Improved Linear Cryptanalysis of Reduced-round SIMON

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

[1] Section for Cryptology, DTU Compute, Technical University of Denmark, Denmark, {hoalk,mohab,mmeh}@dtu.dk
[2] ISSL, E.E. Department, Sharif University of Technology, Iran, alizadja@gmail.com
[3] E.E. Department, Shahid Rajaee Teacher Training University, Iran, NBagheri@srttu.edu
[4] Queensland University of Technology, Brisbane, Australia, p.gauravaram@gmail.com

Abstract. SIMON is a family of ten lightweight block ciphers published by Beaulieu et al. from U.S. National Security Agency (NSA). In this paper we investigate the security of SIMON against different variants of linear cryptanalysis techniques, i.e. classical and multiple linear cryptanalysis and linear hulls. We present a connection between linear- and differential characteristics as well as differentials and linear hulls in SIMON. We employ it to adapt the current known results on differential cryptanalysis of SIMON into the linear setting. In addition to finding a linear approximation with a single characteristic, we show the effect of the linear hulls in SIMON by finding better approximations that enable us to improve the previous results.

Our best linear cryptanalysis employs average squared correlation of the linear hull of SIMON based on correlation matrices. The result covers 21 out of 32 rounds of SIMON32/64 with time and data complexity $2^{54.56}$ and $2^{30.56}$ respectively. We have implemented our attacks for small scale variants of SIMON and our experiments confirm the theoretical biases and correlation 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, correlation matrix, branch and bound

1 Introduction

The rise of ubiquitous computing applications in the past decade has highlighted the criticality of using low-computing devices that are usually incapable of fully performing standard cryptographic algorithms in RFID and sensor networks environments. This trend has increased the need for lightweight cryptographic schemes. Therefore, design of lightweight cryptosystems has been regular practice over the last few years. For example, stream ciphers such as Grain [26] and Trivium [17], block ciphers such as PRESENT [15], LED [24] and PRINCE [16] to hash functions such as QUARK [7], PHOTON [23] and SPONGENT [14] have all been designed meeting the processing and storage demands of resource constrained devices.

In this direction, Beaulieu et al. of the U.S. National Security Agency (NSA) designed the SIMON and SPECK families of lightweight block ciphers that are targeted towards optimal hardware and software performance, respectively [8]. The SIMON family is constructed to meet hardware implementation flexibility and support efficient implementations across a wide variety of platforms. 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. There are ten variants of SIMON, forming a family of lightweight block ciphers.

Previous Work. In [2,3], Abed et al. presented analysis of SIMON using various cryptanalytic techniques including linear-, differential-, impossible differential- and rectangular attacks. In the direction of differential cryptanalysis, the authors presented differential attacks on reduced-round versions of all SIMON variants. In the direction of impossible differential analysis, attacks are presented on 13 out of 32 rounds for SIMON 32/64 with data and time complexities 2^{30} respectively $2^{50.1}$, and up to 25 out of 72 rounds for SIMON 128/256 with data and time complexities 2^{119} respectively 2^{195}. With respect to linear cryptanalysis, [3] 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.

Later, Alizadeh et al. [4] improved linear cryptanalysis of SIMON and presented attacks on 13-round SIMON32, 16-round SIMON48, 19-round SIMON64, 29-round SIMON96 and 36 round SIMON128/128.

In [12], 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. [36] 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. In [37], Wang *et al.* also improved results for SIMON32/64 for impossible differential cryptanalysis to 18 rounds for data and time complexities of 2^{32} and 2^{61} respectively. Other attack vectors are also presented; zero-correlation attacks are applied to 20 rounds with data and time complexities 2^{32} respectively $2^{56.9}$ and integral cryptanalysis techniques to 21 rounds with data and time complexities of 2^{31} respectively 2^{63}.

Contributions. In this paper we analyze the security of SIMON against variants of linear cryptanalysis. In the direction of classic linear cryptanalysis, using Algorithm 2 of Matsui, we extend attack of [4] to 17, 20, 23, 34 and 43 rounds for the respective block sizes of 32, 48, 64, 96 and 128 bits respectively. We also present a generalized algorithm based on the connection given by Alizadeh et al. in [4] 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 characteristics is generalized to a connection between capacity of a system of approximations (in multiple linear cryptanalysis) and a 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 21, 21, 29, 36, and 50 rounds of the respective block/key sizes of 32/64, 48/96, 64/128, 96/144, and 128/256 bits. Our focus on improving the linear cryptanalysis results on SIMON by estimating the average squared correlation of linear hulls. We show the linear hull effect by finding better approximations that enable us to break more rounds. 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 different concepts and notations around linear cryptanalysis of SIMON are described. Also, in Section 4 it is shown that there are different links and connections related to linear cryptanalysis and differential cryptanalysis, multiple linear cryptanalysis and linear hulls of SIMON, which can be used to improve attack results. In Section 5 we used squared correlation matrix to establish a linear hull of SIMON and investigate the data and time complexity for the smallest variant of SIMON. Finally, the paper is concluded in Section 7.

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

	SIMON	# Rounds	Data	Time
Matsui's Algorithm 1 [4]	32/64	13	2^{32}	2^{32}
Matsui's Algorithm 2	32/64	17	2^{32}	$2^{59.5}$
	48/72	19	2^{46}	2^{70}
	48/96	20	2^{46}	$2^{86.5}$
	64/96	22	2^{58}	2^{91}
	64/128	23	2^{58}	2^{108}
	96/144	34	2^{94}	$2^{136.5}$
	128/192	40	2^{128}	$2^{176.5}$
	128/256	42	2^{128}	$2^{235.5}$
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	21	$2^{31.69}$	$2^{63.69}$
	32/64	21	$2^{30.56}$	$2^{55.56}$
	48/72	20	$2^{44.11}$	$2^{70.61}$
	48/96	21	$2^{44.11}$	$2^{87.11}$
	64/96	27	$2^{62.53}$	$2^{88.53}$
	64/128	29	$2^{62.53}$	$2^{123.53}$
	96/144	36	$2^{94.2}$	$2^{135.2}$
	128/192	48	$2^{126.6}$	$2^{187.6}$
	128/256	50	$2^{126.6}$	$2^{242.6}$

2 Description of SIMON

SIMON is a family of lightweight block ciphers, designed by the NSA and published in 2013, to achieve an optimal hardware performance [8]. SIMON has a classical Feistel structure with the round block size of $N = 2n$ bits, where n is the word size representing the left or the right branch of the Feistel scheme at each round. The number of rounds 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 $X^r = X_L^r \| X_R^r$ and the subkey used in round r is denoted by K^r. Given a string X, $(X)_i$ denotes the ith bit of X. Bitwise circular left-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.

Each round of SIMON applies a non-linear, non-bijective (and hence non-invertible) function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ to the left half of the state. The output of F is added using XOR to the right half along with a round key, and the two halves are swapped. The function F is defined as

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

The single round of SIMON is represented in Figure 1. The subkeys are derived from a master key. Depending on the size K 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 [8].

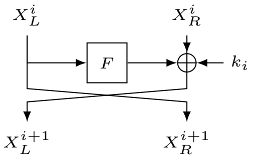


Fig. 1. The SIMON round function

3 Preliminaries

This section presents the main concepts used in the different cryptanalytic methods used throughout the paper.

Linear Cryptanalysis. Linear cryptanalysis [30] is a well-known cryptanalytic technique that has been employed on several block ciphers. Examples include the DES, FEAL-4, Serpent, Shannon and SAFER [30,35,19,25,28]. 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 that that of differential cryptanalysis which works under the chosen plaintext model. Linear cryptanalysis tries to find a highly probable linear expressions involving plaintext bits, ciphertext bits and the subkey bits as

$$\bigoplus_{i \in \mathcal{P}} P_i \bigoplus_{j \in \mathcal{C}} C_j = \bigoplus_{w \in \mathcal{K}} K_w.$$

for some sets $\mathcal{P}, \mathcal{C}, \mathcal{K} \subset \{0, \ldots, N-1\}$, and P, C, and K represents the plaintext, ciphertext and key, respectively. In this scenario, 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, Kaliski and Robshaw proposed in 1994 an algorithm that used several linear approximations [27]. The main constraint in the approach is that it uses only approximations in the same bits of subkeys $\mathcal{K}$, i.e. $\bigoplus_{w \in \mathcal{K}} K_w$. In 2004 Biryukov et al. proposed multiple linear cryptanalysis technique that does not require the constraint [11]. They successfully applied their approach to the DES. This approach has been also used in the cryptanalysis of reduced Serpent [20,21].

Linear Hulls. 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 [31] and used in cryptanalysis of several block ciphers such as PRESENT [29,**?**]. Linear hulls can be used in Matsui's Algorithm 2 [30] to decrease the complexity of linear attacks.

Multiple Linear Hulls. This is a combination of multiple linear cryptanalysis and linear hulls where if there are several linear hulls for a cipher, they can be used in the multiple linear cryptanalysis framework of Biryukov et al. [11] to decrease the complexity of linear attacks.

Correlation Matrix. Linear cryptanalysis finds a linear relation between some plaintexts bits, ciphertexts bits and some secret key bits and then exploits the bias or the correlation of this linear relation. In other words, the adversary finds an input mask α and an output mask β that yield a higher absolute *bias* $\epsilon_F(\alpha, \beta) \in [-\frac{1}{2}, \frac{1}{2}]$. In other words

$$Pr[\langle \alpha, X \rangle + \langle \beta, F_K(X) \rangle = \langle \gamma, K \rangle] = \frac{1}{2} + \epsilon_F(\alpha, \beta)$$

deviates from $\frac{1}{2}$, where $\langle \cdot, \cdot \rangle$ denotes an inner product. The correlation of a linear approximation is defined as

$$C_F(\alpha, \beta) := 2\epsilon_F(\alpha, \beta)$$

Another definition of the correlation which we will use later is

$$C_F(\alpha, \beta) := \hat{F}(\alpha, \beta)/2^n$$

where n is the block size of F in bits and $\hat{F}(\alpha,\beta)$ is the Walsh transform of F defined as follows

$$\hat{F}(\alpha,\beta) := \sum_{x\in\{0,1\}^n} (-1)^{\beta\cdot F(x)\oplus\alpha\cdot x}$$

For a given output mask β, the Fast Walsh Transform algorithm computes the Walsh transforms of an n-bit block size function F for all possible input masks α with output mask β using $n2^n$ arithmetic operations.

In order to find good linear approximations, one can construct a correlation matrix (or a squared correlation matrix). In the following, we state the definition the correlation matrix and show how the average squared correlation over all the keys is estimated.

Given a composite function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ such that

$$F = F_r \circ \cdots \circ F_2 \circ F_1,$$

We estimate the correlation of an r-round linear approximation (α_0, α_r) by considering the correlation of each linear characteristic between α_0 and α_r. The correlation of ith linear characteristic $(\alpha_0 = \alpha_{0i}, \alpha_{1i}, \cdots, \alpha_{(r-1)i}, \alpha_r = \alpha_{ri})$ is

$$C_i = \prod_{j=1}^{r} C_{F_j}(\alpha_{(j-1)i}, \alpha_{ji})$$

It is well known, see e.g. [22], that the correlation of a linear approximation is the sum of all correlations of linear trails starting with the same input mask α and ending with the same output mask β, i.e. $C_F(\alpha_0, \alpha_r) = \sum_{i=1}^{N_l} C_i$, where N_l is the number of all the possible linear characteristics between (α_0, α_r).

When considering the round keys which affects the sign of the correlation of a linear trail, the correlation of the linear hull (α, β) is

$$C_F(\alpha,\beta) = \sum_{i=1}^{N_l} (-1)^{d_i} C_i,$$

where $d_i \in \mathbb{F}_2$ refers to the sign of the addition of the subkey bits on the ith linear trail. In order to estimate the data complexity of a linear attack, one uses the average squared correlation over all the keys which is equivalent to the sum of the squares of the correlations of all trails, $\sum_i C_i^2$, assuming independent round keys [22].

Let C denote the correlation matrix of an n-bit key-alternating cipher. C has size $2^n \times 2^n$ and $C_{i,j}$ corresponds to the correlation of an input mask, say α_i, and output mask, say β_j. Now the correlation matrix for the keyed round function is obtained by changing the signs of each row in C according to the round subkey bits or the round constant bits involved. Squaring each entry of the correlation matrix gives us the squared correlation matrix M. Computing M^r gives us the squared correlations after r number of rounds. This can not be used for real block ciphers that have block sizes of at least 32-bit as in the case of Simon32/64. So in order to find linear approximations one can construct a submatrix of the correlation (or the squared correlation) matrix [1,14]. In Section 5, we construct a squared correlation submatrix for Simon in order to find good linear approximations.

