Hindawi
IET Information Security
Volume 2023, Article ID 6691726, 12 pages
https://doi.org/10.1049/2023/6691726

Research Article

Differential, Linear, and Meet-in-the-Middle Attacks on the Lightweight Block Cipher RBFK

Sugio Nobuyuki

Hokkaido University of Science, 15-4-1, Maeda 7-jo, Teine-ku, Sapporo-shi, Hokkaido 006-8585, Japan

Correspondence should be addressed to Sugio Nobuyuki; sugio-n@hus.ac.jp

Received 14 June 2023; Revised 27 September 2023; Accepted 14 October 2023; Published 23 November 2023

Academic Editor: Qichun Wang

Randomized butterfly architecture of fast Fourier transform for key cipher (RBFK) is the lightweight block cipher for Internet of things devices in an edge computing environment. Although the authors claimed that RBFK is secure against differential cryptanalysis, linear cryptanalysis, impossible differential attack, and zero correlation linear cryptanalysis, the details were not explained in the literature. Therefore, we have evaluated the security of RBFK by application of differential cryptanalysis, linear cryptanalysis, and meet-in-the-middle (MITM) attack and have found that RBFK is not secure against these attacks. This paper introduces not only a distinguish attack but also key recovery attacks on full-round RBFK. In the distinguish attack scenario, data for differential cryptanalysis are two, and the time complexity is one for an exclusive-OR operation. In the key recovery attack scenario, the data for linear cryptanalysis are one pair of known plaintext–ciphertext. The time complexity is one operation for a linear sum. Data for an MITM attack are two. The time complexity is 2^{48} encryptions; the memory complexity is 2^{45} bytes. Because the vulnerabilities are identified in the round function and the key scheduling part, we propose some improvements for RBFK against these attacks.

1. Introduction

Edge computing is a concept of distributed computing that processes data at a location close to the data source, such as Internet of things (IoT) devices or edge servers. Edge computing provides benefits such as real-time performance and security by processing data quickly on devices or servers and sending only necessary data to the cloud. In this context, it is important to evaluate the security of cryptography on IoT devices in edge computing environments because many IoT devices are used. In fact, IoT devices have limited communication and computing capabilities, making it difficult to apply a conventional cryptographic algorithm such as AES [1] or Camellia [2]. Moreover, in edge computing, IoT devices of various types can mutually collaborate to create new services and values. At the same time, security threats also increase.

In recent years, many lightweight cryptographic algorithms have been proposed for IoT devices. Lightweight cryptography is aimed at providing security for devices with limited resources, such as low power consumption, small circuit size, and low computational complexity. An example of lightweight cryptographic algorithms is Ascon [3], a family of authenticated encryption and hashing algorithms with added countermeasures against side-channel attacks. Ascon has been selected as a new standard for lightweight cryptography in the NIST lightweight cryptography competition [4].

The security of the lightweight block ciphers is evaluated by the application of various cryptanalytic attacks such as differential cryptanalysis [5], linear cryptanalysis [6], meet-in-the-middle (MITM) attack [7], impossible differential attack [8], and zero correlation linear cryptanalysis [9],

Randomized Butterfly architecture of fast Fourier transform for key cipher (RBFK) and was developed by Rana et al. [10]. It is a lightweight block cipher for IoT devices in an edge computing environment. For key generation, RBFK has a randomized butterfly architecture of fast Fourier transform. The block size is 64-bit. The secret key sizes are 64-bit and 128-bit. RBFK has two algorithms, named RBFK-64 and RBFK-128, which adopt a 64-bit (or 128-bit) secret key size. The recommended numbers of rounds for RBFK-64 and RBFK-128 are, respectively, 5 and 5.

Although the authors have claimed that RBFK is secure against differential cryptanalysis, linear cryptanalysis, impossible differential attack, and zero correlation linear cryptanalysis, the

Table 1: Lightweight block cipher components and the results of cryptanalysis.

Algorithm	Block size (bits)	Key size (bits)	Structure	Rounds	Attack rounds/method
BORON [11]	64	80/128	SPN	25	10/DC [31]
CHAM [12]	64/128	128/256	ARX	88/112/120	52/DC [32]
Few [13]	64	80/128	Feistel	32	13/HOD attack [44]
GIFT [14]	64/128	128	SPN	28/40	27/DC [33]
LBC-IoT [15]	32	80	Feistel	32	26/LC [40]
LED [16]	64	64/128	SPN	32	16/DC [34]
Midori [17]	64/128	128	SPN	16/20	12/MITM [42]
Piccolo [18]	64	80/128	GFN	25	7/integral attack [45]
PRESENT [19]	64	80/128	SPN	31	17/related key [47]
PRINCE [20]	64	128	SPN	12	12/reflection attack [49]
QTL [21]	64	64/128	Feistel	16/20	15/DC, 15/LC [35]
RBFK [10]	64	80	GFN	5	5/DC, 5/LC, 5/MITM
RECTANGLE [22]	64	80/128	SPN	25	18/DC [22]
SAT_Jo [23]	64	80	SPN	31	31/integral attack [46]
SCENERY [24]	64	80	Feistel	28	13/DC [36]
SFN [25]	64	96	Hybrid	32	32/related key [48]
SIMON [26]	32/48/64	64/72/96/128	ARX	32/36/42/44/52	16/18/24/24/29/DC [37]
SIMON [26]	96/128	144/192/256	ARX	54/68/69/72	29/40/40/40/DC [37]
SIT [27]	64	64	Hybrid	5	5/DC [38]
SLIM [28]	32	80	Feistel	32	14/DC [36], 19/LC [41]
TWINE [29]	64	80/128	GFN	32	25/MITM [43]
WARP [30]	128	128	GFN	41	24/DC [39]

Note. The abbreviations DC and LC denote differential cryptanalysis and linear cryptanalysis.

relevant details were not explained in the literature. Therefore, the purpose of our research is to evaluate the security of RBFK from a third-party perspective.

1.1. Related Works. Recently, lots of lightweight cryptographic algorithms have been published in academic community such as BORON [11], CHAM [12], Few [13], GIFT [14], LBC-IoT [15], LED [16], Midori [17], Piccolo [18], PRESENT [19], PRINCE [20], QTL [21], RECTANGLE [22], SAT_Jo [23], SCENERY [24], SFN [25], SIMON and SPECK [26], SIT [27], SLIM [28], TWINE [29], and WARP [30]. Table 1 summarizes the lightweight block cipher components and the results of cryptanalysis. The structures of lightweight block cipher are substitution permutation network (SPN), Feistel network, generalized Feistel network (GFN), or addition rotation XOR network (ARX). The cryptographic researchers have evaluated the security of these lightweight block ciphers using various attacks such as differential cryptanalysis [31–39], linear cryptanalysis [40, 41], MITM attack [42, 43], higher-order differential attack [44], integral attack [45, 46], and other attacks [47–49]. Most of these cryptanalytic research focus on how many rounds do they attack on a target cipher. Although there are several research [50–53] that compare among the lightweight block ciphers from the point of block sizes, key sizes, structures, and implementations, they do not recommend how to develop a secure cryptographic algorithm from the point of attacker's view.

In this paper, we not only evaluated the security of lightweight block cipher RBFK but also proposed how to design secure cryptographic algorithms using our results and surveys

Table 2: Comparison of this paper against existing works.

Reference	Cryptanalysis	Survey	Recommendations
[31]	✓		
[32]	✓		
[33]	✓		
[34]	✓		
[35]	✓		
[36]	✓		
[37]	✓		
[38]	✓		
[39]	✓		
[40]	✓		
[41]	✓		
[42]	✓		
[43]	✓		
[44]	✓		
[45]	✓		
[46]	✓		
[47]	✓		
[48]	✓		
[49]	✓		
[50]		✓	
[51]		✓	
[52]		✓	
[53]		✓	✓
Our paper	✓	✓	✓

Note. Zakaia et al. [53] have made some recommendations from the developer's insight from their surveys.

Table 3: Results of attacks on full-round RBFK.

Rounds	Data (pairs)	Time (encryptions)	Memory (bytes)	Methods
Full-round RBFK-n $(n=64, 128)$	2	1		Differential cryptanalysis
Full-round RBFK-n $(n=64, 128)$	1	1		Linear cryptanalysis
Full-round RBFK-64	2	2^{48}	2^{45}	MITM attack
Full-round RBFK-128	3	2^{97}	2^{94}	MITM attack

shown in Table 1. Table 2 provides an explicit comparison of this paper against existing works from different aspects and highlights the aspects in which this paper is novel.

