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

Lingyue Qin[1] and Huaifeng Chen[2]

[1] Department of Computer Science and Technology, Tsinghua Universtiy,
Beijing 100084, China
qly14@mails.tsinghua.edu.cn

[2] Key Laboratory of Cryptologic Technology and Information Security,
Ministry of Education, Shandong University, Jinan 250100, China
hfchen@mail.sdu.edu.cn

Abstract. Simeck is a new family of lightweight block ciphers proposed by Yang *et al.* in CHES'15, which has efficient hardware implementation. In this paper, we find differentials with low hamming weight and high probability for Simeck using Kölbl's tool, then we consider the links between the differential and linear characteristic to construct linear hulls for Simeck. We give improved linear hull attack with dynamic key-guessing techniques on Simeck according to the property of the AND operation. Our best results cover Simeck 32/64 reduced to 23 rounds, Simeck 48/96 reduced to 30 rounds, Simeck 64/128 reduced to 37 rounds. Our result is the best known so far for any variant of Simeck.

KeyWords: Simeck, Linear Cryptanalysis, Differential Cryptanalysis, Linear Hull, Dynamic Key-guessing

1 Introduction

Simeck is a new family of lightweight block ciphers proposed in CHES'15 by Yang, Zhu, Suder, Aagaard and Gongbased in [19]. They combined the Simon and Speck block ciphers designed by NSA in [8] to design Simeck, and used a different set of rotation constants of Simon's round function and the key schedule of Speck. The round function of Simeck contains the AND operation, left rotation and the XOR operation, leading to a more compact and efficient implementation in hardware. The Simeck family has three variants with different block size and key size, including Simeck32/64, Simeck48/96, Simeck64/128.

Related Works. Many cryptanalysis techniques of Simon can be used to attack the Simeck due to their similarity, including differential [2][5][9], linear [3][14] cryptanalysis and so on. Wang *et al.* in [18] improved the differential attack results by dynamic key-guessing techniques. Then Chen *et al.* according the dynamic key-guessing techniques in the linear hull cryptanalysis of Simon [10], applied the GUESS, SPLIT and COMBINE techniques to decrease the time complexity in the calculation of the empirical correlations. They can attack one or two more rounds than Wang *et al.*'s results.

For Simeck, there are only a few cryptanalysis results so far. Kölbl *et al.* in [12] compared the Simon and Simeck on the lower bounds of differential and linear characteristic and presented some differentials for Simeck. Based on the differentials, they can recover the key for 19/26/33 rounds for Simeck32/48/64. Bagheri *et al.* in [7] analyzed Simeck's security against linear cryptanalysis. With Matsui's algorithm 2, they can attack 18/23/27 rounds for Simeck32/48/64. Zhang *et al.* evaluated the security on 20/24/27 rounds of Simeck32/48/64 against Zero Correlation Linear cryptanalysis. Qiao *et al.* in [16] used the dynamic key-guessing techniques to attack Simeck and improved the previously best results on all versions of Simeck by 2 rounds.

Table 1: Summary of cryptanalysis results on Simeck

cipher	round	Data Complexity	Time Complexity	Reference
Simeck32/64	18	2^{31}	$2^{63.5}$	[7]
	19	2^{31}	2^{36}	[12]
	20	2^{32}	$2^{56.65}$	[20]
	22	2^{32}	$2^{57.9}$	[16]
	23	$2^{31.91}$	$2^{61.85}A$[a]$+ 2^{56.41}E$[b]	section 4.2
Simeck48/96	24	2^{45}	2^{94}	[7]
	24	2^{48}	$2^{91.6}$	[20]
	26	2^{47}	2^{62}	[12]
	28	2^{46}	$2^{68.3}$	[16]
	30	$2^{47.66}$	$2^{92.26}A + 2^{88.04}E$	section 4.3
Simeck64/128	27	2^{61}	$2^{120.5}$	[7]
	27	2^{64}	$2^{112.79}$	[20]
	33	2^{63}	2^{96}	[12]
	35	2^{63}	$2^{116.3}$	[16]
	37	$2^{63.09}$	$2^{111.44}A + 2^{121.25}E$	section 4.4

[a] additions.

[b] encryption of attacked rounds.

Our contributions. In this paper, we analyze the security of Simeck against improved linear hull cryptanalysis with dynamic key-guessing techniques. We provide some linear hull distinguishers of the Simeck family according to the differentials searched by Kölbl's tool. Then we give the expressions for the parity bits of the distinguishers. With the GUESS, SPLIT and COMBINE techniques to reduce the time complexity in calculation of the correlations, we can attack 23/30/37 rounds of Simeck32/48/64.

This paper is organized as follows. Section 2 gives a brief description of the Simeck family. In section 3, we introduce the linear hulls transformed from the differentials searched by CryptoSMT. Then we give the dynamic key-guessing techniques and the key recovery attack on Simeck in section 4. Finally we conclude in section 5.

2 The Simeck family

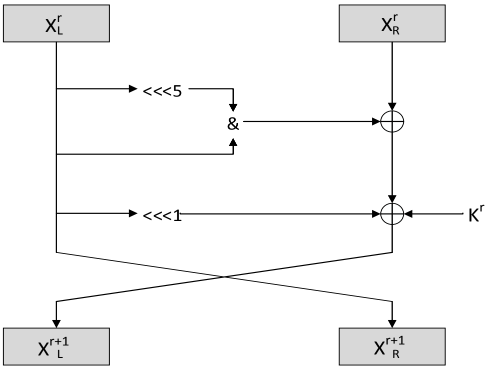
The lightweight block cipher Simeck family with Feistel structures is proposed in CHES'15. The Simeck family can be denoted as Simeck2n/mn, where 2n is the block size and mn is the key size. The n can be 16, 24 or 32 and the m is always 2, so there are three versions. The Simeck32/64 contains 32 rounds, Simeck48/96 contains 36 rounds and Simeck64/128 contains 44 rounds.

In this paper, we use the notations as follows:

X^r	2n bit output of round r
X_L^r	left half of X^r
X_R^r	right half of X^r
K^r	n bit subkey of round $r+1$
$X \lll i$	cycle shift of X to the left by i bits
$\oplus$	bitwise XOR
&	bitwise AND

Round function The round function of Simeck is described in Figure 1.The $(r+1)$ round's input is $(X_L^r \| X_R^r)$ and the output is $(X_L^{r+1} \| X_R^{r+1})$.

Fig. 1: The round function of Simeck



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

where $F(X) = ((X \lll 5) \& X) \oplus (X \lll 1)$. We can also describe the round function for single bit, which we use in the rest of the paper.

Let $X_L^r = \{X_{L,n-1}^r, X_{L,n-2}^r, ..., X_{L,0}^r\}$, $X_R^r = \{X_{R,n-1}^r, X_{R,n-2}^r, ..., X_{R,0}^r\}$, and the round function is denoted as:

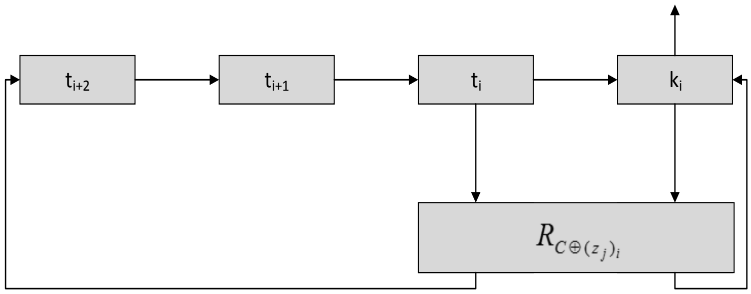
$$X_{L,i}^{r+1} = (X_{L,(i-5+n)\%n}^r \& X_{L,i}) \oplus (X_{L,(i-1+n)\%n}^r) \oplus X_{R,i}^r \oplus K_i^r$$
$$X_{R,i}^{r+1} = X_{L,i}^r$$

where $i = 0, 1, ..., n-1$, and $X_{L,0}^r$,$X_{R,0}^r$ is the LSB of X_L^r and X_R^r.
Key Schedules. The key schedule of Simeck is similar with Speck. We describe it briefly. To generate a sequence of round key $\{K^0, ..., K^{n_r-1}\}$ from the master key, we first initialize the states $\{t^2, t^1, t^0, K^0\}$ with the master key. Then we update the registers to generate the round keys used in all n_r round encryption. The updating process can be denoted as

$$k^{i+1} = t^i$$
$$t^{i+3} = F(t^i) \oplus K^i \oplus C \oplus (z_j)_i$$

where $0 \leq i \leq n_r - 1$, $C = 2^n - 4$, $(z_j)_i$ is the i-th bit of z_j.

