Linear Cryptanalysis of Reduced-Round **Simeck** Using Super Rounds

Reham Almuhlifi and Poorvi Vora

December 2022

The SIMECK family of lightweight block ciphers was proposed by Yang et al. in 2015, which combines the design features of the NSA-designed block ciphers SIMON and SPECK. Linear cryptanalysis using super-rounds was proposed by Almukhlifi and Vora to increase the efficiency of implementing Matsui's second algorithm and achieved good results on all variants of SIMON. The improved linear attacks result from the observation that, after four rounds of encryption, one bit of the left half of the state of the cipher depends on only 17 key bits (19 key bits for the larger variants of the cipher). Furthermore, due to the similarity between the design of SIMON and SIMECK, we were able to follow the same attack model and present improved linear attacks against all variants of SIMECK. In this paper, we present attacks on 19-rounds of SIMECK 32/64, 28-rounds of SIMECK 48/96, and 33-rounds of SIMECK 64/128, often with the direct recovery of the *full master key* without repeating the attack over multiple rounds. We also verified the results of linear cryptanalysis on 8, 10, and 12 rounds for SIMECK 32/64.

1 Introduction

Lightweight cryptography is one of the most active areas in the cryptographic community. In the last decade, several lightweight block ciphers have been designed that aim to work efficiently in constrained environments. SIMECK is a family of lightweight block ciphers that combines design features from SIMON and SPECK, so it makes a slightly modified round function of SIMON and uses SPECK key schedule. Hence, the similar round function makes it vulnerable to most attacks applied on SIMON, one of these attacks is the improved linear attack proposed in [1]. Due to the similarity between the design of SIMECK round function and SIMONround function, we have the same observation that enables us to apply the super-round technique. After four rounds of SIMECK 32/64 encryption, one bit of the left half of the state depends on only 16 key bits, which is equal to the size of one round key. In the right half, one bit of the state depends only on 7 key bits. Therefore, we are able to construct a super round in a similar way to the case of SIMON.

In this paper, we present the improved linear cryptanalysis on all variants of Simeck applying the super-rounds technique, which was newly proposed in [1] to improve the linear attacks on Simon-like ciphers.

1.1 Comparison with other work

We compare our results with Bagheri's [2] results which are currently the best results obtained using the classical linear Matsui's second algorithms, without recourse to linear hull results.

Bagheri presented two results, one for Matsui's first algorithm and the second set of results were for Mastui's second algorithm. Hence, we only compare with their key recovery best results which were achieved using Matsui's second algorithm.

Moreover, we had to make changes to how the data complexity was computed in his work for a fair comparison. Finally, since we are using multiple linear approximations, we apply the capacity model [3] in both our work and his.

Also, we did compute both the average case complexity and the worst case. The average case was a result of counting key bits involved in the XOR as a half bit. Where the worst case, the key bits are counted as a single bit as it has done in the literature. Therefore, we present two comparison tables.In both computations, we were able to go deeper in all variants of Simeck.

Table 1: Comparison of previous results using Matsui's second algorithm and multiple linear cryptanalysis (without recourse to linear hull) on Simeck.

Average Case Computations				
Simeck	**Number of Rounds**	**Data Complexity**	**Time Complexity**	**Presented In**
32/64	20-round	2^{30}	$2^{58.5}$	8.3
	18-round	2^{24}	$2^{61.5}$	[2]
48/96	29-round	$2^{47.42}$	$2^{92.5}$	D
	23-round	$2^{41.42}$	2^{95}	[2]
64/128	34-round	2^{61}	2^{112}	E
	27-round	2^{49}	2^{104}	[2]

Table 2: Comparison of previous results using Matsui's second algorithm and multiple linear cryptanalysis (without recourse to linear hull) on Simeck.

Worst Case Computations				
Simeck	**Number of Rounds**	**Data Complexity**	**Time Complexity**	**Presented In**
32/64	19-round	2^{30}	2^{59}	8.2
	18-round	2^{24}	2^{72}	[2]
48/96	28-round	$2^{47.42}$	2^{93}	D
	23-round	$2^{41.42}$	2^{108}	[2]
64/128	34-round	2^{61}	$2^{126.58}$	E
	27-round	2^{53}	2^{134}	[2]

1.2 Organization

The organization of this paper as follows. Section 2 summarizes the Simeck cipher, and Section 3 describes related work. Section 4 presents the idea of the super round and the super key components and Section 6 presents the linear approximations we used in this paper. Section 7 presents experimental verification, and Section 8 projected results. We conclude in Section 10.

We present the linear attacks on Simeck 48 in appendices A and B. Also, appendices C and D contain the linear attacks of Simeck 64.

2 Simeck

2.1 Notations

We do use the same notations as it been used in [1].

X^j	input to the j-th round beginning with 0
X_i	i-th bit of X beginning with 0
XL^j	the left half inputs to the j-th cipher round
XR^j	the right half inputs to the j-th cipher round
k_i^j	the i-th bit of the j-th round key
PL	left plaintext half
PR	right plaintext half
CL	left ciphertext half
CR	right ciphertext half
$\oplus$	bitwise exclusive OR (XOR)
$\&$	bitwise AND
$X \lll z$	cycle shift to the left by z bits

2.2 Description of Simeck

There are three versions of Simeck, which is denoted by Simeck$2n/mn$, where n is the word size, m is the number of key words and $2n$ is the block size. The following table 3 shows the specification of other variants.

Table 3: Simeck parameters.

Block Size 2n	Key Size mn	Word Size n	Key Words m	Number of Rounds
Simon 32	64	16	4	32
Simeck 48	96	24	4	36
Simon 64	128	32	4	44

The round function (see Figure 1). is defined as:

$$(XL^{j+1}, XR^{j+1}) = R_{k^j}(XL^j, XR^j) = (XR^j \oplus F(XL^j) \oplus k^j, XL^j). \tag{1}$$

where:

$$F(XL^j) = [(XL^j)\&(XL^j \lll 5)] \oplus XL^j \lll 1) \tag{2}$$

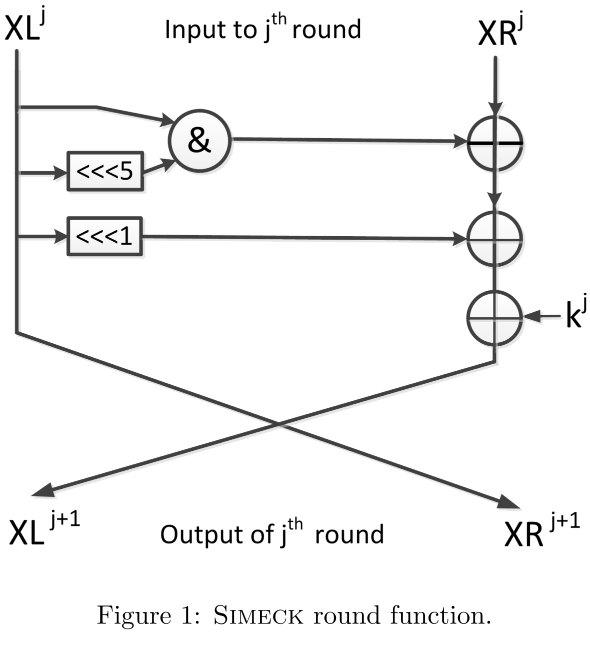


Figure 1: Simeck round function.

The key schedule takes the master key K as an input and generates r subkeys $k^0, k^1, ...k^{r-1}$. The initial states of the feedback shift registers (t_2, t_1, t_0, k_0) are initialized with the master key words. Then, they apply the round function to update the registers and generate the round keys. The updating process is defined as follows:

$k_{i+1} = t_i$, $t_{i+3} = k_i \oplus f(t_i) \oplus C \oplus (z_j)_i$, where $0 \leq i \leq T-1$, $C = 2^n - 4$, n is the word size, $(z_j)_i$ is the i-th bit of z_j.

The sequence z_j for SIMECK32/64 and SIMECK48/96 is generated by the primitive polynomial $X^5 + X^2 + 1$ with the initial states (1, 1, 1, 1, 1). For SIMECK 64/128, the zj is generated by the primitive polynomial $X^6 + X + 1$ with the initial states (1, 1, 1, 1, 1, 1).

3 Related Work

Due to the similarity between the design of SIMON and SIMECK, most of the attacks that have been used against SIMON, is applicable on SIMECK. Hence, the designers of SIMECK have analyzed the security of the cipher against linear and differential cryptanalysis using the best attacks that have been presented on SIMON. In [10], they evaluate the security of SIMECK and conclude with the possibility of launching differential attack covers 19, 20, and 26 rounds of SIMECK32/64, 48 and 128 respectively. Similarly, they present linear cryptanalysis and introduce attacks on 12, 15, and 19 rounds of SIMECK32/64, 48, and 128, respectively.

Bagheri [2] applied the classical linear attacks, which are also considered the best results using the classical linear cryptanalysis. Applying Matsui's first algorithm, they were able to attack 14, 19, and 23 rounds of SIMECK 32/64, 48/96, and 64/128, respectively. Moreover, they successfully present attacks against 18, 24, and 27 rounds using Matsui's second algorithm.

In 2016, Kölbl et al. [5], presented a comparison between SIMON and SIMECK in terms of the upper bounds of the linear and differential trails . Additionally, they present differential attacks against 19, 26 and 33 rounds on SIMECK 32, SIMECK 48, and SIMECK 64 respectively.

Soon later, Qiao et al. [7], successfully were able to present differential attacks using a new technique named dynamic key guessing to attack 22, 28 and 35 rounds on SIMECK 32, SIMECK 48, and SIMECK 64 respectively.

Chin et al. [8] evaluated the security of SIMECK against linear hull cryptanalysis, which is considered the best linear results on SIMECK had been achieved using the linear hull approach. They were able to attack 23, 30 and 37 rounds on SIMECK 32, SIMECK 48, and SIMECK 64 respectively.

Moreover, there have been more results using other cryptanalysis techniques such as zero-correlation and integral attacks.

One of the powerful attack methods recently proposed is zero-correlation linear cryptanalysis [4] which relies on using linear trails with a probability of 0.5. In 2018, Zhang et al. [11] evaluate the security of SIMECK against such an attack. Hence, they present attacks on 20-rounds, 24-rounds and 27-rounds of SIMECK 32, SIMECK 48, and SIMECK 64 respectively.

Moreover, Bagheri and Sadeghi [9] improved these results and presented better attacks using zero-correlation linear trails on SIMECK48 and SIMECK64.

They were able to attack 27-round Simeck48 and 31-round Simeck64.

