*cryptography*

*Article*

# Linear Cryptanalysis of Reduced-Round SIMECK Using Super Rounds

**Reham Almukhlifi [1,*] and Poorvi L. Vora [2]**

[1] Department of Computer Science, Taibah University, Medina 42353, Saudi Arabia
[2] Department of Computer Science, The George Washington University, Washington, DC 20052, USA
[*] Correspondence: rmukhallafi@taibahu.edu.sa

**Abstract:** 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. Previously, we proposed the use of linear cryptanalysis using super-rounds 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). We were able to follow a similar approach, in all variants of SIMECK, with an improvement in SIMECK 32 and SIMECK 48 by relaxing the previous constraint of a single active bit, using multiple active bits instead. In this paper we present improved linear attacks against all variants of SIMECK: attacks on 19-rounds of SIMECK 32/64, 28-rounds of SIMECK 48/96, and 34-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.

**Keywords:** SIMECK; linear cryptanalysis; super round

**Citation:** Almukhlifi, R.; Vora, P.L. Linear Cryptanalysis of Reduced-Round SIMECK Using Super Rounds. *Cryptography* **2023**, *7*, 8. https://doi.org/10.3390/cryptography7010008

Academic Editor: Ki-Hyun Jung

Received: 14 December 2022
Revised: 31 January 2023
Accepted: 1 February 2023
Published: 9 February 2023

## 1. Introduction

Lightweight cryptography is one of the most active research areas in the cryptographic community. In the last decade, several lightweight block ciphers were designed, which aimed to work efficiently in constrained environments. SIMECK is a family of lightweight block ciphers that combines design features from SIMON and SPECK, using a slightly modified round function of SIMON with the SPECK key schedule. The round function makes it vulnerable to most attacks on SIMON, one of which is the improved linear attack proposed by us in [1], where we show that, after four rounds of SIMON 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 seven key bits. We refer to the multiple rounds of encryption as a *super round*. We are able to construct a super round for SIMECK in a similar way, due to the great similarity in their designs.

In this paper, we are able to improve upon the approach of [1] on SIMECK 32/64 and SIMECK 48/96, by using multiple super rounds and multiple active bits, while keeping the number of key bits to be guessed small enough. We present the direct application of the approach [1] on all variants of SIMECK, and demonstrate the improvement for SIMECK 32/64 and SIMECK 48/96 (though the improved approach does not improve on our previous attacks on SIMON).

### 1.1. Our Contributions

In this paper, we present an attack on reduced-round SIMECK. In contrast to the original work by us on the use of a single super round and active bit [1], the approach here uses multiple super rounds and multiple active bits that enable us to attack more rounds on SIMECK 48/96 and enhance the efficiency of the linear attack on SIMECK 32/64. The work presented in [1] was demonstrated exclusively on Simon. The attack presented here is demonstrated exclusively on Simeck. It does not work on Simon because the rotation used in the round functions is different and Simeck's makes it vulnerable to our attack.

The attack presented here on Simeck 32 has larger bias than if we were to apply the attack of [1]. We refer to the application of [1] to Simeck as *single super round* in the table below. We do not cite [1] in the table because the approach was applied only to Simon there. Instead, we cite the section in this paper (Section 7.1) where we report the results of applying [1] to Simeck.

### *1.2. Comparison with Other Work*

We compare our results with Bagheri's [2] best key recovery results, which were achieved using Matsui's second algorithm. These are the best results that were obtained using the classical linear Matsui's second algorithm without recourse to linear hull results. In both average-case and worst-case comparisons, we were able to go deeper in all variants of Simeck, see Tables 1 and 2.

**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 | $2^{30}$ | $2^{61.56}$ | Section 7.1 |
| | 20-round | $2^{30}$ | $2^{58.5}$ | Section 7.3 |
| | 18-round | $2^{24}$ | $2^{61.5}$ | Bagheri [2] |
| 48/96 | 28-round | $2^{47.42}$ | $2^{84.08}$ | Appendix D |
| | 29-round | $2^{47.42}$ | $2^{92.505}$ | Appendix E |
| | 23-round | $2^{41.42}$ | $2^{95}$ | Bagheri [2] |
| 64/128 | 34-round | $2^{61}$ | $2^{112}$ | Appendix F |
| | 34-round | $2^{63}$ | $2^{116.5}$ | Appendix G |
| | 27-round | $2^{49}$ | $2^{104}$ | Bagheri [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 | $2^{30}$ | $2^{59.02}$ | Section 7.1 |
| | 19-round | $2^{30}$ | $2^{61}$ | Section 7.3 |
| | 18-round | $2^{24}$ | $2^{72}$ | Bagheri [2] |
| 48/96 | 2-round | $2^{47.42}$ | $2^{94.58}$ | Appendix D |
| | 28-round | $2^{47.42}$ | $2^{94.005}$ | Appendix E |
| | 23-round | $2^{41.42}$ | $2^{108}$ | Bagheri [2] |
| 64/128 | 34-round | $2^{61}$ | $2^{126.5}$ | Appendix F |
| | 33-round | $2^{63}$ | $2^{115}$ | Appendix G |
| | 27-round | $2^{53}$ | $2^{134}$ | Bagheri [2] |

Note the following details:

1. The average case was a result of counting key bits involved in the XOR as a half bit. For the worst case, the key bits were counted as a single bit as in the literature.
2. We made changes to how the data complexity was computed in his work for a fair comparison. Furthermore, since we are using multiple linear approximations, we applied the capacity model [3] to both our work and his.

## 2. SIMECK

### 2.1. Notations

We used the notation of [1]. Superscripts indicate a round number beginning with 0 for the first round. Subscripts indicate a bit number beginning with 0 for the leftmost bit. $X$ represents input, and $XL$ and $XR$ represent the left-half and right-half inputs, respectively. For example, $XL_5^0$ is the sixth bit from the left of the left-half input of the first round. Similarly, $k_i^j$ is the $i$-th bit of the $j$-th round key, and $k_1^0$ represents the second bit of the first round key.

Moreover, $PL$ represents the left plaintext half, while $PR$ represents the right plaintext half input to the cipher. Similarly, $CL$ means the left ciphertext half and $CR$ is the right ciphertext half, the final output of the cipher. Additionally, $\oplus$ represents bitwise exclusive OR (XOR) and & bitwise AND. Finally, $X \lll z$ represents cyclic shifts to the left by z bits.

### 2.2. Description of SIMECK

There are three versions of SIMECK, each 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 |
|---|---|---|---|---|
| SIMECK 32 | 64 | 16 | 4 | 32 |
| SIMECK 48 | 96 | 24 | 4 | 36 |
| SIMECK 64 | 128 | 32 | 4 | 44 |

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

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

where:

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

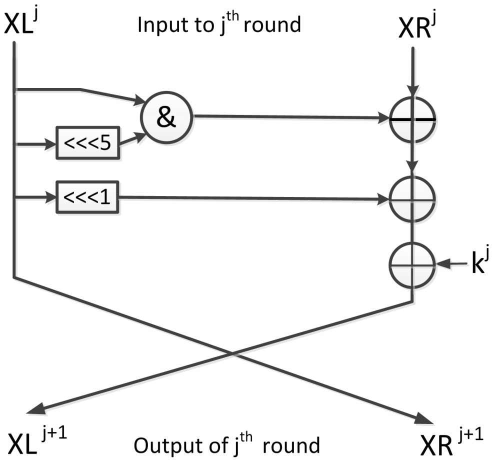


**Figure 1.** SIMECK round function.

The key schedule takes the master key $K$ as an input and generates $r$ subkeys $k^0, k^1, \ldots k^{r-1}$. The initial states of the feedback shift registers $(t_2, t_1, t_0, k_0)$ are initialized with the master key words. Then, the round function is applied 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 $0 \le i \le T-1$, $C = 2^n - 4$, n is the word size, $(z_j)_i$ is the i-th bit of $z_j$.

The sequence $z_j$ for SIMECK 32/64 and SIMECK 48/96 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 similarities between the design of SIMON and SIMECK, most of the attacks that have been used against SIMON are applicable to SIMECK. Hence, the designers of SIMECK have analyzed the security of the cipher against linear and differential cryptanalysis using the best attacks that have occurred against SIMON. In [4], the authors evaluate the security of SIMECK and conclude with the possibility of launching a differential attack over 19, 20, and 26 rounds of SIMECK 32/64, 48 and 128 respectively. Similarly, they present a linear cryptanalysis and introduce attacks on 12, 15, and 19 rounds of SIMECK 32/64, 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 presented 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 presented differential attacks against 19, 26 and 33 rounds on SIMECK 32, SIMECK 48, and SIMECK 64, respectively.