Fig. 2: The key schedule of Simeck



3 The Linear cryptanalysis and Linear Hull

3.1 Linear cryptanalysis

We first give the calculation formula of correlation for boolean function. Let $g(x) : F_2^n \rightarrow F_2$ is a boolean function and $B(g) = \sum_{x \in F_2} (-1)^{g(x)}$, so the correlation $c(g)$ is

$$c(g) = \frac{1}{2^n} B(g) = \frac{1}{2^n} \sum_{x \in F_2} (-1)^{g(x)}$$

Then the bias of $g(x)$ is $\varepsilon(g) = \frac{1}{2} c(g)$. In the rest of the paper, we use the $B(g)$ as correlation for simplicity of description in some situations.

Linear cryptanalysis [13] is an important known plaintext cryptanalytic techniques, and it tries to find a highly probable expression with plaintexts P, ciphertexts C and key bits K as follows:

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

where α, β, γ are masks. The bias of the expression is $\varepsilon(\alpha \cdot P \oplus \beta \cdot C \oplus \gamma \cdot K)$, so at least $O(\frac{1}{\varepsilon^2})$ planitexts are needed to recovery the key.

The linear hull [15] is a set of linear approximations with the same input mask and output mask, and the potential of a linear hull with mask α and β is

$$ALH(\alpha, \beta) = \sum\nolimits_{\gamma} \varepsilon^2(\alpha \cdot P \oplus \beta \cdot C \oplus \gamma \cdot K) = \bar{\varepsilon}^2$$

Notice the $\bar{\varepsilon}^2$ may be higher than ε^2 in most situations, so there needs less plaintexts in linear hull cryptanalysis.

In the round function of Simeck, the only nonlinear operation is the AND operation. For single bit x and y, the probability of $(x \& y) = 0$ is $\frac{3}{4}$. So we can get the approximation expressions of the round function $F(X)$, then extract the expression to get a linear approximation for more rounds.

$$\begin{array}{l}
\text{Approxiamtion1}: \Pr[(F(X))_i = (X)_{i-1}] = \frac{3}{4} \\
\text{Approxiamtion2}: \Pr[(F(X))_i = (X)_{i-1} \oplus (X)_i] = \frac{3}{4} \\
\text{Approxiamtion3}: \Pr[(F(X))_i = (X)_{i-1} \oplus (X)_{i-5}] = \frac{3}{4} \\
\text{Approxiamtion4}: \Pr[(F(X))_i = (X)_{i-1} \oplus (X)_i \oplus (X)_{i-5}] = \frac{1}{4}
\end{array}$$

3.2 Differential cryptanalysis

Differential cryptanalysis is a chosen plaintext/ciphertext cryptanalytic technique. In [11], Kölbl introduced a tool for cryptanalysis of symmetric primitives based on SMT/SAT solvers. They used the tool to find some differentials for Simeck and attacked the Simeck using differential cryptanalysis. We also use the tool to search the differentials which have a balance between low hamming weight and high probability to attack more rounds using less plaintexts. We get the differentials as follows.

Table 2: The differentials of Simeck

cipher	rounds	Δ_{in}	Δ_{out}	log_2diff
Simeck32/64	13	$(0x0, 0x2)$	$(0x2, 0x0)$	-28.91
Simeck48/96	20	$(0x400000, 0xA00000)$	$(0x400000, 0x200000)$	-43.66
Simeck64/128	26	$(0x0, 0x4400000)$	$(0x800000, 0x400000)$	-60.09

Like the linear cryptanalysis, considering the non-linear operation AND, we can extract the highly probable differential expressions of round function $F(X)$

as follows:

$$\begin{array}{l}\text{Differential Characteristic1} : \Pr\left[(\varDelta X))_i \rightarrow (\varDelta F(X))_{i+1}\right] = \frac{1}{2}\\ \text{Differential Characteristic2} : \Pr\left[(\varDelta X))_i \rightarrow (\varDelta F(X))_{i+1,i}\right] = \frac{1}{2}\\ \text{Differential Characteristic3} : \Pr\left[(\varDelta X))_i \rightarrow (\varDelta F(X))_{i+1,i+5}\right] = \frac{1}{2}\\ \text{Differential Characteristic4} : \Pr\left[(\varDelta X))_i \rightarrow (\varDelta F(X))_{i+1,i,i+5}\right] = \frac{1}{2}\end{array}$$

where the $(\varDelta F(X))_{i+1}$ denotes the $(i+1)$-th bit is 1 and the others are 0. In [3], Alizadeh *et al.* noticed each approximation of linear cryptanalysis can be mapped into a differential characteristic as above. So we can construct an equivalent linear characteristic from a differential characteristic.

3.3 Linear Hull

Alizadeh *etal.* in [4] used the connection between differential and linear characteristics to get linear hulls for SIMON. They also showed the relation between EDP of a differential and capacity $\bar{c}_{LH}$ of a system of linear hull

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

[1][6][17] gave other methods to find good linear hulls for Simon, including correlation matrix, Mixed Integer Programming (MIP) and so on. In this paper, we use the similar connection for Simeck to transform the differential characteristics to linear characteristics. The used approximations can been found above. The details for Simeck32/64 are listed in Table 3.

For Simeck48/96 and Simeck64/128, the details can been found in Appendix A. Now we have linear hulls for all versions of Simeck in Table 4.

4 Key Recovery Attack on Simeck

4.1 Linear compression and Dynamic key-guessing

To reduce the time complexity of calculating the correlation, we can compress the linear part of the function at first. Let $y = f(x,k)$ is a boolean function, and x is l_1 bits plaintexts, k is l_2 bits key, the counter $V[x]$ denotes the number of x. If $y = f(x,k) = x_0 \oplus k_0 \oplus f'(x',k')$, we can generate a new counter $V'[x'] = \sum_{x_0 \in F_2} (-1)^{x_0} V[x_0||x']$, so the correlation of y under some k guess is

$$B^k(y) = \sum\nolimits_x (-1)^{f(x,k)} V[x] \Rightarrow B^k(y) = (-1)^{k_0} \sum\nolimits_x' (-1)^{f(x',k')} V'[x']$$

Because the k_0 doesn't affect the absolute value of $B^k(y)$, the k_0 is called related bit and don't need to guess it. Then there needs $2^{l_1+l_2-2}$ computations, less than $2^{l_1+l_2}$. If $y = f(x,k)$ has multiple linear bits of x, k, we can also compress them as the above method.