4 Linear Cryptanalysis with Super Rounds

Linear cryptanalysis is one of the most powerful attacks on iterative block ciphers. In 2020, Almuhlifi and Vora proposed an improved linear attack to significantly increase the recovery attack efficiency using Matsui's second algorithm. The super-round technique essentially works by partitioning the key into smaller parts. The efficiency of this technique depends on reducing the number of key bits require to guess. The standard technique to extend a linear approximation by one round decryption is usually achieved by guessing the full last round key. Hence, the proposed improved technique takes advantage of the fact that one bit depends on only 16 key bits; instead of extending the linear approximation by one round, it can be extended by four rounds with the same cost. Therefore, we apply the super-round technique to recover multiple rounds keys, including the master key for all variants of Simeck, and attack more rounds using Matsui's second algorithm.

The general method of applying Matsui's second algorithm using super rounds as described in [1], is by deriving linear approximations that have a single bit of input —XL_i^4 or XR_i^4, and multiple bits of the ciphertexts (see Figure 2).

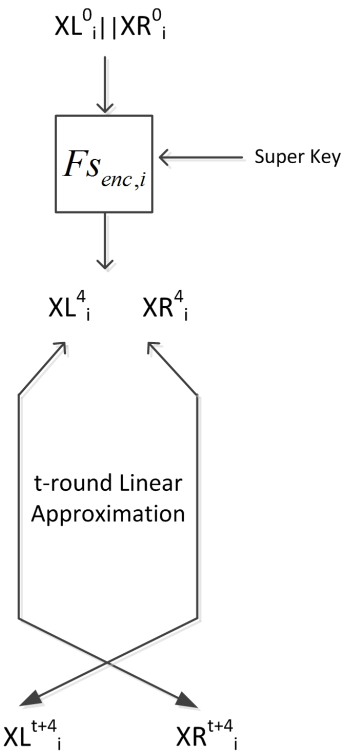


Figure 2: General form of linear attack with super rounds.

In the following, we illustrate the general principles of super rounds. For more details, we refer the readers to [1]'s work.

4.1 The Super Round

The term super round defined in [1] as a function of block cipher representing s-rounds of encryption of the cipher. In the case of Simeck, it represents a four-round encryption.

In the case of Simeck 32/64, there are two super-rounds, as it is shown in Figure 3. There is a super-round that represents the first four rounds, which requires a super key for the left half of size 16 bits and has as a output a single bit of the left half of the cipher text. A similar super round that requires a super key for the right half of size 7 bits shown on the right side of Figure 3. In the case of the other variants Simeck48/96 and Simeck64/128, even though they correspond to larger block and key size, the construction of super-rounds with the exact size of the super keys is applicable.

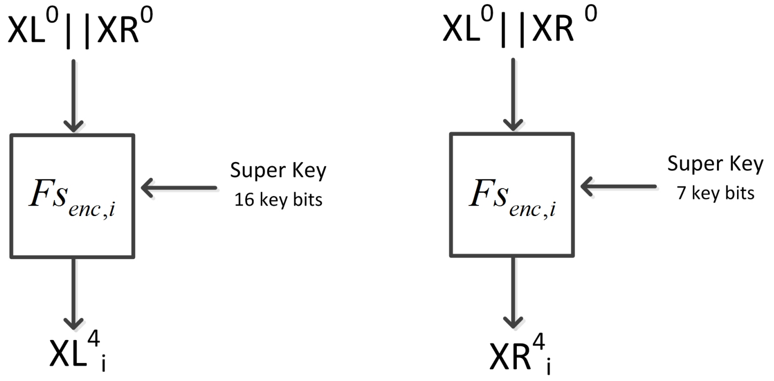


Figure 3: The super rounds.

5 Linear Cryptanalysis with Super Rounds on Simeck

Here, we describe the construction of super rounds and the derivation of super keys for Simeck32/64.

5.1 The Construction of Super Rounds and Derivations of Super Keys

In this section, we demonstrate the construction of the super rounds of Simeck 32/64.

Recall equation (1), describing the round function of Simeck:

$$(XL^{j+1}, XR^{j+1}) = R_{k^j}(XL^j, XR^j) = (XR^j \oplus F(XL^j) \oplus k^j, XL^j)$$

which implies that:

$$\begin{aligned} XL_i^{j+1} &= XR_i^j \oplus Z_i^j \oplus k_i^j \\ &= XL_i^{j-1} \oplus Z_i^j \oplus k_i^j \\ &= XL_i^{j-3} \oplus Z_i^{j-2} \oplus k_i^{j-2} \oplus Z_i^j \oplus k_i^j \end{aligned}$$

And hence that:

$$XL_i^4 = XL_i^0 \oplus Z_i^1 \oplus k_i^1 \oplus Z_i^3 \oplus k_i^3 = PL_i \oplus Z_i^1 \oplus k_i^1 \oplus Z_i^3 \oplus k_i^3$$

Similarly,

$$\begin{aligned} XR_i^{j+1} &= XL_i^j \\ &= XL_i^{j-2} \oplus Z_i^{j-1} \oplus k_i^{j-1} \\ &= XR_i^{j-3} \oplus Z_i^{j-3} \oplus k_i^{j-3} \oplus Z_i^{j-1} \oplus k_i^{j-1} \end{aligned}$$

and hence that:

$$XR_i^4 = XR_i^0 \oplus Z_i^0 \oplus k_i^0 \oplus Z_i^2 \oplus k_i^2 = PR_i \oplus Z_i^0 \oplus k_i^0 \oplus Z_i^2 \oplus k_i^2$$

Now recall equation (2):

$$F(XL^j) = [(XL^j)\&(XL^j \lll 5)] \oplus XL^j \lll 1)$$

which implies that:

$$Z_i^j = (XL_i^j \& XL_{i+5}^j) \oplus XL_{i+1}^j$$

giving us:

$$\begin{aligned}
Z_i^0 &= (PL_i \& PL_{i+5}) \oplus PL_{i+1} \\
Z_i^1 &= [(Z_i^0 \oplus k_i^0 \oplus PR_i)\&(Z_{i+5}^0 \oplus k_{i+5}^0 \oplus PR_{i+5})] \oplus (Z_{i+1}^0 \oplus k_{i+1}^0 \oplus PR_{i+1}) \\
Z_i^2 &= [(Z_i^1 \oplus k_i^1 \oplus XR_i^1)\&(Z_{i+5}^1 \oplus k_{i+5}^1 \oplus XR_{i+5}^1)] \oplus (Z_{i+1}^1 \oplus k_{i+1}^1 \oplus XR_{i+1}^1) \\
&= [(Z_i^1 \oplus k_i^1 \oplus PL_i)\&(Z_{i+5}^1 \oplus k_{i+5}^1 \oplus PL_{i+5})] \oplus (Z_{i+1}^1 \oplus k_{i+1}^1 \oplus PL_{i+1}) \\
Z_i^3 &= (v_1 \& v_2) \oplus v_3
\end{aligned}$$

where:

$$\begin{aligned}
v_1 &= Z_i^2 \oplus k_i^2 \oplus XR_i^2 && = Z_i^2 \oplus k_i^2 \oplus XL_i^1 && = Z_i^2 \oplus Z_i^0 \oplus k_i^0 \oplus PR_i \oplus k_i^2 \\
v_2 &= Z_{i+5}^2 \oplus k_{i+5}^2 \oplus XR_{i+5}^2 && = Z_{i+5}^2 \oplus k_{i+5}^2 \oplus XL_{i+5}^1 && = Z_{i+5}^2 \oplus Z_{i+5}^0 \oplus k_{i+5}^0 \oplus PR_{i+5} \oplus k_{i+5}^2 \\
v_3 &= Z_{i+1}^2 \oplus k_{i+1}^2 \oplus XR_{i+1}^2 && = Z_{i+1}^2 \oplus k_{i+1}^2 \oplus XL_{i+1}^1 && = Z_{i+1}^2 \oplus Z_{i+1}^0 \oplus k_{i+1}^0 \oplus PR_{i+1} \oplus k_{i+1}^2
\end{aligned}$$

Finally,

$$\begin{aligned}
XL_i^4 &= Z_i^3 \oplus k_i^3 \oplus XR_i^3 && = Z_i^3 \oplus k_i^3 \oplus XL_i^2 && = Z_i^3 \oplus k_i^3 \oplus Z_i^1 \oplus k_i^1 \oplus PL_i \\
XR_i^4 &= XL_i^3 && = XL_i^1 \oplus Z_i^2 \oplus k_i^2 && = PR_i \oplus k_i^0 \oplus Z_i^0 \oplus Z_i^2 \oplus k_i^2
\end{aligned}$$

5.2 The Super Key

There is a super key corresponding for each of the super rounds depicted in Figure 3. The following table lists the components of the left and the right super keys, according to the equations described in section 5.1.

Super-key of the left-half	Super-key of the right-half
$k_i^0 \oplus k_{i+2}^0 \oplus k_{i+1}^1 \oplus k_i^2$	$k_{i+1}^0 \oplus k_i^1$
$k_{i+5}^0 \oplus k_{i+7}^0 \oplus k_{i+6}^1 \oplus k_{i+5}^2$	$k_{i+6}^0 \oplus k_{i+5}^1$
$k_{i+1}^0 \oplus k_i^1$	k_i^0
$k_{i+6}^0 \oplus k_{i+5}^1$	k_{i+1}^0
$k_{i+11}^0 \oplus k_{i+10}^1$	k_{i+6}^0
$k_{i+2}^0 \oplus k_{i+1}^1$	k_{i+5}^0
$k_{i+7}^0 \oplus k_{i+6}^1$	k_{i+10}^0
k_{i+1}^0	
k_i^0	
k_{i+2}^0	
k_{i+5}^0	
k_{i+6}^0	
k_{i+7}^0	
k_{i+10}^0	
k_{i+11}^0	
k_{i+15}^0	

Table 4: Super Keys

From the table above, it can be seen that the super key of the left half contains nine bits of k^0, in the form k_{i+m}^0 for $m = 0, 1, 2, 5, 6, 7, 10, 11, 15$. In addition to five bits comes from the super key of the right half, in the form k_{i+m}^0 for $m = 0, 1, 5, 6, 10$. As a result of this redundancy, we will get nine copies, five copies of each bit of k^0, for every super key of the left half and right half of the state, respectively.

As a result of determining the sixteen bits of XL^4 and XR^4, we obtain:

- 14 copies of k_s^0
- 7 copies of $k_s^0 \oplus k_{s+1}^1$
- 2 copies of $k_s^0 \oplus k_{s+2}^0 \oplus k_{s+1}^1 \oplus k_s^2$

for $s = 0, 1, 2, ..., 15$.

