Improved Linear Hull Attack on Round-Reduced SIMON with Dynamic Key-guessing Techniques

Huaifeng Chen[1], Xiaoyun Wang[1,2⋆]

[1] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, Jinan 250100, China
hfchen@mail.sdu.edu.cn
[2] Institute of Advanced Study, Tsinghua University, Beijing 100084, China
xiaoyunwang@mail.tsinghua.edu.cn

Abstract. SIMON is a lightweight block cipher family proposed by NSA in 2013. It has drawn many cryptanalysts' attention and varity of cryptanalysis results have been published, including differential, linear, impossible differential, integral cryptanalysis and so on. In this paper, we give improved linear attack on all versions of SIMON with dynamic key-guessing techniques, which was proposed to improve the differential attack on SIMON recently. By establishing the boolean function of parity bit in the linear hull distinguisher and reducing the function accroding the property of AND operation, we can guess different subkeys (or equivalent subkeys) for different situations, which decrease the number of key bits involved in the attack and decrease the time complexity in a further step. As a result, 23-round SIMON32/64, 24-round SIMON48/72, 25-round SIMON48/96, 30-round SIMON64/96, 31-round SIMON64/128, 37-round SIMON96/96, 38-round SIMON96/144, 49-round SIMON128/128, 51-round SIMON128/192 and 53-round SIMON128/256 can be attacked. The linear attacks on most versions of SIMON are the best attacks among all cryptanalysis results on these variants known up to now. However, this does not shake the security of SIMON family with full rounds.

1 Introduction

In 2013, NSA proposed a new family of lightweight block cipher with Feistel structure, named as SIMON, which is tuned for optimal performance in hardware applications [1]. The SIMON family consists of various block and key sizes to match different application requirements. There is no S-box in the round function. The round function consists of AND, rotation and Xor (ARX structure), leading to a low-area hardware requirement.

Ralated Works. SIMON family has attracted a lot of cryptanalysts' attention since its proposation. Many cryptanalysis results on various versions of SIMON were published. For differential attack, Alkhzaimi and Lauridsen [13] gave the first differential attacks on all versions of SIMON. The atacks cover 16, 18, 24, 29, 40 rounds for the versions with blcok size 32, 48, 64, 96 and 128 respectively. At FSE 2014, Abed *et al.* [9] gave differential attack on variants of SIMON reduced to 18, 19, 26, 35, 46 rounds with respective block size 32, 48, 64, 96 and 128 respectively. At the same time, Biryukov *et al.* [10] gave differentail attack on several versions of SIMON independently. And 19-round SIMON32, 20-round SIMON48, 26-round SIMON64 were attacked. Then Wang *et al.* [14] proposed better differential attacks with existing differentials, using dynamic key-guessing techniques. As a result, 21-round SIMON32/64, 23-round SIMON48/72, 24-round SIMON48/96, 28-round SIMON64/96, 29-round SIMON64/128, 37-round SIMON96/96, 37-round SIMON96/144, 49-round SIMON128/128, 49-round SIMON128/192, 50-round SIMON128/256 were attacked.

For the direction of linear cryptanalysis, 11, 14, 16, 20, 23-round key recovery attacks on SIMON with block size 32, 48, 64, 96, 128 were presented in [9]. Then, Alizadeh *et al.* [15] improved linear attacks and gave cryptanalysis results on 13-round SIMON32, 15-round SIMON48, 19-round SIMON64, 28-round SIMON96, 35-round SIMON128. Recently, Abdelraheem *et al.* [6] took advantage of the links between linear characteirstics and differential characteristics for SIMON and found some linear distinguishers using differential characteristics found earlier. They presented various linear attacks on SIMON with linear, multiple linear, linear hull cryptanalysis. The linear hull cryptanalysis has better attack results, which can attack 21-round

⋆ Corresponding Author

Simon32/64, 20-round Simon48/72, 21-round Simon48/96, 27-round Simon64/96, 29-round Simon64/128, 36-round Simon96/144, 48-round Simon128/192 and 50-round Simon128/256. Then, with the Mixed-integer Linear Programming based technique, Shi *et al.* [7] searched new linear trails and linear hulls, and 21, 21, 29 rounds for Simon32/64, Simon48/96, Simon64/128 were attacked respectively. Also, Sun *et al.* [12] found a 16-round linear hull distinguisher of Simon48, with which he attacked 23-round Simon48/96. Ashur [20] presented a new way to calculate the correlations of short linear hulls and provode a more accurate estimation for some previously published linear trails. He gave multiple linear ctyptanalysis on 24-round Simon32/64, 23-round Simon48/72, 24-round Simon48/96, 24-round Simon64/96 and 25-round Simon64/128. However, it uses the correlation when all the subkeys are zero as the expected correlation under random key situations, which is not exact. What's more, if the potential of each linear hull used in multiple linear is smaller than that of random permutations, the gather of these linear hulls can not distinguish the cipher and random permutation.

Table 1. Summary of Linear Hull Attacks on Simon

Cipher	Total Rounds	Attacked rounds	Data	Time	Reference
Simon32/64	32	21	$2^{30.56}$	$2^{55.56}$	[6]
		21	- [a]	-	[7]
		23	$2^{31.19}$	$2^{57.19}TWO$[b]$+ 2^{61.84}A$[c]$+ 2^{56}E$[d]	Section 4.2
Simon48/72	36	20	$2^{44.11}$	$2^{70.61}$	[6]
		24	$2^{47.92}$	$2^{69.92}ONE$[e]$+ 2^{67.89}A + 2^{56}E$	Appendix B
Simon48/96	36	21	$2^{44.11}$	$2^{70.61}$	[6]
		21	-	-	[7]
		23	$2^{47.92}$	$2^{92.92}$	[12]
		25	$2^{47.92}$	$2^{91.92}TWO + 2^{89.89}A + 2^{80}E$	Appendix B
Simon64/96	42	27	$2^{62.53}$	$2^{88.53}$	[6]
		30	$2^{63.53}$	$2^{89.53}ONE + 2^{93.62}A + 2^{88}E$	Appendix B
Simon64/128	44	29	$2^{62.53}$	$2^{123.53}$	[6]
		29	-	-	[7]
		31	$2^{63.53}$	$2^{115.53}TWO + 2^{119.62}A + 2^{120}E$	Appendix B
Simon96/96	52	37	$2^{95.2}$	$2^{67.94}A + 2^{88}E$	Appendix B
Simon96/144	54	36	$2^{94.2}$	$2^{123.5}$	[6]
		38	$2^{95.2}$	$2^{126.2}ONE + 2^{98.94}A + 2^{136}E$	Appendix B
Simon128/128	68	49	$2^{127.6}$	$2^{87.77}A + 2^{120}E$	Appendix B
Simon128/192	69	48	$2^{126.6}$	$2^{187.6}$	[6]
		51	$2^{127.6}$	$2^{165}ONE + 2^{155.77}A + 2^{184}E$	Appendix B
Simon128/256	72	50	$2^{126.6}$	$2^{242.6}$	[6]
		53	$2^{127.6}$	$2^{249}ONE + 2^{239.77}A + 2^{248}E$	Appendix B

[a] '-' means not given
[b] TWO means two rounds encryption or decryption
[c] A means addition
[d] E means encryption of attacked rounds
[e] ONE means one round encryption or decryption

Also, there are some results with other attack models, such as impossible differential cryptanalysis [15–18], zero-correlation cryptanalysis [16] and integral cryptanalysis [16].

Our Contributions. In this paper, we give improved linear hull cryptanalysis on all versions of Simon family with dynamic key-guessing technique, which was proposed initially to improve the differential attack on Simon [14], using existing linear hull distinguishers. In linear attack, one important point is to compute the empirical correlations (bias) of the parity bit, which derives from the Xor-sum of the active bits at both sides of the linear hull distinguisher, under some key guess. And our attack on Simon improves this procedure efficiently.

The non-linear part in the round function of Simon is mainly dedrived from the bitwise AND (&) operation while it has a significant weakness. For details, if one of the two elements is equal to zero, the result of their AND will be zero, no matter what value the other element is. For a function $f = f_1(x_1, k_1)\&f_2(x_2, k_2)$, if we GUESS k_1 at first, and SPLIT the all $x = x_1||x_2$ into two cases: case 1, $f_1(x_1, k_1) = 0$; case 2, $f_1(x_1, k_1) = 1$, there is no need to guess the key bits k_2 in case 1, since $f = 0$ holds for any value of f_2 in case 1. Then, we can compute the correlations in each case with less time and at last, we COMBINE the two correlations together for corresponding key $k = k_1||k_2$.

At first, we give the boolean representations for the parity bit in the linear distinguisher of Simon. And then we apply the GUESS, SPLIT and COMBINE technique in the calculation of the empirical correlations, which mainly exploits the dynamic key-guessing idea to reduce the number of subkey bits guessed significantly. For example, in the attack on 21-round Simon32, 32 subkey bits are involved. With above technique, we can only guess 12.5 bits from the total 32-bit subkey on average to compute the correlations.

As a result, the improved attack results are shown as follows. We can attack 23-round Simon32/64, 24-round Simon48/72, 25-round Simon48/96, 30-round Simon64/96, 31-round Simon64/128, 37-round Simon96/96, 38-round Simon96/144, 49-round Simon128/128, 51-round Simon128/192 and 53-round Simon128/256. This improves the linear attack results for all versions. From the point of number of rounds attacked, the results on all versions are best known up to state.

The paper is organised as follows. In section 2, we introduce the linear (hull) cryptanalysis and give the description of Simon family. Section 3 gives the time reduction technique used in the linear cryptanalysis. Then the improved attack on Simon32/64 is given in section 4. Finally, we conclude in section 5. Appendix A gives the time complexities to calculate the empirical correlations in some simple situations. The detailed linear attacks on other versions of Simon except Simon32 are given in Appendix B.

2 Preliminaries

2.1 Linear Cryptanalysis and Linear Hull

$\mathbb{F}_2$ denotes the field with two elements and $\mathbb{F}_2^n$ is the n-dimensional vector space of $\mathbb{F}_2$. Let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Let $B(g) = \sum_{x\in\mathbb{F}_2^n}(-1)^{g(x)}$. The correlation $c(g)$ of g is defined by

$$c(g) = 2^{-n} \sum_{x\in\mathbb{F}_2^n}(-1)^{g(x)} = 2^{-n}B(g).$$

(In some situations of the remainder of this paper, we regard $B(g)$ as the correlation for simplicity of description.) The bias of g is defined by half of $c(g)$, which is represented as $\epsilon(g) = \frac{1}{2}c(g)$.

Linear cryptanalysis [2] is a powerful cryptanalytic method proposed in 1993 to cryptanalysis DES. At first, one tries to find a good linear approximation involving some plaintext bits, ciphertext bits and the subkey bits as follows

$$\alpha \cdot P \oplus \beta \cdot C = \gamma \cdot K,$$

where α, β, γ are masks and P, C, K represent the plaintext, ciphertext and keys. 'good' means that the probability of the linear approximations is far away from 1/2, which is the probability in random situations. In other words, higher absolute of bias $\epsilon(\alpha \cdot P \oplus \beta \cdot C \oplus \gamma \cdot K)$ leads to better linear crypanalysis result in general. Algorithm 1 and Algorithm 2 in [2] are two attack models exploiting the linear approximation as distinguisher. $\mathcal{O}(\frac{1}{\epsilon^2})$ known plaintextx are needed in the key-recovery attacks.

Then in 1994, Nyberg [4] studied the linear approximations with same input mask α and output mask β, and denoted them as linear hull. The potential of a linear hull is defined as

$$ALH(\alpha, \beta) = \sum_{\gamma} \epsilon^2(\alpha \cdot P \oplus \beta \cdot C \oplus \gamma \cdot K) = \bar{\epsilon}^2.$$

The effect of linear hull is that the final bias $\bar{\epsilon}$ may become significantly higher than that of any individual linear trail. Then the linear attacks with linear hull require less known plaintexts, *i.e.,* $\mathcal{O}(\frac{1}{\bar{\epsilon}^2})$.

Selçuk and Biçak [5] gave the estimation of success probability in linear attack for achieving a desired advantage level. The advantage is the complexity reduction over the exhaustive search. For example, if m-bit key is attacked and the right key is ranked t-th among all 2^m candidates, the advantage of this attack is $m - log_2(t)$. Theorem 2 in [5] described the relation between success rate, advantage and number of data samples.

Theorem 1 (Theorem 2 in [5]). *Let P_S be the probability that a linear attack, as defined by Algorithm-2 in [2], where all candidates are tried for an m-bit subkey, in an approximation of probability p, with N known plaintext blocks, delivers an a-bit or higher advantage. Assuming that the approximation's probablity is independent for each key tried and is equal to $1/2$ for all wrong keys, we have, for sufficiently large m and N,*

$$P_S = \int_{-2\sqrt{N}|p-1/2|+\Phi^{-1}(1-2^{-a-1})}^{\infty} \phi(x)dx,$$

independent of m.

2.2 Description of SIMON

SIMON is a family of lightweight block cipher with Feistel structure designed by NSA, which is tuned for optimal performance in hardware applications [1]. The SIMON block cipher with an n-bit word (hence $2n$-bit block) is denoted SIMON$2n$, where n is limited to be 16, 24, 32, 48 or 64. The key length is required to be mn where m takes value from $2, 3$ and 4. SIMON$2n$ with m-word key is referred to SIMON$2n/mn$. There are ten versions in the SIMON family and the detailed parameters are listed in Table 2.

Table 2. The SIMON Family Block Ciphers

block size ($2n$)	key size (mn)	rounds
32 ($n = 16$)	64 ($m = 4$)	32
48 ($n = 24$)	72 ($m = 3$)	36
	96 ($m = 4$)	36
64 ($n = 32$)	96 ($m = 3$)	42
	128 ($m = 4$)	44
96 ($n = 48$)	96 ($m = 2$)	52
	144 ($m = 3$)	54
128 ($n = 64$)	128 ($m = 2$)	68
	192 ($m = 3$)	69
	256 ($m = 4$)	72

Before introducing the round functions of SIMON, we give some notations of symbols used throughout this paper.

X^r	$2n$-bit output of round r (input of round $r+1$)
X^r_L	left half n-bit of X^r
X^r_R	right half n-bit of X^r
K^r	subkey used in round $r+1$
x_i	the i-th bit of x, begin with bit 0 from right (e.g., $X^r_{L,0}$ is the LSB of X^r_L)
$x_{i_1,\ldots,i_t}$	the XOR-sum of x_i for $i = i_1, i_2, \ldots, i_t$ (e.g., $x_{0,1} = x_0 \oplus x_1$)
$x \lll i$	left circulant shift by i bits of x
$\oplus$	bitwise XOR
&	bitwise AND
$F(x)$	non-linear function used in round function of SIMON, $F(x) = ((x \lll 1)\&(x \lll 8)) \oplus (x \lll 2)$

The r-th round function of SIMON$2n$ is a Feistel map

$$F_{K^{r-1}} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n,$$
$$(X_L^{r-1}, X_R^{r-1}) \to (X_L^r, X_R^r)$$

where $X^r_R = X^{r-1}_L$ and $X^r_L = F(X^{r-1}_L) \oplus X^{r-1}_R \oplus K^{r-1}$. The round function of SIMON is depicted in Figure 1. Suppose the number of rounds is T, the whole encryption of SIMON is the composition $F_{K^{T-1}} \circ \cdots \circ F_{K^1} \circ F_{K^0}$. The subkeys are derived from the master key. The key schedules are a little different depending on the key size. However, the master key can be derived from any m consecutive subkeys. Please refer to [1] for more details.

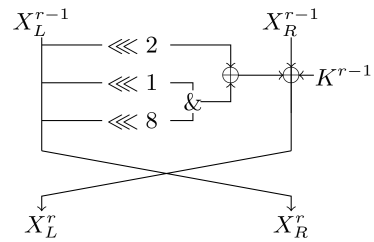

Fig. 1. Round Function of SIMON

3 Time Reduction in Linear Cryptanalysis for Bit-Oriented Block Cipher

For bit-oriented block cipher, such as SIMON, the operations of round function can be seen as the concanetation of some Boolean functions. For example, in SIMON32, the 0-th bit of X_L^r is a Boolean function of some bits of X^{r-1} and subkeys as follows,

$$X_{L,0}^r = (X_{L,15}^{r-1} \& X_{L,8}^{r-1}) \oplus X_{L,14}^{r-1} \oplus X_{R,0}^{r-1} \oplus K_0^{r-1}.$$

Other bits in X_L^r have similar Boolean represetations and the bits in X_R^r are same with the bits in X_L^{r-1}. The Boolean representation of one bit can be extended to multiple rounds.

3.1 Linear Compression

In Matsui's improved linear cryptanalysis [3], the attacker can pre-construct a table to store the plaintexts and ciphertexts. We call this pre-construction procedure as linear compression, since the purpose is to reduce the size of efficient states by compressing the linear part. The detail of the compression is as follows.

Suppose x is a l_1-bit value derived from the n-bit plaintext or cipertext and k_1 is a l-bit value derived from the subkey. $y \in \mathbb{F}_2$ is a Boolean function of x and k, $y = f(x, k)$. Let $V[x]$ denote the number of x. We define $B^k(y)$ with counter vector V and function $y = f(x, k)$ for k as

$$B^k(y) = \sum_x (-1)^{f(x,k)} V[x].$$

So, $B^k(y)$ is the correlation of y under key guess k. One needs to do $2^{l_1+l_2}$ computations of function f to calculate the correlations of y for all k with a straight-forward method at most. If y is linear with some bits of x and k, the time can be decreased.

For simplicity, let $x = x'||x_0$, $k = k'||k_0$ and $y = x_0 \oplus k_0 \oplus g(x', k')$. The correlation of y under some k is

$$B^k(y) = (-1)^{k_0} \sum_{x'} (-1)^{g(x',k')} (V[x'||k_0] - V[x'||k_0 \oplus 1]).$$

It is obvious the correlations of y under same k' and different k_0 have same absolute value, and they are different just in the sign. So if we compress the x_0 bit at first according to $V'[x'] = V[x'||0] - V[x'||1]$, $B^{k'}(y')$ with counter vertor V' and function $y' = g'(x', k')$ for k' can be computed with $2^{l_1+l_2-2}$ calculations of g'. And the correlation $B^k(y)$ can be derived directly from $B^k(y) = (-1)^{k_0} B^{k'}(y')$. We define k_0 the related bit. If the absolute correlations are desired, the related bit k_0 can be omitted directly, since it has no effect on the absolute values.

If y is linear with multiple bits of x and k, the linear bits can be combined at first, then above linear compression can be applied. For example, $y = (x_0 \oplus k_0) \oplus \cdots \oplus (x_t \oplus k_t) \oplus g'(x'', k'')$ where x'', k'' are the other bits of x and k respectively. We can initialize a new counter vector $V'[x''||x_0']$ where x_0' is 1-bit and set $V'[x''||x_0'] = \sum_{x_0 \oplus \cdots \oplus x_t = x_0'} V[x]$. Let $k_0' = k_0 \oplus \cdots \oplus k_t$. The target value y becomes $y = x_0' \oplus k_0' \oplus g'(x'', k'')$ with counter vector $V'[x''||x_0']$, which is the case discussed above.

3.2 Dynamic key-guessing in linear attack: Guess, Split and Combination

Suppose one want to compute $B^k(y)$ with counter vector V and Boolean function $y = f(x, k)$, along with the definitions in the above section. With a straight-forward method, the time to compute $B^k(y)$ is $2^{l_1+l_2}$. If for different values of x, different key bits of k are involved in function $f(x, k)$, the time to calculate $B^k(y)$ can be decreased.

Fig. 2. When k_G is known, the set of x can be splitted to two sets. f is independent of k_B in set S_A and independent of k_A in set S_B.

For simplicity, let $k = k_G||k_A||k_B||k_C$, where k_G, k_A, k_B, k_C are l_2^G, l_2^A, l_2^B and l_2^C bits ($l_2^G + l_2^A + l_2^B + l_2^C = l_2$) respectively. Suppose when k_G is known, the all x can be splitted into two sets, *i.e.* S_A with N_A elements and S_B with N_B elements ($N_A + N_B = 2^{l_1}$). And when $x \in S_A$, $f(x, k) = f_A(x, k_A||k_C)$ which is independent of k_B; when $x \in S_B$, $f(x, k) = f_B(x, k_B||k_C)$ which is independent of k_A (See Figure 2). Then, $B^k(y)$ can be obtained from the following combination

$$B^k(y) = \sum_{x \in S_A} (-1)^{f_A(x,k_A||k_C)} V[x] + \sum_{x \in S_B} (-1)^{f_B(x,k_B||k_C)} V[x]$$

for some guessed k_G. The time to compute $\sum(-1)^{f_A(x,k_A||k_C)} V[x]$ for the $x \in S_A$ needs $N_A 2^{l_2^G + l_2^A + l_2^C}$ calculations, while $\sum(-1)^{f_B(x,k_B||k_C)} V[x]$ for $x \in S_B$ needs $N_B 2^{l_2^G + l_2^B + l_2^C}$. The combination needs 2^{l_2} additions. So the time complexity in total is about

$$N_A 2^{l_2^G + l_2^A + l_2^C} + N_B 2^{l_2^G + l_2^B + l_2^C} + 2^{l_2}$$

which improves the time complexity compared with $2^{l_1+l_2}$.

The AND operation in Simon will generate the situations discussed above. Let $x, k \in \mathbb{F}_2^2$ and $y = f(x, k) = (x_0 \oplus k_0)\&(x_1 \oplus k_1)$. $V[x]$ denotes the number of x. With a straight-forward method, the calculation of correlations for all k need time $2^{2+2} = 2^4$. If one side of the AND in $f(x, k)$ is 0, y would be 0 without knowing the value in the other side. Exploiting this property, we can improve the time complxity for calculating the correlations. At first, we guess one bit of k, *e.g.* k_0. Then we split the x into two sets and compute the correlations in each set. At last, we compose the correlations according to the keys guessed.

- GUESS k_0 and SPLIT the x into two sets
  - For the x with $x_0 = k_0$, initialize a counter T_0 and set $T_0 = V[0||x_0] + V[1||x_0]$
  - For the x with $x_0 = k_0 \oplus 1$, initialize a counter T_1 and set $T_1 = V[0||x_0] - V[1||x_0]$ (Linear compression)
  - COMBINATION $B(y) = T_0 + (-1)^{k_1} T_1$ (k_1 is a related bit)

So in total, it needs $2(1 + 1 + 2) = 2^3$ additions to compute the correlations for all the k, which improves the time complexity compared to the straight-forward method. Although there are 2 bits of k involved in the attack, we guess only one bit and make some computations while another bit is just involved in the final combination. This can be viewed as that we reduce the number of key bits guessed from 2 to 1. Morever, this technique adapts to some complicated Boolean functions and more key (or equivalent key) bits can be reduced significantly. Some cases have been discussed in Appendix A.

4 Linear Cryptanalysis on Simon

In this section, we will give the improved procedure of linear attack on Simon using existing linear hull distinguishers for all versions of Simon

Table 3. Linear Hulls for SIMON

Versions	Input Active Bits	Output Active Bits	ALH	#Rounds	Ref.
SIMON32/K	$X^i_{L,6}$	$X^{i+13}_{R,14}$	$2^{-31.69}$	13	[6]
	$X^i_{L,5}$	$X^{i+13}_{R,13}$	$2^{-30.19}$	13	[7]
	$X^i_{L,0}$	$X^{i+14}_{L,8}, X^{i+14}_{R,6}$	$2^{-32.56}$	14	[6]
SIMON48/K	$X^i_{L,7}, X^i_{L,11}, X^i_{L,19}, X^i_{R,9}, X^i_{R,17}$	$X^{i+15}_{L,5}, X^{i+15}_{R,3}, X^{i+15}_{R,7}, X^{i+15}_{R,11}, X^{i+15}_{R,19}$	$2^{-44.11}$	15	[6]
	$X^i_{L,6}, X^i_{L,14}, X^i_{L,18}, X^i_{L,22}, X^i_{R,16}$	$X^{i+15}_{L,4}, X^{i+15}_{L,20}, X^{i+15}_{R,6}, X^{i+15}_{R,18}, X^{i+15}_{R,20}, X^{i+15}_{R,22}$	$2^{-42.28}$	15	[7]
	$X^i_{L,1}, X^i_{L,5}, X^i_{L,21}, X^i_{R,23}$	$X^{i+16}_{L,1}, X^{i+16}_{L,5}, X^{i+16}_{R,23}$	$2^{-44.92}$	16	[12]
SIMON64/K	$X^i_{L,20}, X^i_{L,24}, X^i_{R,22}$	$X^{i+21}_{L,22}, X^{i+21}_{R,20}, X^{i+21}_{R,24}$	$2^{-62.53}$	21	[6]
	$X^i_{L,6}$	$X^{i+21}_{L,0}, X^{i+21}_{R,2}, X^{i+21}_{R,6}, X^{i+21}_{R,30}$	$2^{-60.72}$	21	[7]
	$X^i_{L,3}, X^i_{L,27}, X^i_{L,31}, X^i_{R,29}$	$X^{i+22}_{L,3}, X^{i+22}_{R,1}, X^{i+22}_{R,2}$	$2^{-63.83}$	22	[7]
SIMON96/K	$X^i_{L,2}, X^i_{L,34}, X^i_{L,38}, X^i_{L,42}, X^i_{R,36}$	$X^{i+30}_{L,2}, X^{i+30}_{L,42}, X^{i+30}_{L,46}, X^{i+30}_{R,0}, X^{i+30}_{R,40}$	$2^{-94.2}$	30	[6]
SIMON128/K	$X^i_{L,2}, X^i_{L,58}, X^i_{L,62}, X^i_{R,60}$	$X^{i+41}_{L,60}, X^{i+41}_{R,0}, X^{i+41}_{R,2}, X^{i+41}_{R,58}, X^{i+41}_{R,62}$	$2^{-126.6}$	41	[6]

4.1 Linear Hulls of SIMON

Some linear hulls have been proposed recently in [6, 7, 12], and they are displayed in Table 3. Abdelraheem *et al.* [6] took advantage of the connection between linear- and differential- characteristics for SIMON and transformed the differential characteristics proposed in [8, 10] to linear characteristics directly. Similarly, differentials can be transformed to the linear hulls. Also, they found a new 14-round linear hull for SIMON32/64, by constructing squared correlation matrix to compute the average squared correlation. Shi *et al.* [7] searched the linear characteristics with same input and output masks using the Mixed-integer Linear Programming modelling, which was investigated to search the differential characteristics for bit-oriented block cipher [11] and then extended to search the linear characteristics (hull) later [12].