In a further step, the dynamic key-guessing techniques can reduce the calculations. For $f = f_1(x_1,k_1) \& f_2(x_2,k_2)$, if we guess k_1 and according the value

Table 3: Linear characteristic based on the differential for Simeck32/64

	Differential		Linear		
r	Δ_L	Δ_R	X_L	X_R	$Used\ App$
0	$-$	1	1	$-$	$-$
1	1	$-$	$-$	1	1
2	2	1	1	0	1
3	$1,3$	2	0	$1,15$	$1\!:1$
4	4	$1,3$	$1,15$	14	1
5	$1,3,5$	4	14	$1,13,15$	$3\!:1\!:2$
6	$2,3$	$1,3,5$	$1,13,15$	$0,15$	$1:1$
7	$1,4,5$	$2,3$	$0,15$	$1,13,14$	$3:2:2$
8	$3,4$	$1,4,5$	$1,13,14$	$14,15$	$1:2$
9	$1,3$	$3,4$	$14,15$	$1,15$	$1:2$
10	2	$1,3$	$1,15$	0	1
11	1	2	0	1	1
12	$-$	1	1	$-$	$-$
13	1	$-$	$-$	1	$-$
	$\sum_r \log_2 pr = -38$ $\log_2 p_{diff} = -28.91$		$\log_2 \varepsilon^2 = -40$ $\log_2 \bar{c}^2_{LH} = -30.91$		

Table 4: The linear hulls for Simeck

cipher	round	Input Active bits	Output Active bits	ALH
Simeck32/64	13	$X^r_{L,1}$	$X^{r+13}_{R,1}$	-30.91
Simeck48/96	20	$X^r_{L,19}, X^r_{L,21}, X^r_{R,20}$	$X^{r+20}_{L,21}, X^{r+20}_{R,20}$	-45.66
Simeck64/128	26	$X^r_{L,18}, X^r_{L,22}$	$X^{r+26}_{L,22}, X^{r+26}_{R,21}$	-62.09

of $f_1(x_1, k_1)$ spilt the $x = x_1||x_2$ into two cases: $f_1(x_1, k_1) = 0$ or 1. When $f_1(x_1, k_1) = 0$, then $f = 0$ and we don't need to guess k_2, so the complexity can be reduced. Chen *et al.* in [10] called this technique as Guess, Split and Combine technique. We introduce the technique briefly as follows. In the calculations of $B^k(y) = \sum_x (-1)^{f(x,k)}V[x]$, let $k = k_G||k_A||k_B||k_C$ and guess the k_G at first, then we can split all the x into two sets S_A and S_B. For N_A values of $x \in S_A$, $f(x) = f_A(x, k_A||k_C)$, and For N_B values of $x \in S_B$, $f(x) = f_B(x, k_B||k_C)$, so

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

There needs $N_A\dot{2}^{l_2^G+l_2^A+l_2^C} + N_B\dot{2}^{l_2^G+l_2^B+l_2^C} + 2^{l_2}$ additions in the guess, spilt and combine process, which reduces the time complexity than $2^{l_1+l_2}$.

4.2 Key Recovery Attack on Simeck32/64

We use the 13 rounds linear hull obtained in section 3.3 to attack the Simeck32/64:

$$X^r_{L,1} \to X^{r+13}_{R,1}$$

The potential of this linear hull is $2^{-30.91}$, and our data complexity is $N = 2 * 2^{30.91} = 2^{31.91}$. We add four more rounds on the top and four more rounds at the bottom to get a 21-round distinguisher.

Table 5: Extend the linear hull to a 21-round distinguisher

r	Active bits in the left	Active bits in the right	Involved subkey bits	♯bits
$i-4$	$0, 1, 2, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15$	$0, 1, 2, 6, 7, 10, 11, 12$ $14, 15$	$0, 1, 2, 6, 7, 10, 11, 12$ $14, 15$	10
$i-3$	$0, 1, 2, 6, 7, 10, 11, 12, 14, 15$	$0, 1, 7, 11, 12, 15$	$0, 1, 7, 11, 12, 15$	6
$i-2$	$0, 1, 7, 11, 12, 15$	$0, 1, 12$	$0, 1, 12$	3
$i-1$	$0, 1, 12$	1	1	1
i	1	$-$	$-$	$-$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$i+13$	$-$	1	1	1
$i+14$	1	$0, 1, 12$	$0, 1, 12$	3
$i+15$	$0, 1, 12$	$0, 1, 7, 11, 12, 15$	$0, 1, 7, 11, 12, 15$	6
$i+16$	$0, 1, 7, 11, 12, 15$	$0, 1, 2, 6, 7, 10, 11, 12$ $14, 15$	$0, 1, 2, 6, 7, 10, 11, 12$ $14, 15$	10
$i+17$	$0, 1, 2, 6, 7, 10, 11, 12$ $14, 15$	$0, 1, 2, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15$	$-$	$-$

Consider the linear subkey bits as a whole, we can get the expression of $X^r_{L,1}$ or $X^{r+13}_{R,1}$ as follows:

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

where $x_{10} = x_3 \oplus x_5$ and $x_{15} = x_4 \oplus x_8$, so there are 15 independent variables of x and 17 independent variables of k. The x denotes the plaintext or ciphertext and the k denotes the subkey bit. We use x_p including$\{x_{p,0}, ..., x_{p,16}\}$ and k_p including $\{k_{p,0}, ..., k_{p,16}\}$ in the representation of $X^r_{L,1}$. For $X^{r+13}_{R,1}$, we use x_c and k_c.Then the $X^r_{L,1}$ can be denoted by $f(x_p, k_p)$ and the $X^{r+13}_{R,1}$ can be denoted by $f(x_c, k_c)$.(More details can be seen in Appendix A).

Let the plaintexts $P = X^{r-4}$ and the ciphertexts $C = X^{r+17}$. We can compress the N pairs P and C into a counter vector $V[x_p, x_c]$. Then we can get the correlation of N plaintext-ciphertext pairs under the subkey k_p and k_c:

$$\overline{c}_{k_p,k_c} = \frac{1}{N}\sum\nolimits_{x_p,x_c} (-1)^{f(x_p,k_p)\oplus f(x_c,k_c)} V[x_p, x_c]$$

As we can see, $f(x, k) = x_0 \oplus k_0 \oplus f(x', k')$ is linear with $x_0 \oplus k_0$. We compress the $x_{p,0}$ and $x_{c,0}$ at first to a new counter vector

$$V_1[x'_p, x'_c] = \sum\nolimits_{x_{p,0},x_{c,0}\in F_2} (-1)^{x_{p,0}\oplus x_{x,0}} V[x_p, x_c]$$

Then the correlation is

$$\overline{c}_{k'_p,k'_c} = \frac{1}{N}(-1)^{k_{p,0}\oplus k_{c,0}} \sum\nolimits_{x'_c} (-1)^{f(x'_c,k'_c)} \sum\nolimits_{x'_p} (-1)^{f(x'_p,k'_p)} V_1[x'_p, x'_c]$$

We first consider constant x'_c to calculate the $\sum_{x'_p} (-1)^{f'(x'_p,k'_p)} V_1[x'_p, x'_c]$ for all possible k'_p. Then we guess the k'_c to get the correlation. The problem becomes the calculation of $B^{k'}(y) = \sum_{x'} (-1)^{f'(x',k')} V'[x']$. (For the first process, the x' represent x'_p, k' represent k'_p, $V'[x']$ represent $V_1[x'_p, x'_c]$ and $y = f(x', k')$).

Procedure A

We use the guess, split and combine technique proposed in[7] to decrease the time complexity in the calculation of $B^{k'}(y) = \sum_{x'} (-1)^{f'(x',k')} V'[x']$. We can see there are only 14 independent variables for x' and 16 independent variables for x', because in $x' = \{x_1, ..., x_{16}\}$ there are $x_{10} = x_3 \oplus x_5, x_{15} = x_4 \oplus x_8$.

