Improved Linear Cryptanalysis of Round Reduced SIMON

Javad Alizadeh[1], Hoda A. Alkhzaimi[2], Mohammad Reza Aref[1], Nasour Bagheri[3], Praveen Gauravaram[4], and Martin M. Lauridsen[2]

[1] ISSL, E.E. Department, Sharif University of Technology, Iran, alizadja@gmail.com
[2] DTU Compute,Section for Cryptology{hoalk, mmeh}@dtu.dk
[3] E.E. Department, Shahid Rajaee Teacher Training University, Iran, NBagheri@srttu.edu
[4] Innovation Labs Hyderabad, Tata Consultancy Services Limited, India, P.Gauravaram@tcs.com

Abstract. SIMON is a family of ten lightweight block ciphers published by Beaulieu *et al.* from U.S. National Security Agency (NSA). A cipher in this family with K-bit key and N-bit block is called SIMON N/K. In this paper we investigate the security of SIMON against different variants of linear cryptanalysis, *i.e.*, classic linear, multiple linear and linear hull attacks. We present a connection between linear characteristic and differential characteristic, multiple linear and differential and linear hull and differential, and employ it to adapt the current known results on differential cryptanalysis of SIMON to linear cryptanalysis of this block cipher. Our best linear cryptanalysis covers SIMON 32/64 reduced to 20 rounds out of 32 rounds with the data complexity $2^{31.69}$ and time complexity $2^{59.69}$. We have implemented our attacks for small scale variants of SIMON and our experiments confirm the theoretical bias presented in this work. So far, our results are the best known with respect to linear cryptanalysis for any variant of SIMON.

Keywords: SIMON, Linear Cryptanalysis, Multiple Linear Cryptanalysis, Linear Hull

1 Introduction

SIMON and SPECK are two families of lightweight block ciphers designed by Beaulieu *et al.* of National Security Agency (NSA) to provide optimal hardware and software performance [4]. SIMON family is constructed to meet hardware implementation flexibility and support efficient implementations across a wide variety of platforms as well as several implementations on a single platform. In particular, SIMON was designed to meet the hardware requirements of low-power limited gate devices such as RFID devices. It is designed to provide block sizes of 32, 48, 64, 96 and 128 bits, with up to three key sizes for each block size. SIMON N/K denotes a variant of SIMON that has the plaintext block length of size N bits and the key size of length K bits. For example, SIMON 32/64 refers to one variant of SIMON with 32-bit plaintext block and 64-bit key. There are ten variants of SIMON, forming a family of lightweight block ciphers.

Linear Cryptanalysis. Linear cryptanalysis [18] is a well-known cryptanalytic technique that has been employed on several block ciphers example DES, FEAL-4, Serpent, Shannon and SAFER [11, 14, 16, 18, 23]. The most important fact about the linear cryptanalysis is that it is a known plaintext attack, which is a more practical and realistic attack model. Linear cryptanalysis tries to find a highly probable linear expressions involving plaintext bits, ciphertext bits and the "subkey" bits as follows:

$$\oplus_i P_{p_i} \oplus_i C_{c_i} = \oplus_i K_{k_i}$$

where, $0 \leq pi \leq |P| - 1$, $0 \leq ci \leq |C| - 1$ and $0 \leq ki \leq |K| - 1$, and P, C, and K represents the 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.

Multiple Linear Cryptanalysis. For improving the linear cryptanalysis, in 1994 Kaliski and Robshaw proposed an algorithm that used several linear approximations [15]. The main constraint in the approach, was that it uses only approximations implying the same bits of subkeys $\oplus_{i=1}^{z} K_{ki}$. In 2004 Biryukov *et al.* proposed multiple linear cryptanalysis technique that doesn't require the constraint [6]. They successfully applied their approach on DES. This approach has been also used in the cryptanalysis of reduced Serpent [12, 13].

Linear Hull. If there are several linear characteristics with the same input and output mask, one can combine these characteristics as a linear hull, which has probability at least as good compared to the classic linear characteristics. Linear hulls have been studied in [20] and used in cryptanalysis of several block ciphers such as PRESENT [10, 17]. Linear hulls can be used in Matsui's Algorithm 2 [18] to decrease the complexity of linear attacks.

Multiple Linear Hull. This is a combination of multiple linear cryptanalysis and linear hull where if there are several linear hulls for a cipher, they can be used in the multiple linear cryptanalysis framework of Biryukov *et al.* [6] to decrease the complexity of linear attacks.

Previous Works. Besides the work presented in this paper, Abed *et al.* [1, 2] presented analysis of SIMON with various techniques including linear, differential, impossible differential and rectangular attacks. In the direction of differential cryptanalysis, the authors have presented differential attacks on reduced-round versions of all SIMON variants. In the direction of impossible differential analysis, the authors attack 13 out of 32 rounds for SIMON 32/64 with data complexity 2^{30} and time complexity $2^{50.1}$, and up to 25 out of 72 rounds for SIMON 128/256 with data complexity 2^{119} and time complexity 2^{195}. With regard to linear cryptanalysis, [2] presented key-recovery attacks on variants of SIMON reduced to 11, 14, 16, 20 and 23 rounds for the respective block sizes of 32, 48, 64, 96 and 128 bits respectively. In [7], Biryukov *et al.* presented a method for searching for differentials in ARX ciphers. The authors apply the method to SIMON and improve the previous differential characteristics to present attacks on 18 out of 32 rounds for SIMON 32/64 and up to 26 out of 44 rounds for SIMON 64/128. Most recently, Wang *et al.* [19] improved the known results on differential cryptanalysis of SIMON and presented attacks on 21-round SIMON32/64, 22-round SIMON48/72, 22-round SIMON48/96, 28-round SIMON64/96 and SIMON64/128.

Contributions. In this paper we analyze the security of SIMON against variants of linear cryptanalysis. In the direction of classic linear cryptanalysis, we present linear characteristics for different variants of SIMON, that can be used in key recovery attack on SIMON reduced to 13, 15, 19, 28 and 35 rounds for the respective block sizes of 32, 48, 64, 96 and 128 bits respectively. Using Algorithm 2 of Matsui, we extend our attack to 16, 18, 23, 33 and 43 rounds for the respective block sizes of 32, 48, 64, 96 and 128 bits respectively. We also, present a connection to convert any given differential characteristic to a linear characteristic for SIMON.

For multiple linear attacks, we attack 18, 20, 22, 33 and 39 rounds of respective block sizes of 32, 48, 64, 96 and 128 bits respectively. Furthermore, the connection between linear and differential characteristic is generalized to a connection between capacity of a system of approximations (in multiple linear cryptanalysis) and differential (in differential cryptanalysis) for SIMON.

We also establish a connection between capacity of a linear hull and differential for SIMON and use the known results on differential cryptanalysis of SIMON to attack 20, 20, 28, 35, and 49 rounds of the respective block/key sizes of 32/64, 48/96, 64/128, 96/144, and 128/256 bits. A brief summary of our results are presented in Table 1.

Organization. The paper is structured as follows. In Section 2 a brief description of SIMON is presented. In Section 3 the idea of linear cryptanalysis of SIMON is described. Also, in this section it is shown that there is a connection between linear cryptanalysis and differential cryptanalysis of SIMON. Multiple linear cryptanalysis of SIMON is described in Section 4 and a linear hull cryptanalysis of SIMON presented in Section 5. Finally, the paper is concluded in Section 6.

Table 1: Linear cryptanalysis of SIMON, using the Matsui's Algorithm 1 and 2, multiple linear, and linear hulls.

	SIMON	# Attacked Rounds	Data	Time
Matsui's Algorithm 1	32/64	13	2^{32}	2^{32}
	$48/k$	16	2^{46}	2^{46}
	$64/k$	19	2^{58}	2^{58}
	$96/k$	29	2^{94}	2^{94}
	$128/k$	36	2^{128}	2^{128}
Matsui's Algorithm 2	32/64	16	2^{32}	2^{54}
	48/72	18	2^{46}	2^{65}
	48/96	19	2^{46}	2^{81}
	64/96	21	2^{58}	2^{82}
	64/128	23	2^{58}	2^{122}
	96/144	33	2^{94}	2^{135}
	128/192	39	2^{128}	2^{167}
	128/192	40	2^{128}	2^{191}
	128/256	41	2^{128}	2^{231}
	128/256	42	2^{128}	2^{255}
Multiple Linear	32/64	18	2^{32}	2^{32}
	$48/k$	20	$2^{47.42}$	$2^{47.42}$
	$64/k$	22	2^{59}	2^{59}
	$96/k$	33	$2^{94.42}$	$2^{94.42}$
	$128/k$	39	2^{128}	2^{128}
Linear Hull	32/64	20	$2^{31.69}$	$2^{59.69}$
	48/72	19	$2^{44.11}$	$2^{65.11}$
	48/96	20	$2^{44.11}$	$2^{80.11}$
	64/96	26	$2^{62.53}$	$2^{86.53}$
	64/128	28	$2^{62.53}$	$2^{119.53}$
	96/144	35	$2^{94.2}$	$2^{129.2}$
	128/192	46	$2^{126.6}$	$2^{178.6}$
	128/256	49	$2^{126.6}$	$2^{232.6}$

2 Description of SIMON Family

SIMON has a classical Feistel structure with the round block size of $N = 2n$ bits, where n is the word size. The number of rounds of cipher is denoted by r and depends on the variant of SIMON. In this paper, 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 a string X, $(X)_i$ denotes the i-th bit of X. Bitwise circular rotation of string a by b positions to the left is denoted by $a \lll b$. Further, $\oplus$ and & denote bitwise XOR and AND operations respectively.

The round function of SIMON can be represented as follows:

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

where $F(X) = (X \lll 2) \oplus ((X \lll 1)\&(X \lll 8))$. We can show the function F as $(F(X))_i = (X)_{i-2} \oplus ((X)_{i-1}\&(X)_{i-8})$ with subtractions being performed modulo n. The F function is an n-bit to n-bit non-linear and non-invertible function.

Given a $2n$-bit internal state, the input of the F-function is the left half of the internal state and its output is XOR'ed with the right half of the internal state and a subkey. The subkeys are driven from a 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. Detailed description of SIMON structure and key scheduling can be found in [4].

3 Linear Cryptanalysis of SIMON

So far the only result on linear cryptanalysis of SIMON is by Abed et. al [1], where an attack on 11 rounds of SIMON 32/64 is shown with the bias being 2^{-11}. In following we present several approaches to produce linear characteristics for SIMON 32/64 and present the best known linear characteristic for 11-round SIMON 32/64 with the bias of 2^{-16}. This characteristic is then extended to 13 rounds of the cipher for no additional complexity. We have implemented the attack on SIMON 32/64 reduced to 11 rounds to demonstrate the validity of our analysis.

3.1 Linear Cryptanalysis of SIMON 32/64

In the round function of SIMON, the only non-linear operation is the bitwise AND. Note that, given single bits A and B, the output of $(A\&B)$ is 0 with probability 0.75. Hence, we can extract the following highly biased linear expressions for the F-function:

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

Given Equations 1 and 2 we can extract the following linear expression for the first round of the SIMON:

$$(P_R)_2 \oplus (P_L)_0 \oplus (X_L^1)_2 = (K^1)_2 \tag{3}$$

Equation 3 holds with probability $\frac{3}{4}$. With the help of the above expression, we can extract a 3-round linear expression as follows (see Figure 1):

$$(X_R^{i-1})_2 \oplus (X_L^{i-1})_0 \oplus (X_R^{i+2})_0 \oplus (X_L^{i+2})_2 = (K^i)_2 \oplus (K^{i+2})_2 \tag{4}$$

Equation 4 can be used to produce a 7-round linear expression as follows:

$$\begin{pmatrix}(X_R^{i-1})_2 \oplus (X_L^{i-1})_0 \oplus (X_R^{i+2})_0 \oplus (X_L^{i+2})_2\\ \oplus(X_R^{i+3})_2 \oplus (X_L^{i+3})_0 \oplus (X_R^{i+6})_0 \oplus (X_L^{i+6})_2\end{pmatrix} = \left((K^i)_2 \oplus (K^{i+2})_2 \oplus (K^{i+4})_2 \oplus (K^{i+6})_2\right) \tag{5}$$

The above expression can be simplified to the following.

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

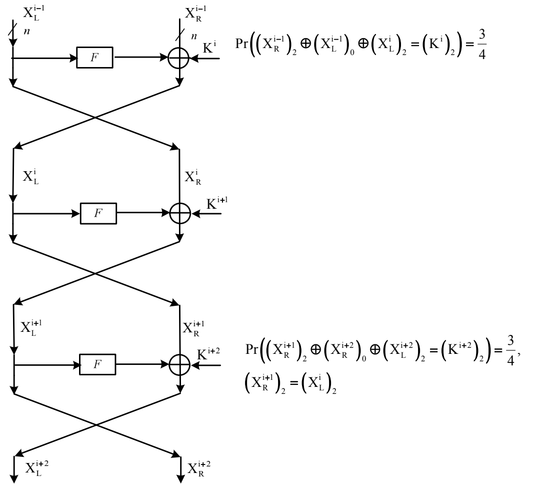

X_L^{i-1}
X_R^{i-1}
n
n
F
K^i
$\Pr\left(\left(X_R^{i-1}\right)_2 \oplus \left(X_L^{i-1}\right)_0 \oplus \left(X_L^i\right)_2 = \left(K^i\right)_2\right) = \frac{3}{4}$
X_L^i
X_R^i
F
K^{i+1}
X_L^{i+1}
X_R^{i+1}
F
K^{i+2}
$\Pr\left(\left(X_R^{i+1}\right)_2 \oplus \left(X_R^{i+2}\right)_0 \oplus \left(X_L^{i+2}\right)_2 = \left(K^{i+2}\right)_2\right) = \frac{3}{4}$,
$\left(X_R^{i+1}\right)_2 = \left(X_L^i\right)_2$
X_L^{i+2}
X_R^{i+2}

Fig. 1: A 3-round linear characteristic for SIMON.