1.2. Our Contributions. The contributions of this paper are presented below:

(1) We reveal some vulnerabilities in the round function and the key scheduling part. The former is that the output of round function can be expressed with a linear form of the input. The latter is that the round keys of RBFK are used only 16-bit (or 32-bit) per round.
(2) We apply differential, linear, and MITM attacks to RBFK-n $(n=64, 128)$ using the above vulnerabilities and show the distinguish attacks and key recovery attacks. The necessary number of chosen plaintext–ciphertext pairs and the time complexity for each attack are presented in Table 3.
(3) We propose some improvements for RBFK-n $(n=64, 128)$ against differential, linear and MITM attacks. We also make recommendations from the point of cryptographic algorithm design.

1.3. Organization of the Paper. The remainder of this paper is organized as explained below. Section 2 explains the preliminary. Section 3 introduces some cryptanalytic methods used for this study. Section 4 explains the algorithms of RBFK-64 and RBFK-128. Section 5 presents the distinguish attack by application of differential cryptanalysis. Section 6 demonstrates the key recovery attacks by application of linear cryptanalysis. Section 7 presents key recovery attacks by application of MITM attack. We discuss some improvements for RBFK in Section 8 and summarize the contents of this paper in Section 9.

2. Preliminary

Table 4 lists notations used for this study.

Table 4: Notations.

$\oplus$	Exclusive-OR operation
$\odot$	Exclusive-NOR operation
$\Vert$	Concatenation
$\cdot$	Inner product of two vectors
P	Plaintext
C	Ciphertext
X^i	ith round input
X^{i+1}	ith round output
K^i	ith round extended key
ΔX^i	ith round input differential
ΔX^{i+1}	ith round output differential
Γ_{X^i}	ith round input mask
$\Gamma_{X^{i+1}}$	ith round output mask
$0x$	This symbol shows a hexadecimal number

3. Methodology

3.1. Differential Cryptanalysis. Differential cryptanalysis has been introduced by Biham and Shamir [5]. It works with a chosen plaintext scenario. Let $\Delta P = P \oplus P^*$ be an exclusive-OR differential with respect to plaintexts pair (P, P^*). The exclusive-OR differential ΔX with respect to inputs $X = P \oplus K$ and $X^* = P^* \oplus K$ is presented below:

$$\Delta X = X \oplus X^* = (P \oplus K) \oplus (P^* \oplus K) = \Delta P. \quad (1)$$

Let ΔX be the input differential, and ΔY be the output differential. The differential probability (DP) of S-box is defined as shown below:

$$DP(\Delta X \to \Delta Y) = \frac{\#\{X | S(X) \oplus S(X \oplus \Delta X) = \Delta Y\}}{2^n}. \quad (2)$$

The expression $\#\{X | S(X) \oplus S(X \oplus \Delta X) = \Delta Y\}$ represents the number of times that the equation $S(X) \oplus S(X \oplus \Delta X) = \Delta Y$ is satisfied when 2^n values of X are inputted to S-box under given ΔX and ΔY. Equation (2) is independent of K, which is inserted into the S-box. When plaintext P is distributed uniformly, the output difference ΔY is expected with probability DP for the input difference ΔP.

3.2. Linear Cryptanalysis. Linear cryptanalysis [6], which was introduced by Matsui, works with a known plaintext scenario. It recovers the secret key using linear correlation between plaintexts and ciphertexts. Let $X = (x_0, x_1, \cdots, x_{n-1})$ be n-bit input for S-box and $Y = (y_0, y_1, \cdots, y_{m-1})$ be m-bit output. Then, the probability of the linear approximation between the input X and output Y is given by the following equation:

$$\frac{\#\{X | \Gamma_X \cdot X = \Gamma_Y \cdot Y\}}{2^n}. \quad (3)$$

The vectors Γ_X and Γ_Y, which choose the bit positions of S-box, are called linear masks, respectively, the input mask

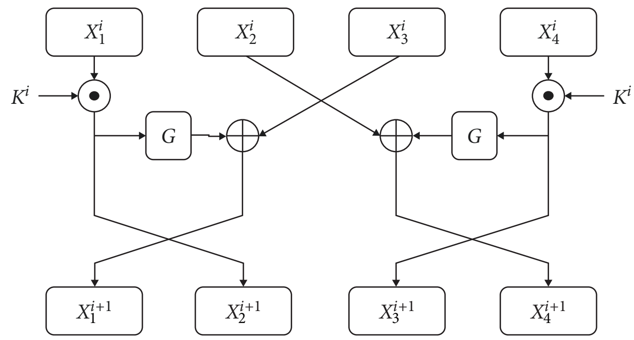

Figure 1: 1-Round encryption of RBFK-64.

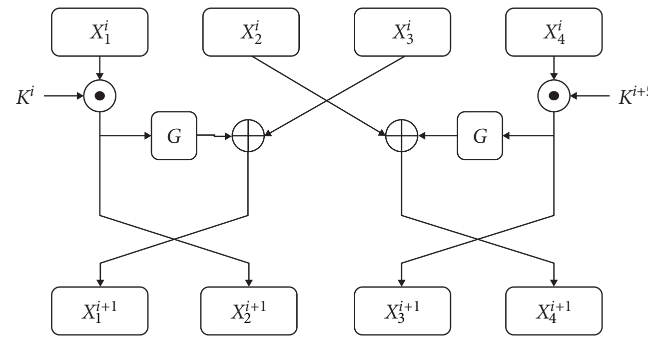

Figure 2: 1-Round encryption of RBFK-128.

and output masks. The expression $\#\{X|\Gamma_X \cdot X = \Gamma_Y \cdot Y\}$ represents the number of times that the equation $\Gamma_X \cdot X = \Gamma_Y \cdot Y$ is satisfied when 2^n values of X are inputted to S-box under given Γ_X and Γ_Y. The linear probability (LP) of the linear mask transitioning from Γ_X to Γ_Y is defined by the following equation:

$$LP(\Gamma_X \rightarrow \Gamma_Y) = \left(2\frac{\#\{X|\Gamma_X \cdot X = \Gamma_Y \cdot Y\}}{2^n} - 1\right)^2. \tag{4}$$

3.3. MITM Attack. The MITM attack [7] was introduced by Diffie and Hellman. It works in a known plaintext scenario. We explain how to launch an MITM attack on the block ciphers.

Let $E(X; K)$ be an encryption function with key $K \in GF(2)^s$. Let $X \in GF(2)^n$ be input and $Y \in GF(2)^m$ be output. Consider an encryption that repeats E twice, as presented below:

$$C = E(E(P; K_1); K_2). \tag{5}$$

Denote the secret key $K = K_1||K_2$ for which the length is $2s$ bits. An MITM attack is a cryptanalytic method for deriving the secret key $K = K_1||K_2$ using the probabilistic coincidence of the intermediate values obtained by partially encrypting a known plaintext P with K_1 and partially decrypting a ciphertext C with K_2.

4. RBFK

RBFK [10] is one of the lightweight block ciphers developed in an edge computing IoT devices. RBFK is a 64-bit block cipher with 64, 128-bit secret keys. RBFK has two variants, named RBFK-64 and RBFK-128, which adopt a 64-bit (or 128-bit) secret key size. The recommended numbers of rounds for RBFK-64 and RBFK-128 are, respectively, 5 and 5.

4.1. Algorithm. The structures of RBFK-64 and RBFK-128 are, respectively, shown in Figures 1 and 2. The difference between RBFK-64 and RBFK-128 is only the extended keys that encrypt with XNOR operations. Also, for both RBFK-64 and RBFK-128, the swap operation of the four blocks is not performed in the final round.