Step 1. First, we compress the $\{x_1, x_2\}$ for each $\{x_3 - x_{15}\}$.

Let $f'(x', k') = (x_1 \oplus k_1)\&(x_2 \oplus k_2) \oplus f''(x'', k'')$, $f_1(x, k) = (x_1 \oplus k_1)\&(x_2 \oplus k_2)$, we use the guess, spilt and combine technique to calculate the $B^{k_1,k_2}(y)$. We guess the k_1 at first and spilt the (x_1, x_2) into two case:

a. For x_1 that satisfy $x_1 \oplus k_1 = 0$, $f_1(x, k) = 0$, we generate a new counter $V'_1[x_2] = \sum_{x_2\in F_2} V'[x_1, x_2]$. There needs 1 addition.

b. For x_1 that satisfy $x_1 \oplus k_1 = 1$, $f_1(x,k) = (x_2 \oplus k_2)$, we generate a new counter $V'_2[x_2] = \sum_{x_2 \in F_2} (-1)^{x_2} V'[x_1, x_2]$. There needs 1 addition.

c. Combine the two cases, $B^{k_1,k_2}(y) = V'_1[x_2] + (-1)^{k_2} V'_2[x_2]$. Considering two possible values of k_2, there needs 2 additions.

So in total there needs $2 \times (1+1+2) = 2^3$ additions to compress x_1, x_2. Now there are 2 bits keys (k_1, k_2) and 12 bits independent variables x to store and the time complexity of this step is $2^{12} \times 2^3 = 2^{15}$ additions.

Step 2. Then we compress $\{x_3 - x_{15}\}$ for each $\{k_1, k_2\}$.

We guess the $\{k_3, k_7, k_{12}\}$ at first, and split the $f''(x'', k'')$ into 8 cases according to the values of $\{x_3 \oplus k_3, x_7 \oplus k_7, x_{12} \oplus k_{12}\}$. When $\{x_3 \oplus k_3, x_7 \oplus k_7, x_{12} \oplus k_{12}\} = \{0, 0, 0\}$, the function of simplified $f''(x'', k'')$ is

$$f''_{000} = ((x_5 \oplus k_5)\&(x_8 \oplus k_8)) \oplus [(x_{10} \oplus k_{10} \oplus ((x_{11} \oplus k_{11})\&(x_{14} \oplus k_{14}))) \\ \&(x_{15} \oplus k_{15} \oplus ((x_{14} \oplus k_{14})\&(x_{16} \oplus k_{16})))]$$

The rest seven cases have the same form expressions and the only differences are the subscripts. So according to different cases, we can calculate the correlation using different key sets with less keys. Let T_g is the time complexity to generate a new counter vector and T_s is the time to calculate the correlation for each case, and T_c is the time of the combination of the 8 cases. So the total time is $T = 2^3 \times (8 \times (T_g + T_s) + T_c)$. There the T_c needs $2^{13} \times 7$ additions(There are 13 bits keys $\{k_3 - k_{15}\}$ in $f''(x'', k'')$).Then we give the procedure to calculate the $B^{k_5,k_8,k_{10},k_{11},k_{14}-k_{16}}(y)$ for f''_{000} as an example to get the T_g and T_s .

At first, we need to generate a new counter vector V''_{000} at first.

$$V''_{000}[x_5, x_8, x_{10}, x_{11}, x_{14} - x_{16}] = \sum_{x_3=k_3, x_7=k_7, x_{12}=k_{12}, x_6 \in F_2, x_9 \in F_2, x_{13} \in F_2} V''[x]$$

Notice $x_{10} = x_3 \oplus x_5$ and $x_4 = x_8 \oplus x_{15}$, so there are only 6 independent variables of x and 7 additions for each possible values. In total, there needs $2^6 \times 7$ additions to generate the new counter vector, that is $T_g = 2^6 \times 7$. Then we also use the guess, split and combine technique to calculate the T_s. For f''_{000}, we guess the k_5, k_{14} to split f''_{000} into 4 cases as the following table. Let the time for the 4 cases are T'_g, T'_s and T'_c, and the total time is $T_s = 2^2 \times (4 \times (T'_g + T'_s) + T'_c)$.

Guess	$x_5 \oplus k_5, x_{14} \oplus k_{14}$	simplified f''_{000}	Related bit
k_5, k_{14}	$0, 0$	$(x_{10} \oplus k_{10})\&(x_{15} \oplus k_{15})$	
	$0, 1$	$(x_{10,11} \oplus k_{10,11})\&(x_{15,16} \oplus k_{15,16})$	
	$1, 0$	$(x_{10} \oplus k_{10})\&(x_{15} \oplus k_{15})$	k_8
	$1, 1$	$(x_{10,11} \oplus k_{10,11})\&(x_{15,16} \oplus k_{15,16})$	k_8

The 4 cases after split have the same form with the $f_1(x,k)$ in step 1, so the time to calculate the correlation is 2^3, that is $T'_s = 2^3$. Since the x_{10} is fixed, the time to generate a new counter vector is different for the 4 cases.

a.For the case $\{x_5 \oplus k_5, x_{14} \oplus k_{14}\} = \{0, 0\}$ or $\{1, 0\}$, we generate a new counter vector

$$V''^{00}_{000}[x_{10}, x_{15}] = \sum_{x_3=k_5, x_{14}=k_{14}, x_8 \in F_2, x_{11} \in F_2, x_{16} \in F_2} V''_{000}[x]$$

Since the x_{10} is fixed, the time is $2 \times (2^3 - 1) = 2^4 - 2$.
b.For the case $\{x_5 \oplus k_5, x_{14} \oplus k_{14}\} = \{0, 1\}$ or $\{1, 1\}$, we generate a new counter vector

$$V''^{01}_{000}[x_{10,11}, x_{15,16}] = \sum_{x_5=k_5, x_{14}=k_{14} \oplus 1, x_8 \in F_2} V''_{000}[x]$$

The time is $2^2 \times (2^2 - 1) = 2^4 - 2^2$.

So the total time to generate new counter vector for the 4 cases is

$$4 \times T'_g = 2 \times (2^4 - 2) + 2 \times (2^4 - 2^2) = 2^6 - 3 \times 2^2$$

To combine the 4 cases for 7 keys involved in f''_{000}, we need to calculate

$$\begin{aligned} B^{k_5, k_8, k_{10}, k_{11}, k_{14} - k_{16}}(y) = {} & B^{k_{10}, k_{15}}_{00}(y) + B^{k_{10,11}, k_{15,16}}_{01}(y) \\ & + (-1)^{k_8}(B^{k_{10}, k_{15}}_{10}(y) + B^{k_{10,11}, k_{15,16}}_{11}(y)) \end{aligned}$$

The time to combine the 4 cases is $T'_c = 2^4 + 2^4 + 2^5 = 2^6$. Then the $T_s = 2^2 \times (2^6 + 2^4 + 2^2 + 2^6) \approx 2^{9.21}$. So we can get the total time

$$T = 2^3 \times (8 \times (T_g + T_s) + T_c) = 2^3(8 \times (2^6 \times 7 + 2^{9.21}) + 2^{11} \times 7) = 2^{17.47}$$

There are 2^2 possible values of (k_1, k_2), so $2^2 \times 2^{17.47} = 2^{19.47}$ additions are needed to compress $\{x_3 - x_{15}\}$ for each $\{k_1, k_2\}$.

The total time to calculate the correlation for $B^{k'}(y) = \sum_{x'} (-1)^{f'(x', k')} V'[x']$ is the sum of step 1 and step 2: $2^{15} + 2^{19.47} = 2^{19.53}$. This time is far lower than 2^{14+16}(calculate for 2^{14} x and 2^{16} keys).

