Research Article

Improved Impossible Differentials and Zero-Correlation Linear Hulls of New Structure III

Jun He ¹, Xuan Shen ¹, and Guoqiang Liu^{2,3}

¹College of Information and Communication, National University of Defense Technology, Wuhan 430010, China

²College of Liberal Arts and Sciences, National University of Defense Technology, Changsha 410073, China

³State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Correspondence should be addressed to Xuan Shen; shenxuan_08@163.com

Received 30 May 2021; Revised 27 August 2021; Accepted 25 September 2021; Published 6 October 2021

Academic Editor: Majid Khan

Copyright © 2021 Jun He et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Impossible differential cryptanalysis and zero-correlation linear cryptanalysis are two kinds of most effective tools for evaluating the security of block ciphers. In those attacks, the core step is to construct a distinguisher as long as possible. In this paper, we focus on the security of New Structure III, which is a kind of block cipher structure with excellent resistance against differential and linear attacks. While the best previous result can only exploit one-round linear layer P to construct impossible differential and zero-correlation linear distinguishers, we try to exploit more rounds to find longer distinguishers. Combining the Miss-in-the-Middle strategy and the characteristic matrix method proposed at EUROCRYPT 2016, we could construct 23-round impossible differentials and zero-correlation linear hulls when the linear layer P satisfies some restricted conditions. To our knowledge, both of them are 1 round longer than the best previous works concerning the two cryptanalytical methods. Furthermore, to show the effectiveness of our distinguishers, the linear layer of the round function is specified to the permutation matrix of block cipher SKINNY which was proposed at CRYPTO 2016. Our results indicate that New Structure III has weaker resistance against impossible differential and zero-correlation linear attacks, though it possesses good differential and linear properties.

1. Introduction

Block cipher structures are regarded as the backbones of block ciphers. When designing a new block cipher, the first step is to choose a proper structure. From the implementation aspect, the structures will significantly influence the implementation cost and latency of the block cipher. From the security part, the structures will affect the diffusion and interaction among different components and give guidance of the parameters of block cipher such as the number of iterated rounds accordingly. Therefore, cryptanalysis of block cipher structures also deserves much attention [1–4].

So far, one of the most popular block cipher structures is the Feistel structure. It divides the input into two halves and updates one half every time. Since decryption of Feistel structures does not involve the inverse of round functions, the

encryption and decryption enjoy similar structure and components, making its design more flexible, versatile, and economical. Its randomness [5] and resistance against Meet-in-the-Middle [6], yoyo [7], and quantum [8] attacks were widely considered. In [9], generalized Feistel structure (GFS) was proposed. While GFS preserves the advantages of Feistel structures, its branch size and round functions are lighter and more portable. GFS is further extended and classified into Type-II GFS, unbalanced GFS, and so on. As shown in Figure 1, Type-II GFS updates one half of branches and follows by a branch-wise circular shift, while unbalanced GFS uses a contracting or expanding round functions. Examples of those GFSs are CLEFIA [10], HIGHT [11], SMS4 [2], MARS [3], GMiMC [12], etc. Those schemes possess relatively high diffusion while keeping portable round function design.

The security of GFS has undergone careful evaluation. After its publication, the diffusion and security regarding

FIGURE 1: 4-branch Type-II GFS (a), 4-branch contracting unbalanced GFS (b), and 4-branch expanding unbalanced GFS (c).

differential and linear attacks of Type-II GFS were evaluated by counting the number of active S-boxes. At SAC 2010, the lower bound of active S-boxes with SP type round functions was evaluated [13]. Then, similar studies with respect to SPS and SPSP type round functions were performed [14, 15]. The impossible differential cryptanalysis and zero-correlation linear and integral cryptanalysis have also been taken into consideration. Based on the Miss-in-the-Middle strategy, Kim et al. [16] analyzed the impossible differential property using a matrix-based method. Yang et al. [17] and Zhang and Wu [18] proposed a search method for zero-correlation linear and integral distinguishers, respectively. At FSE 2015, Blondeau and Minier [19] noticed the links among the three analytical methods for Type-II GFS and performed systematic key recovery attacks. In addition, the security against Meet-in-the-Middle attack [20], known key attack [21], and quantum attack [22] has also been evaluated.

With the improvement of generic analytical techniques, some new variants of GFS are proposed. At ACISP 2009, Choy et al. combined the generalized unbalanced Feistel networks with the MISTY structure and named it GF-NLFSR [23]. GF-NLFSR possess better security in the sense of differential and linear probability bounds. In 2011, Wu and Wang [24] put forward a unified method to assess the lower bounds of the minimal number of differential active S-boxes for block cipher structures. With this method, they presented 4 new structures, namely, New Structure I/II/III/IV. Among them, New Structure III features better properties against differential and linear attacks than other well-known structures like Type-I/II GFS, Skipjack structures, GF-NLFSR, and so on.