Soon after this, Qiao et al. [6], presented 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. [7] evaluated the security of SIMECK against linear hull cryptanalysis, considered the best linear results on SIMECK 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.

A powerful, recently proposed attack method is zero-correlation linear cryptanalysis [8], which relies on the use of linear trails with a probability of 0.5. In 2018, Zhang et al. [9] evaluated the security of SIMECK against such an attack. Hence, they presented attacks on 20 rounds, 24 rounds and 27 rounds of SIMECK 32, SIMECK 48, and SIMECK 64, respectively.

Moreover, Bagheri and Sadeghi [10] improved these results and presented better attacks using zero-correlation linear trails on SIMECK 48 and SIMECK 64. They were able to attack 27-round SIMECK 48 and 31-round SIMECK 64. In 2019, Chen et al. [11] provided improved results using an integral attack.

Side-channel and fault attacks are a powerful category of attacks that compromise the ciphers' physical implementation to recover the secret key. Nalla et al. [12] described the first-fault attack on SIMECK and demonstrated two models of fault attack; in both attacks, they recovered the n-bit last-round key. In 2020, Duc-Phong Le et al. [13] improved the former results for fault attacks and recovered the master key by injecting fewer faults into a single round of cipher. Hence, in [14], a new countermeasure algorithm is proposed, which can detect intelligent injection faults rather than random faults.

A growing interest in side-channel attacks has been noted, especially in the use of deep learning network technology. Various models have been developed and examined to improve the efficiency of side-channel analysis attacks [15]. Wu et al. [16] presented a side-channel attack using electromagnetic leakage data to recover the last-round key of SIMECK 32/64.

Hence, the use of machine learning tools in cryptography is broader than just improving side-channel attacks. Recently, Baksi et al. [17] improved the framework proposed in [18] to find differential distinguishers for SIMECK and Ascon. They presented multi-layer perceptron-based distinguishers for 9-round SIMECK 32, and 14-round SIMECK 64. By employing ML tools, they were able to reduce the search complexity of the classical differential distinguisher.

In the post-quantum era, many cryptography systems are threatened by powerful quantum computers. SIKE is one of the candidates that was submitted to the NIST post-quantum cryptography standardization process. The cipher can provide reliable security for the post-quantum era, in addition to the current environment. Tian et al. [19] designed an improved architecture to enhance the cipher's implementation.

In 2020, the authors of [1] 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; each part is sufficient to relate multiple bits of ciphertext to a single bit of plaintext. The efficiency of this technique depends on reducing the number of key bits that need to be guessed using linear approximations. The standard technique of extending a linear approximation with one round of decryption is usually achieved by guessing the full last round key. The proposed improved technique takes advantage of the fact that one bit of cipher text 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.

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

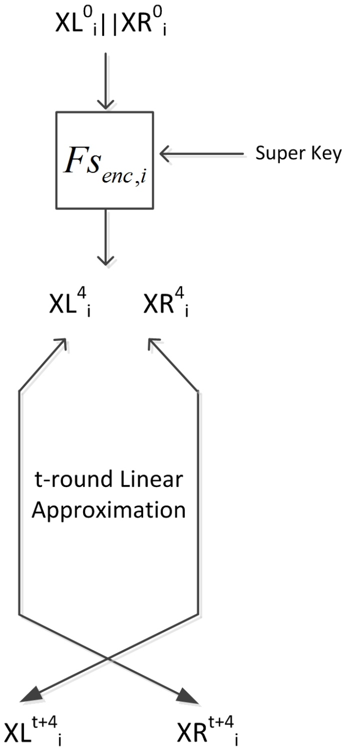


**Figure 2.** General form of linear attack with super rounds.

## 4. Super Rounds and Super Keys for Simeck

We applied the super round technique to recover multiple round keys, including the master key for all variants of Simeck, and attack more rounds using Matsui's second algorithm. The term super round, defined in [1], represents *s*-rounds of encryption of the cipher. In our analysis of Simeck, this represents a four-round encryption.

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

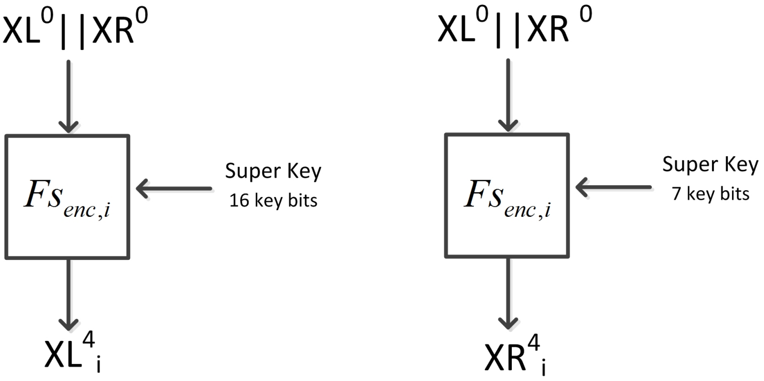


**Figure 3.** The super rounds.

### 4.1. 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:

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

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,

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

and hence that:

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

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,

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

### *4.2. The Super Key*

There is a super key corresponding to each of the super rounds depicted in Figure 3. The following table lists the components of the left and right super keys, according to the equations described in Section 4.1.

From Table 4, 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, five bits come 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 can obtain nine copies, five copies of each bit of $k^0$, for every super key of the left and right half of the state, respectively.

**Table 4.** Superkeys.

| Super Key of the Left Half | Super Key of the Right Half |
|---|---|
| $k_i^0 \oplus k_{i+2}^0 \oplus k_{i+1}^1 \oplus k_i^2$ | $k_{i+1}^0 \oplus k_i^1$ |
| $k_{i+5}^0 \oplus k_{i+7}^0 \oplus k_{i+6}^1 \oplus k_{i+5}^2$ | $k_{i+6}^0 \oplus k_{i+5}^1$ |
| $k_{i+1}^0 \oplus k_i^1$ | $k_i^0$ |
| $k_{i+6}^0 \oplus k_{i+5}^1$ | $k_{i+1}^0$ |
| $k_{i+11}^0 \oplus k_{i+10}^1$ | $k_{i+6}^0$ |
| $k_{i+2}^0 \oplus k_{i+1}^1$ | $k_{i+5}^0$ |
| $k_{i+7}^0 \oplus k_{i+6}^1$ | $k_{i+10}^0$ |
| $k_{i+1}^0$ | |
| $k_i^0$ | |
| $k_{i+2}^0$ | |
| $k_{i+5}^0$ | |
| $k_{i+6}^0$ | |
| $k_{i+7}^0$ | |
| $k_{i+10}^0$ | |
| $k_{i+11}^0$ | |
| $k_{i+15}^0$ | |

After determining the 16 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 $s = 0, 1, 2, \ldots, 15$.

Thus, by obtaining the 16 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 $k^2$. Furthermore, as in [1], we use the majority vote to determine the value of individual key bits. Hence, the final estimation of each bit presents with one of three states: correctly determined bits, incorrectly determined bits, and undetermined bits.

## 5. Linear Approximations for SIMECK 32/64

In this section, we describe 8-round, 10-round, and 12-round attacks using super-rounds of SIMECK 32/64. These attacks are similar to previous work [1] performed on SIMON. At first, we discuss how to derive the required linear approximations. Note that the only non-linear expression in the 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 [20]. Hence, four equivalent approximations can be used:

$$\begin{aligned}
&Approximation\ 1 : Pr[F(XL_i^{j+1}) = XL_{i+1}^{j}] = \frac{3}{4}\\
&Approximation\ 2 : Pr[F(XL_i^{j+1}) = XL_{i+1}^{j} \oplus XL_i^{j}] = \frac{3}{4}\\
&Approximation\ 3 : Pr[F(XL_i^{j+1}) = XL_{i+1}^{j} \oplus XL_{i+5}^{j}] = \frac{3}{4}\\
&Approximation\ 4 : Pr[F(XL_i^{j+1}) = XL_{i+1}^{j} \oplus XL_i^{j} \oplus XL_{i+5}^{j}] = \frac{1}{4}
\end{aligned}$$

### 5.1. 8-Round Attack

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

Using a four-round linear approximation that relates a single bit of the input, we used the super rounds to obtain a single bit of input and then concatenate it with the approximation. Figure 4 depicts the eight-round attack.