Similar to the rotational property of integral distinguishers and zero-correlation linear hull shown in [16], more linear hulls can be constructed as follows.

Property 1. Assume that $X^i_{L,j^0_0}, \dots, X^i_{L,j^0_{t_0}}, X^i_{R,j^1_0}, \dots, X^i_{R,j^1_{t_1}} \to X^{i+r}_{L,j^2_0}, \dots, X^{i+r}_{L,j^2_{t_2}}, X^{i+r}_{R,j^3_0}, \dots, X^{i+r}_{R,j^3_{t_3}}$ is a r-round linear hull with potential $\bar{\epsilon}^2$ for SIMON$2n$, where $j^0_0, \dots, j^0_{t_0}, j^1_0, \dots, j^1_{t_1}, j^2_0, \dots, j^2_{t_2}, j^3_0, \dots, j^3_{t_3} \in \{0, \dots, n-1\}$. Then for any $0 \le s \le n-1$, let $j^{p*}_q = (j^p_q + s) \bmod n$, for $p = 0, \dots, 3$, $q = 0, \dots, t_p$ and the potential of the r-round linear hull $X^i_{L,j^{0*}_0}, \dots, X^i_{L,j^{0*}_{t_0}}, X^i_{R,j^{1*}_0}, \dots, X^i_{R,j^{1*}_{t_1}} \to X^{i+r}_{L,j^{2*}_0}, \dots, X^{i+r}_{L,j^{2*}_{t_2}}, X^{i+r}_{R,j^{3*}_0}, \dots, X^{i+r}_{R,j^{3*}_{t_3}}$ is also $\bar{\epsilon}^2$.

Observe the two 13-round linear hulls of SIMON32 in Table 3 and we can find they are in fact the rotations of same linear hull. The potential of $X^i_{L,6} \to X^{i+13}_{L,14}$ is estimated as $2^{-31.69}$ in [6] while that of $X^i_{L,5} \to X^{i+13}_{L,13}$ is estimated as $2^{-30.19}$ in [7]. The difference may come from the different search methods and different linear trails found. In the following attack, the potential of the two linear hulls is thought to be $2^{-30.19}$.

4.2 Improved Key Recovery Attack on SIMON32/64

We exploit the 13-round linear hull proposed in [7] to make key recovery attack on round-reduced SIMON32. The linear hull is

$$X^i_{L,5} \to X^{i+13}_{R,13}$$

with potential $\bar{\epsilon}^2 = 2^{-30.19}$. We mount a key recovery attack on 21-round SIMON32/64 by adding four rounds before and appending four rounds after the distinguisher. Here let $P = X^{i-4}$ be the plaintext and $C = X^{i+17}$ be the corresponding ciphertext. Suppose the key bits involved in the first four rounds are K_P and those in the last four rounds are K_C. Then $X^i_{L,5}$ is a function of P and K_P, $X^i_{L,5} = E(P, K_P)$. Similarly, $X^{i+13}_{R,13} = D(C, K_C)$ is a function of C and K_C. Let $\mathcal{S}$ be the set of N plaintext-ciphertext pairs obtained, the empirical correlation under some key K_P, K_C is

$$\bar{c}_{K_P,K_C} = \frac{1}{N} \sum_{P,C \in \mathcal{S}} (-1)^{E(P,K_P) \oplus D(C,K_C)}.$$

Table 4. 4 rounds before $X_{L,5}^{i}$ for SIMON32

x_0	$X_{L,13}^{i-4} \oplus (X_{L,14}^{i-4} \& X_{L,7}^{i-4}) \oplus X_{R,15}^{i-4} \oplus X_{L,1}^{i-4} \oplus X_{L,5}^{i-4}$	k_0	$K_{15}^{i-4} \oplus K_{1}^{i-3} \oplus K_{5}^{i-3} \oplus K_{3}^{i-2} \oplus K_{5}^{i-1}$
x_1	$X_{L,14}^{i-4} \oplus (X_{L,15}^{i-4} \& X_{L,8}^{i-4}) \oplus X_{R,0}^{i-4}$	k_1	K_{0}^{i-4}
x_2	$X_{L,7}^{i-4} \oplus (X_{L,8}^{i-4} \& X_{L,1}^{i-4}) \oplus X_{R,9}^{i-4}$	k_2	K_{9}^{i-4}
x_3	$X_{L,2}^{i-4} \oplus (X_{L,3}^{i-4} \& X_{L,12}^{i-4}) \oplus X_{R,4}^{i-4}$	k_3	K_{4}^{i-4}
x_4	$X_{L,11}^{i-4} \oplus (X_{L,12}^{i-4} \& X_{L,5}^{i-4}) \oplus X_{R,13}^{i-4}$	k_4	K_{13}^{i-4}
x_5	$X_{L,14}^{i-4} \oplus (X_{L,15}^{i-4} \& X_{L,8}^{i-4}) \oplus X_{R,0}^{i-4} \oplus X_{L,2}^{i-4}$	k_5	$K_{0}^{i-4} \oplus K_{2}^{i-3}$
x_6	$X_{L,15}^{i-4} \oplus (X_{L,0}^{i-4} \& X_{L,9}^{i-4}) \oplus X_{R,1}^{i-4}$	k_6	K_{1}^{i-4}
x_7	$X_{L,8}^{i-4} \oplus (X_{L,9}^{i-4} \& X_{L,2}^{i-4}) \oplus X_{R,10}^{i-4}$	k_7	K_{10}^{i-4}
x_8	$X_{L,7}^{i-4} \oplus (X_{L,8}^{i-4} \& X_{L,1}^{i-4}) \oplus X_{R,9}^{i-4} \oplus X_{L,11}^{i-4}$	k_8	$K_{9}^{i-4} \oplus K_{11}^{i-3}$
x_9	$X_{L,1}^{i-4} \oplus (X_{L,2}^{i-4} \& X_{L,11}^{i-4}) \oplus X_{R,3}^{i-4}$	k_9	K_{3}^{i-4}
x_{10}	$X_{L,14}^{i-4} \oplus (X_{L,15}^{i-4} \& X_{L,8}^{i-4}) \oplus X_{R,0}^{i-4} \oplus (X_{L,3}^{i-4} \& X_{L,12}^{i-4}) \oplus X_{R,4}^{i-4}$	k_{10}	$K_{0}^{i-4} \oplus K_{2}^{i-3} \oplus K_{4}^{i-4} \oplus K_{4}^{i-2}$
x_{11}	$X_{L,15}^{i-4} \oplus (X_{L,0}^{i-4} \& X_{L,9}^{i-4}) \oplus X_{R,1}^{i-4} \oplus X_{L,3}^{i-4}$	k_{11}	$K_{1}^{i-4} \oplus K_{3}^{i-3}$
x_{12}	$X_{L,0}^{i-4} \oplus (X_{L,1}^{i-4} \& X_{L,10}^{i-4}) \oplus X_{R,2}^{i-4}$	k_{12}	K_{2}^{i-4}
x_{13}	$X_{L,9}^{i-4} \oplus (X_{L,10}^{i-4} \& X_{L,3}^{i-4}) \oplus X_{R,11}^{i-4}$	k_{13}	K_{11}^{i-4}
x_{14}	$X_{L,8}^{i-4} \oplus (X_{L,9}^{i-4} \& X_{L,2}^{i-4}) \oplus X_{R,10}^{i-4} \oplus X_{L,12}^{i-4}$	k_{14}	$K_{10}^{i-4} \oplus K_{12}^{i-3}$
x_{15}	$X_{L,7}^{i-4} \oplus (X_{L,8}^{i-4} \& X_{L,1}^{i-4}) \oplus X_{R,9}^{i-4} \oplus (X_{L,12}^{i-4} \& X_{L,5}^{i-4}) \oplus X_{R,13}^{i-4}$	k_{15}	$K_{9}^{i-4} \oplus K_{11}^{i-3} \oplus K_{13}^{i-4} \oplus K_{13}^{i-2}$
x_{16}	$X_{L,1}^{i-4} \oplus (X_{L,2}^{i-4} \& X_{L,11}^{i-4}) \oplus X_{R,3}^{i-4} \oplus X_{L,5}^{i-4}$	k_{16}	$K_{3}^{i-4} \oplus K_{5}^{i-3}$

Notice: $x_{10} = x_3 \oplus x_5, x_{15} = x_4 \oplus x_8$

Table 5. 4 rounds after $X_{R,13}^{i+13}$ for SIMON32

x_0	$X_{R,5}^{i+17} \oplus (X_{R,6}^{i+17} \& X_{R,15}^{i+17}) \oplus X_{L,7}^{i+17} \oplus X_{R,9}^{i+17} \oplus X_{R,13}^{i+17}$	k_0	$K_{7}^{i+16} \oplus K_{9}^{i+15} \oplus K_{13}^{i+15} \oplus K_{11}^{i+14} \oplus K_{13}^{i+13}$
x_1	$X_{R,6}^{i+17} \oplus (X_{R,7}^{i+17} \& X_{R,0}^{i+17}) \oplus X_{L,8}^{i+17}$	k_1	K_{8}^{i+16}
x_2	$X_{R,15}^{i+17} \oplus (X_{R,0}^{i+17} \& X_{R,9}^{i+17}) \oplus X_{L,1}^{i+17}$	k_2	K_{1}^{i+16}
x_3	$X_{R,10}^{i+17} \oplus (X_{R,11}^{i+17} \& X_{R,4}^{i+17}) \oplus X_{L,12}^{i+17}$	k_3	K_{12}^{i+16}
x_4	$X_{R,3}^{i+17} \oplus (X_{R,4}^{i+17} \& X_{R,13}^{i+17}) \oplus X_{L,5}^{i+17}$	k_4	K_{5}^{i+16}
x_5	$X_{R,6}^{i+17} \oplus (X_{R,7}^{i+17} \& X_{R,0}^{i+17}) \oplus X_{L,8}^{i+17} \oplus X_{R,10}^{i+17}$	k_5	$K_{8}^{i+16} \oplus K_{10}^{i+15}$
x_6	$X_{R,7}^{i+17} \oplus (X_{R,8}^{i+17} \& X_{R,1}^{i+17}) \oplus X_{L,9}^{i+17}$	k_6	K_{9}^{i+16}
x_7	$X_{R,0}^{i+17} \oplus (X_{R,1}^{i+17} \& X_{R,10}^{i+17}) \oplus X_{L,2}^{i+17}$	k_7	K_{2}^{i+16}
x_8	$X_{R,15}^{i+17} \oplus (X_{R,0}^{i+17} \& X_{R,9}^{i+17}) \oplus X_{L,1}^{i+17} \oplus X_{R,3}^{i+17}$	k_8	$K_{1}^{i+16} \oplus K_{3}^{i+15}$
x_9	$X_{R,9}^{i+17} \oplus (X_{R,10}^{i+17} \& X_{R,3}^{i+17}) \oplus X_{L,11}^{i+17}$	k_9	K_{11}^{i+16}
x_{10}	$X_{R,6}^{i+17} \oplus (X_{R,7}^{i+17} \& X_{R,0}^{i+17}) \oplus X_{L,8}^{i+17} \oplus (X_{R,11}^{i+17} \& X_{R,4}^{i+17}) \oplus X_{L,12}^{i+17}$	k_{10}	$K_{8}^{i+16} \oplus K_{10}^{i+15} \oplus K_{12}^{i+16} \oplus K_{12}^{i+14}$
x_{11}	$X_{R,7}^{i+17} \oplus (X_{R,8}^{i+17} \& X_{R,1}^{i+17}) \oplus X_{L,9}^{i+17} \oplus X_{R,11}^{i+17}$	k_{11}	$K_{9}^{i+16} \oplus K_{11}^{i+15}$
x_{12}	$X_{R,8}^{i+17} \oplus (X_{R,9}^{i+17} \& X_{R,2}^{i+17}) \oplus X_{L,10}^{i+17}$	k_{12}	K_{10}^{i+16}
x_{13}	$X_{R,1}^{i+17} \oplus (X_{R,2}^{i+17} \& X_{R,11}^{i+17}) \oplus X_{L,3}^{i+17}$	k_{13}	K_{3}^{i+16}
x_{14}	$X_{R,0}^{i+17} \oplus (X_{R,1}^{i+17} \& X_{R,10}^{i+17}) \oplus X_{L,2}^{i+17} \oplus X_{R,4}^{i+17}$	k_{14}	$K_{2}^{i+16} \oplus K_{4}^{i+15}$
x_{15}	$X_{R,15}^{i+17} \oplus (X_{R,0}^{i+17} \& X_{R,9}^{i+17}) \oplus X_{L,1}^{i+17} \oplus (X_{R,4}^{i+17} \& X_{R,13}^{i+17}) \oplus X_{L,5}^{i+17}$	k_{15}	$K_{1}^{i+16} \oplus K_{3}^{i+15} \oplus K_{5}^{i+16} \oplus K_{5}^{i+14}$
x_{16}	$X_{R,9}^{i+17} \oplus (X_{R,10}^{i+17} \& X_{R,3}^{i+17}) \oplus X_{L,11}^{i+17} \oplus X_{R,13}^{i+17}$	k_{16}	$K_{11}^{i+16} \oplus K_{13}^{i+15}$

Notice: $x_{10} = x_3 \oplus x_5, x_{15} = x_4 \oplus x_8$

In a further step, $X_{L,5}^{i}$ can be represented as

$$
\begin{aligned}
&f(x,k) = x_0 \oplus k_0 \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)) \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4)) \oplus \\
&[(x_5 \oplus k_5 \oplus ((x_6 \oplus k_6)\&(x_7 \oplus k_7)))\&(x_8 \oplus k_8 \oplus ((x_9 \oplus k_9)\&(x_7 \oplus k_7)))] \oplus \\
&\{(x_{10} \oplus k_{10} \oplus ((x_6 \oplus k_6)\&(x_7 \oplus k_7)) \oplus \\
&[(x_{11} \oplus k_{11} \oplus ((x_{12} \oplus k_{12})\&(x_{13} \oplus k_{13})))\&(x_{14} \oplus k_{14} \oplus ((x_3 \oplus k_3)\&(x_{13} \oplus k_{13})))]) \& \\
&(x_{15} \oplus k_{15} \oplus ((x_7 \oplus k_7)\&(x_9 \oplus k_9)) \oplus \\
&[(x_{14} \oplus k_{14} \oplus ((x_{13} \oplus k_{13})\&(x_3 \oplus k_3)))\&(x_{16} \oplus k_{16} \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4)))])\}
\end{aligned}
$$

where the representation of x and k are 17-bit value shown in Table 4. With the same way, $X_{R,13}^{i+13}$ can also be represented as $f(x,k)$ where the corresponding x and k are described in Table 5. To distinguish them, let x_P, k_P be the x, k described in Table 4 and x_C, k_C be the x, k described in Table 5. The N plaintext-ciphertext pairs in $\mathcal{S}$ can be compressed into a counter vector $V[x_P, x_C]$, which stores the number of x_P, x_C. Then there is

$$\bar{c}_{k_P,k_C} = \frac{1}{N} \sum_{x_P,x_C} (-1)^{f(x_P,k_P)\oplus f(x_C,k_C)} V[x_P, x_C].$$

Notice that $f(x,k)$ is linear with $x_0 \oplus k_0$. According to the linear compression technique, the 0-th bit of x_P and x_C could be compressed initially. Suppose that x'_P is the 16-bit value of x_P without the 0-th bit (same representations for x'_C, k'_P, k'_C). Initialize a new counter vector $V_1[x'_P, x'_C] = \sum_{x_{P,0},x_{C,0}} (-1)^{x_{P,0}\oplus x_{C,0}} V[x_P, x_C]$. Then the correlation becomes

$$\bar{c}_{k'_P,k'_C} = \frac{1}{N} \sum_{x'_P,x'_C} (-1)^{f'(x'_P,k'_P)\oplus f'(x'_C,k'_C)} V_1[x'_P, x'_C] = \frac{1}{N} \sum_{x'_C} (-1)^{f'(x'_C,k'_C)} \sum_{x'_P} (-1)^{f'(x'_P,k'_P)} V_1[x'_P, x'_C],$$

where f' is part of f, *i.e.* $f(x,k) = x_0 \oplus k_0 \oplus f'(x',k'), x' = (x_1,\ldots,x_{16}), k' = (k_1,\ldots,k_{16})$.

So we can guess k'_P (16-bit) at first and compress the plaintexts into a counter. Then guess k'_C (16-bit) to decrypt the appending rounds, to achieve the final correlations. In the following, we introduce the attack procedure in the forward rounds in detail. And the procedure to compute $\sum_{x'_P} (-1)^{f'(x'_P,k'_P)} V_1[x'_P, x'_C]$ for some x'_C is same with the procedure to compute $B^{k'}(y)$ with counter vector $V'[x']$ (here $V'[x'] = V_1[x', x'_C]$ when x'_C takes some const value) and Boolean function f'. Morever, there are relations that $x_{10} = x_3 \oplus x_5, x_{15} = x_4 \oplus x_8$ in Table 4,5, which means there are only 14 independent bits for x' (x'_P or x'_C).

Compute $B^{k'}(y)$ with counter vector $V'[x']$ and Boolean function f'. (For simplicity, we define this procedure as Procedure A.) Although x' is a 16-bit value, there are only 2^{14} possible values for x' as explained above. We use the guess, split and combination technique to decrease the time complexity to compute $B^{k'}(y)$ with counter vector $V'[x']$ and Boolean function $y = f'$, for 2^{16} key vaules k'.

1. Guess k_1, k_3, k_7 and split the plaintexts into 8 sets according to the value $(x_1 \oplus k_1, x_3 \oplus k_3, x_7 \oplus k_7)$. The simplification for $f'(x',k')$ after guessing some keys are shown in Table 6. The representation of f_{ij} are

Table 6. Simplification for $f'(x',k')$ after guessing k_1, k_3, k_7

Guess	$x_1 \oplus k_1, x_3 \oplus k_3, x_7 \oplus k_7$	f'	Related Bit
k_1, k_3, k_7	0,0,0	f_{00}	
	0,0,1	f_{01}	
	0,1,0	f_{10}	k_4
	0,1,1	f_{11}	k_4
	1,0,0	f_{00}	k_2
	1,0,1	f_{01}	k_2
	1,1,0	f_{10}	$k_{2,4}$
	1,1,1	f_{11}	$k_{2,4}$

as follows,

$$\begin{aligned} f_{00} =& ((x_5 \oplus k_5)\&(x_8 \oplus k_8)) \oplus \{(x_{10} \oplus k_{10} \oplus [(x_{11} \oplus k_{11} \oplus ((x_{12} \oplus k_{12})\&(x_{13} \oplus k_{13})))\&(x_{14} \oplus k_{14})]) \\ & \&(x_{15} \oplus k_{15} \oplus [(x_{14} \oplus k_{14})\&(x_{16} \oplus k_{16})])\}, \\ f_{01} =& ((x_{5,6} \oplus k_{5,6})\&(x_{8,9} \oplus k_{8,9})) \oplus \{(x_{6,10} \oplus k_{6,10} \oplus [(x_{11} \oplus k_{11} \oplus ((x_{12} \oplus k_{12})\&(x_{13} \oplus k_{13})))\&(x_{14} \oplus k_{14})]) \\ & \&(x_{9,15} \oplus k_{9,15} \oplus [(x_{14} \oplus k_{14})\&(x_{16} \oplus k_{16})])\}, \\ f_{10} =& ((x_5 \oplus k_5)\&(x_8 \oplus k_8)) \oplus \{(x_{10} \oplus k_{10} \oplus [(x_{11} \oplus k_{11} \oplus ((x_{12} \oplus k_{12})\&(x_{13} \oplus k_{13})))\&(x_{13,14} \oplus k_{13,14})]) \\ & \&(x_{15} \oplus k_{15} \oplus [(x_{13,14} \oplus k_{13,14})\&(x_{4,16} \oplus k_{4,16})])\}, \\ f_{11} =& ((x_{5,6} \oplus k_{5,6})\&(x_{8,9} \oplus k_{8,9})) \oplus \{(x_{6,10} \oplus k_{6,10} \oplus [(x_{11} \oplus k_{11} \oplus ((x_{12} \oplus k_{12})\&(x_{13} \oplus k_{13})))\&(x_{13,14} \oplus k_{13,14})]) \\ & \&(x_{9,15} \oplus k_{9,15} \oplus [(x_{13,14} \oplus k_{13,14})\&(x_{4,16} \oplus k_{4,16})])\}. \end{aligned}$$

The counter vectors for x' can be compressed in a further step according to the new representations of f'. For example, if $(x_1 \oplus k_1, x_3 \oplus k_3, x_7 \oplus k_7) = (0,0,0)$, f' will be equal to the formula f_{00}, which is independent of x_2, x_4, x_6, x_9. So we compress the corresponding counters into a new counter V_{000}, and

$$V_{000}[x_5, x_8, x_{10} - x_{16}] = \sum_{x_1=k_1, x_3=k_3, x_7=k_7, x_2 \in \mathbb{F}_2, x_4 \in \mathbb{F}_2, x_6 \in \mathbb{F}_2, x_9 \in \mathbb{F}_2} V'[x'].$$

Notice $x_{10} = x_3 \oplus x_5$, so there are 8 independent x bits for $x_5, x_8, x_{10} - x_{16}$. Notice $x_{15} = x_4 \oplus x_8$, for some fixed value of $x_5, x_8, x_{10} - x_{16}$, there are 7 times addition in above equation. So generating this new counter vectror needs $2^8 \times 7$ additions.
We give another example to illustrate the situations with related key bit. If $(x_1 \oplus k_1, x_3 \oplus k_3, x_7 \oplus k_7) = (1,0,0)$, there is $f' = (x_2 \oplus k_2) \oplus f_{00}$. Notice in this subset, f' is linear with $x_2 \oplus k_2$ and x_2 can be compressed into the new counters with related key k_2. So the new counter vector V_{100} is as follows,

$$V_{100}[x_5, x_8, x_{10} - x_{16}] = \sum_{x_1=k_1 \oplus 1, x_3=k_3, x_7=k_7, x_2 \in \mathbb{F}_2, x_4 \in \mathbb{F}_2, x_6 \in \mathbb{F}_2, x_9 \in \mathbb{F}_2} (-1)^{x_2} V'[x'].$$

Also, there are 8 independent x bits for $x_5, x_8, x_{10} - x_{16}$. For each fixed $x_5, x_8, x_{10} - x_{16}$, the new counter can be obtained with 7 additions according to above equation.
The procedures to generate the new counter vectors for other cases are similar as that of case $(x_1 \oplus k_1, x_3 \oplus k_3, x_7 \oplus k_7) = (0,0,0)$ or $(1,0,0)$. Morever, the time complexity to split the plaintexts and construct new counter vectors is same for each case. Observing the four functions f_{00}, f_{01}, f_{10} and f_{11}, we know that they are with same form. In the following step, we explain the attack procedure of case $(x_1 \oplus k_1, x_3 \oplus k_3, x_7 \oplus k_7) = (0,0,0)$ in detail and the others can be obtained in the same way.
Note that, there are 9 subkey bits in each function of f_{00}, f_{01}, f_{10} and f_{11} after guessing k_1, k_3, k_7. So this can be viewed as that $3 + 9 = 12$ subkey bits are involved in the attack while there are 16 subkey bits are involved initially in f'. In the following, the number of key bits can be reduced in a further step.