4 Connections and Linear Cryptanalysis of SIMON

In this section we will investigate the possibility to use connections between differential and linear cryptanalysis and its variants in order to provide better results on SIMON. In some cases as in multiple linear cryptanalysis and linear hulls, this yields a better time and data complexity for more rounds.

4.1 Connections between Linear- and Differential Characteristics for SIMON

In this section, we explain the connections described in [4] pertaining to the connection between linear- and differential characteristics for SIMON, and its application to SIMON variants other than SIMON32/64.

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 $\frac{3}{4}$. Hence, we can extract the following highly biased linear expressions for the F-function:

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

Similarly, differential cryptanalysis [10] is a widely used chosen plaintext/ciphertext cryptanalytic attack technique. In a differential attack we look for an input pair with difference ΔX that propagates to an output pair with difference ΔY with a high probability p. This differential characteristic is denoted by $\Delta X \xrightarrow{p} \Delta Y$.

There are many works which discuss connection between differential and linear characteristics [18,13]. We observe that there is an explicit connection between linear characteristic and differential characteristic for SIMON. This observation is explained as follows. We can also extract the following highly probable differential expressions for the F-function:

$$\left.\begin{array}{ll}\text{Differential Characteristic 1}: & (\Delta X)_i \xrightarrow{\frac{1}{4}} (\Delta F(X))_{i+2}\\ \text{Differential Characteristic 2}: & (\Delta X)_i \xrightarrow{\frac{1}{4}} (\Delta F(X))_{i+2,i+1}\\ \text{Differential Characteristic 3}: & (\Delta X)_i \xrightarrow{\frac{1}{4}} (\Delta F(X))_{i+2,i+8}\\ \text{Differential Characteristic 4}: & (\Delta X)_i \xrightarrow{\frac{1}{4}} (\Delta F(X))_{i+2,i+1,i+8}\end{array}\right\}, \quad (2)$$

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 (and similarly for the other expressions). Given Equations 2 and comparing it with the related equation for a linear approximation of the function F, i.e. Equations 1, 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 1 and Equations 2. In other words, each approximation in Equation 1 can be mapped to a differential characteristic in Equation 2. Based on this observation, Algorithm 1

Algorithm 1: A general algorithm to convert an r-round differential characteristic (DC) for SIMON N/K to an equivalent r-round linear characteristic (LC) for SIMON N/K.

```
Input:
  – An $r$-round DC for SIMON $N/K$, where
      • $(\Delta X)^i_L; (\Delta X)^i_R$ for $0 \leq i \leq r$
      • $N = 2n$
      • DC is given as a sequence of the location of active bits for each round in the
        left/right side.

$X^i_L \leftarrow (\Delta X)^i_R$ and $X^i_R \leftarrow (\Delta X)^i_L$, for $0 \leq i \leq r$
// $(\Delta X)^i_R$ is the sequence of active bits in the right side of round $i$ of the given DC;
if $(\Delta X)^i_R \neq \phi$ then        // $(\Delta X)^0_R \neq \phi$ means there is no active bit in $(\Delta X)^0_R$
    select $x \in (\Delta X)^0_R$         // $x$ is a location of an active bit in $(\Delta X)^0_R$
else
    select $x \in (\Delta X)^0_L$         // $x$ is a location of an active bit in $(\Delta X)^0_L$

select $y \leq \frac{N}{2}$ // $y$ is a position in LC which corresponds to the position $x$ of the DC, note
  that DC/LC are rotation invariant [2];
for $0 \leq i \leq r$ and for any $z \in \{X^i_L; X^i_R\}$: $z \leftarrow y - (x - z)\ mod\ \frac{N}{2}$ // any active bit in the DC has
  an equivalent active bit in the generated LC;
return $X^i_L; X^i_R$ for $0 \leq i \leq r$ ;
```

represents an approach to convert an r-round differential characteristic to an equivalent r-round linear 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 [2]. For SIMON32/64 reduced to 11 rounds, a linear characteristics based on the Abed *et. al.* [2] 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 found the following pattern

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

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

$$2, 3, 1, 2, 1, 1, 0, 1, 1, 2, 1.$$

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 2. On the other hand, to use an approximation with the bias of ϵ to mount a linear attack the expected complexity is $O(\epsilon^{-2})$ [30]. Hence, we consider a case where $\epsilon \geq 2^{-n+2}$, where $N = 2n$ and for the complexity of $8 \times \epsilon^{-2}$ the success probability of key recovery attack would be 0.997 [2,30]. Our results for different variants of SIMON when $\epsilon \geq 2^{-n+2}$ have been represented in Table 3.

Table 2. Summary of linear analysis for the different variants of SIMON [4]. 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.

	Linear Expression							
	Start		End					
SIMON	Active bits in the left side	Active bits in the right side	Active bits in the left side	Active bits in the right side	# Rounds	# App.	Bias	Attack
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 3. Summary of linear analysis for the different variants of SIMON such that one can mount a linear attack with the success probability of 0.997 [4]. In this table **App.** denotes approximation.

	Linear Expression						
	Start		End				
SIMON	Active bits in the left side	Active bits in the right side	Active bits in the left side	Active bits in the right side	# Rounds	# App.	Bias
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}

Letting $(X)[i_1, ..., i_m] = (X)_{i_1} \oplus \ldots \oplus (X)_{i_m}$, 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 SIMON32/64 is

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

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

Given an 11-round linear characteristic such as Equation 3, 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 [4]. To extend the 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:

$$(X_R^i)[0,8] \oplus (X_L^i)[2,10,14] \oplus (X_R^{i+11})[6,10] \oplus (X_L^{i+11})_4. \quad (4)$$

With respect to Figure 2, we can append a further round to the beginning of the cipher to find a new 12-round linear characteristic. Since SIMON injects the subkey at the end of its round function, then this work does not have any computational complexity. More precisely, for the current 11-round linear hull, we evaluate $(X_R^i)[0,8] \oplus (X_L^i)[2,10,14] \oplus (X_R^{i+11})[6,10] \oplus (X_L^{i+11})_4$. If we add a round in the backwards direction, i.e. round $i-1$, we can determine $(X_L^i)[2,10,14]$ as a function of $F(X_L^{i-1})[2,10,14] \oplus (K^i)[2,10,14] \oplus X_R^i)[2,10,14]$, where we know X_R^{i-1} and X_L^{i-1}. Hence, it is possible to use the correlation of the following linear relation to filter the wrong subkeys:

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

We can continue our method to add more rounds to the beginning of linear hull in the cost of guessing some bits of subkeys. To add more rounds in backward, for example we must guess the bit $(F(X_L^{i-1}))_2 = (X_L^{i-1})_0 \oplus ((X_L^{i-1})_1 \& (X_L^{i-1})_{10})$. On the other hand, to determine $(F(X_L^{i-1}))_2$ one should guess $(X_L^{i-1})_0$ and $(X_L^{i-1})_1$ only if the guessed value for $(X_L^{i-1})_{10}$ is 1. So, in average we need one bit guess for $(X_L^{i-1})_1$ and $(X_L^{i-1})_{10}$ (in Figure 2 such bits are indicated in blue).

Figure 2 shows the bits of subkeys that should be guessed when we add 3 rounds to the beginning and 3 rounds to the end of the above 11-round characteristic (27.5 bits of subkeys). Hence, we can attack 17 rounds of SIMON32/64 using Algorithm 2 of Matsui to recover the key. The time complexity for this attack is $2^{59.5}$ and the data complexity is 2^{32}.

Similarly, in Appendix B, we apply this technique to the variants SIMON48/K, SIMON64/K, SIMON96/K and SIMON128/K, to extend the linear characteristics to more rounds. In particular, we use Algorithm 2 of Matsui to recover the key, where we guess subkeys 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 5, 6, 7 and 8 in Appendix B show the bits of subkeys that should be guessed when we add extra rounds to each variants of SIMON. The results using Matsui's Algorithm 2 are summarized in Table 1.

4.3 Multiple Linear Cryptanalysis of SIMON

The technique of multiple linear cryptanalysis, an improved version of the linear cryptanalysis, is proposed by Biryukov et al. in 2004 [11]. 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:

$$P_{p_j}^i \oplus C_{c_k}^i = K_{k_l}^i \quad (1 \leqslant i \leqslant m). \quad (5)$$

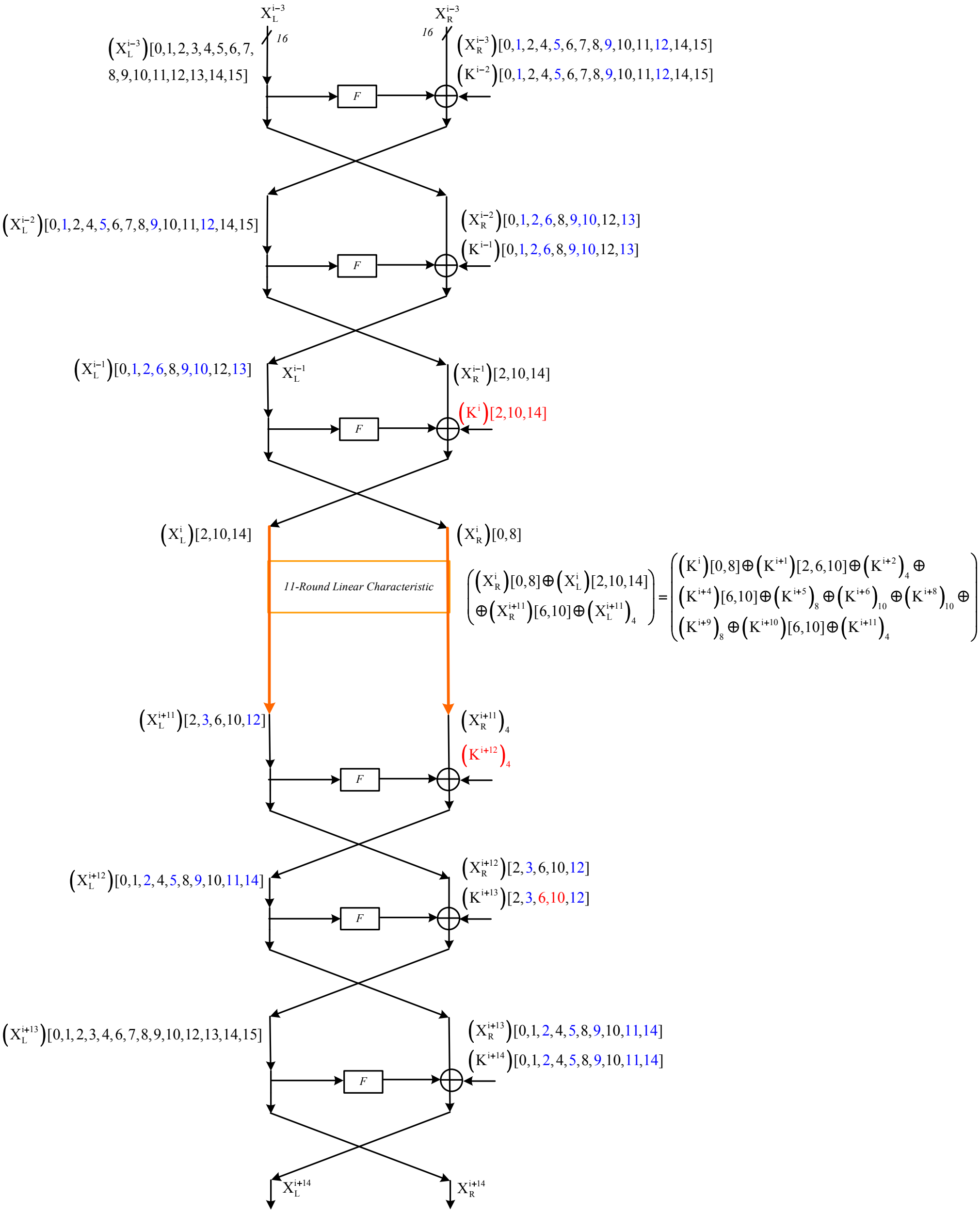

X_L^{i-3}
X_R^{i-3}
16
16
$(X_L^{i-3})[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15]$
$(X_R^{i-3})[0,1,2,4,5,6,7,8,9,10,11,12,14,15]$
$(K^{i-2})[0,1,2,4,5,6,7,8,9,10,11,12,14,15]$
F
$(X_L^{i-2})[0,1,2,4,5,6,7,8,9,10,11,12,14,15]$
$(X_R^{i-2})[0,1,2,6,8,9,10,12,13]$
$(K^{i-1})[0,1,2,6,8,9,10,12,13]$
$(X_L^{i-1})[0,1,2,6,8,9,10,12,13]$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

Fig. 2. The keys (in *black*) that should be guessed to attack 17 rounds of SIMON32/64. The red bits are not required to be guessed and the blue bits cost guessing a half bit on average.