Given Approximation 1, we extracted a four-round linear approximation for the left half with bias $2^{-5}$, as follows:

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

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

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

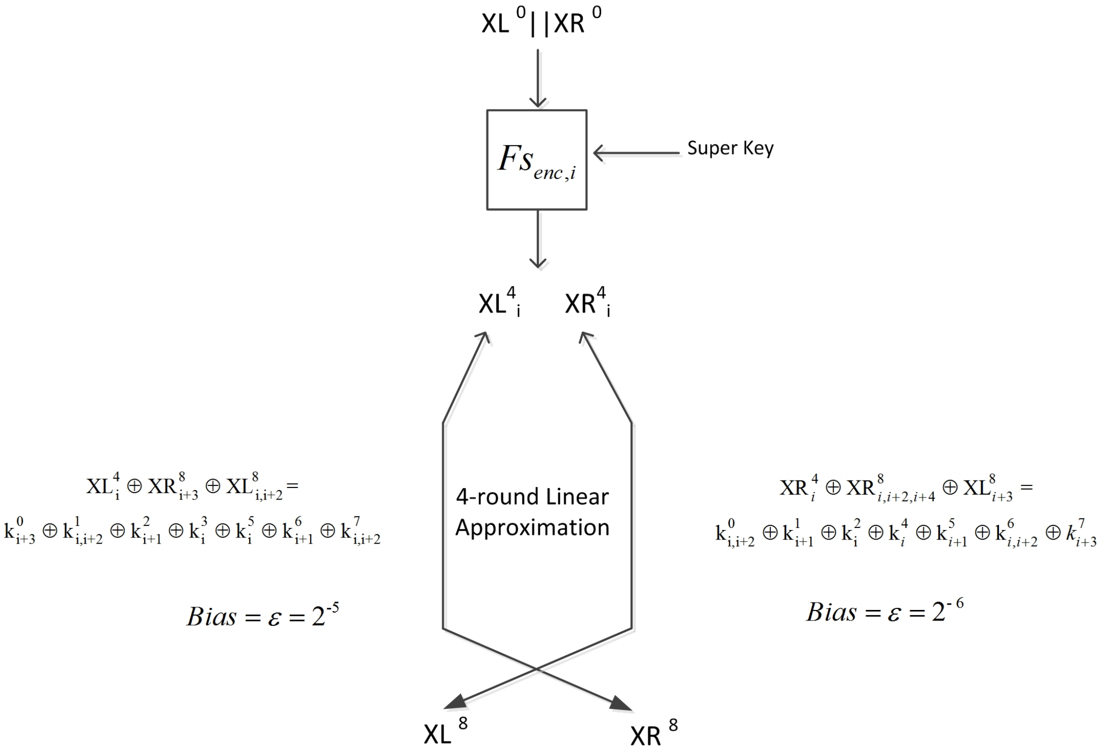

XL 0||XR 0
$Fs_{enc,i}$
Super Key
XL4i
XR4i
$\mathrm{XL}_i^4 \oplus \mathrm{XR}_{i+3}^8 \oplus \mathrm{XL}_{i,i+2}^8 =$
$\mathrm{k}_{i+3}^0 \oplus \mathrm{k}_{i,i+2}^1 \oplus \mathrm{k}_{i+1}^2 \oplus \mathrm{k}_i^3 \oplus \mathrm{k}_i^5 \oplus \mathrm{k}_{i+1}^6 \oplus \mathrm{k}_{i,i+2}^7$
$Bias = \varepsilon = 2^{-5}$
4-round Linear Approximation
$\mathrm{XR}_i^4 \oplus \mathrm{XR}_{i,i+2,i+4}^8 \oplus \mathrm{XL}_{i+3}^8 =$
$\mathrm{k}_{i,i+2}^0 \oplus \mathrm{k}_{i+1}^1 \oplus \mathrm{k}_i^2 \oplus \mathrm{k}_i^4 \oplus \mathrm{k}_{i+1}^5 \oplus \mathrm{k}_{i,i+2}^6 \oplus k_{i+3}^7$
$Bias = \varepsilon = 2^{-6}$
XL 8
XR 8

**Figure 4.** 8-Round Linear Attack.

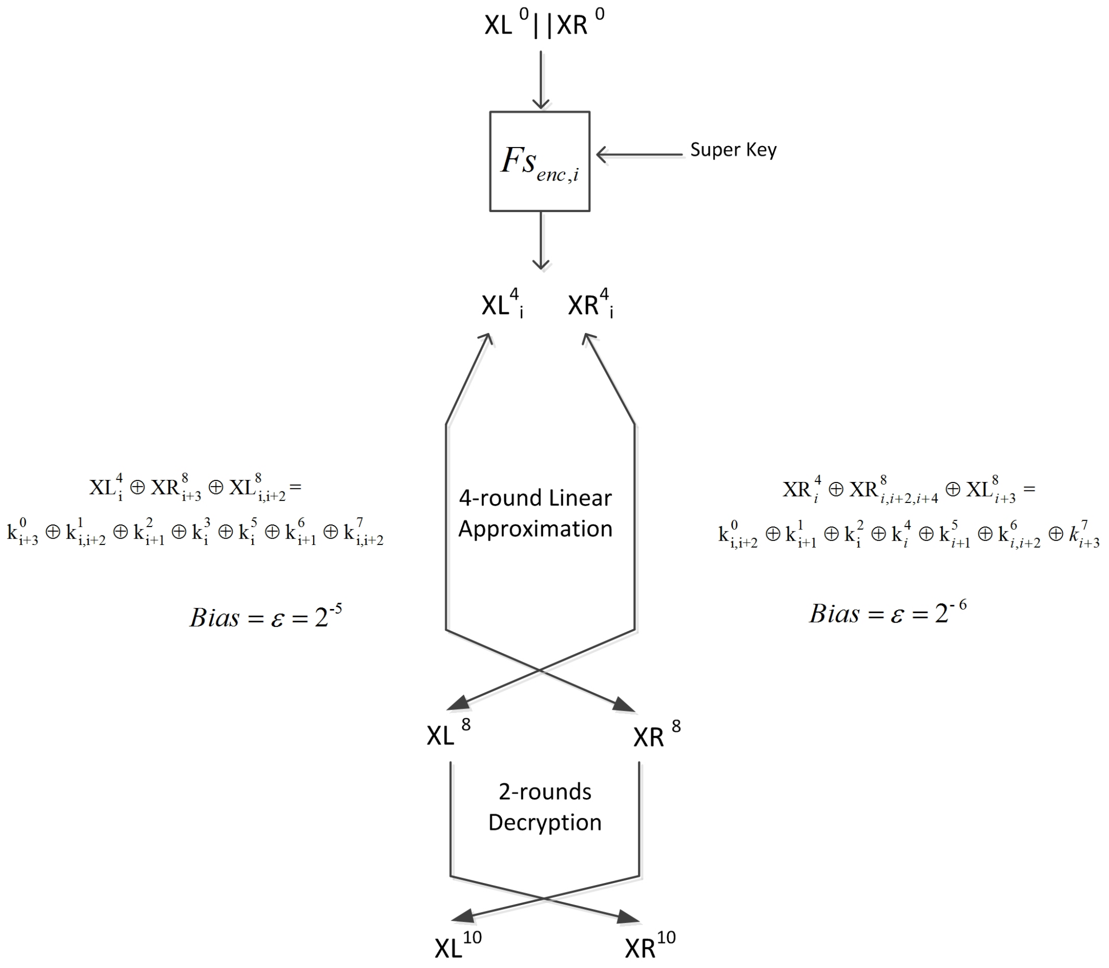
Therefore, we can append the super round to the four-round approximations Equations (3) and (4) to relate the plaintext to the single bit of super round output. Thus, we obtained an approximate relationship between plaintext, ciphertext, and super key bits. This extension enabled us to attack up to eight rounds without further reducing the bias. This gives us the following expressions:

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

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

### 5.2. 10-Round Attack

By adding two rounds of decryption at the end of the 8-round attack, we could obtain a 10-round attack. This extension reuired us to guess 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
$XL^4_i$
$XR^4_i$
$XL^4_i \oplus XR^8_{i+3} \oplus XL^8_{i,i+2} =$
$k^0_{i+3} \oplus k^1_{i,i+2} \oplus k^2_{i+1} \oplus k^3_i \oplus k^5_i \oplus k^6_{i+1} \oplus k^7_{i,i+2}$
$Bias = \varepsilon = 2^{-5}$
4-round Linear Approximation
$XR^4_i \oplus XR^8_{i,i+2,i+4} \oplus XL^8_{i+3} =$
$k^0_{i,i+2} \oplus k^1_{i+1} \oplus k^2_i \oplus k^4_i \oplus k^5_{i+1} \oplus k^6_{i,i+2} \oplus k^7_{i+3}$
$Bias = \varepsilon = 2^{-6}$
$XL^8$
$XR^8$
2-rounds Decryption
$XL^{10}$
$XR^{10}$

**Figure 5.** 10-Round Linear Attack.

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

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

Therefore, the two rounds decryption can be written as follows:

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

Recall Equation (7):

$$XL^4_i \oplus XR^8_{i+3} \oplus XL^8_{i,i+2} = k^7_{i,i+2} \oplus k^6_{i+1} \oplus k^5_i \tag{7}$$

We rewrote $X^8$ in terms of $X^{10}$, which gave us:

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

By substituting the expression of $XL^8$ and $XR^8$, we obtained:

$$XL^4_i \oplus XR^8_{i+3} \oplus XL^8_{i,i+2} = k^7_{i,i+2} \oplus k^6_{i+1} \oplus k^5_i$$

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

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

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

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

Following the same approach, we extended the four-round linear approximation to the right half, and added two rounds of decryption:

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

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

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

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

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

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

In addition to the 16 and 7 key bits required to obtain the input bits for the left and the right half, respectively, extra key bits were required to evaluate the Equations (9) and (10). Two key bits $k_{i+3}^9$ and $k_{i+8}^9$ were required 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).