Table 2: The biases for an 11-round LC

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 6, 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 as follows.

$$\left.\begin{array}{ll} Pr[(F(X_L^{i+2}))_0 = (X_L^{i+2})_{14})] = \frac{3}{4} & \\ Pr[(X_L^{i+2})_{14} & = (X_R^{i+1})_{14} \oplus (K^{i+2})_{14} \oplus (X_L^{i+1})_{12})] = \frac{3}{4} \\ Pr[(X_R^{i+1})_{14} & = (X_R^{i-1})_{14} \oplus (K^i)_{14} \oplus (X_L^{i-1})_{12}] = \frac{3}{4} \\ Pr[(X_L^{i+1})_{12} & = (X_L^{i-1})_{12} \oplus (K^{i+1})_{12} \oplus (X_L^i)_{10}] = \frac{3}{4} \\ Pr[(X_L^i)_{10} & = (X_R^{i-1})_{10} \oplus (K^i)_{10} \oplus (X_L^{i-1})_8] = \frac{3}{4} \end{array}\right\} \tag{7}$$

Then, with probability $(3/4)^5$ and bias 2^{-6}, we get the following expression for $F(X_L^{i+2}))_0$.

$$\big((F(X_L^{i+2}))_0\big) = \big((X_R^{i-1})_{10} \oplus (X_R^{i-1})_{14} \oplus (X_L^{i-1})_8 \oplus (K^i)_{10} \oplus (K^i)_{14} \oplus (K^{i+1})_{12} \oplus (K^{i+2})_{14}\big) \tag{8}$$

Using Equation 8 in Equation 6, we can extract a 7 round linear expression with bias 2^{-10}. It is possible to use Equation 6 and produce an 11-round linear expression as follows :

$$\begin{pmatrix} (X_R^{i-1})_2 \oplus (X_L^{i-1})_0 \oplus (F(X_L^{i+2}))_0 \oplus \\ (F(X_L^{i+6}))_0 \oplus (X_R^{i+10})_0 \oplus (X_L^{i+10})_2 \end{pmatrix} = \begin{pmatrix} (K^i)_2 \oplus (K^{i+2})_2 \oplus (K^{i+3})_0 \oplus (K^{i+4})_2 \oplus \\ (K^{i+6})_2 \oplus (K^{i+7})_0 \oplus (K^{i+8})_2 \oplus (K^{i+10})_2 \end{pmatrix} \tag{9}$$

Thus, Equation 9 will be an 11-round linear expression with bias 2^{-17} (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 2 and the piling-up lemma.

Unfortunately this linear expression can't yield a successful linear attack because the required number of plaintexts exceeds the possible values, i.e. 2^{32}. Although we will introduce an 11-round linear expression with bias 2^{-16} later, but in this section we use the above method and calculate a

Table 3: The biases for a 10-round LC

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

10-round linear expression. The bias of the 10-round linear characteristic is 2^{-14} as given in Table 3 and the expression is as follows:

$$\begin{pmatrix} (X_R^{i-1})_2 \oplus (X_L^{i-1})_0 \oplus (F(X_L^{i+2}))_0 \\ \oplus (F(X_L^{i+6}))_0 \oplus (X_R^{i+9})_2 \end{pmatrix} = \begin{pmatrix} (K^i)_2 \oplus (K^{i+2})_2 \oplus (K^{i+3})_0 \oplus (K^{i+4})_2 \\ \oplus (K^{i+6})_2 \oplus (K^{i+7})_0 \oplus (K^{i+8})_2 \end{pmatrix} \tag{10}$$

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

$$(F(X_L^{i+6}))_0 = (X_R^{i+9})_{10} \oplus (X_L^{i+9})_{12} \oplus (X_R^{i+9})_{14} \oplus (K^{i+8})_{14} \oplus (K^{i+9})_{12} \tag{11}$$

Then the 10-round linear expression gets simplified as follows:

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

Now, we extend our attack by one more round to get an 11-round linear expressions for SIMON 32/64 with bias 2^{-16}.

To produce an 11-round linear characteristic, we consider the given 10-round linear expression and add a single round at its beginning to achieve a 11-round characteristic. In this case we have these changes:

$$\left. \begin{array}{l} (X_R^{i-1})_2 = (X_L^{i-2})_2 \\ Pr[(X_L^{i-1})_0 = (X_R^{i-2})_0 \oplus (K^{i-1})_0 \oplus (X_L^{i-2})_{14}] = \frac{3}{4} \\ (X_R^{i-1})_{14} = (X_L^{i-2})_{14} \\ (X_R^{i-1})_{10} = (X_L^{i-2})_{10} \\ Pr[(X_L^{i-1})_8 = (X_R^{i-2})_8 \oplus (K^{i-1})_8 \oplus (X_L^{i-2})_6] = \ \frac{3}{4} \end{array} \right\} \tag{13}$$

Since bias of added round is 2^{-3}, hence the bias of the 11-round linear expression is 2^{-16}.

Once we have such an 11-round linear characteristic we can add another one round to the beginning and one round to the end of the characteristic 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. In this way we have a 13-round linear characteristic for SIMON 32/64. Hence, using Algorithm 1 of Matsui to recover the key, for the data complexity of 2^{32} the success probability of recovering 1 bit of the key would be 0.921 [21].

3.2 Connections between Linear Characteristic and Differential Characteristic for SIMON and its Application on the Other Variants of SIMON

Differential cryptanalysis [5] is a widely used chosen plaintext/ciphertext cryptanalytic attack technique. In a differential attack we look for an input pair with difference $\varDelta X$ that propagates to an output pair with difference $\varDelta Y$ with a high probability pr. This differential characteristic is denoted by $\varDelta X \overset{pr}{\rightarrow} \varDelta Y$.

There are many works which discuss connection between differential and linear characteristics [8, 9]. We observe that there is an explicit connection between linear characteristic and differential characteristic for SIMON. This observation is explained as follows.

In the round function of SIMON, the only non-linear operation is the bitwise AND. Given two bits A and B, the output of $(A\&B)$ would be "0" with probability 0.75. Hence, we can extract the following highly probable differential expressions for the F-function:

$$\left.\begin{array}{l}\text{Differential Characteristic 1}: \ (\Delta X)_i \overset{\frac{1}{2}}{\rightarrow} (\Delta F(X))_{i+2} \\ \text{Differential Characteristic 2}: \ (\Delta X)_i \overset{\frac{1}{2}}{\rightarrow} (\Delta F(X))_{i+2,i+1} \\ \text{Differential Characteristic 3}: (\Delta X)_i \overset{\frac{1}{2}}{\rightarrow} (\Delta F(X))_{i+2,i+8} \\ \text{Differential Characteristic 4}: (\Delta X)_i \overset{\frac{1}{2}}{\rightarrow} (\Delta F(X))_{i+2,i+1,i+8}\end{array}\right\} \tag{14}$$

where $(\Delta F(X))_{i+1,i+8}$ denotes differences in $(i+1)$-th and $(i+8)$-th bits for $\Delta F(X)$ to be 1 and remaining bit positions of $\Delta F(X)$ are 0, similarly for the other expressions. Given Equations 14 and comparing it with the related equation for a linear approximation of the function F, *i.e.*, Equations 2, and the fact that for linear characteristic we approximate bits from output of F by bits from its input and for a differential characteristic we propagate differences in bits of input to the bits of output of F, we see a unique connection between Equations 2 and Equations 14. In other words, each approximation in Equation 2 can be mapped to a differential characteristic in Equation 14. Given this observation, for an r-round differential characteristic we can construct an equivalent r-round linear characteristic by employing the related approximation of each specific differential characteristic of F-function which has been used through r-round differential characteristic.

Now we investigate the strength of different variants of SIMON against linear attack, given the above observation and the known results on differential cryptanalysis of variants of SIMON from [1]. In Appendix C, Table 12, the propagation of our linear characteristics for SIMON 32/64 are presented (for the detail of each used approximation, see Equation 2). For SIMON 32/64 reduced 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 12:

$$\ldots, 1, 2, 1, 3, 2, 3, 1, 2, 1, 1, 0, 1, 1, 2, 1, 3, 2, 3, 1, 2, 1, 1, 0, 1, 1, 2, 1, 3, 2, 3, \ldots$$

Based on this 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 the previous section to provide a 13-round linear characteristic for SIMON 32/64.

Based on a similar strategy, it is possible to present linear characteristics for other variants of SIMON. We summarize the parameters of our linear attacks for the different variants of SIMON in Table 4. On the other hand, to use an approximation with the bias of ϵ to mount a linear attack the expected complexity is $O(\epsilon^{-2})$ [18]. 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, 18]. Our results for different variants of SIMON when $\epsilon \geq 2^{-n+2}$ have been represented in Table 5.

Letting $(X)[i_1, ..., i_m] = (X)_{i_1} \oplus \ldots \oplus (X)_{i_m}$ and given Table 12, it is possible to extract the linear expression related to each variant of SIMON that include only input, output and key bits. For example, the 11-round linear expression for SIMON 32/64 is as follows (the linear expression for the

Table 4: 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, **Dis** denotes a linear characteristic that can be used trough a distinguishing attack and **App.** denotes approximation.

SIMON	Linear Expression				# Rounds	# App.	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

Table 5: 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. In this table **App.** denotes approximation.

SIMON	Linear Expression				# Rounds	# App.	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}

other variants of reduced-round SIMON is presented in Appendix D):

$$\begin{pmatrix} (P_R)[0,8] \oplus (P_L)[2,10,14] \\ \oplus (C_R)[6,10] \oplus (C_L)_4 \end{pmatrix} = \begin{pmatrix} (K^1)[0,8] \oplus (K^2)[2,6,10] \oplus (K^3)_4 \oplus \\ (K^4)[6,10] \oplus (K^5)_8 \oplus (K^6)_{10} \oplus (K^8)_{10} \\ \oplus (K^9)_8 \oplus (K^{10})[6,10] \oplus (K^{11})_4 \end{pmatrix} \quad (15)$$

3.3 A Key Recovery Attack on SIMON Using the Matsui's Algorithm 2

Similar to section 3, once we have an 11-round linear characteristic such as Equation 15, we can add another one round to the beginning and one round to the end of the characteristic to extend the attack up to 13-rounds free of any extra approximation. To extend the above 11-round linear characteristic to more rounds we use Algorithm 2 of Matsui to recover the key, where 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:

$$(X_R^i)[0,8] \oplus (X_L^i)[2,10,14] \oplus (X_R^{i+11})[6,10] \oplus (X_L^{i+11})_4 \quad (16)$$

Figure 2 shows the bits of subkeys that should be guessed when we add 2 rounds to the beginning and 3 rounds to the end of the above 11-round characteristic (22 bits of subkeys). Hence, we can attack 16 rounds of SIMON 32/64 using Algorithm 2 of Matsui to recover the key. The time complexity for this attack is 2^{54} and the data complexity is 2^{32}.

Similarly, given the linear characteristics for SIMON 48/K, SIMON 64/K, SIMON 96/K and SIMON 128/K in Appendix D, we can add another one round to the beginning and one round to the end of each characteristic to extend the attack up to 2 more rounds free of any extra approximation. To extend the linear characteristics to more rounds we use Algorithm 2 of Matsui to recover the key, where we guess subkyes of rounds at the beginning and the end of each characteristic and determine the correlation of the related linear relation between the input and the output of the characteristic to filter the wrong subkeys. Figures 6, 7, 8 and 9 in Appendix E show the bits of subkeys that should be guessed when we add extra rounds to each variants of SIMON. Hence, using Algorithm 2 of Matsui, we can attack 18 rounds of SIMON 48/72 with the time complexity of 2^{65}, 19 rounds of SIMON 48/96 with the time complexity of 2^{81}, 21 rounds of SIMON 64/96 with the time complexity of 2^{82}, 23 rounds of SIMON 64/128 with the time complexity of 2^{122}, 33 rounds of SIMON 96/144 with the time complexity of 2^{135}, 40 rounds of SIMON 128/192 with the time complexity of 2^{191} and 42 rounds of SIMON 128/256 with the time complexity of 2^{255}. It must be noted that it is possible to attack 39 rounds of SIMON 128/192 with the time complexity of 2^{167} and attack 41 rounds of SIMON 128/256 with the time complexity of 2^{231}. The results are summarized in Table 1.

4 Multiple Linear Cryptanalysis of SIMON

The technique of multiple linear cryptanalysis, an improved version of the linear cryptanalysis, is proposed in 2004 [6]. This attack is applicable to (reduced-round) ciphers that have more than one approximation. Suppose that, there are m approximations on r rounds of a cipher as follows:

$$P^i_{p_j} \oplus C^i_{c_k} = K^i_{k_l} \quad (1 \leqslant i \leqslant m). \quad (17)$$

The goal is to recover bits of key or finding some informations about the key bits that appear in Equation 17. An explicit approach is that a counter t_i is associated with each approximation and increased when the corresponding linear approximation is verified for a particular pair of known plaintext and ciphertext. As for algorithm 1 of Matsui [18], the values of $K^i_{k_l}$ are determined from the