The goal is to recover bits of key or finding some informations about the key bits that appear in Equation 5. 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 [30], the values of $K^i_{k_l}$ are determined from the 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 [30,20]. In [11] the authors show that the 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, which is given by

$$\bar{c}^2 = 4 \times \sum_{i=1}^{m} \epsilon_i^2. \tag{6}$$

In other words, by increasing the quantity of Equation 6, one can decrease the data complexity of the attack. Therefore, finding more approximations is the main task in multiple linear cryptanalysis.

For each variant of reduced-round SIMON, one can find more than one linear characteristic with desirable bias. Thus, we can use the multiple linear cryptanalysis technique to present an improved linear attack on SIMON. To find a linear characteristic for SIMON32/64, 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 SIMON32/64. The results are presented in Table 11. Now, if another bit, except bit “2”, is considered at the beginning of the work, then another table, different from Table 11, and another 11-round linear characteristic with bias 2^{-16} for SIMON32/64 is produced. Since there are 16 bits in the right half of state of SIMON32/64, 16 tables like Table 11 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 1. 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 SIMON32/64 in table 2, 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 4^3 different approximations, but identical probability. The different approximations produce 64 linear characteristics of bias 2^{-16} for 11-round SIMON32/64. With respect to the 16 bits of right half of state in SIMON32/64, the number of 11-round linear characteristics of bias 2^{-16} is

$$4^3 \times 16 = 2^{10}.$$

Given these approximations, one can present an improved linear attack on reduced-round SIMON, explained for SIMON32/64 in Section 4.3.

Similarly, many approximations for reduced rounds of other variants of SIMON can be found, see Tables 11, 12, 13, 14, and 15. Note that the patterns in Tables 11, 12, 13, 14, and 15, are produced by considering only one bit in the state of cipher.

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:

$$EDP(\alpha, \beta) = \sum_i p_i(\alpha, \beta). \tag{7}$$

In this section, we extend the given connection between a linear characteristic and differential characteristic in Section 4.1 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 $1 \leq i \leq m$. Then expected differential probability, p, for the m differential characteristics is:

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

On the other hand in Section 4.1, 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

$$p = \sum_{i=1}^{n} p_i = \sum_{i=1}^{n} 4 \times \epsilon_i^2 = 4 \times \sum_{i=1}^{n} \epsilon_i^2 = \bar{c}^2. \tag{8}$$

□

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 SIMON32/K, 48/K and 64/K in [12] 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 4.

Table 4. 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

A Key Recovery Attack on 18-round of SIMON32/64 based on Multiple Linear Cryptanalysis. In this section, the multiple linear attack on SIMON32/64 is described. One can use Table 11 to construct $4 \times 4 \times 16$ approximations of bias 2^{-22} for 16-round SIMON32/64. The capacity of the system based on those approximations is:

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

Thus, the data complexity of a linear attack based on the system exceeds the full codebook. However, another system of approximations with desirable properties can be constructed. For this, consider Table 5 which is a partition of Table 11. The active bit (the bit that must be approximated) in the right side of 15th round in Table 5 is bit “2”. This bit can be approximated using one of the four approximations in Equation 1.

Suppose that approximation 1 is used. Then the active bit in the right side of 16th round will be bit “0” which can be approximated using one of the four approximations in Equation 1. This results in $4 \times 16 \times 4$ linear characteristics of bias 2^{-22} for 16-round SIMON. Now, suppose that bit “2” in the right side of 15th round is approximated using approximation 2 in Equation 1. Then, the active bits in the right side of 16th round are bits “0” and “1” that each of them can be approximated using one of the four approximations in Equation 1 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 15th round is approximated using approximation 3 in Equation 1, another $4 \times 16 \times 4^2$ linear characteristics of bias 2^{-23} for 16-round SIMON can be produced. Finally, if bit “2” in the right side of 15th round is approximated using approximation 4 in Equation 1, then the active bits in the right side of 16th round are bits “0”, “1”, and “10” that each of them can be approximated using one of the four approximations in Equation 1. In other words, $4 \times 16 \times 4^3$ linear characteristics of bias 2^{-24} for 16-round SIMON32/64 can be found. The results are summarized in Table 6. Hence, the capacity of those approximations will be

Table 5. A system of linear equations for SIMON32/64 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

determined as

$$\bar{c}^2 = 4 \times 16 \times 4 \times (4 \times 2^{-44} + 2 \times 4^2 \times 2^{-46} + 4^3 \times 2^{-48}) = 2^{-32}.$$

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.

Table 6. Different approximations of bit “2” in the 15th round

App. variant	active bit(s) in the left of 15th round	active bit(s) in the right of 16th round	# app in the 16th round	# equations 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

4.4 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*

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

Alkhzaimi and Lauridsen in [6] and Abed et al. in [3] 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. [12]. Based on the connection between linear hulls and differentials of SIMON, one can use the differentials by Abed et al. in [3] or differentials by Biryukov et al. in [12] to find the corresponding linear hulls for variants of reduced-round SIMON. We find the linear characteristics for SIMON32/64, $48/K$, and $64/K$ reduced to 13, 15, and 21 rounds, respectively, based on the differential trails by Biryukov 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 7, and Tables 16, 17, 18, and 19 in Appendix C.

Table 7. Linear characteristics based on the differential trials by Biryukov et al. for SIMON32/64

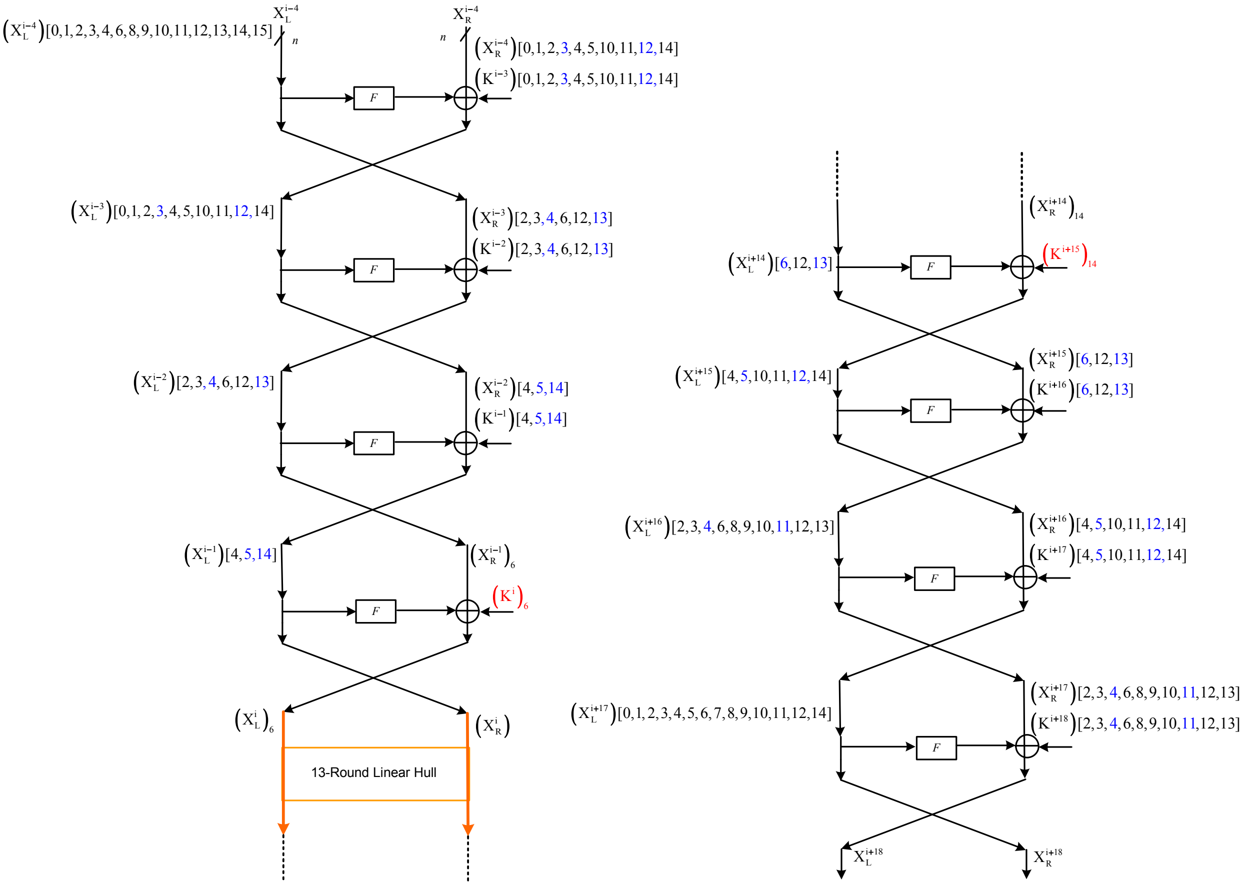
	Differential		Linear		
r	$\triangle_L$	$\triangle_R$	X_L	X_R	Used App.
0	$-$	6	6	$-$	$-$
1	6	$-$	$-$	6	1
2	8	6	6	4	1
3	$6, 10$	8	4	$2, 6$	$1; 1$
4	12	$6, 10$	$2, 6$	0	1
5	$6, 10, 14$	12	0	$2, 6, 14$	$1; 1; 1$
6	$0, 8$	$6, 10, 14$	$2, 6, 14$	$4, 12$	$1; 1$
7	$2, 6, 14$	$0, 8$	$4, 12$	$6, 10, 14$	$1; 1;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

Extending Linear Hulls and Key Recovery Attack on SIMON32/64. Similar to the approach we used to extend a linear characteristic when it is used in Algorithm 2 of Matsui (see Section 4.2), it is possible to extend a given linear hull for more rounds. For example, consider the linear hull based on the differential by Biryukov et al. for 13-round SIMON32/64. The input and output mask of the linear hull is $(\Gamma_6, -)$ and $(-, \Gamma_{14})$. We extend it by adding some rounds to the beginning and the end of the cipher, as follows.

In the backwards direction. With respect to Figure 3, we can append a further round to the beginning of the cipher to find a new 14-round linear hull by input mask $(-, \Gamma_6)$.

Since SIMON injects the subkey at the end of its round function, then this work does not have any computational complexity. We can continue our method to add more rounds to the beginning of linear hull in the cost of guessing some bits of subkeys similar to the approach presented in section 4.2.

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. More details are depicted in Figure 3.



$(X_L^{i-4})[0,1,2,3,4,6,8,9,10,11,12,13,14,15]$
X_L^{i-4}
X_R^{i-4}
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
$(X_R^{i+14})_{14}$
$(X_L^{i+14})[6,12,13]$
F
$(K^{i+15})_{14}$
$(X_L^{i+15})[4,5,10,11,12,14]$
$(X_R^{i+15})[6,12,13]$
$(K^{i+16})[6,12,13]$
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
$(X_L^{i+17})[0,1,2,3,4,5,6,7,8,9,10,11,12,14]$
$(X_R^{i+17})[2,3,4,6,8,9,10,11,12,13]$
$(K^{i+18})[2,3,4,6,8,9,10,11,12,13]$
F
X_L^{i+18}
X_R^{i+18}

Fig. 3. The subkey bits (in black) that should be guessed to attack 21 rounds of SIMON32/64. The red bits are not required to be guessed.

We can extend the 13-round linear hull of SIMON32/64 by eight rounds (by adding four rounds at the beginning and four 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 $2^{31.69} \times 2^{32}$ encryptions to find the round-key bits on average. Therefore, the time complexity of the attack is $2^{31.69} + 2^{31.69} \times 2^{32} \approx 2^{63.69}$.

