New Wine Old Bottles: Feistel Structure Revised

Jiajie Liu, Bing Sun, Guoqiang Liu, Xinfeng Dong, Li Liu, Hua Zhang and Chao Li

***Abstract*—This paper mainly investigates the iterative structures whose decryption is similar to the encryption. Firstly, we unify many well-known structures which share similar procedures between the decryption and the encryption, and give a sufficient and necessary condition for this structure to be bijective, which reveals many new insights into the Feistel structure as well as the Lai-Massey structure. Secondly, we analyze the security of the unified structure against the known cryptanalysis. By extending the dual structure from a Feistel structure to the unified structure, we prove that a differential of the unified structure is impossible if and only if it is a zero-correlation linear hull of its dual structure, which presents a generalized link between the impossible differential and zero-correlation linear cryptanalysis shown in CRYPTO 2015. Significantly, several constraints on the linear components of the cipher and the permutation on the branches of the cipher are specified to make the structure resilient to differential and linear cryptanalysis. Furthermore, in the case that the order of the permutation equals the number of the branches n, we prove that there always exist a $(3n-1)$-round impossible differential and a $(3n-1)$-round zero-correlation linear hull of the structure, and also present an algorithm to construct these distinguishers. Finally, we propose some novel structures which might be used in future block cipher designs.**

***Index Terms*—Feistel structure, Lai-Massey structure, impossible differential, dual structure, zero-correlation linear hull.**

Jiajie Liu, Bing Sun, Guoqiang Liu and Chao Li are with the Science College, National University of Defense Technology, Changsha, 410073, China. Bing Sun is also with the State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China, and Hunan Engineering Research Center of Commercial Cryptography Theory and Technology Innovation, Changsha, 410073, China (e-mail: l.jiajie@yahoo.com, happy_come@163.com, liuguoqiang87@hotmail.com and lichao_nudt@sina.com).

Xinfeng Dong is with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China (e-mail: xinfengdong@163.com).

Li Liu is with the Laboratory for big data and decision, the College of System Engineering, National University of Defense Technology, Changsha, 410073, China, and is also with the Center for Machine Vision and Signal analysis, University of Oulu, Oulu, 014031, Finland (email: dreamliu2010@gmail.com).

Hua Zhang is with State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 10093, China (e-mail: zhanghua@iie.ac.cn).

This work was supported by the National Natural Science Foundation of China under Grant 62272470, 62002370 and 62172427. (Corresponding author: Bing Sun.)

Manuscript received October 31, 2021; revised March 16, 2022.

1. Introduction

BLOCK cipher acts as an essential element in the field of cryptography. Since the publication of the Data Encryption Standard (DES) [1], plenty of instances have been proposed to enrich the choices and in the meanwhile to resist evolving cryptanalysis techniques [2–5]. In the 1990's, along with the development of the computer science and the invention of the differential [6] and linear cryptanalysis [7], DES with 56-bit key could no longer provide security level needed in many applications. Due to this, the National Institute of Standards and Technology (NIST) initiated the competition for Advanced Encryption Standard (AES) in 1997. The Rijndael won the competition and officially became the new AES standard in 2001 [8].

In the last few decades, a lot of researches have been exploited on the design and cryptanalysis of block ciphers, many of which allow the provable security evaluations against known cryptanalytic vectors such as the differential and linear cryptanalysis [9, 10], as well as their extensions such as the impossible differential and zero-correlation linear cryptanalysis [11–13]. Links among different cryptanalytic techniques can help reduce the workload during the process of evaluating the security of a cipher since there might exist some equivalence between different distinguishers constructed by different cryptanalytic methods. As a result, a series of work focus on finding and establishing links between different cryptanalytic techniques.

For instance, Blondeau and Nyberg claimed in 2013 that there exists some equivalence between a zero-correlation linear hull and an impossible differential in some specific cases [14]. Then, Blondeau et al. proposed a practical relation between these two distinguishers for Feistel-type and Skipjack-type ciphers [15]. At CRYPTO 2015, Sun et al. proposed the dual structure and proved that an impossible differential of a structure is a zero-correlation linear hull of its dual structure [16].

The design of modern block ciphers always uses iterative structures to simplify the security analysis and enable better software and hardware efficiencies. Among all the candidates, the structures that have similar procedures between the decryption and the encryption, such as Feistel and Lai-Massey structures, are being especially concerned.

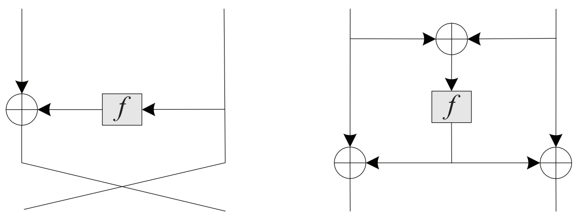

Fig. 1: Feistel structure and Lai-Massay structure

The Feistel structure, which is utilized by SIMON [17], SIMECK [18] and so on, plays an important role in symmetric key cryptography from both theoretical and practical point of view. It becomes popular since the publication of DES. With Feistel structures, it is convenient to generate permutations from various round functions, bijective or not, which allows to construct many schemes for specific needs. In a Feistel cipher, see Fig. 1, the block of plaintext to be encrypted is split into two equal-sized halves. The round function is applied to one half, using a subkey, and then the output is XORed with the other half. The two halves are then swapped. There are many extensions of the Feistel structure, such as the SM4 structure [19], the Mars structure [20], type-1, type-2, and type-3 generalized Feistel structures [21–23].

The Lai-Massey scheme [24] was first used in the design of Proposed Encryption Standard (PES) [25] which was

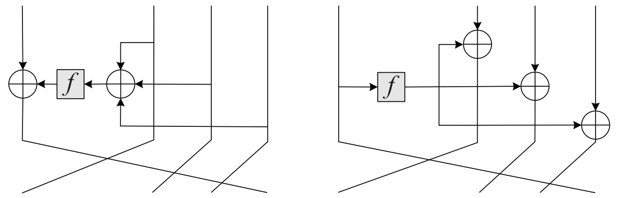

Fig. 2: An SM4 and A Mars Structure

later modified to be the International Data Encryption Algorithm (IDEA) in 1991. Other ciphers making use of this structure include MESH [26], FOX [27], etc. The Lai-Massey structure offers security properties similar to the Feistel structure, and also shares the advantages that the decryption is similar to the encryption and the round functions are not necessarily to be bijective. The input block is also split into two equal-sized halves. The round function is applied to the sum of the two pieces, and the result is then added to both half blocks. Nevertheless, we cannot use it directly as shown in Fig. 1 in order to obtain a secure cipher. Yet this can be overcome by introducing an orthomorphism on one of the two branches [24].

Our Contributions. Many of the iterative structures can be divided into two categories, according to whether the inverse of the round function is necessary to compute the inverse of the structure, and the ones that do not need the inverse, such as the Feistel and Lai-Massey structures, are of special interest in this paper. The main contributions of this paper are as follows.