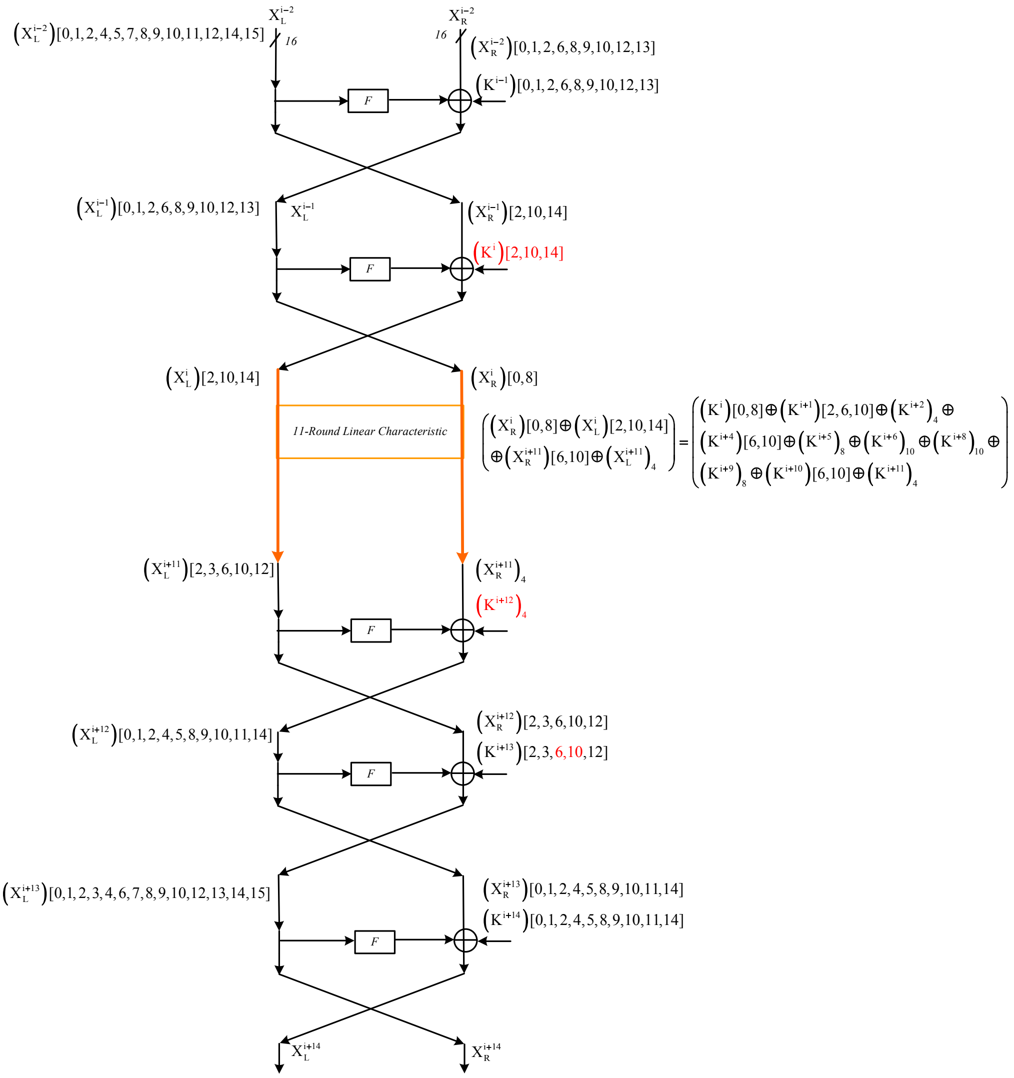

X_L^{i-2}
X_R^{i-2}
$(X_L^{i-2})[0,1,2,4,5,7,8,9,10,11,12,14,15]$
16
16
$(X_R^{i-2})[0,1,2,6,8,9,10,12,13]$
$(K^{i-1})[0,1,2,6,8,9,10,12,13]$
F
$(X_L^{i-1})[0,1,2,6,8,9,10,12,13]$
X_L^{i-1}
$(X_R^{i-1})[2,10,14]$
$(K^{i})[2,10,14]$
F
$(X_L^{i})[2,10,14]$
$(X_R^{i})[0,8]$
11-Round Linear Characteristic
$\begin{pmatrix}(X_R^i)[0,8]\oplus(X_L^i)[2,10,14]\\ \oplus(X_R^{i+11})[6,10]\oplus(X_L^{i+11})_4\end{pmatrix}=\begin{pmatrix}(K^i)[0,8]\oplus(K^{i+1})[2,6,10]\oplus(K^{i+2})_4\oplus\\ (K^{i+4})[6,10]\oplus(K^{i+5})_8\oplus(K^{i+6})_{10}\oplus(K^{i+8})_{10}\oplus\\ (K^{i+9})_8\oplus(K^{i+10})[6,10]\oplus(K^{i+11})_4\end{pmatrix}$
$(X_L^{i+11})[2,3,6,10,12]$
$(X_R^{i+11})_4$
$(K^{i+12})_4$
F
$(X_L^{i+12})[0,1,2,4,5,8,9,10,11,14]$
$(X_R^{i+12})[2,3,6,10,12]$
$(K^{i+13})[2,3,6,10,12]$
F
$(X_L^{i+13})[0,1,2,3,4,6,7,8,9,10,12,13,14,15]$
$(X_R^{i+13})[0,1,2,4,5,8,9,10,11,14]$
$(K^{i+14})[0,1,2,4,5,8,9,10,11,14]$
F
X_L^{i+14}
X_R^{i+14}

Fig. 2: The keys (in *black*) that should be guessed to attack 16 rounds of SIMON 32/64.The *red* bits are not required to be guessed.

experimental bias $(t_i - N/2)/N$ and the theoretical bias ϵ_i (bias of the approximation i) by means of a maximum likelihood rule [13,18]. In [6] Biryukov *et al.* showed that theoretical data complexity of the generalized multiple linear cryptanalysis is decreased compared to the original attack. The data complexity of the attack is inversely proportional to the capacity of the system of m approximations used by the adversary that is defined as:

$$\overline{c}^2 = 4 \times \sum_{i=1}^{m} \epsilon_i^2 \tag{18}$$

In other words, by increasing the quantity of Equation 18, one can decrease the data complexity of the attack. For this, it is required to use more approximations. Therefore, finding more approximations is the main task in multiple linear cryptanalysis.

For each variants of reduced-round SIMON, one can find more than one linear characteristic with desirable bias. Therefore, we can use multiple linear cryptanalysis technique to present an improved linear attack on SIMON.

To find a linear characteristic for SIMON 32/64, if bit "2" in the right half of state is considered, the round function is approximated for the bit, and propagation of the approximation is followed in the forward and the backward direction for SIMON 32/64, then Table 12 is produced. Now, if another bit, except bit "2", is considered at the beginning of the work, then another table, different from Table 12, and another 11-round linear characteristic with bias 2^{-16} for SIMON 32/64 is produced. Since there are 16 bits in the right half of state of SIMON 32/64, 16 tables like Table 12 and 16 linear characteristics of bias 2^{-16} for 11-round SIMON can be found. On the other hand, it is possible to approximate active bits at the beginning and the end of a linear characteristic using approximation 1, 2, 3 or 4 in Equation 2. These changes have no impact on the bias of the linear characteristic. Therefore, corresponding to each active bit at the beginning or the end of a linear characteristic of bias ϵ, there are four linear characteristics of the same bias, ϵ. For example, for the 11-round linear characteristic for SIMON 32/64 in table 4, there are two active bits in the beginning (the bits "8" and "0") and one active bit in the end (bit "4"). The bits can be approximated by $4 \times 4 \times 4$ different approximations, but identical probability. The different approximations produce 64 linear characteristics of bias 2^{-16} for 11-round SIMON 32/64. With respect to the 16 bits of right half of state in SIMON 32/64, the number of 11-round linear characteristics of bias 2^{-16} is:

$$4 \times 4 \times 4 \times 16 = 2^{10}.$$

Given these approximations, one can present an improved linear attack on reduced-round SIMON, explained for SIMON 32/64 in Section 4.2.

Similarly, many approximations for reduced rounds of other variants of SIMON can be found, see Tables 12, 13, 14, 15, and 16. Note that the patterns in Tables 12, 13, 14, 15, and 16, are produced by considering only one bit in the state of cipher.

4.1 Connection between Capacity and Expected Differential Probability for SIMON

A differential of SIMON with fixed input and output difference is composed of many differential characteristics of the cipher, with the same input and output difference. Suppose that there are m differential characteristics with input difference α and output difference β of probability $p_i(\alpha, \beta)$, $1 \leq i \leq m$. Then *Expected Differential Probability* for the differential with the same input and output difference is defined in the following way:

$$EDP(\alpha, \beta) = \sum_{i} p_i(\alpha, \beta) \tag{19}$$

In this section, we extend the given connection between a linear characteristic and differential characteristic in section 3.2 to a connection between capacity of a system of approximations (in multiple linear cryptanalysis) and expected differential probability for SIMON as Theorem 1.

Theorem 1. *Suppose that there are m differential characteristics for SIMON reduced to r rounds that result a differential with probability p for the r rounds. Then there are m linear characteristics for SIMON reduced to r rounds that produce a system of approximations of capacity:*

$$\bar{c}^2 = p.$$

Proof. Suppose that differential characteristic i has probability p_i where $1 \leq i \leq n$. Then expected differential probability, p, for the n differential characteristics is:

$$p = \sum_{i=1}^{n} p_i.$$

On the other hand in Section 3.2, it is shown that for a differential characteristic of probability q, there is a linear characteristic of bias $2^{-1} \cdot q^{1/2}$ for SIMON. Therefore, using the m differential characteristics of probability p_i, m linear characteristics of bias ϵ_i can be found where $\epsilon_i = 2^{-1} \cdot p_i^{1/2}$ or equivalently $\epsilon_i^2 = 2^{-2} \cdot p_i$. Then

$$p = \sum_{i=1}^{n} p_i = \sum_{i=1}^{n} 4 \times \epsilon_i^2 = 4 \times \sum_{i=1}^{n} \epsilon_i^2 = \bar{c}^2. \tag{20}$$

□

Now, given Theorem 1, the connection between capacity and differentials for SIMON can be exploited to find other multiple linear attacks on SIMON based on the differentials that are presented for the cipher. For example, if the differentials for SIMON $32/k$, $48/k$ and $64/k$ in [7] are considered, then it is possible to present a linear attack on 16, 17, and 23 rounds of the variants, with data complexity $2^{30.94}$, $2^{42.11}$, and $2^{60.53}$, respectively. The results on different variants are summarized in Table 6.

4.2 A Key Recovery Attack on 18-round of SIMON 32/64 based on Multiple Linear Cryptanalysis

In this section, the multiple linear attack on SIMON 32/64 is described. One can use Table 12 to construct $4 \times 4 \times 16$ approximations of bias 2^{-22} for 16-round SIMON 32/64. Capacity of the system based on those approximations is:

$$4 \times 4 \times 16 \times 4 \times 2^{-44} = 2^{-34}.$$

This means that, data complexity of a linear attack based on the system exceed the brute force. However, another system of approximations with desirable properties can be constructed. For this, consider Table 7 which is a partition of Table 12. The active bit (the bit that must be approximated) in the right side of 15-th round in Table 7 is bit "2". This bit can be approximated using one of the four approximations in Equation 2. Suppose that approximation 1 is used. Then the active bit in the right side of 16-th round will be bit "0" which can be approximated using one of the four approximations in Equation 2. This conclude $4 \times 16 \times 4$ linear characteristics of bias 2^{-22} for 16-round SIMON. Now, suppose that bit "2" in the right side of 15-th round is approximated using approximation 2 in Equation 2. Then, the active bits in the right side of 16-th round are bits "0" and

Table 6: The number of approximations and cumulative capacities of the extended approximations for SIMON.

SIMON	# rounds	log_2 bias, approx.	# approx.	log_2 capacity	# rounds attacked
32/64	11	-16	$4^2 \times 4 \times 16$	-20	13
32/64	16	-22;-23;-24	2^8;2^{11};2^{12}	-32	18
32/64	13		45083	-29.69	15
32/64	13		full search	-28.11	15
32/64	14		full search	-30.94	16
$48/k$	14	-23	$4 \times 4^3 \times 24$	-31.42	16
$48/k$	18	-33;-34;-35	$2^{14.58}$;$2^{17.58}$;$2^{18.58}$	-47.42	20
$48/k$	15		112573	-42.11	17
$64/k$	17	-29	$4 \times 4 \times 32$	-47	19
$64/k$	20	-40	$4^3 \times 4^4 \times 32$	-59	22
$64/k$	20		210771	-58.68	22
$64/k$	21		337309	-60.53	23
$96/k$	27	-47	$4^2 \times 4 \times 48$	-80.42	29
$96/k$	31	-58	$4^3 \times 4^4 \times 48$	-94.42	33
$128/k$	34	-64	$4^4 \times 4 \times 64$	-110	36
$128/k$	37	-74	$4^3 \times 4^3 \times 64$	-128	39

"1" that each of them can be approximated using one of the four approximations in Equation 2 and $4 \times 16 \times 4^2$ linear characteristics of bias 2^{-23} can be found for 16-round SIMON. If bit "2" in the right side of 15-th round is approximated using approximation 3 in Equation 2, other $4 \times 16 \times 4^2$ linear characteristics of bias 2^{-23} for 16-round SIMON can be produced. Finally, if bit "2" in the right side of 15-th round is approximated using approximation 4 in Equation 2, then the active bits in the right side of 16-th round are bits "0", "1", and "10" that each of them can be approximated using one of the four approximations in Equation 2. In other words, $4 \times 16 \times 4^3$ linear characteristics of bias 2^{-24} for 16-round SIMON 32/64 can be found. The results are summarized in Table 8. Hence,the capacity of those approximations will be determined as follows:

$$\bar{c}^2 = 4 \times 16 \times 4 \times (4 \times 2^{-44} + 2 \times 4^2 \times 2^{-46} + 4^3 \times 2^{-48}) =$$

$$2^8 \times (2^{-42} + 2^{-41} + 2^{-42}) = 2^8 \times (2^{-42}(1 + 2 + 1)) = 2^{-32}$$

Therefore, given this capacity for a 16 round multiple linear characteristics and the fact that one round to the beginning and one round to the end of each characteristic can be added without any extra approximation, the attack can be applied on 18 rounds of SIMON32/64

5 Linear Hulls of SIMON

Similarly to the connection between EDP of a differential and capacity of a system of linear equations (in the multiple linear cryptanalysis), one can show a relation between EDP of a differential and capacity of a system of linear hull for SIMON as Theorem 2.

Theorem 2. *Suppose that there are m differential characteristics for SIMON reduced to r rounds, with fixed input and output difference, that result a differential with probability p for the r rounds. Then there are m linear characteristics for SIMON reduced to r rounds, with fixed input and output mask, that produce a linear hull of capacity:*

$$\bar{c}^2_{LH} = 2^{-2}.p$$

Table 7: A system of linear equations for SIMON 32/64 reduced to 16 rounds.

r	Active bits in the left side	Active bits in the right side	Used App.	# App.
1		10	1 or 2 or 3 or 4	1
2	10	-	-	0
3	8,8	10	1	1
4	10,6,6	8	1	1
5	4,8,4	10,6	1;1	2
6	2,10,6,2	4	1	1
7	0,8,0,8,4	2,10,6	1;1;1	3
8	2,14,10,14,6	0,8	1;1	2
9	12,0,12,8	2,14,10	1;1;1	3
10	2,14,10	12	1	1
11	0,0,12	2,14	1;1	2
12	2,14	0	1	1
13	0	2	1	1
14	2	-	-	0
15	0 or 0,1 or 0,10 or 0,1,10	2	1 or 2 or 3 or 4	1
16		0 or 0,1 or 0,10 or 0,1,10	1 or 2 or 3 or 4	1 or 2 or 3

Table 8: Different approximations of bit "2" in the 15-th round.

app variant	active bit(s) in the left of 15-th round	active bit(s) in the right of 16-th round	# app in the 16-th round	# equat for 16-round	log_2 bias of the 16-round char.
1	0	0	1	$4 \times 16 \times 4$	-22
2	0,1	0,1	2	$4 \times 16 \times 4^2$	-23
3	0,10	0,10	2	$4 \times 16 \times 4^2$	-23
4	0,1,10	0,1,10	3	$4 \times 16 \times 4^3$	-24

Alkhzaimi and Lauridsen in [3] and Abed *et al.* in [2] found many differential characteristics for some variants of SIMON which yield the desirable differentials for the cipher. In addition, a maximum number of the differential characteristics for some variants of SIMON was investigated by Biryukov *et al.* [7]. Based on the connection between linear hulls and differentials of SIMON, one can use the differentials by Abed *et al.* in [2] or differentials by Birukov *et al.* in [7] to find the corresponding linear hulls for variants of reduced-round SIMON. We find the linear characteristics for SIMON 32/64, $48/k$, and $64/k$ reduced to 13, 15, and 21 rounds, respectively, based on the differential trails by Birukov *et al.* For SIMON $96/k$ and $128/k$ reduced to 30 and 41 rounds, we use differential trails by Abed *et al.* Using those linear characteristics, we can find suitable linear hulls for each variant of SIMON. The summary of the results are presented in Table 9, and Tables 17, 18, 19, and 20 in Appendix F.

5.1 Extending Linear Hulls and Key Recovery Attack on SIMON 32/64

Similar to the approach we used to extend a linear characteristic when it is used in Algorithm 2 of Matsui (see section 3.3), it is possible to extend a given linear hull for more rounds. For example, consider the linear hull based on the differential by Birukov *et al.* for 13-round SIMON 32/64. The input and output mask of the linear hull is $(\mathit{\Gamma}_6, -)$ and $(-, \mathit{\Gamma}_{14})$. We extend it by adding some rounds to the beginning and the end of the cipher, as follows.