2. For f_{00}, guess k_5, k_{14} and split the plaintexts into 4 sets according to the value $(x_5 \oplus k_5, x_{14} \oplus k_{14})$. The simplification for f_{00} after guessing some keys are shown in Table 7.

Table 7. Simplification for f_{00} after guessing k_5, k_{14}

Guess	Value	f_{00}	Related key bit
k_5, k_{14}	0,0	$(x_{10} \oplus k_{10}) \& (x_{15} \oplus k_{15})$	
	0,1	$(x_{10,11} \oplus k_{10,11} \oplus ((x_{12} \oplus k_{12}) \& (x_{13} \oplus k_{13}))) \& (x_{15,16} \oplus k_{15,16})$	
	1,0	$(x_{10} \oplus k_{10}) \& (x_{15} \oplus k_{15})$	k_8
	1,1	$(x_{10,11} \oplus k_{10,11} \oplus ((x_{12} \oplus k_{12}) \& (x_{13} \oplus k_{13}))) \& (x_{15,16} \oplus k_{15,16})$	k_8

The time complexity of computing the counters' value $B^{k_5, k_8, k_{10} - k_{16}}(y)$ with counter vector V_{000} and function f_{00} is as follows:

(a) Guess k_5, k_{14} and split the states into four parts
   i. $(x_5 \oplus k_5, x_{14} \oplus k_{14}) = (0,0)$
      A. New counter vector $V^{00}_{000}[x_{10}, x_{15}] = \sum_{x_5=k_5, x_{14}=k_{14}} V_{000}[x_5, x_8, x_{10} - x_{16}]$ needs : $2 \times (2^5 - 1) = 2^6 - 2$ additions. (Notice that x_{10} is fixed here since the dependence between x_5 and x_{10}.)
      B. Partial $B^{k_{10}, k_{15}}_{00}(y)$ with new function and vector V^{00}_{000}: If $k_{10} = x_{10}$, $B^{k_{10}, k_{15}}_{00}(y) = V^{00}_{000}[x_{10}, 0] + V^{00}_{000}[x_{10}, 1]$; if $k_{10} = x_{10} \oplus 1$, $B^{k_{10}, k_{15}}_{00}(y) = (-1)^{k_{15}}(V^{00}_{000}[x_{10}, 0] - V^{00}_{000}[x_{10}, 1])$.So in total there are no more than 2^2 additions.
   ii. $(x_5 \oplus k_5, x_{14} \oplus k_{14}) = (0,1)$
      A. New counter vector $V^{01}_{000}[x_{10,11}, x_{12}, x_{13}, x_{15,16}] = \sum_{x_5=k_5, x_{14}=k_{14} \oplus 1} V_{000}[x_5, x_8, x_{10} - x_{16}]$ needs : $2^4 \times (2^2 - 1) = 2^6 - 2^4$ additions.
      B. Partial $B^{k_{10,11}, k_{12}, k_{13}, k_{15,16}}_{01}(y)$ with new function and vector V^{01}_{000}: $2^{5.64}$ additions (See f_5 in Appendix A)
   iii. $(x_5 \oplus k_5, x_{14} \oplus k_{14}) = (1,0)$

A. New counter vector $V_{000}^{10}[x_{10}, x_{15}] = \sum_{x_5=k_5\oplus1, x_{14}=k_{14}} (-1)^{x_8} V_{000}[x_5, x_8, x_{10} - x_{16}]$ needs : $2 \times (2^5 - 1) = 2^6 - 2$ additions. (Notice that x_{10} is fixed here since the dependence between x_5 and x_{10}.)

B. Partial $B_{10}^{k_{10},k_{15}}(y)$ with new function and vector V_{000}^{10}: 2^2 additions (same with case $(0,0)$).

iv. $(x_5 \oplus k_5, x_{14} \oplus k_{14}) = (1, 1)$

A. New counter vector $V_{000}^{11}[x_{10,11}, x_{12}, x_{13}, x_{15,16}] = \sum_{x_5=k_5, x_{14}=k_{14}\oplus1} (-1)^{x_8} V_{000}[x_5, x_8, x_{10} - x_{16}]$ needs : $2^4 \times (2^2 - 1) = 2^6 - 2^4$ additions.

B. Partial $B_{11}^{k_{10,11},k_{12},k_{13},k_{15,16}}(y)$ with new function and vector V_{000}^{11}: $2^{5.64}$ additions (See f_5 in Appendix A)

(b) For each of 2^9 keys involved in f_{00}, partial $B^{k_5,k_8,k_{10}-k_{16}}(y)$ with function $y = f_{00}$ and counter vector V_{000} under key guess k_5, k_{14} is

$$B^{k_5,k_8,k_{10}-k_{16}}(y) = B_{00}^{k_{10},k_{15}}(y) + B_{01}^{k_{10,11},k_{12},k_{13},k_{15,16}}(y) + (-1)^{k_8}(B_{10}^{k_{10},k_{15}}(y) + B_{01}^{k_{10,11},k_{12},k_{13},k_{15,16}}(y)).$$

We can add $B_{00}^{k_{10},k_{15}}(y)$ and $B_{01}^{k_{10,11},k_{12},k_{13},k_{15,16}}(y)$ at first, then add $B_{10}^{k_{10},k_{15}}(y)$ and $B_{01}^{k_{10,11},k_{12},k_{13},k_{15,16}}(y)$, at last add the two parts according the index value and k_8. The combination phase needs $2^6+2^6+2^7 = 2^8$ additions in total when k_5, k_{14} are fixed.

(c) In total, there are

$$2^2 \times ((2^6 - 2 + 2^2 + 2^6 - 2^4 + 2^{5.64}) \times 2 + 2^8) \approx 2^{11.19}$$

additions to compute $B^{k_5,k_8,k_{10}-k_{16}}(y)$ for all 2^9 possible key values. Note that, about 1 subkey bit is guessed in the first (or third) step of step 2a. In the second (or forth) step of step 2a, 1.5 subkey bits are guessed on average. So, although there are 9 subkey bits in total, only 2+(1+1+1.5+1.5)/4=3.25 bits on average are guessed with dynamic key-guessing technique.

3. The time of computing $B^{k'}(y)$ with counter vector $V'[x']$ and Boolean function f' is shown in Table 8. T_1 denotes the time of seperation of the plaintexts according to the guessed bit of k. T_2 denotes the time of computation in the inner part. T_3 is the time in the combination phase. When k_1, k_3, k_7 are fixed, in each case, $T_1 = 2^8 \times 7$ as explainted in Step 1. T_2 is $2^{11.19}$ as explained in Step 2. There are 13 bits for k' except k_1, k_3, k_7, leading to $T_3 = 2^{13} \times 7$. For all guesses of k_1, k_3, k_7, the total time is about $2^{19.46}$ additions.

Table 8. Time Complexity of computing $B^{k'}(y)$ with counter vector $V'[x']$ and Boolean function f'

Guess	$x_1 \oplus k_1, x_3 \oplus k_3, x_7 \oplus k_7$	f'	Related Bit	Time		
				T_1	T_2	T_3
k_1, k_3, k_7	0,0,0	f_{00}		$2^8 \times 7$	$2^{11.19}$	$2^{13} \times 7$
	0,0,1	f_{01}		$2^8 \times 7$	$2^{11.19}$	
	0,1,0	f_{10}	k_4	$2^8 \times 7$	$2^{11.19}$	
	0,1,1	f_{11}	k_4	$2^8 \times 7$	$2^{11.19}$	
	1,0,0	f_{00}	k_2	$2^8 \times 7$	$2^{11.19}$	
	1,0,1	f_{01}	k_2	$2^8 \times 7$	$2^{11.19}$	
	1,1,0	f_{10}	$k_{2,4}$	$2^8 \times 7$	$2^{11.19}$	
	1,1,1	f_{11}	$k_{2,4}$	$2^8 \times 7$	$2^{11.19}$	
Total Time		$((2^8 \times 7 + 2^{11.19}) \times 8 + 2^{13} \times 7) \times 2^3 = 2^{19.46}$				

In Step 1, 3 key bits are guessed and the plaintexts are splitted into 8 situations. For each situation, 3.25 key bits are guessed as explained above. So on average, about $3 + 3.25 = 6.25$ subkey bits are guessed in this procedure, while there are 16 subkey bits involved.

21-round attack on Simon32/64. Adding four rounds and appending four rounds after the 13-round linear hull distinguisher, we give the 21-round linear attack on Simon32/64. The linear hull holds with potential $\bar{\epsilon}^2 = 2^{-30.19}$. We set $N = 2\bar{\epsilon}^{-2} = 2^{31.19}$ and advantage $a = 8$. The success probability would be 0.477 according to Theorem 1. There are 32 subkey bits involved in this attack. With our attack method, only about $6.25 + 6.25 = 12.5$ bits are guessed on average, which reduces the number of key bits greatly.
Attack:

1. Compress the N plaintext-ciphertext pairs into the counter vector $V_1[x'_P, x'_C]$ of size 2^{14+14}.
2. For each of 2^{14} x'_C
   (a) Call Procedure A. Store the counters according to x'_C and k'_P
3. For each k'_P of 2^{16} possible values.
   (a) Call procedure A. Store the counters according to k'_P and k'_C.
4. The keys with counter values ranked in the largest $2^{32-8} = 2^{24}$ values would be the right subkey candidates. Exploiting the key schedule and guessing some other bits, use two plaintex-ciphertext pairs to check the right key.

Time: (1)$N = 2^{31.19}$ times compression (2) $2^{14} \times 2^{19.46} = 2^{33.46}$ additions. (3)$2^{16} \times 2^{19.46} = 2^{35.46}$ additions. So the time to compute the empirical bias for the subkeys involved is about $2^{35.84}$ while that given in [6] with similar linear hull is $2^{63.69}$. The time is improved significantly. Step (4) is to recovery the master key, which needs $2^{64-8} = 2^{56}$ 21-round encryptions. However, [6] does not give this step.

22-round attack on SIMON32/64. Add one more round before the 21-round attack, we can attack 22-round of SIMON32/64. There are 13 active key bits involved in round $i-5$, which is $\kappa_1 = (K_0^{i-5} - K_3^{i-5}, K_5^{i-5}, K_7^{i-5} - K_{12}^{i-5}, K_{14}^{i-5}, K_{15}^{i-5})$, to obtain the x represented in Table 4.
Attack:

1. Guess each of 2^{13} κ_1
   (a) Encrypt the plaintexts by one round.
   (b) Do as the first three steps in the 21-round attack
2. The keys with counter values ranked in the largest $2^{32+13-8} = 2^{37}$ values would be the right subkey candidates. Exploiting the key schedule and guessing some other bits, use two plaintex-ciphertext pairs to check the right key.

Time: (1.a)$2^{13} \times N = 2^{44.19}$ one-round encryptions. (1.b) $2^{13} \times 2^{35.84} = 2^{48.84}$ additions. (2) Exhaustive phase needs about $2^{64-8} = 2^{56}$ 22-round encryptions.

23-round attack on SIMON32/64. Add one more round before and one round after the 21-round attack, we can attack 23-round of SIMON32/64. There are 13 active key bits involved in round $i+17$, which is $\kappa_2 = (K_0^{i+17} - K_3^{i+17}, K_5^{i+17}, K_7^{i+17} - K_{12}^{i+17}, K_{14}^{i+17}, K_{15}^{i+17})$, to obtain the x represented in Table 5.
Attack:

1. Guess each of 2^{13+13} $\kappa_1||\kappa_2$
   (a) Encrypt the plaintexts by one round and decrypt the ciphertexts by one round.
   (b) Do as the first three steps in the 21-round attack
2. The keys with counter values ranked in the largest $2^{32+26-8} = 2^{50}$ values would be the right subkey candidates. Exploiting the key schedule and guessing some other bits, use two plaintex-ciphertext pairs to check the right key.

Time: (1.a)$2^{26} \times N = 2^{57.19}$ two-round encryptions. (1.b) $2^{26} \times 2^{35.84} = 2^{61.84}$ additions. (2) Exhaustive phase needs about $2^{64-8} = 2^{56}$ 23-round encryptions.

4.3 Improved Key Recovery Attack on Other Variants of SIMON

The improved attack on SIMON32/64 is given above. The similar procedure can be applied to the other variants of SIMON using some linear hulls given in Table 3. See Appendix B for more details.

4.4 Multiple Linear Hull Attack on Simon

Combining multiple linear cryptanalysis [19] and linear hull together, one can make multiple linear hull attack with improved data complexity. Our attack technique can be used in the multiple linear hull attack of Simon well. According to the rotational property, Property 1, of Simon, lots of linear hulls with high potential can be found. For example, the two 13-round linear hulls for Simon32 in Table 3 are rotations of same linear hull.

Suppose that the time to compute the bias for one linear hull is $\mathcal{T}_1$ and data complexity is $\mathcal{N}$. If m linear hulls with same bias are used in the multiple linear hull attack, the data complexity would be decreased to $\mathcal{N}/m$. But the time complexity would increase to $m\mathcal{T}_1 + 2^{\mathcal{K}}$, where $\mathcal{K}$ is the size of the independent key bits involved in all m linear hull attacks. For example, there are 32 independent key bits involved in the 21-round attack of Simon32 with linear hull $X_{L,5}^{i} \rightarrow X_{R,13}^{i+13}$. The data complexity is $2^{31.19}$ known plaintext-ciphertext pairs and the time needs about $2^{35.84}$ additions to get the bias. When another linear hull $X_{L,6}^{i} \rightarrow X_{R,14}^{i+13}$ is taken in to make a multiple linear hull attack, the data size will decrease to $2^{30.19}$. There are also 32 independent key bits involved in this linear hull attack. But, the total independent key size of both linear hulls is 48. So the time to compute the bias for the multiple linear hull attack with above two linear hulls needs about $2^{36.84}$ additions and 2^{48} combinations.

5 Conclusion

In this paper, we gave improved linear attack on all versions of Simon family with dynamic key-guessing technique. By establishing the boolean function of parity bit in the linear hull distinguisher and reducing the function accroding the property of AND operation, we decrease the number of key bits involved in the attack and decrease the attack complexity in a further step. As a result, we can attack 23-round Simon32/64, 24-round Simon48/72, 25-round Simon48/96, 30-round Simon64/96, 31-round Simon64/128, 37-round Simon96/96, 38-round Simon96/144, 49-round Simon128/128, 51-round Simon128/192 and 53-round Simon128/256. The differential attack in [14] and our linear hull attack are bit-level cryptanalysis results, which propose more efficient and precise security estimation results on Simon. The cryptanalysis results imply that the security of Simon family does not shake.

References

1. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, Louid Wingers. The Simon and Speck Families of Lightweight Block Ciphers. 2013
2. Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. EUROCRYPT 1993, LNCS 765, pp. 386-397. Springer- Heidelberg, 1994
3. Mitsuru Matsui. The First Experimental Cryptanalysis of the Data Encryption Standard. CRYPTO 1994. LNCS 839, pp. 1-11. Springer- Heidelberg, 1994
4. Kaisa Nyberg. Linear Approximation of Block Ciphers. EUROCRYPT 1994, LNCS 950, pp. 439-444. Springer-Heidelberg, 1995
5. Ali Aydin Selçuk, Ali Biçak. On Probability of Success in Linear and Differential Cryptanalysis. SCN 2002. LNCS 2576, pp. 174-185. Springer- Heidelberg, 2003.
6. Mohamed Ahmed Abdelraheem, Javad Alizadeh, Hoda A. Alkhzaimi, Mohammad Resa Aref, Nasour Bagheri, Praveen Gauravaram, Martin M. Lauridsen. Improved Linear Cryptanalysis of Reduced-Round Simon. IACR Cryptology ePrint Archive 2014/681, 2014
7. Danping Shi, Lei Hu, Siwei Sun, Ling Song, Kexin Qiao, Xiaoshuang Ma. Improved Linear (Hull) Cryptanalysis of Round-reduced Versions of Simon. IACR Cryptology ePrint Archive 2014/973, 2014
8. Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel. Differential Cryptanalysis of Reduced-Round Simon. IACR Cryptology ePrint Archive, 2013/526, 2013.
9. Farzaneh Abed, Eik List, Jakob Wenzel, and Stefan Lucks. Differential Cryptanalysis of Reduced-Round Simon and SPECK. In FSE (2014)
10. Alex Biryukov, Arnab Roy, and Vesselin Velichkov. Differential analysis of block ciphers SIMON and SPECK. FSE 2014
11. Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, Ling Song. Automatic Security Evaluation and (Related-Key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers. ASIACRYPT 2014, LNCS 8873, pp. 158-178. Springer- Heidelberg, 2014

12. Siwei Sun, Lei Hu, Meiqin Wang, Peng Wang, Kexin Qiao, Xiaoshuang Ma, Danping Ma, Ling Song, Kai Fu. Towards Finding the Best Characteristics of Some Bit-oriented Block Ciphers and Automatic Enumeration of (Related-Key) Differential and Linear Characteristics with Predefined Properties and Its Applications. IACR Cryptology ePrint Archive 2014/747, 2014
13. Hoda A. Alkhzaimi, Martin M. Lauridsen. Cryptanalysis of the SIMON Family of Block Ciphers. IACR Cryptology ePrint Archive 2013, 543 (2013)
14. Ning Wang, Xiaoyun Wang, Keting Jia, Jingyuan Zhao. Differential Attacks on Reduced SIMON Versions with Dynamic Key-guessing Techniques. IACR Cryptology ePrint Archive 2014, 448 (2014)
15. Javad Alizadeh, Hoda A. Alkhzaimi, Mohammad Reza Aref, Nasour Begheri, Paraveen Gauravaram, Abhishek Kumar, Martin M. Lauridsen, and Somitra Kumar Sanadhya. Cryptanalysis of SIMON Variants with Connections. In RFIDsec'14, LNCS, 8651, pp.1-20. Springer- Heidelberg, 2014.
16. Qingju Wang, Zhiqiang Liu, Kerem Varıcı, Yu Sasaki, Vincent Rijmen, and Yosuke Todo. Cryptanalysis of Reudced-round SIMON32 and SIMON48. INDOCRYPT 2014.
17. Zhan Chen, Ning Wang, Xiaoyun Wang. Impossible Differential Cryptanalysis of Reduced Round SIMON. IACR Cryptology ePrint Archive 2015/286 (2015)
18. Boura, C., Naya-Plasencia, M., Suder, V. Scrutinzing and improving impossible differential attacks: Applications to Clefia, Camellia, Lblock and Simon. ASIACRYPT 2014. pp. 179-199. Springer- Heidelberg, 2014
19. Alex Biryukov, Christophe De Cannière, Michaël Quisquater. On Multiple Linear Approximations. CRYPTO 2004, LNCS 3152, pp. 1-22, Springer- Heidelberg, 2004
20. Tomer Asgur. Improved Linear Trails dor the Block Cipher SIMON. IACR Cryptology ePrint Archive 2015/285 (2015)

A Time complexity in some situations

In this section, we give the time complexities of computing the counters $B^k(y)$ for some simple functions of $y = f(x, k)$. This would be the deepest layer's operation in the linear attack to SIMON. Notice in the following, 'Guess' denotes the bits guessed at first. The second column $x_i \oplus k_i$ denotes the value of x_i which is used in the splitting phase. The third column denotes the new representation of the target function according to the value of $x_i \oplus k_i$. 'RB' is the related bit (defined in Section 3). T_1 denotes the time of seperation of the plaintexts according to the guessed bit of k. T_2 denotes the time of computation in the inner part. T_3 is the time in the combination phase. Total Time is the final time complexity, which is twice of the sum of all T_1, T_2 and T_3. Notice that T_1, T_2 and T_3 represent the number of addition operations. For simplicity, we denote $f*$ the function with same form of f. For example, if $f_1 = (x_0 \oplus k_0)\&(x_1 \oplus k_1)$ and $f_1' = (x_0 \oplus k_0)\&(x_3 \oplus k_3)$, we say f_1' is with form f_1*. The calculation of $B(y)$ for the functions with same form have same procedures and time complexties.

1. $f_1 = (x_0 \oplus k_0)\&(x_1 \oplus k_1)$

Guess	$x_0 \oplus k_0$	f_1	RB	T_1	T_2	T_3
k_0	0	0		1		2
	1	0	k_1	1		
Total Time				$2 \times (1 + 1 + 2) = 2^3$		

2. $f_2 = ((x_0 \oplus k_0) \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)))\&((x_3 \oplus k_3) \oplus ((x_1 \oplus k_1)\&(x_4 \oplus k_4)))$

Guess	$x_1 \oplus k_1$	f_2	RB	T_1	T_2	T_3
k_1	0	f_1*		$2^2 \times 3$	2^3	2^4
	1	f_1*		$2^2 \times 3$	2^3	
Total Time				$2 \times ((2^2 \times 3 + 2^3) \times 2 + 2^4) = 2^{6.46}$		

3. $f_3 = ((x_0 \oplus k_0)\&(x_1 \oplus k_1)) \oplus ((x_2 \oplus k_2) \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4)))\&((x_5 \oplus k_5) \oplus ((x_3 \oplus k_3)\&(x_6 \oplus k_6)))$

Guess	$x_0 \oplus k_0$	f_3	RB	T_1	T_2	T_3
k_0	0	f_2*		$2^5 \times 1$	$2^{6.46}$	2^6
	1	f_2*	k_1	$2^5 \times 1$	$2^{6.46}$	
Total Time				$2 \times ((2^5 \times 1 + 2^{6.46}) \times 2 + 2^6) = 2^{9.25}$		

4. $f_4 = (x_0 \oplus k_0) \oplus (x_1 \oplus k_1)\&(x_2 \oplus k_2)$

Guess	x_0	f_4	RB	T_1	T_2	T_3
		f_1*	k_0	$2^2 \times 1$	2^3	2^3
Total Time				$2^2 + 2^3 + 2^3 = 2^{4.32}$		

5. $f_5 = (x_0 \oplus k_0)\&((x_1 \oplus k_1) \oplus (x_2 \oplus k_2)\&(x_3 \oplus k_3))$

Guess	$x_0 \oplus k_0$	f_5	RB	T_1	T_2	T_3
k_0	0	0		$2^3 - 1$		2^3
	1	f_4*			$2^{4.32}$	
Total Time				$2 \times (2^3 - 1 + 2^{4.32} + 2^3) = 2^{5.64}$		

6. $f_6 = ((x_0 \oplus k_0)\&(x_1 \oplus k_1)) \oplus ((x_2 \oplus k_2) \oplus ((x_3 \oplus k_3)\&(x_1 \oplus k_1)))\&((x_4 \oplus k_4) \oplus ((x_3 \oplus k_3)\&(x_5 \oplus k_5)))$

Guess	$x_1 \oplus k_1$	f_6	RB	T_1	T_2	T_3
k_1	0	f_5*		$2^4 \times 1$	$2^{5.64}$	2^5
	1	f_5*	k_0	$2^4 \times 1$	$2^{5.64}$	
Total Time				$2 \times ((2^4 + 2^{5.64}) \times 2 + 2^5) = 2^{8.36}$		

7. $f_7 = [x_0 \oplus k_0 \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)) \oplus ((x_3 \oplus k_3 \oplus ((x_4 \oplus k_4)\&(x_5 \oplus k_5)))\&(x_6 \oplus k_6 \oplus ((x_5 \oplus k_5)\&(x_7 \oplus k_7))))]\&$ $[x_8 \oplus k_8 \oplus ((x_2 \oplus k_2)\&(x_9 \oplus k_9)) \oplus ((x_6 \oplus k_6 \oplus ((x_5 \oplus k_5)\&(x_7 \oplus k_7)))\&(x_{10} \oplus k_{10} \oplus ((x_7 \oplus k_7)\&(x_{11} \oplus k_{11}))))]$

Guess	$x_2 \oplus k_2, x_5 \oplus k_5, x_7 \oplus k_7$	f_7	RB	T_1	T_2	T_3
k_2, k_5, k_7	0,0,0	f_2*		$2^5 \times (2^4 - 1)$	$2^{6.46}$	$2^9 \times 7$
	0,0,1	f_2*		$2^5 \times (2^4 - 1)$	$2^{6.46}$	
	0,1,0	f_2*		$2^5 \times (2^4 - 1)$	$2^{6.46}$	
	0,1,1	f_2*		$2^5 \times (2^4 - 1)$	$2^{6.46}$	
	1,0,0	f_2*		$2^5 \times (2^4 - 1)$	$2^{6.46}$	
	1,0,1	f_2*		$2^5 \times (2^4 - 1)$	$2^{6.46}$	
	1,1,0	f_2*		$2^5 \times (2^4 - 1)$	$2^{6.46}$	
	1,1,1	f_2*		$2^5 \times (2^4 - 1)$	$2^{6.46}$	
Total Time				$2^3 \times ((2^5 \times (2^4 - 1) + 2^{6.46}) \times 8 + 2^9 \times 7) = 2^{15.99}$		

8. $f_8 = f_7 \oplus ((x_{12} \oplus k_{12} \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)))\&(x_{13} \oplus k_{13} \oplus ((x_2 \oplus k_2)\&(x_9 \oplus k_9))))$

Guess	$x_2 \oplus k_2, x_5 \oplus k_5, x_7 \oplus k_7$	f_8	RB	T_1	T_2	T_3
k_2, k_5, k_7	0,0,0	f_3*		$2^7 \times (2^4 - 1)$	$2^{9.25}$	$2^{11} \times 7$
	0,0,1	f_3*		$2^7 \times (2^4 - 1)$	$2^{9.25}$	
	0,1,0	f_3*		$2^7 \times (2^4 - 1)$	$2^{9.25}$	
	0,1,1	f_3*		$2^7 \times (2^4 - 1)$	$2^{9.25}$	
	1,0,0	f_3*		$2^7 \times (2^4 - 1)$	$2^{9.25}$	
	1,0,1	f_3*		$2^7 \times (2^4 - 1)$	$2^{9.25}$	
	1,1,0	f_3*		$2^7 \times (2^4 - 1)$	$2^{9.25}$	
	1,1,1	f_3*		$2^7 \times (2^4 - 1)$	$2^{9.25}$	
Total Time				$2^3 \times ((2^7 \times (2^4 - 1) + 2^{9.25}) \times 8 + 2^{11} \times 7) = 2^{18.08}$		

Case 1 gives the time complexity when $y = f(x,k) = (x_0 \oplus k_0)\&(x_1 \oplus k_1)$. We explain Case 2 in detail and the others are similar. f_2 is a function of 5-bit value x and k. Suppose $V[x]$ denotes the number of x. After k_1 is guessed, the representation of f_2 will be simplified for $x_1 = k_1$ and $x_1 = k_1 \oplus 1$. If $x_1 = k_1$, there is $f_2 = f_2^0 = (x_0 \oplus k_0)\&(x_3 \oplus k_3)$ which is with form f_1*. Initialize a new counter vector $V_0[x^0]$ where x^0 is of 2-bit. Set $V_0[x^0] = \sum_{x_0 = x_0^0, x_3 = x_1^0, x_1 = k_1} V[x]$. There are three additions for each x^0 and in total $T_1 = 2^2 \times 3$. If $x_1 = k_1 \oplus 1$, there is $f_2 = f_2^1 = (x_{0,2} \oplus k_{0,2})\&(x_{3,4} \oplus k_{3,4})$ which is also with form f_1*. Similarly, initialize a new counter vector $V_1[x^1]$ where x^1 is of 2-bit. Set $V_1[x^1] = \sum_{x_{0,2} = x_0^1, x_{3,4} = x_1^1, x_1 = k_1 \oplus 1} V[x]$. There are three additions for each x^1 and in total $T_1 = 2^2 \times 3$. The function in the inner part is with form f_1* for both situations and it is easy to know $T_2 = 2^3$ according to Case 1. Let $B_0^{k_0,k_3}(y)$ be the $B(y)$ with counter vector V_0 and function f_2^0 for k_0, k_3. Let $B_1^{k_{0,2},k_{3,4}}(y)$ be the $B(y)$ with counter vector V_1 and function f_2^1 for $k_{0,2}, k_{3,4}$. When k_1 is fixed, $B(y)$ for k is $B_0^{k_0,k_3}(y) + B_1^{k_{0,2},k_{3,4}}(y)$. Since there are 4 independent bits of

k when k_1 is fixed, leading to $T_3 = 2^4$, which is the complexity of combination. In total, the time is twice of $(2^2 + 2^3) + 2^4$, since there are two possible guesses for k_1.

