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

Abstract. Simeck is a new family of lightweight block cipher proposed by Yang *et al.* in CHES'15, which performs efficiently in hardware implementation. In this paper, we search out differentials with low hamming weight and high probability for Simeck using Kölbl's tool, then exploit 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 in the round function. Our results cover Simeck 32/64 reduced to 23 rounds, Simeck 48/96 reduced to 30 rounds, Simeck 64/128 reduced to 37 rounds, which are 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 cipher 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 [7], using a different set of rotation constants of Simon's round function and the key schedule of Speck. The round function of Simeck only 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, 4, 8], linear [3, 13] cryptanalysis and so on. For Simon, wang *et al.* in [18] improved the differential attack results by dynamic key-guessing techniques. Then Chen *et al.* basing on the dynamic key-guessing techniques in the linear hull cryptanalysis of Simon [9], applied the Guess, Split and Combine technique to reduce the time complexity in the calculation of the empirical correlations. They can attack one or two more rounds for all versions of Simon than Wang *et al.*'s results.

For Simeck, there are only a few cryptanalysis results so far. Kölbl *et al.* in [11] 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 recovered the key for 19/26/33 rounds of Simeck32/48/64. Bagheri *et al.* in [6] analyzed Simeck's security against linear cryptanalysis. With Matsui's algorithm 2, they attacked 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 in [20]. Qiao *et al.* in [15] used the differential cryptanalysis with dynamic key-guessing techniques to attack Simeck and improved the previously best results on all versions by 2 rounds.

Our contributions. This paper analyzes the security of Simeck against improved linear hull cryptanalysis with dynamic key-guessing techniques. At first using Kölbl's tool, we search out better differentials than the previous results. The probability for Simeck32/64

Table 1: Summary of cryptanalysis results on Simeck

cipher	round	Data Complexity	Time Complexity	Reference
Simeck32/64	18	2^{31}	$2^{63.5}$	[6]
	19	2^{31}	2^{36}	[11]
	20	2^{32}	$2^{56.65}$	[20]
	22	2^{32}	$2^{57.9}$	[15]
	23	$2^{31.91}$	$2^{61.78}A^{a}+2^{56.41}E^{b}$	section 4.1
Simeck48/96	24	2^{45}	2^{94}	[6]
	24	2^{48}	$2^{91.6}$	[20]
	26	2^{47}	2^{62}	[11]
	28	2^{46}	$2^{68.3}$	[15]
	30	$2^{47.66}$	$2^{92.2}A+2^{88.04}E$	section 4.2
Simeck64/128	27	2^{61}	$2^{120.5}$	[6]
	27	2^{64}	$2^{112.79}$	[20]
	33	2^{63}	2^{96}	[11]
	35	2^{63}	$2^{116.3}$	[15]
	37	$2^{63.09}$	$2^{111.44}A+2^{121.25}E$	section 4.3

[a] additions.
[b] encryption of attacked rounds.

is more accurate with searching more differential characteristics. For Simeck48/96 and Simeck64/128, the differentials with less active bits are preferred so we can extend the trails for more rounds and attack more rounds. Then we take advantage of the links between linear characteristic and differential characteristic to construct linear hull distinguishers for the Simeck family. After getting the boolean expressions for the parity bits of the distinguishers, we use the Guess, Split and Combine technique to calculate the empirical correlations, which reduces the time complexity greatly. As a result, 23/30/37 rounds of Simeck32/48/64 can be attacked (Table 1), which are the best results so far. We also do some experiments to verify our results. The experiment on the bias of the linear hull for Simeck32/64 meets our expectation and 48.4% of the results have a bias higher than we expect. Due to the time limitation, we implement the attack on 21-round Simeck32/64 to recover 8-bit information of 32-bit subkeys. The success rate is 45.6% corresponding to our estimated value, which proves our algorithm is effective.

This paper is organized as follows. Section 2 gives a brief description of the Simeck family and dynamic key-guessing techniques in the linear hull cryptanalysis. In section 3, we introduce the differential trails searched and transform the differentials to linear hulls. Then linear hull cryptanalysis with the dynamic key-guessing techniques are applied to attack all versions of Simeck in section 4. Finally we conclude in section 5.

2 Preliminaries

2.1 The Simeck family

The lightweight block cipher Simeck with Feistel structure is proposed in CHES'15. The Simeck cipher with $2n$-bit block and mn-bit key will be referred to as Simeck$2n/mn$. There are three versions of Simeck, including Simeck32/64, Simeck48/96 and Simeck64/128. 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 (input of round $r+1$)
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 $(X_L^{r+1} || X_R^{r+1})$. The round function is

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

where function $F(X) = ((X \lll 5) \& X) \oplus (X \lll 1)$. We can also present the round function for single bit, which we will 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 can be 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.