In the backward direction. We start with the input mask of the 13-round linear hull (e.g. $(\mathit{\Gamma}_6, -)$) and go backwards to add some rounds to the beginning. With respect to Figure 3 and Table 10, we can append a further round to the beginning of the cipher to find a new 14-round linear hull by input mask $(-, \mathit{\Gamma}_6)$. Since SIMON injects the subkey at the end of its round function, then this work does not have any computational complexity. If we add a round to the beginning of new 14-round linear

Table 9: Linear characteristics based on the differential trials by Birukov *et al.* for SIMON 32/64.

	Differential		Linear		
r	$\triangle_L$	$\triangle_R$	X_L	X_R	Used App.
0	-	6	6	-	-
1	6	-	-	6	1
2	8	6	6	4	1
3	6,10	8	4	2,6	1;1
4	12	6,10	2,6	0	1
5	6,10,14	12	0	2,6,14	1;1;1
6	0,8	6,10,14	2,6,14	4,12	1;1
7	2,6,14	0,8	4,12	6,10,14	1;1;1
8	4	2,6,14	6,10,14	8	1
9	2,14	4	8	10,14	1;1
10	0	2,14	10,14	12	1
11	14	0	12	14	1
12	-	14	14	-	-
13	14	-	-	14	-
	$\sum_r log_2pr = -36$ $log_2p_{diff} = -29.69$ $\#trails = 45083$		$log_2\epsilon^2 = -38$ $log_2\bar{c}^2_{LH} = -31.69$ $\#characteristics = 45083$		

hull, we must guess the bits 4, 5, and 14 of subkey K^{i-1}. We can continue our method to add more rounds to the beginning of linear hull in the cost of guessing some bits of subkeys.

In the forward direction. We can use the same approach to add some rounds to the end of linear hull in the cost of guessing some bits of subkeys. For example, if we append three rounds to the end of 13-round linear hull, we must guess the bits 12, 13, and 6 of subkey K^{i+16} and the bits 4, 5, 10, 11, 12, and 14 of of subkey K^{i+17}. More details are depicted in Figure 3 and Table 10.

Table 10: Sequence of the bits of subkeys that must be guessed when some rounds are appended to the beginning and the end of the 13-round linear hull for SIMON 32/64.

r	Active bits in the left side	Active bits in the right side	Guessed bits	# Guessing
i-4	0,1,2,3,4,6,8,9,10,11,12,13,14,15	0,1,2,3,4,5,10,11,12,14	0,1,2,3,4,5,10,11,12,14	10
i-3	0,1,2,3,4,5,10,11,12,14	2,3,4,6,12,13	2,3,4,6,12,13	6
i-2	2,3,4,6,12,13	4,5,14	4,5,14	3
i-1	4,5,14	6		
i	6	-		
⋮				
i+14	6,12,13	14		
i+15	4,5,10,11,12,14	6,12,13	6,12,13	3
i+16	2,3,4,6,8,9,10,11,12,13	4,5,10,11,12,14	4,5,10,11,12,14	6

We can extend the 13-round linear hull of SIMON 32/64 by seven rounds (by adding four rounds at the beginning and three rounds to the end) in a key-recovery attack such that the total computational effort for collecting plaintext-ciphertext pairs and testing all subkey candidates for the appended rounds remains significantly smaller than for exhaustively searching the full key space.

Attack Complexity. We require $2^{31.69}$ known plaintexts. We also need $2^{31.69}$ encryptions for producing the required known plaintexts and $2^{31.69} \times 2^{28}$ encryptions to find the round-key bits

$$(K^{i-1})[4,5,14], (K^{i-2})[2,3,4,6,12,13], (K^{i-3})[0,1,2,3,4,5,10,11,12,14], (K^{i+16})[6,12,13],$$

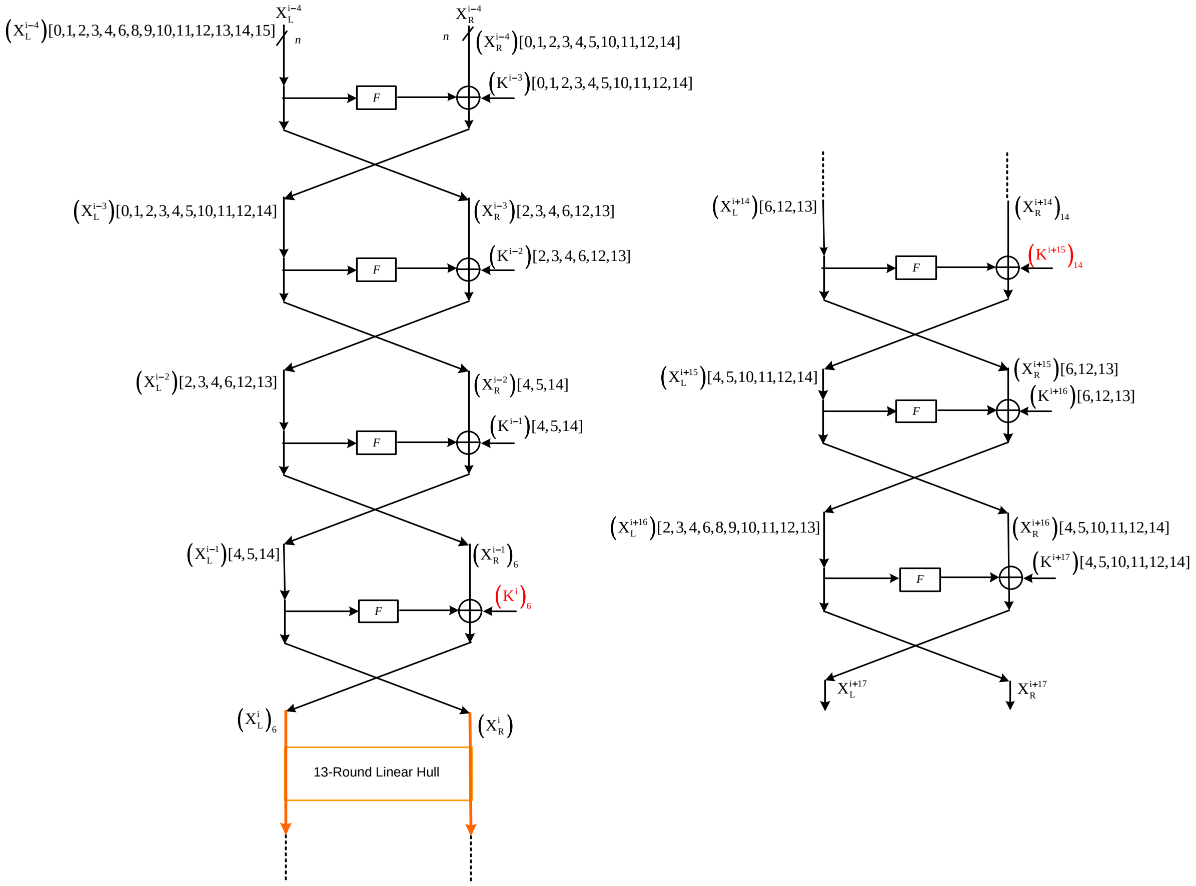

X_L^{i-4}
X_R^{i-4}
$(X_L^{i-4})[0,1,2,3,4,6,8,9,10,11,12,13,14,15]$
n
n
$(X_R^{i-4})[0,1,2,3,4,5,10,11,12,14]$
$(K^{i-3})[0,1,2,3,4,5,10,11,12,14]$
F
$(X_L^{i-3})[0,1,2,3,4,5,10,11,12,14]$
$(X_R^{i-3})[2,3,4,6,12,13]$
$(K^{i-2})[2,3,4,6,12,13]$
F
$(X_L^{i-2})[2,3,4,6,12,13]$
$(X_R^{i-2})[4,5,14]$
$(K^{i-1})[4,5,14]$
F
$(X_L^{i-1})[4,5,14]$
$(X_R^{i-1})_6$
$(K^{i})_6$
F
$(X_L^{i})_6$
(X_R^{i})
13-Round Linear Hull
$(X_L^{i+14})[6,12,13]$
$(X_R^{i+14})_{14}$
$(K^{i+15})_{14}$
F
$(X_L^{i+15})[4,5,10,11,12,14]$
$(X_R^{i+15})[6,12,13]$
$(K^{i+16})[6,12,13]$
F
$(X_L^{i+16})[2,3,4,6,8,9,10,11,12,13]$
$(X_R^{i+16})[4,5,10,11,12,14]$
$(K^{i+17})[4,5,10,11,12,14]$
F
X_L^{i+17}
X_R^{i+17}

Fig. 3: The subkey bits (in *black*) that should be guessed to attack 20 rounds of SIMON 32/64. The *red* bits are not required to be guessed.

and

$$(K^{i+17})[4,5,10,11,12,14].$$

Therefore, the time complexity of the attack is:

$$2^{31.69} + 2^{31.69} \times 2^{28} \approx 2^{59.69}$$

5.2 Key recovery attack on other variants of SIMON

In the above, we explain a key recovery attack which uses a linear hull on SIMON 32/64. The same procedure can be applied to other variants of SIMON, see Appendix G for more details. A summary of our results on the linear hull cryptanalysis of SIMON $48/k$, $64/k$, $96/k$, and $128/k$ is presented in Table 1. It must be noted that we use the linear hulls in Tables 17, 18, 19, and 20 through these attacks.

6 Conclusion

In this paper we analysed the security of SIMON against different variants of linear cryptanalysis, *i.e.*, classic linear, multiple linear and linear hull attacks. We mainly used a connection between linear characteristic and differential characteristic and extended it to a connection between multiple linear and differential and linear hull and differential. Given these connections, we used the known results on differential cryptanalsyis of variants of SIMON to present the best known results on linear cryptanalysis of them.

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/`.
2. F. Abed, E. List, S. Lucks, and J. Wenzel. Differential and linear cryptanalysis of reduced-round simon. Preproceedings of Fast Software Encryption (FSE 2014), 2014.
3. 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/`.
4. 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/`.
5. E. Biham and A. Shamir. Differential Cryptanalysis of the Full 16-Round DES. In E. F. Brickell, editor, *CRYPTO*, volume 740 of *Lecture Notes in Computer Science*, pages 487–496. Springer, 1992.
6. A. Biryukov, C. D. Cannière, and M. Quisquater. On multiple linear approximations. In *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 1–22. Springer, 2004.
7. A. Biryukov, A. Roy, and V. Velichkov. Differential Analysis of Block Ciphers SIMON and SPECK. Preproceedings of Fast Software Encryption (FSE 2014), 2014.
8. C. Blondeau and K. Nyberg. New links between differential and linear cryptanalysis. In T. Johansson and P. Q. Nguyen, editors, *EUROCRYPT*, volume 7881 of *Lecture Notes in Computer Science*, pages 388–404. Springer, 2013.
9. F. Chabaud and S. Vaudenay. Links between differential and linear cryptoanalysis. In Santis [22], pages 356–365.
10. J. Y. Cho. Linear Cryptanalysis of Reduced-Round PRESENT. In *CT-RSA*, pages 302–317, 2010.
11. 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.
12. B. Collard, F.-X. Standaert, and J.-J. Quisquater. Experiments on the multiple linear cryptanalysis of reduced round serpent. In *FSE*, volume 5086 of *Lecture Notes in Computer Science*, pages 382–397. Springer, 2008.

13. B. Collard, F.-X. Standaert, and J.-J. Quisquater. Improved and multiple linear cryptanalysis of reduced round serpent. In *Inscrypt*, volume 4990 of *Lecture Notes in Computer Science*, pages 51–65. Springer, 2008.
14. R. M. Hakala and K. Nyberg. Linear Distinguishing Attack on Shannon. In *ACISP*, pages 297–305, 2008.
15. B. S. K. Jr. and M. J. B. Robshaw. Linear cryptanalysis using multiple approximations. In *CRYPTO*, volume 839 of *Lecture Notes in Computer Science*, pages 26–39. Springer, 1994.
16. J. N. Jr., B. Preneel, and J. Vandewalle. Linear Cryptanalysis of Reduced-Round Versions of the SAFER Block Cipher Family. In *FSE*, pages 244–261, 2000.
17. G. Leander. On Linear Hulls, Statistical Saturation Attacks, PRESENT and a Cryptanalysis of PUFFIN. In *EUROCRYPT*, pages 303–322, 2011.
18. 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.
19. K. J. J. Z. Ning Wang, Xiaoyun Wang. Improved differential attacks on reduced simon versions. Cryptology ePrint Archive, Report 2014/448, 2014. `http://eprint.iacr.org/2014/448`.
20. K. Nyberg. Linear Approximation of Block Ciphers. In Santis [22], pages 439–444.
21. K. Nyberg. Linear Cryptanalysis. Icebreak 2013, 2013. `http://ice.mat.dtu.dk/slides/kaisa_1.pdf?`.
22. 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*. Springer, 1995.
23. A. Tardy-Corfdir and H. Gilbert. A known plaintext attack of feal-4 and feal-6. In *CRYPTO*, pages 172–181, 1991.

A Other Linear Characteristics for SIMON

In Figure 4 and Figure 5 two distinct 3-round linear characteristic are depicted. The interesting point of these characteristics is that they can be combined to receive a characteristic for extra rounds that do not include any intermediate values. For example, concatenating these figures 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 nine rounds then the probability of such characteristic is expected to be $\frac{1}{2}+2^{-25}$. Although such characteristic cannot be used to recover the key but maybe considered as a distinguisher for the reduced cipher. It must be noted, based on the same argument, it is possible to extract similar linear characteristics for any variant of SIMON.

B Experimental Results of Linear Cryptanalysis for SIMON 32/64

We evaluated the theoretical results presented in Equation 15 for 11-round SIMON 32/64 experimentally. Table 11 represents the results. In this table P_n is the number of known plaintexts, C_n is the number of palintext and ciphertext pairs that satisfied Equation 15, Pr is the probability that Equation 15 holds. It shows that, experimental results justify the theory and the bias of the presented path is not less than 2^{-16}

C Sequences of Approximation used through Driving the Linear Characteristic of each Variant of SIMON

Tables 12 represent the propagation of our linear characteristics for SIMON 32/64, entries under used App. column denotes approximation used for corresponding active bit of column 2 of the table.