### *5.3. 12-Round Attack*

Here, we extend the four-round linear approximations Equations (3) and (4) into seven-round linear approximations, using Equations (11) and (12) for the left and right half with biases $2^{-10}$ and $2^{-12}$, respectively (see Tables A1 and A2 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 obtained 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 added one more round of decryption at the end of the 11-round trails and obtained the following 12-round trails for the left half:

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

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

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

A similar process was followed to obtain the 11-round linear approximation for the right half:

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

Figure 6 depicts the 12-round linear attack.

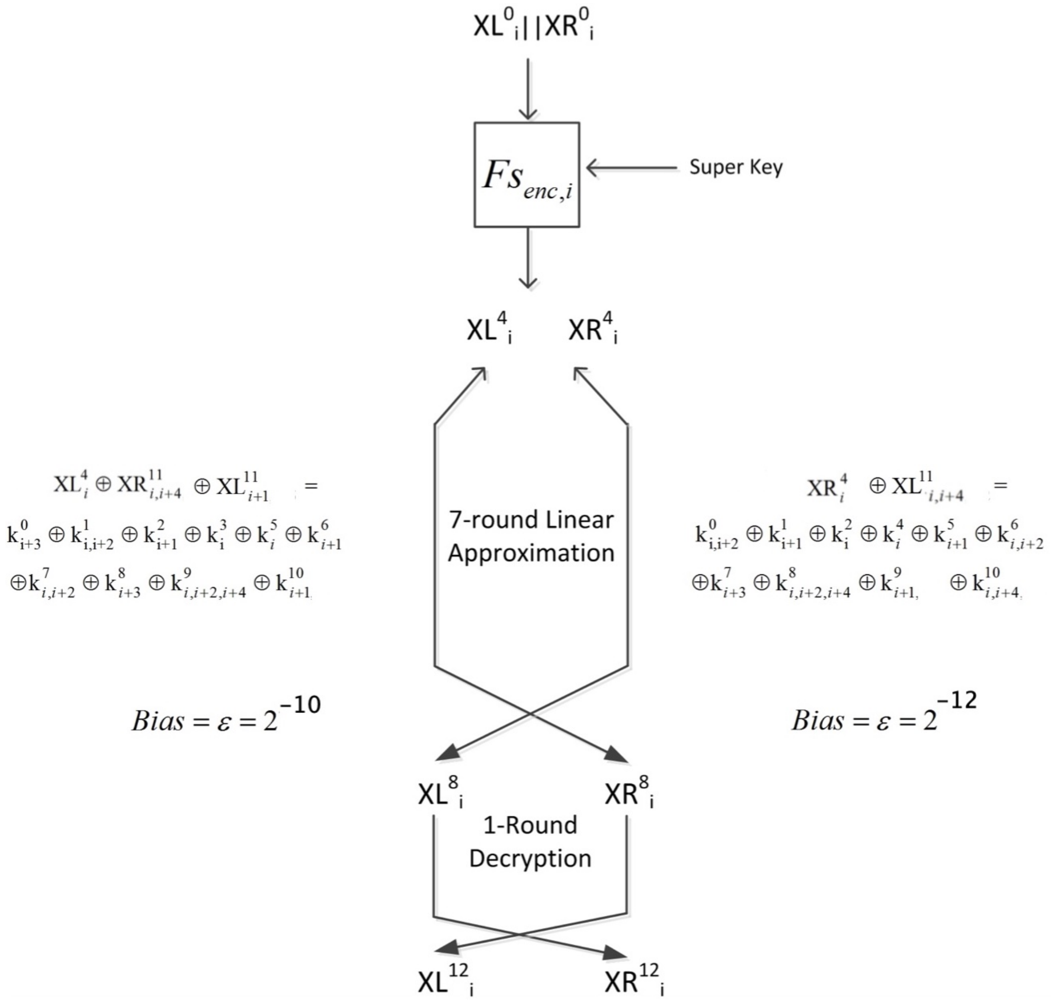

$XL^0_i||XR^0_i$
$Fs_{enc,i}$
Super Key
$XL^4_i$
$XR^4_i$
$XL_i^4 \oplus XR_{i,i+4}^{11} \oplus XL_{i+1}^{11} =$
$k_{i+3}^0 \oplus k_{i,i+2}^1 \oplus k_{i+1}^2 \oplus k_i^3 \oplus k_i^5 \oplus k_{i+1}^6$
$\oplus k_{i,i+2}^7 \oplus k_{i+3}^8 \oplus k_{i,i+2,i+4}^9 \oplus k_{i+1}^{10}$
7-round Linear Approximation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

**Figure 6.** 12-Round Linear Attack.

## 6. Experimental Verification

We conducted several experiments to verify the attacks presented in Section 5 and provide the experimental results presented in this section.

Recall the super key bits shown in Table 4, which come in three forms: $k_i^0$, $k_{i+2}^0 \oplus k_i^1$, or $k_i^0 \oplus k_{i+4}^0 \oplus k_{i+2}^1 \oplus k_i^2$. We reused the notations that appeared in [1], for $Bit1$, $Bit2$, $Bit3$ and $Bit4$. These four bits were determined using Equation (17).

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

### 6.1. 8-Round Key Recovery Attack

To determine the data that were required to conduct the experiments, we followed Matsui's rule [21], which suggests using some multiple of $bias^{-2}$. Thus, the required data complexity for the eight-round attack is a multiple of $2^{-6*-2}$. Therefore, we conducted 14 experiments with $2^{14}$ plain text and cipher text pairs.

Table 5 shows that the estimates derived from evaluating the linear approximation of the right half did not improve the overall results. This is because of the low bias approximations used in this case. As the number of copies of $Bit1$, $Bit2$, and $Bit3$ increased, the accuracy of the estimation results also 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) | Number of Experiments (Out of 14) |
|---|---|---|---|
| 8-round<br>(left half) | $Bit1$ | 16 | 14 |
| | $Bit2$ | 16 | 10 |
| | average number of bits guessed correctly = 15.7 | 15 | 4 |
| | | 15 | 3 |
| | $Bit3$ | 14 | 2 |
| | | 13 | 2 |
| | average number of bits guessed correctly =12.6 | 12 | 2 |
| | | 11 | 3 |
| | | 10 | 2 |
| 8-round<br>(left and right halves) | $Bit1$ | 16 | 14 |
| | $Bit2$ | 16 | 10 |
| | | 15 | 3 |
| | average number of bits guessed correctly = 15.6 | 14 | 1 |
| | | 15 | 3 |
| | $Bit3$ | 14 | 2 |
| | | 13 | 3 |
| | average number of bits guessed correctly = 12.7 | 12 | 2 |
| | | 11 | 2 |
| | | 10 | 2 |

### 6.2. 10-Round Key Recovery Attack

Similar to the previous attack, we implemented a 10-round attack with 14 keys chosen at random and $2^{14}$ P/C pairs. Table 6 shows that, compared to the results obtained in the 8-round attack, we obtained a different observation. 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, and only two copies from the left-half evaluation.