(1) We find a unified description for the known structures that share similar procedures for decryption and encryption, and find a sufficient and necessary condition for this structure to be bijective, which enlarges the choices of structures for block cipher designs.
(2) By introducing the dual structure, we prove that an r-round differential of a structure is impossible if and only if it is an r-round zero-correlation linear hull of the dual structure. Then, to make the unified structure resilient to differential and linear cryptanalysis, we give some constraints on linear components. Furthermore, We prove that there always exist a $(3n-1)$-round impossible differential and a $(3n-1)$-round zero-correlation linear hull when some conditions are

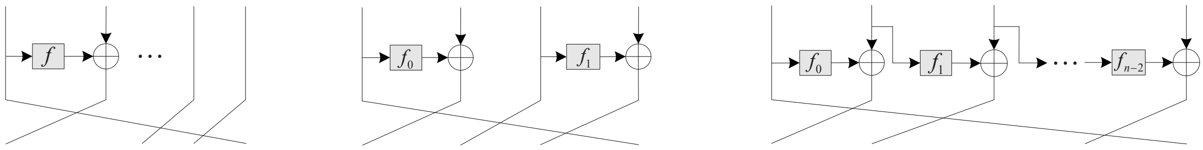

Fig. 3: A Type-1, A Type-2 and A Type-3 generalized Feistel Structure

specified.

(3) We propose several new structures as instances which might be used in future block cipher designs.

Organization. The rest of the paper is organized as follows. Section 2 presents the unified description of the structures sharing similar decryption and encryption procedures. Section 3 gives some preliminary cryptanalysis results of the structure. Section 4 proposes some new structures as instances for block cipher designs. At last, Section 5 concludes this paper.

2. THE UNIFIED STRUCTURE

In this section, we propose the unified structure whose decryption procedure is similar to that of the encryption, and give a sufficient and necessary condition for the structure to be bijective.

Let $\mathbb{F}_2$ denote the binary field and $\mathbb{F}_2^n$ denote the n-dimensional vector space over $\mathbb{F}_2$. Throughout this paper, $x = (x_0, x_1, \ldots, x_{n-1})$ always corresponds to a column vector. Depending on whether the inverse of the nonlinear round function is needed for the decryption, the iterative structures of the block ciphers can be grouped into two broad categories: the first one does not need the inverse of round function for decryption, while the second one generally requires the inverse of the round function for decryption. The aim of this section is to give a unified view of the structures which do not need the inverse of the round function.

Let b and t be positive integers, $A = [A_0, A_1, \ldots, A_{n-1}]$ and $B = [B_0, B_1, \ldots, B_{n-1}]$ where $A_i \in \mathbb{F}_2^{t\times b}$ and $B_j \in \mathbb{F}_2^{b\times t}$. Let f be any map over $\mathbb{F}_2^t$. Then, the map $f_{A,B} : \mathbb{F}_2^{b\times n} \to \mathbb{F}_2^{b\times n}$ is defined as:

$$y_i = x_i \oplus B_i f(h), \quad 0 \le i \le n-1,$$

where $(y_0, y_1, \ldots, y_{n-1}) = f_{A,B}(x_0, x_1, \ldots, x_{n-1})$, $h = A_0x_0 \oplus A_1x_1 \oplus \cdots \oplus A_{n-1}x_{n-1}$, and $x_i, y_i \in \mathbb{F}_2^b$, see Fig. 4.

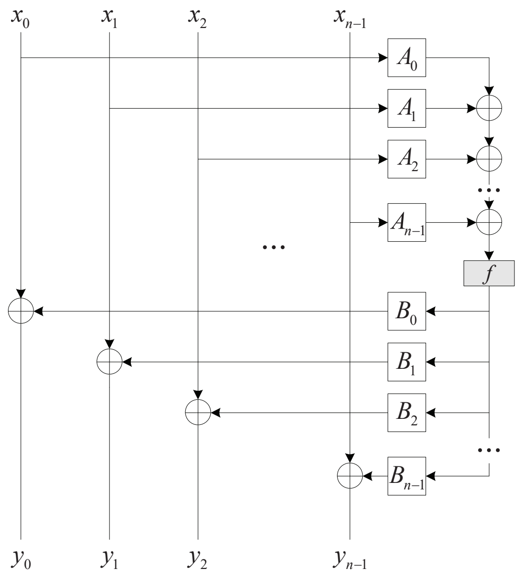

Fig. 4: The Unified Structure $f_{A,B}$

Denote by $\mathcal{B}_t$ all the maps from $\mathbb{F}_2^t$ to $\mathbb{F}_2^t$. Then, as illustrated in [16], the structure $\mathcal{F}_{A,B}$ is defined as $\mathcal{F}_{A,B} = \{f_{A,B} \mid f \in \mathcal{B}_t\}$, and $\mathcal{F}_{A,B}$ is said to be invertible if $f_{A,B}$ is invertible for all possible $f \in \mathcal{B}_t$.

Firstly, we give a sufficient condition for the structure to be bijective.

Lemma 1. *Assume $A_0B_0 \oplus A_1B_1 \oplus \cdots \oplus A_{n-1}B_{n-1} = 0$. Then, $\mathcal{F}_{A,B}$ is invertible. Furthermore, for any invertible instance $f_{A,B}$, $f_{A,B}^{-1} = f_{A,B}$ always holds.*

Proof: If $A_0B_0 \oplus A_1B_1 \oplus \cdots \oplus A_{n-1}B_{n-1} = 0$, then we can check the following equation holds for any

$X = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{b\times n}$:

$$\sum_{i=0}^{n-1} A_i y_i = \sum_{i=0}^{n-1} A_i (x_i \oplus B_i f(h)) = \sum_{i=0}^{n-1} A_i x_i \bigoplus \left(\sum_{i=0}^{n-1} A_i B_i\right) f(h) = \sum_{i=0}^{n-1} A_i x_i.$$

Thus for any $f_{A,B}$,

$$f_{A,B} \circ f_{A,B}(X) = X,$$

which indicates that $\mathcal{F}_{A,B}$ is invertible and $f_{A,B}^{-1} = f_{A,B}$. ■

Fortunately, the sufficient condition shown in Lemma 1 is also necessary for the structure to be bijective.

Lemma 2. *Assume $\mathcal{F}_{A,B}$ is invertible. Then, we always have $A_0B_0 \oplus A_1B_1 \oplus \cdots \oplus A_{n-1}B_{n-1} = 0$.*

Proof: Suppose $A_0B_0 \oplus A_1B_1 \oplus \cdots \oplus A_{n-1}B_{n-1} \neq 0$. Then, there is a non-zero vector β in $\mathbb{F}_2^t$ such that

$$(A_0B_0 \oplus A_1B_1 \oplus \cdots \oplus A_{n-1}B_{n-1})\beta \neq 0.$$

Given β, we are going to construct a map f such that $f_{A,B}$ is not invertible by showing two values mapping to the same image under f.