The related bit (RB) is generated in linear compression. For example in Case 3, when $x_0 \oplus k_0 = 1$, f_3 is linear with $x_1 \oplus k_1$. As explained in Section 3, x_1 is compressed and k_1 becomes a related bit. In Case 4, linear compression is done before any key guess, leading to the compression of bit x_0 and generation of related bit k_0.

B Improved Linear Attacks on SIMON48, SIMON64, SIMON96, SIMON128

B.1 Linear Attack on SIMON48/K

The linear hull we used to attack SIMON48/K is

$$X^i_{L,1} \oplus X^i_{L,5} \oplus X^i_{L,21} \oplus X^i_{R,23} \rightarrow X^{i+16}_{L,1} \oplus X^{i+16}_{L,5} \oplus X^{i+16}_{R,23}$$

which is proposed in [12], with potential $\bar{\epsilon}^2 = 2^{-44.92}$.

Table 9. 3 rounds before $X^i_{L,1} \oplus X^i_{L,5} \oplus X^i_{L,21} \oplus X^i_{R,23}$ for SIMON48

x_0	$X^{i-3}_{L,15} \oplus X^{i-3}_{R,17} \oplus (X^{i-3}_{L,16} \& X^{i-3}_{L,9}) \oplus X^{i-3}_{R,5} \oplus (X^{i-3}_{L,4} \& X^{i-3}_{L,21}) \oplus X^{i-3}_{R,21} \oplus (X^{i-3}_{L,20} \& X^{i-3}_{L,13})$	k_0	$K^{i-2}_3 \oplus K^{i-3}_{17} \oplus K^{i-2}_{19} \oplus K^{i-1}_1 \oplus K^{i-3}_5 \oplus K^{i-3}_{21} \oplus K^{i-1}_5 \oplus K^{i-1}_{21}$
x_1	$X^{i-3}_{L,0} \oplus X^{i-3}_{R,2} \oplus (X^{i-3}_{L,1} \& X^{i-3}_{L,18})$	k_1	K^{i-3}_2
x_2	$X^{i-3}_{L,17} \oplus X^{i-3}_{R,19} \oplus (X^{i-3}_{L,18} \& X^{i-3}_{L,11})$	k_2	K^{i-3}_{19}
x_3	$X^{i-3}_{L,16} \oplus X^{i-3}_{R,18} \oplus (X^{i-3}_{L,17} \& X^{i-3}_{L,10})$	k_3	K^{i-3}_{18}
x_4	$X^{i-3}_{L,9} \oplus X^{i-3}_{R,11} \oplus (X^{i-3}_{L,10} \& X^{i-3}_{L,3})$	k_4	K^{i-3}_{11}
x_5	$X^{i-3}_{L,20} \oplus X^{i-3}_{R,22} \oplus (X^{i-3}_{L,21} \& X^{i-3}_{L,14}) \oplus X^{i-3}_{L,0}$	k_5	$K^{i-3}_{22} \oplus K^{i-2}_0$
x_6	$X^{i-3}_{L,21} \oplus X^{i-3}_{R,23} \oplus (X^{i-3}_{L,22} \& X^{i-3}_{L,15})$	k_6	K^{i-3}_{23}
x_7	$X^{i-3}_{L,14} \oplus X^{i-3}_{R,16} \oplus (X^{i-3}_{L,15} \& X^{i-3}_{L,8})$	k_7	K^{i-3}_{16}
x_8	$X^{i-3}_{L,13} \oplus X^{i-3}_{R,15} \oplus (X^{i-3}_{L,14} \& X^{i-3}_{L,7}) \oplus X^{i-3}_{L,17}$	k_8	$K^{i-3}_{15} \oplus K^{i-2}_{17}$
x_9	$X^{i-3}_{L,7} \oplus X^{i-3}_{R,9} \oplus (X^{i-3}_{L,8} \& X^{i-3}_{L,1})$	k_9	K^{i-3}_9
x_{10}	$X^{i-3}_{L,0} \oplus X^{i-3}_{R,2} \oplus (X^{i-3}_{L,1} \& X^{i-3}_{L,18}) \oplus X^{i-3}_{L,4}$	k_{10}	$K^{i-3}_2 \oplus K^{i-2}_4$
x_{11}	$X^{i-3}_{L,1} \oplus X^{i-3}_{R,3} \oplus (X^{i-3}_{L,2} \& X^{i-3}_{L,19})$	k_{11}	K^{i-3}_3
x_{12}	$X^{i-3}_{L,18} \oplus X^{i-3}_{R,20} \oplus (X^{i-3}_{L,19} \& X^{i-3}_{L,12})$	k_{12}	K^{i-3}_{20}
x_{13}	$X^{i-3}_{L,17} \oplus X^{i-3}_{R,19} \oplus (X^{i-3}_{L,18} \& X^{i-3}_{L,11}) \oplus X^{i-3}_{L,21}$	k_{13}	$K^{i-3}_{19} \oplus K^{i-2}_{21}$
x_{14}	$X^{i-3}_{L,11} \oplus X^{i-3}_{R,13} \oplus (X^{i-3}_{L,12} \& X^{i-3}_{L,5})$	k_{14}	K^{i-3}_{13}
x_{15}	$X^{i-3}_{L,16} \oplus X^{i-3}_{R,18} \oplus (X^{i-3}_{L,17} \& X^{i-3}_{L,10}) \oplus X^{i-3}_{L,20}$	k_{15}	$K^{i-3}_{18} \oplus K^{i-2}_{20}$
x_{16}	$X^{i-3}_{L,10} \oplus X^{i-3}_{R,12} \oplus (X^{i-3}_{L,11} \& X^{i-3}_{L,4})$	k_{16}	K^{i-3}_{12}
x_{17}	$X^{i-3}_{L,9} \oplus X^{i-3}_{R,11} \oplus (X^{i-3}_{L,10} \& X^{i-3}_{L,3}) \oplus X^{i-3}_{L,13}$	k_{17}	$K^{i-3}_{11} \oplus K^{i-2}_{13}$
x_{18}	$X^{i-3}_{L,3} \oplus X^{i-3}_{R,5} \oplus (X^{i-3}_{L,4} \& X^{i-3}_{L,21})$	k_{18}	K^{i-3}_5

Similar to the attack on SIMON32, at first we give the procedure to compress the plaintexts, then the procedure to compress the ciphertexts. Add 3 rounds before the distinguisher. According to the representations for x, k in Table 9, $X^i_{L,1} \oplus X^i_{L,5} \oplus X^i_{L,21} \oplus X^i_{R,23}$ can be represented as

$$\begin{aligned}
&x_0 \oplus k_0 \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)) \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4)) \oplus \\
&((x_5 \oplus k_5 \oplus ((x_6 \oplus k_6)\&(x_7 \oplus k_7)))\&(x_8 \oplus k_8 \oplus ((x_7 \oplus k_7)\&(x_9 \oplus k_9)))) \oplus \\
&((x_{10} \oplus k_{10} \oplus ((x_{11} \oplus k_{11})\&(x_{12} \oplus k_{12})))\&(x_{13} \oplus k_{13} \oplus ((x_{12} \oplus k_{12})\&(x_{14} \oplus k_{14})))) \oplus \\
&((x_{15} \oplus k_{15} \oplus ((x_2 \oplus k_2)\&(x_{16} \oplus k_{16})))\&(x_{17} \oplus k_{17} \oplus ((x_{16} \oplus k_{16})\&(x_{18} \oplus k_{18}))))
\end{aligned}$$

Compress the plaintexts: (Procedure SIMON48-Head) At first compress the data samples into a counter vertor $V[x_1 - x_{18}]$, then DO

1. For each $x_3 - x_{14}$

(a) Guess the keys related to $x_1 - x_2, x_{15} - x_{18}$ and compress $x_1 - x_2, x_{15} - x_{18}$ as the Case f_6 in Appendix A. There are 6-bit keys $(k_1 - k_2, k_{15} - k_{18})$ to store, and the time is about $2^{8.36}$. So here the memory is about $2^6 \times 2^{12}$ counters, and the total time is about $2^{12} \times 2^{8.36} = 2^{20.36}$.

2. For each key $k_1 - k_2, k_{15} - k_{18}$

   (a) For each $x_{10} - x_{14}$

      i. Guess the keys related to $x_3 - x_9$ and compress $x_3 - x_9$ as Case f_3 in Appendix A. There are 7-bit keys $(k_3 - k_9)$ to store, and the time is about $2^{9.25}$. So here the memory is about $2^{6+7} \times 2^5$ counters, and the total time is about $2^{6+5} \times 2^{9.25} = 2^{20.25}$.

3. For each key $k_1 - k_9, k_{15} - k_{18}$

   (a) Guess the keys related to $x_{10} - x_{14}$ and compress $x_{10} - x_{14}$ as Case f_2 in Appendix A. There are 5-bit keys $(k_{10} - k_{14})$ to store, and the time is about $2^{6.46}$. So here the memory is about 2^{13+5} counters, and the total time is about $2^{13} \times 2^{6.46} = 2^{19.46}$.

4. Total time is $2^{20.36} + 2^{20.25} + 2^{19.46} = 2^{21.66}$ additions. Memory is about $O(2^{18})$.

Table 10. 4 rounds after $X^{i+16}_{L,1} \oplus X^{i+16}_{L,5} \oplus X^{i+16}_{R,23}$ for SIMON48

x_0	$X^{i+20}_{R,3} \oplus X^{i+20}_{L,5} \oplus (X^{i+20}_{R,4} \& X^{i+20}_{R,21}) \oplus X^{i+20}_{R,3} \oplus X^{i+20}_{R,15} \oplus X^{i+20}_{L,17}$ $\oplus (X^{i+20}_{R,16} \& X^{i+20}_{R,9}) \oplus X^{i+20}_{L,21} \oplus (X^{i+20}_{R,20} \& X^{i+20}_{R,13})$	k_0	$K^{i+19}_{1} \oplus K^{i+17}_{1} \oplus K^{i+16}_{23}$ $K^{i+19}_{1} \oplus K^{i+19}_{5} \oplus K^{i+18}_{3} \oplus K^{i+17}_{5}$ $K^{i+19}_{17} \oplus K^{i+19}_{21} \oplus K^{i+18}_{19} \oplus K^{i+17}_{21}$
x_1	$X^{i+20}_{R,16} \oplus X^{i+20}_{L,18} \oplus (X^{i+20}_{R,17} \& X^{i+20}_{R,10})$	k_1	K^{i+19}_{18}
x_2	$X^{i+20}_{R,9} \oplus X^{i+20}_{L,11} \oplus (X^{i+20}_{R,10} \& X^{i+20}_{R,3})$	k_2	K^{i+19}_{11}
x_3	$X^{i+20}_{R,0} \oplus X^{i+20}_{L,2} \oplus (X^{i+20}_{R,1} \& X^{i+20}_{R,18})$	k_3	K^{i+19}_{2}
x_4	$X^{i+20}_{R,17} \oplus X^{i+20}_{L,19} \oplus (X^{i+20}_{R,18} \& X^{i+20}_{R,11})$	k_4	K^{i+19}_{19}
x_5	$X^{i+20}_{R,20} \oplus X^{i+20}_{L,22} \oplus (X^{i+20}_{R,21} \& X^{i+20}_{R,14}) \oplus X^{i+20}_{R,0}$	k_5	$K^{i+19}_{22} \oplus K^{i+18}_{0}$
x_6	$X^{i+20}_{R,21} \oplus X^{i+20}_{L,23} \oplus (X^{i+20}_{R,22} \& X^{i+20}_{R,15})$	k_6	K^{i+19}_{23}
x_7	$X^{i+20}_{R,14} \oplus X^{i+20}_{L,16} \oplus (X^{i+20}_{R,15} \& X^{i+20}_{R,8})$	k_7	K^{i+19}_{16}
x_8	$X^{i+20}_{R,13} \oplus X^{i+20}_{L,15} \oplus (X^{i+20}_{R,14} \& X^{i+20}_{R,7}) \oplus X^{i+20}_{R,17}$	k_8	$K^{i+19}_{15} \oplus K^{i+18}_{17}$
x_9	$X^{i+20}_{R,7} \oplus X^{i+20}_{L,9} \oplus (X^{i+20}_{R,8} \& X^{i+20}_{R,1})$	k_9	K^{i+19}_{9}
x_{10}	$X^{i+20}_{R,0} \oplus X^{i+20}_{L,2} \oplus (X^{i+20}_{R,1} \& X^{i+20}_{R,18}) \oplus X^{i+20}_{R,4}$	k_{10}	$K^{i+19}_{2} \oplus K^{i+18}_{4}$
x_{11}	$X^{i+20}_{R,1} \oplus X^{i+20}_{L,3} \oplus (X^{i+20}_{R,2} \& X^{i+20}_{R,19})$	k_{11}	K^{i+19}_{3}
x_{12}	$X^{i+20}_{R,18} \oplus X^{i+20}_{L,20} \oplus (X^{i+20}_{R,19} \& X^{i+20}_{R,12})$	k_{12}	K^{i+19}_{20}
x_{13}	$X^{i+20}_{R,11} \oplus X^{i+20}_{L,13} \oplus (X^{i+20}_{R,12} \& X^{i+20}_{R,5}) \oplus X^{i+20}_{R,21}$	k_{13}	$K^{i+19}_{19} \oplus K^{i+18}_{21}$
x_{14}	$X^{i+20}_{R,11} \oplus X^{i+20}_{L,13} \oplus (X^{i+20}_{R,12} \& X^{i+20}_{R,5})$	k_{14}	K^{i+19}_{13}
x_{15}	$X^{i+20}_{R,16} \oplus X^{i+20}_{L,18} \oplus (X^{i+20}_{R,17} \& X^{i+20}_{R,10}) \oplus X^{i+20}_{R,20}$	k_{15}	$K^{i+19}_{18} \oplus K^{i+18}_{20}$
x_{16}	$X^{i+20}_{R,10} \oplus X^{i+20}_{L,12} \oplus (X^{i+20}_{R,11} \& X^{i+20}_{R,4})$	k_{16}	K^{i+19}_{12}
x_{17}	$X^{i+20}_{R,9} \oplus X^{i+20}_{L,11} \oplus (X^{i+20}_{R,10} \& X^{i+20}_{R,3}) \oplus X^{i+20}_{R,13}$	k_{17}	$K^{i+19}_{11} \oplus K^{i+18}_{13}$
x_{18}	$X^{i+20}_{R,3} \oplus X^{i+20}_{L,5} \oplus (X^{i+20}_{R,4} \& X^{i+20}_{R,21})$	k_{18}	K^{i+19}_{5}
x_{19}	$X^{i+20}_{R,16} \oplus X^{i+20}_{L,18} \oplus (X^{i+20}_{R,17} \& X^{i+20}_{R,10}) \oplus X^{i+20}_{L,22} \oplus (X^{i+20}_{R,21} \& X^{i+20}_{R,14})$	k_{19}	$K^{i+19}_{18} \oplus K^{i+18}_{20} \oplus K^{i+19}_{22} \oplus K^{i+17}_{22}$
x_{20}	$X^{i+20}_{R,10} \oplus X^{i+20}_{L,12} \oplus (X^{i+20}_{R,11} \& X^{i+20}_{R,4}) \oplus X^{i+20}_{R,14}$	k_{20}	$K^{i+19}_{12} \oplus K^{i+18}_{14}$
x_{21}	$X^{i+20}_{R,9} \oplus X^{i+20}_{L,11} \oplus (X^{i+20}_{R,10} \& X^{i+20}_{R,3}) \oplus X^{i+20}_{L,15} \oplus (X^{i+20}_{R,14} \& X^{i+20}_{R,7})$	k_{21}	$K^{i+19}_{11} \oplus K^{i+18}_{13} \oplus K^{i+19}_{15} \oplus K^{i+17}_{15}$
x_{22}	$X^{i+20}_{R,4} \oplus X^{i+20}_{L,6} \oplus (X^{i+20}_{R,5} \& X^{i+20}_{R,22})$	k_{22}	K^{i+19}_{6}
x_{23}	$X^{i+20}_{R,3} \oplus X^{i+20}_{L,5} \oplus (X^{i+20}_{R,4} \& X^{i+20}_{R,21}) \oplus X^{i+20}_{R,7}$	k_{23}	$K^{i+19}_{5} \oplus K^{i+18}_{7}$

If we append four rounds at the end of the linear distinguisher, according to Table 10, $X_{L,1}^{i+16} \oplus X_{L,5}^{i+16} \oplus X_{R,23}^{i+16}$ can be represented as

$$
\begin{aligned}
& x_0 \oplus k_0 \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)) \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4))\oplus \\
& ((x_5 \oplus k_5 \oplus ((x_6 \oplus k_6)\&(x_7 \oplus k_7)))\&(x_8 \oplus k_8 \oplus ((x_7 \oplus k_7)\&(x_9 \oplus k_9)))\oplus \\
& ((x_{10} \oplus k_{10} \oplus ((x_{11} \oplus k_{11})\&(x_{12} \oplus k_{12})))\&(x_{13} \oplus k_{13} \oplus ((x_{12} \oplus k_{12})\&(x_{14} \oplus k_{14})))\oplus \\
& ((x_{15} \oplus k_{15} \oplus ((x_4 \oplus k_4)\&(x_{16} \oplus k_{16})))\&(x_{17} \oplus k_{17} \oplus ((x_{16} \oplus k_{16})\&(x_{18} \oplus k_{18})))\oplus \\
& \{(x_{19} \oplus k_{19} \oplus ((x_4 \oplus k_4)\&(x_{16} \oplus k_{16}))\oplus \\
& ((x_{13} \oplus k_{13} \oplus ((x_{12} \oplus k_{12})\&(x_{14} \oplus k_{14})))\&(x_{20} \oplus k_{20} \oplus ((x_{14} \oplus k_{14})\&(x_{22} \oplus k_{22})))))) \\
& \& \\
& (x_{21} \oplus k_{21} \oplus ((x_{16} \oplus k_{16})\&(x_{18} \oplus k_{18}))\oplus \\
& ((x_{20} \oplus k_{20} \oplus ((x_{14} \oplus k_{14})\&(x_{22} \oplus k_{22})))\&(x_{23} \oplus k_{23} \oplus ((x_{22} \oplus k_{22})\&(x_6 \oplus k_6))))))\}
\end{aligned}
$$

Compress the ciphertexts: (Procedure SIMON48-Tail) To simplify our description, we introduce the situations that the XOR for the guessed k bit and corresponding x bit is zero in Step 2 to Step 8, since the representation of the target parity bit in another situation has same form with it. At first compress the data samples into a counter vertor $V[x_1 - x_{23}]$, then DO

1. For each of $x_3 - x_{23}$
   (a) Compress $x_1 - x2$ as Case f_1 in Appendix A. There is 2-bit key $(k_1 - k_2)$ to store and the time is 2^3. So this step needs memory 2^{23} counters and total time is about $2^{21} \times 2^3 = 2^{24}$.
2. Guess k_4. Since $x_4 \oplus k_4 = 0$, x_3 can be compressed. The time is about 2^{19} additions.
3. Guess k_7. Since $x_7 \oplus k_7 = 0$, x_9 can be compressed. The time is about 2^{17} additions.
4. Guess k_5. Since $x_5 \oplus k_5 = 0$, x_8 can be compressed. The time is about 2^{15} additions.
5. Guess k_{12}. Since $x_{12} \oplus k_{12} = 0$, x_{11} can be compressed. The time is about 2^{13} additions.
6. Guess k_{22}. Since $x_{22} \oplus k_{22} = 0$, x_{14}, x_6 can be compressed. The time is about $2^{10} \times 3$ additions.
7. Guess k_{16}. Since $x_{16} \oplus k_{16} = 0$, x_{18} can be compressed. The time is about 2^8 additions.
8. Guess k_{15}. Since $x_{15} \oplus k_{15} = 0$, x_{17} can be compressed. The time is about 2^6 additions.
9. After above guessing and split, remained bits for x and k are bit 10, 13, 19, 20, 21, 23. We can compress them as Case f_6 in Appendix A. The time is $2^{8.36}$.
10. Calculate the other situations similar to that above.

Time is estimated from the inner part to outer part. Step 9 needs about $T_9 = 2^{8.36}$ additions. In Step 8, the two cases, $x_{15} \oplus k_{15} = 0$, $x_{15} \oplus k_{15} = 1$ have same time complexity and there are two possible guesses for k_{15}. So the total time for Step 8 and 9 is $T_8 = 2 \times ((2^6 + T_9) \times 2 + 2^7) = 2^{10.83}$, where 2^7 is the time for combination. Similarly, the time for Step 2 to Step 9 is as follows.

Step	Time
8-9	$T_8 = 2 \times ((2^6 + T_9) \times 2 + 2^7) = 2^{10.83}$
7-9	$T_7 = 2 \times ((2^8 + T_8) \times 2 + 2^9) = 2^{13.19}$
6-9	$T_6 = 2 \times ((2^{10} \times 3 + T_7) \times 2 + 2^{12}) = 2^{15.82}$
5-9	$T_5 = 2 \times ((2^{13} + T_6) \times 2 + 2^{14}) = 2^{18.18}$
4-9	$T_4 = 2 \times ((2^{15} + T_5) \times 2 + 2^{16}) = 2^{20.47}$
3-9	$T_3 = 2 \times ((2^{17} + T_4) \times 2 + 2^{18}) = 2^{22.71}$
2-9	$T_2 = 2 \times ((2^{19} \times 3 + T_3) \times 2 + 2^{20}) = 2^{24.91}$

So in total, the time is $2^{24.91} \times 2^2 + 2^{24} \approx 2^{27.09}$. The memory is about $\mathcal{O}(2^{23})$ counters.