Thus, obtaining the sixteen super keys for the left and right halves of Simeck32/64, we can estimate 48 independent key bits, consisting of k^0,k^1, and k^2. However, in [1], they use the majority vote to determine the value of the individual key bits. Hence, the final estimation of each bit is one of the three states, correctly determined bits, incorrectly determined bits, and undetermined bits.

6 Linear Approximations for Simeck 32/64

In this section, we describe 8-round, 10-round, and 12-round attacks using super-rounds of Simeck32/64. These attacks are similar to previous work [1] done on

SIMON. At first, we discuss how to derive the required linear approximations. Note that the only non-linear expression in SIMECK round function is the bit-wise AND [2]. Thus, we can approximate the result of the bit-wise AND by 0 with a probability of 0.75. Hence, there are four equivalent approximations can be used:

$$
\begin{aligned}
&Approximation1 : Pr[F(XL_i^{j+1}) = XL_{i+1}^j] = \frac{3}{4}\\
&Approximation2 : Pr[F(XL_i^{j+1}) = XL_{i+1}^j \oplus XL_i^j] = \frac{3}{4}\\
&Approximation3 : Pr[F(XL_i^{j+1}) = XL_{i+1}^j \oplus XL_{i+5}^j] = \frac{3}{4}\\
&Approximation4 : Pr[F(XL_i^{j+1}) = XL_{i+1}^j \oplus XL_i^j \oplus XL_{i+5}^j] = \frac{1}{4}
\end{aligned}
$$

6.1 8-round Attack

Following the attack procedure of SIMON presented in [1], we need to derive two linear approximations for the left and the right half inputs. The approximations have a single bit of the input related to a few output bits after four rounds.

Deriving a 4-round linear approximation that relates a single bit of the input; hence we use the super rounds to obtain a single bit of input and then concatenate it with the approximation. Figure 4 depicts the 8-round attack.

Given Approximation 1, we extract a 4-round linear approximation for the left half with bias 2^{-5} as the following:

$$
\begin{aligned}
PL_i &= XL_i^0 = XR_i^1\\
&= F(XR^2)_i \oplus XL_i^2 \oplus k_i^1\\
&\approx XR_{i+1}^2 \oplus XL_i^2 \oplus k_i^1\\
&= XR_{i+1}^2 \oplus XL_i^2 \oplus k_i^1\\
&= F(XR^3)_{i+1} \oplus XL_{i+1}^3 \oplus k_{i+1}^2 \oplus XR_i^3 \oplus k_i^1\\
&\approx XR_{i+2}^3 \oplus XL_{i+1}^3 \oplus k_{i+1}^2 \oplus XR_i^3 \oplus k_i^1\\
&= XR_{i,i+2}^3 \oplus XL_{i+1}^3 \oplus k_{i+1}^2 \oplus k_i^1\\
&= F(XR^4)_{i,i+2} \oplus XL_{i,i+2}^4 \oplus k_{i,i+2}^3 \oplus XR_{i+1}^4 \oplus k_{i+1}^2 \oplus k_i^1\\
&\approx XR_{i+1,i+3}^4 \oplus XR_{i+1}^4 \oplus XL_{i,i+2}^4 \oplus k_{i,i+2}^3 \oplus k_{i+1}^2 \oplus k_i^1\\
&= XR_{i+3}^4 \oplus XL_{i,i+2}^4 \oplus k_{i,i+2}^3 \oplus k_{i+1}^2 \oplus k_i^1
\end{aligned}
\tag{3}
$$

Similarly, we extract a 4-round linear approximation that relates a single bit of the right half input with bias=2^{-6}:

$$\begin{aligned}
PR_i = XR_i^0 &= F(XR^1)_i \oplus XL_i^1 \oplus k_i^0 \\
&\approx XR_{i+1}^1 \oplus XL_i^1 \oplus k_i^0 \\
&= F(XR^2)_{i+1} \oplus XL_{i+1}^2 \oplus k_{i+1}^1 \oplus XR_i^2 \oplus k_i^0 \\
&\approx XR_{i+2}^2 \oplus XL_{i+1}^2 \oplus k_{i+1}^1 \oplus XR_i^2 \oplus k_i^0 \\
&= XR_{i,i+2}^2 \oplus XL_{i+1}^2 \oplus k_{i+1}^1 \oplus k_i^0 \\
&= F(XR^3)_{i,i+2} \oplus XL_{i,i+2}^3 \oplus k_{i,i+2}^2 \oplus XL_{i+1}^2 \oplus k_{i+1}^1 \oplus k_i^0 \\
&\approx XR_{i+1,i+3}^3 \oplus XL_{i,i+2}^3 \oplus k_{i,i+2}^2 \oplus XR_{i+1}^3 \oplus k_{i+1}^1 \oplus k_i^0 \\
&= XR_{i+3}^3 \oplus XL_{i,i+2}^3 \oplus k_{i,i+2}^2 \oplus k_{i+1}^1 \oplus k_i^0 \\
&= F(XR^4)_{i+3} \oplus XL_{i+3}^4 \oplus k_{i+3}^3 \oplus XR_{i,i+2}^4 \oplus k_{i,i+2}^2 \oplus k_{i+1}^1 \oplus k_i^0 \\
&= XR_{i,i+2,i+4}^4 \oplus XL_{i+3}^4 \oplus k_{i+3}^3 \oplus k_{i,i+2}^2 \oplus k_{i+1}^1 \oplus k_i^0
\end{aligned} \tag{4}$$

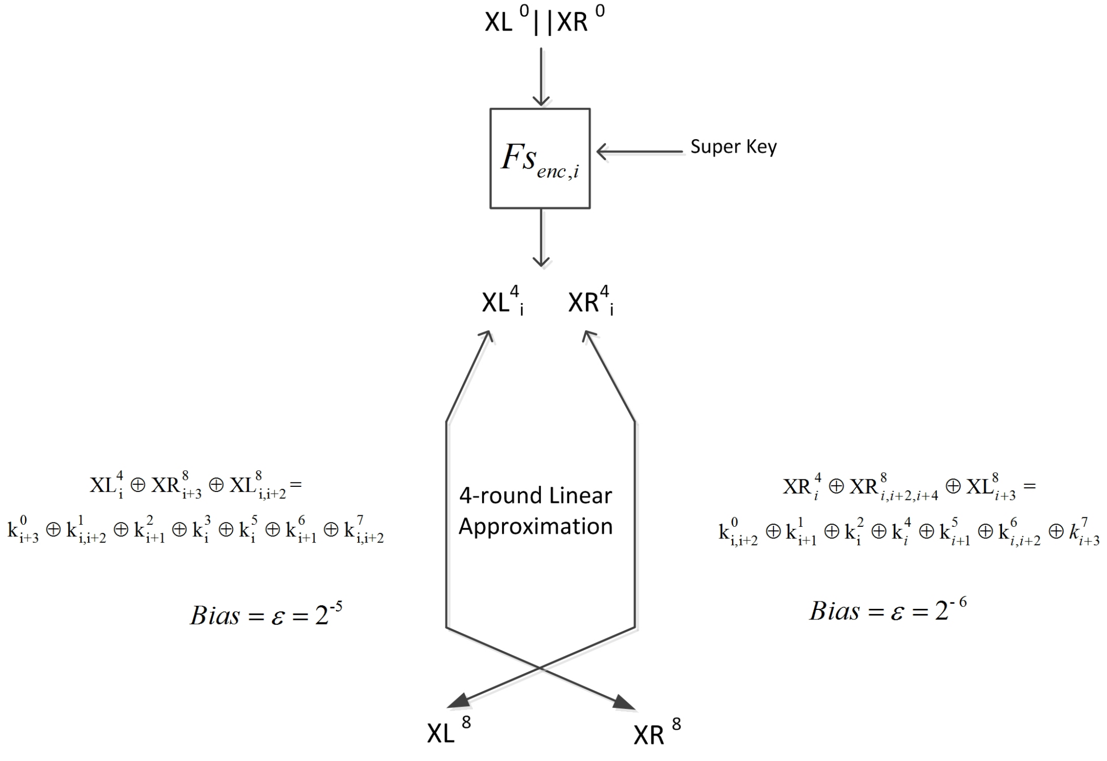

$XL^0 || XR^0$
$Fs_{enc,i}$
Super Key
XL_i^4
XR_i^4
4-round Linear Approximation
$XL_i^4 \oplus XR_{i+3}^8 \oplus XL_{i,i+2}^8 =$
$k_{i+3}^0 \oplus k_{i,i+2}^1 \oplus k_{i+1}^2 \oplus k_i^3 \oplus k_i^5 \oplus k_{i+1}^6 \oplus k_{i,i+2}^7$
$Bias = \varepsilon = 2^{-5}$
$XR_i^4 \oplus XR_{i,i+2,i+4}^8 \oplus XL_{i+3}^8 =$
$k_{i,i+2}^0 \oplus k_{i+1}^1 \oplus k_i^2 \oplus k_i^4 \oplus k_{i+1}^5 \oplus k_{i,i+2}^6 \oplus k_{i+3}^7$
$Bias = \varepsilon = 2^{-6}$
XL^8
XR^8

Figure 4: 8-Round Linear Attack

Now, we can append the super round to the 4-round approximations Equations (3) and (4) to relate the plaintext to the single bit of super round output.