Apart from the resistance against differential and linear cryptanalysis, the security evaluation of New Structure family mainly concentrates on the impossible differential and zero-correlation linear attacks. In [25], Cui and Jin constructed the first impossible differentials for New Structure family. They showed that there exist 15/∞/19/16-round impossible differentials for New Structure I/II/III/IV, respectively. Recently, in 2018, Fu et al. [26] further extended the results by exploiting the information of the round function. They constructed 16/∞/22/16-round impossible differentials by considering the SP type round functions. Moreover, 16/∞/22/16-round zero-correlation linear distinguishers were also built by similar methods. Compared with the above results, the impossible differentials of New Structure III were significantly improved.

Inspired by the characteristic matrix method used at EUROCRYPT 2016 [27], we also study the security against impossible differential and zero-correlation linear attacks of New Structures III with SP type round functions in this paper. The distinguishers are constructed in two steps. We first derive the differential and linear propagation patterns. Then, contradictions are detected by adding some constraints to the linear layer of the round function. Taking advantage of the characteristic matrix method, more information of some rounds of linear layer P can be exploited instead of only one round. Therefore, more rounds of impossible differentials and zero-correlation linear hulls will be constructed. In this paper, we improve the best previous results of New Structure III by 1 round. Those results are summarized in Table 1.

The rest of this paper is organized as follows. In Section 2, some notations and concepts will be introduced. Impossible differentials and zero-correlation linear hulls of New Structure III will be constructed in Sections 3 and 4, respectively. Section 5 concludes this paper.

2. Preliminary

In this section, we will introduce the impossible differentials and zero-correlation linear hulls. Then, detailed description of New Structure III will be depicted. Before that, we will first introduce some notations that will be used throughout this paper.

2.1. Notations. The state of the round function is regarded as a d -dimensional column vector v , and its i -th element is denoted as v_i . The transpose of v is denoted as v^T . Moreover, e_i denotes the d -dimensional unit vector whose i -th element is nonzero and others are zero. Similarly, for a $d \times d$ matrix M , the element in row i and column j is defined as $M_{i,j}$. M^{-1} and M^T are the inverse and transpose operations of M , respectively.

In [27], a characteristic matrix method is proposed to evaluate the impossible differentials and zero-correlation linear hulls of SPN ciphers. The definition of a characteristic matrix is given below.

Definition 1 (characteristic matrix) (see [27]). Let P be a linear mapping, and it can be expressed as a $d \times d$ matrix; the characteristic matrix of $P = (p_{i,j})_{d \times d}$ is defined as $P^* = (p_{i,j}^*)_{d \times d}$, where

TABLE 1: Distinguishers of New Structure III.

Distinguisher types	Distinguisher rounds	References
Impossible differentials	19	[25]
Impossible differentials	22	[26]
Impossible differentials	23	Section 3
Zero-correlation linear hulls	22	[26]
Zero-correlation linear hulls	23	Section 4

$$p_{i,j}^* = \begin{cases} 0, & p_{i,j} = 0, \\ 1, & p_{i,j} \neq 0. \end{cases} \quad (1)$$

The characteristic matrix is used to express the dependency between the input and output. For a characteristic matrix M , when $M_{i,j} = 0$, it means the i -th element of the output is independent of the j -th element of the input. Otherwise, $M_{i,j} = 1$. Based on this characteristic matrix method, the round function of SPN ciphers could be reflected as matrix multiplication. Denote M^t as the t -th power of M , and the multiplication of matrix is defined as

$$(M \times M)_{i,j} = (M_{i,1} \cdot M_{1,j}) \mid (M_{i,2} \cdot M_{2,j}) \mid \dots \mid (M_{i,d} \cdot M_{d,j}), \quad (2)$$

where “ $\mid$ ” is the bitwise OR operation. Given that the nonlinear bijective function S [28] does not change the differential/mask pattern, if there exists one zero element in row i and column j of M^t , it means that the i -th element of the output is independent of the j -th element of the input for t -round SPN ciphers. In addition, if M works on a column vector v , it is also defined as

$$(M \times v)_i = (M_{i,1} \cdot v_1) \mid (M_{i,2} \cdot v_2) \mid \dots \mid (M_{i,d} \cdot v_d). \quad (3)$$

2.2. Impossible Differentials. The impossible differential attack is a variant of differential attack, and it was proposed by Knudsen [29] and Biham et al. [30] independently. Different from differential attack which uses differential with high probability, impossible differential attack exploits differentials which occur with probability 0 instead. For an n -bit block cipher E_k with input difference α and output difference β , its differential probability is defined as the percentage of right inputs:

$$\Pr(\alpha \longrightarrow \beta) = 2^{-n} \# \{X \mid E_k(X) \oplus E_k(X \oplus \alpha) = \beta\}. \quad (4)$$

If the above probability equals zero, i.e.,

$$\Pr(\alpha \longrightarrow \beta) = 0, \quad (5)$$

the differential from α to β is regarded to be impossible.