Fig. 1: The round function of Simeck

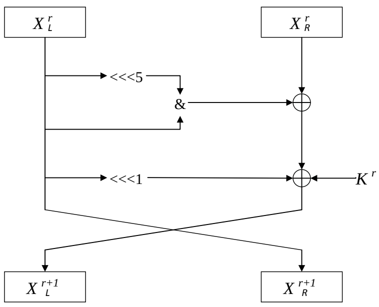
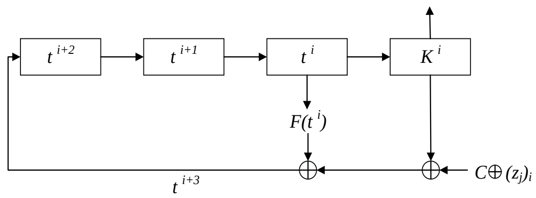


Fig. 2: The key schedule of Simeck



Key Schedule. 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, the states $\{t^2, t^1, t^0, K^0\}$ are initialized with the master key at first. Then the registers are updated 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 $0 \le i \le n_r - 1$, $C = 2^n - 4$(n is the word size), $(z_j)_i$ is the i-th bit of z_j. For Simeck32/64 and Simeck48/96, the sequence z_j is generated by the primitive polynomial $X^5 + X^2 + 1$ with the initial states $(1,1,1,1,1)$. And for Simeck64/128, the z_j is generated by the primitive polynomial $X^6 + X + 1$ with the initial states $(1,1,1,1,1,1)$.

2.2 Linear cryptanalysis

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

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

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

Linear cryptanalysis [12] is an important known plaintext cryptanalytic technique, and it tries to find a highly probable expression with plaintexts P, ciphertexts C and key bits K as

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

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 $O(\frac{1}{\epsilon^2})$ planitexts are needed in the key recovery attack.

The linear hull [14] 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

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

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

2.3 Linear compression and Dynamic key-guessing

To reduce the time complexity of calculating the correlation in linear hull cryptanalysis, the linear part of the function can be compressed at first. Let $y = f(x, k)$ is a boolean function, and x is l_1-bit plaintext, k is l_2-bit key, the counter vector $V[x]$ 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 vector $V'[x'] = \sum_{x_0 \in F_2} (-1)^{x_0} V[x_0 || x']$, so the correlation of y under some k guess is

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

Since 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. So 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 using the above method.

Besides, Chen *et al.* in [9] introduced the Guess, Split and Combine technique to reduce the time complexity based on the dynamic key-guessing techniques. In the calculations of $B^k(y) = \sum_x (-1)^{f(x,k)} V[x]$, let $k = k_G || k_A || k_B || k_C$ ((k_G, k_A, k_B, k_C) are $l_2^G, l_2^A, l_2^B, l_2^C$-bit) and guess the k_G at first. Then all the x values are split 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

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

There needs $N_A 2^{l_2^G + l_2^A + l_2^C} + N_B 2^{l_2^G + l_2^B + l_2^C} + 2^{l_2}$ additions in the guess, split and combine process, which takes less time than the general method with $2^{l_1+l_2}$.

For example, we use the Guess, Split and Combine technique to calculate the correlations $B^{k_1,k_2}(y)$ of $f_1 = (x_1 \oplus k_1) \& (x_2 \oplus k_2)$ with the counter $V[x_1, x_2]$.

1. Guess k_1 at first.
2. Split the $x = x_1 || x_2$ into two cases according the value of $(x_1 \oplus k_1)$.
   (a) For x_1 that satisfy $x_1 \oplus k_1 = 0$, $f_1 = 0$. There needs to generate a new counter $V_1 = \sum_{x_2 \in F_2} V[x_1 = k_1, x_2]$.
   (b) For x_1 that satisfy $x_1 \oplus k_1 = 1$, $f_1(x,k) = (x_2 \oplus k_2)$. There needs to generate a new counter $V_2 = \sum_{x_2 \in F_2} (-1)^{x_2} V[x_1 = k_1 \oplus 1, x_2]$, and k_2 is related bit.
3. Combine the two cases, $B^{k_1,k_2}(y) = V_1 + (-1)^{k_2} V_2$.

Step 2.(a)/2.(b) needs 1 addition, and step c needs 2 additions. So in total there needs $2 \times (1 + 1 + 2) = 2^3$ additions to compress x_1, x_2, less than the general method.