**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) | *Bit*1 | 16 | 14 |
| | *Bit*2 | 16 | 10 |
| | average no. bits guessed correctly = 15.7 | 15 | 4 |
| | *Bit*3 | 16 | 2 |
| | average no. bits guessed correctly = 12.6 | 14 | 4 |
| | | 13 | 1 |
| | | 11 | 5 |
| | | 10 | 2 |
| | *Bit*4 | 16 | 1 |
| | average no. bits guessed correctly = 13 | 15 | 1 |
| | | 14 | 3 |
| | | 13 | 4 |
| | | 12 | 3 |
| | | 11 | 2 |
| 10-round (left and right halves) | *Bit*1 | 16 | 14 |
| | *Bit*2 | 16 | 11 |
| | average no. bits guessed correctly =15.7 | 15 | 2 |
| | | 14 | 1 |
| | *Bit*3 | 16 | 2 |
| | average no. bits guessed correctly = 12.6 | 14 | 4 |
| | | 13 | 1 |
| | | 11 | 5 |
| | | 10 | 2 |
| | *Bit*4 | 16 | 9 |
| | average no. bits guessed correctly = 15.5 | 15 | 3 |
| | | 14 | 2 |

### *6.3. 12-Round Key Recovery Attack*

We conducted three experiments regarding the 12-round attack using $2^{24}$ P/C pairs, with keys chosen at random. Table 7 shows similar results to those of the eight-round attack. The combined estimation of both halves (left and right) did not enhance the results obtained 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) | *Bit*1 | 16 | 3 |
| | *Bit*2 | 16 | 3 |
| | *Bit*3 | 15 | 1 |
| | average no. bits guessed correctly = 14.3 | 14 | 2 |
| 12-round (left and right halves) | *Bit*1 | 16 | 3 |
| | *Bit*2 | 16 | 3 |
| | *Bit*3 | 15 | 1 |
| | average no. bits guessed correctly = 14.3 | 14 | 2 |

### 6.4. *Experimental Results of 8-Round Attack without Approximations*

Since SIMECK is designed based on the Feistel structure, and an essential features of this design is that the same algorithm was used for encryption and decryption, an equivalent super-round of four rounds of decryption was also established. We can launch a meet-in-the-middle attack on eight-round linear cryptanalyses of SIMECK 32/64 without any approximations, which is the same attack that was launched 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 started with one super round in the forward direction and the second super round in the backward direction; hence, we could 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 four-rounds encryption $XL_i^4$. Then, the second super round $F_{S2}$ takes the ciphertext and eight key bits $K2$, and generates a single bit of four-rounds decryption. Following the procedure described in [1], we computed $F_{S1}$ and $F_{S2}$ for all possible values of the encryption and decryption super-keys for every bit $i$.

We conducted two experiments using only 48 plain text and cipher text pairs; we were able to retrieve the correct value of the 112 bits.

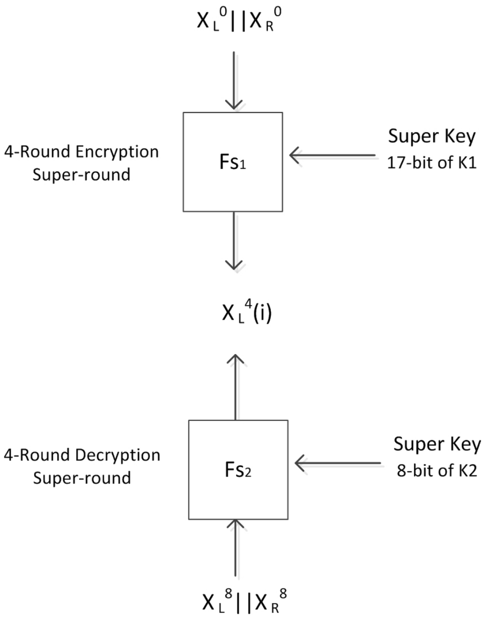


**Figure 7.** 8-Round attack without approximations.

### 6.5. *Summary of Experimental Results*

Here, we provide a summary of our experimental results. See Table 8.

**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% |

## 7. Projected Results Using Multiple Linear Cryptanalysis

This section presents two projected linear attacks; the first uses a single super-round, which is the direct application of the approach presented in [1], and the second is a new class of attacks where we use multiple super-rounds.

### *7.1. Linear Attacks Using a Single Super-Round*

Here, we present a 19-round linear attack, a direct application of the original attack that we proposed in [1]. This is achieved by extending the 12-round linear approximations in Equation (18) and appending the super rounds of four rounds of encryption and three rounds of decryption.

To compute the data complexity, we first compute the capacity:

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

Nine key bits must be estimated to add three rounds of decryption to the approximations for the left half:

- Seven bits of $k_i^{19}$ for $i = 3, 8, 13, 0, 5, 2, 7$;
- Two bits of the sum:$k_{i+1}^{19} \oplus k_i^{18}$ for $i = 3, 8$.

Twelve key bits must be estimated to add three rounds of decryption to the approximations for the right half:

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

The time complexity required for this attack to evaluate the approximations for the left half is $16 \times 2^{30} \times 2^{16} \times 2^9 = 2^{59}$. For the right side, it is $16 \times 2^{30} \times 2^7 \times 2^{12} = 2^{53}$. The overall complexity required to evaluate the two halves is $2^{59.02}$.

Hence, we can attack 20 rounds in the case of average-case computations by extending the 12-round linear approximations of Equation (18), appending a single super round of four rounds of encryption and adding four rounds of decryption.

We extended the seven-round linear characteristics in 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.

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

We compute the capacity for the system of approximations as follows:

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

The super round costs on average 11.5 and 4.5 were appended for the left and the right half, respectively. Moreover, four rounds of decryption costs were appended by estimating, on average, 16 key bits and 18.5 key bits for the left- and right-half approximations, respectively.

Twenty-three key bits (16 bits on average) are needed to estimate the left-half approximations:

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

Twenty-five key bits (18.5 bits on average) are required to estimate the right-half approximations:

- Thirteen bits of $k_i^{19}$ for $i = 0, 5, 8, 10, 1, 6, 15, 11, 2, 7, 12, 3, 13$, each counted as a half bit
- Eight bits of the sum : $k_{i+1}^{19} \oplus k_i^{18}$ for $i = 0, 5, 10, 2, 7, 12, 1, 6$.
- Four 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 required to evaluate the approximations for the left half is $2^4 \times 2^{30} \times 2^{11.5} \times 2^{16} = 2^{61.5}$, in addition to the complexity of evaluating the approximations for the right half = $2^4 \times 2^{30} \times 2^{4.5} \times 2^{18.5} = 2^{57}$. Thus, the total time complexity is $2^{61.56}$.

### 7.2. *Improved Linear Approximations for* SIMECK *32/64*

The approximations used in the attack presented in Section 7.1 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 Table A3 for the derivation).

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

### 7.3. *Linear Attacks Using Multiple Super Rounds*

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

The system of approximations has the following capacity:

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

Thus, the data complexity for this attack is $2^{30}$.

The three super-rounds require that three super-keys are estimated, which consist of:

- Fourteen bits of the last round key $k_i^0$ for $i = 10, 5, 14, 9, 4, 8, 3, 2, 13, 0, 1, 6, 7, 12$, with each counted as a half bit.
- Nine bits of the sum $k_{i+1}^0 \oplus k_i^1$ for $i = 9, 4, 13, 8, 3, 0, 5, 2, 7$.
- Two bits of the sum $k_{i,i+2}^0 \oplus k_{i+1}^1 \oplus k_i^2$ for $i = 3, 8$.

The cost of appending three super-rounds (one for each input mask bit) is guessing 25 key bits. Additionally, two more key bits $k_{0,5}^{18}$ required estimation to append two decryption rounds. The time complexity for this attack is $2^4 \times 2^{25} \times 2^2 \times 2^{30} = 2^{61}$.

In the average-case complexity, we can add one more round of decryption to the 19-round attack and present a 20-round attack.

Nine key bits must be estimated to add three rounds of decryption:

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

As a result, the average cost of 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 $2^4 \times 2^{30} \times 2^{18} \times 2^{6.5} = 2^{58.5}$.

Table 9 summarizes our results of SIMECK 32/64 and compares them with the best results presented in [2]. We were able to go deeper by two rounds.

**Table 9.** Comparison results on SIMECK 32.

| Average Case Computations | | | |
|---|---|---|---|
| **SIMECK** | **Number of Rounds** | **Data Complexity** | **Time Complexity** |
| 32/64 | Using Single Super Round Presented in Section 7.1 | | |
| | 20-round | $2^{30}$ | $2^{61.56}$ |
| | Using Multiple Super Rounds Presented in Section 7.3 | | |
| | 20-round | $2^{30}$ | $2^{58.5}$ |
| | Projections from data in [2] | | |
| | 18-round | $2^{24}$ | $2^{60.5}$ |

## 8. The Effect of Super Rounds on Larger Variants of SIMECK

In contrast to SIMON, the larger versions of SIMECK have the same super keys with the same size. Therefore, we were able to attack larger number of rounds.

For SIMECK 48, incorporating multiple super-rounds instead of a single super-round yields better results. 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 approximation and added nine rounds at both ends: four rounds of encryption and five rounds of decryption, at the cost of guessing 49 key bits on average. Thus we attack up to 34 rounds of this version of SIMECK.