At FSE 1999, Biham et al. [31] systematically introduced the Miss-in-the-Middle approach which is still the most commonly used strategy in searching for impossible differentials so far. It propagates the input difference of some rounds from the encryption direction with probability 1 and some rounds for the output difference from the decryption direction similarly. Then, the intermediate state is tested whether there is a contradiction. If detected, then an impossible differential is found.

2.3. Zero-Correlation Linear Hulls. The zero-correlation linear attack is a novel extension of linear cryptanalysis. It was first formalized by Bogdanov et al. in 2011 [32]. The zero-correlation linear attack utilizes linear hull whose correlation is zero. For a block cipher E_k , its linear approximation $p(\alpha, \beta)$ is defined as the percentage of inputs X that satisfy $\alpha \cdot X = \beta \cdot E_k(X)$, i.e.,

$$p(\alpha, \beta) = 2^{-n} \# \{X \mid \alpha \cdot X = \beta \cdot E_k(X)\}, \quad (6)$$

where “ $\cdot$ ” means the inner product and α, β are the input mask and output mask, respectively. Then, the correlation of linear hull (α, β) is defined as

$$c(\alpha, \beta) = 2p(\alpha, \beta) - 1. \quad (7)$$

Linear cryptanalysis employs linear hulls with high correlation, while zero-correlation linear cryptanalysis uses that with correlation $c(\alpha, \beta) = 0$.

Similar to the impossible differentials, the Miss-in-the-Middle approach could also be applied to the construction of zero-correlation linear hulls. The procedure is similar. The input mask propagates some rounds forward and the output mask propagates some rounds backward with probability 1. Then, the correlation of this linear hull is zero once the intermediate states are checked for the contradiction.

2.4. The New Structure Series of Block Cipher Structures. The New Structure series of block cipher structures were proposed by Wu et al. in 2011. They provided a generalized approach using integer programming to estimate the lower bound of the minimal active S-boxes for various structures. With this approach in hand, they are able to search for new structures with good immune against differential and linear attacks. The New Structure series were designed in this way. They could provide 22 active S-boxes with 25/22/21/24 rounds.

The New Structure families are specified to be 4 branches, and only one-round function is employed in a single round. The diffusion and confusion are achieved by different combination of XOR, branch-wise circular shift, and nonlinear part. The schematic diagram is shown in Figure 2.

For New Structure III, its leftmost branch is first nonlinearly transformed by the round function F . Then, the nonlinearly transformed state is XORed to its right branch. Finally, the branches are left circular shifted by 1. Assume that the input and output are (x_0, x_1, x_2, x_3) and (y_0, y_1, y_2, y_3) , respectively; then, one-round transformation of New Structure III is

$$(y_0, y_1, y_2, y_3) = (x_1 \oplus F(x_0), x_2, x_3, F(x_0)). \quad (8)$$

For GFS and its extension, the round functions are flexible, versatile, and not necessarily bijective. However, round functions adopting Substitution-Permutation (SP) type structures are preferable. Since SP structure features better diffusion property and well-understood security, many block ciphers employing GFS use SP type round

FIGURE 2: New Structures I, II, III, and IV.

functions such as SMS4 [2], CLEFIA [10], and so on. The SP type round function consists of nonlinear layer S and linear layer P , where S is made up of d parallel s -bit S-boxes and P could be expressed as a $d \times d$ matrix operating on sd bits with word length s . It should be pointed out that both of the nonlinear layer S and linear layer P in this paper are bijective.

To describe the differential/mask propagation through the linear layer, the proposition is shown below.

Proposition 1 (see [33]). *Let P be a linear bijective layer; then,*

- (i) *For any input-output difference $\Delta_{in} \rightarrow \Delta_{out}$, if the differential probability is nonzero, we always have $\Delta_{out} = P\Delta_{in}$.*
- (ii) *For any input-output mask $\Lambda_{in} \rightarrow \Lambda_{out}$, if the correlation is nonzero, we always have $\Lambda_{out} = (P^{-1})^T \Lambda_{in}$.*

3. Impossible Differentials of New Structure III

In this section, we first give one-round differential propagation and then construct 23-round impossible differential distinguishers of New Structure III by the Miss-in-the-Middle method if the linear layer P satisfies some extra conditions. To describe the differential properties better, we first give some notations. $\Delta F(a)$ represents all possible output differences of the nonlinear function F when the input difference is a . Similarly, $\Delta F^r(a)$ represents all possible output differences of the continuous r -round F when the input difference is a , and $\Delta F^{-r}(a)$ represents all possible output differences of the continuous r -round F^{-1} (inverse of F) when the input difference is a .