23-round attack on SIMON48/72. We add three rounds before and four rounds after the 16-round linear distinguisher to attack 23-round SIMON48/K. Suppose we use $N = 8\bar{\epsilon}^{-2} = 2^{47.92}$ known plaintext-ciphertext pairs. Set advantage $a = 16$. The success probability would be 0.909. At first, compress the N plaintext-ciphertext pairs to 2^{18+23} counters according to Table 9, 10. Suppose the plaintext be compressed to x_P and ciphertext be compressed to x_C.

1. For each of 2^{23} x_C

(a) Call Procedure SIMON48-Head, and store the counters according to the keys used in the forward rounds
2. For each of 2^{18} keys involved in the forward rounds
   (a) Call Procedure SIMON48-Tail, and store the counters according to the keys used in the backward rounds
3. Rank the keys and exhaustive the candidates with the help of key schedule

Time: 1. $2^{23} \times 2^{21.66} = 2^{44.66}$ additions; 2. $2^{18} \times 2^{27.09} = 2^{45.09}$ additions. So it needs $2^{44.66} + 2^{45.09} = 2^{45.89}$ additions to get the correlations. 3. Since the size of master key is 72, the exhaustive phase needs $2^{72-16} = 2^{56}$ 23-round encryptions.

24-round attack on SIMON48/72. Expand one more round before X^{i-3}. The key bits of K^{i-4} involved to obtain the x represented in Table 9 are $\kappa_1 = (K_0^{i-4} - K_5^{i-4}, K_7^{i-4} - K_{22}^{i-4})$, in total 22 bits.

1. Guess each of 2^{22} κ_1
   (a) Encrypt the N plaintexts by one round
   (b) Do as first two steps of the 23-round attack
2. Rank the keys and exhaustive the candidates with the help of key schedule

Time: (1.a) $2^{22} \times N = 2^{69.92}$ one-round encryptions. (1.b) $2^{22} \times 2^{45.89} = 2^{67.89}$ additons. 2. Since the size of master key is 72, the exhaustive phase needs $2^{72-16} = 2^{56}$ 24-round encryptions.

25-round attack on SIMON48/96. Expand one more round before X^{i-3} and one more round after X^{i+20}. The key bits of K^{i+20} involved to obtain the x represented in Table 10 are $\kappa_2 = (K_0^{i+20} - K_5^{i+20}, K_7^{i+20} - K_{22}^{i+18})$, in total 22 bits.

1. Guess each of 2^{44} $\kappa_1 || \kappa_2$
   (a) Encrypt the N plaintexts by one round
   (b) Do as first two steps of the 23-round attack
2. Rank the keys and exhaustive the candidates with the help of key schedule

Time: (1.a) $2^{44} \times N = 2^{91.92}$ two-round encryptions. (1.b) $2^{44} \times 2^{45.89} = 2^{89.89}$ additons. 2. The exhaustive phase needs $2^{96-16} = 2^{80}$ 25-round encryptions.

B.2 Linear Attack on SIMON64/*K*

The linear hull we used to attack SIMON64/K is

$$X_{L,20}^i \oplus X_{L,24}^i \oplus X_{R,22}^i \to X_{L,22}^{i+21} \oplus X_{R,20}^{i+21} \oplus X_{R,24}^{i+21}$$

which is proposed in [6], with potential $\bar{\epsilon}^2 = 2^{-62.53}$.

If we add four rounds before the linear hull, accodring to Table 11, $X_{L,20}^i \oplus X_{L,24}^i \oplus X_{R,22}^i$ can be represented as

$$\begin{aligned}
&x_0 \oplus k_0 \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)) \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4)) \oplus ((x_5 \oplus k_5)\&(\underline{x_6 \oplus k_6}))\oplus\\
&((x_7 \oplus k_7 \oplus ((x_6 \oplus k_6)\&(x_8 \oplus k_8)))\&(x_9 \oplus k_9 \oplus ((x_8 \oplus k_8)\&(x_{10} \oplus k_{10})))\oplus\\
&\{(x_{11} \oplus k_{11} \oplus ((x_6 \oplus k_6)\&(x_8 \oplus k_8))\oplus\\
&((x_{12} \oplus k_{12} \oplus ((x_{13} \oplus k_{13})\&(x_{14} \oplus k_{14})))\&(x_{15} \oplus k_{15} \oplus ((x_{13} \oplus k_{13})\&(x_{16} \oplus k_{16}))))\\
&\&\\
&(x_{17} \oplus k_{17} \oplus ((x_8 \oplus k_8)\&(x_{10} \oplus k_{10}))\oplus\\
&((x_{15} \oplus k_{15} \oplus ((x_{13} \oplus k_{13})\&(x_{16} \oplus k_{16})))\&(x_{18} \oplus k_{18} \oplus ((x_{16} \oplus k_{16})\&(x_{19} \oplus k_{19}))))\}\oplus\\
&\{(x_{20} \oplus k_{20} \oplus ((x_{21} \oplus k_{21})\&(x_{22} \oplus k_{22}))\oplus\\
&((x_{23} \oplus k_{23} \oplus ((x_{24} \oplus k_{24})\&(x_{25} \oplus k_{25})))\&(x_{26} \oplus k_{26} \oplus ((x_{25} \oplus k_{25})\&(x_{27} \oplus k_{27}))))\\
&\&\\
&(x_{28} \oplus k_{28} \oplus ((x_{22} \oplus k_{22})\&(x_{29} \oplus k_{29}))\oplus\\
&((x_{26} \oplus k_{26} \oplus ((x_{25} \oplus k_{25})\&(x_{27} \oplus k_{27})))\&(x_{30} \oplus k_{30} \oplus ((x_{27} \oplus k_{27})\&(x_{31} \oplus k_{31}))))\}.
\end{aligned}$$

Since $x_{11} = x_1 \oplus x_7$ and $x_{17} = x_2 \oplus x_9$, there are 30 independent bits for x and 32 independent bits for k.

Compress the plaintexts: (Procedure SIMON64-Head) At first, compress the plaintexts into a counter vector $V[x_1 - x_{31}]$ using the linear compression technique. There are 2^{29} elements for V. To simplify our description of attack, the x_6, k_6 with underline above are regarded as new variables x_6', k_6'.

1. For each $x_3 - x_{31}$
   (a) Compress x_1, x_2. Since $x_1 = x_7 \oplus x_{11}, x_2 = x_9 \oplus x_{17}$, there is only one value for x_1, x_2. There is 2-bit key to store (k_1, k_2), and the time is 2^2. So here the memory is about $2^{29} \times 2^2 = 2^{31}$ counters and total time is $2^{29} \times 2^2 = 2^{31}$.
2. For each $k_1, k_2, x_5 - x_{31}$
   (a) Compress x_3, x_4 as the Case f_1 in Appendix A. There is 2-bit key to store (k_3, k_4), and the time is 2^3. So here the memory is about $2^{29} \times 2^2 = 2^{31}$ counters and total time is $2^{29} \times 2^3 = 2^{32}$.
3. For each $k_1 - k_4, x_6 - x_{31}$
   (a) Compress x_5, x_6'. Since $x_6' = x_6$, there is only two values for x_5, x_6'. There is 1-bit key to store (k_5) since $k_6' = k_6$ becomes a related bit, which will be determined in the following steps. The time is 2^3. So here the memory is about $2^{30} \times 2^1 = 2^{31}$ counters and total time is $2^{30} \times 2^3 = 2^{33}$.
4. For each $k_1 - k_5, x_{20} - x_{31}$
   (a) Compress $x_6 - x_{19}$ as Case f_8 in Appendix A. There is 14-bit key to store $(k_6 - k_{19})$and the time is $2^{18.08}$. So here the memory is about $2^{17} \times 2^{14} = 2^{31}$ counters and total time is $2^{17} \times 2^{18.08} = 2^{35.08}$.
5. For each $k_1 - k_{19}$
   (a) Compress $x_{20} - x_{31}$ as Case f_7 in Appendix A. There is 12-bit key to store $(k_{20} - k_{31})$and the time is $2^{15.99}$. So here the memory is about $2^{19} \times 2^{12} = 2^{31}$ counters and total time is $2^{19} \times 2^{15.99} = 2^{34.99}$.
6. The total time is about $2^{36.31}$ additions and memory is $\mathcal{O}(2^{31})$.

Compress the ciphertexts: (Procedure SIMON64-Tail) Add four rounds after the distinguisher, the representation of $X_{R,20}^{i+21} \oplus X_{R,24}^{i+21} \oplus X_{L,22}^{i+21}$ is same as that of $X_{L,20}^{i} \oplus X_{L,24}^{i} \oplus X_{R,22}^{i}$, except that the new representations for x and k are shown in Table 12. Compress the ciphertexts to a counter vector $V[x_1 - x_{31}]$ at first. Then do as the compressing procedure SIMON64-Head.

29-round attack on SIMON64/96. We add four rounds before and after the 21-round linear distinguisher to attack 29-round SIMON64/96. Suppose we use $N = 2\bar{\epsilon}^{-2} = 2^{63.53}$ known plaintext-ciphertext pairs. Set advantage $a = 8$. The success probability would be 0.477. At first, compress the N plaintext-ciphertext pairs to 2^{29+29} counters according to Table 11 and 12. Suppose the plaintext be compressed to x_P and ciphertext be compressed to x_C.

1. For each of 2^{29} x_C
   (a) Call Procedure SIMON64-Head, and store the counters according to the keys used in the first four rounds
2. For each of 2^{31} keys involved in the first four rounds
   (a) Call Procedure SIMON64-Tail, and store the counters according to the keys used in the last four rounds
3. Rank the keys and exhaustive the candidates with the help of key schedule

Time: 1. $2^{29} \times 2^{36.31} = 2^{65.31}$ additions; 2. $2^{31} \times 2^{36.31} = 2^{67.31}$ additions. So it needs $2^{65.31} + 2^{67.31} = 2^{67.62}$ additions to get the bias for the subkeys. 3. The exhaustive phase needs $2^{96-8} = 2^{88}$ 29-round encryptions.

30-round attack on SIMON64/96. Expand one more round before X^{i-4}. The key bits of K^{i-5} involved to obtain the x represented in Table 11 are $\kappa_1 = (K_0^{i-5} - K_2^{i-5}, K_4^{i-5} - K_{22}^{i-5}, K_{24}^{i-5}, K_{26}^{i-5}, K_{30}^{i-5}, K_{31}^{i-5})$, in total 26 bits.

1. Guess each of 2^{26} κ_1
   (a) Encrypt the N plaintexts by one round. Compress the internal states to a counter vectr of size 2^{58}.
   (b) Do as first two steps of the 29-round attack
2. Rank the keys and exhaustive the candidates with the help of key schedule

Table 11. 4 rounds before $X^i_{L,20} \oplus X^i_{L,24} \oplus X^i_{R,22}$ for Simon64

x_0	$X^{i-4}_{L,20} \oplus X^{i-4}_{L,16} \oplus X^{i-4}_{L,12} \oplus (X^{i-4}_{L,13} \& X^{i-4}_{L,6}) \oplus X^{i-4}_{R,14} \oplus$ $X^{i-4}_{L,24} \oplus X^{i-4}_{L,20} \oplus (X^{i-4}_{L,21} \& X^{i-4}_{L,14}) \oplus X^{i-4}_{R,22}$	k_0	$K^{i-3}_{20} \oplus K^{i-3}_{16} \oplus K^{i-2}_{18} \oplus K^{i-1}_{20} \oplus$ $K^{i-3}_{24} \oplus K^{i-1}_{24} \oplus K^{i-4}_{14} \oplus K^{i-4}_{22}$
x_1	$X^{i-4}_{L,17} \oplus (X^{i-4}_{L,18} \& X^{i-4}_{L,11}) \oplus X^{i-4}_{R,19}$	k_1	K^{i-4}_{19}
x_2	$X^{i-4}_{L,10} \oplus (X^{i-4}_{L,11} \& X^{i-4}_{L,4}) \oplus X^{i-4}_{R,12}$	k_2	K^{i-4}_{12}
x_3	$X^{i-4}_{L,13} \oplus (X^{i-4}_{L,14} \& X^{i-4}_{L,7}) \oplus X^{i-4}_{R,15}$	k_3	K^{i-4}_{15}
x_4	$X^{i-4}_{L,6} \oplus (X^{i-4}_{L,7} \& X^{i-4}_{L,0}) \oplus X^{i-4}_{R,8}$	k_4	K^{i-4}_{8}
x_5	$X^{i-4}_{L,21} \oplus (X^{i-4}_{L,22} \& X^{i-4}_{L,15}) \oplus X^{i-4}_{R,23}$	k_5	K^{i-4}_{23}
x_6	$X^{i-4}_{L,14} \oplus (X^{i-4}_{L,15} \& X^{i-4}_{L,8}) \oplus X^{i-4}_{R,16}$	k_6	K^{i-4}_{16}
x_7	$X^{i-4}_{L,17} \oplus X^{i-4}_{L,13} \oplus (X^{i-4}_{L,14} \& X^{i-4}_{L,7}) \oplus X^{i-4}_{R,15}$	k_7	$K^{i-3}_{17} \oplus K^{i-4}_{15}$
x_8	$X^{i-4}_{L,7} \oplus (X^{i-4}_{L,8} \& X^{i-4}_{L,1}) \oplus X^{i-4}_{R,9}$	k_8	K^{i-4}_{9}
x_9	$X^{i-4}_{L,10} \oplus X^{i-4}_{L,6} \oplus (X^{i-4}_{L,7} \& X^{i-4}_{L,0}) \oplus X^{i-4}_{R,8}$	k_9	$K^{i-3}_{10} \oplus K^{i-4}_{8}$
x_{10}	$X^{i-4}_{L,0} \oplus (X^{i-4}_{L,1} \& X^{i-4}_{L,26}) \oplus X^{i-4}_{R,2}$	k_{10}	K^{i-4}_{2}
x_{11}	$(X^{i-4}_{L,18} \& X^{i-4}_{L,11}) \oplus X^{i-4}_{R,19} \oplus X^{i-4}_{L,13} \oplus (X^{i-4}_{L,14} \& X^{i-4}_{L,7}) \oplus X^{i-4}_{R,15}$	k_{11}	$K^{i-3}_{17} \oplus K^{i-2}_{19} \oplus K^{i-4}_{19} \oplus K^{i-4}_{15}$
x_{12}	$X^{i-4}_{L,18} \oplus X^{i-4}_{L,14} \oplus (X^{i-4}_{L,15} \& X^{i-4}_{L,8}) \oplus X^{i-4}_{R,16}$	k_{12}	$K^{i-3}_{18} \oplus K^{i-4}_{16}$
x_{13}	$X^{i-4}_{L,8} \oplus (X^{i-4}_{L,9} \& X^{i-4}_{L,2}) \oplus X^{i-4}_{R,10}$	k_{13}	K^{i-4}_{10}
x_{14}	$X^{i-4}_{L,15} \oplus (X^{i-4}_{L,16} \& X^{i-4}_{L,9}) \oplus X^{i-4}_{R,17}$	k_{14}	K^{i-4}_{17}
x_{15}	$X^{i-4}_{L,11} \oplus X^{i-4}_{L,7} \oplus (X^{i-4}_{L,8} \& X^{i-4}_{L,1}) \oplus X^{i-4}_{R,9}$	k_{15}	$K^{i-3}_{11} \oplus K^{i-4}_{9}$
x_{16}	$X^{i-4}_{L,1} \oplus (X^{i-4}_{L,2} \& X^{i-4}_{L,27}) \oplus X^{i-4}_{R,3}$	k_{16}	K^{i-4}_{3}
x_{17}	$(X^{i-4}_{L,11} \& X^{i-4}_{L,4}) \oplus X^{i-4}_{R,12} \oplus X^{i-4}_{L,6} \oplus (X^{i-4}_{L,7} \& X^{i-4}_{L,0}) \oplus X^{i-4}_{R,8}$	k_{17}	$K^{i-3}_{10} \oplus K^{i-2}_{12} \oplus K^{i-4}_{12} \oplus K^{i-4}_{8}$
x_{18}	$X^{i-4}_{L,4} \oplus X^{i-4}_{L,0} \oplus (X^{i-4}_{L,1} \& X^{i-4}_{L,26}) \oplus X^{i-4}_{R,2}$	k_{18}	$K^{i-3}_{4} \oplus K^{i-4}_{2}$
x_{19}	$X^{i-4}_{L,26} \oplus (X^{i-4}_{L,27} \& X^{i-4}_{L,20}) \oplus X^{i-4}_{R,28}$	k_{19}	K^{i-4}_{28}
x_{20}	$(X^{i-4}_{L,22} \& X^{i-4}_{L,15}) \oplus X^{i-4}_{R,23} \oplus X^{i-4}_{L,27} \oplus (X^{i-4}_{L,18} \& X^{i-4}_{L,11}) \oplus X^{i-4}_{R,19}$	k_{20}	$K^{i-3}_{21} \oplus K^{i-2}_{23} \oplus K^{i-4}_{23} \oplus K^{i-4}_{19}$
x_{21}	$X^{i-4}_{L,18} \oplus (X^{i-4}_{L,19} \& X^{i-4}_{L,12}) \oplus X^{i-4}_{R,20}$	k_{21}	K^{i-4}_{20}
x_{22}	$X^{i-4}_{L,11} \oplus (X^{i-4}_{L,12} \& X^{i-4}_{L,5}) \oplus X^{i-4}_{R,13}$	k_{22}	K^{i-4}_{13}
x_{23}	$X^{i-4}_{L,22} \oplus X^{i-4}_{L,18} \oplus (X^{i-4}_{L,19} \& X^{i-4}_{L,12}) \oplus X^{i-4}_{R,20}$	k_{23}	$K^{i-3}_{22} \oplus K^{i-4}_{20}$
x_{24}	$X^{i-4}_{L,19} \oplus (X^{i-4}_{L,20} \& X^{i-4}_{L,13}) \oplus X^{i-4}_{R,21}$	k_{24}	K^{i-4}_{21}
x_{25}	$X^{i-4}_{L,12} \oplus (X^{i-4}_{L,13} \& X^{i-4}_{L,6}) \oplus X^{i-4}_{R,14}$	k_{25}	K^{i-4}_{14}
x_{26}	$X^{i-4}_{L,15} \oplus X^{i-4}_{L,11} \oplus (X^{i-4}_{L,12} \& X^{i-4}_{L,5}) \oplus X^{i-4}_{R,13}$	k_{26}	$K^{i-3}_{15} \oplus K^{i-4}_{13}$
x_{27}	$X^{i-4}_{L,5} \oplus (X^{i-4}_{L,6} \& X^{i-4}_{L,31}) \oplus X^{i-4}_{R,7} f_7$	k_{27}	K^{i-4}_{7}
x_{28}	$(X^{i-4}_{L,15} \& X^{i-4}_{L,8}) \oplus X^{i-4}_{R,16} \oplus X^{i-4}_{L,10} \oplus (X^{i-4}_{L,11} \& X^{i-4}_{L,4}) \oplus X^{i-4}_{R,12}$	k_{28}	$K^{i-3}_{14} \oplus K^{i-2}_{16} \oplus K^{i-4}_{16} \oplus K^{i-4}_{12}$
x_{29}	$X^{i-4}_{L,4} \oplus (X^{i-4}_{L,5} \& X^{i-4}_{L,30}) \oplus X^{i-4}_{R,6}$	k_{29}	K^{i-4}_{6}
x_{30}	$X^{i-4}_{L,8} \oplus X^{i-4}_{L,4} \oplus (X^{i-4}_{L,5} \& X^{i-4}_{L,30}) \oplus X^{i-4}_{R,6}$	k_{30}	$K^{i-3}_{8} \oplus K^{i-4}_{6}$
x_{31}	$X^{i-4}_{L,30} \oplus (X^{i-4}_{L,31} \& X^{i-4}_{L,24}) \oplus X^{i-4}_{R,0}$	k_{31}	K^{i-4}_{0}

$x_{11} = x_1 \oplus x_7, x_{17} = x_2 \oplus x_9,$

Table 12. 4 rounds after $X_{L,20}^{i+21} \oplus X_{L,24}^{i+21} \oplus X_{R,22}^{21}$ for SIMON64

x_0	$X_{R,20}^{i+25} \oplus X_{R,16}^{i+25} \oplus X_{R,12}^{i+25} \oplus (X_{R,13}^{i+25} \& X_{R,6}^{i+25}) \oplus X_{L,14}^{i+25} \oplus$ $X_{R,24}^{i+25} \oplus X_{R,20}^{i+25} \oplus (X_{R,21}^{i+25} \& X_{R,14}^{i+25}) \oplus X_{L,22}^{i+25}$	k_0	$K_{20}^{i+23} \oplus K_{16}^{i+23} \oplus K_{18}^{i+22} \oplus K_{20}^{i+21} \oplus$ $K_{24}^{i+23} \oplus K_{24}^{i+21} \oplus K_{14}^{i+24} \oplus K_{22}^{i+24}$
x_1	$X_{R,17}^{i+25} \oplus (X_{R,18}^{i+25} \& X_{R,11}^{i+25}) \oplus X_{L,19}^{i+25}$	k_1	K_{19}^{i+24}
x_2	$X_{R,10}^{i+25} \oplus (X_{R,11}^{i+25} \& X_{R,4}^{i+25}) \oplus X_{L,12}^{i+25}$	k_2	K_{12}^{i+24}
x_3	$X_{R,13}^{i+25} \oplus (X_{R,14}^{i+25} \& X_{R,7}^{i+25}) \oplus X_{L,15}^{i+25}$	k_3	K_{15}^{i+24}
x_4	$X_{R,6}^{i+25} \oplus (X_{R,7}^{i+25} \& X_{R,0}^{i+25}) \oplus X_{L,8}^{i+25}$	k_4	K_{8}^{i+24}
x_5	$X_{R,21}^{i+25} \oplus (X_{R,22}^{i+25} \& X_{R,15}^{i+25}) \oplus X_{L,23}^{i+25}$	k_5	K_{23}^{i+24}
x_6	$X_{R,14}^{i+25} \oplus (X_{R,15}^{i+25} \& X_{R,8}^{i+25}) \oplus X_{L,16}^{i+25}$	k_6	K_{16}^{i+24}
x_7	$X_{R,17}^{i+25} \oplus X_{R,13}^{i+25} \oplus (X_{R,14}^{i+25} \& X_{R,7}^{i+25}) \oplus X_{L,15}^{i+25}$	k_7	$K_{17}^{i+23} \oplus K_{15}^{i+24}$
x_8	$X_{R,7}^{i+25} \oplus (X_{R,8}^{i+25} \& X_{R,1}^{i+25}) \oplus X_{L,9}^{i+25}$	k_8	K_{9}^{i+24}
x_9	$X_{R,10}^{i+25} \oplus X_{R,6}^{i+25} \oplus (X_{R,7}^{i+25} \& X_{R,0}^{i+25}) \oplus X_{L,8}^{i+25}$	k_9	$K_{10}^{i+23} \oplus K_{8}^{i+24}$
x_{10}	$X_{R,0}^{i+25} \oplus (X_{R,1}^{i+25} \& X_{R,26}^{i+25}) \oplus X_{L,2}^{i+25}$	k_{10}	K_{2}^{i+24}
x_{11}	$(X_{R,18}^{i+25} \& X_{R,11}^{i+25}) \oplus X_{L,19}^{i+25} \oplus X_{R,13}^{i+25} \oplus (X_{R,14}^{i+25} \& X_{R,7}^{i+25}) \oplus X_{L,15}^{i+25}$	k_{11}	$K_{17}^{i+23} \oplus K_{19}^{i+22} \oplus K_{19}^{i+24} \oplus K_{15}^{i+24}$
x_{12}	$X_{R,18}^{i+25} \oplus X_{R,14}^{i+25} \oplus (X_{R,15}^{i+25} \& X_{R,8}^{i+25}) \oplus X_{L,16}^{i+25}$	k_{12}	$K_{18}^{i+23} \oplus K_{16}^{i+24}$
x_{13}	$X_{R,8}^{i+25} \oplus (X_{R,9}^{i+25} \& X_{R,2}^{i+25}) \oplus X_{L,10}^{i+25}$	k_{13}	K_{10}^{i+24}
x_{14}	$X_{R,15}^{i+25} \oplus (X_{R,16}^{i+25} \& X_{R,9}^{i+25}) \oplus X_{L,17}^{i+25}$	k_{14}	K_{17}^{i+24}
x_{15}	$X_{R,11}^{i+25} \oplus X_{R,7}^{i+25} \oplus (X_{R,8}^{i+25} \& X_{R,1}^{i+25}) \oplus X_{L,9}^{i+25}$	k_{15}	$K_{11}^{i+23} \oplus K_{9}^{i+24}$
x_{16}	$X_{R,1}^{i+25} \oplus (X_{R,2}^{i+25} \& X_{R,27}^{i+25}) \oplus X_{L,3}^{i+25}$	k_{16}	K_{3}^{i+24}
x_{17}	$(X_{R,11}^{i+25} \& X_{R,4}^{i+25}) \oplus X_{L,12}^{i+25} \oplus X_{R,6}^{i+25} \oplus (X_{R,7}^{i+25} \& X_{R,0}^{i+25}) \oplus X_{L,8}^{i+25}$	k_{17}	$K_{10}^{i+23} \oplus K_{12}^{i+22} \oplus K_{12}^{i+24} \oplus K_{8}^{i+24}$
x_{18}	$X_{R,4}^{i+25} \oplus X_{R,0}^{i+25} \oplus (X_{R,1}^{i+25} \& X_{R,26}^{i+25}) \oplus X_{L,2}^{i+25}$	k_{18}	$K_{4}^{i+23} \oplus K_{2}^{i+24}$
x_{19}	$X_{R,26}^{i+25} \oplus (X_{R,27}^{i+25} \& X_{R,20}^{i+25}) \oplus X_{L,28}^{i+25}$	k_{19}	K_{28}^{i+24}
x_{20}	$(X_{R,22}^{i+25} \& X_{R,15}^{i+25}) \oplus X_{L,23}^{i+25} \oplus X_{R,27}^{i+25} \oplus (X_{R,18}^{i+25} \& X_{R,11}^{i+25}) \oplus X_{L,19}^{i+25}$	k_{20}	$K_{21}^{i+23} \oplus K_{23}^{i+22} \oplus K_{23}^{i+24} \oplus K_{19}^{i+24}$
x_{21}	$X_{R,18}^{i+25} \oplus (X_{R,19}^{i+25} \& X_{R,12}^{i+25}) \oplus X_{L,20}^{i+25}$	k_{21}	K_{20}^{i+24}
x_{22}	$X_{R,11}^{i+25} \oplus (X_{R,12}^{i+25} \& X_{R,5}^{i+25}) \oplus X_{L,13}^{i+25}$	k_{22}	K_{13}^{i+24}
x_{23}	$X_{R,22}^{i+25} \oplus X_{R,18}^{i+25} \oplus (X_{R,19}^{i+25} \& X_{R,12}^{i+25}) \oplus X_{L,20}^{i+25}$	k_{23}	$K_{22}^{i+23} \oplus K_{20}^{i+24}$
x_{24}	$X_{R,19}^{i+25} \oplus (X_{R,20}^{i+25} \& X_{R,13}^{i+25}) \oplus X_{L,21}^{i+25}$	k_{24}	K_{21}^{i+24}
x_{25}	$X_{R,12}^{i+25} \oplus (X_{R,13}^{i+25} \& X_{R,6}^{i+25}) \oplus X_{L,14}^{i+25}$	k_{25}	K_{14}^{i+24}
x_{26}	$X_{R,15}^{i+25} \oplus X_{R,11}^{i+25} \oplus (X_{R,12}^{i+25} \& X_{R,5}^{i+25}) \oplus X_{L,13}^{i+25}$	k_{26}	$K_{15}^{i+23} \oplus K_{13}^{i+24}$
x_{27}	$X_{R,5}^{i+25} \oplus (X_{R,6}^{i+25} \& X_{R,31}^{i+25}) \oplus X_{L,7}^{i+25}$	k_{27}	K_{7}^{i+24}
x_{28}	$(X_{R,15}^{i+25} \& X_{R,8}^{i+25}) \oplus X_{L,16}^{i+25} \oplus X_{R,10}^{i+25} \oplus (X_{R,11}^{i+25} \& X_{R,4}^{i+25}) \oplus X_{L,12}^{i+25}$	k_{28}	$K_{14}^{i+23} \oplus K_{16}^{i+22} \oplus K_{16}^{i+24} \oplus K_{12}^{i+24}$
x_{29}	$X_{R,4}^{i+25} \oplus (X_{R,5}^{i+25} \& X_{R,30}^{i+25}) \oplus X_{L,6}^{i+25}$	k_{29}	K_{6}^{i+24}
x_{30}	$X_{R,8}^{i+25} \oplus X_{R,4}^{i+25} \oplus (X_{R,5}^{i+25} \& X_{R,30}^{i+25}) \oplus X_{L,6}^{i+25}$	k_{30}	$K_{8}^{i+23} \oplus K_{6}^{i+24}$
x_{31}	$X_{R,30}^{i+25} \oplus (X_{R,31}^{i+25} \& X_{R,24}^{i+25}) \oplus X_{L,0}^{i+25}$	k_{31}	K_{0}^{i+24}