4.5 Key Recovery Attack on Other Variants of SIMON

In the above, we explain a key recovery attack which uses a linear hull on SIMON32/64. The same procedure can be applied to other variants of SIMON, see Appendix D for more details. A summary of our results on the linear hull cryptanalysis of SIMON48/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 16, 17, 18, and 19 throughout these attacks.

5 Linear Hull Effect in SIMON

In this section we will investigate the linear hull effect on SIMON using the correlation matrix method to compute the average squared correlation.

5.1 Correlation of the SIMON F Function

This section is provides an analysis on some linear properties of the SIMON F function regarding the squared correlation. This will assist in providing an intuition around the design rationale when it comes to linear properties of SIMON round Function F. A general linear analysis was applied on the F function of SIMON, with regards to limits around the squared correlations for all possible Hamming weights on input masks α and output masks β, for SIMON32/64. The following observations were made based on results in Table 9.

- The best linear characteristics for a single application of F is obtained for input and output masks with Hamming weight as low as 1 and 2.
- The best squared correlation obtained is 2^{-2} and the lowest is 2^{-16} for all possible Hamming weights on the input and output masks of F.

5.2 Constructing Correlation Submatrix for SIMON

To construct a correlation submatrix for SIMON, we make use of the following proposition.

Proposition 1 (Correlation of a one-round linear approximation [9]). *Let $\alpha = (\alpha_L, \alpha_R)$ and $\beta = (\beta_L, \beta_R)$ be the input and output masks of a one-round linear approximation of SIMON. Let α_F and β_F be the input and output masks of the SIMON F function. Then the correlation of the linear approximation (α, β) is $C(\alpha, \beta) = C_F(\alpha_F, \beta_F)$ where $\alpha_F = \alpha_L \oplus \beta_R$ and $\beta_F = \beta_L = \alpha_R$.*

As our goal is to perform a linear attack on SIMON, we construct a squared correlation matrix in order to compute the average squared correlation (the sum of the squares of the correlations of all trails) in order to estimate the required data complexity. Algorithm 2 constructs a squared correlation submatrix whose input and output masks have Hamming weight less than a certain Hamming weight m. Algorithm 2 uses the Fast Walsh Transform algorithm to compute the correlations of a given input and output masks for the F function of SIMON.

Algorithm 2: Construction of SIMON's Correlation Submatrix

```
Require: Hamming weight $m$, bit size of SIMON's $F$ function $n$ and a $map$ function.
Ensure: Squared Correlation Submatrix $M$
for all output masks $\beta$ with Hamming weight $\leq m$ do
    Extract from $\beta$ the left/right output masks $\beta_L$ and $\beta_R$.
    $\alpha_R \leftarrow \beta_L$.
    Compute $\hat{F}(\alpha_F, \beta_L)$ to SIMON's $F$ function for all possible $\alpha_F$.
    for all input masks $\alpha_F$ to SIMON's $F$ function do
        $c \leftarrow \hat{F}(\alpha_F, \beta_L)/2^n$.
        $\alpha_L \leftarrow \alpha_F \oplus \beta_R$.
        $\alpha = \alpha_L || \alpha_R$.
        if $c \neq 0$ and Hamming weight of $\alpha \leq m$ then
            $i \leftarrow map(\alpha)$. {map $\alpha$ to a row index $i$ in the matrix $M$}
            $j \leftarrow map(\beta)$. {map $\alpha$ to a column index $j$ in the matrix $M$}
            $M(i, j) = c \times c$.
        end if
    end for
end for
```

The size of the submatrix is $\sum_{i=0}^{m}\binom{2n}{i} \times \sum_{i=0}^{m}\binom{2n}{i}$ where n is the block size of SIMON's F function. One can see that the time complexity is in the order of $2^n \sum_{i=0}^{m}\binom{2n}{i}$ arithmetic operations. The submatrix size is large when $m > 5$, but most of its elements are zero and therefore it can easily fit in memory using a sparse matrix storage format. The table below shows the number of nonzero elements of the squared correlation submatrices of SIMON32/K when $1 \leq m \leq 9$. One can see that these matrices are very sparse (see Table 8). For instance, when $m \leq 8$, the density of the correlation matrix is very low, namely $\frac{133253381}{15033173 \times 15033173} \approx 2^{-20.7}$.

Table 8. SIMON32/K matrices using masks with Hamming weight $\leq$ m, nnz = number of nonzero elements

m	Size of M	nnz
1	33×33	17
2	529×529	233
3	5489×5489	2835
4	41449×41449	31381
5	242825×242825	308805
6	1149017×1149017	2671829
7	4514873×4514873	20206757
8	15033173×15033173	133253381
9	43081973×43081973	763347577

5.3 Improved Linear Approximations

One can see that Algorithm 2 is embarrassingly parallelizable. Thus, the memory complexity rather than the time complexity is dominating. On a standard PC, we are able to construct a sparse squared correlation matrix of SIMON32/K with input and output masks that have Hamming weight ≤ 8. Using this matrix, we find new 14-round linear approximations with an average squared correlation $\leq 2^{-32}$ for SIMON32/K. We also get better estimations for the previously found linear approximations which were estimated before using only a single linear characteristic rather than considering many linear characteristics with the same input and output masks. For example, in [3], the squared correlation of the 9-round single linear characteristic with input mask `0x01110004` and output mask `0x00040111` is 2^{-20}. Using our matrix, we find that this same approximation has a squared correlation $\approx 2^{-18.4}$ with $11455 \approx 2^{13.5}$ trails, which gives us an improvement by a factor of $2^{1.5}$. Note that this approximation can be found using a smaller correlation matrix of Hamming weight ≤ 4 and we get an estimated squared correlation equal to $2^{-18.83}$ and only 9 trails. So the large number of other trails resulting covering Hamming weights ≥ 5 is insignificant as they only cause a factor of $2^{0.5}$ improvement.

Also, the 10-round linear characteristic in [5] with input mask `0x01014404` and output mask `0x10004404` has squared correlation 2^{-26}. Using our correlation matrix, we find that this same approximation has an estimated squared correlation $2^{-23.2}$ and the number of trails is $588173 \approx 2^{19.2}$. This gives an improvement by a factor of 2^3. Note also that this approximation can be found using a smaller correlation matrix with Hamming weight ≤ 5 and we get an estimated squared correlation equal to $2^{-23.66}$ and only 83 trails. So the large number of other trails resulting covering Hamming weights ≥ 5 is insignificant as they only cause a factor of $2^{0.4}$ improvement. Both of these approximations give us squared correlations less than 2^{-32} when considering more than 12 rounds.

In the following, we describe the new 14-round linear hulls found using a squared correlation matrix with Hamming weight ≤ 8.

New 14-round Linear Hulls. Consider a squared correlation matrix M whose input and output masks have Hamming weight m. When $m \geq 6$, raising the matrix to the rth power, in order to estimate the average squared correlation, will not work as the resulting matrix will not be sparse even when r is small. For example, we are able only to compute M^6 where M is a squared correlation matrix whose masks have Hamming weight ≤ 6. Therefore, we use matrix-vector multiplication or row-vector matrix multiplications in order to estimate the squared correlations for any number of rounds r.

It is obvious that input and output masks with low Hamming weight gives us better estimations for the squared correlation. So we performed row-vector matrix multiplications using row vectors corresponding to Hamming weight one. We found that when the left part of the input mask has Hamming weight one and the right part of input mask is zero, we always get a 14-round squared correlation $\approx 2^{-30.9}$ for four different output masks. So in total we get 64 linear approximations with an estimated 14-round squared correlation $\approx 2^{-30.9}$.

We also constructed a correlation matrix with masks of Hamming weight ≤ 9 but we have only got a slight improvement for these 14-round approximations by a factor of $2^{0.3}$. We have found no 15-round approximation with squared correlation more than 2^{-32}. Table 10 shows the 14-round approximations with input and output masks written in hexadecimal notation.

Table 9. General analysis to the best and lowest squared correlations in SIMON32/64 for all possible Hamming weights entering the F function

Hamming weight	Best Sq. Corr	Lowest Sq. Corr
1	2^{-2}	2^{-2}
2	2^{-2}	2^{-4}
3	2^{-4}	2^{-6}
4	2^{-4}	2^{-8}
5	2^{-6}	2^{-10}
6	2^{-6}	2^{-12}
7	2^{-8}	2^{-14}
8	2^{-8}	2^{-16}
9	2^{-10}	2^{-16}
10	2^{-10}	2^{-16}
11	2^{-12}	2^{-16}
12	2^{-12}	2^{-16}
13	2^{-14}	2^{-16}
14	2^{-14}	2^{-16}
15	2^{-16}	2^{-16}
16	2^{-14}	2^{-14}

Table 10. 14-round linear hulls for SIMON32/K found, using Hamming weight ≤ 9

α	β	$\log_2 c^2$	$\log_2 N_t$
80000000	00800020, 00800060, 00808020, 00808060	−30.5815	28.11
40000000	00400010, 00400030, 00404010, 00404030	−30.5815	28.11
20000000	00200008, 00200018, 00202008, 00202018	−30.5815	28.11
10000000	00100004, 0010000C, 00101004, 0010100C	−30.5815	28.11
08000000	00080002, 00080006, 00080802, 00080806	−30.5815	28.11
04000000	00040001, 00040003, 00040401, 00040403	−30.5816	28.11
02000000	00028000, 00028001, 00028200, 00028201	−30.5815	28.10
01000000	00014000, 00014100, 0001C000, 0001C100	−30.5815	28.10
00800000	80002000, 80002080, 80006000, 80006080	−30.5816	28.06
00400000	40001000, 40001040, 40003000, 40003040	−30.5815	28.11
00200000	20000800, 20000820, 20001800, 20001820	−30.5815	28.11
00100000	10000400, 10000410, 10000C00, 10000C10	−30.5815	28.11
00080000	08000200, 08000208, 08000600, 08000608	−30.5815	28.11
00040000	04000100, 04000104, 04000300, 04000304	−30.5816	28.10
00020000	02000080, 02000082, 02000180, 02000182	−30.5815	28.11
00010000	01000040, 01000041, 010000C0, 010000C1	−30.5814	28.11

6 Key Recovery Attack using Linear Hulls

Similar to the approach we used in previous sections to add extra rounds to the given linear trail, we extend the given linear hull for 14 rounds of SIMON32/64 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 14-round linear hull (e.g. $(\Gamma_0, -)$) and go backwards to add some rounds to the beginning. With respect to Figure 4, we can append a further round to the beginning of the cipher to find a new 15-round linear hull by input mask $(-, \Gamma_0)$. Since SIMON injects the subkey at the end of its round function, then this work does not have any computational complexity. More precisely, for the current 14-round linear hull, we evaluate $((X_L^i)_0 \oplus (X_R^{i+14})_8 \oplus (X_L^{i+14})_6)$. If we add a round in the backwards direction, i.e. round $i-1$, we know X_R^{i-1} and X_L^{i-1}, so

$$(X_L^{i-1})_{14} \oplus ((X_L^{i-1})_{15} \& (X_L^{i-1})_8) = (X_R^{i-1})_0 \oplus (K^i)_0 \oplus (X_L^i)_0.$$

Hence, we can consider $((X_L^i)_0 \oplus (X_R^{i+14})_8 \oplus (X_L^{i+14})_6) \oplus (K^i)_0$ as the new linear hull. We can continue our method to add more rounds to the beginning of linear hull at the cost of guessing some bits of subkeys.

To add more rounds in the backwards direction, we must guess the bit

$$(F(X_L^{i-1}))_0 = (X_L^{i-1})_{14} \oplus ((X_L^{i-1})_{15} \& (X_L^{i-1})_8).$$

On the other hand, to determine $(F(X_L^{i-1}))_0$ one should guess $(X_L^{i-1})_{14}$ and $(X_L^{i-1})_{15}$ only if the guessed value for $(X_L^{i-1})_8$ is 1. So, in average we need one bit guess for $(X_L^{i-1})_{15}$ and $(X_L^{i-1})_8$ (in Figure 4 such bits are indicated in blue).

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. More details are depicted in Figure 4.