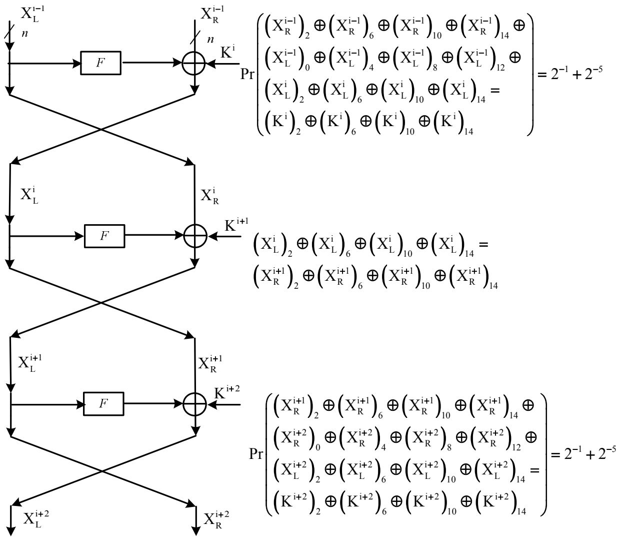

X_L^{i-1}
n
F
X_R^{i-1}
n
K^i
$\Pr\begin{pmatrix}(X_R^{i-1})_2\oplus(X_R^{i-1})_6\oplus(X_R^{i-1})_{10}\oplus(X_R^{i-1})_{14}\oplus\\(X_L^{i-1})_0\oplus(X_L^{i-1})_4\oplus(X_L^{i-1})_8\oplus(X_L^{i-1})_{12}\oplus\\(X_L^{i})_2\oplus(X_L^{i})_6\oplus(X_L^{i})_{10}\oplus(X_L^{i})_{14}=\\(K^i)_2\oplus(K^i)_6\oplus(K^i)_{10}\oplus(K^i)_{14}\end{pmatrix}=2^{-1}+2^{-5}$
X_L^{i}
X_R^{i}
F
K^{i+1}
$(X_L^{i})_2\oplus(X_L^{i})_6\oplus(X_L^{i})_{10}\oplus(X_L^{i})_{14}=$
$(X_R^{i+1})_2\oplus(X_R^{i+1})_6\oplus(X_R^{i+1})_{10}\oplus(X_R^{i+1})_{14}$
X_L^{i+1}
X_R^{i+1}
F
K^{i+2}
$\Pr\begin{pmatrix}(X_R^{i+1})_2\oplus(X_R^{i+1})_6\oplus(X_R^{i+1})_{10}\oplus(X_R^{i+1})_{14}\oplus\\(X_R^{i+2})_0\oplus(X_R^{i+2})_4\oplus(X_R^{i+2})_8\oplus(X_R^{i+2})_{12}\oplus\\(X_L^{i+2})_2\oplus(X_L^{i+2})_6\oplus(X_L^{i+2})_{10}\oplus(X_L^{i+2})_{14}=\\(K^{i+2})_2\oplus(K^{i+2})_6\oplus(K^{i+2})_{10}\oplus(K^{i+2})_{14}\end{pmatrix}=2^{-1}+2^{-5}$
X_L^{i+2}
X_R^{i+2}

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

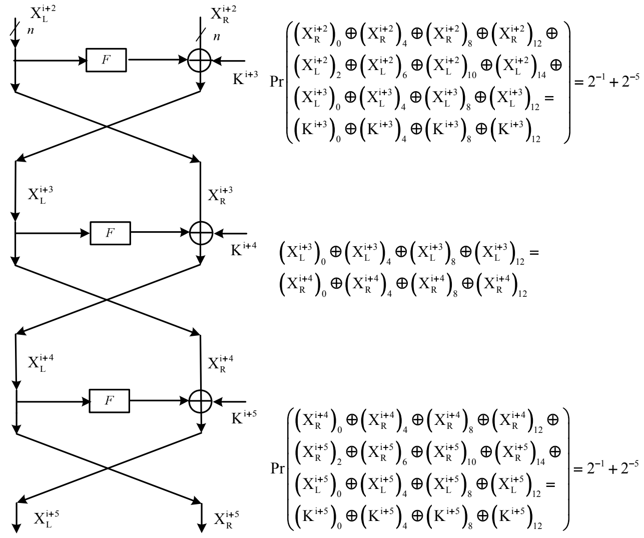

X_L^{i+2}
n
F
X_R^{i+2}
n
K^{i+3}
$\Pr\begin{pmatrix}(X_R^{i+2})_0\oplus(X_R^{i+2})_4\oplus(X_R^{i+2})_8\oplus(X_R^{i+2})_{12}\oplus\\(X_L^{i+2})_2\oplus(X_L^{i+2})_6\oplus(X_L^{i+2})_{10}\oplus(X_L^{i+2})_{14}\oplus\\(X_L^{i+3})_0\oplus(X_L^{i+3})_4\oplus(X_L^{i+3})_8\oplus(X_L^{i+3})_{12}=\\(K^{i+3})_0\oplus(K^{i+3})_4\oplus(K^{i+3})_8\oplus(K^{i+3})_{12}\end{pmatrix}=2^{-1}+2^{-5}$
X_L^{i+3}
X_R^{i+3}
F
K^{i+4}
$(X_L^{i+3})_0\oplus(X_L^{i+3})_4\oplus(X_L^{i+3})_8\oplus(X_L^{i+3})_{12}=$
$(X_R^{i+4})_0\oplus(X_R^{i+4})_4\oplus(X_R^{i+4})_8\oplus(X_R^{i+4})_{12}$
X_L^{i+4}
X_R^{i+4}
F
K^{i+5}
$\Pr\begin{pmatrix}(X_R^{i+4})_0\oplus(X_R^{i+4})_4\oplus(X_R^{i+4})_8\oplus(X_R^{i+4})_{12}\oplus\\(X_R^{i+5})_2\oplus(X_R^{i+5})_6\oplus(X_R^{i+5})_{10}\oplus(X_R^{i+5})_{14}\oplus\\(X_L^{i+5})_0\oplus(X_L^{i+5})_4\oplus(X_L^{i+5})_8\oplus(X_L^{i+5})_{12}=\\(K^{i+5})_0\oplus(K^{i+5})_4\oplus(K^{i+5})_8\oplus(K^{i+5})_{12}\end{pmatrix}=2^{-1}+2^{-5}$
X_L^{i+5}
X_R^{i+5}

Fig. 5: Another 3-round linear characteristic for SIMON include 4 active bits.

Table 11: Experimental results for the linear characteristic of 11-round SIMON 32/64, Equation 15.

P_n	Log (P_n)	C_n	Pr	Log(Bias)
179702664	27.42	89867759	0.5000914	-14.00378
1073741824	30	536877274	0.500005925	-12.63526
2526206249	31.2343	1263137717	0.50001369	-15.07817
4294967296	32	2147550464	0.500015557	-16.02790

Table 12: Sequences of approximation for SIMON 32/64.

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

D Linear Expressions for SIMON

A 14-Round Linear Expression for SIMON48/72 and SIMON48/96 is as follows:

$$\left(\begin{array}{l}(P_R)_{12} \oplus (P_L)[2,10,14,18] \oplus \\ (C_R)[0,16] \oplus (C_L)[2,18,22]\end{array}\right) = \left(\begin{array}{l}(K^1)_{12} \oplus (K^2)[2,14,18] \oplus (K^3)[0,16] \\ \oplus (K^4)[2,18,22] \oplus (K^5)_{20} \oplus (K^6)[2,22] \\ \oplus (K^7)_0 \oplus (K^8)_2 \oplus (K^{10})_2 \oplus (K^{11})_0 \oplus \\ (K^{12})[2,22] \oplus (K^{13})_{20} \oplus (K^{14})[2,18,22]\end{array}\right) \tag{21}$$

A 17-Round Linear Expression for SIMON64/96 and SIMON64/128 is as follows:

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

Table 13: Sequences of approximation for SIMON48/96.

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

A 27-Round Linear Expression for SIMON96/96 and SIMON96/144 is as follows:

$$\begin{pmatrix} (P_R)[0,40] \oplus (P_L)[2,38,42] \\ \oplus (C_R)[2,46,42] \oplus (C_L)_{44} \end{pmatrix} = \begin{pmatrix} (K^1)[0,40] \oplus (K^2)[2,42,46] \oplus (K^3)_{44} \oplus \\ (K^4)[2,46] \oplus (K^5)_0 \oplus (K^6)_2 \oplus (K^8)_2 \oplus (K^9)_0 \\ \oplus (K^{10})[2,46] \oplus (K^{11})_{44} \oplus (K^{12})[2,42,46] \oplus \\ (K^{13})[0,40,41] \oplus (K^{14})[2,38,42] \oplus \\ (K^{15})[36,41,42] \oplus (K^{16})[2,38,39,42] \oplus \\ (K^{17})[0,40] \oplus (K^{18})[2,42,46] \oplus (K^{19})_{44} \oplus \\ (K^{20})[2,46] \oplus (K^{21})_0 \oplus (K^{22})_2 \oplus (K^{24})_2 \oplus \\ (K^{25})_0 \oplus (K^{26})[2,46] \oplus (K^{27})_{44} \end{pmatrix} \tag{23}$$

A 34-Round Linear Expression for SIMON128/128, SIMON128/192 and SIMON128/256 is as follows:

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

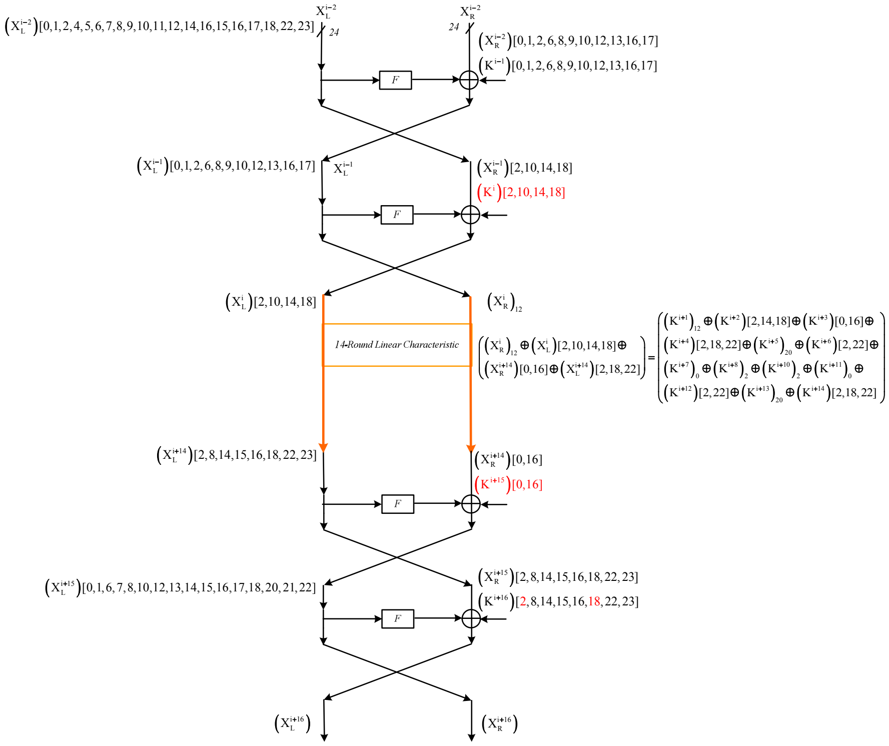
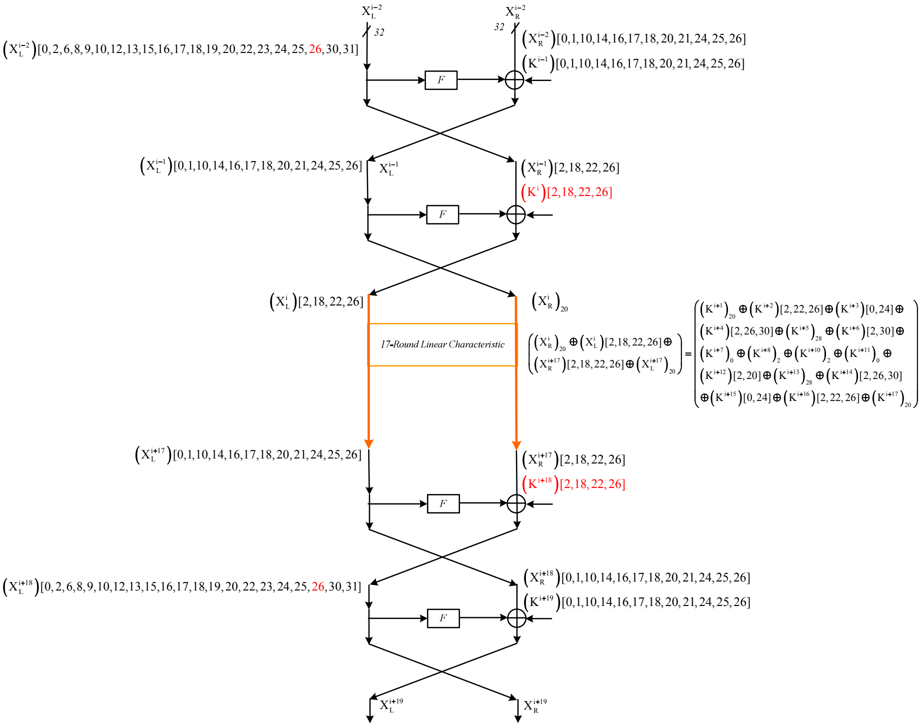
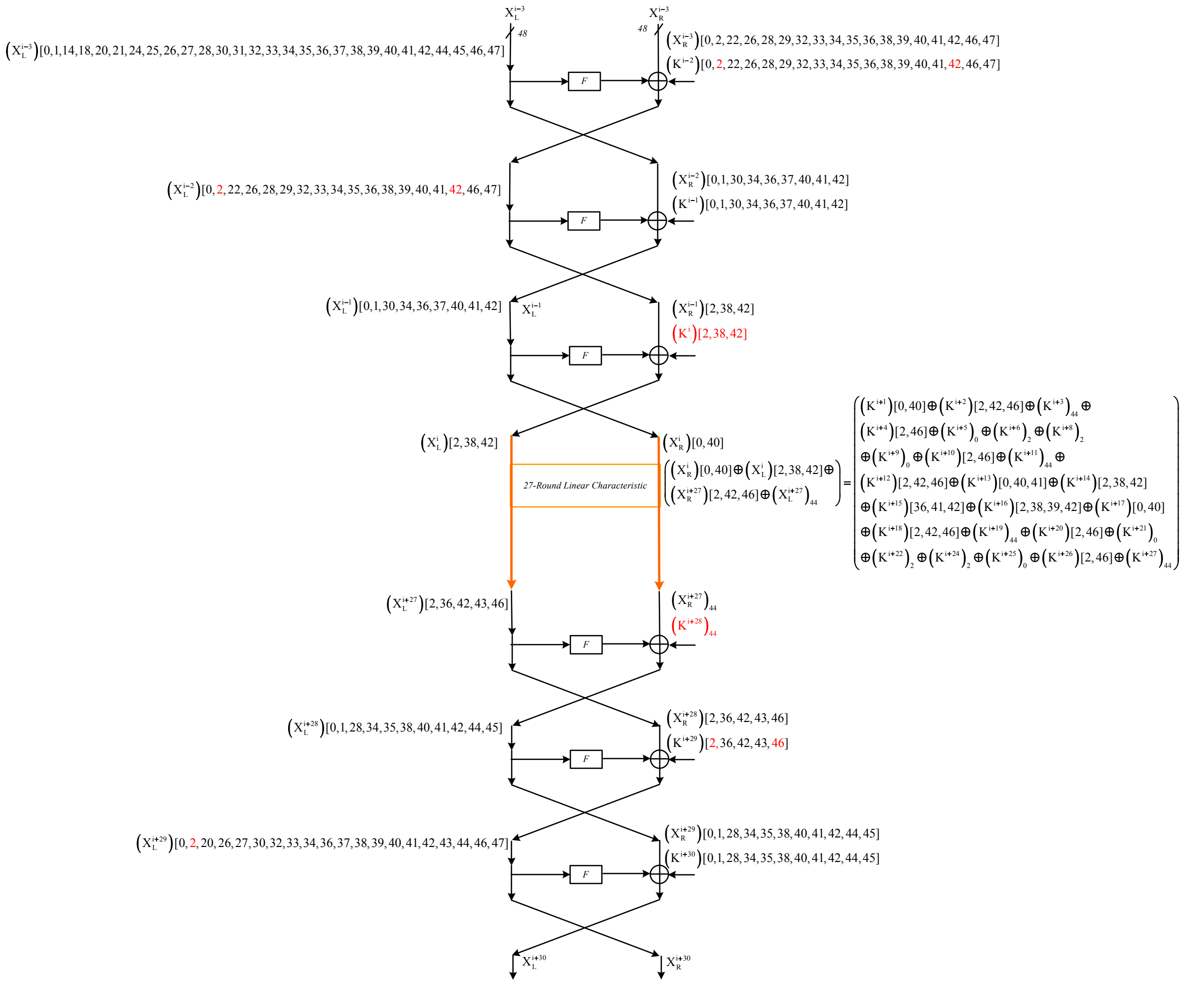