3 The Linear Hull distinguishers of Simeck

3.1 Differential distinguishers of Simeck

Differential cryptanalysis is a chosen plaintext/ciphertext cryptanalytic technique. In the round function of Simeck, the only non-linear operation is the AND operation. For single bit x and y, the probability of $(x\&y) = 0$ is 0.75. We can extract the highly probable differential expressions of round function $F(X)$ as

$$\begin{aligned}
&\text{Differential Characteristic 1} : \Pr\left[(\Delta X))_i \to (\Delta F(X))_{i+1}\right] = 0.5,\\
&\text{Differential Characteristic 2} : \Pr\left[(\Delta X))_i \to (\Delta F(X))_{i+1,i}\right] = 0.5,\\
&\text{Differential Characteristic 3} : \Pr\left[(\Delta X))_i \to (\Delta F(X))_{i+1,i+5}\right] = 0.5,\\
&\text{Differential Characteristic 4} : \Pr\left[(\Delta X))_i \to (\Delta F(X))_{i+1,i,i+5}\right] = 0.5,
\end{aligned}$$

where the $(\Delta F(X))_{i+1}$ denotes the $(i+1)$-th bit is 1 and the others are 0.

In [10], 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. [15] also gave a differential for Simeck32/64 with less active bits. We 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. The differentials are listed in Table 2.

Table 2: The differentials of Simeck

cipher	rounds	Δ_{in}	Δ_{out}	log_2diff	Reference
Simeck32/64	13	$(0x0, 0x2)$	$(0x2, 0x0)$	-29.64	[15]
Simeck32/64	13	$(0x0, 0x2)$	$(0x2, 0x0)$	-28.91	this papaer
Simeck48/96	20	$(0x400000, 0xE00000)$	$(0x400000, 0x200000)$	-43.65	[11]
Simeck48/96	20	$(0x400000, 0xA00000)$	$(0x400000, 0x200000)$	-43.66	this papaer
Simeck64/128	26	$(0x0, 0x4400000)$	$(0x8800000, 0x400000)$	-60.02	[11]
Simeck64/128	26	$(0x0, 0x4400000)$	$(0x800000, 0x400000)$	-60.09	this papaer

For Simeck32/64, by searching all the characteristics with probability higher than 2^{-52}, we get more accurate probability than [15]. For Simeck48/96 and Simeck64/128, the differentials with less active bits in the input difference and output difference are preferred, since less key bits are involved in the attack. At the same time, the probability of the differentials must be higher than 2^{-45} or 2^{-61}, to ensure in the attack the data complexity and success rate can be achieved.

3.2 Linear Hull distinguishers of Simeck

In [3], Alizadeh *et al.* noticed each differential characteristic can be mapped into an approximation of linear cryptanalysis for Simon. The property is based on the round function of Simon, so we can use the similar property for Simeck to construct an equivalent linear characteristic from a differential characteristic. The relation between the probability p of a differential and the potential $\bar{\epsilon}^2$ of a linear hull is $\bar{\epsilon}^2 = 2^{-2}p$. The linear approximation expressions of the round function $F(X)$ for Simeck are

$$\begin{aligned}
&\text{Linear Approxiamtion 1} : \Pr[(F(X))_i = (X)_{i-1}] = 0.75,\\
&\text{Linear Approxiamtion 2} : \Pr[(F(X))_i = (X)_{i-1} \oplus (X)_i] = 0.75,\\
&\text{Linear Approxiamtion 3} : \Pr[(F(X))_i = (X)_{i-1} \oplus (X)_{i-5}] = 0.75,\\
&\text{Linear Approxiamtion 4} : \Pr[(F(X))_i = (X)_{i-1} \oplus (X)_i \oplus (X)_{i-5}] = 0.25.
\end{aligned}$$

[1, 5, 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 differential characteristics to get linear characteristics. The used linear approximations (Used App) can be found above. The details for Simeck32/64 are listed in Table 3. (For Simeck48/96 and Simeck64/128, the details of the linear hulls can be found in Appendix A.) The linear hulls for all versions of Simeck can be seen in Table 4.

Table 3: Linear hull 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	–
	$\sum_r \log_2 pr = -38$		$\log_2 \varepsilon^2 = -40$		
	$\log_2 p_{diff} = -28.91$		$\log_2 \bar{\varepsilon}^2 = -30.91$		
	$\#trails = 1846518$		$\#characteristics = 1846518$		

Since the block of Simeck32/64 only contains 32 bits, we can iterate over the 2^{32} possible plaintexts to validate the bias ($\bar{\varepsilon}^2$) of the 13-round linear hull. Randomly select 1000 keys and the experimental results are listed in Table 5. In the experiments, 48.4% of the keys have a bias higher than $2^{-30.91}$, which is corresponding to the linear hull's $ALH = 2^{-30.91}$.