To construct impossible differentials, one-round differential propagation should be presented firstly. The property is given below.

Proposition 2 (see [25, 26]). *For one-round encryption of New Structure III, let (a_0, a_1, a_2, a_3) and (b_0, b_1, b_2, b_3) be the input and output difference, respectively, and we have*

$$\begin{cases} b_0 = \Delta F(a_0) \oplus a_1, \\ b_1 = a_2, \\ b_2 = a_3, \\ b_3 = \Delta F(a_0). \end{cases} \quad (9)$$

FIGURE 3: One-round differential propagation of New Structure III.

One-round differential propagation is given in Figure 3, and we will study how to construct longer impossible differentials. The following theorem shows the impossible differential distinguisher.

Theorem 1. *For New Structure III with SP type round functions, if there exist i, j such that $(P^*)^4_{i,j} = 0$ and $P^{-1}_{i,i} = 0$, the following 23-round differential is impossible:*

$$(0, \alpha, 0, 0) \rightarrow (\beta, 0, 0, \beta), \quad (10)$$

where $\alpha = e_j$, $\beta = Pe_i$, and P^* denotes the characteristic matrix of the linear layer P .

Proof. The 23-round differential propagation of New Structure III is depicted in Figure 4. It consists of 13-round encryption and 10-round decryption, whose last round is marked by red color and blue color, respectively. The details of differential propagation are given in Table 2, where ? denotes the unknown difference.

From the encryption direction, the input difference $(0, \alpha, 0, 0)$ propagates 13 rounds and the middle difference becomes $(?, \alpha_4, ?, ?)$, where $\alpha_4 = \Delta F^4(\alpha)$. From the decryption direction, the output difference $(\beta, 0, 0, \beta)$ is decrypted by 10 rounds to $(?, \beta_1 \oplus \beta_2, ?, ?)$, where $\beta_1 = \Delta F^{-1}(\beta)$ and $\beta_2 = \Delta F^{-2}(\beta)$. If the middle differences could match each other, there must be

$$\alpha_4 = \beta_1 \oplus \beta_2. \quad (11)$$

It indicates that

$$\Delta F^4(\alpha) = \Delta F^{-1}(\beta) \oplus \Delta F^{-2}(\beta). \quad (12)$$

Considering the fact that the round functions are SP type,

FIGURE 4: 23-round impossible differentials of New Structure III.

TABLE 2: 23-round differential propagation of New Structure III.

Rounds	0	A	0	0	Conditions
1	0	0	α	0	
2	0	0	0	α	
3	α	0	0	0	
4	0	α_1	α_1	0	$\alpha_1 = \Delta F(\alpha)$
5	0	0	α_1	α_1	
6	α_1	0	0	α_1	
7	?	?	α_2	0	$\alpha_2 = \Delta F^2(\alpha)$
8	0	?	?	α_2	
9	α_2	0	?	?	
10	?	?	α_3	?	$\alpha_3 = \Delta F^3(\alpha)$
11	?	?	?	α_3	
12	α_3	?	?	?	
13	?	α_4	?	?	$\alpha_4 = \Delta F^4(\alpha)$
13	?	$\beta_1 \oplus \beta_2$	?	?	
14	?	β_1	β_2	?	
15	?	β_1	0	β_2	
16	β_2	β_1	0	0	$\beta_2 = \Delta F^{-2}(\beta)$
17	0	β_1	0	0	
18	0	0	β_1	0	
19	0	0	0	β_1	
20	β_1	0	0	0	$\beta_1 = \Delta F^{-1}(\beta)$
21	0	β	β	0	
22	0	0	β	β	
23	β	0	0	β	

$$\Delta P S P S P S P S(\alpha) = \Delta S^{-1} P^{-1}(\beta) \oplus \Delta S^{-1} P^{-1} S^{-1} P^{-1}(\beta). \quad (13)$$

For the left part of equation (13), according to the characteristic matrix method, the condition $(P^*)^4_{i,j} = 0$ indicates that the i -th element of the output $\Delta P S P S P S P S(\alpha)$ is

not influenced by the j -th element of α . Furthermore, if $\alpha = e_j$ which means only the j -th element of α is nonzero, the i -th element of $\Delta P S P S P S P S(\alpha)$ is zero.