$x_{11} = x_1 \oplus x_7, x_{17} = x_2 \oplus x_9$

Time: (1.a) $2^{26} \times N = 2^{89.53}$ one-round encryptions. (1.b) $2^{26} \times 2^{67.62} = 2^{93.62}$ additons. 2. The exhaustive phase needs $2^{96-8} = 2^{88}$ 30-round encryptions.

31-round attack on SIMON64/128. Expand one more round before X^{i-4} and one more round after X^{i+25}. The key bits of K^{i+25} involved to obtain the x represented in Table 12 are

$$\kappa_2 = (K_0^{i+25} - K_2^{i+25}, K_4^{i+25} - K_{22}^{i+25}, K_{24}^{i+25}, K_{26}^{i+25}, K_{30}^{i+25}, K_{31}^{i+25}),$$

in total 26 bits.

1. Guess each of 2^{52} $\kappa_1 || \kappa_2$
   (a) Encrypt the N plaintexts by one round and decrypt coresponding ciphertext by one round. Compress the internal states to a counter vectr of size 2^{58}.
   (b) Do as first two steps of the 29-round attack
2. Rank the keys and exhaustive the candidates with the help of key schedule

Time: (1.a) $2^{52} \times N = 2^{115.53}$ two-round encryptions. (1.b) $2^{52} \times 2^{67.62} = 2^{119.62}$ additons. 2.The exhaustive phase needs $2^{128-8} = 2^{120}$ 31-round encryptions.

B.3 Linear Attack on SIMON96/K

The linear hull used to attack SIMON96/K is

$$X^i_{L,2} \oplus X^i_{L,34} \oplus X^i_{L,38} \oplus X^i_{L,42} \oplus X^i_{R,36} \to X^{i+30}_{L,2} \oplus X^{i+30}_{L,42} \oplus X^{i+30}_{L,46} \oplus X^{i+30}_{R,0} \oplus X^{i+30}_{R,40},$$

which is proposed in [6] with potential $2^{-94.2}$.

Table 13. Add 3 rounds before $X^i_{L,2} \oplus X^i_{L,34} \oplus X^i_{L,38} \oplus X^i_{L,42} \oplus X^i_{R,36}$ for SIMON96

x_0	$X^{i-3}_{R,2} \oplus (X^{i-3}_{L,1} \& X^{i-3}_{L,42}) \oplus X^{i-3}_{R,34} \oplus (X^{i-3}_{L,33} \& X^{i-3}_{L,26}) \oplus X^{i-3}_{R,42} \oplus$ $(X^{i-3}_{L,41} \& X^{i-3}_{L,34}) \oplus X^{i-3}_{R,46} \oplus X^{i-3}_{L,44} \oplus (X^{i-3}_{L,45} \& X^{i-3}_{L,38}) \oplus X^{i-3}_{R,30}$ $\oplus X^{i-3}_{L,28} \oplus (X^{i-3}_{L,29} \& X^{i-3}_{L,22})$	k_0	$K^{i-3}_{2} \oplus K^{i-3}_{34} \oplus K^{i-3}_{42} \oplus K^{i-2}_{0}$ $\oplus K^{i-2}_{32} \oplus K^{i-2}_{40} \oplus K^{i-3}_{46} \oplus K^{i-3}_{30}$ $\oplus K^{i-1}_{2} \oplus K^{i-1}_{34} \oplus K^{i-1}_{38} \oplus K^{i-1}_{42}$
x_1	$X^{i-3}_{R,47} \oplus X^{i-3}_{L,45} \oplus (X^{i-3}_{L,46} \& X^{i-3}_{L,39})$	k_1	K^{i-3}_{47}
x_2	$X^{i-3}_{R,40} \oplus X^{i-3}_{L,38} \oplus (X^{i-3}_{L,39} \& X^{i-3}_{L,32})$	k_2	K^{i-3}_{40}
x_3	$X^{i-3}_{R,31} \oplus X^{i-3}_{L,29} \oplus (X^{i-3}_{L,30} \& X^{i-3}_{L,23})$	k_3	K^{i-3}_{31}
x_4	$X^{i-3}_{R,24} \oplus X^{i-3}_{L,22} \oplus (X^{i-3}_{L,23} \& X^{i-3}_{L,16})$	k_4	K^{i-3}_{24}
x_5	$X^{i-3}_{R,39} \oplus X^{i-3}_{L,37} \oplus (X^{i-3}_{L,38} \& X^{i-3}_{L,31})$	k_5	K^{i-3}_{39}
x_6	$X^{i-3}_{R,32} \oplus X^{i-3}_{L,30} \oplus (X^{i-3}_{L,31} \& X^{i-3}_{L,24})$	k_6	K^{i-3}_{32}
x_7	$X^{i-3}_{R,47} \oplus X^{i-3}_{L,45} \oplus (X^{i-3}_{L,46} \& X^{i-3}_{L,39}) \oplus X^{i-3}_{L,1}$	k_7	$K^{i-3}_{47} \oplus K^{i-2}_{1}$
x_8	$X^{i-3}_{R,0} \oplus X^{i-3}_{L,46} \oplus (X^{i-3}_{L,47} \& X^{i-3}_{L,40})$	k_8	K^{i-3}_{0}
x_9	$X^{i-3}_{R,41} \oplus X^{i-3}_{L,39} \oplus (X^{i-3}_{L,40} \& X^{i-3}_{L,33})$	k_9	K^{i-3}_{41}
x_{10}	$X^{i-3}_{R,40} \oplus X^{i-3}_{L,38} \oplus (X^{i-3}_{L,39} \& X^{i-3}_{L,32}) \oplus X^{i-3}_{L,42}$	k_{10}	$K^{i-3}_{40} \oplus K^{i-2}_{42}$
x_{11}	$X^{i-3}_{R,34} \oplus X^{i-3}_{L,32} \oplus (X^{i-3}_{L,33} \& X^{i-3}_{L,26})$	k_{11}	K^{i-3}_{34}
x_{12}	$X^{i-3}_{R,31} \oplus X^{i-3}_{L,29} \oplus (X^{i-3}_{L,30} \& X^{i-3}_{L,23}) \oplus X^{i-3}_{L,33}$	k_{12}	$K^{i-3}_{31} \oplus K^{i-2}_{33}$
x_{13}	$X^{i-3}_{R,25} \oplus X^{i-3}_{L,23} \oplus (X^{i-3}_{L,24} \& X^{i-3}_{L,17})$	k_{13}	K^{i-3}_{25}
x_{14}	$X^{i-3}_{R,24} \oplus X^{i-3}_{L,22} \oplus (X^{i-3}_{L,23} \& X^{i-3}_{L,16}) \oplus X^{i-3}_{L,26}$	k_{14}	$K^{i-3}_{24} \oplus K^{i-2}_{26}$
x_{15}	$X^{i-3}_{R,18} \oplus X^{i-3}_{L,16} \oplus (X^{i-3}_{L,17} \& X^{i-3}_{L,10})$	k_{15}	K^{i-3}_{18}
x_{16}	$X^{i-3}_{R,35} \oplus X^{i-3}_{L,33} \oplus (X^{i-3}_{L,34} \& X^{i-3}_{L,27}) \oplus X^{i-3}_{L,37}$	k_{16}	$K^{i-3}_{35} \oplus K^{i-2}_{37}$
x_{17}	$X^{i-3}_{R,36} \oplus X^{i-3}_{L,34} \oplus (X^{i-3}_{L,35} \& X^{i-3}_{L,28})$	k_{17}	K^{i-3}_{36}
x_{18}	$X^{i-3}_{R,29} \oplus X^{i-3}_{L,27} \oplus (X^{i-3}_{L,28} \& X^{i-3}_{L,21})$	k_{18}	K^{i-3}_{29}
x_{19}	$X^{i-3}_{R,28} \oplus X^{i-3}_{L,26} \oplus (X^{i-3}_{L,27} \& X^{i-3}_{L,20}) \oplus X^{i-3}_{L,30}$	k_{19}	$K^{i-3}_{28} \oplus K^{i-2}_{30}$
x_{20}	$X^{i-3}_{R,22} \oplus X^{i-3}_{L,20} \oplus (X^{i-3}_{L,21} \& X^{i-3}_{L,14})$	k_{20}	K^{i-3}_{22}
x_{21}	$X^{i-3}_{R,39} \oplus X^{i-3}_{L,37} \oplus (X^{i-3}_{L,38} \& X^{i-3}_{L,31}) \oplus X^{i-3}_{L,41}$	k_{21}	$K^{i-3}_{39} \oplus K^{i-2}_{41}$
x_{22}	$X^{i-3}_{R,33} \oplus X^{i-3}_{L,31} \oplus (X^{i-3}_{L,32} \& X^{i-3}_{L,25})$	k_{22}	K^{i-3}_{33}
x_{23}	$X^{i-3}_{R,32} \oplus X^{i-3}_{L,30} \oplus (X^{i-3}_{L,31} \& X^{i-3}_{L,24}) \oplus X^{i-3}_{L,34}$	k_{23}	$K^{i-3}_{32} \oplus K^{i-2}_{34}$
x_{24}	$X^{i-3}_{R,26} \oplus X^{i-3}_{L,24} \oplus (X^{i-3}_{L,25} \& X^{i-3}_{L,18})$	k_{24}	K^{i-3}_{26}

If we add three rounds before the linear hull, according to Table 13, $X^i_{L,2} \oplus X^i_{L,34} \oplus X^i_{L,38} \oplus X^i_{L,42} \oplus X^i_{R,36}$ can be represented as

$$\begin{aligned}
&x_0 \oplus k_0 \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)) \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4)) \oplus ((x_5 \oplus k_5)\&(x_6 \oplus k_6)) \\
&\oplus ((x_7 \oplus k_7 \oplus ((x_8 \oplus k_8)\&(x_9 \oplus k_9)))\&(x_{10} \oplus k_{10} \oplus ((x_9 \oplus k_9)\&(x_{11} \oplus k_{11})))) \\
&\oplus ((x_{12} \oplus k_{12} \oplus ((x_6 \oplus k_6)\&(x_{13} \oplus k_{13})))\&(x_{14} \oplus k_{14} \oplus ((x_{13} \oplus k_{13})\&(x_{15} \oplus k_{15})))) \\
&\oplus ((x_{16} \oplus k_{16} \oplus ((x_{17} \oplus k_{17})\&(x_{18} \oplus k_{18})))\&(x_{19} \oplus k_{19} \oplus ((x_{18} \oplus k_{18})\&(x_{20} \oplus k_{20})))) \\
&\oplus ((x_{21} \oplus k_{21} \oplus ((x_2 \oplus k_2)\&(x_{22} \oplus k_{22})))\&(x_{23} \oplus k_{23} \oplus ((x_{22} \oplus k_{22})\&(x_{24} \oplus k_{24}))))
\end{aligned}$$

Compress the plaintexts: (Procedure SIMON96-Head) At first, compress the plaintexts into a counter vector $V[x_1 - x_{24}]$ using the linear compression technique.

1. For each $x_3 - x_{20}$

(a) Compress $x_1, x_2, x_{21}-x_{24}$ as Case f_6 in Appendix A. There is 6-bit key $(k_1, k_2, k_{21}-k_{24})$ to store and time is $2^{8.36}$. So here the memory is about $2^{18}\times 2^6 = 2^{24}$ counters and total time is $2^{18}\times 2^{8.36} = 2^{26.36}$.

2. For each $x_3, x_4, x_7 - x_{11}, x_{16} - x_{20}, k_1, k_2, k_{21} - k_{24}$
   (a) Compress $x_5, x_6, x_{12}-x_{15}$ as Case f_6 in Appendix A. There is 6-bit key $(k_5, k_6, k_{12}-k_{15})$ to store and time is $2^{8.36}$. So here the memory is about $2^{18}\times 2^6 = 2^{24}$ counters and total time is $2^{18}\times 2^{8.36} = 2^{26.36}$.
3. For each $x_{16} - x_{20}, k_1, k_2, k_5, k_6, k_{12} - k_{15}, k_{21} - k_{24}$
   (a) Compress $x_3, x_4, x_7 - x_{11}$ as Case f_3 in Appendix A. There is 7-bit key $(k_3, k_4, k_7 - k_{11})$ to store and time is $2^{9.25}$. So here the memory is about $2^{17}\times 2^7 = 2^{24}$ counters and total time is $2^{17}\times 2^{9.25} = 2^{26.25}$.
4. For each $k_1 - k_{15}, k_{21} - k_{24}$
   (a) Compress $x_{16} - x_{20}$, as Case f_2 in Appendix A. There is 5-bit key $(k_{16} - k_{20})$ to store and time is $2^{6.46}$. So here the memory is about $2^{19} \times 2^5 = 2^{24}$ counters and total time is $2^{19} \times 2^{6.46} = 2^{25.46}$.
5. The total time is about $2^{28.15}$ additions and memory is $\mathcal{O}(2^{24})$

If we add four rounds after the linear hull, according to Table 14, $X^{i+30}_{L,2} \oplus X^{i+30}_{L,42} \oplus X^{i+30}_{L,46} \oplus X^{i+30}_{R,0} \oplus X^{i+30}_{R,40}$ can be represented as

$$
\begin{aligned}
&x_0 \oplus k_0 \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2))\oplus \\
&((x_3 \oplus k_3 \oplus ((x_4 \oplus k_4)\&(x_5 \oplus k_5)))\&(x_6 \oplus k_6 \oplus ((x_5 \oplus k_5)\&(x_7 \oplus k_7))))\oplus \\
&((x_8 \oplus k_8 \oplus ((x_9 \oplus k_9)\&(x_{10} \oplus k_{10})))\&(x_{11} \oplus k_{11} \oplus ((x_{10} \oplus k_{10})\&(x_{12} \oplus k_{12}))))\oplus \\
&((x_{13} \oplus k_{13} \oplus ((x_{14} \oplus k_{14})\&(x_{15} \oplus k_{15})))\&(x_{16} \oplus k_{16} \oplus ((x_{15} \oplus k_{15})\&(x_{17} \oplus k_{17}))))\oplus \\
&\{(x_{18} \oplus k_{18} \oplus ((x_{19} \oplus k_{19})\&(\underline{x_{20} \oplus k_{20}}))\oplus \\
&((x_{21} \oplus k_{21} \oplus ((x_{22} \oplus k_{22})\&(x_{23} \oplus k_{23})))\&(x_{24} \oplus k_{24} \oplus ((x_{23} \oplus k_{23})\&(x_{25} \oplus k_{25})))))\& \\
&(x_{26} \oplus k_{26} \oplus ((\underline{x_{20} \oplus k_{20}})\&(\underline{x_{27} \oplus k_{27}}))\oplus \\
&((x_{24} \oplus k_{24} \oplus ((x_{23} \oplus k_{23})\&(x_{25} \oplus k_{25})))\&(x_{28} \oplus k_{28} \oplus ((x_{25} \oplus k_{25})\&(x_{29} \oplus k_{29})))))\}\oplus \\
&\{(x_{30} \oplus k_{30} \oplus ((x_{31} \oplus k_{31})\&(x_{15} \oplus k_{15}))\oplus \\
&((x_{32} \oplus k_{32} \oplus ((x_{20} \oplus k_{20})\&(x_{27} \oplus k_{27})))\&(x_{33} \oplus k_{33} \oplus ((x_{27} \oplus k_{27})\&(x_{34} \oplus k_{34})))))\& \\
&(x_{35} \oplus k_{35} \oplus ((x_{15} \oplus k_{15})\&(x_{17} \oplus k_{17}))\oplus \\
&((x_{33} \oplus k_{33} \oplus ((x_{27} \oplus k_{27})\&(x_{34} \oplus k_{34})))\&(x_{36} \oplus k_{36} \oplus ((x_{34} \oplus k_{34})\&(x_{37} \oplus k_{37})))))\}
\end{aligned}
$$

Compress the ciphertexts: (Procedure SIMON96-Tail) At first, compress the ciphertexts into a counter vector $V[x_1 - x_{37}]$ using the linear compression technique. To simplify our description of attack, we regard the x_{20}, x_{27} with underline as new variables x'_{20}, x'_{27}. It is the same with k_{20} and k_{27}.

1. For each $x_8 - x_{37}$
   (a) Compress $x_1 - x_7$ as Case f_3 in Appendix A. There is 7-bit key $(k_1 - k_7)$ to store and time is $2^{9.25}$. So here the memory is about $2^{30} \times 2^7 = 2^{37}$ counters and total time is $2^{30} \times 2^{9.25} = 2^{39.25}$.
2. For each $x_{13} - x_{37}, k_1 - k_7$
   (a) Compress $x_8 - x_{12}$ as Case f_2 in Appendix A. There is 5-bit key $(k_8 - k_{12})$ to store and time is $2^{6.46}$. So here the memory is about $2^{32} \times 2^5 = 2^{37}$ counters and total time is $2^{32} \times 2^{6.46} = 2^{38.46}$.
3. For each $x_{18}, x_{19}, x'_{20}, x_{21} - x_{26}, x'_{27}, x_{28}, x_{29}, k_1 - k_{12}$
   (a) Compress $x_{13} - x_{17}, x_{20}, x_{27}, x_{30} - x_{37}$ as Case f_7 in Appendix A. There is 15-bit key $(k_{13} - k_{17}, k_{20}, k_{27}, k_{30} - k_{37})$ to store and time is $2^{18.08}$. So here the memory is about $2^{24} \times 2^{15} = 2^{39}$ counters and total time is $2^{24} \times 2^{18.08} = 2^{42.08}$.
4. For each $k_1 - k_{17}, k_{20}, k_{27}, k_{30} - k_{37}$
   (a) Compress $x_{18}, x_{19}, x'_{20}, x_{21}-x_{26}, x'_{27}, x_{28}, x_{29}$, as Case f_7 in Appendix A. There is 10-bit key $(k_{18}, k_{19}, k_{21} - k_{26}, k_{28}, k_{29})$ to store and time is $2^{15.99}$. So here the memory is about $2^{27} \times 2^{10} = 2^{37}$ counters and total time is $2^{27} \times 2^{15.99} = 2^{42.99}$.
5. The total time is less than $2^{43.71}$ additions and memory is $\mathcal{O}(2^{39})$.

37-round attack on SIMON96/96. We add three rounds before and four rounds after the 30-round linear distinguisher to attack 37-round SIMON96/K. Suppose we use $N = 2\bar{\epsilon}^{-2} = 2^{95.2}$ known plaintext-ciphertext pairs. Set advantage $a = 8$. The success probability would be 0.477. At first, compress the N plaintext-ciphertext pairs to 2^{24+37} counters according to Table 13 and 14. Suppose the plaintext be compressed to x_P and ciphertext be compressed to x_C.