## 9. Discussion

The outcomes of this research have provided insight into the differences between SIMON and SIMECK; even though they are very similar in design, hence applying our attack model on reduced round SIMECK results in better attacks on most of SIMECK versions than on SIMON. We are able to present linear cryptanalysis on 29-round SIMECK 48/96 and 34-round SIMECK 64/128, whereas in the case of SIMON for the same versions, we are only able to attack 21-round and 25-round respectively. These improved results are caused by the rotational functions, which is the only difference between the two ciphers.

We observed in that experiments that we got the same number of master key bits in the 8-round and 12-round versions, but recovered more key bits with the 10-round attack. This is because $k_9$ consists of some bits of the master key; see Appendix A for more details. Additionally, the 8-round versions of both SIMON and SIMECK are broken employing two super-rounds.

## 10. Conclusions and Future Work

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. 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 attacks on 20 rounds of SIMECK 32, 29 rounds of SIMECK 48 and 34 rounds of SIMECK 64. Thus, relaxing the constraint of using only linear approximations with one active input mask enhances the efficiency of attack on SIMECK 32 and enables us to present a better attack on SIMECK 48.

In future work, it would be interesting to examine similar lightweight ciphers, such as Spix, and see if our attack using super-rounds are applicable. Another aspect that could be investigated is combining the proposed model with linear-differential cryptanalysis.

**Author Contributions:** R.A. led the work for her doctoral dissertation, contributing most of the effort. P.L.V. provided guidance. All authors have read and approved the final version of the manuscript.

**Funding:** This research was sponsored in part by NSF Award 1421373.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix 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 (A1), which is expressed in terms of the master key bits in Equation (A2).

$$k^9 = k^5 \oplus F(k^6) \oplus c \oplus (z_0)_5 \tag{A1}$$

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

$$k^9 = k^1 \oplus F(k^2) \oplus F(k^2 \oplus f(k^3)) \oplus C \oplus (Z_0)_1 \oplus C \oplus (Z_0)_2 \oplus C \oplus (Z_0)_5 \tag{A2}$$

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 can assume that the output of $f$ is zero:

$$\begin{aligned} F(X) &= (0^n \oplus XL^j \lll 1) \\ &= XL^j \lll 1 \end{aligned} \tag{A3}$$

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

We can write the inverse function as follows:

$$F^{-1}(X) = X \lll 1 \tag{A4}$$

Therefore, to write $k^9$ in terms of the master key, we apply (A4) in (A2):

$$\begin{aligned} k^9 &= k^1 \oplus f^{-1}(k^2) \oplus f^{-1}(k^2 \oplus f^{-1}(k^3))C \oplus (Z_0)_1 \oplus C \oplus (Z_0)_2 \oplus C \oplus (Z_0)_5 \\ &= k^1 \oplus (k^2 \lll 1) \oplus (k^2 \lll 1) \oplus (k^3 \lll 2) \oplus C \oplus (Z_0)_1 \oplus C \oplus (Z_0)_2 \oplus C \oplus (Z_0)_5 \end{aligned} \tag{A5}$$

## Appendix B. Derive 13-Round Linear Approximations for SIMECK 32/64

**Table A1.** The sequence of approximations used to derive 13-round 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 A2.** 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 | | |

## Appendix C. Derive an Improved 13-Round Linear Approximations for SIMECK 32/64

**Table A3.** The sequence of approximations used to derive a 13-round 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 | | |

## Appendix D. Linear Cryptanalysis of SIMECK 48/96 Using a Single Super Round

In contrast to SIMON, the larger versions of SIMECK have exact super keys of the same size. Therefore, we can attack up to 27 rounds of SIMECK 48/96.

### *Appendix D.1. Linear Approximations for* SIMECK *48/96*

We can extend the 12-round linear trail Equation (18) into 20-round linear expressions, with biases $=2^{-27}$ and $2^{-28}$ for the left half and right half, respectively (see Tables A4 and A5 for more details):

$$PL_i \oplus XR^{20}_{i+3} \oplus XL^{20}_{i,i+2} = k^{19}_{i,i+2} \oplus k^{18}_{i+1} \oplus k^{17}_{i} \oplus k^{15}_{i} \oplus k^{14}_{i+1} \oplus k^{13}_{i,i+2} \oplus k^{12}_{i+3} \oplus$$
$$k^{11}_{i,i+4,i+2} \oplus k^{10}_{i+1,i+5} \oplus k^{9}_{i,i+4} \oplus k^{7}_{i,i+4} \oplus k^{6}_{i+1} \oplus k^{5}_{i,i+2,i+4} \oplus k^{4}_{i+3} \oplus k^{3}_{i,i+2} \oplus k^{2}_{i+1} \oplus k^{1}_{i} \tag{A6}$$

$$PR_i \oplus XR^{20}_{i,i+2,i+4} \oplus XL^{20}_{i+3} = k^{19}_{i+3} \oplus k^{18}_{i,i+2} \oplus k^{17}_{i+1} i \oplus k^{16}_{i} \oplus k^{14}_{i} \oplus k^{13}_{i+1} \oplus k^{12}_{i,i+2} \oplus k^{11}_{i+3}$$
$$\oplus k^{10}_{i+2,i,i+4} \oplus k^{9}_{i+1,i+5} \oplus k^{8}_{i,i+4} \oplus k^{6}_{i,i+4} \oplus k^{5}_{i+1} \oplus k^{4}_{i,i+2,i+4} \oplus k^{3}_{i+3} \oplus k^{2}_{i,i+2} \oplus k^{1}_{i+1} \oplus k^{0}_{i}$$

**Table A4.** The sequence of approximations used to derive 20-round linear trails for the left-half of SIMECK 48.

| Active Bits on the Left Side | Active Bits on 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 | 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 | | |

**Table A5.** The sequence of approximations used to derive 20 rounds for the right-half of SIMECK 48.

| Active Bits on the Left Side | Active Bits on 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 | 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 | | |

### *Appendix D.2. 28-Round Linear Attacks of* SIMECK *48/96*

We can append four rounds encryption and four rounds decryption to the 20-round linear trails, and we get a 28-round linear attack.

To determine the number of plaintext and ciphertext pairs required, we compute the capacity:

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

The key bits required guessing to add four rounds of decryption to the left half approximations are:

- 14 bits of $k_i^{27}$, for $i = 3, 8, 13, 4, 7, 18, 9, 14, 0, 5, 10, 2, 6, 12$
- 9 bits of the sum $k_{i,i+2}^{27} \oplus k_{i+1}^{26}$ for $i = 3, 8, 13, 0, 5, 2, 7, 4, 9$
- 2 bits of the sum $k_{i,i+2}^{27} \oplus k_{i+1}^{26} \oplus k_i^{25}$ for $i = 3, 8$

The key bits required guessing to add four rounds of decryption to the right half approximations are:

- 18 bits of $k_i^{27}$, for $i = 0, 5, 10, 15, 1, 6, 11, 2, 7, 12, 3, 8, 17, 13, 4, 9, 14, 19$
- 11 bits of the last round key $k_i^{26}$ for $i = 0, 5, 10, 2, 7, 12, 4, 9, 14, 1, 6$
- 6 bits of the sum $k_{i+1}^{26} \oplus k_i^{25}$ for $i = 0, 5, 2, 7, 4, 9$

The complexity to evaluate the approximations for the left half is $2^{4.585} \times 2^{47.42} \times 2^{16} \times 2^{25} = 2^{93}$. In addition to the complexity for evaluating the right half approximations which is $2^{4.585} \times 2^{47.42} \times 2^7 \times 2^{35} = 2^{94}$. Therefore the overall time complexity to mount a 28-round linear attack is $2^{94.58}$.

In the case of average-case computations, the complexity to evaluate the approximations for the left half is $24 \times 2^{47.42} \times 2^{11.5} \times 2^{18} = 2^{82.5}$. In addition to the complexity for right half approximations which is $24 \times 2^{47.42} \times 2^{4.5} \times 2^{26} = 2^{83.5}$. Therefore the overall time complexity to mount a 28-round linear attack is $2^{84.08}$.