For the right part of equation (13), when $\beta = P e_i$, it becomes

$$\begin{aligned} \Delta S^{-1} P^{-1}(\beta) \oplus \Delta S^{-1} P^{-1}(\beta) &= \Delta S^{-1} P^{-1}(P e_i) \oplus \Delta S^{-1} P^{-1} S^{-1} P^{-1}(P e_i) \\ &= \Delta S^{-1}(e_i) \oplus \Delta S^{-1} P^{-1} S^{-1}(e_i). \end{aligned} \quad (14)$$

Given that the nonlinear bijective S^{-1} does not change the difference pattern, it means that $\Delta S^{-1}(e_i) = e_i$. So, $\Delta S^{-1}(e_i) \oplus \Delta S^{-1} P^{-1} S^{-1}(e_i) = e_i \oplus \Delta S^{-1} P^{-1}(e_i)$. Moreover, when $P^{-1}_{i,i} = 0$, the i -th element of $P^{-1}(e_i)$ is zero. Furthermore, the i -th element of $\Delta S^{-1} P^{-1}(e_i)$ and $e_i \oplus \Delta S^{-1} P^{-1}(e_i)$ is zero and nonzero, respectively.

For the two parts of equation (13), the i -th element of the left and the right is zero and nonzero, respectively. Thus,

equation (13) cannot be established when the restricted conditions of P are satisfied. Therefore, the 23-round impossible differential is constructed.

To achieve the above 23-round impossible differentials, some extra limits of the linear layer P need to be satisfied according to Theorem 1. In fact, they can be achieved. For example, the permutation layer of block cipher SKINNY which was designed at CRYPTO 2016 [34] is

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{16 \times 16} \quad (15)$$

By calculating the characteristic matrix, $(P^*)^4$ and P^{-1} are presented below. For P^{-1} , every i ($0 \leq i \leq 15$) satisfies $P^{-1}_{i,i} = 0$. Therefore, those (i, j) pairs that make $P^{-1}_{i,j} = 0$ will satisfy the condition in Theorem 1. There are 64 possible (i, j) pairs in total.

$$(P^*)^4 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \quad (16)$$

FIGURE 5: One-round linear propagation of New Structure III.

$$P^{-1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (17)$$

□

4. Zero-Correlation Linear Hulls of New Structure III

In this section, we first give one-round linear propagation and then construct 23-round zero-correlation linear hulls of New Structure III similarly by constructing impossible differentials. To describe the linear properties better, we first give some notations. $\Delta F(a)$ represents all possible output masks of the nonlinear function F when the input mask is a . Similarly, $\Delta F^r(a)$ represents all possible output masks of the continuous r -round F when the input mask is a , and $\Delta F^r(a)$ represents all possible output masks of the continuous r -round F^{-1} (inverse of F) when the input mask is a .

To construct zero-correlation linear hulls, one-round linear propagation should be presented firstly. The property is given below.

Proposition 3 (see [26]). *For one round of New Structure III, let (a_0, a_1, a_2, a_3) and (b_0, b_1, b_2, b_3) be the input mask and output mask, respectively, and we have*

$$\begin{cases} b_0 = a_1, \\ b_1 = a_2, \\ b_2 = a_3, \\ b_3 = \Delta F(a_0) \oplus a_1. \end{cases} \quad (18)$$

The above proposition can be easily proved with the linear propagation rules referred to [26]. One-round linear

FIGURE 6: 23-round zero-correlation linear hulls of New Structure III.

propagation is shown in Figure 5, and we will study how to construct longer zero-correlation linear hulls. The following theorem shows the zero-correlation linear hulls.

Theorem 2. *For New Structure III with SP type round functions, if there exist i, j such that $((P^*)^4)^T_{i,j} = 0$ and $(P^{-1})^T_{i,i} = 0$, the following 23-round linear hulls are zero-correlation linear hulls:*

$$(0, 0, \alpha, 0) \rightarrow (\beta, \beta, \beta, \beta), \quad (19)$$

where $\alpha = e_p$, $\beta = (P^{-1})^T e_p$, and P^* denotes the characteristic matrix of the linear layer P .

Proof. The 23-round linear propagation of New Structure III is depicted in Figure 6. It consists of 10-round encryption and 13-round decryption, whose last round is marked by red color and blue color, respectively. The details of the linear propagation are given in Table 3, where ? denotes the unknown mask.