Let X^i and X^{i+1} be 64-bit input and 64-bit output, respectively. Let X_j^i, $(j = 1, 2, 3, 4)$ be a 16-bit sub-block of X^i and the upper sub-block is denoted as X_1^i and the lower sub-block is denoted as X_4^i. Let the most significant bit (MSB) be x_0^i in X_1^i, and the least significant bit be x_{63}^i in X_4^i. Let the ith round extended key be $K^i = (k_0^i, k_1^i, \cdots, k_{15}^i)$.

$$\begin{aligned} X^i &= X_1^i||X_2^i||X_3^i||X_4^i \\ X_1^i &= (x_0^i, x_1^i, \cdots, x_{15}^i) \\ X_2^i &= (x_{16}^i, x_{17}^i, \cdots, x_{31}^i), \\ X_3^i &= (x_{32}^i, x_{33}^i, \cdots, x_{47}^i) \\ X_4^i &= (x_{48}^i, x_{49}^i, \cdots, x_{63}^i) \end{aligned} \tag{6}$$

$$\begin{aligned} X^{i+1} &= X_1^{i+1}||X_2^{i+1}||X_3^{i+1}||X_4^{i+1} \\ X_1^{i+1} &= \left(x_0^{i+1}, x_1^{i+1}, \cdots, x_{15}^{i+1}\right) \\ X_2^{i+1} &= \left(x_{16}^{i+1}, x_{17}^{i+1}, \cdots, x_{31}^{i+1}\right) \\ X_3^{i+1} &= \left(x_{32}^{i+1}, x_{33}^{i+1}, \cdots, x_{47}^{i+1}\right) \\ X_4^{i+1} &= \left(x_{48}^{i+1}, x_{49}^{i+1}, \cdots, x_{63}^{i+1}\right) \end{aligned}. \tag{7}$$

G function is a nonlinear function whose input size is 16-bit. Figure 3 shows the algorithm of the G function.

Figure 4 shows the scan pattern permutation. The values are read from the left (upper) in the first row and from the right (lower) in the second row. The same applies to the third and fourth rows. For example, 16 bits written in binary (1011, 1100, 0010, 0101) become (1011, 0011, 0010, 1010) by the scan pattern permutation.

S-box in the G function is shown in Table 5. The middle four bits of the eight bits are replaced by S-box.

The coin flip operation and the output are calculated as follows:

$$\begin{aligned} B_1 &= B_1 \oplus (0x81) \\ B_2 &= B_2 \oplus (0x81). \\ \text{Output} &= B_1||B_2 \end{aligned} \tag{8}$$

4.2. Key Generation Part. From Figures 1 and 2, the round keys are used 16-bit (or 32-bit) per one round. Because the key generation part is not used in our paper, we omit the

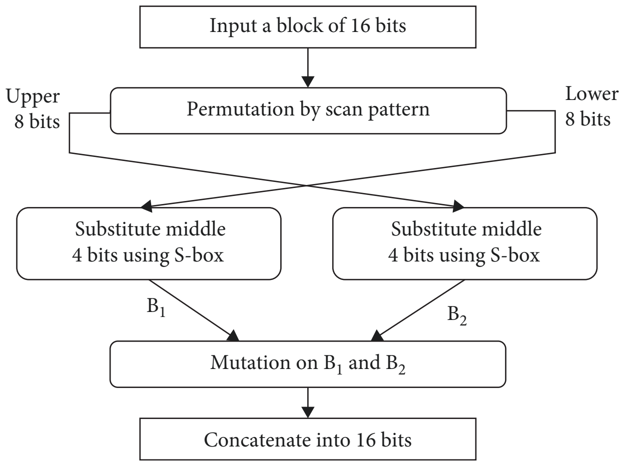

FIGURE 3: *G* function.

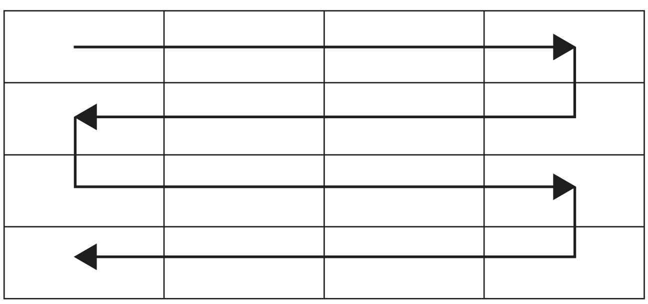

FIGURE 4: Scan pattern with 16 bits input and 16 bits output.

TABLE 5: S-box.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	A	E	D	C	B	F	9	8	7	6	0	4	3	2	1	5

explanation of it. For details, refer to the study of Rana et al. [10].

5. Differential Cryptanalysis of RBFK

5.1. Differential Characteristics of G Function. As shown in Figure 3, each bit of input undergoes one of the following processes:

(i) Scan pattern permutation.
(ii) Scan pattern permutation and the coin flip operation.
(iii) Scan pattern permutation and S-box operation.

Because both the scan pattern permutation and the coin flip operation are linear operations, the corresponding 8-bit output can be expressed with a linear form of the input. By letting $X=(x_0, x_1, \cdots, x_{15})$ be input and by letting $Y=(y_0, y_1, \cdots, y_{15})$ be the output of G function, the following equations hold:

TABLE 6: Example of differential path.

ΔX^0	(0x0000, 0x0000, 0x8000, 0x0000)
ΔX^1	(0x8000, 0x0000, 0x0000, 0x0000)
ΔX^2	(0x0080, 0x8000, 0x0000, 0x0000)
ΔX^3	(0x8000, 0x0080, 0x0000, 0x8000)
ΔX^4	(0x0080, 0x8000, 0x8000, 0x0000)
ΔX^5	(0x0080, 0x0000, 0x8000, 0x0000)

$$\begin{cases} y_0 = x_8 \oplus 1 \\ y_1 = x_9 \\ y_6 = x_{13} \\ y_7 = x_{12} \oplus 1 \\ y_8 = x_0 \oplus 1 \\ y_9 = x_1 \\ y_{14} = x_5 \\ y_{15} = x_4 \oplus 1 \end{cases}. \tag{9}$$

Let $\Delta X_G = (\delta x_0, \delta x_1, \cdots, \delta x_{15})$ be the input difference of the G function and let $\Delta Y_G = (\delta y_0, \delta y_1, \cdots, \delta y_{15})$ be the output difference. In addition, let 1 and 0, respectively, represent the presence and absence of difference in each bit. From Equation (9), the following equations hold with probability 1:

$$\begin{cases} \delta y_0 = \delta x_8 \\ \delta y_1 = \delta x_9 \\ \delta y_6 = \delta x_{13} \\ \delta y_7 = \delta x_{12} \\ \delta y_8 = \delta x_0 \\ \delta y_9 = \delta x_1 \\ \delta y_{14} = \delta x_5 \\ \delta y_{15} = \delta x_4 \end{cases}. \tag{10}$$

There are two S-boxes in the G function. We have evaluated DP of S-box. Letting ΔX_S be the input difference of S-box and letting ΔY_S be the output difference of S-box. The maximum DP, $\mathrm{DP}_{\max}=1$ when $(\Delta X_S, \Delta Y_S) = \{(0x5, 0x5), (0xA, 0xA), (0xF, 0xF)\}$. Because this result means that S-box is not secure against differential cryptanalysis, we propose an improvement for S-box in Section 8.

5.2. Distinguish Attacks on RBFK. Using $\delta y_0 = \delta x_8$, $\delta y_1 = \delta x_9$, $\delta y_8 = \delta x_0$, and $\delta y_9 = \delta x_1$ from Equation (10), an attacker can perform a distinguishing attack on RBFK-64. Let the input differential of the first round be $\Delta P = \Delta X^0 = (\delta x_0^0, \delta x_1^0, \cdots, \delta x_{63}^0)$ and let the output differential of the last round be $\Delta C = \Delta X^5 = (\delta x_0^5, \delta x_1^5, \cdots, \delta x_{63}^5)$. Assume at least 1 bit of the input differential δx_{i+j}^0 $(i=0,1,8,9, j=0,16,32,48)$ are active and the others are nonactive. The total number of input differential patterns is estimated as $2^{16}-1=65535$.