Attack on 23 rounds. We add one more round before and one more round after the 21-round distinguisher. According the plaintexts and ciphertexts we need in the 21-round distinguisher, we need to guess 13 bits keys in $(r-5)$-th round and 13 bits in $(r+17)$-th round. The potential of the linear hull is $2^{-30.91}$ and our data complexity is $N = 2^{31.91}$. Set the advantage $a = 8$ and the success rate is 0.477.
1.Guess 13 bits $\{K_0^{r-5} - K_2^{r-5}, K_5^{r-5} - K_7^{r-5}, K_9^{r-5} - K_{15}^{r-5}\}$ and 13 bits $\{K_0^{r+17} - K_2^{r+17}, K_5^{r+17} - K_7^{r+17}, K_9^{r+17} - K_{15}^{r+17}\}$. For each of the 2^{26} values,

a.Encrypt the plaintexts by one round and decrypt the ciphertexts by one round to get the $P = X^{r-4}$ and $C = X^{r+17}$. Then Compress the N pairs X^{r-4} and X^{r+17} into a counter vector $V_1[x'_p, x'_c]$, there are total 2^{14+14} counters. There needs $N = 2^{31.91}$ times compression.

b.For each of 2^{14} x'_c, call Procedure A to calculate the correlation for different k'_p and constant x'_c. Now we have 2^{16+14} counters according 14 bits x'_c and 16 bits k'_p. This step needs $2^{14} \times 2^{19.53}$ times additions.

c.For each of 2^{16} k'_p, call Procedure A to calculate the correlation for different k'_c. Now we have 2^{16+16} counters according 16 bits k'_p and 16 bits k'_c. This step needs $2^{16} \times 2^{19.53}$ times additions.

This step needs $2^{26} \times 2^{31.91}$ times two-round encryption. To calculate the correlation of the 21-round attack distinguisher, there needs $2^{26} \times (2^{33.53} + 2^{35.53}) = 2^{61.85}$ times additions.

2.We have $2^{26+32} = 2^{58}$ counters in total. Because the advantage is 8, so the key ranked in the largest 2^{58-8} counters can be the right key. Guess some other key bits to check the right key, there needs 2^{64-8} times 23-round encryption to recover the master key.

Attack complexity: $2^{61.85}$ additions and $2^{56.41}$ 23-round encryption.

4.3 Key Recovery Attack on Simeck48/96

We use the linear hull obtained in section 3:

$$X^r_{L,19} \oplus X^r_{L,21} \oplus X^r_{R,20} \rightarrow X^{r+20}_{L,21} \oplus X^{r+20}_{R,20}$$

with a potential $2^{-45.66}$ to attack the Simeck48/96. Let data complexity is $N = 2^{47.66}$, the advantage $a = 8$, so the success rate is 0.867. We add four more rounds on the top and four more rounds on the bottom to get a 28 rounds distinguisher.(More details can be seen in Appendix C).

Attack on 30 rounds. We add one more round before and one more round after the 28 rounds distinguisher. According the plaintexts and ciphertexts we need in the 28 rounds distinguisher, we need to guess 21 bits keys in $(r-5)$-th round and 18 bits in $(r+24)$-th round.

1.Guess 21 bits $\{K^{r-5}_1, K^{r-5}_3 - K^{r-5}_{21}, K^{r-5}_{23}\}$ and 18 bits $\{K^{r+24}_0, K^{r+24}_4 - K^{r+24}_6, K^{r+24}_8 - K^{r+24}_{21}\}$. For each of 2^{39} values,

a.Encrypt the plaintexts by one round and decrypt the ciphertexts by one round to get the $P = X^{r-4}$ and $C = X^{r+24}$. Then Compress the N pairs X^{r-4} and X^{r+24} into a counter vector $V_1[x'_p, x'_c]$, there are total 2^{45} counters. The time needs $N = 2^{47.66}$ times compression.

b.For each of 2^{19} x'_c, call Procedure B. Now we have 2^{19+28} counters according 19 bits x'_c and 28 bits k'_p. The time needs $2^{19} \times 2^{32.78}$ times additions.

c.For each of 2^{28} k'_p, call Procedure C. Now we have 2^{28+21} counters according 28 bits k'_p and 21 bits k'_c. The time needs $2^{28} \times 2^{24.62}$ times additions.

This step needs $2^{39} \times 2^{47.66}$ times two-round encryption. To calculate the correlation of the 28-round attack distinguisher, the time needs $2^{39} \times 2^{53.26}$ times additions.

2.We have $2^{39+49} = 2^{88}$ counters in total and the key ranked in the largest 2^{88-8} counters can be the right key. Guess some other key bits and use two pairs plaintext-ciphertext to check the right key, the time needs 2^{96-8} times 30-round encryption to recover the master key.

Attack complexity: $2^{92.26}$ additions and $2^{88.04}$ 30-round encryption.

4.4 Key Recovery Attack on Simeck64/128

We use the linear hull obtained in section 3.3:

$$X^r_{L,18} \oplus X^r_{L,22} \to X^{r+26}_{L,22} \oplus X^{r+26}_{R,21}$$

with a potential $2^{-62.09}$ to attack the Simeck64/128. Let data complexity is $N = 2^{63.09}$, the advantage $a = 8$, so the success rate is 0.477.We add four more rounds on the top and four more rounds on the bottom to get a 34 rounds distinguisher.(More details can be seen in Appendix D).

Attack on 37 rounds. We add two more rounds before and one more round after the 34 rounds distinguisher. According the plaintexts and ciphertexts we need in the 34 rounds distinguisher, we need to guess 24 bits keys in $(r-6)$-th round, 19 bits keys in $(r-5)$-th round and 18 bits in $(r+30)$-th round.
1.Guess the 24 bits $\{K_1^{r-6} - K_3^{r-6}, K_5^{r-6} - K_{22}^{r-6}, K_{25}^{r-6}, K_{29}^{r-6}, K_{30}^{r-6}\}$, 19 bits $\{K_2^{r-5}, K_3^{r-5}, K_6^{r-5} - K_8^{r-5}, K_{10}^{r-5} - K_{22}^{r-5}, K_{30}^{r-5}\}$ and 18 bits $\{K_0^{r+30}, K_4^{r+30} - K_6^{r+30}, K_8^{r+30} - K_{21}^{r+30}\}$. For each of 2^{61} values,

a.Encrypt the plaintexts by two rounds and decrypt the ciphertexts by one round to get the $P = X^{r-4}$ and $C = X^{r+30}$. Then Compress the N pairs X^{r-4} and X^{r+30} into a counter vector $V_1[x'_p, x'_c]$, there are total 2^{46} counters. The time needs $N = 2^{63.09}$ times compression.

b.For each of 2^{19} x'_c, call Procedure D. Now we have 2^{19+25} counters according 19 bits x'_c and 25 bits k'_p. The time needs $2^{19} \times 2^{30.24}$ times additions.

c.For each of 2^{25} k'_p, call Procedure E. Now we have 2^{25+21} counters according 25 bits k'_p and 21 bits k'_c. The time needs $2^{25} \times 2^{24.62}$ times additions.

This step needs $2^{61} \times 2^{63.09}$ times three-round encryption. To calculate the correlation of the 34-round distinguisher, the time needs $2^{61} \times 2^{50.44}$ times additions.

2.We have $2^{61+46} = 2^{107}$ counters in total and the key ranked in the largest 2^{107-8} counters can be the right key. Guess some other key bits and use two pairs plaintext-ciphertext to check the right key, the time needs 2^{128-8} times 37-round encryption to recover the master key.

Attack complexity: $2^{111.44}$ additions and $2^{121.25}$ 37-round encryption.