From the encryption direction, the input mask $(0, 0, \alpha, 0)$ will propagate to $(\alpha_1 \oplus \alpha_2, ?, ?, ?)$ after 10 rounds with probability 1, where $\alpha_1 = \Lambda F(\alpha)$ and $\alpha_2 = \Lambda F^2(\alpha)$. From the decryption direction, the output mask $(\beta, \beta, \beta, \beta)$ is decrypted to $(\beta_4, ?, ?, ?)$ after 13 rounds with probability 1, where $\beta_4 = \Lambda F^{-4}(\beta)$. If the intermediate masks could match each other, there must be

$$\alpha_1 \oplus \alpha_2 = \beta_4. \quad (20)$$

It indicates that

$$\Lambda F(\alpha) \oplus \Lambda F^2(\alpha) = \Lambda F^{-4}(\beta). \quad (21)$$

Considering the fact that the round functions are SP type, the above equation becomes

$$\Lambda P S(\alpha) \oplus \Lambda P S P S(\alpha) = \Lambda S^{-1} P^{-1} S^{-1} P^{-1} S^{-1} P^{-1}(\beta). \quad (22)$$

Furthermore, equation (22) can also become the following equation:

$$P(\Lambda S(\alpha) \oplus \Lambda S P S(\alpha)) = \Lambda S^{-1} P^{-1} S^{-1} P^{-1} S^{-1} P^{-1}(\beta). \quad (23)$$

Given that P is linear bijective, equation (23) becomes

$$\Lambda S(\alpha) \oplus \Lambda S P S(\alpha) = \Lambda P^{-1} S^{-1} P^{-1} S^{-1} P^{-1} S^{-1} P^{-1}(\beta). \quad (24)$$

Note that the nonlinear bijective S does not change the mask pattern. Thus, for the left part of equation (24), if $\alpha = e_p$, $\Lambda S(\alpha) \oplus \Lambda S P S(\alpha) = \Lambda S(e_p) \oplus \Lambda S P S(e_p) = e_p \oplus \Lambda S P(e_p)$. When $(P^{-1})^T_{i,i} = 0$, the i -th element of $\Lambda S P(e_p)$ and $e_p \oplus \Lambda S P(e_p)$ is zero and nonzero, respectively. Thus, it can be obtained that the i -th element of the left part for equation (24) is nonzero.

For the right part of equation (24), according to Proposition 1, when the mask $\beta = (P^{-1})^T e_p$, the mask will be e_j through P^{-1} . Furthermore, we have

$$\Lambda P^{-1} S^{-1} P^{-1} S^{-1} P^{-1} S^{-1} P^{-1}(\beta) = \Lambda P^{-1} S^{-1} P^{-1} S^{-1} P^{-1} S^{-1}(e_j). \quad (25)$$

Since $((P^*)^4)^T_{i,j} = 0$, according to the definition of the characteristic matrix and Proposition 1, the i -th element of $\Lambda P^{-1} S^{-1} P^{-1} S^{-1} P^{-1} S^{-1}(e_j)$ is zero.

TABLE 3: 23-round linear propagation of New Structure III.

Rounds	0	0	α	0	Conditions
1	0	0	0	α	
2	α	0	0	0	
3	0	α_1	0	0	$\alpha_1 = \Lambda F(\alpha)$
4	0	α_1	α_1	0	
5	0	α_1	α_1	α_1	
6	α_1	α_1	α_1	α_1	
7	?	$\alpha_1 \oplus \alpha_2$	?	?	$\alpha_2 = \Lambda F^2(\alpha)$
8	?	?	$\alpha_1 \oplus \alpha_2$	?	
9	?	?	?	$\alpha_1 \oplus \alpha_2$	
10	$\alpha_1 \oplus \alpha_2$	?	?	?	
10	β_4	?	?	?	$\beta_4 = \Lambda F^{-4}(\beta)$
11	?	0	β_3	?	
12	?	?	0	β_3	
13	β_3	?	?	0	$\beta_3 = \Lambda F^{-3}(\beta)$
14	0	0	β_2	?	
15	?	0	0	β_2	
16	β_2	?	0	0	$\beta_2 = \Lambda F^{-2}(\beta)$
17	0	0	β_1	0	
18	0	0	0	β_1	
19	β_1	0	0	0	$\beta_1 = \Lambda F^{-1}(\beta)$
20	0	β	0	0	
21	0	β	β	0	
22	0	β	β	β	
23	β	β	β	β	

Therefore, for the two parts of equation (24), the i -th element of the left and the right is zero and nonzero, respectively. So, equation (24) cannot be established when the restricted conditions of P are satisfied. Therefore, the 23-round zero-correlation linear hulls are constructed.