X_L^{i-2}
X_R^{i-2}
$\left(X_L^{i-2}\right)[0,1,2,4,5,6,7,8,9,10,11,12,14,16,15,16,17,18,22,23]$
24
24
$\left(X_R^{i-2}\right)[0,1,2,6,8,9,10,12,13,16,17]$
$\left(K^{i-1}\right)[0,1,2,6,8,9,10,12,13,16,17]$
F
$\left(X_L^{i-1}\right)[0,1,2,6,8,9,10,12,13,16,17]$
X_L^{i-1}
$\left(X_R^{i-1}\right)[2,10,14,18]$
$\left(K^{i}\right)[2,10,14,18]$
F
$\left(X_L^{i}\right)[2,10,14,18]$
$\left(X_R^{i}\right)_{12}$
14-Round Linear Characteristic
$\begin{pmatrix}\left(X_R^{i}\right)_{12}\oplus\left(X_L^{i}\right)[2,10,14,18]\oplus\\ \left(X_R^{i+14}\right)[0,16]\oplus\left(X_L^{i+14}\right)[2,18,22]\end{pmatrix}=\begin{pmatrix}\left(K^{i+1}\right)_{12}\oplus\left(K^{i+2}\right)[2,14,18]\oplus\left(K^{i+3}\right)[0,16]\oplus\\ \left(K^{i+4}\right)[2,18,22]\oplus\left(K^{i+5}\right)_{20}\oplus\left(K^{i+6}\right)[2,22]\oplus\\ \left(K^{i+7}\right)_{0}\oplus\left(K^{i+8}\right)_{2}\oplus\left(K^{i+10}\right)_{2}\oplus\left(K^{i+11}\right)_{0}\oplus\\ \left(K^{i+12}\right)[2,22]\oplus\left(K^{i+13}\right)_{20}\oplus\left(K^{i+14}\right)[2,18,22]\end{pmatrix}$
$\left(X_L^{i+14}\right)[2,8,14,15,16,18,22,23]$
$\left(X_R^{i+14}\right)[0,16]$
$\left(K^{i+15}\right)[0,16]$
F
$\left(X_L^{i+15}\right)[0,1,6,7,8,10,12,13,14,15,16,17,18,20,21,22]$
$\left(X_R^{i+15}\right)[2,8,14,15,16,18,22,23]$
$\left(K^{i+16}\right)[2,8,14,15,16,18,22,23]$
F
$\left(X_L^{i+16}\right)$
$\left(X_R^{i+16}\right)$

Fig. 6: The keys (in *black*) that should be guessed to attack 18 rounds of SIMON48/72.The *red* bits are not required to be guessed. For SIMON48/96 we add one round to the end of the current characteristic that needs guessing 16 bits its subkey.



X_L^{i-2}
X_R^{i-2}
32
32
$(X_L^{i-2})[0,2,6,8,9,10,12,13,15,16,17,18,19,20,22,23,24,25,26,30,31]$
$(X_R^{i-2})[0,1,10,14,16,17,18,20,21,24,25,26]$
$(K^{i-1})[0,1,10,14,16,17,18,20,21,24,25,26]$
F
$(X_L^{i-1})[0,1,10,14,16,17,18,20,21,24,25,26]$
X_L^{i-1}
$(X_R^{i-1})[2,18,22,26]$
$(K^{i})[2,18,22,26]$
F
$(X_L^{i})[2,18,22,26]$
$(X_R^{i})_{20}$
17-Round Linear Characteristic
$\left((X_R^{i})_{20}\oplus(X_L^{i})[2,18,22,26]\oplus (X_R^{i+17})[2,18,22,26]\oplus(X_L^{i+17})_{20}\right)=\left((K^{i+1})_{20}\oplus(K^{i+2})[2,22,26]\oplus(K^{i+3})[0,24]\oplus (K^{i+4})[2,26,30]\oplus(K^{i+5})_{28}\oplus(K^{i+6})[2,30]\oplus (K^{i+7})_{0}\oplus(K^{i+8})_{2}\oplus(K^{i+10})_{2}\oplus(K^{i+11})_{0}\oplus (K^{i+12})[2,20]\oplus(K^{i+13})_{28}\oplus(K^{i+14})[2,26,30] \oplus(K^{i+15})[0,24]\oplus(K^{i+16})[2,22,26]\oplus(K^{i+17})_{20}\right)$
$(X_L^{i+17})[0,1,10,14,16,17,18,20,21,24,25,26]$
$(X_R^{i+17})[2,18,22,26]$
$(K^{i+18})[2,18,22,26]$
F
$(X_L^{i+18})[0,2,6,8,9,10,12,13,15,16,17,18,19,20,22,23,24,25,26,30,31]$
$(X_R^{i+18})[0,1,10,14,16,17,18,20,21,24,25,26]$
$(K^{i+19})[0,1,10,14,16,17,18,20,21,24,25,26]$
F
X_L^{i+19}
X_R^{i+19}

Fig. 7: The keys (in *black*) that should be guessed to attack 21 rounds of SIMON64/96.The *red* bits are not required to be guessed. For SIMON64/128 we add one round to the end and one round to the beginning of the current characteristic that needs guessing 40 bits of their subkey.



X_L^{i-3}
X_R^{i-3}
48
48
$(X_L^{i-3})[0,1,14,18,20,21,24,25,26,27,28,30,31,32,33,34,35,36,37,38,39,40,41,42,44,45,46,47]$
$(X_R^{i-3})[0,2,22,26,28,29,32,33,34,35,36,38,39,40,41,42,46,47]$
$(K^{i-2})[0,2,22,26,28,29,32,33,34,35,36,38,39,40,41,42,46,47]$
F
$(X_L^{i-2})[0,2,22,26,28,29,32,33,34,35,36,38,39,40,41,42,46,47]$
$(X_R^{i-2})[0,1,30,34,36,37,40,41,42]$
$(K^{i-1})[0,1,30,34,36,37,40,41,42]$
F
$(X_L^{i-1})[0,1,30,34,36,37,40,41,42]$
X_L^{i-1}
$(X_R^{i-1})[2,38,42]$
$(K^{i})[2,38,42]$
F
$(X_L^{i})[2,38,42]$
$(X_R^{i})[0,40]$
27-Round Linear Characteristic
$\left((X_R^{i})[0,40]\oplus(X_L^{i})[2,38,42]\oplus (X_R^{i+27})[2,42,46]\oplus(X_L^{i+27})_{44}\right) = \left((K^{i+1})[0,40]\oplus(K^{i+2})[2,42,46]\oplus(K^{i+3})_{44}\oplus (K^{i+4})[2,46]\oplus(K^{i+5})_0\oplus(K^{i+6})_2\oplus(K^{i+8})_2 \oplus(K^{i+9})_0\oplus(K^{i+10})[2,46]\oplus(K^{i+11})_{44}\oplus (K^{i+12})[2,42,46]\oplus(K^{i+13})[0,40,41]\oplus(K^{i+14})[2,38,42] \oplus(K^{i+15})[36,41,42]\oplus(K^{i+16})[2,38,39,42]\oplus(K^{i+17})[0,40] \oplus(K^{i+18})[2,42,46]\oplus(K^{i+19})_{44}\oplus(K^{i+20})[2,46]\oplus(K^{i+21})_0 \oplus(K^{i+22})_2\oplus(K^{i+24})_2\oplus(K^{i+25})_0\oplus(K^{i+26})[2,46]\oplus(K^{i+27})_{44}\right)$
$(X_L^{i+27})[2,36,42,43,46]$
$(X_R^{i+27})_{44}$
$(K^{i+28})_{44}$
F
$(X_L^{i+28})[0,1,28,34,35,38,40,41,42,44,45]$
$(X_R^{i+28})[2,36,42,43,46]$
$(K^{i+29})[2,36,42,43,46]$
F
$(X_L^{i+29})[0,2,20,26,27,30,32,33,34,36,37,38,39,40,41,42,43,44,46,47]$
$(X_R^{i+29})[0,1,28,34,35,38,40,41,42,44,45]$
$(K^{i+30})[0,1,28,34,35,38,40,41,42,44,45]$
F
X_L^{i+30}
X_R^{i+30}

Fig. 8: The keys (in *black*) that should be guessed to attack 32 rounds of SIMON96/144.The *red* bits are not required to be guessed.

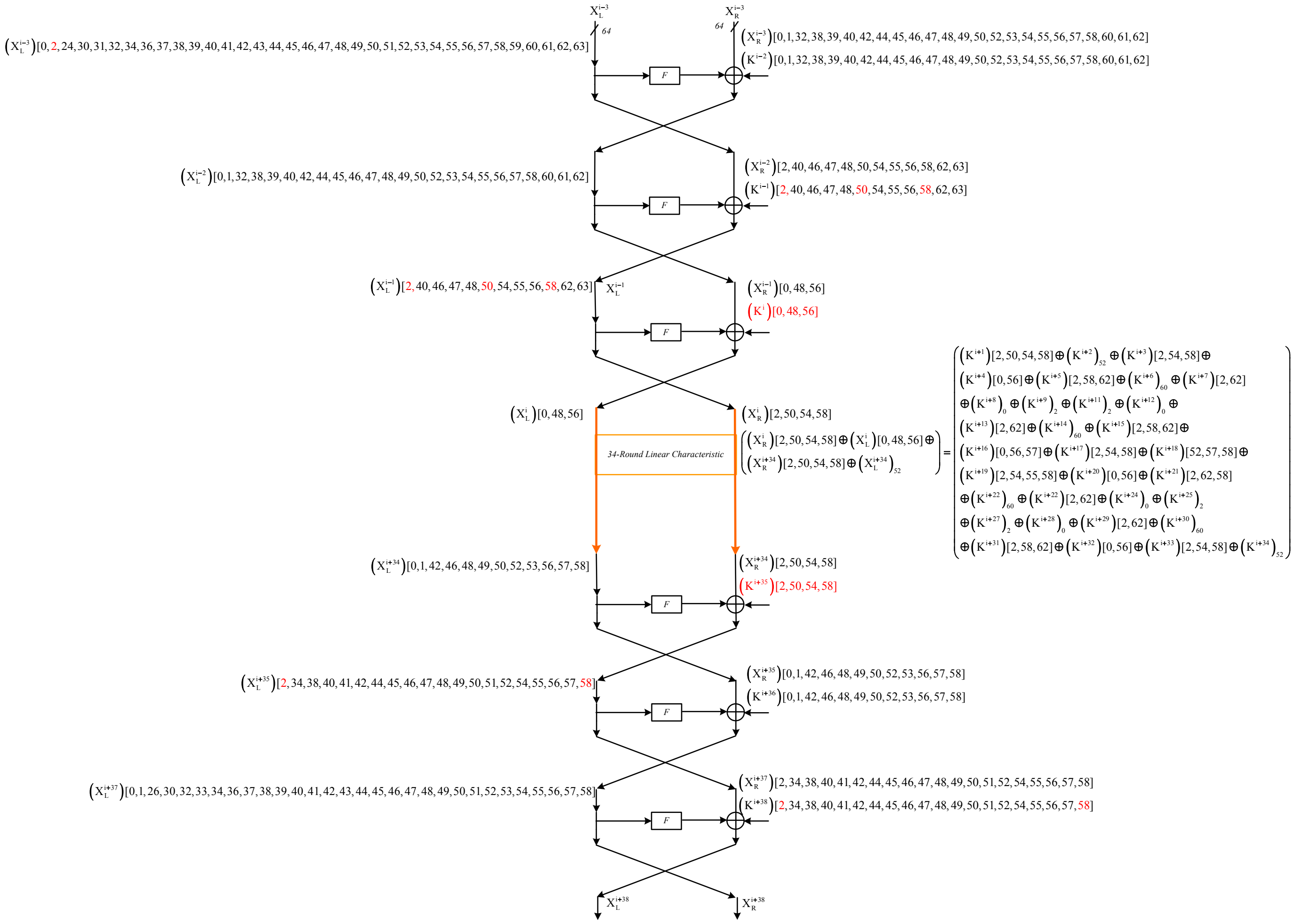

X_L^{i-3}
X_R^{i-3}
64
64
$(X_L^{i-3})[0,2,24,30,31,32,34,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]$
$(X_R^{i-3})[0,1,32,38,39,40,42,44,45,46,47,48,49,50,52,53,54,55,56,57,58,60,61,62]$
$(K^{i-2})[0,1,32,38,39,40,42,44,45,46,47,48,49,50,52,53,54,55,56,57,58,60,61,62]$
F
$(X_L^{i-2})[0,1,32,38,39,40,42,44,45,46,47,48,49,50,52,53,54,55,56,57,58,60,61,62]$
$(X_R^{i-2})[2,40,46,47,48,50,54,55,56,58,62,63]$
$(K^{i-1})[2,40,46,47,48,50,54,55,56,58,62,63]$
F
$(X_L^{i-1})[2,40,46,47,48,50,54,55,56,58,62,63]$
X_L^{i-1}
$(X_R^{i-1})[0,48,56]$
$(K^{i})[0,48,56]$
F
$(X_L^{i})[0,48,56]$
$(X_R^{i})[2,50,54,58]$
34-Round Linear Characteristic
$\begin{pmatrix}(X_R^{i})[2,50,54,58]\oplus(X_L^{i})[0,48,56]\oplus\\(X_R^{i+34})[2,50,54,58]\oplus(X_L^{i+34})_{52}\end{pmatrix}=\begin{pmatrix}(K^{i+1})[2,50,54,58]\oplus(K^{i+2})_{52}\oplus(K^{i+3})[2,54,58]\oplus\\(K^{i+4})[0,56]\oplus(K^{i+5})[2,58,62]\oplus(K^{i+6})_{60}\oplus(K^{i+7})[2,62]\\\oplus(K^{i+8})_{0}\oplus(K^{i+9})_{2}\oplus(K^{i+11})_{2}\oplus(K^{i+12})_{0}\oplus\\(K^{i+13})[2,62]\oplus(K^{i+14})_{60}\oplus(K^{i+15})[2,58,62]\oplus\\(K^{i+16})[0,56,57]\oplus(K^{i+17})[2,54,58]\oplus(K^{i+18})[52,57,58]\oplus\\(K^{i+19})[2,54,55,58]\oplus(K^{i+20})[0,56]\oplus(K^{i+21})[2,62,58]\\\oplus(K^{i+22})_{60}\oplus(K^{i+22})[2,62]\oplus(K^{i+24})_{0}\oplus(K^{i+25})_{2}\\\oplus(K^{i+27})_{2}\oplus(K^{i+28})_{0}\oplus(K^{i+29})[2,62]\oplus(K^{i+30})_{60}\\\oplus(K^{i+31})[2,58,62]\oplus(K^{i+32})[0,56]\oplus(K^{i+33})[2,54,58]\oplus(K^{i+34})_{52}\end{pmatrix}$
$(X_L^{i+34})[0,1,42,46,48,49,50,52,53,56,57,58]$
$(X_R^{i+34})[2,50,54,58]$
$(K^{i+35})[2,50,54,58]$
F
$(X_L^{i+35})[2,34,38,40,41,42,44,45,46,47,48,49,50,51,52,54,55,56,57,58]$
$(X_R^{i+35})[0,1,42,46,48,49,50,52,53,56,57,58]$
$(K^{i+36})[0,1,42,46,48,49,50,52,53,56,57,58]$
F
$(X_L^{i+37})[0,1,26,30,32,33,34,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58]$
$(X_R^{i+37})[2,34,38,40,41,42,44,45,46,47,48,49,50,51,52,54,55,56,57,58]$
$(K^{i+38})[2,34,38,40,41,42,44,45,46,47,48,49,50,51,52,54,55,56,57,58]$
F
X_L^{i+38}
X_R^{i+38}

Fig. 9: The keys (in *black*) that should be guessed to attack 40 rounds of SIMON128/192.The *red* bits are not required to be guessed. For SIMON128/256 we add one round to the end and one round to the beginning of the current characteristic that needs guessing 64 bits of their subkey.