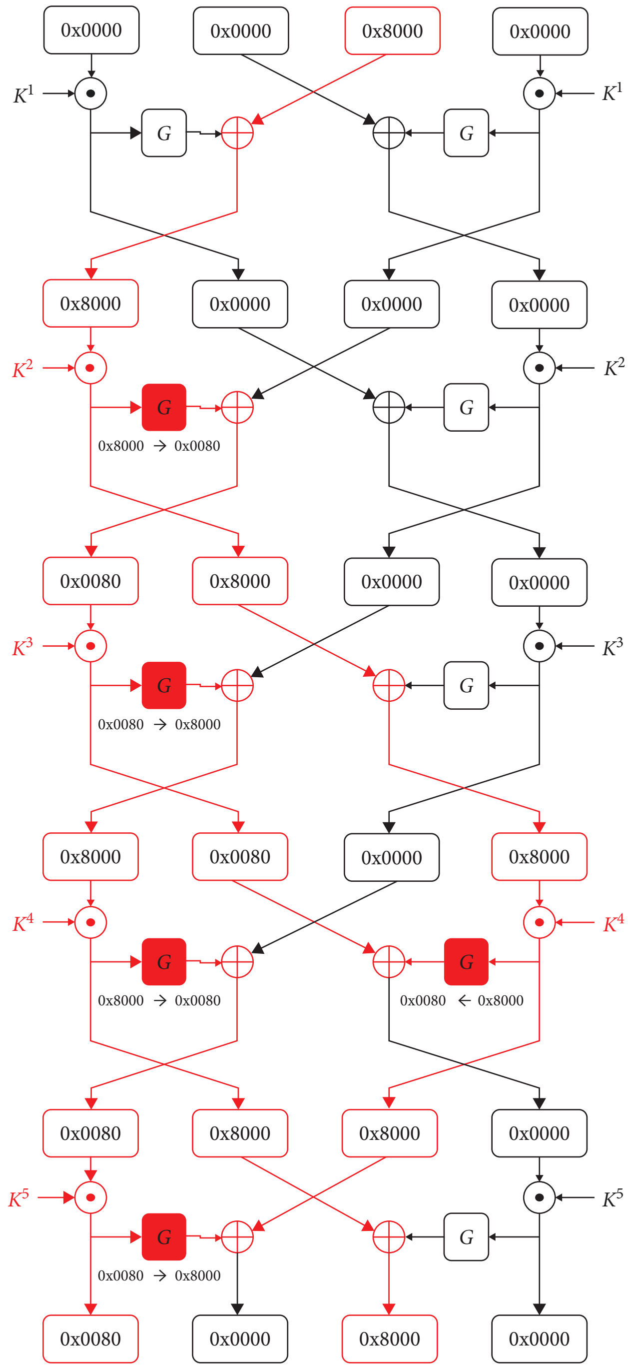

FIGURE 5: Differential path of RBFK-64.

Table 6 presents one of the differential paths. Figure 5 shows the result obtained from applying the differential path in Table 6 to RBFK-64.

The differential path shown in Figure 5 holds with probability 1 and allows an attacker to perform a distinguishing attack on RBFK-64. The number of chosen plaintext–ciphertext pairs is two; the computational complexity is one for exclusive-OR operation.

An attacker can also perform a distinguishing attack on RBFK-64 using differential characteristics of S-box. For example, when the input differential is set $\Delta X^0 = (0x3300, 0x0000, 0x003C, 0x0000)$, the output differential always becomes $\Delta X^5 = ((0x3300, 0x0000, 0x00??, 0x??00))$. The symbol ? denotes unknown. Table 7 presents the differential path using $(\Delta X_S, \Delta Y_S) = (0xF, 0xF)$.

TABLE 7: The differential path using $(\Delta X_S, \Delta Y_S) = (0xF, 0xF)$.

ΔX^0	(0x3300, 0x0000, 0x003C, 0x0000)
ΔX^1	(0x0000, 0x3300, 0x0000, 0x0000)
ΔX^2	(0x0000, 0x0000, 0x0000, 0x3300)
ΔX^3	(0x0000, 0x0000, 0x3300, 0x003C)
ΔX^4	(0x3300, 0x0000, 0x003C, 0x??00)
ΔX^5	(0x3300, 0x0000, 0x00??, 0x??00)

The differential path shown in Table 7 holds with probability 1 and allows an attacker to perform a distinguishing attack on RBFK-64. The number of chosen plaintext–ciphertext pairs is two; the computational complexity is one for exclusive-OR operation.

Because RBFK-128 has the same structure except for the extended round keys used, as shown in Figure 2, an attacker can perform the distinguishing attack on RBFK-128 using differential cryptanalysis in the same way.

6. Linear Cryptanalysis of RBFK

6.1. Linear Characteristics of G Function. As described in Section 5, a part of the output of the G function can be expressed with a linear form of the input. Let $\Gamma_{X_G} = (\gamma x_0, \gamma x_1, \cdots, \gamma x_{15})$ be the input mask of the G function and let $\Gamma_{Y_G} = (\gamma y_0, \gamma y_1, \cdots, \gamma y_{15})$ be the output mask. In addition, let 1 and 0, respectively, represent the presence and absence of a mask in each bit. From Equation (9), the following equations hold with probability 1:

$$\begin{cases} \gamma y_0 = \gamma x_8 \oplus 1 \\ \gamma y_1 = \gamma x_9 \\ \gamma y_6 = \gamma x_{13} \\ \gamma y_7 = \gamma x_{12} \oplus 1 \\ \gamma y_8 = \gamma x_0 \oplus 1 \\ \gamma y_9 = \gamma x_1 \\ \gamma y_{14} = \gamma x_5 \\ \gamma y_{15} = \gamma x_4 \oplus 1 \end{cases}. \tag{11}$$

We also have evaluated the LP of S-box. Letting Γ_{X_S} be the input mask of S-box and letting Γ_{Y_S} be the output difference of S-box. The maximum LP, $LP_{max} = 1$ when $(\Gamma_{X_S}, \Gamma_{Y_S}) = \{(0x2, 0x2), (0x5, 0x5), (0x7, 0x7), (0x8, 0x8), (0xA, 0xA), (0xD, 0xD), (0xF, 0xF)\}$. Because this result means that S-box is not secure against linear cryptanalysis, we propose an improvement for S-box in Section 8.

6.2. Linear Equation of 1-Round RBFK. From Figure 1, the following equations hold for RBFK-64:

$$\begin{cases} X_1^{i+1} = G(X_1^i \odot K^i) \oplus X_3^i \\ X_2^{i+1} = X_1^i \odot K^i \\ X_3^{i+1} = X_4^i \odot K^i \\ X_4^{i+1} = X_2^i \oplus G(X_4^i \odot K^i) \end{cases}. \quad (12)$$

On GF(2), $a \odot b = a \oplus b \oplus 1$. From Equations (9) and (12), the following linear equations hold with probability 1.

$$\begin{cases} x_0^{i+1} = x_8^i \oplus x_{32}^i \oplus k_8^i \\ x_1^{i+1} = x_9^i \oplus x_{33}^i \oplus k_9^i \oplus 1 \\ x_6^{i+1} = x_{13}^i \oplus x_{38}^i \oplus k_{13}^i \oplus 1 \\ x_7^{i+1} = x_{12}^i \oplus x_{39}^i \oplus k_{12}^i \\ x_8^{i+1} = x_0^i \oplus x_{40}^i \oplus k_0^i \\ x_9^{i+1} = x_1^i \oplus x_{41}^i \oplus k_1^i \oplus 1 \\ x_{14}^{i+1} = x_5^i \oplus x_{46}^i \oplus k_5^i \oplus 1 \\ x_{15}^{i+1} = x_4^i \oplus x_{47}^i \oplus k_4^i \end{cases}, \quad (13)$$

$$\begin{cases} x_{48}^{i+1} = x_{16}^i \oplus x_{56}^i \oplus k_8^i \\ x_{49}^{i+1} = x_{17}^i \oplus x_{57}^i \oplus k_9^i \oplus 1 \\ x_{54}^{i+1} = x_{22}^i \oplus x_{61}^i \oplus k_{13}^i \oplus 1 \\ x_{55}^{i+1} = x_{23}^i \oplus x_{60}^i \oplus k_{12}^i \\ x_{56}^{i+1} = x_{24}^i \oplus x_{48}^i \oplus k_0^i \\ x_{57}^{i+1} = x_{25}^i \oplus x_{49}^i \oplus k_1^i \oplus 1 \\ x_{62}^{i+1} = x_{30}^i \oplus x_{53}^i \oplus k_5^i \oplus 1 \\ x_{63}^{i+1} = x_{31}^i \oplus x_{52}^i \oplus k_4^i \end{cases}. \quad (14)$$

In addition, from Figure 2, the following equations hold with probability 1 on RBFK-128.