To achieve the above 23-round zero-correlation linear hulls, some extra limits of the linear layer P need to be satisfied according to Theorem 2. Note that they can be achieved as well. For example, for the permutation layer of block cipher SKINNY which is described in Section 3, $(P^*)^4$ and P^{-1} are presented in equations (16) and (17), respectively. Also, they can easily satisfy the conditions in Theorem 2. $\square$

5. Conclusions

In this paper, we improved impossible differentials and zero-correlation linear hulls of New Structure III to 23 rounds. Both of them are 1 round longer than the best previous works. Firstly, through careful analysis of its differential and linear propagation rules, the intermediate states were derived after some rounds of encryption and decryption. Then, a contradiction was detected by exploiting the details of the permutation layer which should satisfy some constraints. To show the effectiveness of our constructions, P is specified to the permutation matrix of block cipher SKINNY and 64 distinguishers are detected. From the point of the length of distinguishers, our results indicate that New Structure III has weaker resistance against impossible differential and zero-correlation linear attacks than other GFSs such as SMS4 and MARS-like structures whose length of constructed distinguishers was only 12 rounds so far. Although a block cipher structure or concrete cipher may be designed to possess

optimal resistance against one attack, it might be vulnerable to other cryptanalysis techniques since different attack methods start from differential perspective of view. Therefore, dedicated and comprehensive efforts will be necessary.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This study was funded by the National Natural Science Foundation of China (nos. 62002370, 61772545, and 61702537), Scientific Research Plan of National University of Defense Technology (no. ZK21-36), and State Key Laboratory of Information Security (2020-MS-02).

References

- [1] H. Wang, W. Ma, L. Liao, Y. Li, and L. Zheng, "Impossible differential distinguishers of two generalized feistel structures," *Security and Communication Networks*, vol. 2020, no. 1, 9 pages, Article ID 8828504, 2020.
- [2] L. Cheng, B. Sun, and C. Li, "Revised cryptanalysis for SMS4," *Science China Information Sciences*, vol. 60, no. 12, Article ID 122101, 2017.
- [3] L. Cheng and C. Li, "Revisiting impossible differentials of MARS-like structures," *IET Information Security*, vol. 11, no. 5, pp. 273–276, 2017.
- [4] A. H. , H. M. Ismail, M. I. Waseem, S. S. Jamal, and M. Khan, "Quantum spin half algebra and generalized megrelshvili protocol for confidentiality of digital images," *International Journal of Theoretical Physics*, vol. 60, pp. 1720–1741, 2021.
- [5] J. Patarin, "Security of random feistel schemes with 5 or more rounds," *Advances in Cryptology - CRYPTO 2004, LNCS*, Springer, vol. 3152, pp. 106–122, Berlin, Germany, 2004.
- [6] I. Dinur, O. Dunkelman, N. Keller, and A. Shamir, "New attacks on feistel structures with improved memory complexities," *Lecture Notes in Computer Science*, Springer, Berlin, Germany, pp. 433–454, 2015.
- [7] A. Biryukov, G. Leurent, and L. Perrin, "Cryptanalysis of feistel networks with secret round functions," *Selected Areas in Cryptography-SAC 2015*, pp. 102–121, Springer, Berlin, Germany, 2015.
- [8] X. Dong and X. Wang, "Quantum key-recovery attack on Feistel structures," *Science China Information Sciences*, vol. 61, no. 10, Article ID 102501, 2018.
- [9] K. Nyberg, "Generalized feistel networks," *Lecture Notes in Computer Science*, Springer, Berlin, Germany, pp. 91–104, 1996.
- [10] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher CLEFIA (extended abstract)," *Fast Software Encryption*, Springer, Berlin, Germany, pp. 181–195, 2007.
- [11] D. Hong, J. Sung, S. Hong et al., "HIGHT: a new block cipher suitable for low-resource device," *Lecture Notes in Computer Science*, Springer, Berlin, Germany, pp. 46–59, 2006.
- [12] M. R. Albrecht, L. Grassi, L. Perrin et al., "Feistel structures for MPC, and more," *Lecture Notes in Computer Science*, Springer, Berlin, Germany, pp. 151–171, 2019.
- [13] K. Shibutani, "On the diffusion of generalized feistel structures regarding differential and linear cryptanalysis," *Selected Areas in Cryptography-SAC 2010*, pp. 211–228, Springer, Berlin, Germany, 2011.
- [14] A. Bogdanov and K. Shibutani, "Generalized Feistel networks revisited," *Designs, Codes and Cryptography* 66, Springer, no. 1-3, pp. 75–97, Berlin, Germany, 2013.
- [15] A. Bogdanov and K. Shibutani, "Double SP-functions: enhanced generalized feistel networks," in *Information Security and Privacy, acisp 2011, lncs 6812*, U. Paramalli and P. Hawkes, Eds., Springer, Berlin, Germany, pp. 106–119, 2011.
- [16] J. Kim, S. Hong, and J. Lim, "Impossible differential cryptanalysis using matrix method," *Discrete Mathematics*, vol. 310, no. 5, pp. 988–1002, 2010.
- [17] D. Yang, W.-F. Qi, and H.-J. Chen, "Provable security against impossible differential and zero correlation linear cryptanalysis of some feistel structures," *Designs, Codes and Cryptography*, vol. 87, no. 11, pp. 2683–2700, 2019.
- [18] H. Zhang and W. Wu, "Structural evaluation for generalized feistel structures and applications to LBlock and TWINE," *Progress in Cryptology -- INDOCRYPT 2015*, Springer, Berlin, Germany, pp. 218–237, 2015.
- [19] C. Blondeau and M. Minier, "Analysis of impossible, integral and zero-correlation attacks on type-II generalized feistel networks using the matrix method," *Fast Software Encryption*, pp. 92–113, Springer, Berlin, Germany, 2015.
- [20] L. Lin, W. Wu, and Y. Zheng, "Improved meet-in-the-middle distinguisher on feistel schemes," in *Selected Areas In Cryptography - SAC 2015*, O. Dunkelman and L. Keliher, Eds., pp. 122–142, Springer, Lecture Notes in Computer Science, Berlin, Germany, 2016.
- [21] L. Dong, Y. Wang, W. Wu, and J. Zou, "Known-key distinguishers on 15-round 4-branch type-2 generalised Feistel networks with single substitution-permutation functions and near-collision attacks on its hashing modes," *IET Information Security*, vol. 9, no. 5, pp. 277–283, 2015.
- [22] X. Dong, Z. Li, and X. Wang, "Quantum cryptanalysis on some generalized Feistel schemes," *Science China Information Sciences*, vol. 62, no. 2, Article ID 22501, 2019.
- [23] J. Choy, G. Chew, K. Khoo, and H. Yap, "Cryptographic properties and application of a generalized unbalanced feistel network structure," *Information Security and Privacy*, vol. 5594, pp. 73–89, 2009.
- [24] S. Wu and M. Wang, "Security Evaluation against Differential Cryptanalysis for Block Cipher Structures," 2011, <http://eprint.iacr.org/2011/551>.
- [25] T. Cui and C. Jin, "Impossible differential evaluations for new-structure series," *Chinese Journal of Electronics*, vol. 23, no. 2, pp. 357–360, 2014.
- [26] L. Fu, T. Cui, and C. Jin, "Zero correlation linear approximations and impossible differentials of new-structure series with SP networks," *Acta Electronica Sinica*, vol. 45, no. 6, pp. 1367–1374, 2017.
- [27] B. Sun, M. Liu, J. Guo, V. Rijmen, and R. Li, "Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis," *Advances in Cryptology - EUROCRYPT 2016*, Springer, Berlin, Germany, pp. 196–213, 2016.
- [28] M. Khan, A. H. Ismail, I. Ishaque, and H. Iqtadar, "New combination of simple additive and entropy weighting criteria