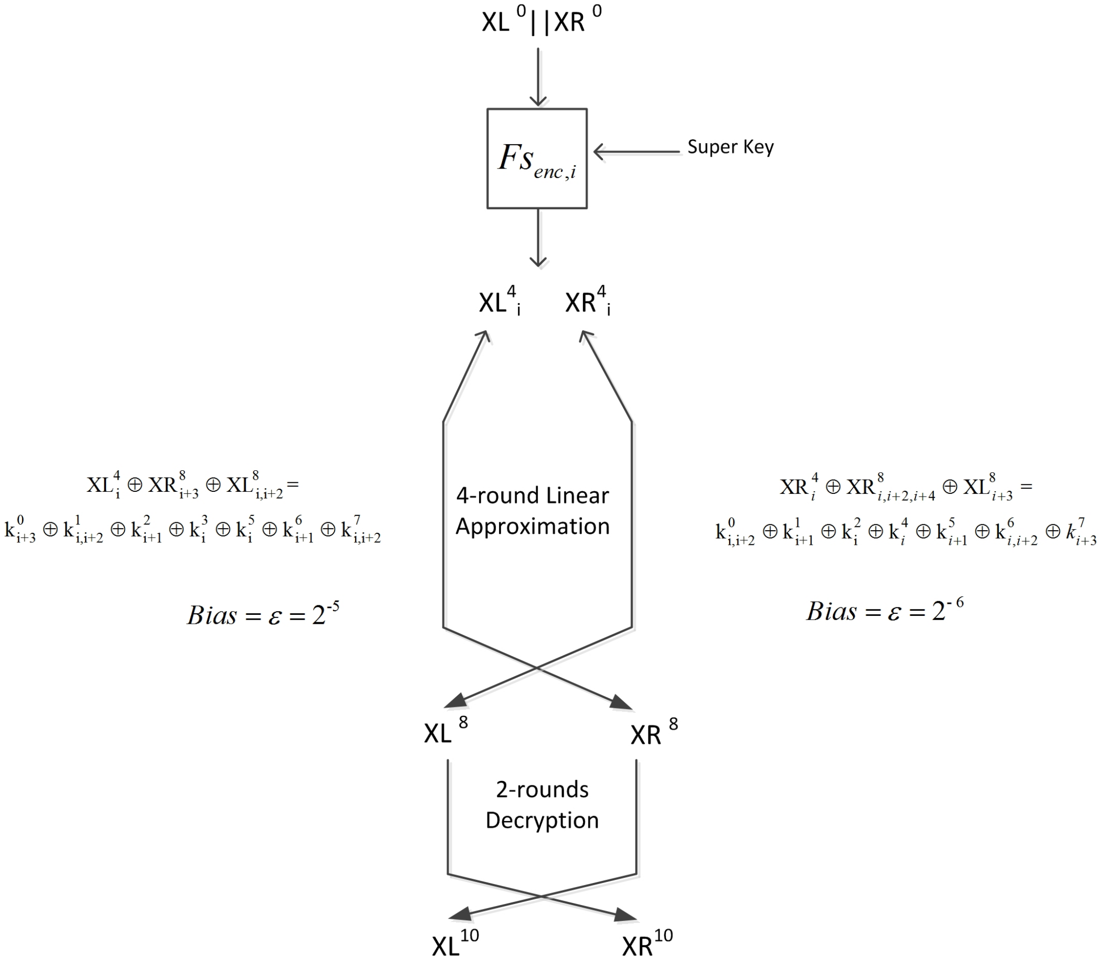
Thus we obtain an approximate relationship between plaintext, ciphertext, and super key bits. This extension enables up to attack up to eight rounds without reducing the bias further. This gives us the following expressions:

$$XL_i^4 \oplus XR_{i+3}^8 \oplus XL_{i,i+2}^8 = k_{i,i+2}^7 \oplus k_{i+1}^6 \oplus k_i^5 \tag{5}$$

$$XR_i^4 \oplus XR_{i,i+2,i+4}^8 \oplus XL_{i+3}^8 = k_{i+3}^7 \oplus k_{i,i+2}^6 \oplus k_{i+1}^5 \oplus k_i^4 \tag{6}$$

6.2 10-Round Attack

Adding two rounds of decryption at the end of the 8-round attack and get a 10-round attack. This extension comes at the cost of guessing a few bits of the last round key. Figure 5 depicts the 10-round linear attack.



$XL^0||XR^0$
$Fs_{enc,i}$
Super Key
XL_i^4
XR_i^4
$XL_i^4 \oplus XR_{i+3}^8 \oplus XL_{i,i+2}^8 =$
$k_{i+3}^0 \oplus k_{i,i+2}^1 \oplus k_{i+1}^2 \oplus k_i^3 \oplus k_i^5 \oplus k_{i+1}^6 \oplus k_{i,i+2}^7$
$Bias = \varepsilon = 2^{-5}$
4-round Linear Approximation
$XR_i^4 \oplus XR_{i,i+2,i+4}^8 \oplus XL_{i+3}^8 =$
$k_{i,i+2}^0 \oplus k_{i+1}^1 \oplus k_i^2 \oplus k_i^4 \oplus k_{i+1}^5 \oplus k_{i,i+2}^6 \oplus k_{i+3}^7$
$Bias = \varepsilon = 2^{-6}$
XL^8
XR^8
2-rounds Decryption
XL^{10}
XR^{10}

Figure 5: 10-Round Linear Attack

Single-round decryption can be expressed with the following equation [1]:

$$\begin{aligned} XL^j &= XR^{j+1} \\ XR^j &= F(XR^{j+1}) \oplus XL^{j+1} \oplus k^j, \end{aligned}$$

so, the two rounds decryption can be written as following:

$$\begin{aligned} XL^j &= F(XR^{j+2}) \oplus XL^{j+2} \oplus k^{j+1} \\ XR^j &= F(F(XR^{j+2}) \oplus XL^{j+2} \oplus k^{j+1}) \oplus XR^{j+2} \oplus k^j, \end{aligned}$$

Recall Equation 7:

$$XL_i^4 \oplus XR_{i+3}^8 \oplus XL_{i,i+2}^8 = k_{i,i+2}^7 \oplus k_{i+1}^6 \oplus k_i^5 \tag{7}$$

Rewrite X^8 in terms of X^{10}, which gives us:

$$\begin{aligned} XL^8 &= F(XR^{10}) \oplus XL^{10} \oplus k^9 \\ XR^8 &= F(F(XR^{10}) \oplus XL^{10} \oplus k^9) \oplus XR^{10} \oplus k^8 \end{aligned} \tag{8}$$

Substitute the expression of XL^8 and XR^8, we got:

$$XL_i^4 \oplus XR_{i+3}^8 \oplus XL_{i,i+2}^8 = k_{i,i+2}^7 \oplus k_{i+1}^6 \oplus k_i^5$$

$$\begin{aligned} & XL_i^4 \oplus F(XR_{i+3}^9) \oplus XL_{i+3}^9 \oplus k_{i+3}^8 \oplus XR_{i,i+2}^9 \\ & = k_{i,i+2}^7 \oplus k_{i+1}^6 \oplus k_i^5 \end{aligned}$$

$$\begin{aligned} & XL_i^4 \oplus (XR_{i+3}^9 \& XR_{i+8}^9) \oplus XR_{i+4}^9 \oplus XL_{i+3}^9 \oplus k_{i+3}^8 \oplus XR_{i,i+2}^9 \\ & = k_{i,i+2}^7 \oplus k_{i+1}^6 \oplus k_i^5 \end{aligned}$$

Hence, the 10-round expression for the left-half is:

$$\begin{aligned} & XL_i^4 \oplus (F(XR_{i+3}^{10}) \oplus XL_{i+3}^{10} \oplus k_{i+3}^9 \& F(XR_{i+8}^{10}) \oplus XL_{i+8}^{10} \oplus k_{i+8}^9) \oplus F(XR_{i+4}^{10}) \oplus XL_{i+4}^{10} \\ & = k_{i+4}^9 \oplus XR_{i+3}^{10} \oplus k_{i+3}^8 \oplus F(XR_{i,i+2}^{10}) \oplus XL_{i,i+2}^{10} \oplus k_{i,i+2}^9 = k_{i,i+2}^7 \oplus k_{i+1}^6 \oplus k_i^5 \end{aligned} \tag{9}$$

Following the same approach, we extend the 4-round linear approximation for the right half, and add two rounds decryption:

$$XR_i^4 \oplus XR_{i,i+2,i+4}^8 \oplus XL_{i+3}^8 = k_{i+3}^7 \oplus k_{i,i+2}^6 \oplus k_{i+1}^5 \oplus k_i^4$$

$$XR_i^4 \oplus F(XR_{i,i+2,i+4}^9) \oplus XL_{i,i+2,i+4}^9 \oplus k_{i,i+2,i+4}^8 \oplus XR_{i+3}^9 = k_{i+3}^7 \oplus k_{i,i+2}^6 \oplus k_{i+1}^5 \oplus k_i^4$$

$$XR_i^4 \oplus (XR_i^9 \& XR_{i+5}^9) \oplus (XR_{i+2}^9 \& XR_{i+7}^9) \oplus (XR_{i+4}^9 \& XR_{i+9}^9) \oplus XR_{i+1,i+3,i+5}^9 \oplus XL_{i,i+2,i+4}^9 \oplus k_{i,i+2,i+4}^8 \oplus XR_{i+3}^9 = k_{i+3}^7 \oplus k_{i,i+2}^6 \oplus k_{i+1}^5 \oplus k_i^4$$

$$XR_i^4 \oplus (XR_i^9 \& XR_{i+5}^9) \oplus (XR_{i+2}^9 \& XR_{i+7}^9) \oplus (XR_{i+4}^9 \& XR_{i+9}^9) \oplus XR_{i+1,i+5}^9 \oplus XR_{i,i+2,i+4}^{10} = k_{i,i+2,i+4}^8 \oplus k_{i+3}^7 \oplus k_{i,i+2}^6 \oplus k_{i+1}^5 \oplus k_i^4$$

Thus, the 10-round linear expression for the right half is:

$$\begin{aligned} & XR_i^4 \oplus (F(XR_i^{10}) \oplus XL_i^{10} \oplus k_i^9 \& F(XR_{i+5}^{10}) \oplus XL_{i+5}^{10} \oplus k_{i+5}^9) \oplus \\ & (F(XR_{i+2}^{10}) \oplus XL_{i+2}^{10} \oplus k_{i+2}^9 \& F(XR_{i+7}^{10}) \oplus XL_{i+7}^{10} \oplus k_{i+7}^9) \oplus \\ & (F(XR_{i+4}^{10}) \oplus XL_{i+4}^{10} \oplus k_{i+4}^9 \& F(XR_{i+9}^{10}) \oplus XL_{i+9}^{10} \oplus k_{i+9}^9) \oplus \\ & F(XR_{i+1,i+5}^{10}) \oplus XL_{i+1,i+5}^{10} \oplus k_{i+1,i+5}^9 \oplus XR_{i,i+2,i+4}^{10} = \\ & k_{i,i+2,i+4}^8 \oplus k_{i+3}^7 \oplus k_{i,i+2}^6 \oplus k_{i+1}^5 \oplus k_i^4 \end{aligned} \tag{10}$$

In addition to the 16 and 7 key bits required to get the input bits for the left and the right half, respectively, there are extra key bits required to evaluate the Equations 9 and 10. There are two key bits k_{i+3}^9 and k_{i+8}^9 to evaluate Equation 9 and six key bits k_i^9, k_{i+5}^9, k_{i+2}^9, k_{i+7}^9, k_{i+4}^9, and k_{i+9}^9 to evaluate Equation 10.