Attack Complexity. We require $2^{30.5593}$ known plaintexts. We also need $2^{30.5593}$ encryptions for producing the required known plaintexts and $2^{30.5593} \times 2^{25}$ encryptions to find the related key bits of the extended rounds. Therefore, the time complexity of the attack is

$$2^{30.5593} + 2^{30.5593} \times 2^{25} \approx 2^{55.56}.$$

7 Conclusion

In this paper we have analyzed the security of SIMON against different variants of linear cryptanalysis, i.e. classical- and multiple linear cryptanalysis as well as linear hull attacks. We mainly used a connection between linear- and differential characteristics and extended it to a connection between linear hulls and differentials. Given these connections, we used the

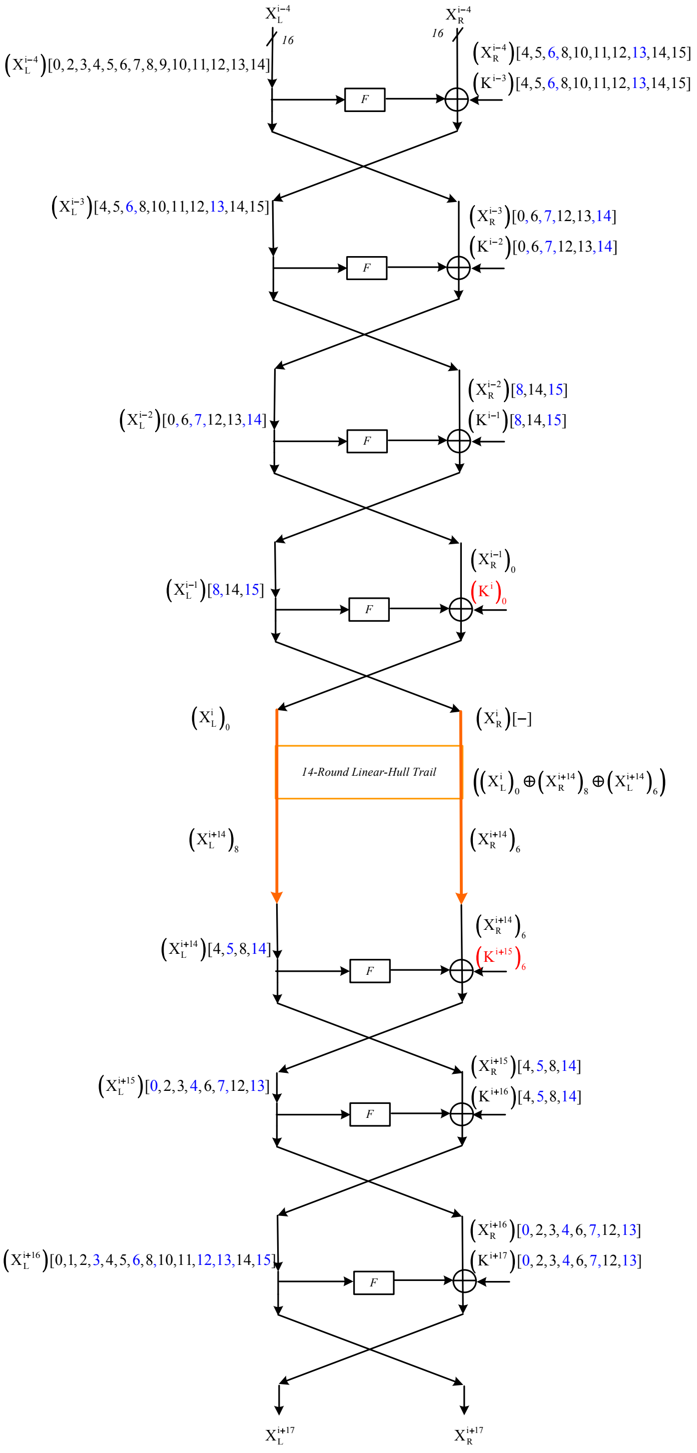

X_L^{i-4}
X_R^{i-4}
16
16
$(X_L^{i-4})[0,2,3,4,5,6,7,8,9,10,11,12,13,14]$
$(X_R^{i-4})[4,5,6,8,10,11,12,13,14,15]$
$(K^{i-3})[4,5,6,8,10,11,12,13,14,15]$
F
$(X_L^{i-3})[4,5,6,8,10,11,12,13,14,15]$
$(X_R^{i-3})[0,6,7,12,13,14]$
$(K^{i-2})[0,6,7,12,13,14]$
F
$(X_R^{i-2})[8,14,15]$
$(X_L^{i-2})[0,6,7,12,13,14]$
$(K^{i-1})[8,14,15]$
F
$(X_R^{i-1})_0$
$(X_L^{i-1})[8,14,15]$
$(K^{i})_0$
F
$(X_L^{i})_0$
$(X_R^{i})[-]$
14-Round Linear-Hull Trail
$((X_L^{i})_0 \oplus (X_R^{i+14})_8 \oplus (X_L^{i+14})_6)$
$(X_L^{i+14})_8$
$(X_R^{i+14})_6$
$(X_R^{i+14})_6$
$(X_L^{i+14})[4,5,8,14]$
$(K^{i+15})_6$
F
$(X_R^{i+15})[4,5,8,14]$
$(X_L^{i+15})[0,2,3,4,6,7,12,13]$
$(K^{i+16})[4,5,8,14]$
F
$(X_R^{i+16})[0,2,3,4,6,7,12,13]$
$(X_L^{i+16})[0,1,2,3,4,5,6,8,10,11,12,13,14,15]$
$(K^{i+17})[0,2,3,4,6,7,12,13]$
F
X_L^{i+17}
X_R^{i+17}

Fig. 4. 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 the blue bits cost guessing a half bit on average.

known results on differential cryptanalysis on SIMON variants to present the best known results on SIMON using linear cryptanalysis.

Furthermore, we have investigated the linear hull effect on SIMON32/64 using the correlation matrix of the average squared correlations. Utilizing this technique, we achieve a lower time and data complexity than other attack variants by having a key recovery attack on 21-round SIMON32/64 with data complexity $2^{30.56}$ and time complexity $2^{55.6}$.

References

1. Mohamed Ahmed Abdelraheem. Estimating the Probabilities of Low-Weight Differential and Linear Approximations on PRESENT-Like Ciphers. In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, *Information Security and Cryptology - ICISC 2012 - 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers*, volume 7839 of *Lecture Notes in Computer Science*, pages 368–382. Springer, 2012.
2. Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel. Differential Cryptanalysis of Reduced-Round Simon. *IACR Cryptology ePrint Archive*, 2013:526, 2013.
3. Farzaneh Abed, Eik List, Jakob Wenzel, and Stefan Lucks. Differential Cryptanalysis of round-reduced Simon and Speck. In *FSE (to appear)*, 2014.
4. Javad Alizadeh, Hoda A. Alkhzaimi, Mohammad Reza Aref, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar, Martin M. Lauridsen, and Somitra Kumar Sanadhya. Cryptanalysis of SIMON Variants with Connections. In *RFIDSec'14*, volume 8651 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2014.
5. Javad Alizadeh, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar, and Somitra Kumar Sanadhya. Linear Cryptanalysis of Round Reduced SIMON. *IACR Cryptology ePrint Archive*, 2013:663, 2013.
6. Hoda AlKhzaimi and Martin M. Lauridsen. Cryptanalysis of the SIMON Family of Block Ciphers. *IACR Cryptology ePrint Archive*, 2013:543, 2013.
7. Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia. Quark: A Lightweight Hash. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings*, volume 6225 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2010.
8. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. *IACR Cryptology ePrint Archive*, 2013:404, 2013.
9. Eli Biham. On Matsui's Linear Cryptanalysis. In Santis [34], pages 341–355.
10. Eli Biham and Adi Shamir. Differential Cryptanalysis of the Full 16-Round DES. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 487–496. Springer, 1992.
11. Alex Biryukov, Christophe De Cannière, and Michaël Quisquater. On Multiple Linear Approximations. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*, pages 1–22. Springer, 2004.
12. Alex Biryukov, Arnab Roy, and Vesselin Velichkov. Differential analysis of block ciphers SIMON and SPECK. *FSE (to appear)*, 2014.
13. Céline Blondeau and Kaisa Nyberg. New Links between Differential and Linear Cryptanalysis. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 388–404. Springer, 2013.
14. Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede. SPONGENT: A Lightweight Hash Function. In Preneel and Takagi [32], pages 312–325.

15. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.
16. Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225. Springer, 2012.
17. Christophe De Cannière and Bart Preneel. Trivium. In Robshaw and Billet [33], pages 244–266.
18. Florent Chabaud and Serge Vaudenay. Links Between Differential and Linear Cryptoanalysis. In Santis [34], pages 356–365.
19. Joo Yeon Cho, Miia Hermelin, and Kaisa Nyberg. A New Technique for Multidimensional Linear Cryptanalysis with Applications on Reduced Round Serpent. In Pil Joong Lee and Jung Hee Cheon, editors, *Information Security and Cryptology - ICISC 2008, 11th International Conference, Seoul, Korea, December 3-5, 2008, Revised Selected Papers*, volume 5461 of *Lecture Notes in Computer Science*, pages 383–398. Springer, 2008.
20. Baudoin Collard, François-Xavier Standaert, and Jean-Jacques Quisquater. Improved and Multiple Linear Cryptanalysis of Reduced Round Serpent. In Dingyi Pei, Moti Yung, Dongdai Lin, and Chuankun Wu, editors, *Information Security and Cryptology, Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31 - September 5, 2007, Revised Selected Papers*, volume 4990 of *Lecture Notes in Computer Science*, pages 51–65. Springer, 2007.
21. Baudoin Collard, François-Xavier Standaert, and Jean-Jacques Quisquater. Experiments on the Multiple Linear Cryptanalysis of Reduced Round Serpent. In Kaisa Nyberg, editor, *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, volume 5086 of *Lecture Notes in Computer Science*, pages 382–397. Springer, 2008.
22. Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard.* Information Security and Cryptography. Springer, 2002.
23. Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON Family of Lightweight Hash Functions. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 222–239. Springer, 2011.
24. Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED Block Cipher. In Preneel and Takagi [32], pages 326–341.
25. Risto M. Hakala and Kaisa Nyberg. Linear Distinguishing Attack on Shannon. In Yi Mu, Willy Susilo, and Jennifer Seberry, editors, *Information Security and Privacy, 13th Australasian Conference, ACISP 2008, Wollongong, Australia, July 7-9, 2008, Proceedings*, volume 5107 of *Lecture Notes in Computer Science*, pages 297–305. Springer, 2008.
26. Martin Hell, Thomas Johansson, Alexander Maximov, and Willi Meier. The Grain Family of Stream Ciphers. In Robshaw and Billet [33], pages 179–190.
27. Burton S. Kaliski Jr. and Matthew J. B. Robshaw. Linear Cryptanalysis Using Multiple Approximations. In Yvo Desmedt, editor, *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 26–39. Springer, 1994.
28. Jorge Nakahara Jr., Bart Preneel, and Joos Vandewalle. Linear cryptanalysis of reduced-round versions of the SAFER block cipher family. In Bruce Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*, volume 1978 of *Lecture Notes in Computer Science*, pages 244–261. Springer, 2000.
29. Gregor Leander. On linear hulls, statistical saturation attacks, PRESENT and a cryptanalysis of PUFFIN. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual*

International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings, volume 6632 of *Lecture Notes in Computer Science*, pages 303–322. Springer, 2011.

30. Mitsuru Matsui. Linear Cryptoanalysis Method for DES Cipher. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.
31. Kaisa Nyberg. Linear Approximation of Block Ciphers. In Santis [34], pages 439–444.
32. Bart Preneel and Tsuyoshi Takagi, editors. *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, volume 6917 of *Lecture Notes in Computer Science*. Springer, 2011.
33. Matthew J. B. Robshaw and Olivier Billet, editors. *New Stream Cipher Designs - The eSTREAM Finalists*, volume 4986 of *Lecture Notes in Computer Science*. Springer, 2008.
34. Alfredo De 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.
35. Anne Tardy-Corfdir and Henri Gilbert. A Known Plaintext Attack of FEAL-4 and FEAL-6. In Joan Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, volume 576 of *Lecture Notes in Computer Science*, pages 172–181. Springer, 1991.
36. Ning Wang, Xiaoyun Wang, Keting Jia, and Jingyuan Zhao. Improved Differential Attacks on Reduced SIMON Versions, 2014.
37. Qingju Wang, Zhiqiang Liu, Kerem Varici, Yu Sasaki, Vincent Rijmen, and Yosuke Todo. Cryptanalysis of Reduced-Round SIMON32 and SIMON48, 2014.