5 Conclusion and Future Work

In this paper, we give some linear hulls for Simeck using the differentials searched by Kölbl's tool. Then analyze the security of Simeck against the linear hull attack using dynamic key-guessing techniques. With Chen *et al.*'s Guess, split, Combine technique to reduce the time complexity, we can recovery the key for 23-round Simeck32/64, 30-round Simeck48/96, 37-round Simeck64/128, which is the best results from the point of rounds attacked.

In the future, we will try to search better linear hulls for Simeck using other methods like correlation matrix, Mixed Integer Programming (MIP) and so on. Then we will apply the linear hull attack with dynamic key-guessing techniques for other bit-oriented block cipher.

References

1. Mohamed Ahmed Abdelraheem, Javad Alizadeh, Hoda A Alkhzaimi, Mohammad Reza Aref, Nasour Bagheri, and Praveen Gauravaram. Improved linear cryptanalysis of reduced-round simon-32 and simon-48. In *Progress in Cryptology–INDOCRYPT 2015*, pages 153–179. Springer, 2015.
2. Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel. Differential cryptanalysis of round-reduced simon and speck. In *Fast Software Encryption*, pages 525–545. Springer, 2014.
3. Javad Alizadeh, Hoda A Alkhzaimi, Mohammad Reza Aref, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar, Martin M Lauridsen, and Somitra Kumar Sanadhya. Cryptanalysis of simon variants with connections. In *Radio Frequency Identification: Security and Privacy Issues*, pages 90–107. Springer, 2014.
4. Javad Alizadeh, Hoda A Alkhzaimi, Mohammad Reza Aref, Nasour Bagheri, Praveen Gauravaram, and Martin M Lauridsen. Improved linear cryptanalysis of round reduced simon. Technical report, Citeseer, 2014.
5. Hoda AlKhzaimi and Martin M Lauridsen. Cryptanalysis of the simon family of block ciphers. *IACR Cryptology ePrint Archive*, 2013:543, 2013.
6. Tomer Ashur. Improved linear trails for the block cipher simon. Cryptology ePrint Archive, Report 2015/285, 2015. http://eprint.iacr.org/.
7. Nasour Bagheri. Linear cryptanalysis of reduced-round simeck variants. In *Progress in Cryptology–INDOCRYPT 2015*, pages 140–152. Springer, 2015.
8. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The simon and speck families of lightweight block ciphers. *IACR Cryptology ePrint Archive*, 2013:404, 2013.
9. Alex Biryukov, Arnab Roy, and Vesselin Velichkov. Differential analysis of block ciphers simon and speck. In *Fast Software Encryption*, pages 546–570. Springer, 2014.
10. Huaifeng Chen and Xiaoyun Wang. Improved linear hull attack on round-reduced simon with dynamic key-guessing techniques. Technical report, Cryptology ePrint Archive, Re port 2015/666, July 201 5. http://eprint. iacr. org/2015/666. pdf, 2015.
11. Stefan Kölbl, Gregor Leander, and Tyge Tiessen. Observations on the simon block cipher family.
12. Stefan Kölbl and Arnab Roy. A brief comparison of simon and simeck. Technical report, Cryptology ePrint Archive, Report 2015/706, 2015.
13. Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Advances in Cryptology—EUROCRYPT' 93*, pages 386–397. Springer, 1994.
14. Hoda A. Alkhzaimi Mohammad Reza Aref Nasour Bagheri Praveen Gauravaram Mohamed Ahmed Abdelraheem, Javad Alizadeh and Martin M. Lauridsen. Improved linear cryptanalysis of reduced-round simon. Cryptology ePrint Archive, Report 2014/681, 2014. http://eprint.iacr.org/.
15. Kaisa Nyberg. Linear approximation of block ciphers. In *Advances in Cryptology—EUROCRYPT'94*, pages 439–444. Springer, 1995.
16. Kexin Qiao, Lei Hu, and Siwei Sun. Differential security evaluation of simeck with dynamic key-guessing techniques. Technical report, IACR Cryptology ePrint Archive, 2015, 902. pdf at eprint. iacr. org, 2015.
17. Danping Shi, Lei Hu, Siwei Sun, Ling Song, Kexin Qiao, and Xiaoshuang Ma. Improved linear (hull) cryptanalysis of round-reduced versions of simon. Technical report, IACR Cryptology ePrint Archive, Report 2014/973, 2014. http://eprint. iacr. org/2014/973, 2015.

18. Ning Wang, Xiaoyun Wang, Keting Jia, and Jingyuan Zhao. Differential attacks on reduced simon versions with dynamic key-guessing techniques.
19. Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D Aagaard, and Guang Gong. The simeck family of lightweight block ciphers. In *Cryptographic Hardware and Embedded Systems–CHES 2015*, pages 307–329. Springer, 2015.
20. Kai Zhang, Jie Guan, Bin Hu, and Dongdai Lin. Security evaluation on simeck against zero correlation linear cryptanalysis.

A

In the Appendix A, we give the details of linear hull for Simeck48/96 and Simeck64/128.

Table 6: Linear characteristic based on the differential for Simeck48/96

	Differential		Linear		
r	Δ_L	Δ_R	X_L	X_R	$Used\ App$
0	22	$21, 23$	$19, 21$	20	1
1	21	22	20	21	1
2	–	21	21	–	–
3	21	–	–	21	1
4	22	21	21	20	1
5	$21, 23$	22	20	$19, 21$	$1: 1$
6	0	$21, 23$	$19, 21$	18	1
7	$1, 21, 23$	0	18	$17, 19, 21$	$1:1:3$
8	22	$1, 21, 23$	$17, 19, 21$	20	1
9	$1, 21$	22	20	$17, 21$	$1:3$
10	–	$1, 21$	$17, 21$	–	–
11	$1, 21$	–	–	$17, 21$	$1:3$
12	22	$1, 21$	$17, 21$	20	1
13	$1, 21, 23$	22	20	$17, 19, 21$	$1:1:3$
14	0	$1, 21, 23$	$17, 19, 21$	18	1
15	$21, 23$	0	18	$19, 21$	$1:1$
16	22	$21, 23$	$19, 21$	20	1
17	21	22	20	21	1
18	–	21	21	–	–
19	21	–	–	21	1
20	22	21	21	20	–
	$\sum_r \log_2 pr = -50$ $\log_2 p_{diff} = -43.66$		$\log_2 \varepsilon^2 = -52$ $\log_2 \bar{c}^2_{LH} = -45.66$		

B

The appendix B gives the expressions for $X^r_{L,1}$ in the following table.

Table 7: Linear characteristic based on the differential for Simeck48/96

	Differential		Linear		
r	$\varDelta_L$	$\varDelta_R$	X_L	X_R	$Used\ App$
0	$-$	$22, 26$	$18, 22$	$-$	$-$
1	$22, 26$	$-$	$-$	$18, 22$	$1 : 3$
2	23	$22, 26$	$18, 22$	21	1
3	$22, 24, 26$	23	32	$18, 20, 22$	$1 : 1 : 3$
4	25	$22, 24, 26$	$18, 20, 22$	19	1
5	$22, 24$	25	19	$20, 22$	$1 : 1$
6	23	$22, 24$	$20, 22$	21	1
7	22	23	21	22	1
8	$-$	22	22	$-$	$-$
9	22	$-$	$-$	22	1
10	23	22	22	21	1
11	$22, 24$	23	21	$20, 22$	$1 : 1$
12	25	$22, 24$	$20, 22$	19	1
13	$22, 24, 26$	25	19	$18, 20, 22$	$1 : 1 : 3$
14	23	$22, 24, 26$	$18, 20, 22$	21	1
15	$22, 26$	23	21	$18, 22$	$1 : 3$
16	$-$	$22, 26$	$18, 22$	$-$	$-$
17	$22, 26$	$-$	$-$	$18, 22$	$1 : 3$
18	23	$22, 26$	$18, 22$	21	1
19	$22, 24, 26$	23	21	$18, 20, 22$	$1 : 1 : 3$
20	25	$22, 24, 26$	$18, 20, 22$	19	1
21	$22, 24$	25	19	$20, 22$	$1 : 1$
22	23	$22, 24$	$20, 22$	21	1
23	22	23	21	22	1
24	$-$	22	22	$-$	$-$
25	22	$-$	$-$	22	1
26	23	22	22	21	1
	$\sum_r \log_2 pr = -68$ $\log_2 p_{diff} = -60.09$		$\log_2 \varepsilon^2 = -70$ $\log_2 \bar{c}^2_{LH} = -62.09$		