Table 14. Add 4 rounds after $X^{i+30}_{L,2} \oplus X^{i+30}_{L,42} \oplus X^{i+30}_{L,46} \oplus X^{i+30}_{R,0} \oplus X^{i+30}_{R,40}$ for SIMON96

x_0	$X^{i+34}_{R,0} \oplus X^{i+34}_{L,2} \oplus (X^{i+34}_{R,1} \& X^{i+34}_{R,42}) \oplus X^{i+34}_{R,40} \oplus X^{i+34}_{L,42} \oplus (X^{i+34}_{R,41} \& X^{i+34}_{R,34}) \oplus X^{i+34}_{L,38} \oplus (X^{i+34}_{R,37} \& X^{i+34}_{R,30}) \oplus X^{i+34}_{R,32} \oplus X^{i+34}_{L,34} \oplus (X^{i+34}_{R,33} \& X^{i+34}_{R,26})$	k_0	$K^{i+33}_{2} \oplus K^{i+33}_{34} \oplus K^{i+33}_{38} \oplus K^{i+33}_{42} \oplus K^{i+32}_{36} \oplus K^{i+31}_{2} \oplus K^{i+31}_{38} \oplus K^{i+31}_{42} \oplus K^{i+30}_{0} \oplus K^{i+31}_{40}$
x_1	$X^{i+34}_{R,33} \oplus X^{i+34}_{L,35} \oplus (X^{i+34}_{R,34} \& X^{i+34}_{R,27})$	k_1	K^{i+33}_{35}
x_2	$X^{i+34}_{R,26} \oplus X^{i+34}_{L,28} \oplus (X^{i+34}_{R,27} \& X^{i+34}_{R,20})$	k_2	K^{i+33}_{28}
x_3	$X^{i+34}_{R,45} \oplus X^{i+34}_{L,47} \oplus (X^{i+34}_{R,46} \& X^{i+34}_{R,39}) \oplus X^{i+34}_{R,1}$	k_3	$K^{i+33}_{47} \oplus K^{i+32}_{1}$
x_4	$X^{i+34}_{R,46} \oplus X^{i+34}_{L,0} \oplus (X^{i+34}_{R,47} \& X^{i+34}_{R,40})$	k_4	K^{i+33}_{0}
x_5	$X^{i+34}_{R,39} \oplus X^{i+34}_{L,41} \oplus (X^{i+34}_{R,40} \& X^{i+34}_{R,33})$	k_5	K^{i+33}_{41}
x_6	$X^{i+34}_{R,38} \oplus X^{i+34}_{L,40} \oplus (X^{i+34}_{R,39} \& X^{i+34}_{R,32}) \oplus X^{i+34}_{R,42}$	k_6	$K^{i+33}_{40} \oplus K^{i+32}_{42}$
x_7	$X^{i+34}_{R,32} \oplus X^{i+34}_{L,34} \oplus (X^{i+34}_{R,33} \& X^{i+34}_{R,26})$	k_7	K^{i+33}_{34}
x_8	$X^{i+34}_{R,37} \oplus X^{i+34}_{L,39} \oplus (X^{i+34}_{R,38} \& X^{i+34}_{R,31}) \oplus X^{i+34}_{R,41}$	k_8	$K^{i+33}_{39} \oplus K^{i+32}_{41}$
x_9	$X^{i+34}_{R,38} \oplus X^{i+34}_{L,40} \oplus (X^{i+34}_{R,39} \& X^{i+34}_{R,32})$	k_9	K^{i+33}_{40}
x_{10}	$X^{i+34}_{R,31} \oplus X^{i+34}_{L,33} \oplus (X^{i+34}_{R,32} \& X^{i+34}_{R,25})$	k_{10}	K^{i+33}_{33}
x_{11}	$X^{i+34}_{R,30} \oplus X^{i+34}_{L,32} \oplus (X^{i+34}_{R,31} \& X^{i+34}_{R,24}) \oplus X^{i+34}_{R,34}$	k_{11}	$K^{i+33}_{32} \oplus K^{i+32}_{34}$
x_{12}	$X^{i+34}_{R,24} \oplus X^{i+34}_{L,26} \oplus (X^{i+34}_{R,25} \& X^{i+34}_{R,18})$	k_{12}	K^{i+33}_{26}
x_{13}	$X^{i+34}_{R,33} \oplus X^{i+34}_{L,35} \oplus (X^{i+34}_{R,34} \& X^{i+34}_{R,27}) \oplus X^{i+34}_{R,37}$	k_{13}	$K^{i+33}_{35} \oplus K^{i+32}_{37}$
x_{14}	$X^{i+34}_{R,34} \oplus X^{i+34}_{L,36} \oplus (X^{i+34}_{R,35} \& X^{i+34}_{R,28})$	k_{14}	K^{i+33}_{36}
x_{15}	$X^{i+34}_{R,27} \oplus X^{i+34}_{L,29} \oplus (X^{i+34}_{R,28} \& X^{i+34}_{R,21})$	k_{15}	K^{i+33}_{29}
x_{16}	$X^{i+34}_{R,26} \oplus X^{i+34}_{L,28} \oplus (X^{i+34}_{R,27} \& X^{i+34}_{R,20}) \oplus X^{i+34}_{R,30}$	k_{16}	$K^{i+33}_{28} \oplus K^{i+32}_{30}$
x_{17}	$X^{i+34}_{R,20} \oplus X^{i+34}_{L,22} \oplus (X^{i+34}_{R,21} \& X^{i+34}_{R,14})$	k_{17}	K^{i+33}_{22}
x_{18}	$X^{i+34}_{R,41} \oplus X^{i+34}_{L,43} \oplus (X^{i+34}_{R,42} \& X^{i+34}_{R,35}) \oplus X^{i+34}_{L,47} \oplus (X^{i+34}_{R,46} \& X^{i+34}_{R,39})$	k_{18}	$K^{i+33}_{43} \oplus K^{i+33}_{47} \oplus K^{i+32}_{45} \oplus K^{i+31}_{47}$
x_{19}	$X^{i+34}_{R,42} \oplus X^{i+34}_{L,44} \oplus (X^{i+34}_{R,43} \& X^{i+34}_{R,36})$	k_{19}	K^{i+33}_{44}
x_{20}	$X^{i+34}_{R,35} \oplus X^{i+34}_{L,37} \oplus (X^{i+34}_{R,36} \& X^{i+34}_{R,29})$	k_{20}	K^{i+33}_{37}
x_{21}	$X^{i+34}_{R,42} \oplus X^{i+34}_{L,44} \oplus (X^{i+34}_{R,43} \& X^{i+34}_{R,36}) \oplus X^{i+34}_{R,46}$	k_{21}	$K^{i+33}_{44} \oplus K^{i+32}_{46}$
x_{22}	$X^{i+34}_{R,43} \oplus X^{i+34}_{L,45} \oplus (X^{i+34}_{R,44} \& X^{i+34}_{R,37})$	k_{22}	K^{i+33}_{45}
x_{23}	$X^{i+34}_{R,36} \oplus X^{i+34}_{L,38} \oplus (X^{i+34}_{R,37} \& X^{i+34}_{R,30})$	k_{23}	K^{i+33}_{38}
x_{24}	$X^{i+34}_{R,35} \oplus X^{i+34}_{L,37} \oplus (X^{i+34}_{R,36} \& X^{i+34}_{R,29}) \oplus X^{i+34}_{R,39}$	k_{24}	$K^{i+33}_{37} \oplus K^{i+32}_{39}$
x_{25}	$X^{i+34}_{R,29} \oplus X^{i+34}_{L,31} \oplus (X^{i+34}_{R,30} \& X^{i+34}_{R,23})$	k_{25}	K^{i+33}_{31}
x_{26}	$X^{i+34}_{R,34} \oplus X^{i+34}_{L,36} \oplus (X^{i+34}_{R,35} \& X^{i+34}_{R,28}) \oplus X^{i+34}_{L,40} \oplus (X^{i+34}_{R,39} \& X^{i+34}_{R,32})$	k_{26}	$K^{i+33}_{36} \oplus K^{i+33}_{40} \oplus K^{i+32}_{38} \oplus K^{i+31}_{40}$
x_{27}	$X^{i+34}_{R,28} \oplus X^{i+34}_{L,30} \oplus (X^{i+34}_{R,29} \& X^{i+34}_{R,22})$	k_{27}	K^{i+33}_{30}
x_{28}	$X^{i+34}_{R,28} \oplus X^{i+34}_{L,30} \oplus (X^{i+34}_{R,29} \& X^{i+34}_{R,22}) \oplus X^{i+34}_{R,32}$	k_{28}	$K^{i+33}_{30} \oplus K^{i+32}_{32}$
x_{29}	$X^{i+34}_{R,22} \oplus X^{i+34}_{L,24} \oplus (X^{i+34}_{R,23} \& X^{i+34}_{R,16})$	k_{29}	K^{i+33}_{24}
x_{30}	$X^{i+34}_{R,33} \oplus X^{i+34}_{L,35} \oplus (X^{i+34}_{R,34} \& X^{i+34}_{R,27}) \oplus X^{i+34}_{L,39} \oplus (X^{i+34}_{R,38} \& X^{i+34}_{R,31})$	k_{30}	$K^{i+33}_{35} \oplus K^{i+33}_{39} \oplus K^{i+32}_{37} \oplus K^{i+31}_{39}$
x_{31}	$X^{i+34}_{R,34} \oplus X^{i+34}_{L,36} \oplus (X^{i+34}_{R,35} \& X^{i+34}_{R,28})$	k_{31}	K^{i+33}_{36}
x_{32}	$X^{i+34}_{R,34} \oplus X^{i+34}_{L,36} \oplus (X^{i+34}_{R,35} \& X^{i+34}_{R,28}) \oplus X^{i+34}_{R,38}$	k_{32}	$K^{i+33}_{36} \oplus K^{i+32}_{38}$
x_{33}	$X^{i+34}_{R,27} \oplus X^{i+34}_{L,29} \oplus (X^{i+34}_{R,28} \& X^{i+34}_{R,21}) \oplus X^{i+34}_{R,31}$	k_{33}	$K^{i+33}_{29} \oplus K^{i+32}_{31}$
x_{34}	$X^{i+34}_{R,21} \oplus X^{i+34}_{L,23} \oplus (X^{i+34}_{R,22} \& X^{i+34}_{R,15})$	k_{34}	K^{i+33}_{23}
x_{35}	$X^{i+34}_{R,26} \oplus X^{i+34}_{L,28} \oplus (X^{i+34}_{R,27} \& X^{i+34}_{R,20}) \oplus X^{i+34}_{L,32} \oplus (X^{i+34}_{R,31} \& X^{i+34}_{R,24})$	k_{35}	$K^{i+33}_{28} \oplus K^{i+33}_{32} \oplus K^{i+32}_{30} \oplus K^{i+31}_{32}$
x_{36}	$X^{i+34}_{R,20} \oplus X^{i+34}_{L,22} \oplus (X^{i+34}_{R,21} \& X^{i+34}_{R,14}) \oplus X^{i+34}_{R,24}$	k_{36}	$K^{i+33}_{22} \oplus K^{i+32}_{24}$
x_{37}	$X^{i+34}_{R,14} \oplus X^{i+34}_{L,16} \oplus (X^{i+34}_{R,15} \& X^{i+34}_{R,8})$	k_{37}	K^{i+33}_{16}

1. For each of 2^{37} x_C
   (a) Call Procedure SIMON96-Head, and store the counters according to the keys used in the first three rounds
2. For each of 2^{24} keys involved in the first three rounds
   (a) Call Procedure SIMON96-Tail, and store the counters according to the keys used in the last four rounds
3. Rank the keys and exhaustive the candidates with the help of key schedule

Time: 1. $2^{37} \times 2^{28.15} = 2^{65.15}$ additions; 2. $2^{24} \times 2^{43.71} = 2^{67.71}$ additions. So it needs $2^{65.15} + 2^{67.71} = 2^{67.94}$ additions to get the bias for the subkeys. 3. The exhaustive phase needs $2^{96-8} = 2^{88}$ 37-round encryptions.

38-round attack on SIMON96/144. Expand one more round before X^{i-3}. The key bits of K^{i-4} involved to obtain the x represented in Table 13 are $\kappa_1 = (K_1^{i-4}, K_{10}^{i-4}, K_{14}^{i-4}, K_{16}^{i-4} - K_{18}^{i-4}, K_{20}^{i-4} - K_{35}^{i-4}, K_{37}^{i-4} - K_{42}^{i-4}, K_{45}^{i-4} - K_{47}^{i-4})$, in total 31 bits.

1. Guess each of 2^{31} κ_1
   (a) Encrypt the N plaintexts by one round. Compress the internal states to a counter vectr of size 2^{61}.
   (b) Do as first two steps of the 37-round attack
2. Rank the keys and exhaustive the candidates with the help of key schedule

Time: (1.a) $2^{31} \times N = 2^{126.2}$ one-round encryptions. (1.b) $2^{31} \times 2^{67.94} = 2^{98.94}$ additons. 2.The exhaustive phase needs $2^{144-8} = 2^{136}$ 38-round encryptions.

B.4 Linear Attack on SIMON128/*K*

The linear hull used to attack SIMON128/K is

$$X_{L,2}^i \oplus X_{L,58}^i \oplus X_{L,62}^i \oplus X_{R,60}^i \rightarrow X_{L,60}^{i+41} \oplus X_{R,2}^{i+41} \oplus X_{R,58}^{i+41} \oplus X_{R,62}^{i+41},$$

which is proposed in [6] with popential $2^{-126.6}$.

If we add four rounds before the linear hull, according to Table 15, $X_{L,2}^i \oplus X_{L,58}^i \oplus X_{L,62}^i \oplus X_{R,60}^i$ can be represented as

$$\begin{aligned}
&x_0 \oplus k_0 \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)) \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4)) \oplus ((x_5 \oplus k_5)\&(x_6 \oplus k_6))\oplus \\
&((x_7 \oplus k_7 \oplus ((x_8 \oplus k_8)\&(x_9 \oplus k_9)))\&(x_{10} \oplus k_{10} \oplus ((x_9 \oplus k_9)\&(x_{11} \oplus k_{11}))))\oplus \\
&((x_{12} \oplus k_{12} \oplus ((x_{13} \oplus k_{13})\&(x_{14} \oplus k_{14})))\&(x_{15} \oplus k_{15} \oplus ((x_{13} \oplus k_{13})\&(x_{16} \oplus k_{16}))))\oplus \\
&\{(x_{17} \oplus k_{17} \oplus ((x_8 \oplus k_8)\&(x_9 \oplus k_9))\oplus \\
&((x_{18} \oplus k_{18} \oplus ((x_{19} \oplus k_{19})\&(x_{20} \oplus k_{20})))\&(x_{21} \oplus k_{21} \oplus ((x_{20} \oplus k_{20})\&(x_{22} \oplus k_{22})))))\& \\
&(x_{23} \oplus k_{23} \oplus ((x_9 \oplus k_9)\&(x_{11} \oplus k_{11}))\oplus \\
&((x_{21} \oplus k_{21} \oplus ((x_{20} \oplus k_{20})\&(x_{22} \oplus k_{22})))\&(x_{24} \oplus k_{24} \oplus ((x_{22} \oplus k_{22})\&(x_{25} \oplus k_{25})))))\}\oplus \\
&\{(x_{26} \oplus k_{26} \oplus ((x_{13} \oplus k_{13})\&(x_{16} \oplus k_{16}))\oplus \\
&((x_{10} \oplus k_{10} \oplus ((x_9 \oplus k_9)\&(x_{11} \oplus k_{11})))\&(x_{27} \oplus k_{27} \oplus ((x_{11} \oplus k_{11})\&(x_{28} \oplus k_{28})))))\& \\
&(x_{29} \oplus k_{29} \oplus ((x_{13} \oplus k_{13})\&(x_{14} \oplus k_{14}))\oplus \\
&((x_{27} \oplus k_{27} \oplus ((x_{11} \oplus k_{11})\&(x_{28} \oplus k_{28})))\&(x_{30} \oplus k_{30} \oplus ((x_{28} \oplus k_{28})\&(x_{34} \oplus k_{34})))))\}\oplus \\
&\{(x_{32} \oplus k_{32} \oplus ((\underline{x_2 \oplus k_2})\&(x_{33} \oplus k_{33}))\oplus \\
&((x_{34} \oplus k_{34} \oplus ((x_{35} \oplus k_{35})\&(x_{36} \oplus k_{36})))\&(x_{37} \oplus k_{37} \oplus ((x_{36} \oplus k_{36})\&(x_{38} \oplus k_{38})))))\& \\
&(x_{39} \oplus k_{39} \oplus ((x_{33} \oplus k_{33})\&(x_{40} \oplus k_{40}))\oplus \\
&((x_{37} \oplus k_{37} \oplus ((x_{36} \oplus k_{36})\&(x_{38} \oplus k_{38})))\&(x_{41} \oplus k_{41} \oplus ((x_{38} \oplus k_{38})\&(x_{42} \oplus k_{42})))))\}
\end{aligned}$$

Compress the plaintexts: (Procedure SIMON128-Head) At first, compress the plaintexts into a counter vector $V[x_1 - x_{42}]$. In fact, there are 2^{38} elements for vector V, since $x_{17} = x_1 \oplus x_7, x_{23} = x_2 \oplus x_{10}, x_{26} =$

$x_5 \oplus x_{15}$ and $x_{29} = x_6 \oplus x_{12}$. To simplify our description, we introduce the situations that the XOR for the guessed k bit and corresponding x bit is zero in Step 2 to Step 9, since the representation of the target parity bit in another situation has same form with it. x_2, k_2 with underline shown above are regarded as new variables x'_2, k'_2, independent of x_2, k_2.

1. Guess k_1, k_2, k_5, k_6
   (a) x_1, x_2, x_5, x_6 can be removed and the index value for counter vectors becomes $x'_2, x_3, x_4, x_7 - x_{42}$. There are 2^{38} new counters and the counter values are refreshed according to $((x_1 \oplus k_1)\&(x_2 \oplus k_2)) \oplus ((x_5 \oplus k_5)\&(x_6 \oplus k_6))$. The time is $2^{38} \times 2^4 = 2^{42}$ simple calculations.
2. Guess k_{13}. Since $x_{13} \oplus k_{13} = 0$, x_{14}, x_{16} can be compressed. The time is $2^{35} \times 3$ additions.
3. Guess k_9. Since $x_9 \oplus k_9 = 0$, x_8 can be compressed. The time is 2^{33} additions.
4. Guess k_{20}. Since $x_{20} \oplus k_{20} = 0$, x_{19} can be compressed. The time is 2^{31} additions.
5. Guess k_{22}. Since $x_{22} \oplus k_{22} = 0$, x_{25} can be compressed. The time is 2^{29} additions.
6. Guess k_{28}. Since $x_{28} \oplus k_{28} = 0$, x_{11}, x_{34} can be compressed. The time is $2^{26} \times 3$ additions.
7. Guess k_{36}. Since $x_{36} \oplus k_{36} = 0$, x_{35} can be compressed. The time is 2^{24} additions.
8. Guess k_{33}. Since $x_{33} \oplus k_{33} = 0$, x_2 with underline and x_{40} can be compressed. The time is 2^{22} additions.
9. Guess k_{38}. Since $x_{38} \oplus k_{38} = 0$, x_{42} can be compressed. The time is 2^{20} additions.
10. After above guess and split, remained bits for x and k are bit 3,4,7,10,12,15,17,18,21,23,24,26,27,29,30,32, 34,37, 39,41. We can compress $x_3, x_4, x_{17}, x_{18}, x_{21}, x_{23}, x_{24}$ as case f_3 in Appendix A. The time is $2^{13} \times 2^{9.25} = 2^{22.25}$. Then we compress $x_7, x_{10}, x_{26}, x_{27}, x_{29}, x_{30}$ as case f_6 in Appendix A. The time is $2^{14} \times 2^{8.36} = 2^{22.36}$. At last, we compress $x_{12}, x_{15}, x_{32}, x_{34}, x_{37}, x_{39}, x_{41}$ as case f_3 in Appendix A. The time is $2^{13} \times 2^{9.25} = 2^{22.25}$.
11. Calculate the other situations as above.

Time is estimated from the inner part to outer part. Step 10 needs about $T_{10} = 2^{23.87}$ additions. In Step 9, the two cases, $x_{38} \oplus k_{38} = 0$, $x_{38} \oplus k_{38} = 1$ have same time complexity and there are two possible guesses for k_{38}. So the total time for Step 9 and 10 is $T_9 = 2 \times ((2^{20} + T_{10}) \times 2 + 2^{21}) = 2^{26.05}$, where 2^{21} is the time for combination. Similarly, the time for Step 2 to Step 10 is as follows.

Step	Time
9-10	$T_9 = 2 \times ((2^{20} + T_{10}) \times 2 + 2^{21}) = 2^{26.05}$
8-10	$T_8 = 2 \times ((2^{22} + T_9) \times 2 + 2^{23}) = 2^{28.21}$
7-10	$T_7 = 2 \times ((2^{24} + T_8) \times 2 + 2^{25}) = 2^{30.36}$
6-10	$T_6 = 2 \times ((2^{26} \times 3 + T_7) \times 2 + 2^{28}) = 2^{32.67}$
5-10	$T_5 = 2 \times ((2^{29} + T_6) \times 2 + 2^{30}) = 2^{34.88}$
4-10	$T_4 = 2 \times ((2^{31} + T_5) \times 2 + 2^{32}) = 2^{37.06}$
3-10	$T_3 = 2 \times ((2^{33} + T_4) \times 2 + 2^{34}) = 2^{39.22}$
2-10	$T_2 = 2 \times ((2^{35} \times 3 + T_3) \times 2 + 2^{37}) = 2^{41.56}$

So in total, the time is $2^{41.56} \times 2^4 + 2^{42} \approx 2^{45.68}$. The memory is about $\mathcal{O}(2^{42})$ counters.

Compress the ciphertexts: (Procedure Simon128-Tail) Since the input active bits and output active bits in the linear hull distinguisher for Simon128 are one-to-one, the representation for $X_{L,60}^{i+41} \oplus X_{R,2}^{i+41} \oplus X_{R,58}^{i+41} \oplus X_{R,62}^{i+41}$ expanding four rounds (see Table 16) are same with that for $X_{L,2}^{i} \oplus X_{L,58}^{i} \oplus X_{L,62}^{i} \oplus X_{R,60}^{i}$. So at first compress the ciphertexts into a counter vector $V[x_1 - x_{42}]$, then do as Procedure Simon128-Head.

49-round attack on Simon128/128. We add four rounds before and after the 41-round linear hull distinguisher to attack 49-round Simon128/K. We use $N = 2\bar{\epsilon}^{-2} = 2^{127.6}$ known plaintexts. Set advantage $a = 8$. The success probability would be 0.477. At first, compress the plaintext-ciphertext pairs to 2^{38+38} counters according to Table 15 and Table 16. Suppose the plaintext be compressed to x_P and ciphertext be compressed to x_C.

1. For each of 2^{38} x_C
   (a) Call Procedure Simon128-Head, and store the keys used in the first four rounds
2. For each of 2^{42} keys involved in the first four rounds
   (a) Call Procedure Simon128-Tail, and store the keys used in the last four rounds

3. Rank the keys and exhaustive the candidates with the help of key schedule.

Time: 1. $2^{38} \times 2^{45.68} = 2^{83.68}$ additions. 2. $2^{42} \times 2^{45.68} = 2^{87.68}$. So the total time to compute the bias is $2^{83.68} + 2^{87.68} \approx 2^{87.77}$ 3. The exhaustive phase needs $2^{128-8} = 2^{120}$ 49-round encryptions.

51-round attack on Simon128/192. We add five rounds before and after the 41-round linear hull distinguisher to attack 51-round Simon128/K. Compared with the 49-round attack, we expand one more round at each side. To get the x represented in Table 15, we should know the $0, 2, 26, 30, 32-34, 36-63$ bits (35 bits) of X_L^{i-5} and the $1, 34, 38, 40-42, 44-59, 61-63$ bits (25 bits) of X_R^{i-5}. Notice that the input parity bit of the linear hull is linear with $X_{L,2}^{i-5}$ and this bit can be compressed at first. So we can compress the plaintexts into one counter vector with $2^{34+25} = 2^{59}$ elements. The key bits involved in round $i-5$ are the $0, 26, 30, 32-34, 36-63$ (34 bits) of K^{i-5}. Similarly, we can compress the ciphertexts to a counter vector with 2^{59} elements and there are 34 bits of K^{i+45} involved. So, at first, we compress the the plaintext-ciphertext pairs to a counter vector of size $2^{59+59} = 2^{118}$.

1. Guess the 2^{34} bits of K^{i-5}
   (a) Encrypt the plaintexts by one round and compress the states into a counter vector of size $2^{38+59} = 2^{97}$
2. Guess the 2^{34} bits of K^{i+45}
   (a) Decrypt the ciphertexts by one round and compress the states into a counter vector of size $2^{38+38} = 2^{76}$
3. Do as Step 1 and 2 in the 49-round attack
4. Rank the keys and exhaustive the candidates with the help of key schedule.

Time: 1. $2^{118} \times 2^{34} = 2^{152}$ one-round encryptions. 2. $2^{97} \times 2^{34+34} = 2^{165}$ one-round encryptions. 3. $2^{68} \times 2^{87.77} = 2^{155.77}$ additions. So the total time to compute the bias is $2^{152} + 2^{165} \approx 2^{165}$ one-round encryptions and $2^{155.77}$ additions, which is approximately equal to 2^{165} one-round encryptions. 4. The exhaustive phase needs $2^{192-8} = 2^{184}$ 51-round encryptions.

53-round attack on Simon128/256. We add six rounds before and after the 41-round linear hull distinguisher to attack 53-round Simon128/K. Compared with the 51-round attack, we expand one more round at each side. The $1, 18, 22, 24-26, 28-63$ bits (42 bits) of K^{i-6} and K^{i+45} are involved in the attack.

1. Guess the 2^{42+42} bits of K^{i-6}, K^{i+46} involved
   (a) Encrypt the plaintexts by one round and decrypt the corresponding ciphertext by one round
2. Do as Step 1-3 in the 51-round attack
3. Rank the keys and exhaustive the candidates with the help of key schedule.

Time: 1. $2^{127.6} \times 2^{84} = 2^{211.6}$ two-round encryptions. 2. $2^{165} \times 2^{84} = 2^{249}$ one-round encryptions. So the total time to compute the bias is about 2^{249} one-round encryptions. 3. Since $K = 256$, the exhaustive phase needs $2^{256-8} = 2^{248}$ 53-round encryptions.