- for the selection of best substitution box,” *Journal of Intelligent and Fuzzy Systems*, vol. 3, pp. 1–14, 2021.
- [29] L. Knudsen, “DEAL - A 128-bit Block Cipher,” *Technical report*, University of Bergen, Bergen, Norway, 1998.
- [30] E. Biham, A. Biryukov, and A. Shamir, “Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials,” in *Advances In Cryptology — EUROCRYPT 1999*, J. Stern, Ed., Springer, Berlin, Germany, pp. 12–23, 1999.
- [31] E. Biham, A. Biryukov, and A. Shamir, “Miss in the middle attacks on IDEA and khufu,” in *Fast Software Encryption-FSE 1999*, L. Knudsen, Ed., Springer, Berlin, Germany, pp. 124–138, 1999.
- [32] A. Bogdanov and V. Rijmen, “Linear hulls with correlation zero and linear cryptanalysis of block ciphers,” *Designs, Codes and Cryptography*, vol. 70, no. 3, pp. 369–383, 2014.
- [33] B. Sun, M. Liu, J. Guo, L. Qu, and V. Rijmen, “New insights on AES-like SPN ciphers,” *Advances in Cryptology - CRYPTO 2016*, Springer, Berlin, Germany, pp. 605–624, 2016.
- [34] C. Beierle, J. Jean, S. Kölbl et al., “The SKINNY family of block ciphers and its low-latency variant MANTIS,” *Advances in Cryptology - CRYPTO 2016*, Springer, Berlin, Germany, pp. 123–153, 2016.