Table 4: The linear hulls for Simeck

cipher	round	linear hull		ALH
Simeck32/64	13	Input	$X_{L,1}^{r}$	$2^{-30.91}$
		Output	$X_{R,1}^{r+13}$	
Simeck48/96	20	Input	$X_{L,19}^{r}, X_{L,21}^{r}, X_{R,20}^{r}$	$2^{-45.66}$
		Output	$X_{L,21}^{r+20}, X_{R,20}^{r+20}$	
Simeck64/128	26	Input	$X_{L,18}^{r}, X_{L,22}^{r}$	$2^{-62.09}$
		Output	$X_{L,22}^{r+26}, X_{R,21}^{r+26}$	

Table 5: Bias of the 13-round linear hull

$log_2(\bar{\varepsilon}^2)$	Num	Probability
$[-27.91, 0)$	56	0.056
$[-28.91, -27.91)$	123	0.123
$[-29.91, -28.91)$	154	0.154
$[-30.91, -29.91)$	151	0.151
$[-31.91, -30.91)$	144	0.144
$(-\infty, -31.91)$	372	0.372

4 Key Recovery Attack on Simeck

4.1 Key Recovery Attack on Simeck32/64

We use the 13-round linear hull

$$X_{L,1}^{r} \rightarrow X_{R,1}^{r+13}$$

obtained in section 3.2 to attack Simeck32/64. At first four more rounds before and four more rounds after the linear hull are added to get a 21-round distinguisher. Take some plaintexts or subkeys as a whole, we can get the expression for $X_{L,1}^{r}$ as $f(x,k) = x_0 \oplus k_0 \oplus f'(x',k')$, where

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

In the expression, $x' = \{x_1, ..., x_{16}\}$ and $k' = \{k_1, ..., k_{16}\}$. The details of $\{x_0, x_1, \ldots x_{16}\}$, $\{k_0, k_1, \ldots, k_{16}\}$ are given in Table 6. Notice $x_{10} = x_3 \oplus x_5$ and $x_{15} = x_4 \oplus x_8$, so there are 15 independent bits of x and 17 independent bits of k. The $X_{R,1}^{r+13}$ also can be represented as $f(x,k)$ where x,k have similar expressions as that in Table 6. (The expressions of x,k for $X_{R,1}^{r+13}$ is so similar to Table 6 that we omit them in this paper).

The x denotes the plaintexts or ciphertexts and the k denotes the subkey bits. We use $x_p = \{x_{p,0}, ..., x_{p,16}\}$ and $k_p = \{k_{p,0}, ..., k_{p,16}\}$ to represent the x,k for $X_{L,1}^{r}$. For $X_{R,1}^{r+13}$, we use x_c and k_c. Then the $X_{L,1}^{r}$ can be denoted by $f(x_p,k_p)$ and the $X_{R,1}^{r+13}$ can be denoted by $f(x_c,k_c)$.

Let the plaintexts $P = X^{r-4}$ and the ciphertexts $C = X^{r+17}$. We can compress the N pairs (P,C) into a counter vector $V[x_p,x_c]$ of size $2^{15+15} = 2^{30}$. Then the empirical correlation under some subkey k_p and k_c is

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

As we can see, $f(x,k) = x_0 \oplus k_0 \oplus f'(x',k')$ is linear with $x_0 \oplus k_0$. So the $x_{p,0}$ and $x_{c,0}$ can be compressed at first as following

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

Table 6: 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}	$K_0^{r-4} \oplus K_1^{r-3}$

The target correlation becomes

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

and the $k_{p,0}$, $k_{c,0}$ can be regarded as related bits and omitted in the calculation. We introduce how to calculate the $B^{k'}(y) = \sum_{x'} (-1)^{f'(x',k')} V'[x']$ efficiently using dynamic key-guessing techniques in the following Procedure A, where $y = f'(x', k')$ and $V'[x']$ is the num of x'. The calculation of $B^{k'_p}(y) = \sum_{x'_p} (-1)^{f'(x'_p,k'_p)} V_1[x'_p, x'_c]$ for constant x'_c is same with $B^{k'}(y)$, so calculating the $\bar{c}_{k'_p,k'_c}$ needs to call Procedure A twice.