6.3 12-Round Attack

Here, we extend the 4-round linear approximations Equations 3 and 4 into 7-round linear approximations Equations 11 and 12 for the left and the right half with biases 2^{-10} and 2^{-12} respectively (see Tables 10 and 11 for the derivation):

$$PL_i \oplus XR_{i,i+4}^7 \oplus XL_{i+1}^7 = k_{i+1}^6 \oplus k_{i,i+2,i+4}^5 \oplus k_{i+3}^4 \oplus k_{i,i+2}^3 \oplus k_{i+1}^2 \oplus k_i^1 \tag{11}$$

$$PR_i \oplus XL_{i,i+4}^7 = k_{i,i+4}^6 \oplus k_{i+1}^5 \oplus k_{i,i+2,i+4}^4 \oplus k_{i+3}^3 \oplus k_{i,i+2}^2 \oplus k_{i+1}^1 \oplus k_i^0 \tag{12}$$

Thus, we obtain the 11-round linear trails by appending the super round at the beginning of Equations 11 and 12, as follows:

$$XL_i^4 \oplus XR_{i,i+4}^{11} \oplus XL_{i+1}^{11} = k_{i+1}^{10} \oplus k_{i,i+2,i+4}^9 \oplus k_{i+3}^8 \oplus k_{i,i+2}^7 \oplus k_{i+1}^6 \oplus k_i^5 \tag{13}$$

$$XR_i^4 \oplus XL_{i,i+4}^{11} = k_{i,i+4}^{10} \oplus k_{i+1}^9 \oplus k_{i,i+2,i+4}^8 \oplus k_{i+3}^7 \oplus k_{i,i+2}^6 \oplus k_{i+1}^5 \oplus k_i^4 \tag{14}$$

Then, we add one more round of decryption at the end of the 11-round trails and get the following 12-round trails for the left-half:

$$XL_i^4 \oplus XR_{i,i+4}^{11} \oplus XL_{i+1}^{11} = k_{i+1}^{10} \oplus k_{i,i+2,i+4}^{9} \oplus k_{i+3}^{8} \oplus k_{i,i+2}^{7} \oplus k_{i+1}^{6} \oplus k_i^5$$

$$XL_i^4 \oplus F(XR_{i,i+4}^{12}) \oplus XL_{i,i+4}^{12} \oplus k_{i,i+4}^{11} \oplus XR_{i+1}^{12} \oplus k_{i+1}^{10} \oplus k_{i,i+2,i+4}^{9} \oplus k_{i+3}^{8} \oplus k_{i,i+2}^{7} \oplus k_{i+1}^{6} \oplus k_i^5$$

$$\begin{aligned}&XL_i^4 \oplus (XR_i^{12} \& XR_{i+5}^{12}) \oplus (XR_{i+4}^{12} \& XR_{i+9}^{12}) \oplus XR_{i+5}^{12} \oplus XL_{i,i+4}^{12} = k_{i,i+4}^{11} \oplus k_{i+1}^{10} \oplus k_{i,i+2,i+4}^{9} \\ &\oplus k_{i+3}^{8} \oplus k_{i,i+2}^{7} \oplus k_{i+1}^{6} \oplus k_i^5\end{aligned} \tag{15}$$

Similarly, for the 11-round linear approximation for the right half:

$$\begin{aligned}XR_i^4 \oplus XL_{i,i+4}^{11} &= k_{i,i+4}^{10} \oplus k_{i+1}^{9} \oplus k_{i,i+2,i+4}^{8} \oplus k_{i+3}^{7} \oplus k_{i,i+2}^{6} \oplus k_{i+1}^{5} \oplus k_i^4 \\ XR_i^4 \oplus XR_{i,i+4}^{12} &= k_{i,i+4}^{10} \oplus k_{i+1}^{9} \oplus k_{i,i+2,i+4}^{8} \oplus k_{i+3}^{7} \oplus k_{i,i+2}^{6} \oplus k_{i+1}^{5} \oplus k_i^4\end{aligned} \tag{16}$$

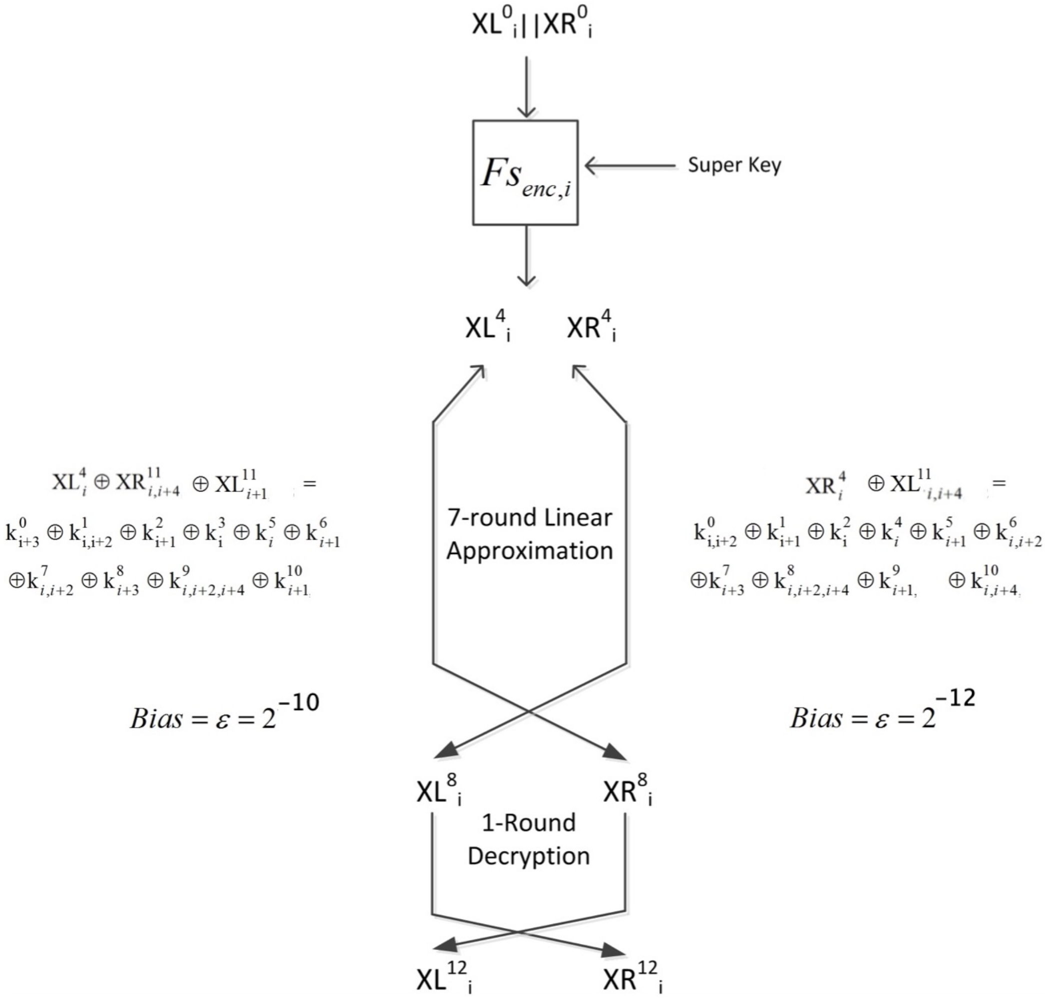

$XL^0_i||XR^0_i$
$Fs_{enc,i}$
Super Key
XL^4_i
XR^4_i
$XL^4_i \oplus XR^{11}_{i,i+4} \oplus XL^{11}_{i+1} =$
$k^0_{i+3} \oplus k^1_{i,i+2} \oplus k^2_{i+1} \oplus k^3_i \oplus k^5_i \oplus k^6_{i+1}$
$\oplus k^7_{i,i+2} \oplus k^8_{i+3} \oplus k^9_{i,i+2,i+4} \oplus k^{10}_{i+1}$
7-round Linear Approximation
$XR^4_i \oplus XL^{11}_{i,i+4} =$
$k^0_{i,i+2} \oplus k^1_{i+1} \oplus k^2_i \oplus k^4_i \oplus k^5_{i+1} \oplus k^6_{i,i+2}$
$\oplus k^7_{i+3} \oplus k^8_{i,i+2,i+4} \oplus k^9_{i+1,} \oplus k^{10}_{i,i+4,}$
$Bias = \varepsilon = 2^{-10}$
$Bias = \varepsilon = 2^{-12}$
XL^8_i
XR^8_i
1-Round Decryption
XL^{12}_i
XR^{12}_i

Figure 6: 12-Round Linear Attack

7 Experimental Verification

We implement several experiments to verify the attacks presented in section 6 and provide the experimental results in this section.

Recall the super keys bits shown in Table 4, which comes in three forms k_i^0, $k_{i+2}^0 \oplus k_i^1$, or $k_i^0 \oplus k_{i+4}^0 \oplus k_{i+2}^1 \oplus k_i^2$. Note, we reuse the notations that appeared in [1], for $Bit1$, $Bit2$, $Bit3$ and $Bit4$. These four bits are determined using the following Equation (17).

$$
\begin{aligned}
k_i^0 &= Bit1_i \\
k_i^1 &= Bit2_i \oplus Bit1_{i+2} \\
k_i^2 &= Bit1_i \oplus Bit2_{i+2} \oplus Bit3_i \\
k_i^9 &= Bit4_i
\end{aligned}
\tag{17}
$$

7.1 8-Round Key Recovery Attack

To determine the required data for conducting the experiments, we follow Matsui's rule [6], which suggests using some multiple of $bais^{-2}$. Thus, the required data complexity for the 8-round attack is a multiple of 2^{-6*-2}. Therefore, we conducted 14 experiments with 2^{14} plaintext and ciphertext pairs.

It can be seen in Table 5 that the estimates contributed from evaluating the linear approximation of the right half do not improve the overall results. This is because of the low bias approximations used in this case. We notice that as the number of copies of $Bit1$, $Bit2$, and $Bit3$ increased as the accuracy of the estimation results increased. Thus, the estimates of $Bit1$ are more accurate than those of $Bit2$ and $Bit3$.

Table 5: Comparison of 8-round attack results using the left half only and using both halves.