Table 8: The expressions for $X_{L,1}^{r}$

x_0	$X_{L,1}^{r-4} \oplus X_{L,15}^{r-4}$ $\oplus(X_{L,9}^{r-4} \& \oplus X_{L,14}^{r-4}) \oplus X_{L,13}^{r-4} \oplus X_{R,14}^{r-4}$	k_0	$K_1^{r-1} \oplus K_0^{r-2} \oplus K_1^{r-3}$ $\oplus K_{15}^{r-3} \oplus K_{14}^{r-4}$
x_1	$(X_{L,5}^{r-4} \& \oplus X_{L,10}^{r-4}) \oplus X_{L,9}^{r-4} \oplus X_{R,10}^{r-4}$	k_1	K_{10}^{r-4}
x_2	$(X_{L,10}^{r-4} \& \oplus X_{L,15}^{r-4}) \oplus X_{L,14}^{r-4} \oplus X_{R,15}^{r-4}$	k_2	K_{15}^{r-4}
x_3	$(X_{L,7}^{r-4} \& \oplus X_{L,12}^{r-4}) \oplus X_{L,11}^{r-4} \oplus X_{R,12}^{r-4}$	k_3	K_{12}^{r-4}
x_4	$(X_{L,12}^{r-4} \& \oplus X_{L,1}^{r-4}) \oplus X_{L,0}^{r-4} \oplus X_{R,1}^{r-4}$	k_4	K_1^{r-4}
x_5	$(X_{L,5}^{r-4} \& \oplus X_{L,10}^{r-4}) \oplus X_{L,9}^{r-4} \oplus X_{R,10}^{r-4} \oplus X_{L,11}^{r-4}$	k_5	$K_{10}^{r-4} \oplus K_{11}^{r-3}$
x_6	$(X_{L,1}^{r-4} \& \oplus X_{L,6}^{r-4}) \oplus X_{L,5}^{r-4} \oplus X_{R,6}^{r-4}$	k_6	K_6^{r-4}
x_7	$(X_{L,6}^{r-4} \& \oplus X_{L,11}^{r-4}) \oplus X_{L,10}^{r-4} \oplus X_{R,11}^{r-4}$	k_7	K_{11}^{r-4}
x_8	$(X_{L,10}^{r-4} \& \oplus X_{L,15}^{r-4}) \oplus X_{L,14}^{r-4} \oplus X_{R,15}^{r-4} \oplus X_{L,0}^{r-4}$	k_8	$K_{15}^{r-4} \oplus K_0^{r-3}$
x_9	$(X_{L,11}^{r-4} \& \oplus X_{L,0}^{r-4}) \oplus X_{L,15}^{r-4} \oplus X_{R,0}^{r-4}$	k_9	K_0^{r-4}
x_{10}	$x_3 \oplus x_5$	k_{10}	$k_3 \oplus k_5 \oplus K_{12}^{r-2}$
x_{11}	$(X_{L,1}^{r-4} \& \oplus X_{L,6}^{r-4}) \oplus X_{L,5}^{r-4} \oplus X_{R,6}^{r-4} \oplus X_{L,7}^{r-4}$	k_{11}	$K_6^{r-4} \oplus K_7^{r-3}$
x_{12}	$(X_{L,13}^{r-4} \& \oplus X_{L,2}^{r-4}) \oplus X_{L,1}^{r-4} \oplus X_{R,2}^{r-4}$	k_{12}	K_2^{r-4}
x_{13}	$(X_{L,2}^{r-4} \& \oplus X_{L,7}^{r-4}) \oplus X_{L,6}^{r-4} \oplus X_{R,7}^{r-4}$	k_{13}	K_7^{r-4}
x_{14}	$(X_{L,6}^{r-4} \& \oplus X_{L,11}^{r-4}) \oplus X_{L,10}^{r-4} \oplus X_{R,11}^{r-4} \oplus X_{L,12}^{r-4}$	k_{14}	$K_{11}^{r-4} \oplus K_{12}^{r-3}$
x_{15}	$x_4 \oplus x_8$	k_{15}	$k_4 \oplus k_8 \oplus K_1^{r-2}$
x_{16}	$(X_{L,11}^{r-4} \& \oplus X_{L,0}^{r-4}) \oplus X_{L,15}^{r-4} \oplus X_{R,0}^{r-4} \oplus X_{L,1}^{r-4}$	k_{16}	$K_0^{r-4} \oplus K_1^{r-3}$

C

In the Appendix C, we give the details for key recovery attack on Simeck48/96. First, we give the time complexity for some common boolean function.

	Expression	Time
f_1	$(x_1 \oplus k_1) \& (x_2 \oplus k_2)$	2^3
f_2	$(x_1 \oplus k_1 \oplus (x_2 \oplus k_2) \& (x_3 \oplus k_3)) \& (x_4 \oplus k_4 \oplus (x_2 \oplus k_2) \& (x_3 \oplus k_3))$	$2^{5.64}$
f_3	$[x_1 \oplus k_1 \oplus (x_2 \oplus k_2) \& (x_3 \oplus k_3) \oplus$ $(x_4 \oplus k_4 \oplus (x_5 \oplus k_5) \& (x_6 \oplus k_6)) \& (x_7 \oplus k_7 \oplus (x_6 \oplus k_6) \& (x_8 \oplus k_8))]$ $\&[x_9 \oplus k_9 \oplus (x_3 \oplus k_3) \& (x_{10} \oplus k_{10}) \oplus$ $(x_7 \oplus k_7 \oplus (x_6 \oplus k_6) \& (x_8 \oplus k_8)) \& (x_{11} \oplus k_{11} \oplus (x_8 \oplus k_8) \& (x_{12} \oplus k_{12}))]$	$2^{15.99}$
f_4	$f_3 \oplus ((x_7 \oplus k_7) \& (x_{11} \oplus k_{11})) \oplus$ $(x_{12} \oplus k_{12} \oplus (x_1 \oplus k_1) \& (x_2 \oplus k_2)) \& (x_{13} \oplus k_{13} \oplus (x_2 \oplus k_2) \& (x_9 \oplus k_9))$ $Notice : x_0 = x_7 \oplus x_{12}, x_8 = x_{11} \oplus x_{13}$	$2^{17.47}$

The linear hull is

$$X_{L,19}^{r} \oplus X_{L,21}^{r} \oplus X_{R,20}^{r} \to X_{L,21}^{r+20} \oplus X_{R,20}^{r+20}$$

Add 4 rounds before r-th round, we get the expression for $X_{L,19}^{r} \oplus X_{L,21}^{r} \oplus X_{R,20}^{r}$:

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

Procedure B.
First compress the plaintexts into a counter $V[x_1, ..., x_{28}]$, there are only 26 independent x values.