Procedure A. The expression of $f'(x', k')$ is the same with the expression for Simon32/64, so the calculation process is similar. The details can be seen in the section 4.2 of [9], and we gives the basic ideas in the following. There are only 14 independent bits for $\{x_1, \ldots x_{16}\}$ and 16 independent bits for $\{k_1, \ldots, k_{16}\}$. We introduces the procedure briefly.

1. Guess k_1, k_3, k_7 at first.
2. Split the $f'(x', k')$ into 8 cases according to the values of $\{x_1 \oplus k_1, x_3 \oplus k_3, x_7 \oplus k_7\}$. For each case, there needs $2^8 \times 7$ additions to generate a new counter vector. Then also apply the guess, split and combine technique to calculate the partial correlation of each case, and the time is $2^{11.19}$ additions each.
3. Combine the 8 cases to get the final correlation, there needs $2^{13} \times 7$ additions.

The total time of Procedure A is

$$T = 2^3 \times (8 \times (2^8 \times 7 + 2^{11.19}) + 2^{13} \times 7) = 2^{19.46}.$$

Attack on 23 rounds. We add one more round before and one more round after the 21-round distinguisher. According the plaintexts and ciphertexts involved in the 21-round distinguisher, there needs to guess 13-bit keys in $(r-5)$-th round and 13-bit keys in $(r+17)$-th round. The estimated potential $\bar{\varepsilon}^2$ of the linear hull is $2^{-30.91}$. Set the advantage $a = 8$ and data complexity $N = 2 \times 2^{30.19} = 2^{31.19} = c_N \cdot \bar{\varepsilon}^2$. According to the experiments on the bias of the 13-round linear hull in the section 3.2 and the theory of success rate in [16], we can get the range of the success rate $(0.411, 0.532)$ of the attack in Table 7.

Table 7: Experimental results for the 13-round linear hull of Simeck32/64

$log_2(\bar{\varepsilon}^2)$	Probability p	c_N	lower success rate s_l	Upper success rate s_u
$[-27.91, 0)$	0.056	$c_N \geq 16$	1	1
$[-28.91, -27.91)$	0.123	$8 \leq c_N < 16$	0.997	1
$[-29.91, -28.91)$	0.154	$4 \leq c_N < 8$	0.867	0.997
$[-30.91, -29.91)$	0.151	$2 \leq c_N < 4$	0.477	0.867
$[-31.91, -30.91)$	0.144	$1 \leq c_N < 2$	0.188	0.477
			$\sum p \cdot s_l = 0.411$	$\sum p \cdot s_u = 0.532$

The details of the attack are as follows.

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 X^{r-4} and X^{r+17}. Then compress the N pairs (X^{r-4}, X^{r+17}) into a counter vector $V_1[x'_p, x'_c]$ of size $2^{14+14} = 2^{28}$. This step takes $N = 2^{31.91}$ times two-round encryptions and compressions.
   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 of 14 bits x'_c and 16 bits k'_p. This step needs $2^{14} \times 2^{19.46}$ 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 of 16 bits k'_p and 16 bits k'_c. This step needs $2^{16} \times 2^{19.46}$ additions.

   In total, there needs $2^{26} \times 2^{31.91}$ times two-round encryptions and $2^{26} \times (2^{33.46} + 2^{35.46}) = 2^{61.78}$ additions.
2. We have $2^{26+32} = 2^{58}$ counters now. Since the advantage is 8, so the key ranked in the largest 2^{58-8} counters can be the right key. Get 2^{56} candidates of the master key according to the the key schedule and do exhaustive search to find the right key. There needs 2^{56} times 23-round encryptions.

Attack complexity: $2^{61.78}$ additions and $2^{56.41}$ 23-round encryptions.

Implementation of the 21-round attack. If we don't consider the $(r-5)$-th round and $(r+17)$-th round in the 23-round attack, the 21-round attack needs $2^{35.78}$ additions to get 2^{24} possible values of 32 subkey bits. (Due to the time limitation, we don't do the exhaustive search to recover the whole master key).

We randomly select the master key to do experiments on the recovery of 8-bit key information for the 32 bits subkey involved in the 21-round attack. If the correct subkey bits are in the first 2^{24} counters of all the 2^{32} counters in descending order, we believe the attack is successful and can recover the correct key bits. There are 1000 master keys tested and the success rate is 0.456, which meets our expectation $(0.411, 0.531)$ and our attack algorithm is effective.