Number of Rounds	**Super Key Bits Estimated**	**Bits Correctly Guessed (out of 16 Bits)**	**No. of Experiments (out of 14)**
8-round (left half)	$Bit1$	16	14
	$Bit2$	16	10
	average no. bits guessed correctly = 15.7	15	4
	$Bit3$	15	3
		14	2
		13	2
	average no. bits guessed correctly =12.6	12	2
		11	3
		10	2
8-round (left and right halves)	$Bit1$	16	14
	$Bit2$	16	10
		15	3
	average no. bits guessed correctly = 15.6	14	1
	$Bit3$	15	3
		14	2
		13	3
	average no. bits guessed correctly = 12.7	12	2
		11	2
		10	2

7.2 10-round Key Recovery Attack

Similar to the previous attack, we implement the 10-round attack with 14 keys chosen at random and 2^{14} P/C pairs. We can deduce from Table 6 that compared to the results obtained in the 8-round attack, we have a different observation. The votes contributed from the approximations of the right half improved the overall results. Especially in the estimations of k^9; hence every bit of k^9 received six copies from the right half evaluation, where only two copies from the left half.

Table 6: Comparison of 10-round attack results using the left half only and using both halves.

Number of Rounds	Super Key Bits Estimated	Bits Correctly Guessed (out of 16 Bits)	No. of Experiments (out of 14)
10-round (left half)	$Bit1$	16	14
	$Bit2$ average no. bits guessed correctly = 15.7	16	10
		15	4
	$Bit3$ average no. bits guessed correctly = 12.6	16	2
		14	4
		13	1
		11	5
		10	2
	$Bit4$ average no. bits guessed correctly = 13	16	1
		15	1
		14	3
		13	4
		12	3
		11	2
10-round (left and right halves)	$Bit1$	16	14
	$Bit2$ average no. bits guessed correctly =15.7	16	11
		15	2
		14	1
	$Bit3$ average no. bits guessed correctly = 12.6	16	2
		14	4
		13	1
		11	5
		10	2
	$Bit4$ average no. bits guessed correctly = 15.5	16	9
		15	3
		14	2

7.3 12-Round Key Recovery Attack

Due to the time limitation, we only implement three experiments of the 12-round attack using 2^{24} P/C pairs with keys chosen at random. Table 7 shows similar results to the results of 8-round attack. The combined estimation from both halves (left and right) did not enhance the results using only the left half estimations.

Table 7: Comparison of 12-round attack results using the left half only and using both halves.

Number of Rounds	**Super Key Bits Estimated**	**Bits Correctly Guessed (out of 16 Bits)**	**No. of Experiments (out of 3)**
12-round (left half)	$Bit1$	16	3
	$Bit2$	16	3
	$Bit3$	15	1
	average no. bits guessed correctly = 14.3	14	2
12-round (left and right halves)	$Bit1$	16	3
	$Bit2$	16	3
	$Bit3$	15	1
	average no. bits guessed correctly = 14.3	14	2

7.4 Experimental Results of 8-round Attack Without Approximations

Since Simeck is designed based on the Feistel structure, and one of the essential features of this design is that the same algorithm is used for encryption and decryption; hence an equivalent super-round of 4-rounds decryption is established as well. We can launch a meet-in-the-middle attack on 8-round linear cryptanalysis of Simeck 32/64 without any approximations, which is the same attack that has been applied on Simon in the previous work [1].

Figure 7 depicts how the two super-rounds are connected to attack eight rounds of Simeck 32/64. We start with one super-round in the forward direction and the second super-round in the backward direction; hence we efficiently apply the meet-in-the-middle technique.

The first super-round F_{S1} starts with a plaintext and 17 key bits $K1$ to produce a single bit of 4-rounds encryption XL_i^4. Then, the second super-round F_{S2} takes the ciphertext, and 8 key bits $K2$ and generates a single bit of 4-rounds decryption. Following the procedure described in [1], we compute F_{S1} and F_{S2}, for all possible values of the encryption and decryption super-keys, for every bit i.

We conduct two experiments using only 48 plaintext and ciphertext pairs; hence, we were able to retrieve the correct value of the 112 bits we are trying to recover.

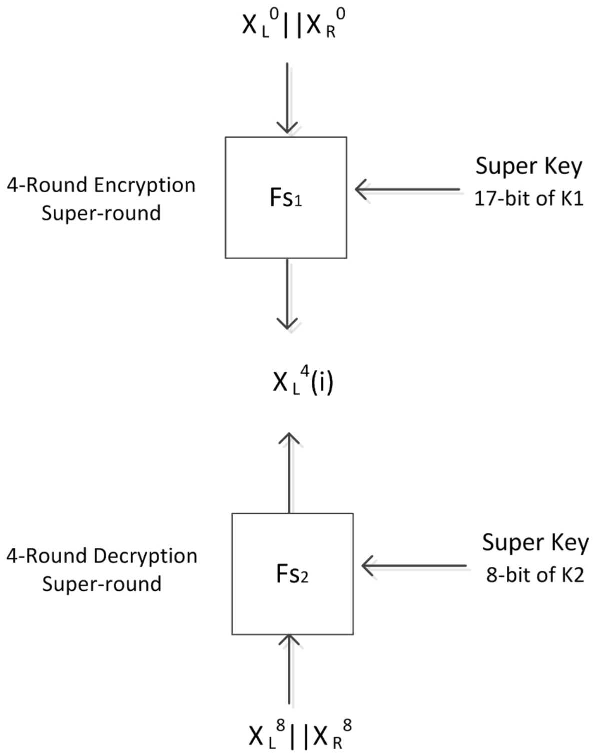


Figure 7: 8-Round Attack Without Approximations

7.5 Summary of Projected Results

Here we provide a summary of our experimental results.

Table 8: Summary of the Experimental Results.

Experimental Results	**Super Key Bits Recovered**	**Master Key Bits Recovered**	**Data Complexity**	**Time Complexity**	**Success Probability**
8-round	46–48 bits	46–48 bits	2^{14}	$2^{34.0028}$	93%
10-round	62–64 bits	56–62 bits	2^{14}	$2^{36.044}$	93.4%
12-round	46–48 bits	46–48 bits	2^{24}	$2^{44.0028}$	96.45%
8-round without approximations	112 bits	64 bits	$2^{5.58}$	$2^{30.58}$	100%

8 Projected Results Using Multiple Linear Cryptanalysis

This section presents two projected linear attacks; the first uses a single super-round, and the second is a new class of attacks where we use multiple super-rounds.

8.1 20-round Linear Attack Using a Single Super-Round

Here, we present a 20-round linear attack by extending the 12-round linear approximations Equation (18) and append a single super round of four rounds encryption and add four rounds of decryption.

We extend the 7-round linear characteristics Equations (11) and (12) into the following 12-round linear approximations for the left and the right sides with biases=2^{-18} and 2^{-19} respectively.

$$\begin{aligned}
&PL_i \oplus CR_{i+3} \oplus CL_{i,i+2,i+4} = k^{11}_{i,i+2,i+4} \oplus k^{10}_{i+1} \oplus k^{9}_{i,i+4} \oplus k^{7}_{i,i+4} \oplus k^{6}_{i+1} \oplus k^{5}_{i,i+2,i+4} \\
&\oplus k^{4}_{i+3} \oplus k^{3}_{i,i+2} \oplus k^{2}_{i+1} \oplus k^{1}_{i} \\
&PR_i \oplus CR_{i,i+2} \oplus CL_{i+3} = k^{11}_{i+3} \oplus k^{10}_{i+2,i,i+4} \oplus k^{9}_{i+1} \oplus k^{8}_{i,i+4} \oplus k^{6}_{i,i+4} \oplus k^{5}_{i+1} \oplus k^{4}_{i,i+2,i+4} \\
&\oplus k^{3}_{i+3} \oplus k^{2}_{i,i+2} \oplus k^{1}_{i+1} \oplus k^{0}_{i}
\end{aligned} \tag{18}$$

Following the approach presented in [1], first, we compute the capacity for the system of approximations.

$$\overline{c}^2 = 4 \times 16 \times 2^{-18 \times 2} = 2^6 \times 2^{-18^2} = 2^{-30}$$

Appending the super round costs on average 11.5 and 4.5 for the left and the right half, respectively. Moreover, appending four rounds of decryption costs guessing on average 16 key bits and 18.5 key bits for the left and right half approximations respectively.

There are 23 key bits (16 bits on average) required guessing for the left half approximations:

- 14 bits of k^{19}_i for $i = 3, 8, 13, 4, 2, 7, 9, 14, 0, 5, 10, 12, 1, 6$, each counted as a half bit
- 7 bits of the sum:$k^{19}_{i+1} \oplus k^{18}_i$ for $i = 5, 13, 2, 7, 3, 58$.
- 2 bits of the sum:$k^{19}_{i,i+2} \oplus k^{18}_{i+1} \oplus k^{17}_i$, for $i = 3, 8$

There are 25 key bits (18.5 bits on average) required guessing for the right half approximations:

- 13 bits of k^{19}_i for $i = 0, 5, 8, 10, 1, 6, 15, 11, 2, 7, 12, 3, 13$, each counted as a half bit

- 8 bits of the sum : $k_{i+1}^{19} \oplus k_i^{18}$ for $i = 0, 5, 10, 2, 7, 12, 1, 6$.
- 4 bits of the sum: $k_{i,i+2}^{19} \oplus k_{i+1}^{18} \oplus k_i^{17}$, for $i = 0, 5, 2, 7$

Thus, the time complexity for evaluating the approximations for left half is $16 \times 2^{30} \times 2^{11.5} \times 2^{16} = 2^{61.5}$. In addition to the complexity to evaluate the approximations for the right half $= 16 \times 2^{30} \times 2^{4.5} \times 2^{18.5} = 2^{57}$. Thus, the total time complexity is $2^{61.56}$.

8.2 Improved Linear Approximations for Simeck 32/64

The approximations used in the attack presented in 8.1 have a single bit of the input mask due to the constraint of incorporating only a single super-round. This constraint is relaxed in this work. We can improve the overall attack efficiency by deriving a linear approximation with multiple input masks, which means we can employ multiple super-rounds.

Therefore, we are able to derive this improved 13-round approximation with bias equal to 2^{-18}. (see 12 for the derivation).

$$PL_{i+3} \oplus PR_{i,i+2} \oplus XR_{i+1}^{13} \oplus XL_{i,i+4}^{13} \oplus k_{i,i+4}^{10} \oplus k_{i+1}^{9} \oplus k_{i,i+2,i+4}^{8} \oplus k_{i+3}^{7} \oplus k_{i,i+2}^{6} \oplus k_{i+1}^{5} \oplus k_i^{4} \oplus k_i^{2} \oplus k_{i+1}^{1} \oplus k_{i,i+2}^{0} \tag{19}$$

8.3 20-round Linear Attacks Using Multiple Super-Rounds

Incorporating multiple super rounds enables us to enhance the time complexity of the attack. Thus, we extend the 13-round linear trail Equation 19 into a 20-round linear attack by appending six rounds, four rounds of encryption (three super-rounds), and three rounds of decryption.