$$\begin{cases} X_1^{i+1} = G(X_1^i \odot K^i) \oplus X_3^i \\ X_2^{i+1} = X_1^i \odot K^i \\ X_3^{i+1} = X_4^i \odot K^{i+5} \\ X_4^{i+1} = X_2^i \oplus G(X_4^i \odot K^{i+5}) \end{cases}. \quad (15)$$

From Equations (9) and (15), Equations (16) hold with probability 1.

$$\begin{cases} x_{48}^{i+1} = x_{16}^i \oplus x_{56}^i \oplus k_8^{i+5} \\ x_{49}^{i+1} = x_{17}^i \oplus x_{57}^i \oplus k_9^{i+5} \oplus 1 \\ x_{54}^{i+1} = x_{22}^i \oplus x_{61}^i \oplus k_{13}^{i+5} \oplus 1 \\ x_{55}^{i+1} = x_{23}^i \oplus x_{60}^i \oplus k_{12}^{i+5} \\ x_{56}^{i+1} = x_{24}^i \oplus x_{48}^i \oplus k_0^{i+5} \\ x_{57}^{i+1} = x_{25}^i \oplus x_{49}^i \oplus k_1^{i+5} \oplus 1 \\ x_{62}^{i+1} = x_{30}^i \oplus x_{53}^i \oplus k_5^{i+5} \oplus 1 \\ x_{63}^{i+1} = x_{31}^i \oplus x_{52}^i \oplus k_4^{i+5} \end{cases}. \quad (16)$$

Table 8: Propagation of linear masks.

Γ_{X^0}	(0x0000, 0x0000, 0x0080, 0x8000)
Γ_{X^1}	(0x0080, 0x8000, 0x8000, 0x0000)
Γ_{X^2}	(0x8000, 0x0000, 0x0080, 0x8000)
Γ_{X^3}	(0x0080, 0x0000, 0x8000, 0x0000)
Γ_{X^4}	(0x8000, 0x0000, 0x0000, 0x0000)
Γ_{X^5}	(0x8000, 0x0000, 0x0000, 0x0000)

6.3. Key Recovery Attacks on RBFK. An attacker can perform key recovery attacks on RBFK-*n* $(n = 64, 128)$ by application of the linear Equations (12)–(16). Let the input mask of the first round be $\Gamma_{X^0} = (\gamma x_0^0, \gamma x_1^0, \cdots, \gamma x_{63}^0)$ and let the output mask of the last round be $\Gamma_{X^5} = (\gamma x_0^5, \gamma x_1^5, \cdots, \gamma x_{63}^5)$. Assume at least 1 bit of the output mask γx_{i+j}^5 $(i = 0, 1, 8, 9, j = 0, 16, 32, 48)$ are active and the others are nonactive. The total number of output mask patterns is estimated as $2^{16} - 1 = 65535$.

Table 8 shows the propagation of linear masks, particularly addressing the MSB of the ciphertext. Figures 6 and 7, respectively, present the results of application of the linear masks in Table 8 to RBFK-*n* $(n = 64, 128)$.

From Figure 6, an attacker obtains the following linear equation:

$$x_{40}^1 \oplus x_{48}^1 \oplus x_0^6 = k_0^1 \oplus k_8^2 \oplus k_8^4 \oplus k_0^5 \oplus 1. \quad (17)$$

In Equation (17), x_{40}^1 and x_{48}^1 are 2 bits of plaintext; x_0^6 is 1 bit of ciphertext. If an attacker has one pair of known plaintext–ciphertext, then an attacker can uniquely ascertain the linear sum of the extended key of RBFK-64.

Because an attacker can obtain the following linear equation from Figure 7, an attacker can uniquely ascertain the linear sum of the extended key of RBFK-128.

$$x_{40}^1 \oplus x_{48}^1 \oplus x_0^6 = k_8^2 \oplus k_0^3 \oplus k_8^4 \oplus k_0^5 \oplus k_0^6 \oplus k_0^8 \oplus 1. \quad (18)$$

The data for linear cryptanalysis are one pair of known plaintext–ciphertext. The time complexity is one for a linear sum operation.

7. MITM Attacks on RBFK

Because RBFK-64 only uses 16-bit key K^i for each round (32-bit for RBFK-128), an attacker can perform key recovery attacks by the application of an MITM attack. As described in this paper, we do not evaluate the improved techniques of MITM attacks, such as the splice-and-cut technique [54] and the three-subset technique [55], but apply an MITM attack as described in Section 3.

7.1. Application to RBFK-64. Assume that an attacker obtains, in advance, two pairs of known plaintext–ciphertext (P_1, C_1) and (P_2, C_2). The attack procedure is presented below:

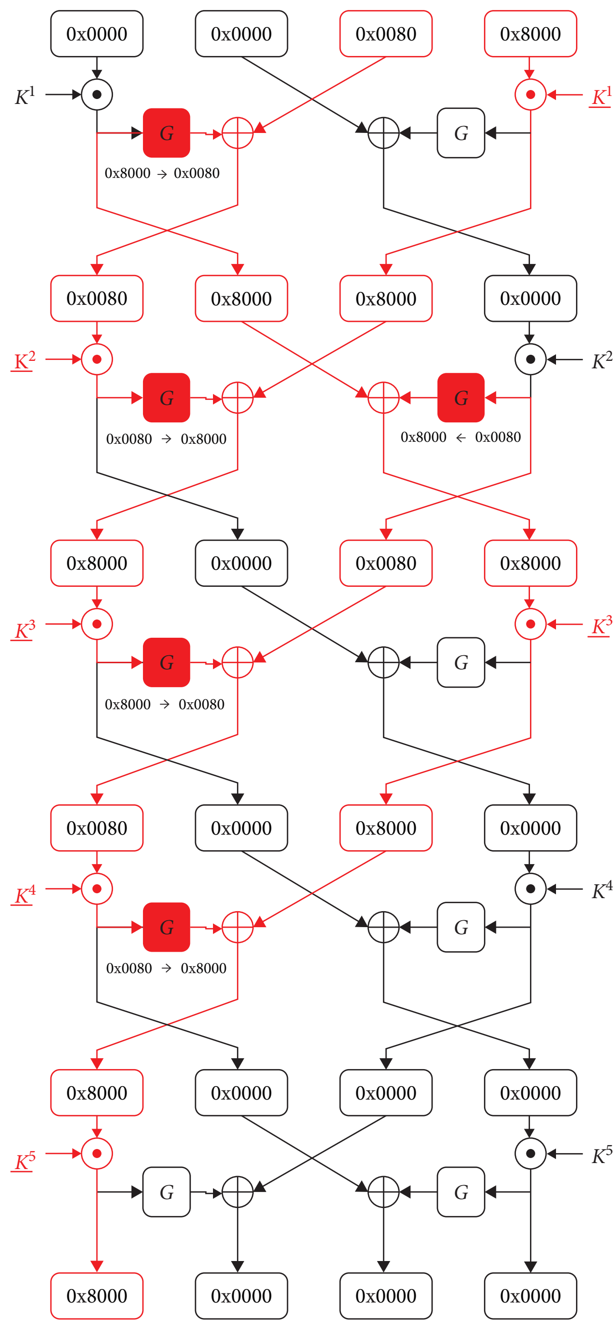

FIGURE 6: Propagation of linear masks on RBFK-64.