4.2 Key Recovery Attack on Simeck48/96

We use the 20-round linear hull

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

obtained in section 3.2 to attack Simeck48/96. Add 4 rounds before r-th round, we get the expression $f_B(x_B, k_B)$ for $X^r_{L,19} \oplus X^r_{L,21} \oplus X^r_{R,20}$ and the expression of $x_B = \{x_0, x_1, \ldots x_{28}\}$, $k_B = \{k_0, k_1, \ldots, k_{28}\}$ are given in Table 11 (Appendix B). Add 4 rounds after $(r+20)$-th round, we get the expression $f_C(x_C, k_C)$ for $X^{r+20}_{L,21} \oplus X^{r+20}_{R,20}$ and and the expressions of $x_C = \{x_0, x_1, \ldots x_{21}\}$, $k_C = \{k_0, k_1, \ldots, k_{21}\}$ are given in Table 12 (Appendix B). Then we can get a 28-round distinguisher for Simeck48/96.

$$\begin{aligned}
f_B(x_B, k_B) = {} & 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))]\} \\
f_C(x_C, k_C) = {} & 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}$$

For simplicity, we give the time complexity of calculating the correlation for some common boolean functions in Table 8. Case f_1 and f_2 can be found in [9] and the time complexity is $2^{6.46}$ and $2^{15.99}$. There is a little difference between the case f_2 and f_3, where $f_3 = f_2 \oplus ((x_8 \oplus k_8)\&(x_{12} \oplus k_{12}))$. Because the x_8, x_{12} and k_8, k_{12} are also involved in f_2 and compressed at first, so in the calculation using dynamic techniques the only change is the method of generating the new counter vector, and the time complexity is equal for the two cases. The case f_4 is same with the Procedure A in section 4.1 and the time complexity is $2^{19.46}$. For the similar reason like f_2 and f_3, the f_5 have a time complexity of $2^{19.46}$ as f_4.

Procedure B. Here introduces how to calculate the $B^{k_B}(y) = \sum_{x_B} (-1)^{f_B(x_B,k_B)} V_B[x]$ efficiently using dynamic key-guessing techniques. Compress the plaintexts of r-th round into a counter $V_B[x_1, ..., x_{28}]$. Since $x_{12} = x_3 \oplus x_7, x_{17} = x_4 \oplus x_{10}$, there are only 26 independent x bits.

Table 8: Time complexity for some functions

Case	Expression	Time
f_1	$(x_1 \oplus k_1 \oplus (x_2 \oplus k_2)\&(x_3 \oplus k_3))\&(x_4 \oplus k_4 \oplus (x_2 \oplus k_2)\&(x_5 \oplus k_5))$	$2^{6.46}$
f_2	$[x_1 \oplus k_1 \oplus (x_2 \oplus k_2)\&(x_3 \oplus k_3)\oplus$ $(x_4 \oplus k_4 \oplus (x_5 \oplus k_5)\&(x_6 \oplus k_6))\&(x_7 \oplus k_7 \oplus (x_6 \oplus k_6)\&(x_8 \oplus k_8))]$ $\&[x_9 \oplus k_9 \oplus (x_3 \oplus k_3)\&(x_{10} \oplus k_{10})\oplus$ $(x_7 \oplus k_7 \oplus (x_6 \oplus k_6)\&(x_8 \oplus k_8))\&(x_{11} \oplus k_{11} \oplus (x_8 \oplus k_8)\&(x_{12} \oplus k_{12}))]$	$2^{15.99}$
f_3	$f_2 \oplus ((x_8 \oplus k_8)\&(x_{12} \oplus k_{12}))$	$2^{15.99}$
f_4	$f_2 \oplus ((x_{13} \oplus k_{13})\&(x_{14} \oplus k_{14})) \oplus ((x_8 \oplus k_8)\&(x_{12} \oplus k_{12}))\oplus$ $(x_{15} \oplus k_{15} \oplus (x_2 \oplus k_2)\&(x_3 \oplus k_3))\&(x_{16} \oplus k_{16} \oplus (x_{10} \oplus k_{10})\&(x_3 \oplus k_3))$ $Notice: x_1 = x_8 \oplus x_{15}, x_9 = x_{12} \oplus x_{16}$	$2^{19.46}$
f_5	$f_4 \oplus ((x_8 \oplus k_8)\&(x_{12} \oplus k_{12}))$	$2^{19.46}$

1. Compress $\{x_1 - x_4, x_7 - x_{18}\}$ as case f_4 for each $\{x_5, x_6, x_{19} - x_{28}\}$, the time complexity is $2^{19.46}$. This step needs $2^{12} \cdot 2^{19.46} = 2^{31.46}$ additions in total. Now we have a counter vector for 16 bits keys and 12 bits x.
2. Compress $\{x_5, x_6, x_{19} - x_{28}\}$ as case f_3 for each $\{k_1 - k_4, x_7 - x_{18}\}$, the time complexity is also $2^{15.99}$. This step needs $2^{16} \cdot 2^{15.99} = 2^{31.99}$ additions in total. Now we have a counter vector for 28 bits keys.