The system of approximations has the capacity of:

$$\bar{c}^2 = 4 \times 16 \times 2^{-18 \times 2} = 2^6 \times 2^{-18^2} = 2^{-30}$$

Hence, the data complexity for this attack is 2^{30}.
The three super-rounds require guessing three super-keys which consist of:

- 14 bits of the last round key k_i^0 for $i = 10, 5, 14, 9, 4, 8, 3, 2, 13, 0, 1, 6, 7, 12$
- 9 bits of the sum $k_{i+1}^0 \oplus k_i^1$ for $i = 9, 4, 13, 8, 3, 0, 5, 2, 7$
- 2 bits of the sum $k_{i,i+2}^0 \oplus k_{i+1}^1 \oplus k_i^2$ for $i = 3, 8$

There are 7 key bits required guessing for adding three rounds of decryption (see **??** for details):

- 5 bits of k_i^{19} for $i = 0, 5, 10, 1, 6$, each counted as a half bit
- 4 bits of the sum:$k_{i+1}^{19} \oplus k_i^{18}$ for $i = 0, 5$.

The average cost for appending three super-rounds is to guess 18 key bits, in addition to 6.5 key bits to add three rounds of decryption; thus, the time complexity for this attack is $2^4 \times 2^{30} \times 2^{18} \times 2^{6.5} = 2^{58.5}$.

Thus, the time complexity for evaluating the approximations for left half is $2^4 \times 2^{30} \times 2^{18} \times 2^{6.5} = 2^{58.5}$. In addition to the complexity to evaluate the approximations for the right half $= 16 \times 2^{30} \times 2^{4.5} \times 2^{18.5} = 2^{57}$. Thus, the total time complexity is $2^{58.58}$.

Table 9 summarize our results of Simeck 32/64 and compares it with the best results presented in [2]. We are able to go deeper by two rounds.

Average Case Computations			
Simeck	Number of Rounds	Data Complexity	Time Complexity
32/64	Using Single Super-Round Presented in Section 8.1		
	17-round	2^{30}	$2^{60.5}$
	Using Multiple Super-Rounds Presented in Section 8.3		
	20-round	2^{30}	$2^{58.58}$
	Projections from data in [2]		
	18-round	2^{24}	$2^{60.5}$

Table 9: Comparison results on Simeck 32

9 The Effect of Super Rounds on Larger Variants of Simeck

Contrary to Simon, the larger versions of Simeck have the same super keys of the same size. Therefore, incorporating multiple super-rounds instead of one super-round still yields better results on all versions of Simeck than one super-round.

For Simeck 48, we derived a 20-round linear approximation that has three active bits in the input mask and one bit of the output mask. We employ this approximation to attack 29-rounds of Simeck 48 by adding three super rounds (four rounds of encryption) at the beginning and five rounds of decryption at the end. This comes at the cost of guessing 41 key bits on average.

For Simeck 64, we derived a 25-round and added nine rounds at both ends. Four rounds of encryption and five rounds of decryption cost guessing 49 key bits on average. Hence, we attack up to 34-round of this version of Simeck.

10 Conclusions

This paper presents the results of applying the novel notion of super rounds presented in [1] on all versions of the Simeck lightweight block cipher. Hence, we got very similar results on Simeck 32 and better results on Simeck48 and

Simeck64. We presented experimental results on 8-round, 10-round, and 12 - rounds attacks on Simeck 32, and we recovered a large number of the master key bits with high accuracy. Theoretically, we present a 20-round on Simeck 32, 29-rounds on Simeck 48 and 35-rounds on Simeck 64. Applying the super-rounds model of linear cryptanalysis on Simeck 32 results in similar attacks to what has been presented in [1]. Thus, we improved the complexity of applying the super-rounds by relaxing the constraint of using only the linear approximations with one active input mask; this enables us to derive linear trails with higher bias. As a result, we are able to attack a significant number of rounds of Simeck48 and Simeck 64.

A The Deduction of k^3 from k^9

Simeck key schedule generates r-4 more round keys from the 64-bit master key. Therefore, we are able to write the round keys in terms of the master key bits k^0, k^1, k^2, and k^3.

k^9 is generated as in equation 20, which is expressed in terms of the master key bits in equation (21).

$$k^9 = k^5 \oplus F(k^6) \oplus c \oplus (z_0)_5 \tag{20}$$

Hence, k^3 may be expressed in terms of k^0, k^1, k^2, and k^9 as follows:

$$k^9 = k^1 \oplus F(k^2) \oplus F(k^2 \oplus f(k^3)) \oplus C \oplus (Z_0)_1 \oplus C \oplus (Z_0)_2 \oplus C \oplus (Z_0)_5 \tag{21}$$

Recall the round function f:

$$F(XL^j) = [(XL^j)\&(XL^j \lll 5)] \oplus XL^j \lll 1)$$

It is clear that f consists of the non-invertible bitwise AND, hence we assume the output of f is Zero:

$$\begin{aligned} F(X) &= (0^n \oplus XL^j \lll 1) \\ &= XL^j \lll 1 \end{aligned} \tag{22}$$

where 0^n denotes a zero vector of n-bits.

We can write the inverse function as:

$$F^{-1}(X) = X \lll 1 \tag{23}$$

Therefore, to write k^9 in terms of the master key, we apply 23 in 21:

$$\begin{aligned} k^9 &= k^1 \oplus f^{-1}(k^2) \oplus f^{-1}(k^2 \oplus f^{-1}(k^3))C \oplus (Z_0)_1 \oplus C \oplus (Z_0)_2 \oplus C \oplus (Z_0)_5 \\ &= k^1 \oplus (k^2 \lll 1) \oplus (k^2 \lll 1) \oplus (k^3 \lll 2) \oplus C \oplus (Z_0)_1 \oplus C \oplus (Z_0)_2 \oplus C \oplus (Z_0)_5 \end{aligned} \tag{24}$$

B Derive 13-round Linear Approximations for Simeck 32/64

Table 10: The sequence of approximations used to derive 13-rounds linear trails for the left-half of Simeck 32.

Active Bits in the Left Side	**Active Bits in the Right Side**	**Used Approximation**	**Number of Approximations**
0	-		
-	0	1	1
0	1	1	1
1	0,2	1;1	2
0,2	3	1	1
3	0,2,4	3;1;1	3
0,2,4	1	1	1
1	0,4	3;1	2
0,4			0
	0,4	3;1	2
0,4	1	1	1
1	0,2,4	3;1;1	3
0,2,4	3		

Table 11: The sequence of approximations used to derive 13-rounds for the right-half of Simeck 32.

Active Bits in the Left Side	**Active Bits in the Right Side**	**Used Approximation**	**Number of Approximations**
-	0	1	1
0	1	1	1
1	0,2	1:1	2
0,2	3	1	1
3	0,2,4	3;1;1	3
0,2,4	1	1	1
1	0,4	3;1	2
0,4	-		
	0,4	3;1	2
0,4	1	1	1
1	0,2,4	3;1;1	3
0,2,4	3	1	1
3	0,2		

C Derive an improved 13-round Linear Approximations for Simeck 32/64

Table 12: The sequence of approximations used to derive 13-rounds linear trails of Simeck 32.

Active Bits in the Left Side	**Active Bits in the Right Side**	**Used Approximation**	**Number of Approximations**
3	0, 2	1:1	2
0,2	1	1	1
1	0	1	1
0	-		
0	1	1	1
	0	1	1
1	0,2	1;1	2
0,2	3	1	1
3	0,2,4	3;1;1	3
0,2,4	1	1	1
1	0,4	3;1	2
0,4	-		
	0.4	3;1	2
0,4	1		

D Linear Cryptanalysis of Simeck 48/96 Using Multiple Super-Rounds

Here, we continue using multiple super-rounds, so we extend the 13-round linear approximation Equation (19) into a 20-round approximation with bias=2^{-27} (see 13 for detailed derivation).

$$PL_{i+3} \oplus PR_{i,i+2} \oplus XR_i^{20} = k_i^{18} \oplus k_{i+1}^{17} \oplus k_{i,i+2}^{16} \oplus k_{i+3}^{15} \oplus k_{i,i+2,i+4}^{14} \oplus k_{i,i+4}^{10} \oplus k_{i+1}^{9} \oplus k_{i,i+2,i+4}^{8} \oplus k_{i+3}^{7} \oplus k_{i,i+2}^{6} \oplus k_{i+1}^{5} \oplus k_i^{4} \oplus k_i^{2} \oplus k_{i+1}^{1} \oplus k_{i,i+2}^{0} \tag{25}$$

D.1 28-round and 29-round Linear Attacks of SIMECK 48/96

Here, we describe an improved linear attack of 28-round of SIMECK 48/96. We append the super rounds of four rounds encryption and four rounds of decryption to the 20-round linear approximation.

The system of approximations has the capacity of:

$$\overline{c}^2 = 4 \times 24 \times 2^{-27 \times 2} = 2^6 \times 2^{-27^2} = 2^{-47.42}$$

The components of three super-keys, a total of 26 key bits:

- 15 bits of the last round key k_i^0 for $i = 10, 5, 14, 9, 4, 8, 3, 2, 18, 13, 0, 1, 6, 7, 12$
- 9 bits of the sum $k_{i+1}^0 \oplus k_i^1$ for $i = 9, 4, 13, 8, 3, 0, 5, 2, 7$
- 2 bits of the sum $k_{i,i+2}^0 \oplus k_{i+1}^1 \oplus k_i^2$ for $i = 3, 8$

There is a single bit of the output mask represents one bit of the right half, hence we can use our super-round to add four rounds of decryption. Therefore, adding four rounds of decryption requires guessing 16 key bits:

- 9 bits of the last round key k_i^{19} for $i = 7, 2, 11, 6, 1, 5, 0, 15, 10$
- 5 bits of the sum $k_{i+1}^{19} \oplus k_i^{18}$ for $i = 6, 1, 10, 5, 0$
- 2 bits of the sum $k_{i,i+2}^{19} \oplus k_{i+1}^{18} \oplus k_i^{17}$ for $i = 0, 5$

Thus, the time complexity for this attack is $24 \times 2^{47.42} \times 2^{25} \times 2^{16} = 2^{93}$.