## Appendix E. Linear Cryptanalysis of SIMECK 48/96 Using Multiple Super-Rounds

Here, we extend the 13-round linear approximation Equation (19) into a 20-round approximation (A7) with bias=$2^{-27}$ (see Table A6 for detailed derivation).

$$PL_{i+3} \oplus PR_{i,i+2} \oplus XR_i^{20} = k_i^{18} \oplus k_{i+1}^{17} \oplus k_{i,i+2}^{16} \oplus k_{i+3}^{15} \oplus k_{i,i+2,i+4}^{14} \oplus k_{i,i+4}^{10} \oplus \\ k_{i+1}^{9} \oplus k_{i,i+2,i+4}^{8} \oplus k_{i+3}^{7} \oplus k_{i,i+2}^{6} \oplus k_{i+1}^{5} \oplus k_i^{4} \oplus k_i^{2} \oplus k_{i+1}^{1} \oplus k_{i,i+2}^{0} \tag{A7}$$

### *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 of encryption and four rounds of decryption to the 20-round linear approximation.

The system of approximations has the following capacity:

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

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

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

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. Adding four rounds of decryption requires the estimation of 16 key bits:

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

Thus, the required time complexity for this attack is $2^{4.585} \times 2^{47.42} \times 2^{26} \times 2^{16} = 2^{94.005}$.

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

- Twelve bits of the last round key $k_i^{28}$ for $i = 0, 5, 10, 1, 6, 15, 11, 2, 7, 16, 12, 20$, with each counted as a half bit.
- Nine bits of the sum $k_{i+1}^{28} \oplus k_i^{27}$ for $i = 7, 2, 11, 6, 1, 5, 0, 15, 10$.
- Five bits of the sum $k_{i,i+2}^{28} \oplus k_{i+1}^{27} \oplus k_i^{26}$ for $i = 6, 1, 10, 5, 0$.
- Two 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 was, on average, reduced to the estimation of 18.5 key bits.

**Table A6.** The sequence of approximations used to derive 20 rounds of 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 | | |

## Appendix F. Linear Cryptanalysis of SIMECK 64/128 Using a Single Super-Round

Here, we present a 33-round linear attack of SIMECK 64/128.

### *Appendix F.1. Linear Approximations for* SIMECK *64/128*

We extend the 20-round linear expressions Equation (A8) into 25-round linear trails for the left and right half with biases $2^{-34}$ and $2^{-36}$, respectively (see Tables A7 and A8 for details) :

$$\begin{aligned}
&PL_i \oplus XR^{25}_{i,i+4} \oplus k^{23}_{i,i+4} \oplus k^{22}_{i+1} \oplus k^{21}_{i+4,i,i+2} \oplus k^{20}_{i+3} \oplus k^{19}_{i,i+2} \oplus k^{18}_{i+1} \oplus k^{17}_{i} \oplus k^{15}_{i} \oplus k^{14}_{i+1} \\
&\oplus k^{13}_{i,i+2} \oplus k^{12}_{i+3} \oplus k^{11}_{i,i+4,i+2} \oplus k^{10}_{i+1,i+5} \oplus k^{9}_{i,i+4} \oplus k^{7}_{i,i+4} \oplus k^{6}_{i+1} \oplus k^{5}_{i,i+2,i+4} \oplus k^{4}_{i+3} \oplus k^{3}_{i,i+2} \\
&\oplus k^{2}_{i+1} \oplus k^{1}_{i} \\
&PR_i \oplus XR^{25}_{i+1,i+5} \oplus XL^{25}_{i,i+4} \oplus k^{24}_{i,i+4} \oplus k^{22}_{i,i+4} \oplus k^{21}_{i+1} \oplus k^{20}_{i,i+2,i+4} \oplus k^{19} \oplus k^{18}_{i,i+2} \oplus k^{17}_{i+1} \\
&\oplus k^{16}_{i} \oplus k^{14}_{i} \oplus k^{13}_{i+1} \oplus k^{12}_{i,i+2} \oplus k^{11}_{i+3} \oplus k^{10}_{i+2,i,i+4} \oplus k^{9}_{i+1,i+5} \oplus k^{8}_{i,i+4} \oplus k^{6}_{i,i+4} \oplus k^{5}_{i+1} \\
&\oplus k^{4}_{i,i+2,i+4} \oplus k^{3}_{i+3} \oplus k^{2}_{i,i+2} \oplus k^{1}_{i+1} \oplus k^{0}_{i}
\end{aligned} \tag{A8}$$

**Table A7.** The sequence of approximations used to derive 25-round linear trails for the left half of SIMECK 64.

| 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 | 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 | 1;1;1 | 3 |
| 0,2,4 | 1 | 1 | 1 |
| 1 | 0,4 | 1;1 | 2 |
| 0,4 | - | | |
| | 0,4 | | |

**Table A8.** The sequence of approximations used to derive 25 rounds for the right half of SIMECK 64.

| Active Bits on the Left Side | Active Bits on 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 | 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 | 1;1;1 | 3 |
| 0,2,4 | 1 | 1 | 1 |
| 1 | 0,4 | 1;3 | 2 |
| 0,4 | - | | |
| - | 0,4 | 1;1 | 2 |
| 0,4 | 1,5 | | |

### *Appendix F.2. 34-Round Linear Attacks of* SIMECK *64/128*

We produce a 34-round linear cryptanalysis by appending four rounds of encryption and five rounds of decryption to the 25-round linear approximations, as follows:

The capacity of the 25-round linear trail is:

$$\bar{c}^2 = 4 \times 32 \times 2^{-34\times 2} = 2^6 \times 2^{-34^2} = 2^{-61}$$

Forty-three key bits must be estimated to add five rounds of decryption to the left-half approximations:

- Eighteen bits of $k_i^{33}$ for $i = 0, 5, 10, 1, 6, 11, 2, 7, 20, 16, 12, 4, 9, 14, 19, 24, 3, 8$.
- Thirteen bits of the last round key $k_i^{32}$ for $i = 0, 3, 10, 1, 6, 15, 11, 4, 9, 14, 5, 19, 2$.
- Eight bits of the sum $k_{i+1}^{32} \oplus k_i^{31}$ for $i = 6, 1, 10, 5, 0, 14, 9, 4$.
- Four bits of the sum $k_{i,i+2}^{32} \oplus k_{i+1}^{31} \oplus k_i^{30}$ for $i = 0, 5, 9, 4$.

Fifty-three key bits must be estimated to add five rounds of decryption to the right-half approximations:

- Twenty-one bits of $k_i^{33}$ for $i = 15, 20, 10, 5, 6, 11, 2, 7, 1, 12, 8, 13, 4, 9, 14, 19, 16, 21, 3, 17, 0$.

- Seventeen bits of the last round key $k_i^{32}$ for $i = 1, 6, 11, 2, 7, 16, 12, 5, 10, 15, 20, 0, 4, 9, 14, 3, 8$.
- Eleven bits of the sum $k_{i+1}^{32} \oplus k_i^{31}$ for $i = 7, 2, 11, 6, 1, 15, 10, 5, 0, 4, 9$.
- Four bits of the sum $k_{i,i+2}^{32} \oplus k_{i+1}^{31} \oplus k_i^{30}$ for $i = 6, 1, 10, 5$.

Thus, the time complexity required to evaluate the left-half approximations is $2^5 \times 2^{16} \times 2^{43} \times 2^{61} = 2^{125}$, in addition to the complexity required to evaluate the right-half approximations, which is $2^5 \times 2^7 \times 2^{53} \times 2^{61} = 2^{126}$. The overall time complexity is $2^{126.5}$.

In the case of average time computations, we can reduce the complexity of the 34-round linear attack and count some bits as a half bit. Thus, the time complexity required to evaluate the left-half approximations reduced to $2^5 \times 2^{11.5} \times 2^{34} \times 2^{61} = 2^{111.5}$. Additionally, evaluating the right-half approximations requires the estimation of 53 key bits, on average, which reduced to 43; hence, the time complexity required to evaluate the right-half approximations is $2^5 \times 2^{4.5} \times 2^{40.5} \times 2^{61} = 2^{112}$. The total complexity required to evaluate the two halves is $2^{112}$.

## Appendix G. Linear Cryptanalysis of SIMECK 64/128 Using Multiple Super Rounds

In this section, we apply the attack model using multiple super rounds.

### *Appendix G.1. Improved Linear Approximation for* SIMECK *64/128*

We extended the 20-round linear approximation (A7) into a 25-round linear approximation (A9) with bias=$2^{-35}$ (see Table A9 for derivation).

$$\begin{aligned}&PL_{i+3} \oplus PR_{i,i+2} \oplus XR_{i+1}^{25} \oplus XL_{i,i+2,i+4}^{25} = k_{i,i+2,i+4}^{24} \oplus k_{i+3}^{23} \oplus k_{i,i+2}^{22} \oplus XR_{i+1}^{23} \oplus k_i^{20} \oplus k_i^{18}\\&\oplus k_{i+1}^{17} \oplus k_{i,i+2}^{16} \oplus k_{i+3}^{15} \oplus k_{i,i+2,i+4}^{14} \oplus k_{i,i+4}^{10} \oplus k_{i+1}^{9} \oplus k_{i,i+2,i+4}^{8} \oplus k_{i+3}^{7} \oplus k_{i,i+2}^{6} \oplus k_{i+1}^{5}\\&\oplus k_i^4 \oplus k_i^2 \oplus k_{i+1}^1 \oplus k_{i,i+2}^0\end{aligned} \tag{A9}$$

### *Appendix G.2. 33-Round and 34-Round Linear Attacks of* SIMECK *64/128 Using Multiple Super-Rounds*

We extended the 25-round linear trail (A9), and added four rounds of encryption and four rounds of decryption; hence we could attack up to 33 rounds 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 $2^{63}$.