In total, the time complexity of procedure B is $2^{31.46} + 2^{31.99} = 2^{32.75}$ additions.

Procedure C. Here introduces how to calculate the $B^{k_C}(y) = \sum_{x_C} (-1)^{f_C(x_C, k_C)} V_C[x]$ efficiently using dynamic key-guessing techniques. Compress the ciphertexts of $(r+20)$-th round into a counter $V_C[x_1, ..., x_{21}]$, since $x_{13} = x_8 \oplus x_{18}, x_{19} = x_{11} \oplus x_{21}$, there are only 19 independent x bits.

1. Compress $\{x_3 - x_7\}$ as case f_1 for each $\{x_1, x_2, x_8 - x_{21}\}$, the time complexity is $2^{6.46}$. This step needs $2^{14} \cdot 2^{6.46} = 2^{20.46}$ additions in total. Now we have a counter vector for 5 bits keys and 14 bits x.
2. Compress $\{x_1, x_2, x_8 - x_{21}\}$ as case f_5 for each $\{k_3 - k_7\}$, the time complexity is $2^{19.46}$, and this step needs $2^5 \cdot 2^{19.46} = 2^{24.46}$ additions.

In total, the time complexity of procedure C is $2^{20.46} + 2^{24.46} = 2^{24.55}$ additions.

Attack on 30 rounds. We add one more round before and one more round after the 28-round distinguisher. According the plaintexts and ciphertexts involved in the 28-round distinguisher, there needs to guess 21-bit keys in $(r-5)$-th round and 18-bit keys in $(r+24)$-th round. The estimated potential of this linear hull is $2^{-45.66}$. Set the advantage $a = 8$ and data complexity $N = 4 \times 2^{45.66} = 2^{47.66}$, the success rate is 0.867.

1. Guess 21 bits $\{K_1^{r-5}, K_3^{r-5} - K_{21}^{r-5}, K_{23}^{r-5}\}$ and 18 bits $\{K_0^{r+24}, K_4^{r+24} - K_6^{r+24}, K_8^{r+24} - K_{21}^{r+24}\}$. For each of 2^{39} values,
   a. Encrypt the plaintexts by one round and decrypt the ciphertexts by one round to get the X^{r-4} and X^{r+24}. Then compress the N pairs (X^{r-4}, X^{r+24}) into a counter vector of size 2^{45}. This step takes $N = 2^{47.66}$ times two-round encryptions and compressions.
   b. For each of 2^{19} x_C in f_C, call Procedure B. Now we have 2^{19+28} counters of 19 bits x_C and 28 bits k_B. This step needs $2^{19} \times 2^{32.75}$ additions.

c. For each of 2^{28} k_B, call Procedure C. Now we have 2^{28+21} counters of 28 bits k_B and 21 bits k_C. This step needs $2^{28} \times 2^{24.55}$ additions.

In total, this step needs $2^{39} \times 2^{47.66}$ times two-round encryptions and $2^{39} \times 2^{53.2}$ 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. Get 2^{88} candidates of the master key according to the the key schedule and do exhaustive search to find the right key.

Attack complexity: $2^{92.2}$ additions and $2^{88.04}$ 30-round encryptions.

4.3 Key Recovery Attack on Simeck64/128

We use the 26-round linear hull

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

obtained in section 3.2 to attack Simeck64/128. Add four more rounds on the top and four more rounds on the bottom to get a 34-round distinguisher. The expression $f_D(x_D, k_D)$ for the parity bits $X^r_{L,18} \oplus X^r_{L,22}$ and the details of $\{x_D, k_D\}$ are given in Appendix C. For the parity bits $X^{r+26}_{L,22} \oplus X^{r+26}_{R,21}$, it's expression is same with $f_C(x_C, k_C)$ and the details for $\{x_C, k_C\}$ are also similar that we omit them in this paper.

Then adding two more rounds before and one more round after the 34-round distinguisher we can attack the 37-round Simeck64/128. The procedure is similar with the attack on Simeck32/64 and Simeck48/96, and due to the space limitation we will not repeat it. The estimated potential of this linear hull is $2^{-62.09}$. Set the advantage $a = 8$ and data complexity $N = 2 \times 2^{62.09} = 2^{63.09}$, the success rate is 0.477. The time complexity of the 37-round attack is $2^{111.44}$ additions and $2^{121.25}$ 37-round encryptions.