In the average-case complexity, we can add one more round decryption to the 28-round linear attack; hence we attack up to 29 rounds of SIMECK 48/96. The cost of adding five rounds of decryption, a total of 28 key bits (22 bits on average):

- 12 bits of the last round key k_i^{28} for $i = 0, 5, 10, 1, 6, 15, 11, 2, 7, 16, 12, 20$, each counted as a half bit
- 9 bits of the sum $k_{i+1}^{28} \oplus k_i^{27}$ for $i = 7, 2, 11, 6, 1, 5, 0, 15, 10$
- 5 bits of the sum $k_{i,i+2}^{28} \oplus k_{i+1}^{27} \oplus k_i^{26}$ for $i = 6, 1, 10, 5, 0$
- 2 bits of the sum $k_{i+3}^{28} \oplus k_{i,i+2}^{27} \oplus k_{i+1}^{26} \oplus k_i^{25}$ for s$i = 0, 5$

The cost of appending four rounds of encryption on average reduced to guess 18.5 key bits. The average time complexity is $24 \times 2^{47.42} \times 2^{18.5} \times 2^{22.5} = 2^{92.5}$.

Table 13: The sequence of approximations used to derive 20-rounds linear trails of Simeck 48.

Active Bits in the Left Side	**Active Bits in the Right Side**	**Used Approximation**	**Number of Approximations**
3	0, 2	1:1	2
0,2	1	1	1
1	0	1	1
0	-		
0	1	1	1
	0	1	1
1	0,2	1;1	2
0,2	3	1	1
3	0,2,4	1;1;1	3
0,2,4	1	1	1
1	0,4	1;1	2
0,4	-		
	0.4	1;1	2
0,4	1	1	1
1	0,2,4	3;1;1	3
0,2,4	3	1	1
3	0,2	1;1	2
0,2	1	1	1
1	0	1	1
0	-		
-	0		

Tables 14 and 15 summarize our results of Simeck 48/96 and compares it with the best results presented in [2]. We are able to attack seven more rounds, and five more rounds in the average-case complexity and worst-case complexity receptively.

Average Case Computations			
Simeck	Number of Rounds	Data Complexity	Time Complexity
	Using Multiple Super-Rounds Presented in Section D		
	29-round	$2^{47.42}$	$2^{92.5}$
	Projections from Data in [2]		
	23-round	$2^{41.42}$	2^{95}

Table 14: Summary of the average case analysis of our results on Simeck 48

Worst Case Computations

Simeck	Number of Rounds	Data Complexity	Time Complexity
	Using Multiple Super-Rounds Presented in Section D		
	28-round	$2^{47.42}$	2^{93}
	Projections from Data in [2]		
	23-round	$2^{41.42}$	2^{108}

Table 15: Summary of the worst case analysis of our results on Simeck 48

E Linear Cryptanalysis of Simeck 64/128 Using Multiple Super-Rounds

In this section, we try to improve the results obtained using a single-super round by using multiple super-rounds.

E.1 Improved Linear Approximation for Simeck 64/128

We extend the 20-round linear approximation 19 into a 25-round linear approximation with bias=2^{-35} (see 16 for derivation).

$$PL_{i+3} \oplus PR_{i,i+2} \oplus XR^{25}_{i+1} \oplus XL^{25}_{i,i+2,i+4} = k^{24}_{i,i+2,i+4} \oplus k^{23}_{i+3} \oplus k^{22}_{i,i+2} \oplus XR^{23}_{i+1} \oplus k^{20}_{i} \oplus k^{18}_{i} \oplus k^{17}_{i+1} \oplus k^{16}_{i,i+2} \oplus k^{15}_{i+3} \oplus k^{14}_{i,i+2,i+4} \oplus k^{10}_{i,i+4} \oplus k^{9}_{i+1} \oplus k^{8}_{i,i+2,i+4} \oplus k^{7}_{i+3} \oplus k^{6}_{i,i+2} \oplus k^{5}_{i+1} \oplus k^{4}_{i} \oplus k^{2}_{i} \oplus k^{1}_{i+1} \oplus k^{0}_{i,i+2} \tag{26}$$

E.2 33-round and 34-round Linear Attacks of Simeck 64/128 Using Multiple Super-Rounds

We extend the 25-round linear trail 26, and add four rounds of encryption and four rounds of decryption, hence we are able to attack up to 33-round of Simeck 64/128.

The capacity of the 25-round linear trail is:

$$\bar{c}^2 = 4 \times 32 \times 2^{-35 \times 2} = 2^7 \times 2^{-35^2} = 2^{-63}$$

Thus, the required data complexity is 2^{63}.

The cost of adding four rounds of encryption, the components of three super-keys, a total of 26 key bits:

- 14 bits of the last round key k^0_i for $i = 10, 5, 14, 9, 4, 8, 3, 2, 18, 13, 0, 1, 6, 7, 12$
- 9 bits of the sum $k^0_{i+1} \oplus k^1_i$ for $i = 9, 4, 13, 8, 3, 0, 5, 2, 7$
- 2 bits of the sum $k^0_{i,i+2} \oplus k^1_{i+1} \oplus k^2_i$ for $i = 3, 8$

The cost of adding four rounds of decryption, a total of 22 key bits (see **??** for details):

- 13 bits of the last round key k_i^{32} for $i = 7, 2, 11, 6, 1, 5, 0, 15, 10, 14, 3, 4, 9$
- 7 bits of the sum $k_{i+1}^{32} \oplus k_i^{31}$ for $i = 1, 6, 11, 0, 5, 4, 9$
- 2 bits of the sum $k_{i,i+2}^{32} \oplus k_{i+1}^{31} \oplus k_i^{30}$ for $i = 1, 6$

The time complexity for this attack is $2^5 \times 2^{63} \times 2^{25} \times 2^{22} = 2^{115}$.

In the average-case complexity, we extend the 33-round attack by one more round and present a 34-round linear attack. Thus, we add five rounds of decryption. The cost of adding five rounds of decryption, a total of 39 key bits (30.5 bits on average):

- 17 bits of the last round key k_i^{33} for $i = 1, 6, 11, 16, 2, 7, 12, 21, 17, 0, 5, 10, 15, 4, 9, 14, 19$, each counted as a half bit
- 13 bits of the sum $k_{i+1}^{33} \oplus k_i^{32}$ for $i = 7, 2, 11, 6, 1, 5, 0, 15, 10, 14, 3, 4, 9$
- 7 bits of the sum $k_{i,i+2}^{33} \oplus k_{i+1}^{32} \oplus k_i^{30}$ for $i = 1, 6, 11, 0, 5, 4, 9$
- 2 bits of the sum $k_{i+3}^{33} \oplus k_{i,i+2}^{32} \oplus k_{i+1}^{31} \oplus k_i^{30}$ for s$i = 1, 6$

The average time complexity for this attack is $2^5 \times 2^{63} \times 2^{18} \times 2^{30.5} = 2^{116.5}$.

Table 16: The sequence of approximations used to derive 25-rounds linear trails of Simeck 64.

Active Bits in the Left Side	**Active Bits in the Right Side**	**Used Approximation**	**Number of Approximations**
3	0, 2	1:1	2
0,2	1	1	1
1	0	1	1
0	-		
0	1	1	1
	0	1	1
1	0,2	1;1	2
0,2	3	1	1
3	0,2,4	1;1;1	3
0,2,4	1	1	1
1	0,4	1;1	2
0,4	-		
	0.4	1;1	2
0,4	1	1	1
1	0,2,4	3;1;1	3
0,2,4	3	1	1
3	0,2	1;1	2
0,2	1	1	1
1	0	1	1
0	-		
-	0	1	1
0	1	1	1
1	0,2	1;1	2
0,2	3	1	1
3	0,2,4	3;1;1	3
0,2,4	1		

Tables 17 and 18 summarize our results of Simeck 64/128 and compares it with the best results presented in [2]. We are able to attack seven more rounds, and six more rounds more efficiently in both cases of time complexity receptively.

Average Case Computations			
Simeck	Number of Rounds	Data Complexity	Time Complexity
	Using Multiple Super-Rounds Presented in Section E		
	34-round	2^{63}	$2^{116.5}$
	Projections from Data in [2]		
	27-round	2^{49}	2^{107}

Table 17: Summary of the average case analysis of our results on Simeck 64

Worst Case Computations			
Simeck	Number of Rounds	Data Complexity	Time Complexity
	Using Multiple Super-Rounds Presented in Section E		
	33-round	2^{63}	2^{115}
	Projections from Data in [2]		
	27-round	2^{53}	2^{134}

Table 18: Summary of the worst case analysis of our results on Simeck 64

References

[1] Reham Almukhlifi and Poorvi L. Vora. Linear cryptanalysis of reduced-round simon using super rounds. *Cryptogr.*, 4(1):9, 2020.

[2] Nasour Bagheri. Linear cryptanalysis of reduced-round simeck variants. *IACR Cryptology ePrint Archive*, 2015:716, 2015.

[3] Alex Biryukov, Christophe De Cannière, and Michaël Quisquater. On multiple linear approximations. In Matt Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, pages 1–22, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[4] Andrey Bogdanov and Vincent Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Des. Codes Cryptogr.*, 70(3):369–383, 2014.

[5] Stefan Kölbl and Arnab Roy. A brief comparison of simon and simeck. In Andrey Bogdanov, editor, *Lightweight Cryptography for Security and Privacy - 5th International Workshop, LightSec 2016, Aksaray, Turkey, September 21-22, 2016, Revised Selected Papers*, volume 10098 of *Lecture Notes in Computer Science*, pages 69–88. Springer, 2016.

[6] Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, EUROCRYPT '93, pages 386–397, Berlin, Heidelberg, 1994. Springer-Verlag.

[7] Kexin Qiao, Lei Hu, and Siwei Sun. Differential security evaluation of simeck with dynamic key-guessing techniques. In Olivier Camp, Steven Furnell, and Paolo Mori, editors, *Proceedings of the 2nd International Conference on Information Systems Security and Privacy, ICISSP 2016, Rome, Italy, February 19-21, 2016*, pages 74–84. SciTePress, 2016.

[8] Lingyue Qin, Huaifeng Chen, and Xiaoyun Wang. Linear hull attack on round-reduced simeck with dynamic key-guessing techniques. In *ACISP*, 2016.

[9] Sadegh Sadeghi and Nasour Bagheri. Improved zero-correlation and impossible differential cryptanalysis of reduced-round SIMECK block cipher. *IET Inf. Secur.*, 12(4):314–325, 2018.

[10] Gangqiang Yang, Bo Zhu, Valentin Suder, Mark Aagaard, and Guang Gong. The simeck family of lightweight block ciphers. In *CHES*, 2015.

[11] K. Zhang, J. Guan, B. Hu, and D. Lin. Security evaluation on simeck against zero-correlation linear cryptanalysis. *IET Information Security*, 12(1):87–93, 2018.