To obtain the components of three super-keys, leading to a total of 26 key bits, four rounds of encryption must be added:

- Fourteen bits of the last round key $k_i^0$ for $i = 10, 5, 14, 9, 4, 8, 3, 2, 18, 13, 0, 1, 6, 7, 12$, with each counted as a half bit.
- Nine bits of the sum $k_{i+1}^0 \oplus k_i^1$ for $i = 9, 4, 13, 8, 3, 0, 5, 2, 7$.
- Two bits of the sum $k_{i,i+2}^0 \oplus k_{i+1}^1 \oplus k_i^2$ for $i = 3, 8$.

The cost of adding four rounds of decryption, leading to a total of 22 key bits, is as follows:

- Thirteen bits of the last round key $k_i^{32}$ for $i = 7, 2, 11, 6, 1, 5, 0, 15, 10, 14, 3, 4, 9$.
- Seven bits of the sum $k_{i+1}^{32} \oplus k_i^{31}$ for $i = 1, 6, 11, 0, 5, 4, 9$.
- Two 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 added five rounds of decryption. Five rounds of decryption were added, leading to a total of 39 key bits (30.5 bits on average):

- Seventeen bits of the last round key $k_i^{33}$ for $i = 1, 6, 11, 16, 2, 7, 12, 21, 17, 0, 5, 10, 15, 4, 9, 14, 19$, with each counted as a half bit.
- Thirteen bits of the sum $k_{i+1}^{33} \oplus k_i^{32}$ for $i = 7, 2, 11, 6, 1, 5, 0, 15, 10, 14, 3, 4, 9$.
- Seven bits of the sum $k_{i,i+2}^{33} \oplus k_{i+1}^{32} \oplus k_i^{30}$ for $i = 1, 6, 11, 0, 5, 4, 9$.
- Two 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 required for this attack is $2^5 \times 2^{63} \times 2^{18} \times 2^{30.5} = 2^{116.5}$.

**Table A9.** The sequence of approximations used to derive 25-round 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 | | |

## References

1. Almukhlifi, R.; Vora, P. Linear Cryptanalysis of Reduced-Round Simon Using Super Rounds. *Cryptography* **2020**, *4*, 9. [CrossRef]
2. Bagheri, N. Linear Cryptanalysis of Reduced-Round SIMECK Variants. In Proceedings of the Progress in Cryptology—INDOCRYPT 2015—16th International Conference On Cryptology In India, Bangalore, India, 6–9 December 2015; Volume 9462, pp. 140–152. [CrossRef]
3. Biryukov, A.; Cannière, C.; Quisquater, M. On Multiple Linear Approximations. In Proceedings of the Advances in Cryptology—CRYPTO 2004, 24th Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 2004; Volume 3152, pp. 1–22. [CrossRef]

4. Yang, G.; Zhu, B.; Suder, V.; Aagaard, M.; Gong, G. The Simeck Family of Lightweight Block Ciphers. In Proceedings of the Cryptographic Hardware and Embedded Systems—CHES 2015—17th International Workshop, Saint-Malo, France, 13–16 September 2015; Volume 9293, pp. 307–329. [CrossRef]
5. Kölbl, S.; Roy, A. A Brief Comparison of Simon and Simeck. In Proceedings of the Lightweight Cryptography for Security And Privacy—5th International Workshop, LightSec 2016, Aksaray, Turkey, 21–22 September 2016; Volume 10098, pp. 69–88. [CrossRef]
6. Qiao, K.; Hu, L.; Sun, S. Differential Security Evaluation of Simeck with Dynamic Key-guessing Techniques. In Proceedings of the 2nd International Conference on Information Systems Security and Privacy, ICISSP 2016, Rome, Italy, 19–21 February 2016; pp. 74–84. [CrossRef]
7. Qin, L.; Chen, H.; Wang, X. Linear Hull Attack on Round-Reduced Simeck with Dynamic Key-Guessing Techniques. In Proceedings of the Information Security And Privacy—21st Australasian Conference, ACISP 2016, Proceedings, Part II, Melbourne, VIC, Australia, 4–6 July 2016; Volume 9723, pp. 409–424. [CrossRef]
8. Bogdanov, A.; Rijmen, V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Des. Codes Cryptogr.* **2014**, *70*, 369–383. [CrossRef]
9. Zhang, K.; Guan, J.; Hu, B.; Lin, D. Security evaluation on Simeck against zero-correlation linear cryptanalysis. *IET Inf. Secur.* **2018**, *12*, 87–93. [CrossRef]
10. Sadeghi, S.; Bagheri, N. Improved zero-correlation and impossible differential cryptanalysis of reduced-round SIMECK block cipher. *IET Inf. Secur.* **2018**, *12*, 314–325. [CrossRef]
11. Li, H.; Ren, J.; Chen, S. Improved Integral Attack on Reduced-Round Simeck. *IEEE Access* **2019**, *7*, 118806–118814. [CrossRef]
12. Nalla, V.; Sahu, R.; Saraswat, V. Differential Fault Attack on SIMECK. In Proceedings of the Third Workshop on Cryptography and Security in Computing Systems, CS2@HiPEAC, Prague, Czech Republic, 20 January 2016; pp. 45–48. [CrossRef]
13. Le, D.; Lu, R.; Ghorbani, A. Improved fault analysis on SIMECK ciphers. *J. Cryptogr. Eng.* **2022**, *12*, 169–180. [CrossRef]
14. Dofe, J.; Frey, J.; Pahlevanzadeh, H.; Yu, Q. Strengthening SIMON Implementation Against Intelligent Fault Attacks. *IEEE Embed. Syst. Lett.* **2015**, *7*, 113–116. [CrossRef]
15. Benjamin, A.; Herzoff, J.; Babinkostova, L.; Serra, E. Deep Learning Based Side Channel Attacks on Lightweight Cryptography (Student Abstract). In Proceedings of the Thirty-Sixth AAAI Conference on Artificial Intelligence, AAAI 2022, Thirty-Fourth Conference on Innovative Applications of Artificial Intelligence, IAAI 2022, the Twelveth Symposium on Educational Advances in Artificial Intelligence, EAAI 2022, Virtual Event, 22 February–1 March 2022; pp. 12911–12912.
16. Wu, C.; Zhang, H.; Xu, J.; Sun, S. Side Channel Attack of Lightweight Block Cipher Simeck Based on Deep Learning. In Proceedings of the 2019 IEEE 6th International Symposium on Electromagnetic Compatibility (ISEMC), Nanjing, China, 1–4 November 2019; pp. 1–5.
17. Baksi, A.; Breier, J.; Dasu, V.; Dong, X.; Yi, C. Following-up on Machine Learning Assisted Differential Distinguishers. (SILC Workshop, 2020). Available online: https://www.esat.kuleuven.be/cosic/events/silc2020/wp-content/uploads/sites/4/2020/10/Submission4.pdf (accessed on 24 January 2023).
18. Baksi, A.; Breier, J.; Chen, Y.; Dong, X. Machine Learning Assisted Differential Distinguishers For Lightweight Ciphers. In Proceedings of the Design, Automation & Test in Europe Conference & Exhibition, DATE 2021, Grenoble, France, 1–5 February 2021; pp. 176–181. [CrossRef]
19. Tian, J.; Wu, B.; Wang, Z. High-Speed FPGA Implementation of SIKE Based on an Ultra-Low-Latency Modular Multiplier. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2021**, *68*, 3719–3731. [CrossRef]
20. Nyberg, K. Linear Approximation of Block Ciphers. In Proceedings of the Advances in Cryptology—EUROCRYPT'94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, 9–12 May 1994; Volume 950, pp. 439–444. [CrossRef]
21. Matsui, M. Linear Cryptanalysis Method for DES Cipher. In Proceedings of the Advances in Cryptology—EUROCRYPT'93, Workshop on the Theory And Application of Cryptographic Techniques, Lofthus, Norway, 23–27 May 1993; Volume 765, pp. 386–397. [CrossRef]

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.