Table 14: Sequences of approximation for SIMON64/128.

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

E Adding Extra Rounds to Each Variants of SIMON When Algorithm 2 of Matsui is Used

F Linear Hulls for SIMON

G Extending the Linear Hulls of SIMON

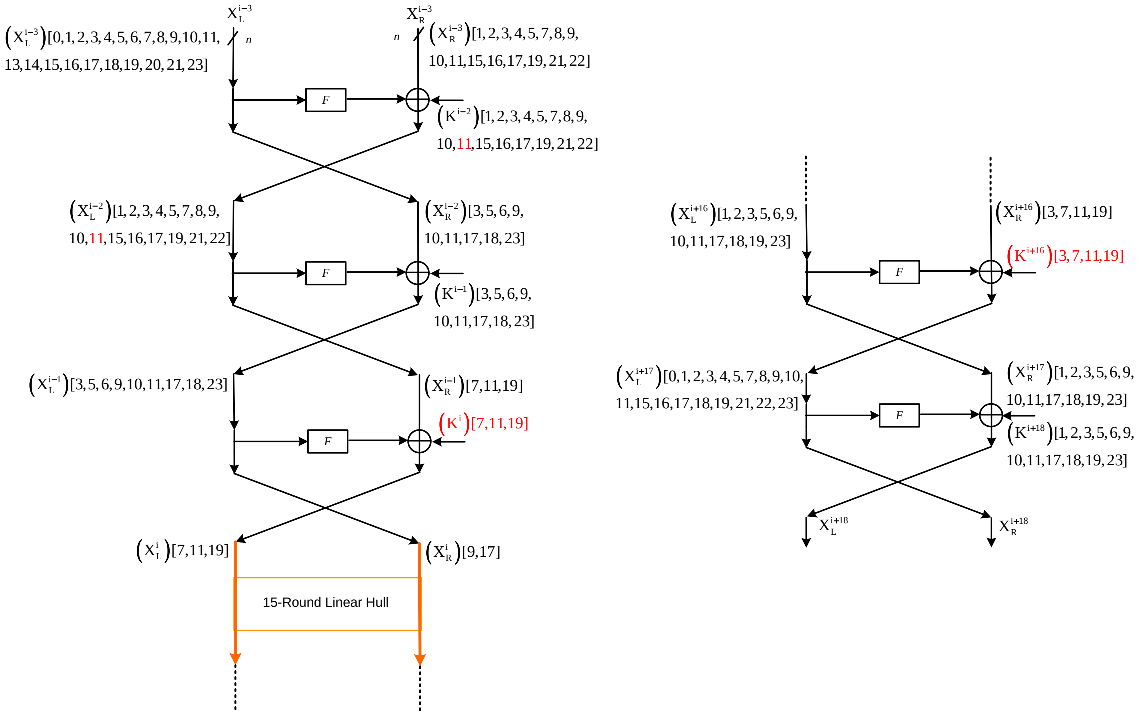


Fig. 10: Adding some rounds to the beginning and the end of the 15-round linear hull for SIMON 48/k.

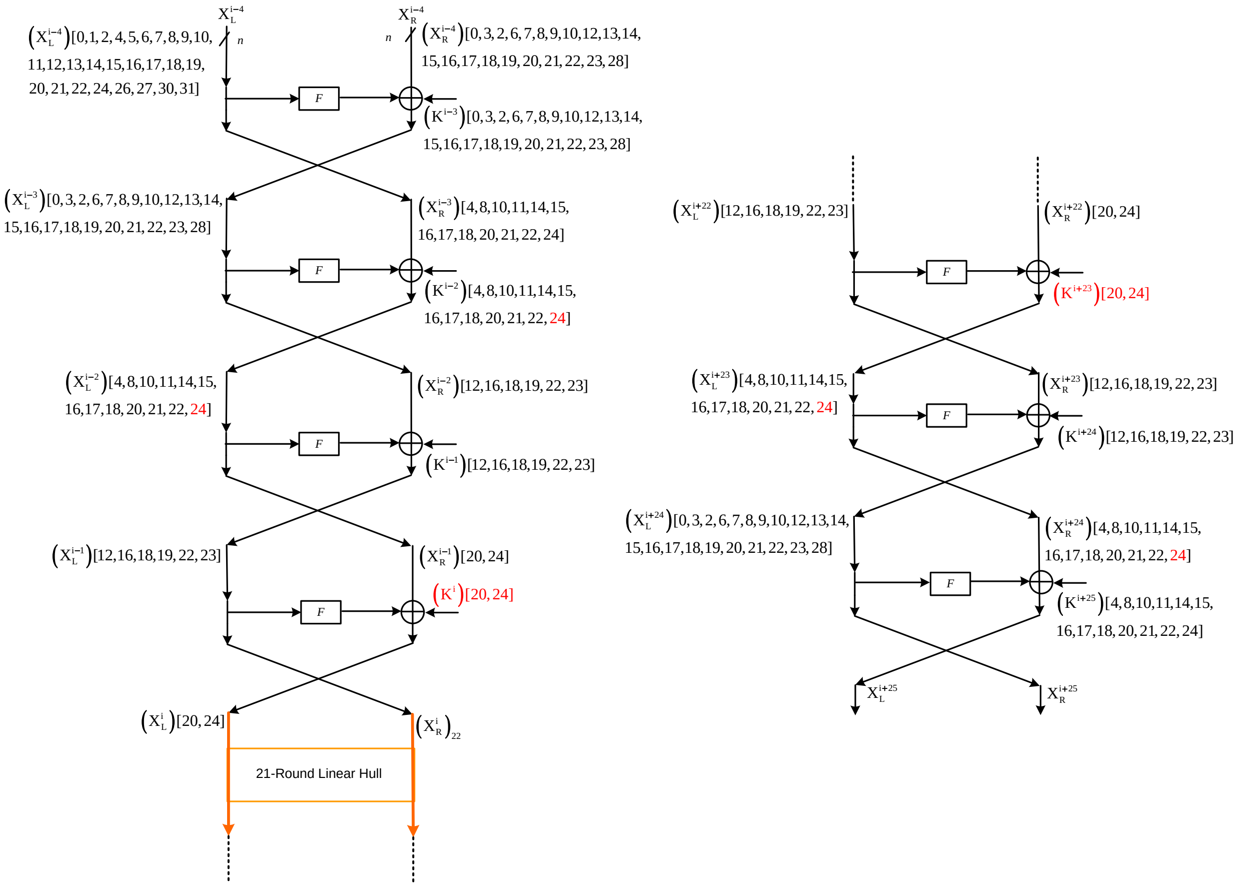

X_L^{i-4}
X_R^{i-4}
n
n
(X_L^{i-4})[0,1,2,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,24,26,27,30,31]
(X_R^{i-4})[0,3,2,6,7,8,9,10,12,13,14,15,16,17,18,19,20,21,22,23,28]
F
(K^{i-3})[0,3,2,6,7,8,9,10,12,13,14,15,16,17,18,19,20,21,22,23,28]
(X_L^{i-3})[0,3,2,6,7,8,9,10,12,13,14,15,16,17,18,19,20,21,22,23,28]
(X_R^{i-3})[4,8,10,11,14,15,16,17,18,20,21,22,24]
F
(K^{i-2})[4,8,10,11,14,15,16,17,18,20,21,22,24]
(X_L^{i-2})[4,8,10,11,14,15,16,17,18,20,21,22,24]
(X_R^{i-2})[12,16,18,19,22,23]
F
(K^{i-1})[12,16,18,19,22,23]
(X_L^{i-1})[12,16,18,19,22,23]
(X_R^{i-1})[20,24]
F
(K^{i})[20,24]
(X_L^{i})[20,24]
$(X_R^{i})_{22}$
21-Round Linear Hull
(X_L^{i+22})[12,16,18,19,22,23]
(X_R^{i+22})[20,24]
F
(K^{i+23})[20,24]
(X_L^{i+23})[4,8,10,11,14,15,16,17,18,20,21,22,24]
(X_R^{i+23})[12,16,18,19,22,23]
F
(K^{i+24})[12,16,18,19,22,23]
(X_L^{i+24})[0,3,2,6,7,8,9,10,12,13,14,15,16,17,18,19,20,21,22,23,28]
(X_R^{i+24})[4,8,10,11,14,15,16,17,18,20,21,22,24]
F
(K^{i+25})[4,8,10,11,14,15,16,17,18,20,21,22,24]
X_L^{i+25}
X_R^{i+25}

Fig. 11: Adding some rounds to the beginning and the end of the 21-round linear hull for SIMON 64/k.

Table 15: Sequences of approximation for SIMON96/144.

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 16: Sequences of approximation for SIMON128/256.

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

Table 17: Linear characteristics based on the differential trials by Birukov *et al.* for SIMON 48/k.

	Differential		Linear		
r	$\triangle_L$	$\triangle_R$	X_L	X_R	Used App.
0	5,21	3,7,19	7,11,19	9,17	1;1
1	3,19,23	5,21	9,17	11,15,19	1;1;1
2	1	3,19,23	11,15,19	13	1
3	19,23	1	13	15,19	1;1
4	21	19,23	15,19	17	1
5	19	21	17	19	1
6	-	19	19	-	-
7	19	-	-	19	1
8	21	19	19	17	1
9	19,23	21	17	15,19	1;1
10	1	19,23	15,19	13	1
11	3,19,23	1	13	11,15,19	1;1;1
12	5,21	3,19,23	11,15,19	9,17	1;1
13	3,7,19	5,21	9.17	7,11,19	1;1;1
14	9	3,7,19	7,11,19	5	1
15	3,7,11,19	9	5	3,7,11,19	-
	$\sum_r log_2 pr = -48$ $log_2 p_{diff} = -42.11$ $\#trails = 112573$		$log_2 \epsilon^2 = -50$ $log_2 \overline{c}_{LH}^2 = -44.11$ $\#characteristics = 112573$		

Table 18: Linear characteristics based on the differential trials by Birukov *et al.* for SIMON 64/k.

	Differential		Linear		
r	$\triangle_L$	$\triangle_R$	X_L	X_R	Used App.
0	26	24,28	20,24	22	1
1	24	26	22	24	1
2	-	24	24	-	-
3	24	-	-	24	1
4	26	24	24	22	1
5	24,28	26	22	20,24	1;2
6	29,30	24,28	20,24	18,19	2;2
7	0,24,28,30	29,30	18,19	16,18,20,24	1;3;2;1
8	2,26	0,24,28,30	16,18,20,24	14,22	1;1
9	0,4,24,30	2,26	14,22	12,16,18,24	1;1;3;3
10	-	0,4,24,30	12,16,18,24	-	-
11	0,4,24,30	-	-	12,16,18,24	1;1;3;3
12	2,26	0,4,24,30	12,16,18,24	14,22	1;1
13	0,24,28,30	2,26	14,22	16,18,20,24	1;3;2;1
14	29,30	0,24,28,30	16,18,20,24	18,19	2;2
15	24,28	29,30	18,19	20,24	1;2
16	26	24,28	20,24	22	1
17	24	26	22	24	1
18	-	24	24	-	-
19	24	-	-	24	1
20	26	24	24	22	1
21	24,28	26	22	20,24	-
	$\sum_r log_2pr = -72$ $log_2p_{diff} = -60.53$ $\#trails = 337309$		$log_2\epsilon^2 = -74$ $log_2\bar{c}_{LH}^2 = -62.53$ $\#characteristics = 337309$		

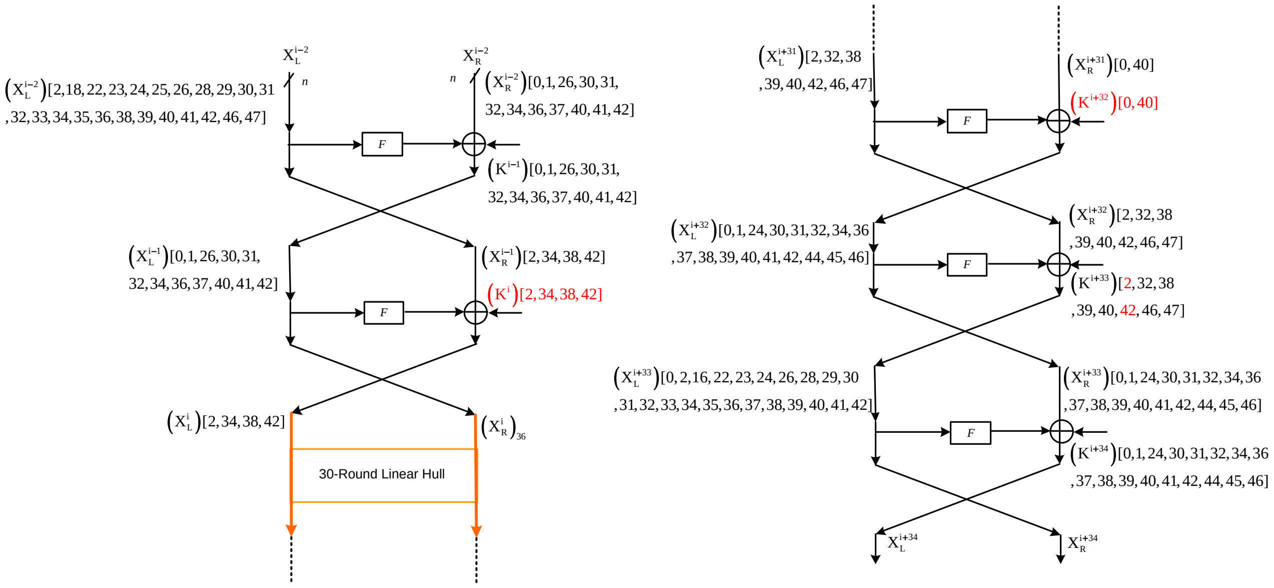


Fig. 12: Adding some rounds to the beginning and the end of the 30-round linear hull for SIMON 96/k.