Table 15. 4 rounds beofre $X^i_{L,2} \oplus X^i_{L,58} \oplus X^i_{L,62} \oplus X^i_{R,60}$ for SIMON128

x_0	$X^{i-4}_{L,2} \oplus X^{i-4}_{L,50} \oplus X^{i-4}_{R,52} \oplus (X^{i-4}_{L,51} \& X^{i-4}_{L,44}) \oplus X^{i-4}_{L,54} \oplus X^{i-4}_{L,58}$	k_0	$K^{i-4}_{52} \oplus K^{i-2}_{0} \oplus K^{i-3}_{2} \oplus K^{i-3}_{54} \oplus K^{i-2}_{56}$ $\oplus K^{i-3}_{58} \oplus K^{i-1}_{2} \oplus k^{i-1}_{58} \oplus K^{i-1}_{62}$
x_1	$X^{i-4}_{L,63} \oplus X^{i-4}_{R,1} \oplus (X^{i-4}_{L,0} \& X^{i-4}_{L,57})$	k_1	K^{i-4}_{1}
x_2	$X^{i-4}_{L,56} \oplus X^{i-4}_{R,58} \oplus (X^{i-4}_{L,57} \& X^{i-4}_{L,50})$	k_2	K^{i-4}_{58}
x_3	$X^{i-4}_{L,51} \oplus X^{i-4}_{R,53} \oplus (X^{i-4}_{L,52} \& X^{i-4}_{L,45})$	k_3	K^{i-4}_{53}
x_4	$X^{i-4}_{L,44} \oplus X^{i-4}_{R,46} \oplus (X^{i-4}_{L,45} \& X^{i-4}_{L,38})$	k_4	K^{i-4}_{46}
x_5	$X^{i-4}_{L,55} \oplus X^{i-4}_{R,57} \oplus (X^{i-4}_{L,56} \& X^{i-4}_{L,49})$	k_5	K^{i-4}_{57}
x_6	$X^{i-4}_{L,48} \oplus X^{i-4}_{R,50} \oplus (X^{i-4}_{L,49} \& X^{i-4}_{L,42})$	k_6	K^{i-4}_{50}
x_7	$X^{i-4}_{L,59} \oplus X^{i-4}_{R,61} \oplus (X^{i-4}_{L,60} \& X^{i-4}_{L,53}) \oplus X^{i-4}_{L,63}$	k_7	$K^{i-4}_{61} \oplus K^{i-3}_{63}$
x_8	$X^{i-4}_{L,60} \oplus X^{i-4}_{R,62} \oplus (X^{i-4}_{L,61} \& X^{i-4}_{L,54})$	k_8	K^{i-4}_{62}
x_9	$X^{i-4}_{L,53} \oplus X^{i-4}_{R,55} \oplus (X^{i-4}_{L,54} \& X^{i-4}_{L,47})$	k_9	K^{i-4}_{55}
x_{10}	$X^{i-4}_{L,52} \oplus X^{i-4}_{R,54} \oplus (X^{i-4}_{L,53} \& X^{i-4}_{L,46}) \oplus X^{i-4}_{L,56}$	k_{10}	$K^{i-4}_{54} \oplus K^{i-3}_{56}$
x_{11}	$X^{i-4}_{L,46} \oplus X^{i-4}_{R,48} \oplus (X^{i-4}_{L,47} \& X^{i-4}_{L,40})$	k_{11}	K^{i-4}_{48}
x_{12}	$X^{i-4}_{L,44} \oplus X^{i-4}_{R,46} \oplus (X^{i-4}_{L,45} \& X^{i-4}_{L,38}) \oplus X^{i-4}_{L,48}$	k_{12}	$K^{i-4}_{46} \oplus K^{i-3}_{48}$
x_{13}	$X^{i-4}_{L,45} \oplus X^{i-4}_{R,47} \oplus (X^{i-4}_{L,46} \& X^{i-4}_{L,39})$	k_{13}	K^{i-4}_{47}
x_{14}	$X^{i-4}_{L,38} \oplus X^{i-4}_{R,40} \oplus (X^{i-4}_{L,39} \& X^{i-4}_{L,32})$	k_{14}	K^{i-4}_{40}
x_{15}	$X^{i-4}_{L,51} \oplus X^{i-4}_{R,53} \oplus (X^{i-4}_{L,52} \& X^{i-4}_{L,45}) \oplus X^{i-4}_{L,55}$	k_{15}	$K^{i-4}_{53} \oplus K^{i-3}_{55}$
x_{16}	$X^{i-4}_{L,52} \oplus X^{i-4}_{R,54} \oplus (X^{i-4}_{L,53} \& X^{i-4}_{L,46})$	k_{16}	K^{i-4}_{54}
x_{17}	$X^{i-4}_{L,59} \oplus X^{i-4}_{R,61} \oplus (X^{i-4}_{L,60} \& X^{i-4}_{L,53}) \oplus X^{i-4}_{R,1} \oplus (X^{i-4}_{L,0} \& X^{i-4}_{L,57})$	k_{17}	$K^{i-4}_{1} \oplus K^{i-4}_{61} \oplus K^{i-3}_{63} \oplus K^{i-2}_{1}$
x_{18}	$X^{i-4}_{L,60} \oplus X^{i-4}_{R,62} \oplus (X^{i-4}_{L,61} \& X^{i-4}_{L,54}) \oplus X^{i-4}_{L,0}$	k_{18}	$K^{i-4}_{62} \oplus K^{i-3}_{0}$
x_{19}	$X^{i-4}_{L,61} \oplus X^{i-4}_{R,63} \oplus (X^{i-4}_{L,62} \& X^{i-4}_{L,55})$	k_{19}	K^{i-4}_{63}
x_{20}	$X^{i-4}_{L,54} \oplus X^{i-4}_{R,56} \oplus (X^{i-4}_{L,55} \& X^{i-4}_{L,48})$	k_{20}	K^{i-4}_{56}
x_{21}	$X^{i-4}_{L,53} \oplus X^{i-4}_{R,55} \oplus (X^{i-4}_{L,54} \& X^{i-4}_{L,47}) \oplus X^{i-4}_{L,57}$	k_{21}	$K^{i-4}_{55} \oplus K^{i-3}_{57}$
x_{22}	$X^{i-4}_{L,47} \oplus X^{i-4}_{R,49} \oplus (X^{i-4}_{L,48} \& X^{i-4}_{L,41})$	k_{22}	K^{i-4}_{49}
x_{23}	$X^{i-4}_{L,52} \oplus X^{i-4}_{R,54} \oplus (X^{i-4}_{L,53} \& X^{i-4}_{L,46}) \oplus X^{i-4}_{R,58} \oplus (X^{i-4}_{L,57} \& X^{i-4}_{L,50})$	k_{23}	$K^{i-4}_{54} \oplus K^{i-4}_{58} \oplus K^{i-3}_{56} \oplus K^{i-2}_{58}$
x_{24}	$X^{i-4}_{L,46} \oplus X^{i-4}_{R,48} \oplus (X^{i-4}_{L,47} \& X^{i-4}_{L,40}) \oplus X^{I-4}_{L,50}$	k_{24}	$K^{i-4}_{48} \oplus K^{i-3}_{50}$
x_{25}	$X^{i-4}_{L,40} \oplus X^{i-4}_{R,42} \oplus (X^{i-4}_{L,41} \& X^{i-4}_{L,34})$	k_{25}	K^{i-4}_{42}
x_{26}	$X^{i-4}_{L,51} \oplus X^{i-4}_{R,53} \oplus (X^{i-4}_{L,52} \& X^{i-4}_{L,45}) \oplus X^{i-4}_{R,57} \oplus (X^{i-4}_{L,56} \& X^{i-4}_{L,49})$	k_{26}	$K^{i-4}_{53} \oplus K^{i-4}_{57} \oplus K^{i-3}_{55} \oplus K^{i-2}_{57}$
x_{27}	$X^{i-4}_{L,45} \oplus X^{i-4}_{R,47} \oplus (X^{i-4}_{L,46} \& X^{i-4}_{L,39}) \oplus X^{i-4}_{L,49}$	k_{27}	$K^{i-4}_{49} \oplus K^{i-3}_{49}$
x_{28}	$X^{i-4}_{L,39} \oplus X^{i-4}_{R,41} \oplus (X^{i-4}_{L,40} \& X^{i-4}_{L,33})$	k_{28}	K^{i-4}_{41}
x_{29}	$X^{i-4}_{L,44} \oplus X^{i-4}_{R,46} \oplus (X^{i-4}_{L,45} \& X^{i-4}_{L,38}) \oplus X^{i-4}_{R,50} \oplus (X^{i-4}_{L,49} \& X^{i-4}_{L,42})$	k_{29}	$K^{i-4}_{46} \oplus K^{i-4}_{50} \oplus K^{i-3}_{48} \oplus K^{i-2}_{50}$
x_{30}	$X^{i-4}_{L,38} \oplus X^{i-4}_{R,40} \oplus (X^{i-4}_{L,39} \& X^{i-4}_{L,32}) \oplus X^{i-4}_{L,42}$	k_{30}	$K^{i-4}_{40} \oplus K^{i-3}_{42}$
x_{31}	$X^{i-4}_{L,32} \oplus X^{i-4}_{R,34} \oplus (X^{i-4}_{L,33} \& X^{i-4}_{L,26})$	k_{31}	K^{i-4}_{34}
x_{32}	$X^{i-4}_{L,55} \oplus X^{i-4}_{R,57} \oplus (X^{i-4}_{L,56} \& X^{i-4}_{L,49}) \oplus X^{i-4}_{R,61} \oplus (X^{i-4}_{L,60} \& X^{i-4}_{L,53})$	k_{32}	$K^{i-4}_{57} \oplus K^{i-4}_{61} \oplus K^{i-3}_{59} \oplus K^{i-2}_{61}$
x_{33}	$X^{i-4}_{L,49} \oplus X^{i-4}_{R,51} \oplus (X^{i-4}_{L,50} \& X^{i-4}_{L,43})$	k_{33}	K^{i-4}_{51}
x_{34}	$X^{i-4}_{L,56} \oplus X^{i-4}_{R,58} \oplus (X^{i-4}_{L,57} \& X^{i-4}_{L,50}) \oplus X^{i-4}_{L,60}$	k_{34}	$K^{i-4}_{58} \oplus K^{i-3}_{60}$
x_{35}	$X^{i-4}_{L,57} \oplus X^{i-4}_{R,59} \oplus (X^{i-4}_{L,58} \& X^{i-4}_{L,51})$	k_{35}	K^{i-4}_{59}
x_{36}	$X^{i-4}_{L,50} \oplus X^{i-4}_{R,52} \oplus (X^{i-4}_{L,51} \& X^{i-4}_{L,44})$	k_{36}	K^{i-4}_{52}
x_{37}	$X^{i-4}_{L,49} \oplus X^{i-4}_{R,51} \oplus (X^{i-4}_{L,50} \& X^{i-4}_{L,43}) \oplus X^{i-4}_{L,53}$	k_{37}	$K^{i-4}_{51} \oplus K^{i-3}_{53}$
x_{38}	$X^{i-4}_{L,43} \oplus X^{i-4}_{R,45} \oplus (X^{i-4}_{L,44} \& X^{i-4}_{L,37})$	k_{38}	K^{i-4}_{45}
x_{39}	$X^{i-4}_{L,48} \oplus X^{i-4}_{R,50} \oplus (X^{i-4}_{L,49} \& X^{i-4}_{L,42}) \oplus X^{i-4}_{R,54} \oplus (X^{i-4}_{L,53} \& X^{i-4}_{L,46})$	k_{39}	$K^{i-4}_{50} \oplus K^{i-4}_{54} \oplus K^{i-3}_{52} \oplus K^{i-2}_{54}$
x_{40}	$X^{i-4}_{L,42} \oplus X^{i-4}_{R,44} \oplus (X^{i-4}_{L,43} \& X^{i-4}_{L,36})$	k_{40}	K^{i-4}_{44}
x_{41}	$X^{i-4}_{L,42} \oplus X^{i-4}_{R,44} \oplus (X^{i-4}_{L,43} \& X^{i-4}_{L,36}) \oplus X^{i-4}_{L,46}$	k_{41}	$K^{i-4}_{44} \oplus K^{i-3}_{46}$
x_{42}	$X^{i-4}_{L,36} \oplus X^{i-4}_{R,38} \oplus (X^{i-4}_{L,37} \& X^{i-4}_{L,30})$	k_{42}	K^{i-4}_{38}

Notice: $x_{17} = x_1 \oplus x_7, x_{23} = x_2 \oplus x_{10}, x_{26} = x_5 \oplus x_{15}, x_{29} = x_6 \oplus x_{12}$

Table 16. 4 rounds after $X_{L,60}^{i+41} \oplus X_{R,2}^{i+41} \oplus X_{R,58}^{i+41} \oplus X_{R,62}^{i+41}$ for Simon128

x_0	$X_{R,2}^{i+44} \oplus X_{R,50}^{i+44} \oplus X_{L,52}^{i+44} \oplus (X_{R,51}^{i+44} \& X_{R,44}^{i+44}) \oplus X_{R,54}^{i+44} \oplus X_{R,58}^{i+44}$	k_0	$K_{52}^{i+44} \oplus K_0^{i+42} \oplus K_2^{i+43} \oplus K_{54}^{i+43} \oplus K_{56}^{i+42}$ $\oplus K_{58}^{i+43} \oplus K_2^{i+41} \oplus k_{58}^{i+41} \oplus K_{62}^{i+41}$
x_1	$X_{R,63}^{i+44} \oplus X_{L,1}^{i+44} \oplus (X_{R,0}^{i+44} \& X_{R,57}^{i+44})$	k_1	K_1^{i+44}
x_2	$X_{R,56}^{i+44} \oplus X_{L,58}^{i+44} \oplus (X_{R,57}^{i+44} \& X_{R,50}^{i+44})$	k_2	K_{58}^{i+44}
x_3	$X_{R,51}^{i+44} \oplus X_{L,53}^{i+44} \oplus (X_{R,52}^{i+44} \& X_{R,45}^{i+44})$	k_3	K_{53}^{i+44}
x_4	$X_{R,44}^{i+44} \oplus X_{L,46}^{i+44} \oplus (X_{R,45}^{i+44} \& X_{R,38}^{i+44})$	k_4	K_{46}^{i+44}
x_5	$X_{R,55}^{i+44} \oplus X_{L,57}^{i+44} \oplus (X_{R,56}^{i+44} \& X_{R,49}^{i+44})$	k_5	K_{57}^{i+44}
x_6	$X_{R,48}^{i+44} \oplus X_{L,50}^{i+44} \oplus (X_{R,49}^{i+44} \& X_{R,42}^{i+44})$	k_6	K_{50}^{i+44}
x_7	$X_{R,59}^{i+44} \oplus X_{L,61}^{i+44} \oplus (X_{R,60}^{i+44} \& X_{R,53}^{i+44}) \oplus X_{R,63}^{i+44}$	k_7	$K_{61}^{i+44} \oplus K_{63}^{i+43}$
x_8	$X_{R,60}^{i+44} \oplus X_{L,62}^{i+44} \oplus (X_{R,61}^{i+44} \& X_{R,54}^{i+44})$	k_8	K_{62}^{i+44}
x_9	$X_{R,53}^{i+44} \oplus X_{L,55}^{i+44} \oplus (X_{R,54}^{i+44} \& X_{R,47}^{i+44})$	k_9	K_{55}^{i+44}
x_{10}	$X_{R,52}^{i+44} \oplus X_{L,54}^{i+44} \oplus (X_{R,53}^{i+44} \& X_{R,46}^{i+44}) \oplus X_{R,56}^{i+44}$	k_{10}	$K_{54}^{i+44} \oplus K_{56}^{i+43}$
x_{11}	$X_{R,46}^{i+44} \oplus X_{L,48}^{i+44} \oplus (X_{R,47}^{i+44} \& X_{R,40}^{i+44})$	k_{11}	K_{48}^{i+44}
x_{12}	$X_{R,44}^{i+44} \oplus X_{L,46}^{i+44} \oplus (X_{R,45}^{i+44} \& X_{R,38}^{i+44}) \oplus X_{R,48}^{i+44}$	k_{12}	$K_{46}^{i+44} \oplus K_{48}^{i+43}$
x_{13}	$X_{R,45}^{i+44} \oplus X_{L,47}^{i+44} \oplus (X_{R,46}^{i+44} \& X_{R,39}^{i+44})$	k_{13}	K_{47}^{i+44}
x_{14}	$X_{R,38}^{i+44} \oplus X_{L,40}^{i+44} \oplus (X_{R,39}^{i+44} \& X_{R,32}^{i+44})$	k_{14}	K_{40}^{i+44}
x_{15}	$X_{R,51}^{i+44} \oplus X_{L,53}^{i+44} \oplus (X_{R,52}^{i+44} \& X_{R,45}^{i+44}) \oplus X_{R,55}^{i+44}$	k_{15}	$K_{53}^{i+44} \oplus K_{55}^{i+43}$
x_{16}	$X_{R,52}^{i+44} \oplus X_{L,54}^{i+44} \oplus (X_{R,53}^{i+44} \& X_{R,46}^{i+44})$	k_{16}	K_{54}^{i+44}
x_{17}	$X_{R,59}^{i+44} \oplus X_{L,61}^{i+44} \oplus (X_{R,60}^{i+44} \& X_{R,53}^{i+44}) \oplus X_{L,1}^{i+44} \oplus (X_{R,0}^{i+44} \& X_{R,57}^{i+44})$	k_{17}	$K_1^{i+44} \oplus K_{61}^{i+44} \oplus K_{63}^{i+43} \oplus K_1^{i+42}$
x_{18}	$X_{R,60}^{i+44} \oplus X_{L,62}^{i+44} \oplus (X_{R,61}^{i+44} \& X_{R,54}^{i+44}) \oplus X_{R,0}^{i+44}$	k_{18}	$K_{62}^{i+44} \oplus K_0^{i+43}$
x_{19}	$X_{R,61}^{i+44} \oplus X_{L,63}^{i+44} \oplus (X_{R,62}^{i+44} \& X_{R,55}^{i+44})$	k_{19}	K_{63}^{i+44}
x_{20}	$X_{R,54}^{i+44} \oplus X_{L,56}^{i+44} \oplus (X_{R,55}^{i+44} \& X_{R,48}^{i+44})$	k_{20}	K_{56}^{i+44}
x_{21}	$X_{R,53}^{i+44} \oplus X_{L,55}^{i+44} \oplus (X_{R,54}^{i+44} \& X_{R,47}^{i+44}) \oplus X_{R,57}^{i+44}$	k_{21}	$K_{55}^{i+44} \oplus K_{57}^{i+43}$
x_{22}	$X_{R,47}^{i+44} \oplus X_{L,49}^{i+44} \oplus (X_{R,48}^{i+44} \& X_{R,41}^{i+44})$	k_{22}	K_{49}^{i+44}
x_{23}	$X_{R,52}^{i+44} \oplus X_{L,54}^{i+44} \oplus (X_{R,53}^{i+44} \& X_{R,46}^{i+44}) \oplus X_{L,58}^{i+44} \oplus (X_{R,57}^{i+44} \& X_{R,50}^{i+44})$	k_{23}	$K_{54}^{i+44} \oplus K_{58}^{i+44} \oplus K_{56}^{i+43} \oplus K_{58}^{i+42}$
x_{24}	$X_{R,46}^{i+44} \oplus X_{L,48}^{i+44} \oplus (X_{R,47}^{i+44} \& X_{R,40}^{i+44}) \oplus X_{R,50}^{i+44}$	k_{24}	$K_{48}^{i+44} \oplus K_{50}^{i+43}$
x_{25}	$X_{R,40}^{i+44} \oplus X_{L,42}^{i+44} \oplus (X_{R,41}^{i+44} \& X_{R,34}^{i+44})$	k_{25}	K_{42}^{i+44}
x_{26}	$X_{R,51}^{i+44} \oplus X_{L,53}^{i+44} \oplus (X_{R,52}^{i+44} \& X_{R,45}^{i+44}) \oplus X_{L,57}^{i+44} \oplus (X_{R,56}^{i+44} \& X_{R,49}^{i+44})$	k_{26}	$K_{53}^{i+44} \oplus K_{57}^{i+44} \oplus K_{55}^{i+43} \oplus K_{57}^{i+42}$
x_{27}	$X_{R,45}^{i+44} \oplus X_{L,47}^{i+44} \oplus (X_{R,46}^{i+44} \& X_{R,39}^{i+44}) \oplus X_{R,49}^{i+44}$	k_{27}	$K_{49}^{i+44} \oplus K_{49}^{i+43}$
x_{28}	$X_{R,39}^{i+44} \oplus X_{L,41}^{i+44} \oplus (X_{R,40}^{i+44} \& X_{R,33}^{i+44})$	k_{28}	K_{41}^{i+44}
x_{29}	$X_{R,44}^{i+44} \oplus X_{L,46}^{i+44} \oplus (X_{R,45}^{i+44} \& X_{R,38}^{i+44}) \oplus X_{L,50}^{i+44} \oplus (X_{R,49}^{i+44} \& X_{R,42}^{i+44})$	k_{29}	$K_{46}^{i+44} \oplus K_{50}^{i+44} \oplus K_{48}^{i+43} \oplus K_{50}^{i+42}$
x_{30}	$X_{R,38}^{i+44} \oplus X_{L,40}^{i+44} \oplus (X_{R,39}^{i+44} \& X_{R,32}^{i+44}) \oplus X_{R,42}^{i+44}$	k_{30}	$K_{40}^{i+44} \oplus K_{42}^{i+43}$
x_{31}	$X_{R,32}^{i+44} \oplus X_{L,34}^{i+44} \oplus (X_{R,33}^{i+44} \& X_{R,26}^{i+44})$	k_{31}	K_{34}^{i+44}
x_{32}	$X_{R,55}^{i+44} \oplus X_{L,57}^{i+44} \oplus (X_{R,56}^{i+44} \& X_{R,49}^{i+44}) \oplus X_{L,61}^{i+44} \oplus (X_{R,60}^{i+44} \& X_{R,53}^{i+44})$	k_{32}	$K_{57}^{i+44} \oplus K_{61}^{i+44} \oplus K_{59}^{i+43} \oplus K_{61}^{i+42}$
x_{33}	$X_{R,49}^{i+44} \oplus X_{L,51}^{i+44} \oplus (X_{R,50}^{i+44} \& X_{R,43}^{i+44})$	k_{33}	K_{51}^{i+44}
x_{34}	$X_{R,56}^{i+44} \oplus X_{L,58}^{i+44} \oplus (X_{R,57}^{i+44} \& X_{R,50}^{i+44}) \oplus X_{R,60}^{i+44}$	k_{34}	$K_{58}^{i+44} \oplus K_{60}^{i+43}$
x_{35}	$X_{R,57}^{i+44} \oplus X_{L,59}^{i+44} \oplus (X_{R,58}^{i+44} \& X_{R,51}^{i+44})$	k_{35}	K_{59}^{i+44}
x_{36}	$X_{R,50}^{i+44} \oplus X_{L,52}^{i+44} \oplus (X_{R,51}^{i+44} \& X_{R,44}^{i+44})$	k_{36}	K_{52}^{i+44}
x_{37}	$X_{R,49}^{i+44} \oplus X_{L,51}^{i+44} \oplus (X_{R,50}^{i+44} \& X_{R,43}^{i+44}) \oplus X_{R,53}^{i+44}$	k_{37}	$K_{51}^{i+44} \oplus K_{53}^{i+43}$
x_{38}	$X_{R,43}^{i+44} \oplus X_{L,45}^{i+44} \oplus (X_{R,44}^{i+44} \& X_{R,37}^{i+44})$	k_{38}	K_{45}^{i+44}
x_{39}	$X_{R,48}^{i+44} \oplus X_{L,50}^{i+44} \oplus (X_{R,49}^{i+44} \& X_{R,42}^{i+44}) \oplus X_{L,54}^{i+44} \oplus (X_{R,53}^{i+44} \& X_{R,46}^{i+44})$	k_{39}	$K_{50}^{i+44} \oplus K_{54}^{i+44} \oplus K_{52}^{i+43} \oplus K_{54}^{i+42}$
x_{40}	$X_{R,42}^{i+44} \oplus X_{L,44}^{i+44} \oplus (X_{R,43}^{i+44} \& X_{R,36}^{i+44})$	k_{40}	K_{44}^{i+44}
x_{41}	$X_{R,42}^{i+44} \oplus X_{L,44}^{i+44} \oplus (X_{R,43}^{i+44} \& X_{R,36}^{i+44}) \oplus X_{R,46}^{i+44}$	k_{41}	$K_{44}^{i+44} \oplus K_{46}^{i+43}$
x_{42}	$X_{R,36}^{i+44} \oplus X_{L,38}^{i+44} \oplus (X_{R,37}^{i+44} \& X_{R,30}^{i+44})$	k_{42}	K_{38}^{i+44}

Notice: $x_{17} = x_1 \oplus x_7, x_{23} = x_2 \oplus x_{10}, x_{26} = x_5 \oplus x_{15}, x_{29} = x_6 \oplus x_{12}$