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

Tables 11 represent the propagation of our linear characteristics for SIMON32/64, entries under used App. column denotes approximation used for corresponding active bit of column 2 of the table.

Table 11. Sequences of approximation for SIMON32/64

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

Table 12. 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

Table 13. 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

Table 14. 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 15. 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

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

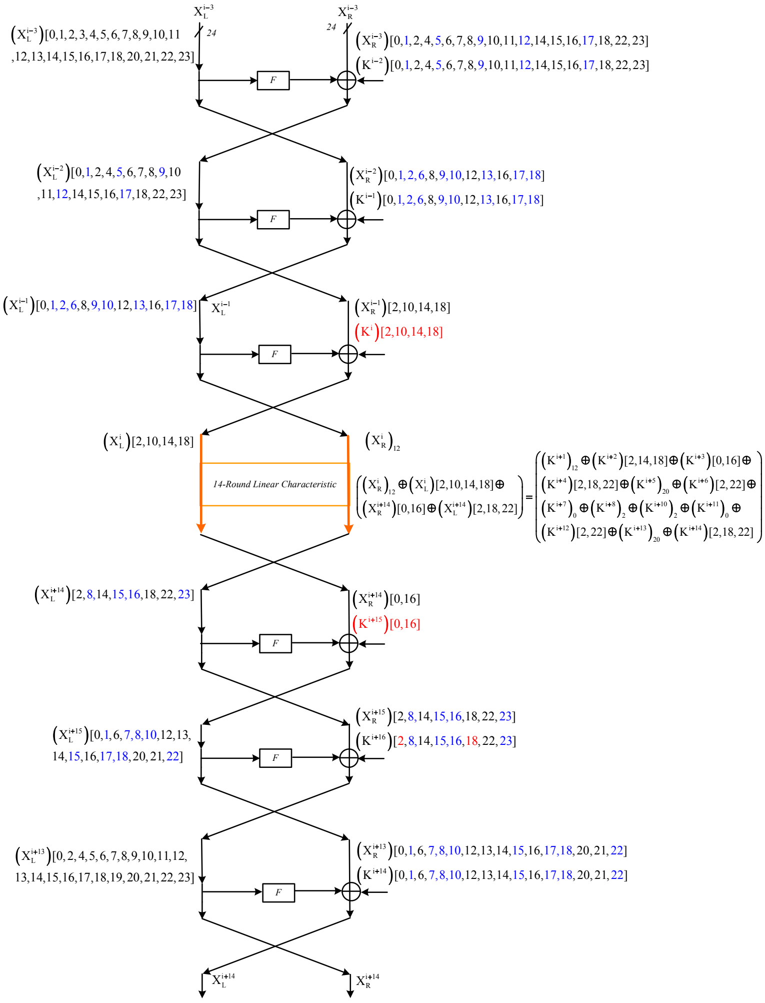

X_L^{i-3}
X_R^{i-3}
24
24
$(X_L^{i-3})[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,20,21,22,23]$
$(X_R^{i-3})[0,1,2,4,5,6,7,8,9,10,11,12,14,15,16,17,18,22,23]$
$(K^{i-2})[0,1,2,4,5,6,7,8,9,10,11,12,14,15,16,17,18,22,23]$
F
$(X_L^{i-2})[0,1,2,4,5,6,7,8,9,10,11,12,14,15,16,17,18,22,23]$
$(X_R^{i-2})[0,1,2,6,8,9,10,12,13,16,17,18]$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

Fig. 5. The keys (in *black*) that should be guessed to attack 19 rounds of SIMON48/72 (exclude round $i-2$). The red bits are not required to be guessed. For SIMON48/96 we include round $i-2$ that needs guessing 16 bits of its subkey in average.

C Linear Hulls for SIMON

D Linear Hulls Extensions and Based on Correlation Matrix of SIMON

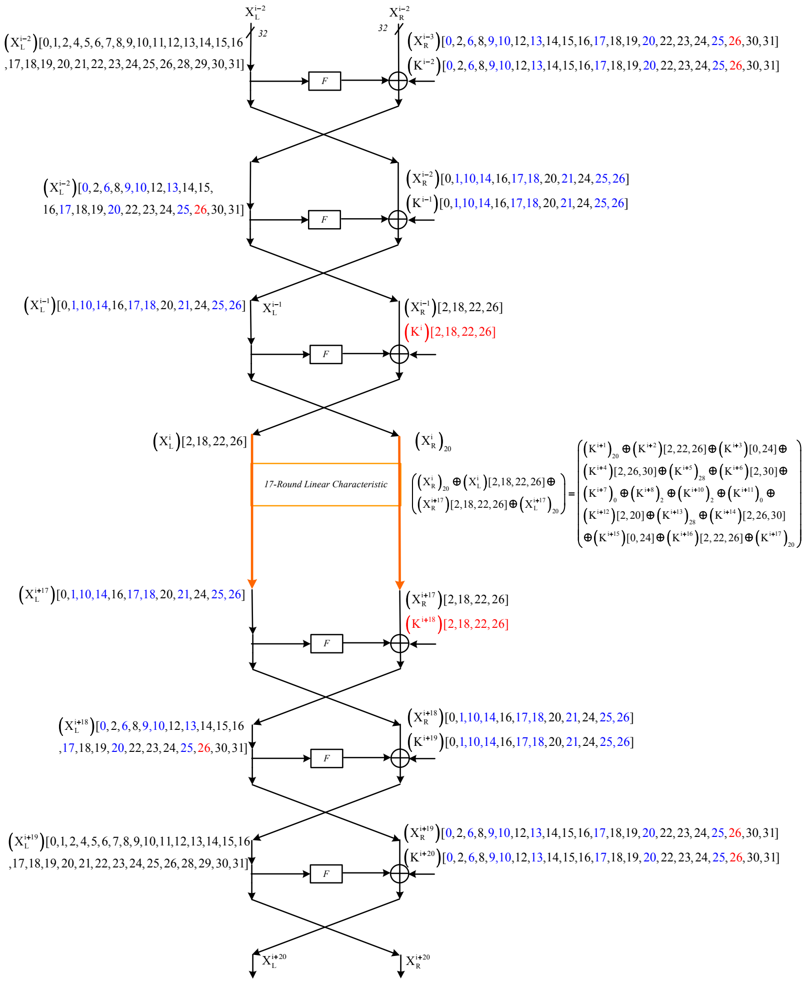

X_L^{i-2}
32
X_R^{i-2}
32
$(X_L^{i-2})[0,1,2,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,28,29,30,31]$
$(X_R^{i-3})[0,2,6,8,9,10,12,13,14,15,16,17,18,19,20,22,23,24,25,26,30,31]$
$(K^{i-2})[0,2,6,8,9,10,12,13,14,15,16,17,18,19,20,22,23,24,25,26,30,31]$
F
$(X_L^{i-2})[0,2,6,8,9,10,12,13,14,15,16,17,18,19,20,22,23,24,25,26,30,31]$
$(X_R^{i-2})[0,1,10,14,16,17,18,20,21,24,25,26]$
$(K^{i-1})[0,1,10,14,16,17,18,20,21,24,25,26]$
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
$\begin{pmatrix}(X_R^{i})_{20}\oplus(X_L^{i})[2,18,22,26]\oplus\\(X_R^{i+17})[2,18,22,26]\oplus(X_L^{i+17})_{20}\end{pmatrix}=\begin{pmatrix}(K^{i+1})_{20}\oplus(K^{i+2})[2,22,26]\oplus(K^{i+3})[0,24]\oplus\\(K^{i+4})[2,26,30]\oplus(K^{i+5})_{28}\oplus(K^{i+6})[2,30]\oplus\\(K^{i+7})_{0}\oplus(K^{i+8})_{2}\oplus(K^{i+10})_{2}\oplus(K^{i+11})_{0}\oplus\\(K^{i+12})[2,20]\oplus(K^{i+13})_{28}\oplus(K^{i+14})[2,26,30]\\\oplus(K^{i+15})[0,24]\oplus(K^{i+16})[2,22,26]\oplus(K^{i+17})_{20}\end{pmatrix}$
$(X_L^{i+17})[0,1,10,14,16,17,18,20,21,24,25,26]$
$(X_R^{i+17})[2,18,22,26]$
$(K^{i+18})[2,18,22,26]$
F
$(X_L^{i+18})[0,2,6,8,9,10,12,13,14,15,16,17,18,19,20,22,23,24,25,26,30,31]$
$(X_R^{i+18})[0,1,10,14,16,17,18,20,21,24,25,26]$
$(K^{i+19})[0,1,10,14,16,17,18,20,21,24,25,26]$
F
$(X_L^{i+19})[0,1,2,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,28,29,30,31]$
$(X_R^{i+19})[0,2,6,8,9,10,12,13,14,15,16,17,18,19,20,22,23,24,25,26,30,31]$
$(K^{i+20})[0,2,6,8,9,10,12,13,14,15,16,17,18,19,20,22,23,24,25,26,30,31]$
F
X_L^{i+20}
X_R^{i+20}

Fig. 6. The keys (in *black*) that should be guessed to attack 22 rounds of SIMON64/96 (exclude round $i-2$). The red bits are not required to be guessed. For SIMON64/128 we include round $i-2$ that needs guessing 17 bits of its subkey in average.

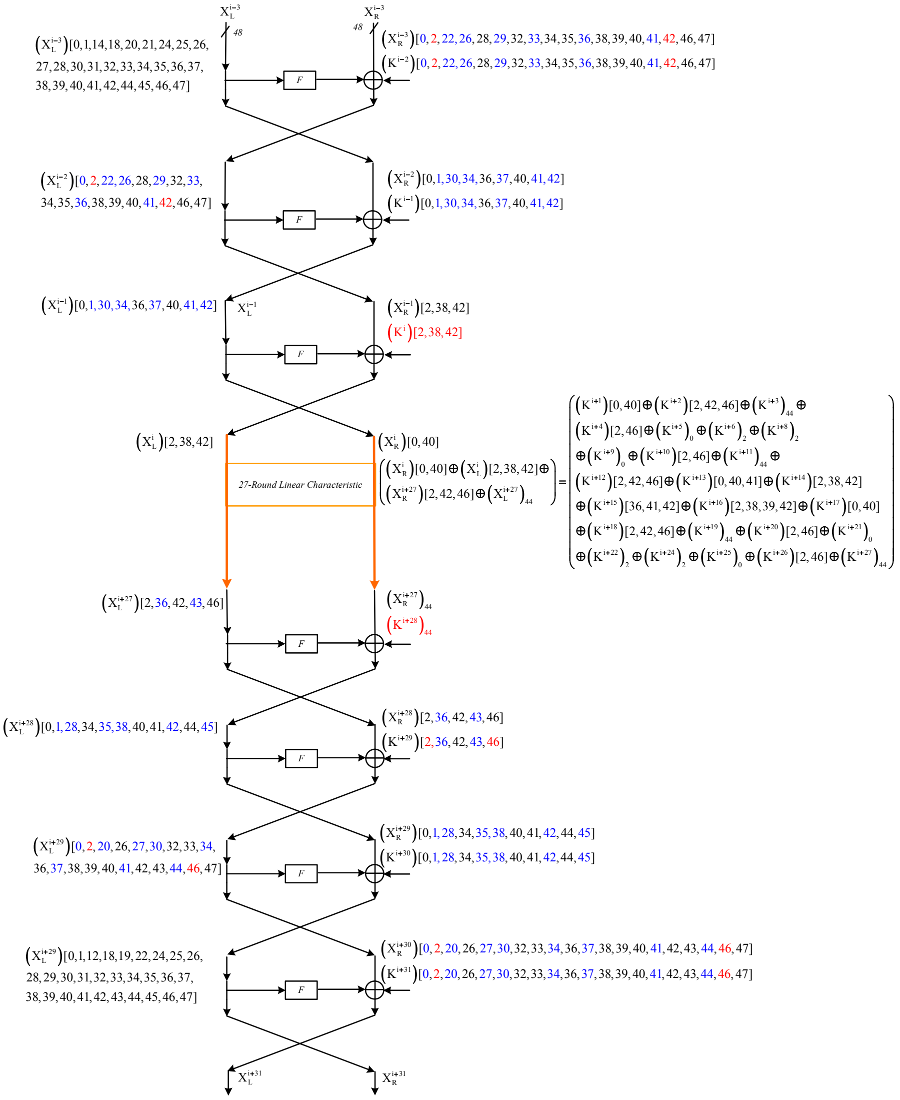

X_L^{i-3}
X_R^{i-3}
48
48
$(X_L^{i-3})[0,1,14,18,20,21,24,25,26,27,28,30,31,32,33,34,35,36,37,38,39,40,41,42,44,45,46,47]$
$(X_R^{i-3})[0,2,22,26,28,29,32,33,34,35,36,38,39,40,41,42,46,47]$
$(K^{i-2})[0,2,22,26,28,29,32,33,34,35,36,38,39,40,41,42,46,47]$
F
$(X_L^{i-2})[0,2,22,26,28,29,32,33,34,35,36,38,39,40,41,42,46,47]$
$(X_R^{i-2})[0,1,30,34,36,37,40,41,42]$
$(K^{i-1})[0,1,30,34,36,37,40,41,42]$
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
$(X_L^{i+29})[0,1,12,18,19,22,24,25,26,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47]$
$(X_R^{i+30})[0,2,20,26,27,30,32,33,34,36,37,38,39,40,41,42,43,44,46,47]$
$(K^{i+31})[0,2,20,26,27,30,32,33,34,36,37,38,39,40,41,42,43,44,46,47]$
F
X_L^{i+31}
X_R^{i+31}

Fig. 7. The keys (in *black*) that should be guessed to attack 34 rounds of SIMON96/144.The red bits are not required to be guessed.