For any $(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{b\times n}$, let

$$\begin{cases} f(A_0x_0 \oplus A_1x_1 \oplus \cdots \oplus A_{n-1}x_{n-1}) = 0, \\ f(A_0x_0 \oplus A_1x_1 \oplus \cdots \oplus A_{n-1}x_{n-1} \\ \oplus (A_0B_0 \oplus A_1B_1 \oplus \cdots \oplus A_{n-1}B_{n-1})\beta) = \beta. \end{cases}$$

Then, according to the procedure of $f_{A,B}$, we have

$$f_{A,B}(x_0, x_1, \ldots, x_{n-1}) = (x_0, x_1, \ldots, x_{n-1}),$$

and

$$f_{A,B}(x_0 \oplus B_0\beta, x_1 \oplus B_1\beta, \ldots, x_{n-1} \oplus B_{n-1}\beta) \\ = (x_0, x_1, \ldots, x_{n-1}).$$

Obviously we have $(B_0\beta, B_1\beta, \ldots, B_{n-1}\beta) \neq 0$, since otherwise $(A_0B_0 \oplus A_1B_1 \oplus \cdots \oplus A_{n-1}B_{n-1})\beta \neq 0$. Therefore,

$$(x_0, x_1, \ldots, x_{n-1}) \neq (x_0 \oplus B_0\beta, x_1 \oplus B_1\beta, \ldots, x_{n-1} \oplus B_{n-1}\beta),$$

which shows $(x_0, x_1, \ldots, x_{n-1})$ has at least two different pre-images. Thus, for the f defined as above, $f_{A,B}$ is not injective, hence not invertible. ■

According to Lemma 1 and Lemma 2, we have the following theorem:

Theorem 3. *$\mathcal{F}_{A,B}$ is invertible if and only if $A_0B_0 \oplus A_1B_1 \oplus \cdots \oplus A_{n-1}B_{n-1} = 0$. Furthermore, for any invertible instance $f_{A,B}$, $f_{A,B}^{-1} = f_{A,B}$ always holds.*

We emphasize b and t can be equal, but they are allowed to be different as well. In addition, f can be either bijective or non-bijective. Theorem 3 summarizes the known structures that have a decryption process similar with that of the encryption. Table I lists several instances that are involved in the unified structure together with their corresponding instantiations for the A and B, where I and O stand for the identity matrix and zero matrix, respectively.

Besides Feistel, Lai-Massey, SM4, Mars and type-1 generalized Feistel listed above, the type-2 generalized Feistel structure can also be viewed as an instance of the unified structure. We take the one as shown in Fig. 3 as an example to show the parameters:

$$A_0 = \begin{bmatrix} I \\ O \end{bmatrix}, A_2 = \begin{bmatrix} O \\ I \end{bmatrix}, B_1 = \begin{bmatrix} I, & O \end{bmatrix}, B_3 = \begin{bmatrix} O, & I \end{bmatrix},$$

$A_1 = A_3 = B_0 = B_2 = O$, and the round function is the concatenation of f_0 and f_1. In addition, the type-3 generalized Feistel structure can be viewed as the parallelism of the type-1 generalized Feistel structure.

Following are three important notes:

(1) Theorem 3 gives the guidelines to ensure invertibility of the round under universal choices of f. This does not rule out the possibility that, for some (not all) f, dedicated choices of A, B not fulfilling the theorem may still make the round function invertible.

(2) The conditions above only guarantee the invertibility. To design a secure cipher, more constraints to the choices of A and B as well as f have to be put in place, in order to make the cipher resilient to known attacks such as differential attack and impossible differential attack. These will be discussed in the

TABLE I: Special Instances of the Unified Structure

Feistel structure	$n=2$	$A_0=I, A_1=O$
		$B_0=O, B_1=I$
Lai-Massey structure	$n=2$	$A_0=I, A_1=I$
		$B_0=I, B_1=I$
SM4 structure	$n=4$	$A_0=O, A_1=A_2=A_3=I$
		$B_0=I, B_1=B_2=B_3=O$
Mars structure	$n=4$	$A_0=I, A_1=A_2=A_3=O$
		$B_0=O, B_1=B_2=B_3=I$
Type-1 generalized Feistel structure	n	$A_0=I, A_1=A_2=\cdots=A_{n-1}=O$
		$B_1=I, B_0=B_2=\cdots=B_{n-1}=O$

following sections.

(3) To design a secure structure, we always adopt a permutation π on the n output branches of $\mathcal{F}_{A,B}$, which is denoted as $\mathcal{F}_{A,B,\pi}$ in the following.

3. Structural Cryptanalysis of $\mathcal{F}_{A,B}$

This section analyzes the security of the unified structure against the impossible differential and zero-correlation linear cryptanalysis which do not investigate the details of the round function, and also gives some constraints on the linear parameters of the structure such that it can be resilient to the differential and linear cryptanalysis. Firstly, by introducing the dual structure of the unified structure, we prove that a differential of the unified structure is impossible if and only if it is a zero-correlation linear hull of its dual structure. Secondly, to make the structure resilient to differential and linear cryptanalysis, the ranks of the linear components should be at least the product of the number of the branches n and the width of the branches b. Furthermore, taking account the circularly shift is widely used in the design of ciphers, we investigate the generalised situation that the order of the permutation equals n. Under this setting, we prove that there always exist $(3n-1)$-round impossible differentials and zero-correlation linear hulls of the structure, which presents an algorithm to construct these distinguishers as well.

Let $A^* = [A_0^{\mathrm{T}}, A_1^{\mathrm{T}}, \ldots, A_{n-1}^{\mathrm{T}}]$ and $B^* = [B_0^{\mathrm{T}}, B_1^{\mathrm{T}} \ldots, B_{n-1}^{\mathrm{T}}]$. Denote by q the order of permutation π, i.e., $q = \mathrm{ord}(\pi)$ is the least positive integer d such that π^d is the identity. Given a permutation π, there is always a permutation matrix P_π which is an $n\times n$ block matrix $(P_{i,j})_{n\times n}$, where $P_{i,j}$ is a $b\times b$ zero matrix for all (i,j) except $P_{i,\pi(i)} = I_b$, $i=1,2,\ldots,n$ which is the $b\times b$ identity matrix. For an integer $r\geq 1$, we further associate A, B and π with the following two matrices:

$$\mathcal{A}_\pi^{(r)} = \begin{bmatrix} A \\ AP_\pi \\ \vdots \\ AP_\pi^{r-1} \end{bmatrix}, \quad \mathcal{B}_\pi^{(r)} = \begin{bmatrix} B^* \\ B^*P_\pi \\ \vdots \\ B^*P_\pi^{r-1} \end{bmatrix}.$$

A. Dual Structure

At CRYPTO 2015, Sun et al. defined the dual structure of a Feistel structure in [16]. In the following, we are going to extend the dual structure from the Feistel structure to the unified structure. As illustrated in Fig. 5, we give the dual structure of $\mathcal{F}_{A,B,\pi}$ as follows.

Definition 4. *Let $\mathcal{F}_{A,B,\pi}$ be an iterative structure with matrices A, B and permutation π. Then the dual structure $\mathcal{F}_{A,B,\pi}^{\perp}$ is defined as $\mathcal{F}_{B^*,A^*,\pi}$.*

As in [16], we can build the following link between the impossible differential and zero-correlation linear hull of the unified structure.

Theorem 5. *$\alpha\to\beta$ is an r-round impossible differential of $\mathcal{F}_{A,B,\pi}$ if and only if it is an r-round zero-correlation linear hull of $\mathcal{F}_{A,B,\pi}^{\perp} = \mathcal{F}_{B^*,A^*,\pi}$.*

Proof: The proof can be divided into the following two parts:

Part(I). We prove that for $\delta_0\to\delta_r$, $\delta_0,\delta_r\in\mathbb{F}_2^{b\times n}$, if there is an instance $F\in\mathcal{F}_{B^*,A^*,\pi}$ such that the correlation is non-zero, i.e., $c(\delta_0\cdot x\oplus\delta_r\cdot F(x))\neq 0$, we can find an instance $F'\in\mathcal{F}_{A,B,\pi}$ such that the corresponding

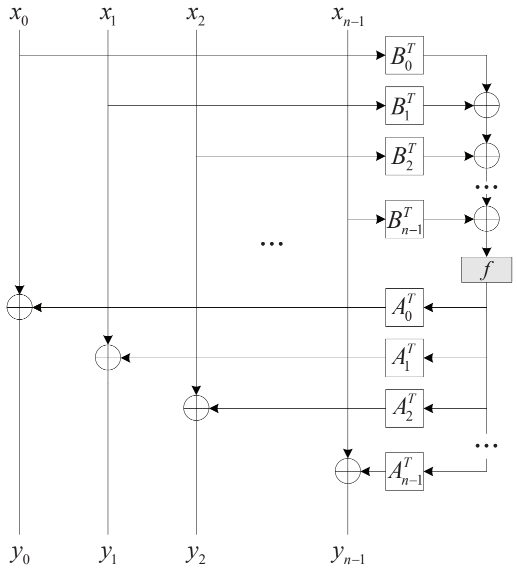

Fig. 5: Dual structure $\mathcal{F}^{\perp}_{A,B,\pi}$ of $\mathcal{F}_{A,B,\pi}$

differential characteristic is with positive probability, i.e., $p(\delta_0 \to \delta_r) > 0$.

Assume that $\delta_0 \to \delta_r$ is a linear hull with a non-zero correlation for some $F \in \mathcal{F}_{B^*,A^*,\pi}$. Then there exists a linear trail with a non-zero correlation:

$$\delta_0 \to \cdots \to \delta_i \to \cdots \to \delta_r.$$

where $\delta_i \in \mathbb{F}_2^{b\times n}$. Denote by u_i the input mask of f_i and $\hat{B}$ the block matrix whose i-th row is B_i. Then we have

$$\delta_{i+1} = P_\pi(\delta_i \oplus \hat{B}u_i).$$

In the following, for any $x \in \mathbb{F}_2^{b\times n}$, we are going to construct an r-round cipher $F_r \in \mathcal{F}_{A,B,\pi}$, such that $F_r(x) \oplus F_r(x \oplus \delta_0) = \delta_r$. If $r = 0$, we define

$$f_0(Ax) = Ax, \quad f_0(A(x \oplus \delta_0)) = Ax \oplus u_0.$$

Then, for $F_0 \in \mathcal{F}_{A,B,\pi}$ which adopts such f_0, $F_0(x) \oplus F_0(x \oplus \delta_0) = \delta_1$.

Assume we have constructed F_{r-1} such that $F_{r-1}(x) \oplus F_{r-1}(x \oplus \delta_0) = \delta_r$, and denote by y the output of $F_{r-1}(x)$. In the r-th round, define f_r as follows:

$$f_r(Ay) = Ay, \quad f_r(A(y \oplus \delta_r)) = Ay \oplus u_r.$$

Then

$$F_r(x) = P_\pi(y \oplus \hat{B}Ay)$$

and

$$F_r(x \oplus \delta_0) = P_\pi(y \oplus \delta_r \oplus \hat{B}(Ay \oplus u_r)).$$

Therefore, $F_r(x) \oplus F_r(x \oplus \delta_0) = P_\pi(\delta_r \oplus \hat{B}u_r) = \delta_{r+1}$.

Part(II). We prove that for $\delta_0 \to \delta_r$, if $p(\delta_0 \to \delta_r) > 0$ holds for an instance $F \in \mathcal{F}_{A,B,\pi}$, there exists some $F' \in \mathcal{F}_{B^*,A^*,\pi}$ such that $c(\delta_0 \cdot x \oplus \delta_r \cdot F'(x)) \neq 0$.

Assume that $\delta_0 \to \delta_r$ is a differential of $F \in \mathcal{F}_{A,B,\pi}$. Then there exists a differential characteristic with positive probability:

$$\delta_0 \to \cdots \to \delta_i \to \cdots \to \delta_r$$

where $\delta_i \in \mathbb{F}_2^{b\times n}$. In this characteristic, the input difference of f_i is $A\delta_i \in \mathbb{F}_2^b$. Denote by $v_i \in \mathbb{F}_2^b$ the output difference of f_i. Then $\delta_{i+1} = P_\pi(\delta_i \oplus \hat{B}v_i)$.

Taking the following fact into consideration: for $(A\delta_i, v_i)$, there always exists a $b \times b$ binary matrix L_i such that $v_i = L_i A\delta_i$. Therefore, we can simply let $f_i(x) = L_i x$, which results in $c(v_i \cdot x \oplus A\delta_i \cdot f_i(x)) = 1$.

Now we are going to construct an r-round cipher $F_r \in \mathcal{F}_{B^*,A^*,\pi}$ such that $c(\delta_0 \cdot x \oplus \delta_r \cdot F_r(x)) \neq 0$. If $r = 0$, let $f_0(x) = L_0 x$. Then all operations in $F_0 \in \mathcal{F}_{B^*,A^*,\pi}$ are linear over $\mathbb{F}_2$, which implies the existence of a $bn \times bn$ binary matrix M_0 such that $F_0(x) = M_0 x$, and

$$c(\delta_0 \cdot x \oplus \delta_1 \cdot F_0(x)) = 1.$$

Assume we have constructed $F_{r-1}(x) = M_{r-1}x$, with M_{r-1} being a $bn \times bn$ binary matrix such that

$$c(\delta_0 \cdot x \oplus \delta_{r-1} \cdot F_{r-1}(x)) = 1$$

and we can define f_r in the r-round similarly, then $F_r(x) = M_r x$ for some $bn \times bn$ binary matrix M_r, and

$$c(\delta_0 \cdot x \oplus \delta_r \cdot F_r(x)) = 1$$

which ends our proof. ■

Theorem 5 is fundamental in the cryptanalysis of $\mathcal{F}_{A,B,\pi}$, since it reveals the fact that constructing a zero-correlation linear hull of an instance of the unified structure is equivalent to constructing an impossible differential of another instance of the unified structure, which generalizes the link between the impossible differential and zero-correlation linear hulls from the Feistel structure to the unified structures.

B. Differential and Linear Cryptanalysis

To design an iterative structure, extra constraints to A and B as well as π might be imposed, in order to make the structure resilient to differential and linear cryptanalysis, and so on.

Firstly, we recall that b is the width of the branch, n is the number of branches, and q is the order of π.

Theorem 6. *The rank of $\mathcal{A}_\pi^{(q)}$ needs to be bn. Otherwise, there always exists an r-round differential of $\mathcal{F}_{A,B,\pi}$ with probability 1 no matter how large r is. Furthermore, when the rank of $\mathcal{A}_\pi^{(q)}$ equals bn, there exists at least 1 differentially active round function f in $\mathcal{F}_{A,B,\pi}$ covering consecutive q rounds.*

Proof: There are bn columns in $\mathcal{A}_\pi^{(q)}$, so $\mathrm{rank}(\mathcal{A}_\pi^{(q)}) \le bn$. If $\mathrm{rank}(\mathcal{A}_\pi^{(q)}) < bn$, then $\mathcal{A}_\pi^{(q)} x = 0$ has a non-zero solution. To be specific, there is a non-zero vector $\delta \in \mathbb{F}_2^{b\times n}$ such that

$$\begin{cases} A\delta = 0 \\ AP_\pi\delta = 0 \\ \quad\vdots \\ AP_\pi^{q-1}\delta = 0 \end{cases} \tag{1}$$

Let the input difference of the first round be δ, then the input difference to the first f is $A\delta = 0$. And thus the output difference, which is also the input to the second round, is $P_\pi\delta$.

Following Equ. (1), for any $j \in \{1, 2, \ldots, q\}$, both of the input and output differences of f in the j-round are 0. Obviously, the output difference of the q-th round equals to $P_\pi^q\delta$. Taking $P_\pi^q = I$ into consideration, the input difference of f in the $(q+1)$-th round is $AP_\pi^{q+1}\delta = AP_\pi\delta = 0$. Then the output difference of the r-th round is $P_\pi^r\delta$. So

$$\delta \to P_\pi^r\delta$$

is an r-round differential with probability 1 regardless of rounds.

We assume none of the round function in q consecutive rounds is differentially active, which means the input differences to the q round functions are 0.

Let the input difference to the first round be $0 \ne \delta \in \mathbb{F}_2^{b\times n}$. Since the output differences of these rounds functions are 0, the input differences of the i-th round is $P_\pi^{i-1}\delta$, where $i = 1, 2, \ldots, q$. Then, the input difference to the i-th f is $AP_\pi^{i-1}\delta = 0$, $i = 1, 2, \ldots, q$. So, we get Equ. (1), i.e., $\mathcal{A}_\pi^{(q)}\delta = 0$ and $\delta \ne 0$. However, $\mathrm{rank}(\mathcal{A}_\pi^{(q)}) = bn$ implies that $\mathcal{A}_\pi^{(q)}\delta = 0$ only has zero solution, which contradicts with $\delta \ne 0$.

Thus, at least 1 round function f of consecutive q rounds is differentially active.

■

We use the Lai-Massey structure to verify Theorem 6. The Lai-Massey structure with the orthomorphism is not an instance of $\mathcal{F}_{A,B,\pi}$ since the decryption procedure is different from the encryption procedure, i.e. $f_{A,B}^{-1} \ne f_{A,B}$. However, the Lai-Massey structure without the orthomorphism can be considered as a specific example of $\mathcal{F}_{A,B,\pi}$ with the following parameters: $n = 2, A_0 = I, A_1 = I, B_0 = I, B_1 = I$, $\pi(1) = 2$ and $\pi(2) = 1$, as seen in Fig. 1.

Then we have $A = [I, I]$, $B^* = [I, I]$, and

$$\mathcal{A}_\pi^{(2)} = \begin{bmatrix} I & I \\ I & I \end{bmatrix} \text{ and } \mathcal{B}_\pi^{(2)} = \begin{bmatrix} I & I \\ I & I \end{bmatrix}.$$

Let

$$\begin{bmatrix} I & I \\ I & I \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = 0.$$

We find $x_1 = x_2$. Accordingly, $(\alpha, \alpha) \to (\alpha, \alpha)$ where $\alpha \ne 0$ is an r-round differential of this structure with probability 1 for any value of r. Therefore, an orthomorphism is needed to get rid of this iterative differential.

Following Theorem 5, we have a similar constraint on B which shows there might be a potential linear weakness if B is not carefully designed:

Corollary 7. *The rank of $\mathcal{B}_\pi^{(q)}$ needs to be bn. Otherwise, there always exists an r-round linear hull of $\mathcal{F}_{A,B,\pi}$ with* *correlation* 1*, regardless of the value of* r*. Furthermore, when the rank of* $\mathcal{B}_\pi^{(q)}$ *equals* bn*, there exists at least* 1 *linearly active round function* f *in* $\mathcal{F}_{A,B,\pi}$ *covering consecutive* q *rounds.*

Both Theorem 6 and Corollary 7 show that, as long as the round function is carefully designed, $\mathcal{F}_{A,B,\pi}$ with enough rounds can resist differential and linear cryptanalysis.

In summary, to avoid these weakness with respect to the differential and linear cryptanalysis, the following equation must hold:

$$\mathrm{rank}(\mathcal{A}_\pi^{(q)}) = \mathrm{rank}(\mathcal{B}_\pi^{(q)}) = bn.$$

Since the rank of a matrix cannot be larger than either the columns or the rows, $\mathrm{rank}(\mathcal{A}_\pi^{(q)}) \le \min\{\mathrm{ord}(\pi) \times t, bn\}$, we have:

Corollary 8. *The order of the permutation on* n *branches must be at least* $\mathrm{ord}(\pi) = \frac{b}{t}n$*.*

Since the circularly shift is very popular in the design of a cipher, we are now investigating this case. Particularly, we assume $\pi_0(i) = i+1$ for $1 \le i \le n-1$ and $\pi_0(n) = 1$. And a more generalized case is that $\mathrm{ord}(\pi) = n$ which contains π_0 as an instance.

Corollary 9. *If we adopt* π_0 *or generally a permutation whose order is* n*, the length of the output of each* A_i *is at least that of the input, i.e.,* $t \ge b$*.*

C. Impossible Differential and Zero-Correlation Linear Cryptanalysis

In this part, we assume A_i and B_j are squares, and the round function is bijective.

Proposition 10. *Assume* $\mathrm{ord}(\pi) = n$*,* $\mathrm{rank}(\mathcal{A}_\pi^{(q)}) = \mathrm{rank}(\mathcal{B}_\pi^{(q)}) = bn$ *and* $t = b$*. Then, there is a* $(3n-1)$*-round impossible differential of* $\mathcal{F}_{A,B,\pi}$*, provided* A_i *and* B_j *are squares, and* f *is bijective.*

Proof: We consider the solutions for the following equations:

$$\begin{cases} A\delta = 0 \\ AP_\pi\delta = 0 \\ \quad\vdots \\ AP_\pi^{n-2}\delta = 0 \end{cases} \tag{2}$$

and $AP_\pi^{n-1}\delta \ne 0$.

When $q = \mathrm{ord}(\pi) = n$, we recall that

$$\mathcal{A}_\pi^{(q)} = \begin{bmatrix} A \\ AP_\pi \\ \vdots \\ AP_\pi^{n-1} \end{bmatrix}, \quad \mathcal{B}_\pi^{(q)} = \begin{bmatrix} B^* \\ B^*P_\pi \\ \vdots \\ B^*P_\pi^{n-1} \end{bmatrix}.$$

Since $\mathrm{rank}(\mathcal{A}_\pi^{(q-1)}) \le (n-1)b < nb$, there is a non-zero solution δ of Equ. (2).

Denote by δ the input difference to the first round. Since the input difference to the first f is $A\delta = 0$, the output difference of the first f is also 0. Thus the output difference of the first round is $P_\pi\delta$.

Then, the input difference to the second f is $AP_\pi\delta = 0$, thus the output differences of the second f and the second round are 0 and $P_\pi^2\delta$, respectively.

Similarly, according to Equ. (2), for any $i \in \{3, \ldots, n-1\}$ the input difference to the i-th f is always 0, and the output difference to the i-th round is $P_\pi^i\delta$. Particularly, the output difference of the $(n-1)$-th round is $P_\pi^{n-1}\delta$.

Denote by $\gamma_1, \gamma_2, \ldots, \gamma_{n+1}$ and $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n+1}$ the input and output differences to f in the n-th, $(n+1)$-th, …, $(2n)$-th rounds, respectively. Since $\gamma_1 = AP_\pi^{n-1}\delta \ne 0$ and f is bijective, we have $\varepsilon_1 \ne 0$. Then, the output difference of the n-th round is

$$\delta_n = \delta \oplus P_\pi\hat{B}\varepsilon_1.$$

Denote by δ_{2n} the output difference of the $2n$-th round. Then,

$$\delta_{2n} = \delta \oplus P_\pi^{n+1}\hat{B}\varepsilon_1 \oplus \cdots \oplus P_\pi\hat{B}\varepsilon_{n+1}.$$

Since the output difference of the $(3n-1)$-th round is $P_\pi^{n-1}\delta$, and the structure has a similar decryption procedure as that of the encryption, we could infer from the decryption direction that the input difference of the $(2n+1)$-th round is $\eta_{2n+1} = \delta$.

If the $(3n-1)$-round differential $\delta \to P_\pi^{n-1}\delta$ is possible, we have $\delta_{2n} = \eta_{2n+1}$, which implies

$$P_\pi^{n+1}\hat{B}\varepsilon_1 \oplus \cdots \oplus P_\pi \hat{B}\varepsilon_{n+1} = 0.$$

Then, taking $P_\pi^{n+1} = P_\pi$ into account, we have:

$$\begin{bmatrix} \hat{B} & P_\pi \hat{B} & P_\pi^2 \hat{B} & \cdots & P_\pi^{n-1}\hat{B} \end{bmatrix} \begin{bmatrix} \varepsilon_2 \\ \varepsilon_1 \oplus \varepsilon_{n+1} \\ \varepsilon_n \\ \vdots \\ \varepsilon_3 \end{bmatrix} = 0. \tag{3}$$

Since P_π is a permutation matrix, $(P_\pi^j)^{\mathrm{T}} = (P_\pi^j)^{-1} = P_\pi^{n-j}$. As a result,

$$\begin{bmatrix} \hat{B} & P_\pi \hat{B} & P_\pi^2 \hat{B} & \cdots & P_\pi^{n-1}\hat{B} \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} B^* \\ B^* P_\pi^{n-1} \\ \vdots \\ B^* P_\pi \end{bmatrix}$$

whose rank is nb. Thus, Equ. (3) has only zero solution which demonstrates

$$(\varepsilon_1 \oplus \varepsilon_{n+1}) = \varepsilon_2 = \cdots = \varepsilon_n = 0.$$

Therefore, $\gamma_2 = \cdots = \gamma_n = 0$, due to the fact f is bijective. On the other hand, $\gamma_2, \ldots, \gamma_n$ can be computed as follows:

$$\begin{cases} \gamma_2 = A\delta \oplus AP_\pi \hat{B}\varepsilon_1 \\ \gamma_3 = AP_\pi\delta \oplus AP_\pi^2 \hat{B}\varepsilon_1 \\ \quad \vdots \\ \gamma_n = AP_\pi^{n-2}\delta \oplus AP_\pi^{n-1}\hat{B}\varepsilon_1 \end{cases}$$

Following $A_1B_1 \oplus A_2B_2 \oplus \cdots \oplus A_nB_n = 0$, we can get $A\hat{B}\varepsilon_1 = 0$. Thus

$$\begin{cases} A\hat{B}\varepsilon_1 = 0 \\ AP_\pi\hat{B}\varepsilon_1 = 0 \\ \quad \vdots \\ AP_\pi^{n-1}\hat{B}\varepsilon_1 = 0 \end{cases}$$

Since the columns of $\mathcal{A}_\pi^{(q)}$ are linearly independent, we have $\hat{B}\varepsilon_1 = 0$. The columns of $\mathcal{B}_\pi^{(q)}$ being independent indicates $\mathrm{rank}(\hat{B}) = \mathrm{rank}(B^*) = b$. So, we have $\varepsilon_1 = 0$ which contradicts $\varepsilon_1 \neq 0$. Thus, the $(3n-1)$-round differential $\delta \to P_\pi^{n-1}\delta$ is an impossible differential of $\mathcal{F}_{A,B,\pi}$. ■

Algorithm 1: Constructing $(3n-1)$-round impossible differential of $\mathcal{F}_{A,B,\pi}$

Input: matrix A, permutation π, the number of branches n;
Output: input difference δ^{in}, output difference δ^{out};

```
Computing the order of π, q = ord(π);
if q ≠ n then
    return ∅;
else
    Computing A_π^(n-1) = [A; ⋮; A P_π^(n-2)];
    Computing a non-zero solution δ for the equation A_π^(n-1) x = 0;
    δ^in ← δ;
    δ^out ← P_π^(n-1) δ;
return δ^in, δ^out;
```

Algorithm 1 gives an algorithm for computing the $(3n-1)$-round impossible differential of $\mathcal{F}_{A,B,\pi}$ provided the order of the permutation is n.

Due to Theorem 5, Proposition 10 can be projected to zero-correlation linear cryptanalysis of $\mathcal{F}_{A,B,\pi}$:

Proposition 11. *Assume* $\mathrm{ord}(\pi) = n$, $\mathrm{rank}(\mathcal{A}_\pi^{(q)}) = \mathrm{rank}(\mathcal{B}_\pi^{(q)}) = bn$ *and* $t = b$. *Then, there is a* $(3n-1)$*-round zero-correlation linear hull of* $\mathcal{F}_{A,B,\pi}$ *as long as* A_i *and* B_j *are squares, and* f *is bijective.*

Both Propositions 10 and 11 indicate that, as long as f is bijective, $\mathrm{ord}(\pi) = n$ and $\mathrm{rank}(\mathcal{A}_\pi^{(q)}) = \mathrm{rank}(\mathcal{B}_\pi^{(q)}) =$

bn, the structures might have the same security margin with respect to impossible differential and zero-correlation linear cryptanalysis, even if different A_i's and B_j's are specified.

Following are some notes:

(1) The SM4 structure is a specific example of $\mathcal{F}_{A,B,\pi}$, as seen in Fig. 2. According to Algorithm 1 and Proposition 10, $(\alpha,\alpha,\alpha,0) \rightarrow (0,\alpha,\alpha,\alpha)$ is an 11-round impossible differential of SM4 structure, where $\alpha \in \mathbb{F}_2^{32}$ and $\alpha \neq 0$. It is consistent with the results given in [28]. Notice the Mars structure is the dual structure of the SM4 structure, according to Proposition 11, $(\alpha,\alpha,\alpha,0) \rightarrow (0,\alpha,\alpha,\alpha)$ is also an 11-round zero-correlation linear hull of the Mars structure.

(2) Algorithm 1 can only compute $(3n-1)$-round impossible differentials from the perspective of structure without considering the details of round functions. In other words, if details of the round functions are investigated, the rounds of a distinguisher might be extended. For example, a 12-round impossible differential of SM4 was constructed using the fact that the round function f is composed of the non-linear layer followed by an MDS matrix [29, 30].

(3) We have shown a lower bound for the rounds of the impossible differential and zero-correlation linear hull of the unified structure by only using linear algebra. For a specific cipher, there might be some distinguishers that cover more rounds. Due to the complex round function, the automated tools are used to find these distinguishers. For a specific cipher, automatic search tools might help find out longer distinguishers since the details of round functions are taken into consideration which also consumes more computation and time.

Deal, SMS4 and Mars are specific instances of $\mathcal{F}_{A,B,\pi}$ with 2, 4 and 4 branches respectively. According to Proposition 10, there exist 5-, 11- and 11-round impossible differentials of these three ciphers, respectively, which is consistent with the results given in [28, 31]. Furthermore, assume conditions in Proposition 10 are satisfied, we can always construct $(3n-1)$-round impossible differentials, which shows that these structures have the same security with respect to impossible differential attack, even if different A's and B's are specified.

4. Proposals for New Structures

In this section, we propose two new structures as instances of $\mathcal{F}_{A,B}$ which may be used in future block cipher designs. Theorem 3 gives new approaches to select the structure of an iterative cipher. For example, based on Theorem 3, Fig. 6 gives a new structure whose encryption and decryption are the same:

Example 1. *Denote by (L_i, R_i) and (L_{i+1}, R_{i+1}) the input and output of the iterative structure, respectively, where $L_i, L_{i+1}, R_i, R_{i+1}$ are elements in $\mathbb{F}_{2^b}$. Then,*

$$\begin{cases} L_{i+1} = R_i \oplus \mathsf{a} w_i, \\ R_{i+1} = L_i \oplus w_i, \end{cases}$$

where a is the multiplication by a over the finite field $\mathbb{F}_{2^b}$ and $w_i = f(\mathsf{a}L_i \oplus R_i)$. Furthermore, following Theorem 6, a should not be equal to 1.

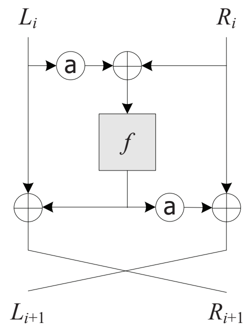

Fig. 6: Procedure of Example 1

In addition, we propose a new structure with 4 branches based on Theorem 3, see Fig. 7.

Example 2. *Let $\mathbb{F}_{2^{32}} = \mathbb{F}_2\langle u \rangle$, where u is a root of $g(x) = x^{32} \oplus x^{22} \oplus x^2 \oplus x \oplus 1$ in $\mathbb{F}_{2^{32}}$. Denote by (x_0, x_1, x_2, x_3) and (y_0, y_1, y_2, y_3) the input and output of the iterative structure, respectively, where x_i, y_i are elements in $\mathbb{F}_{2^{32}}$.*

Then,

$$\begin{cases} y_0 = x_1 \oplus w_i, \\ y_1 = x_2 \oplus \mathsf{2} w_i, \\ y_2 = x_3 \oplus \mathsf{3} w_i, \\ y_3 = x_0 \oplus w_i, \end{cases}$$

where $\mathsf{2}$ and $\mathsf{3}$ are the multiplications by $\mathsf{2}$ and $\mathsf{3}$ respectively over the finite field $\mathbb{F}_{2^{32}}$ and $w_i = f(\mathsf{2}x_0 \oplus \mathsf{3}x_1 \oplus x_2 \oplus x_3)$.

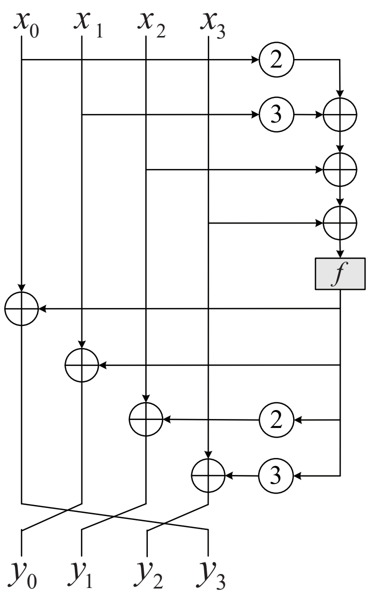

Fig. 7: Procedure of Example 2

The multiplications by $\mathsf{2}$ and $\mathsf{3}$ can be respectively written as M_2 and M_3, where $M_2, M_3 \in \mathbb{F}_2^{32\times 32}$. The structure is a specific example of $\mathcal{F}_{A,B,\pi}$ with the following parameters: $n = 4, A_0 = M_2, A_1 = M_3, A_2 = A_3 = I, B_0 = B_1 = I, B_2 = M_2, B_3 = M_3$, $\pi(1) = 4, \pi(2) = 1, \pi(3) = 2$ and $\pi(4) = 3$, as seen in Fig. 7.

Then we have $A = [M_2, M_3, I, I]$, $B^* = [I, I, M_2^{\mathrm{T}}, M_3^{\mathrm{T}}]$,

$$\mathcal{A}_\pi^{(4)} = \begin{bmatrix} M_2 & M_3 & I & I \\ I & M_2 & M_3 & I \\ I & I & M_2 & M_3 \\ M_3 & I & I & M_2 \end{bmatrix}$$

$$\text{and} \qquad \mathcal{B}_\pi^{(4)} = \begin{bmatrix} I & I & M_2^{\mathrm{T}} & M_3^{\mathrm{T}} \\ M_3^{\mathrm{T}} & I & I & M_2^{\mathrm{T}} \\ M_2^{\mathrm{T}} & M_3^{\mathrm{T}} & I & I \\ I & M_2^{\mathrm{T}} & M_3^{\mathrm{T}} & I \end{bmatrix}.$$

After calculation, $\mathrm{rank}(\mathcal{A}_\pi^{(4)}) = \mathrm{rank}(\mathcal{B}_\pi^{(4)}) = 128$. Let

$$\begin{bmatrix} M_2 & M_3 & I & I \\ I & M_2 & M_3 & I \\ I & I & M_2 & M_3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} \mathsf{0} \\ \mathsf{0} \\ \mathsf{0} \end{bmatrix}.$$

We find $x_1 = \mathsf{9}\alpha, x_2 = \mathsf{d}\alpha, x_3 = \mathsf{b}\alpha, x_4 = \mathsf{e}\alpha$ is a non-zero solution for the equation, where $\alpha \in \mathbb{F}_{2^{32}}, \alpha \neq 0$ and $\mathsf{9}, \mathsf{d}, \mathsf{b}, \mathsf{e}$ are the multiplications by $\mathsf{9}, \mathsf{d}, \mathsf{b}, \mathsf{e}$ respectively over the finite field $\mathbb{F}_{2^{32}}$. According to Proposition 10,

$$(\mathsf{9}\alpha, \mathsf{d}\alpha, \mathsf{b}\alpha, \mathsf{e}\alpha) \to (\mathsf{e}\alpha, \mathsf{9}\alpha, \mathsf{d}\alpha, \mathsf{b}\alpha)$$

is an 11-round impossible differential of this structure.

5. Conclusion

Many iterative structures have the same procedure of the decryption and the encryptions. In this paper, we give a unified view of these structures, which surprisingly gives many new structures as well. We analyze the security of this unified structure against differential cryptanalysis, linear cryptanalysis, impossible differential and zero-correlation linear cryptanalysis which also gives the constraints on the linear parameters of the structure. Firstly, we define the dual structure of $\mathcal{F}_{A,B}$ and prove the equivalence of the existences of impossible differential and zero-correlation linear hull between these two structures. To make the structure resilient to differential and linear cryptanalysis, we give some constraints which are necessary to be appended to the matrices A and B. Under such conditions and the assumption that the order of the permutation is n, we prove the existences of a

$(3n-1)$-round impossible differential and a $(3n-1)$-round zero-correlation linear hull of $\mathcal{F}_{A,B}$. Based on the unified structure, we propose some new structures as applications which may be used in future block cipher designs.

Acknowledgment

The authors would like to thank the anonymous reviews for their helpful suggestions.

References

[1] National Institute of Standards and Technology, “Data Encryption Standard (DES),” FIPS Publication 46-3, October 1999.

[2] C. Beierle, A. Biryukov, L. C. dos Santos, J. Großschädl, L. Perrin, A. Udovenko, V. Velichkov, and Q. Wang, “Alzette: A 64-bit arx-box - (feat. CRAX and TRAX),” in *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III*, ser. Lecture Notes in Computer Science, D. Micciancio and T. Ristenpart, Eds., vol. 12172. Springer, 2020, pp. 419–448. [Online]. Available: https://doi.org/10.1007/978-3-030-56877-1_15

[3] S. Banik, Z. Bao, T. Isobe, H. Kubo, F. Liu, K. Minematsu, K. Sakamoto, N. Shibata, and M. Shigeri, “WARP : Revisiting GFN for lightweight 128-bit block cipher,” *IACR Cryptol. ePrint Arch.*, p. 1320, 2020. [Online]. Available: https://eprint.iacr.org/2020/1320

[4] N. Mouha, B. Mennink, A. V. Herrewege, D. Watanabe, B. Preneel, and I. Verbauwhede, “Chaskey: An efficient MAC algorithm for 32-bit microcontrollers,” in *Selected Areas in Cryptography - SAC 2014 - 21st International Conference, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, ser. Lecture Notes in Computer Science, A. Joux and A. M. Youssef, Eds., vol. 8781. Springer, 2014, pp. 306–323. [Online]. Available: https://doi.org/10.1007/978-3-319-13051-4_19

[5] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim, “The SKINNY family of block ciphers and its low-latency variant MANTIS,” in *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, ser. Lecture Notes in Computer Science, M. Robshaw and J. Katz, Eds., vol. 9815. Springer, 2016, pp. 123–153. [Online]. Available: https://doi.org/10.1007/978-3-662-53008-5_5

[6] E. Biham and A. Shamir, “Differential cryptanalysis of des-like cryptosystems,” *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, 1991. [Online]. Available: https://doi.org/10.1007/BF00630563

[7] M. Matsui, “Linear cryptanalysis method for DES cipher,” in *Advances in Cryptology - EUROCRYPT ’93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, ser. Lecture Notes in Computer Science, T. Helleseth, Ed., vol. 765. Springer, 1993, pp. 386–397. [Online]. Available: https://doi.org/10.1007/3-540-48285-7_33

[8] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, ser. Information Security and Cryptography. Springer, 2002. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-04722-4

[9] ——, “The wide trail design strategy,” in *Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings*, ser. Lecture Notes in Computer Science, B. Honary, Ed., vol. 2260. Springer, 2001, pp. 222–238. [Online]. Available: https://doi.org/10.1007/3-540-45325-3_20

[10] ——, “AES and the wide trail design strategy,” in *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, ser. Lecture Notes in

Computer Science, L. R. Knudsen, Ed., vol. 2332. Springer, 2002, pp. 108–109. [Online]. Available: https://doi.org/10.1007/3-540-46035-7_7

[11] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," in *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, ser. Lecture Notes in Computer Science, J. Stern, Ed., vol. 1592. Springer, 1999, pp. 12–23. [Online]. Available: https://doi.org/10.1007/3-540-48910-X_2

[12] A. Bogdanov and V. Rijmen, "Linear hulls with correlation zero and linear cryptanalysis of block ciphers," *Des. Codes Cryptogr.*, vol. 70, no. 3, pp. 369–383, 2014. [Online]. Available: https://doi.org/10.1007/s10623-012-9697-z

[13] B. Sun, M. Liu, J. Guo, V. Rijmen, and R. Li, "Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis," in *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, ser. Lecture Notes in Computer Science, M. Fischlin and J. Coron, Eds., vol. 9665. Springer, 2016, pp. 196–213. [Online]. Available: https://doi.org/10.1007/978-3-662-49890-3_8

[14] C. Blondeau and K. Nyberg, "New links between differential and linear cryptanalysis," in *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, ser. Lecture Notes in Computer Science, T. Johansson and P. Q. Nguyen, Eds., vol. 7881. Springer, 2013, pp. 388–404. [Online]. Available: https://doi.org/10.1007/978-3-642-38348-9_24

[15] C. Blondeau, A. Bogdanov, and M. Wang, "On the (in)equivalence of impossible differential and zero-correlation distinguishers for feistel- and skipjack-type ciphers," in *Applied Cryptography and Network Security - 12th International Conference, ACNS 2014, Lausanne, Switzerland, June 10-13, 2014. Proceedings*, ser. Lecture Notes in Computer Science, I. Boureanu, P. Owesarski, and S. Vaudenay, