19	2^{-20}
64/128	2,26,22,18	20	2,26,22,18	20	17	28	2^{-29}
96/144	2,46,42,46,38	0,40	0,0,4	2,46	26	45	2^{-46}
128/256	2,58,54,50	52	2,58,54,50	52	33	59	2^{-60}

17-Round Linear Expression for SIMON 64/128:

$$\begin{aligned}&(P_L)_{2,26,22,18} \oplus (P_R)_{20} \oplus (C_L)_{20} \oplus (C_R)_{2,26,22,18} = (K^1)_{20} \oplus (K^2)_{2,26,22} \oplus (K^3)_{0,24} \\ &\oplus (K^4)_{2,30,26} \oplus (K^5)_{28} \oplus (K^6)_{2,30} \oplus (K^7)_0 \oplus (K^8)_2 \oplus (K^{10})_2 \oplus (K^{11})_0 \\ &\oplus (K^{12})_{2,30} \oplus (K^{13})_{28} \oplus (K^{14})_{2,30,26} \oplus (K^{15})_{0,24} \oplus (K^{16})_{2,26,22} \oplus (K^{17})_{20}\end{aligned} \tag{26}$$

27-Round Linear Expression for SIMON 96/144:

$$\begin{aligned}&(P_L)_{2,42,38} \oplus (P_R)_{0,40} \oplus (C_L)_{44} \oplus (C_R)_{2,46,42} = (K^1)_{0,40} \oplus (K^2)_{2,46,42} \oplus (K^3)_{44} \oplus (K^4)_{2,46} \\ &\oplus (K^5)_0 \oplus (K^6)_2 \oplus (K^8)_2 \oplus (K^9)_0 \oplus (K^{10})_{2,46} \oplus (K^{11})_{44} \\ &\oplus (K^{12})_{2,46,42} \oplus (K^{13})_{0,41,40} \oplus (K^{14})_{2,42,38} \oplus (K^{15})_{42,41,36} \oplus (K^{16})_{2,42,39,38} \oplus (K^{17})_{0,40} \\ &\oplus (K^{18})_{2,46,42} \oplus (K^{19})_{44} \oplus (K^{20})_{2,46} \oplus (K^{21})_0 \\ &\oplus (K^{22})_2 \oplus (K^{24})_2 \oplus (K^{25})_0 \oplus (K^{26})_{2,46} \oplus (K^{27})_{44}\end{aligned} \tag{27}$$

34-Round Linear Expression for SIMON 128/256:

$$\begin{aligned}&(P_L)_{0,48,56} \oplus (P_R)_{2,58,54,50} \oplus (C_L)_{52} \oplus (C_R)_{2,58,54,50} = (K^1)_{2,58,54,50} \oplus (K^2)_{52} \oplus (K^3)_{2,58,54} \\ &\oplus (K^4)_{0,56} \oplus (K^5)_{2,62,58} \oplus (K^6)_{60} \oplus (K^7)_{2,62} \oplus (K^8)_0 \oplus (K^9)_2 \oplus (K^{11})_2 \oplus (K^{12})_0 \\ &\oplus (K^{13})_{2,62} \oplus (K^{14})_{60} \oplus (K^{15})_{2,58,62} \oplus (K^{16})_{0,56,57} \oplus (K^{17})_{2,58,54} \\ &\oplus (K^{18})_{52,57,58} \oplus (K^{19})_{2,54,55,58} \oplus (K^{20})_{0,56} \oplus (K^{21})_{2,62,58} \oplus (K^{22})_{60} \oplus (K^{23})_{2,62} \oplus (K^{24})_0 \\ &\oplus (K^{25})_2 \oplus (K^{27})_2 \oplus (K^{28})_0 \oplus (K^{29})_{2,62} \oplus (K^{30})_{60} \\ &\oplus (K^{31})_{2,58,62} \oplus (K^{32})_{0,56} \oplus (K^{33})_{2,58,54} \oplus (K^{34})_{52}\end{aligned} \tag{28}$$

5 Conclusion

In this paper we analyzed the security of SIMON family against linear attack. We presented several characteristics for different variants of SIMON. Although the presented results are advanced, compared to the previously known results on the linear cryptanalysis of SIMON, it only covers less than half of the rounds of the cipher.

References

1. 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/`.

Table 8. Sequences of approximation for SIMON 32/64, where entries under used app. column denotes approximation used for corresponding active bit of column 2 of the table.

Active bits in the left side	Active bits in the right side	Used app.	# app.
10,6,2,6,14	8,0	1;1	2
4,8,4,0	10,6,2	1;1;1	3
10,6,2	4	1	1
8,8,4	10,6	1;1	2
10,6	8	1	1
8	10	1	1
10	-	-	0
8,8	10	1	1
10,6,6	8	1	1
4,8,4	10,6	1;1	2
2,10,6,2	4	1	1
0,8,0,8,4	2,10,6	1;1;1	3
2,14,10,14,6	0,8	1;1	2
12,0,12,8	2,14,10	1;1;1	3
2,14,10	12	1	1
0,0,12	2,14	1;1	2
2,14	0	1	1
0	2	1	1
2	-	-	0
0	2	1	1
2,14	0	1	1
0,0,12	2,14	1;1	2
2,14,10	12	1	1
12,0,12,8	2,14,10	1;1;1	3

2. H. A. Alkhzaimi and M. M. Lauridsen. Cryptanalysis of the simon family of block ciphers. Cryptology ePrint Archive, Report 2013/543, 2013. `http://eprint.iacr.org/`.
3. 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/`.
4. 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.

Table 9. Sequences of approximation for SIMON 48/96,where entries under used app. column denotes approximation used for corresponding active bit of column 2 of the table.

Active bits in the left side	Active bits in the right side	Used app.	# app.
12,0,16,12,8	2,18,14,10	1;1;1;1	4
2,18,14,10	12	1	1
0,16,0,16,12	2,18,14	1;1;1	3
2,22,18,22,14	0,16	1;1	2
20,0,20,16	2,22,18	1;1;1	3
2,22,18	20	1	1
0,0,20	2,22	1;1	2
2,22	0	1	1
0	2	1	1
2	-	-	0
0	2	1	1
2,22	0	1	1
0,0,20	2,22	1;1	2
2,22,18	20	1	1
20,0,20,16	2,22,18	1;1;1	3
2,22,18,22,14	0,16	1;1	2
0,16,0,16,12	2,18,14	1;1;1	3
2,18,14,10	12	1	1
12,0,16,12,8	2,18,14,10	1;1;1;1	4

Table 10. Sequences of approximation for SIMON 64/128, where entries under used app. column denotes approximation used for corresponding active bit of column 2 of the table.

Active bits in the left side	Active bits in the right side	Used app.	# app.
20,30,24,20,16	2,26,22,18	1;1;1;1	4
2,26,22,18	20	1	1
0,24,0,24,20	2,26,22	1;1;1	3
2,30,26,30,22	0,24	1;1	2
28,0,28,24	2,30, 26	1;1;1	3
2,30,26	28	1	1
0,0,28	2,30	1;1	2
2,30	0	1	1
0	2	1	1
2	-	-	0
0	2	1	1
2,30	0	1	1
0,0,28	2,30	1;1	2
2,30,26	28	1	1
28,0,28,24	2,30, 26	1;1;1	3
2,30,26,30,22	0,24	1;1	2
0,24,0,24,20	2,26,22	1;1;1	3
2,26,22,18	20	1	1
20,30,24,20,16	2,26,22,18	1;1;1;1	4

Table 11. Sequences of approximation for SIMON 96/144, where entries under used app. column denotes approximation used for corresponding active bit of column 2 of the table.

Active bits in the left side	Active bits in the right side	Used app.	# app.
36,0,40,36,32	2,42,38,34	1;1;1;1	4
2,42,38,34	36	1	1
0,40,0,40,36	2,42,38	1;1;1	3
2,46,42,46,38	0,40	1;1	2
44,0,44,40	2,46,42	1;1;1	3
2,46,42	44	1	1
0,0,44	2,46	1;1	2
2,46	0	1	1
0	2	1	1
2	-	-	0
0,0	2	1	1
2,46,46	0	1;	1
44,0,44	2,46	1;1	2
2,46,42,42	44	1	1
0,41,40,0,44,41,40,	2,46,42	1;1;2	3
2,42,38,46,39,39,38	0,41,40	1;1;2	3
42,41,36,0,42,40,36	2,42,38	3;1;1;	3
2,42,39,38,40,34,40,39,34	42,41,36	3;2;1	3
0,40,0,42,41,40,37,37,36	2,42,39,38	3;2;1;2	4
2,46,42,46,39,38	0,40	1;2	2
44,0,44,40	2,46,42	1;1;1;	3
2,46,42	44	1	1
0,0,44	2,46	1;1	2
2,46	0	1	1
0	2	1	1
2	-	-	0
0	2	1	1
2,46	0	1	1
0,0,44	2,46	1;1	2
2,46,42	44	1	1
44,0,44,40	2,46,42	1;1;1	3
2,46,42,46,38	0,40	1;1	2
0,40,0,40,36	2,42,38	1;1;1	3
2,42,38,34	36	1	1

Table 12. Sequences of approximation for SIMON 128/256, where entries under used app. column denotes approximation used for corresponding active bit of column 2 of the table.

Active bits in the left side	Active bits in the right side	Used app.	# app.
52,0,56,52,48	2,58,54,50	1;1;1;1	4
2,58,54,50	52	1	1
0,56,0,56,52	2,58,54	1;1;1	3
2,62,58,62,54	0,56	1;1	2
60,0,60,56	2,62,58	1;1;1	3
2,62,58	60	1	1
0,0,60	2,62	1;1	2
2,62	0	1	1
0	2	1	1
2	-	-	0
0,0	2	1	1
2,62,62	0	1;	1
60,0,60	2,62	1;1	2
2,62,58,58	60	1	1
0,57,56,0,60,57,56,	2,62,58	1;1;2	3
2,58,54,62,55,55,54	0,57,56	1;1;2	3
58,57,52,0,58,56,52	2,58,54	3;1;1;	3
2,58,55,54,56,50,56,55,50	58,57,52	3;2;1	3
0,56,0,58,57,56,53,53,52	2,58,55,54	3;2;1;2	4
2,62,58,62,55,54	0,56	1;2	2
60,0,60,56	2,62,58	1;1;1;	3
2,62,58	60	1	1
0,0,60	2,62	1;1	2
2,62	0	1	1
0	2	1	1
2	-	-	0
0	2	1	1
2,62	0	1	1
0,0,60	2,62	1;1	2
2,62,58	60	1	1
60,0,60,56	2,62,58	1;1;1	3
2,62,58,62,54	0,56	1;1	2
0,56,0,56,52	2,58,54	1;1;1	3
2,58,54,50	52	1	1