Table 19: Linear characteristics based on the differential trials by Abed *et al.* for SIMON 96/k.

	Differential		Linear		
r	$\triangle_L$	$\triangle_R$	X_L	X_R	Used App.
0	20	6,14,18,22	2,42,38,34	36	1
1	6,14,18	20	0,40,0,40,36	2,42,38	1;1;1
2	8,16	6,14,18	2,46,42,46,38	0,40	1;1
3	6,10,14	8,16	44,0,44,40	2,46,42	1;1;1
4	12	6,10,14	2,46,42	44	1
5	6,10	12	0,0,44	2,46	1;1
6	8	6,10	2,46	0	1
7	6	8	0	2	1
8	-	6	2	-	-
9	6	-	0,0	2	1
10	8	6	2,46,46	0	1
11	6,10	8	44,0,44	2,46	1;1
12	12	6,10	2,46,42,42	44	1
13	6,10,14	12	0,41,40,0,44,41,40,	2,46,42	1;1;2
14	8,15,16	6,10,14	2,42,38,46,39,39,38	0,41,40	1;1;2
15	6,14,18	8,15,16	42,41,36,0,42,40,36	2,42,38	3;1;1
16	14,15,20	6,14,18	2,42,39,38,40,34,40,39,34	42,41,36	3;2;1
17	6,14,17,18	14,15,20	0,40,0,42,41,40,37,37,36	2,42,39,38	3;2;1;2
18	8,16	6,14,17,18	2,46,42,46,39,38	0,40	1;2
19	6,10,14	8,16	44,0,44,40	2,46,42	1;1;1
20	12	6,10,14	2,46,42	44	1
21	6,10	12	0,0,44	2,46	1;1
22	8	6,10	2,46	0	1
23	6	8	0	2	1
24	-	6	2	-	-
25	6	-	0	2	1
26	8	6	2,46	0	1
27	6,10	8	0,0,44	2,46	1;1
28	12	6,10	2,46,42	44	1
29	6,10,14	12	44,0,44,40	2,46,42	1;1;1
30	8,16	6,10,14	2,46,42	0,40	-
	$\sum_r log_2 pr = -106$ $log_2 p_{diff} = -92.2$		$log_2 \epsilon^2 = -108$ $log_2 \bar{c}^2_{LH} = -94.2$		

Table 20: Linear characteristics based on the differential trials by Abed *et al.* for SIMON 128/k.

	Differential		Linear		
r	$\triangle_L$	$\triangle_R$	X_L	X_R	Used App.
0	12	6,10,14	2,62,58	60	1
1	6,10	12	0,0,60	2,62	1;1
2	8	6,10	2,62	0	1
3	6	8	0	2	1
4	-	6	2	-	-
5	6	-	0,0	2	1
6	8	6	2,62,62	0	1
7	6,10	8	60,0,60	2,62	1;1
8	12	6,10	2,62,58,58	60	1
9	6,10,14	12	0,57,56,0,60,57,56,	2,62,58	1;1;2
10	8,15,16	6,10,14	2,58,54,62,55,55,54	0,57,56	1;1;2
11	6,14,18	8,15,16	58,57,52,0,58,56,52	2,58,54	3;1;1
12	14,15,20	6,14,18	2,58,55,54,56,50,56,55,50	58,57,52	3;2;1
13	6,14,17,18	14,15,20	0,56,0,58,57,56,53,53,52	2,58,55,54	3;2;1;2
14	8,16	6,14,17,18	2,62,58,62,55,54	0,56	1;2
15	6,10,14	8,16	60,0,60,56	2,62,58	1;1;1
16	12	6,10,14	2,62,58	60	1
17	6,10	12	0,0,60	2,62	1;1
18	8	6,10	2,62	0	1
19	6	8	0	2	1
20	-	6	2	-	-
21	6	-	0	2	1
22	8	6	2,62	0	1
23	6,10	8	0,0,60	2,62	1;1
24	12	6,10	2,62,58	60	1
25	6,10,14	12	60,0,60,56,57	2,62,58	1;1;2
26	8,15,16	6,10,14	2,62,58,62,55,54,55	0,57,56	1;1;2
27	6,14,18	8,15,16	0,57,56,0,58,56,52	2,58,54	3;1;1
28	14,15,20	6,14,18	2,58,54,56,50,55,56,50	58,57,52	3;2;1
29	6,14,17,18	14,15,20	58,57,52,0,58,56,57,53,52,53	2,58,55,54	3;2;1;2
30	8,16	6,14,17,18	2,58,55,54,62,54,55	0,56	1;2
31	6,10,14	8,16	0,56,0,60,56	2,62,58	1;1;1
32	12	6,10,14	2,62,58,58	60	1
33	6,10	12	60,0,60	2,62	1;1
34	8	6,10	2,62,62	0	1
35	6	8	0,0	2	1
36	-	6	2	-	-
37	6	-	0	2	1
38	8	6	2,62	0	1
39	6,10	8	0,0,60	2,62	1;1
40	12	6,10	2,62,58	60	1
41	6,10,14	12	60	2,62,58	-
	$\sum_r log_2pr = -144$ $log_2p_{diff} = -124.6$		$log_2\epsilon^2 = -146$ $log_2\overline{c}_{LH}^2 = -126.6$		

Table 21: Sequence of the bits of subkeys that must be guessed when some rounds is appended to the beginning and the end of the 15-round linear hull of SIMON 48/k.

r	Active bits in the left side	Active bits in the right side	# Guessing
i-3	0,1,2,3,4,5,6,7,8,9,10,11,13,14,15,16,17,18,19, 20,21,23	1,2,3,4,5,7,8,9,10,11,15,16,17,19,21,22	15
i-2	1,2,3,4,5,7,8,9,10,11,15,16,17,19,21,22	3,5,6,9,10,11,17,18,23	9
i-1	3,5,6,9,10,11,17,18,23	7,11,19	
i	7,11,19	9,17	
$\vdots$			
i+16	1,2,3,5,6,9,10,11,17,18,19,23	3,7,11,19	
i+17	0,1,2,3,4,5,7,8,9,10,11,15,16,17,18,19,21,22,23	1,2,3,5,6,9,10,11,17,18,19,23	12

Table 22: Sequence of the bits of subkeys that must be guessed when some rounds is appended to the beginning and the end of the 21-round linear hull of SIMON64/k.

r	Active bits in the left side	Active bits in the right side	# Guessing
i-4	0,1,2,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21, 22,24,26,27,30,31	0,3,2,6,7,8,9,10,12,13,14,15,16,17,18,19,20,21,22,23,28	21
i-3	0,3,2,6,7,8,9,10,12,13,14,15,16,17,18,19,20,21,22,23,28	4,8,10,11,14,15,16,17,18,20,21,22,24	12
i-2	4,8,10,11,14,15,16,17,18,20,21,22,24	12,16,18,19,22,23	6
i-1	12,16,18,19,22,23	20,24	
i	20,24	22	
⋮			
i+22	12,16,18,19,22,23	20,24	
i+23	4,8,10,11,14,15,16,17,18,20,21,22,24	12,16,18,19,22,23	6
i+24	0,3,2,6,7,8,9,10,12,13,14,15,16,17,18,19,20,21,22,23,28	4,8,10,11,14,15,16,17,18,20,21,22,24	12

Table 23: Sequence of the bits of subkeys that must be guessed when some rounds is appended to the beginning and the end of the 30-round linear hull of SIMON96/k.

r	Active bits in the left side	Active bits in the right side	# Guessing
i-2	2,18,22,23,24,25,26,28,29,30,31,32,33,34,35,36,38,39,40,41,42,46,47	0,1,26,30,31,32,34,36,37,40,41,42	12
i-1	0,1,26,30,31,32,34,36,37,40,41,42	2,34,38,42	
i	2,34,38,42	36	
⋮			
i+31	2,32,38,39,40,42,46,47	0,40	
i+32	0,1,24,30,31,32,34,36,37,38,39,40,41,42,44,45,46	2,32,38,39,40,42,46,47	6
i+33	0,2,16,22,23,24,26,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42 ,43,44,45,46,47	0,1,24,30,31,32,34,36,37,38,39,40,41,42,44,45,46	17

Table 24: Sequence of the bits of subkeys that must be guessed when some rounds is appended to the beginning and the end of the 41-round linear hull of SIMON128/k.

r	Active bits in the left side	Active bits in the right side	# Guessing
i-4	0,2,26,30,32,33,34,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63	0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63	27
i-3	0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63	0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63	17
i-2	0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63	0,1,50,54,56,57,58,60,61	9
i-1	0,1,50,54,56,57,58,60,61	2,58,62	
i	2,58,62	60	
⋮			
i+42	0,1,50,54,56,57,58,60,61	2,58,62	
i+43	0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63	0,1,50,54,56,57,58,60,61	9
i+44	0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63	0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63	17
i+45	0,2,26,30,32,33,34,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63	0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63	27

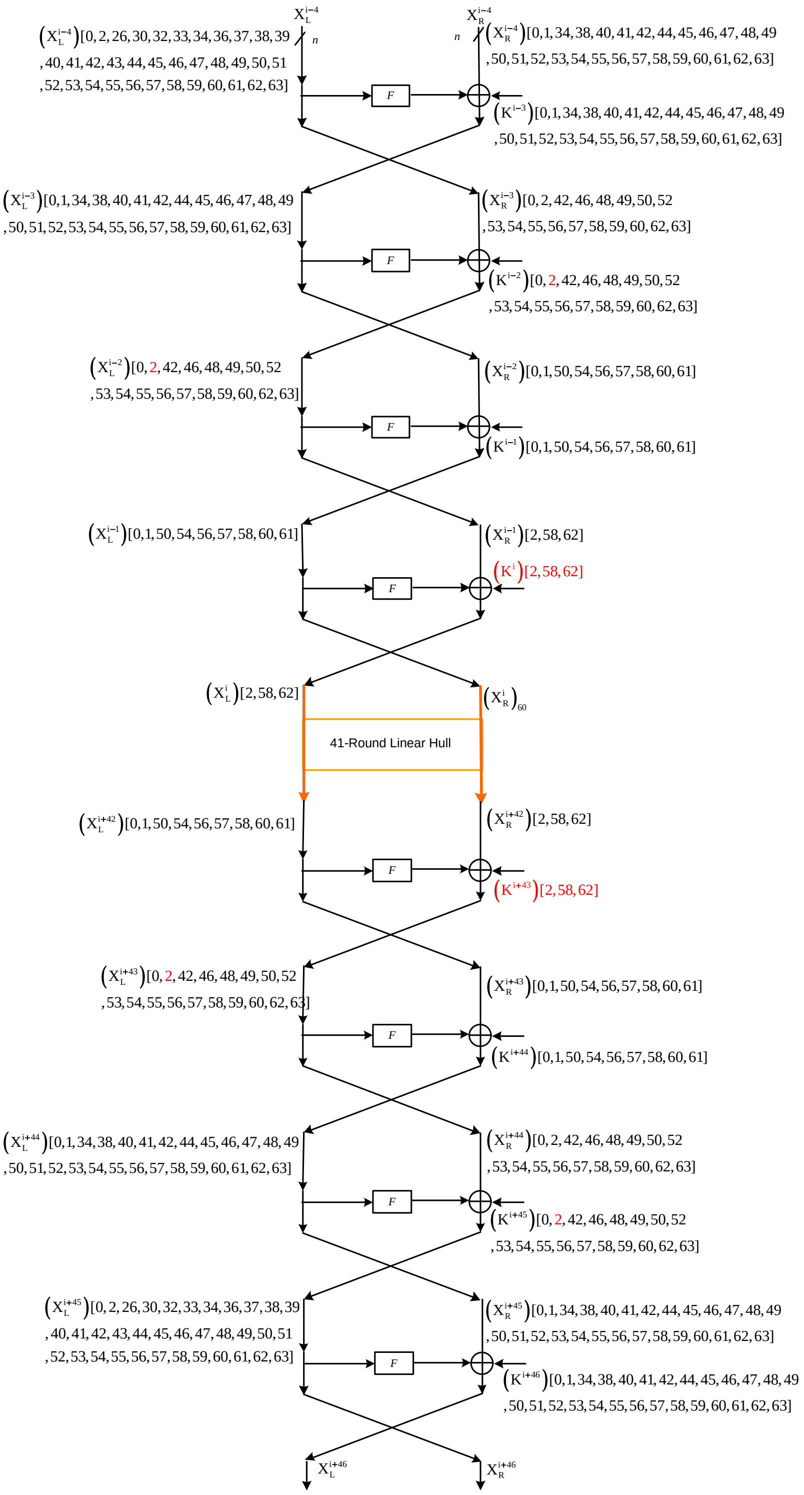

X_L^{i-4}
X_R^{i-4}
n
n
(X_L^{i-4})[0,2,26,30,32,33,34,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
(X_R^{i-4})[0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
F
(K^{i-3})[0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
(X_L^{i-3})[0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
(X_R^{i-3})[0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63]
F
(K^{i-2})[0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63]
(X_L^{i-2})[0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63]
(X_R^{i-2})[0,1,50,54,56,57,58,60,61]
F
(K^{i-1})[0,1,50,54,56,57,58,60,61]
(X_L^{i-1})[0,1,50,54,56,57,58,60,61]
(X_R^{i-1})[2,58,62]
(K^{i})[2,58,62]
F
(X_L^{i})[2,58,62]
$(X_R^{i})_{60}$
41-Round Linear Hull
(X_L^{i+42})[0,1,50,54,56,57,58,60,61]
(X_R^{i+42})[2,58,62]
F
(K^{i+43})[2,58,62]
(X_L^{i+43})[0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63]
(X_R^{i+43})[0,1,50,54,56,57,58,60,61]
F
(K^{i+44})[0,1,50,54,56,57,58,60,61]
(X_L^{i+44})[0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
(X_R^{i+44})[0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63]
F
(K^{i+45})[0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63]
(X_L^{i+45})[0,2,26,30,32,33,34,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
(X_R^{i+45})[0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
F
(K^{i+46})[0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
X_L^{i+46}
X_R^{i+46}

Fig. 13: Adding some rounds to the beginning and the end of the 30-round linear hull for SIMON 128/k.