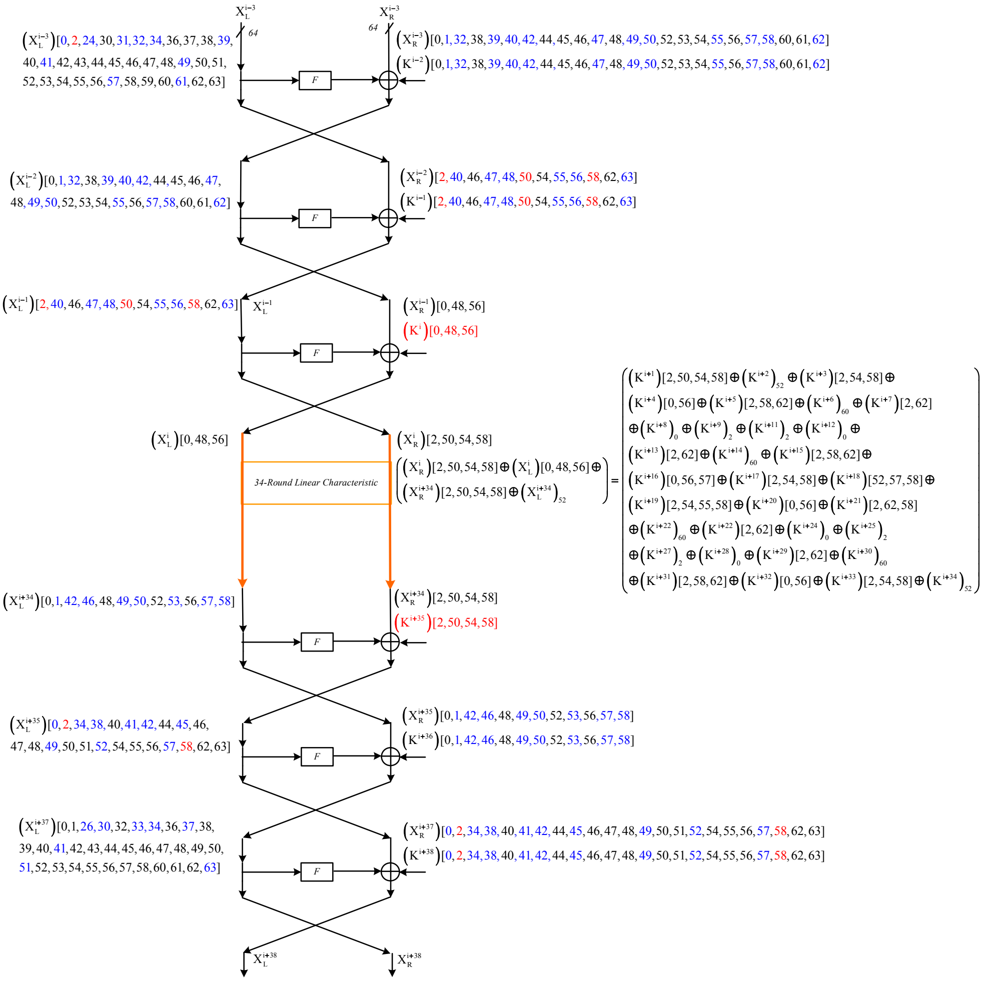

X_L^{i-3}
X_R^{i-3}
64
64
$\left(X_L^{i-3}\right)[0,2,24,30,31,32,34,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]$
$\left(X_R^{i-3}\right)[0,1,32,38,39,40,42,44,45,46,47,48,49,50,52,53,54,55,56,57,58,60,61,62]$
$\left(K^{i-2}\right)[0,1,32,38,39,40,42,44,45,46,47,48,49,50,52,53,54,55,56,57,58,60,61,62]$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

Fig. 8. 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 61.5 bits of their subkey in average.

Table 16. Linear characteristics based on the differential trials by Biryukov et al. for SIMON48/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	$3, 7, 11, 19$	$-$
	$\sum_r \log_2 pr = -48$		$\log_2 \epsilon^2 = -50$		
	$\log_2 p_{diff} = -42.11$		$\log_2 \overline{c}^2_{LH} = -44.11$		
	# trails = 112573		# characteristics = 112573		

Table 17. Linear characteristics based on the differential trials by Biryukov et al. for SIMON64/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	$20, 24$	$-$
	$\sum_r \log_2 pr = -72$		$\log_2 \epsilon^2 = -74$		
	$\log_2 p_{diff} = -60.53$		$\log_2 \overline{c}^2_{LH} = -62.53$		
	# trails = 337309		# characteristics = 337309		

Table 18. Linear characteristics based on the differential trials by Abed et al. for SIMON96/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	–
	$\sum_r \log_2 pr = -106$		$\log_2 \epsilon^2 = -108$		
	$\log_2 p_{diff} = -92.20$		$\log_2 \overline{c}^2_{LH} = -94.20$		

Table 19. Linear characteristics based on the differential trials by Abed et al. for SIMON128/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	–
	$\sum_r \log_2 pr = -144$ $\log_2 p_{diff} = -124.60$		$\log_2 \epsilon^2 = -146$ $\log_2 \overline{c}_{LH}^2 = -126.60$		

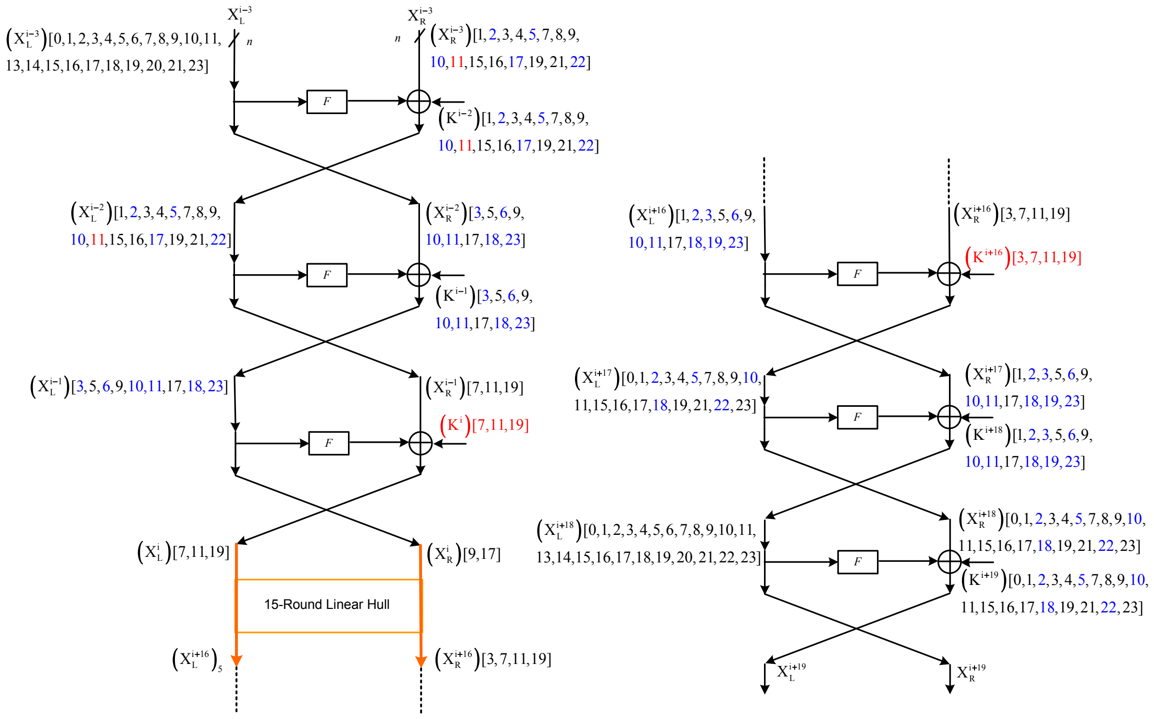

X_L^{i-3}
X_R^{i-3}
n
n
(X_L^{i-3})[0,1,2,3,4,5,6,7,8,9,10,11, 13,14,15,16,17,18,19,20,21,23]
(X_R^{i-3})[1,2,3,4,5,7,8,9, 10,11,15,16,17,19,21,22]
F
(K^{i-2})[1,2,3,4,5,7,8,9, 10,11,15,16,17,19,21,22]
(X_L^{i-2})[1,2,3,4,5,7,8,9, 10,11,15,16,17,19,21,22]
(X_R^{i-2})[3,5,6,9, 10,11,17,18,23]
F
(K^{i-1})[3,5,6,9, 10,11,17,18,23]
(X_L^{i-1})[3,5,6,9,10,11,17,18,23]
(X_R^{i-1})[7,11,19]
F
(K^{i})[7,11,19]
(X_L^{i})[7,11,19]
(X_R^{i})[9,17]
15-Round Linear Hull
$(X_L^{i+16})_5$
(X_R^{i+16})[3,7,11,19]
(X_L^{i+16})[1,2,3,5,6,9, 10,11,17,18,19,23]
(X_R^{i+16})[3,7,11,19]
F
(K^{i+16})[3,7,11,19]
(X_L^{i+17})[0,1,2,3,4,5,7,8,9,10, 11,15,16,17,18,19,21,22,23]
(X_R^{i+17})[1,2,3,5,6,9, 10,11,17,18,19,23]
F
(K^{i+18})[1,2,3,5,6,9, 10,11,17,18,19,23]
(X_L^{i+18})[0,1,2,3,4,5,6,7,8,9,10,11, 13,14,15,16,17,18,19,20,21,22,23]
(X_R^{i+18})[0,1,2,3,4,5,7,8,9,10, 11,15,16,17,18,19,21,22,23]
F
(K^{i+19})[0,1,2,3,4,5,7,8,9,10, 11,15,16,17,18,19,21,22,23]
X_L^{i+19}
X_R^{i+19}

Fig. 9. Adding some rounds to the beginning and the end of the 15-round linear hull for SIMON48/K