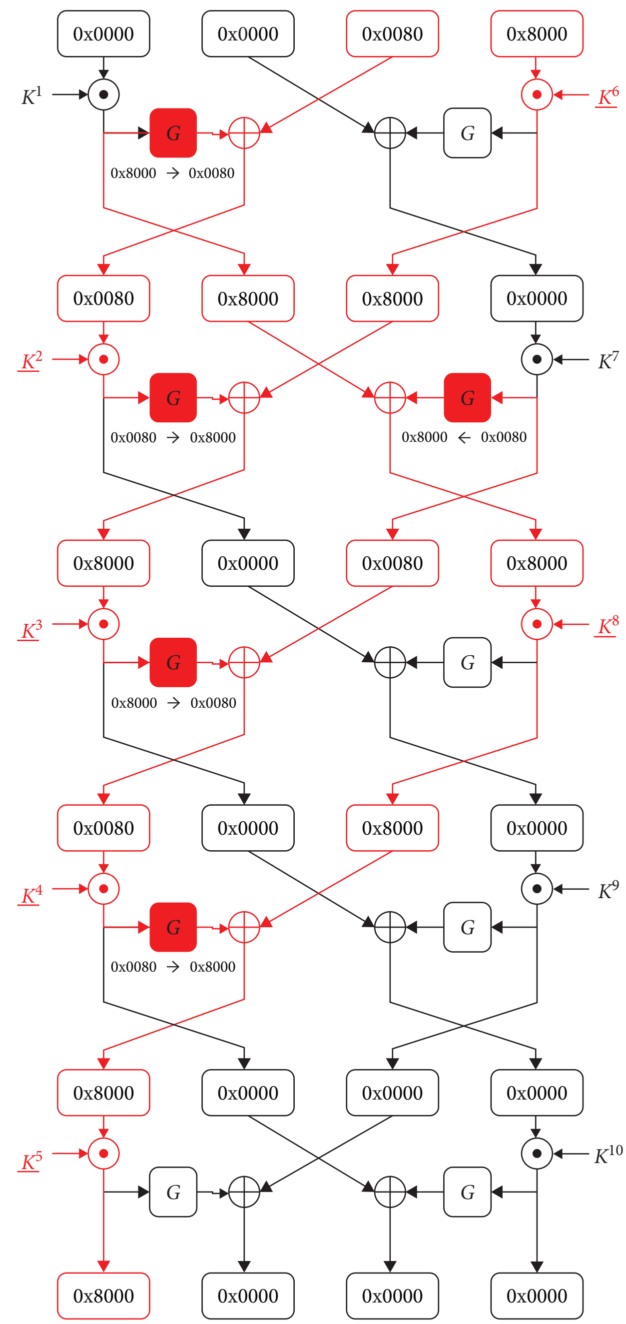

FIGURE 7: Propagation of linear masks on RBFK-128.

(1) Encrypt the plaintext P_1 for all values of round keys $K_f = K^1||K^2||K^3$ and obtain a 64-bit intermediate value Z_{K_f}. In addition, create a table M_1 that stores K_f, whose memory address is Z_{K_f}.

(2) Decrypt ciphertext C_1 for all values of round keys $K_b = K^4||K^5$ and obtain a 64-bit intermediate value Z_{K_b}. In addition, create a table M_2 that stores K_b, for which the memory address is Z_{K_b}.

(3) There are one or more candidates of an extended key in the tables M_1 and M_2, which have the same address (i.e., $Z_{K_f} = Z_{K_b}$). In this case, the number of candidates of the extended key is reduced to $2^{80} \times 2^{-64} = 2^{16}$. Ascertain whether $C_2 = \text{RBFK-64}(P_2; K)$ holds, or not, for each candidate of extended key $K = K_f||K_b$. If the equation holds, then it is the correct key; otherwise, check another candidate.

Because the probability that a false key remains in Step (3) is $2^{16} \times 2^{-64} \ll 1$, it is possible to eliminate all false keys by preparing two pairs of known plaintext–ciphertext. The number of data required for an MITM attack is 2. The computational complexity is $T = 2^{48} + 2^{32} + 2^{16} \approx 2^{48}$ times

Table 9: PRESENT S-box.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

of RBFK-64 encryptions. The memory necessary for two tables is $M = (2^{48} + 2^{32})/8 \approx 2^{45}$ bytes.

Because the secret key size of RBFK-64 is 64, an attacker can recover the 80-bit extended key faster than when using the brute-force search method.

7.2. Application to RBFK-128. Assume that an attacker obtains three pairs of known plaintext–ciphertext (P_1, C_1), (P_2, C_2), and (P_3, C_3) in advance. Also, RBFK-128 might be attacked using an MITM attack in an equivalent manner to that explained in the preceding subsection. However, Steps (1) and (2) are performed using two pairs of known plaintext–ciphertext (P_1, C_1) and (P_2, C_2) to eliminate false keys. The numbers of extended key candidates in Steps (1) and (2) are reduced to $2^{128} \times 2^{-128} = 1$. Because the probability that a false key remains in Step (3) is $1 \times 2^{-64} \ll 1$, it is possible to eliminate all false keys by preparing three known plaintext–ciphertext pairs. Therefore, the number of data is three. The computational complexity is $T = 2 \times (2^{96} + 2^{64}) + 1 \approx 2^{97}$ times of RBFK-128 encryptions. The memory which is necessary for two tables is $M = 2 \times (2^{96} + 2^{64})/8 \approx 2^{94}$ bytes.

8. Discussions

RBFK is vulnerable to differential, linear, and MITM attacks, as demonstrated in the explanation presented above. Using the current RBFK in IoT devices for edge computing might pose a considerable risk of information leakage and other threats. Therefore, we propose some improvements to enhance RBFK security.

8.1. Improvement of S-Box. Because S-box defined in Table 5 is not secure against differential cryptanalysis and linear cryptanalysis, it must be improved. As described in this paper, we propose the replacement of the RBFK S-box with the PRESENT S-box shown in Table 9. By adopting PRESENT S-box, the maximum DP and the maximum LP are both 2^{-2}, which is expected to improve security against differential cryptanalysis and linear cryptanalysis.

8.2. Improvement of the Round Function. Eight bits of the output of the G function are expressed with a linear form of the input. Therefore, we propose an application of the PRESENT S-box, shown in the preceding section, to these 8 bits. Specifically, we replace a part of Figure 3 that says "Replace intermediate 4 bits with S-box" with "Replace intermediate 4 bits and another 4 bits, respectively, with PRESENT S-box." This improvement eliminates the differential paths and linear masks that hold with probability 1, which is expected to improve security against differential cryptanalysis and linear cryptanalysis.

8.3. Improvement of the Number of Rounds. Although the numbers of rounds for RBFK-n $(n = 64, 128)$ are 5 and 5, they are insufficient for the attacks described herein. Therefore, we applied the evaluation method based on the estimation of the minimum number of active S-box using mixed integer linear programing (MILP) proposed by Mouha et al. [56] to RBFK with improved G function. Then, we estimated the number of rounds that are resistant to differential cryptanalysis and to linear cryptanalysis. Because Mouha et al. [56] evaluated the number of active S-box by the application of word-level truncated differential paths and truncated linear masks, we performed the analysis while assuming 1 word = 1 byte. Results are presented in Table 10. From Table 10, it is apparent that more than 34 rounds are secure against differential cryptanalysis and linear cryptanalysis (i.e., $2^{-2 \times N_A} < 2^{-64}$). This result is based on truncated differential paths and truncated linear masks, which represent the presence or absence of differential or linear masks at the byte level. It does not reflect consideration of whether differential paths or linear masks exist.

Table 10: Number of active S-box (N_A).

Rounds	N_A (truncated differential path)	N_A (truncated linear mask)
5	4	4
10	9	9
15	14	14
20	19	19
25	24	24
30	30	30
33	32	32
34	33	33
35	34	34
40	39	39
45	44	44
50	49	49

8.4. Improvement of the Key Generation Part. RBFK uses only a 16-bit (or 32-bit) extended key in each round, which renders an MITM attack possible. Although we assume that the round keys of RBFK are all independent. We do not use the key generation part in this paper; we propose the addition of 64 bits of key whitening processing at two places: on the plaintext side and on the ciphertext side. Key whitening processing is adopted for work reported by Camellia [2]. It is expected to improve resistance to an MITM attack by increasing the number of extended keys to be estimated.

8.5. Recommendations from the Point of Cryptographic Algorithms Design. We make recommendations for the design of cryptographic algorithms by Schneier [57] and Shimizu et al. [58] and the point of attacker's view summarized in Table 1. We hope that the following recommendations will contribute to the secure design of cryptography.

8.5.1. S-Box and Round Function. The nonlinear function S-box is a critical component for the symmetric-key block ciphers. It is important for the designers to make S-box secure against differential cryptanalysis [5], linear cryptanalysis [6], higher-order differential attack [59, 60], integral attack [61–63], and the division property [64–67]. Therefore, the designers should make DP_{max} and LP_{max} low and should make the algebraic degree of S-box large. For example, the S-box of AES [1] is well-designed against these cryptanalyses.

The round functions are composed of S-box and permutation layer. The permutation layers are designed with bit-wise [19], nibble-wise [30], and byte-wise [1, 2]. The designer should make the permutation layers as diffusive as possible.

8.5.2. Number of Rounds. The number of rounds should be set to larger necessary to ensure security as long as the computational cost, speed, gate size, etc., are within an acceptable range.