5 Conclusion

In this paper, we analyzed the security of Simeck against improved linear hull cryptanalysis with dynamic key-guessing techniques. We searched out better differentials using Kölbl's tool, then got linear hulls for all versions of Simeck. With Chen *et al.*'s Guess, Split, Combine technique to reduce the time complexity in the calculation of empirical correlations, we made the improved linear hull attack on Simeck. As a result, we can attack 23-round Simeck32/64, 30-round Simeck48/96 and 37-round Simeck64/128, which are the best results so far from the point of rounds attacked. The experiments on the bias of the linear hull for Simeck32/64 met our expectation and 48.4% of the results have a bias higher than we expected. We also implemented the attack on 21-round Simeck32/64, and the success rate is 45.6% corresponding to our estimated value, which proves our algorithm is effective.

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 improved linear hull attack with dynamic key-guessing techniques for other bit-oriented block ciphers.

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. Hoda AlKhzaimi and Martin M Lauridsen. Cryptanalysis of the simon family of block ciphers. *IACR Cryptology ePrint Archive*, 2013:543, 2013.
5. Tomer Ashur. Improved linear trails for the block cipher simon. Cryptology ePrint Archive, Report 2015/285, 2015. http://eprint.iacr.org/.
6. Nasour Bagheri. Linear cryptanalysis of reduced-round simeck variants. In *Progress in Cryptology–INDOCRYPT 2015*, pages 140–152. Springer, 2015.
7. 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.
8. Alex Biryukov, Arnab Roy, and Vesselin Velichkov. Differential analysis of block ciphers simon and speck. In *Fast Software Encryption*, pages 546–570. Springer, 2014.
9. 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.
10. Stefan Kölbl, Gregor Leander, and Tyge Tiessen. Observations on the simon block cipher family.
11. Stefan Kölbl and Arnab Roy. A brief comparison of simon and simeck. Technical report, Cryptology ePrint Archive, Report 2015/706, 2015.
12. Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Advances in CryptologyEUROCRYPT93*, pages 386–397. Springer, 1994.
13. 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/.
14. Kaisa Nyberg. Linear approximation of block ciphers. In *Advances in CryptologyEUROCRYPT'94*, pages 439–444. Springer, 1995.
15. 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.
16. Ali Aydin Selçuk and Ali Biçak. *On Probability of Success in Linear and Differential Cryptanalysis*. Springer Berlin Heidelberg, 2003.
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 Linear hulls for Simeck48/96 and Simeck64/128

In this section, we list the details of how to get linear hulls for Simeck48/96 and Simeck64/128 from the differentials given in section 3.1.

Table 9: Linear hull 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	–
	$\sum_r \log_2 pr = -50$ $\log_2 p_{diff} = -43.66$ $\#trails = 1798015$		$\log_2 \epsilon^2 = -52$ $\log_2 \bar{\epsilon}^2 = -45.66$ $\#characteristics = 1798015$		

Table 10: Linear hull based on the differential for Simeck48/96

	Differential		Linear		
r	Δ_L	Δ_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
	$\sum_r \log_2 pr = -68$ $\log_2 p_{diff} = -60.09$ $\#trails = 1632506$		$\log_2 \epsilon^2 = -70$ $\log_2 \bar{\epsilon}^2 = -62.09$ $\#characteristics = 1632506$		

B Attack on Simeck48/96

In this section, we give the details of expressions of $\{x_B, k_B\}$ in $f_B(x_B, k_B)$ in Tale 11 and $\{x_C, k_C\}$ in $f_C(x_C, k_C)$ in Tale 12 for Simeck48/96.

Table 11: 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}	$K^{r-4}_{20} \oplus K^{r-3}_{21}$

C Attack on Simeck64/128

In this section, we give the details for the key recovery attack on Simeck64/128. The 26-round linear hull is

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

Add 4 rounds before r-th round, we get the expression $f_D(x_D, k_D)$ for $X^r_{L,18} \oplus X^r_{L,22}$ and the expression of $x_D = \{x_0, x_1, \ldots x_{25}\}$, $k_D = \{k_0, k_1, \ldots, k_{25}\}$ can be seen in Table 13. Add 4 rounds after $(r+26)$-th round, the expression for $X^{r+26}_{L,22} \oplus X^{r+26}_{R,21}$ is same with the $f_C(x_C, k_C)$ in Appendix B and the computation is also similar with Procedure C. We can get a 34-round distinguisher for Simeck64/128.

Table 12: 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}

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

Table 13: 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_{25}	$K^{r-4}_{21} \oplus K^{r-3}_{22}$