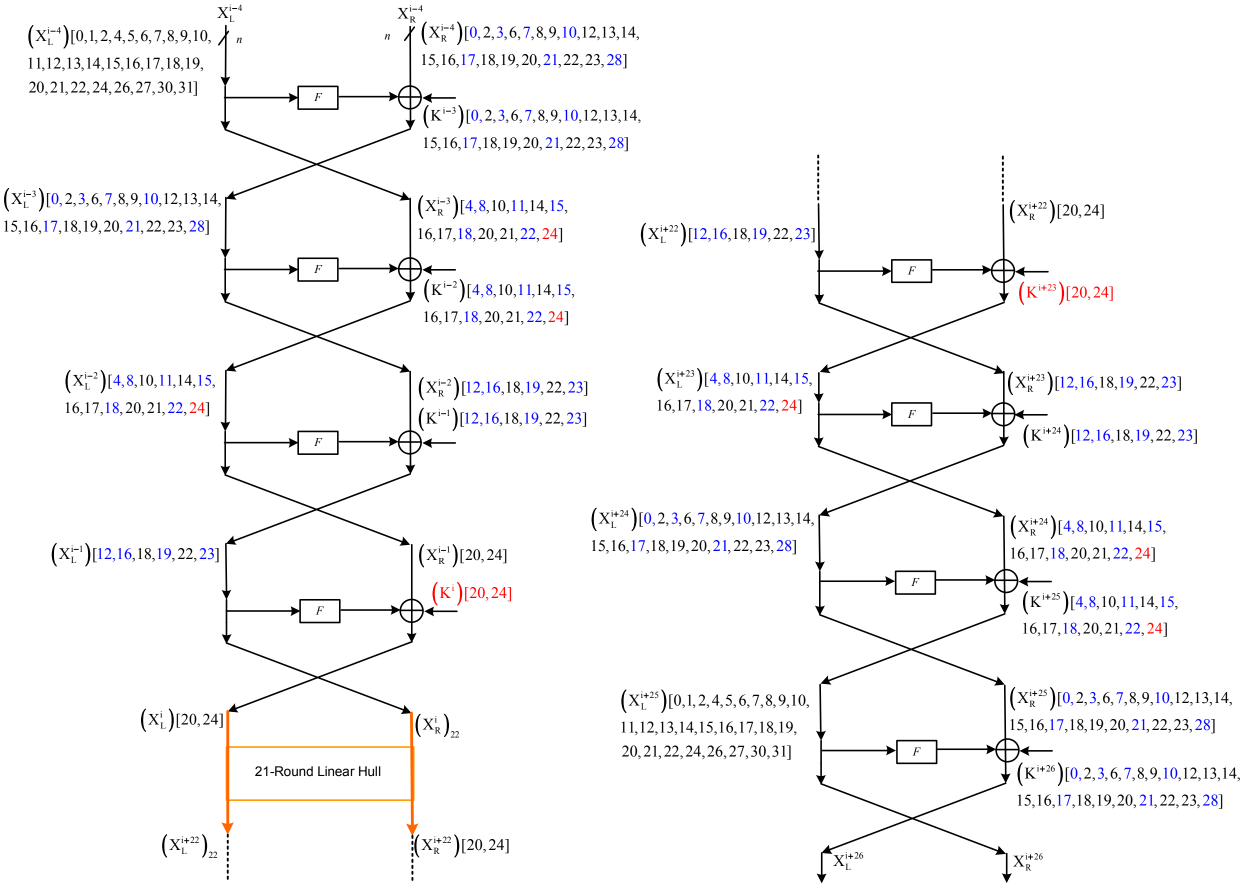

X_L^{i-4}
X_R^{i-4}
n
n
(X_L^{i-4})[0,1,2,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,24,26,27,30,31]
(X_R^{i-4})[0,2,3,6,7,8,9,10,12,13,14,15,16,17,18,19,20,21,22,23,28]
F
(K^{i-3})[0,2,3,6,7,8,9,10,12,13,14,15,16,17,18,19,20,21,22,23,28]
(X_L^{i-3})[0,2,3,6,7,8,9,10,12,13,14,15,16,17,18,19,20,21,22,23,28]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

Fig. 10. Adding some rounds to the beginning and the end of the 21-round linear hull for SIMON64/K

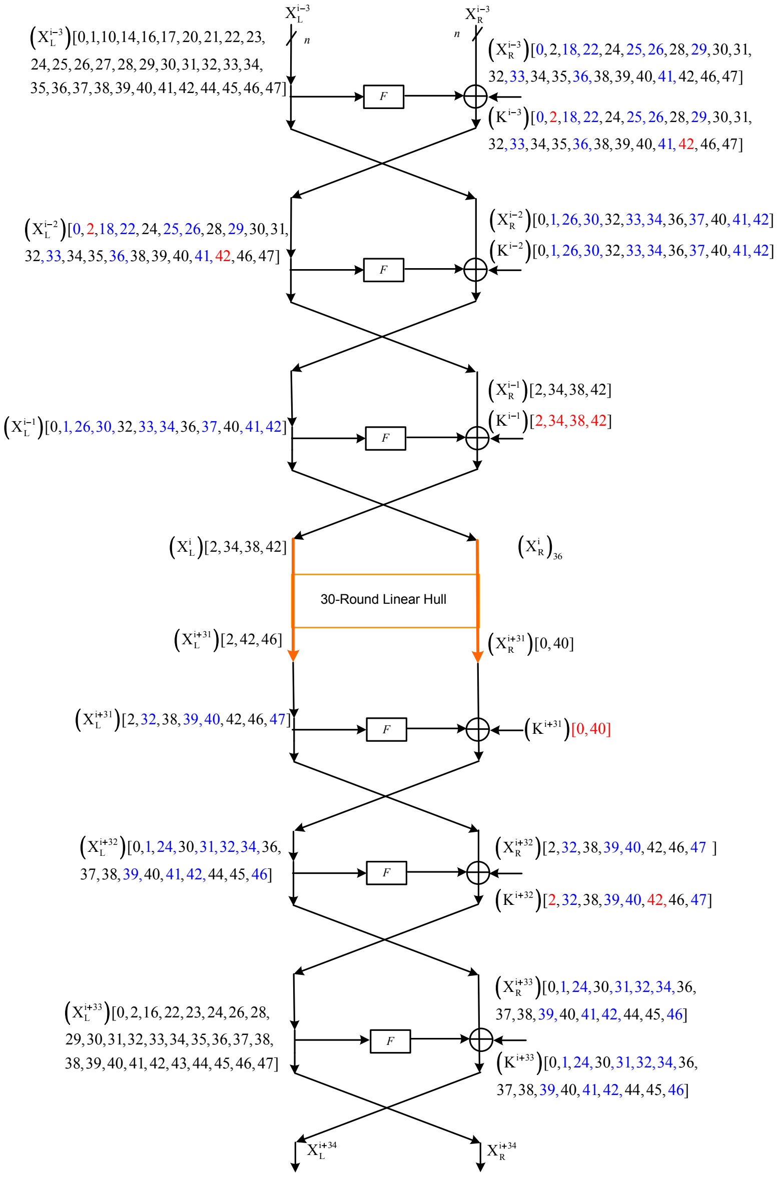

X_L^{i-3}
X_R^{i-3}
n
n
(X_L^{i-3})[0,1,10,14,16,17,20,21,22,23, 24,25,26,27,28,29,30,31,32,33,34, 35,36,37,38,39,40,41,42,44,45,46,47]
(X_R^{i-3})[0,2,18,22,24,25,26,28,29,30,31, 32,33,34,35,36,38,39,40,41,42,46,47]
(K^{i-3})[0,2,18,22,24,25,26,28,29,30,31, 32,33,34,35,36,38,39,40,41,42,46,47]
F
(X_L^{i-2})[0,2,18,22,24,25,26,28,29,30,31, 32,33,34,35,36,38,39,40,41,42,46,47]
(X_R^{i-2})[0,1,26,30,32,33,34,36,37,40,41,42]
(K^{i-2})[0,1,26,30,32,33,34,36,37,40,41,42]
F
(X_R^{i-1})[2,34,38,42]
(K^{i-1})[2,34,38,42]
(X_L^{i-1})[0,1,26,30,32,33,34,36,37,40,41,42]
F
(X_L^{i})[2,34,38,42]
$(X_R^{i})_{36}$
30-Round Linear Hull
(X_L^{i+31})[2,42,46]
(X_R^{i+31})[0,40]
(X_L^{i+31})[2,32,38,39,40,42,46,47]
F
(K^{i+31})[0,40]
(X_L^{i+32})[0,1,24,30,31,32,34,36, 37,38,39,40,41,42,44,45,46]
(X_R^{i+32})[2,32,38,39,40,42,46,47]
F
(K^{i+32})[2,32,38,39,40,42,46,47]
(X_R^{i+33})[0,1,24,30,31,32,34,36, 37,38,39,40,41,42,44,45,46]
(X_L^{i+33})[0,2,16,22,23,24,26,28, 29,30,31,32,33,34,35,36,37,38, 38,39,40,41,42,43,44,45,46,47]
F
(K^{i+33})[0,1,24,30,31,32,34,36, 37,38,39,40,41,42,44,45,46]
X_L^{i+34}
X_R^{i+34}

Fig. 11. Adding some rounds to the beginning and the end of the 30-round linear hull for SIMON96/K

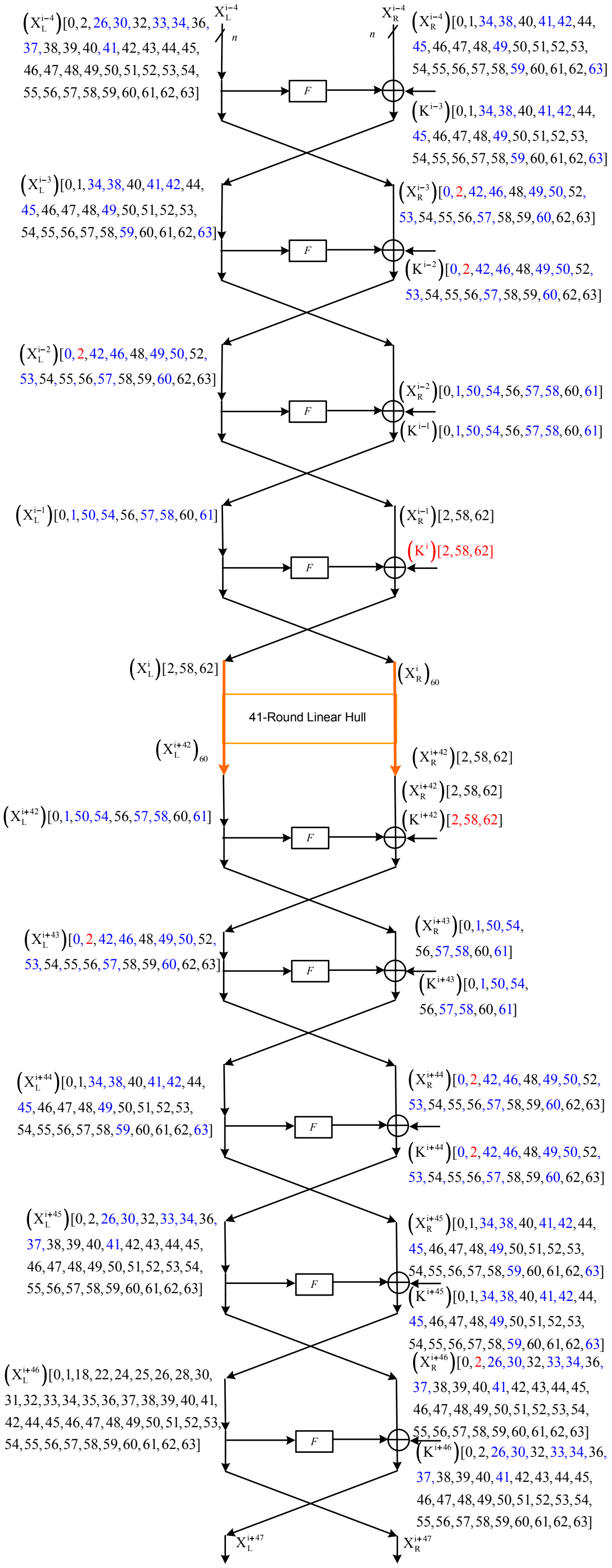

(X_L^{i-4})[0,2,26,30,32,33,34,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
X_L^{i-4}
n
X_R^{i-4}
n
(X_R^{i-4})[0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
F
(K^{i-3})[0,1,34,38,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
(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
$(X_L^{i+42})_{60}$
(X_R^{i+42})[2,58,62]
(X_R^{i+42})[2,58,62]
(X_L^{i+42})[0,1,50,54,56,57,58,60,61]
(K^{i+42})[2,58,62]
F
(X_R^{i+43})[0,1,50,54,56,57,58,60,61]
(X_L^{i+43})[0,2,42,46,48,49,50,52,53,54,55,56,57,58,59,60,62,63]
F
(K^{i+43})[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+44})[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+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]
(X_L^{i+46})[0,1,18,22,24,25,26,28,30,31,32,33,34,35,36,37,38,39,40,41,42,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63]
(X_R^{i+46})[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]
F
(K^{i+46})[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_L^{i+47}
X_R^{i+47}

Fig. 12. Adding some rounds to the beginning and the end of the 30-round linear hull for SIMON128/K