1. Compress x_1, x_2 as f_1 for each $x_3 - x_{28}$, there needs $2^{24}\cdot 2^3 = 2^{27}$ additions.

2. Compress $x_3, x_4, x_7 - x_{18}$ as f_4 for each $k_1, k_2, x_5, x_6, x_{19} - x_{28}$. There needs $2^{14} \cdot 2^{17.47} = 2^{31.47}$ additions.

3. Compress $x_5, x_6, x_{19} - x_{28}$ as f_3 for each $k_1 - k_4, x_7 - x_{18}$. Three needs $2^{16} \cdot 2^{15.99} = 2^{31.99}$ additions.

In total, time complexity is $2^{27} + 2^{31.47} + 2^{31.99} = 2^{32.78}$ additions.

Add 4 rounds after $r + 20$-th round, we get the expression for $X_{L,21}^{r+20} \oplus X_{R,20}^{r+20}$.

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

Procedure C. First compress the ciphertexts into a counter $V[x_1, ..., x_{21}]$, there are only 19 independent x values.

1. Compress x_1, x_2 as f_1 for each $x_3 - x_{21}$, there needs $2^{17}\cdot 2^3 = 2^{20}$ additions.

2. Compress $x_3 - x_7$ as f_2 for each $k_1, k_2, x_8 - x_{21}$. There needs $2^{14} \cdot 2^{6.46} = 2^{20.46}$ additions.

3. Compress $x_5, x_6, x_{19} - x_{28}$ as f_4 for each $k_1 - k_7$. Three needs $2^7 \cdot 2^{17.47} = 2^{24.27}$ additions.

In total, time complexity is $2^{20} + 2^{20.46} + 2^{24.47} = 2^{24.62}$ additions.

Table 9: The expressions for $X^r_{L,19} \oplus X^r_{L,21} \oplus X^r_{R,20}$

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

Table 10: The expressions for $X_{L,21}^{r+20} \oplus X_{R,20}^{r+20}$

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

D

In the Appendix D, we give the details for key recovery attack on Simeck64/128. The linear hull is

$$X_{L,18}^r \oplus X_{L,22}^r \to X_{L,22}^{r+26} \oplus X_{R,21}^{r+26}$$

Add 4 rounds before r-th round, we get the expression for $X_{L,18}^r \oplus X_{L,22}^r$:

$$\begin{aligned}
&f(x,k) = x_0 \oplus k_0 \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)) \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4))\\
&\oplus((x_5 \oplus k_5)\&(x_6 \oplus k_6)) \oplus ((x_7 \oplus k_7)\&(x_8 \oplus k_8))\\
&\oplus[(x_9 \oplus k_9 \oplus ((x_{10} \oplus k_{10})\&(x_{11} \oplus k_{11})))\&(x_{12} \oplus k_{12} \oplus ((x_{11} \oplus k_{11})\&(x_7 \oplus k_7)))]\\
&\oplus[(x_{13} \oplus k_{13} \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2)))\&(x_{14} \oplus k_{14} \oplus ((x_2 \oplus k_2)\&(x_{15} \oplus k_{15})))]\\
&\oplus\{[x_{16} \oplus k_{16} \oplus ((x_{10} \oplus k_{10})\&(x_{11} \oplus k_{11}))\oplus\\
&(x_{17} \oplus k_{17} \oplus ((x_{18} \oplus k_{18})\&(x_{19} \oplus k_{19})))\&(x_{20} \oplus k_{20} \oplus ((x_{19} \oplus k_{19})\&(x_3 \oplus k_3)))]\\
&\&[x_{21} \oplus k_{21} \oplus ((x_7 \oplus k_7)\&(x_{11} \oplus k_{11}))\oplus\\
&(x_{20} \oplus k_{20} \oplus ((x_{19} \oplus k_{19})\&(x_3 \oplus k_3)))\&(x_{22} \oplus k_{22} \oplus ((x_3 \oplus k_3)\&(x_4 \oplus k_4)))]\}\\
&\oplus\{[x_{23} \oplus k_{23} \oplus ((x_1 \oplus k_1)\&(x_2 \oplus k_2))\oplus\\
&(x_9 \oplus k_9 \oplus ((x_{10} \oplus k_{10})\&(x_{11} \oplus k_{11})))\&(x_{12} \oplus k_{12} \oplus ((x_{11} \oplus k_{11})\&(x_7 \oplus k_7)))]\\
&\&[x_{24} \oplus k_{24} \oplus ((x_2 \oplus k_2)\&(x_{15} \oplus k_{15}))\oplus\\
&(x_{12} \oplus k_{12} \oplus ((x_{11} \oplus k_{11})\&(x_7 \oplus k_7)))\&(x_{25} \oplus k_{25} \oplus ((x_7 \oplus k_7)\&(x_8 \oplus k_8)))]\}
\end{aligned}$$

Procedure D.
First compress the plaintexts into a counter $V[x_1, ..., x_{25}]$, there are only 21 independent x values.

1. Compress x_5, x_6 as f_1 for each $x_1 - x_4, x_7 - x_{25}$, there needs $2^{19} \cdot 2^3 = 2^{22}$ additions.

2. Compress $x_1 - x_4, x_7 - x_{25}$ for each k_5, k_6. There are 19 bits independent x. First we guess 5 bit $x_2, x_3, x_7, x_{10}, x_{18}$ and split the all values of x into 2^5 cases, each case has same complexity. For example, we calculate the

$$\begin{aligned}
&f = ((x_9 \oplus k_9)\&(x_{12} \oplus k_{12})) \oplus [(x_{16} \oplus k_{16} \oplus ((x_{17} \oplus k_{17})\&(x_{20} \oplus k_{20})))\\
&\&(x_{21} \oplus k_{21} \oplus ((x_{20} \oplus k_{20})\&(x_{22} \oplus k_{22})))]\\
&\oplus((x_{13} \oplus k_{13})\&(x_{14} \oplus k_{14})) \oplus [(x_{23} \oplus k_{23} \oplus ((x_9 \oplus k_9)\&(x_{12} \oplus k_{12})))\\
&\&(x_{24} \oplus k_{24} \oplus ((x_{12} \oplus k_{12})\&(x_{25} \oplus k_{25})))]
\end{aligned}$$

To generate a new counter for f needs $2^{10} \cdot (2^4 - 1)$ additions. Then to calculate the correlation of function f, we first guess x_{12}, x_{13}, x_{20} and split x into 8 cases. To generate the new counters for the 8 cases, we need $(2^3 \cdot (2^4 - 1) \cdot 4 + 2^4 \cdot (2^3 - 1) \cdot 4)$ additions. The each case can be compressed as f_2 where needs $2^{5.64}$ additions. Combine the 8 cases needs $2^9 \cdot 7$ additions. So the total time to calculate the correlation of function f is

$$2^3 \cdot (2^3 \cdot (2^4 - 1) \cdot 4 + 2^4 \cdot (2^3 - 1) \cdot 4 + 2^{5.64} \cdot 8 + 2^9 \cdot 7) = 2^{15.26}$$

Table 11: The expressions for $X^r_{L,18} \oplus X^r_{L,22}$

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

Then for 2^5 cases as f, the generate a new counter needs $2^{10} \cdot (2^4 - 1)$ additions, the calculation needs $2^{15.26}$ and the combination needs $2^{18} \cdot (2^5 - 1)$ additions, so the total time is

$$2^5 \cdot (2^{10} \cdot (2^4 - 1) \cdot 2^5 + 2^{15.26} \cdot 2^5 + 2^{18} \cdot (2^5 - 1)) = 2^{28.24}$$

so for each k_5, k_6, there needs $2^2 \cdot 2^{28.24} = 2^{30.24}$.

In total, time complexity is $2^{22} + 2^{30.24} = 2^{30.24}$ additions.