Recently, the cryptographic evaluation tools have been proposed. Mouha et al. [56] proposed the MILP-based tool, which can evaluate the number of active S-box by the application of word-level truncated differential paths and truncated linear masks. Sun et al. [68] improved the tool proposed by Mouha et al. [56] by applying bit-based differential characteristics. Sasaki et al. [69] introduced the impossible differential search tool from design and cryptanalysis aspects. The designer should use these tools to determine the necessary number of rounds on the original cipher.

8.5.3. Key Generation Part. The key generation part is used to generate round keys from the secret key. A lot of key generation parts have been proposed. We introduce some key generation parts. The key generation part of KASUMI [70] is only composed of linear functions such as shift rotations and XOR with constants. The key generation part of MISTY [71] uses the FI-function, which is a part of the round function. The key generation parts of AES [1] and Camellia [2] use round functions. The designer should make the key generation part secure against MITM attack [7] and related-key attack [72] as long as the designer manages tradeoffs [73].

9. Conclusion

As described in this paper, we have demonstrated that differential cryptanalysis, linear cryptanalysis, and MITM attacks are applicable to RBFK-64 and RBFK-128. We have also proposed some improvement methods for the *G* function and key generation part as countermeasures against these attacks.

Although the lightweight cryptography must be implemented on devices with scarce computing resources, such as IoT devices for edge computing, it is necessary to provide security against typical cryptographic attacks.

Data Availability

The experimentally obtained data and source codes used to support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Authors' Contributions

The author wrote the entire manuscript text, tables, and figures.

References

[1] NIST, *Advanced Encryption Standard (AES)*, Vol. 197, National Institute of Standards and Technology (NIST), FIPS Publication, 2001.

[2] K. Aoki, T. Ichikawa, M. Kanda et al., *Specification of Camellia a 128-Bit Block Cipher*, Springer, Berlin, 2001.

[3] C. Dobraug, M. Eichlseder, F. Mendel, and M. Schlaffer, "Ascon: lightweight authenticated encryption & hashing," 2021, https://ascon.iaik.tugraz.at/index.html.

[4] NIST, "Lightweight cryptography standardization process: NIST selects ascon," 2023, https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon.

[5] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer, New York, 1993.

[6] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, EUROCRYPT '93*, vol. 765 of *LNCS*, pp. 386–397, 1993.

[7] W. Diffie and M. E. Hellman, "Exhaustive cryptanalysis of the NBS data encryption standard," *Journals of the Computer*, vol. 10, pp. 74–84, 1977.

[8] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials," in *Proceedings of the Advances in Cryptology, EUROCRYPT'99*, vol. 1592 of *LNCS*, pp. 12–23, 1999.

[9] A. Bogdanov and V. Rijmen, "Zero Correlation Linear Cryptanalysis of Block Ciphers," International Association for Cryptologic Research (IACR), Cryptology ePrint Archive Report 2011/123, 2011.

[10] S. Rana, M. R. H. Mondal, and J. Kamruzzaman, "RBFK cipher: a randomized butterfly architecture-based lightweight block cipher for IoT devices in the edge computing environment," *Journal of the Cybersecurity*, vol. 6, no. 1, 2023.

[11] G. Bansod, N. Pisharoty, and A. Patil, "BORON: an ultra-lightweight and low power encryption design for pervasive computing," *Journal of Frontiers of Information Technology & Electronic Engineering*, vol. 18, no. 3, pp. 317–331, 2017.

[12] B. Koo, D. Roh, H. Kim, Y. Jung, D. Lee, and D. Kwon, "CHAM: a family of lightweight block ciphers for resource-constrained devices," in *Proceedings of the International Conference on Information Security and Cryptology, ICISC 2017*, vol. 10779 of *LNCS*, pp. 3–25, 2017.

[13] M. Kumar, S. K. Pal, and A. Panigrahi, "FeW: a lightweight block cipher," IACR Cryptology ePrint Archive, Report 2014/326, 2014.

[14] S. Banik, S. Kumar Pandey, T. Peyrin, Y. Sasaki, S. Meng Sim, and Y. Todo, "GIFT: a small present, towards reaching the limit of lightweight encryption," in *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems, CHES 2017*, vol. 10529 of *LNCS*, pp. 321–345, 2017.

[15] R. A. Ramadan, B. W. Aboshosha, K. Yadav, I. M. Alseadoon, M. J. Kashout, and M. Elhoseny, "LBC-IoT: lightweight block cipher for IoT constraint devices," *Journal of Computers, Materials & Continua*, vol. 67, no. 3, pp. 3563–3579, 2021, 2021.

[16] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED block cipher," in *Proceedings of the International Workshop on*

Cryptographic Hardware and Embedded Systems, CHES 2011, vol. 6917 of *LNCS*, pp. 326–341, 2011.
[17] S. Banik, A. Bogdanov, T. Isobe et al., "Midori: a block cipher for low energy," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2015*, vol. 9453 of *LNCS*, pp. 411–436, 2015.
[18] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "Piccolo: an ultra-lightweight blockcipher," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2011*, vol. 6917 of *LNCS*, pp. 342–357, 2011.
[19] A. Bogdanov, L. R. Knudsen, G. Leander et al., "PRESENT: an ultra-lightweight block cipher," in *Proceeding of the CHES*, vol. 4727 of *LNCS*, pp. 450–466, 2007.
[20] J. Borghoff, A. Canteaut, T. Güneysu et al., "A low-latency block cipher for pervasive computing applications," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT*, vol. 7658 of *LNCS*, pp. 208–225, 2012.
[21] L. Li, B. Liu, and H. Wang, "QTL: a new ultra-lightweight block cipher," *Microprocessors and Microsystems*, vol. 45, pp. 45–55, 2016.
[22] W. T. Zhang, Z. Z. Bao, D. D. Lin, V. Rijmen, B. H. Yang, and I. Verbauwhede, "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms," *Science China Information Sciences*, vol. 58, no. 12, pp. 1–15, 2015.
[23] M. J. R. Shantha and L. Arockiam, "SAT_Jo: an enhanced lightweight block cipher for the internet of things," in *Proceedings of the 2018 Second International Conference on Intelligent Computing and Control Systems, ICICCS*, pp. 1146–1150, 2018.
[24] J. Feng and L. Li, "SCENERY: a lightweight block cipher based on Feistel structure," *Frontiers of Computer Science*, vol. 16, Article ID 163813, 2022.
[25] L. Li, B. Liu, Y. Zhou, and Y. Zou, "SFN: a new lightweight block cipher," *Microprocessors and Microsystems*, vol. 60, pp. 138–150, 2018.
[26] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," in *Proceedings of the Annual Design Automation Conference*, pp. 1–6, IEEE, 2015.
[27] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, "SIT: a lightweight encryption algorithm for secure internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 1, 2017.
[28] B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed, and M. M. Dessouky, "SLIM a lightweight block cipher for internet of health things," *Journal of IEEE Access*, vol. 8, pp. 203747–203757, 2020.
[29] T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, "TWINE: a lightweight block cipher for multiple platforms," in *Proceedings of the International Conference on Selected Areas in Cryptography, SAC 2012*, vol. 7707 of *LNCS*, pp. 339–354, 2012.
[30] S. Banik, Z. Bao, T. Isobe et al., "Revisiting GFN for lightweight 128-bit block cipher," in *Proceedings of the International Conference on Selected Areas in Cryptography, SAC 2020*, vol. 12804 of *LNCS*, pp. 535–564, 2020.
[31] J. S. Teh, L. J. Tham, N. Jamil, and W.-S. Yap, "New differential cryptanalysis results for the lightweight block cipher BORON," *Journal of Information Security and Applications*, vol. 66, Article ID 103129, 2022.
[32] A. Biryukov, J. S. Teh, and A. Udovenko, "Advancing the meet-in-the-filter technique applications to CHAM and KATAN," IACR Cryptology ePrint Archive, Report 2023/851, 2023.
[33] R. Zong, X. Dong, H. Chen, Y. Luo, S. Wang, and Z. Li, "Towards key-recovery-attack friendly distinguishers: application to GIFT-128," *IACR Transactions on Symmetric Cryptology*, vol. 2021, no. 1, pp. 156–184, 2021.
[34] F. Mendel, V. Rijmen, D. Toz, and K. Varıcı, "Differential analysis of the LED block cipher," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2012*, vol. 7658 of *LNCS*, pp. 190–207, 2012.
[35] S. Sadeghi, N. Bagheri, and M. A. Abdelraheem, "Cryptanalysis of reduced QTL block cipher," *Microprocessors and Microsystems*, vol. 52, pp. 34–48, 2017.
[36] Y. Y. Chan, C.-Y. Khor, B. T. Khoo, J. S. Teh, W. J. Teng, and N. Jamil, "On the resistance of new lightweight block ciphers against differential cryptanalysis," *Heliyon*, vol. 9, no. 4, Article ID e15257, 2023.
[37] H. AlKhzaimi and M. M. Lauridsen, "Cryptanalysis of the SIMON family of block ciphers," IACR Cryptology ePrint Archive, Report 2013/543, 2013.
[38] R. Nishiyama, Y. Igarashi, and T. Kaneko, "Differential cryptanalysis of block cipher SIT," in *Proceedings of the 2020 Symposium on Cryptography and Information Security*, pp. 2B1–2B3, 2020.
[39] J. S. Teh and A. Biryukov, "Differential cryptanalysis of WARP," *Journal of Information Security and Applications*, vol. 70, Article ID 103316, 2022.
[40] S. Yasushi and Y. Igarashi, "MILP-based linear attack on lightweight block cipher LBC-IoT," in *2022 Symposium on Cryptography and Information Security, SCIS2022, 1F2-1*, 2022.
[41] N. Sugio, "Linear cryptanalysis of the lightweight block cipher SLIM," in *Proceedings of the IPSJ SIG Technical Report, vol.2023-CSEC-102*, pp. 1–8, 2023.
[42] L. Lin and W. Wu, "Meet-in-the-middle attacks on reduced-round midori-64," IACR Cryptology ePrint Archive, Report 2015/1165, 2015.
[43] Ö. Boztas, F. Karakoç, and M. çoban, "Multidimensional meet-in-the-middle attacks on reduced-round TWINE-128," in *Proceedings of the Second International Workshop Lightweight Cryptography for Security and Privacy*, vol. 8162 of *LNCS*, pp. 55–67, 2013.
[44] N. Shibayama, Y. Igarashi, and T. Kaneko, "Higher order differential property of few," pp. 37–42, 2017, IEICE Technical Report, IT2017-7.
[45] S. Utsumi, K. Sakamoto, and T. Isobe, "Bit-level evaluation of piccolo block cipher by satisfiability problem solver," *Journal of IET Information Security*, vol. 17, no. 4, pp. 616–625, 2023.
[46] X. Qiu, Y. Wei, S. Hodzic, and E. Pasalic, "Integral distinguishers of the full-round lightweight block cipher SAT_Jo," *Journal of Security and Communication Networks*, vol. 2021, Article ID 5310545, 2021.
[47] O. Özen, K. Varıcı, C. Tezcan, and Kocair ç., "Lightweight block ciphers revisited: cryptanalysis of reduced round PRESENT and HIGHT," in *Proceedings of the Australasian Conference on Information Security and Privacy, ACISP 2009*, vol. 5594 of *LNCS*, pp. 90–107, 2009.
[48] S. Sadeghi and N. Bagheri, "Cryptanalysis of SFN block cipher," IACR Cryptology ePrint Archive, Report 2018/594, 2018.

[49] H. Soleimany, C. Blondeau, X. Yu et al., "Reflection cryptanalysis of PRINCE-like ciphers," *Journal of Cryptology*, vol. 28, no. 3, pp. 718–744, 2015.

[50] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *Journal of Cryptographic Engineering*, vol. 8, no. 2, pp. 141–184, 2018.

[51] A. B. Dara, M. J. Lonea, and N. Hussainb, "Revisiting lightweight block ciphers: review, taxonomy and future directions," IACR Cryptology ePrint Archive, Report 2021/476, 2021.

[52] A. Sevin and A. A. O. Mohammed, "A survey on software implementation of lightweight block ciphers for IoT devices," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 3, pp. 1801–1815, 2023.

[53] A. A. Zakaria, A. H. Azni, F. Ridzuan, N. H. Zakaria, and M. Daud, "Systematic literature review: trend analysis on the design of lightweight block cipher," *Journal of King Saud University—Computer and Information Sciences*, vol. 35, no. 5, Article ID 101550, 2023.

[54] K. Aoki and Y. Sasaki, "Meet-in-the-middle attack against reduced SHA-0 and SHA-1," in *Proceeding of the 29th International Cryptology Conference, CRYPTO 2009*, vol. 5677 of *LNCS*, pp. 70–89, 2009.

[55] A. Bogdanov and C. Rechberger, "A 3-subset meet-in-the-middle attack: cryptanalysis of the lightweight block cipher KTANTAN," in *Proceedings of the 17th International Workshop, SAC 2010*, vol. 6544 of *LNCS*, pp. 229–240, 2010.

[56] N. Mouha, Q. Wang, D. Gu, and B. Preneel, "Differential and linear cryptanalysis using mixed-integer linear programming," in *Proceeding of the International Conference on Information Security and Cryptology, Inscrypt 2011*, vol. 7537 of *LNCS*, pp. 57–76, 2011.

[57] B. Schneier, *Applied Cryptography, Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, 1996.

[58] H. Shimizu, H. Seki, Y. Kaneko, H. Miyano, and T. Kaneko, "On the block cipher guidebook," IPSJ SIG Technical Report, computer security group, 2000.

[59] X. Lai, "Higher order derivatives and differential cryptanalysis," in *Proceedings of the Communications and Cryptography*, pp. 227–233, 1994.

[60] N. Sugio, H. Aono, S. Hongo, and T. Kaneko, "A study on higher order differential attack of KASUMI," *Transactions of the IEICE on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E90-A, no. 1, pp. 14–21, 2007.

[61] J. Daemen, L. Knudsen, and V. Rijmen, "The block cipher square," in *Proceedings of the 4th International Workshop on Fast Software Encryption, FSE '97*, vol. 1267 of *LNCS*, pp. 149–165, 1997.

[62] L. R. Knudsen and D. Wagner, "Integral cryptanalysis," in *Proceedings of Fast Software Encryption, FSE 2002*, vol. 2365 of *LNCS*, pp. 112–127, 2002.

[63] N. Sugio, Y. Igarashi, and S. Hongo, "Integral cryptanalysis of reduced-round KASUMI," *Transactions of the IEICE on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E105.A, no. 9, pp. 1309–1316, 2022.

[64] Y. Todo, "Structural evaluation by generalized integral property," in *Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2015*, vol. 9056, part1 of *LNCS*, pp. 287–314, 2015.

[65] Y. Todo and M. Morii, "Bit-based division property and application to Simon family," in *Proceedings of the 23rd International Conference on Fast Software Encryption, FSE 2016*, vol. 9783 of *LNCS*, pp. 357–377, 2016.

[66] Z. Xiang, W. Zhang, Z. Bao, and D. Lin, "Applying MILP Method to searching integral distinguishers based on division property for 6 lightweight block ciphers," in *Proceedings of the 22nd International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT2016*, vol. 10031 of *LNCS*, pp. 648–678, 2016.

[67] K. Hu, S. Sun, M. Wang, and Q. Wang, "An algebraic formulation of the division property: revisiting degree evaluations, cube attacks, and key-independent sums," in *Proceedings of the 26th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2020*, vol. 12491 of *LNCS*, pp. 446–476, 2020.

[68] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, "Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers," in *Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2014, LNCS*, vol. 8873, pp. 158–178, 2014.

[69] Y. Sasaki and Y. Todo, "Impossible differential search tool from design and cryptanalysis aspects," in *Proceeding of the 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2017*, vol. 10212 of *LNCS*, pp. 185–215, 2017.

[70] GPP, "Specification of the 3GPP confidentiality and integrity algorithms; document 2: Kasumi specification," TS 35.202, 2017.

[71] M. Matsui, "New block encryption algorithm MISTY," in *Proceedings the 4th International Workshop on Fast Software Encryption (FSE '97)*, vol. 1267 of *LNCS*, pp. 54–67, Haifa, Israel, January 1997.

[72] E. Biham, "New types of cryptanalytic attacks using related keys," *Journal of Cryptology*, vol. 7, no. 4, pp. 229–246, 1994.

[73] A. Y. Poschmann, "LIGHTWEIGHT CRYPTOGRAPHY cryptographic engineering for a pervasive world," IACR ePrint Archive, Report 2009/516, 2009.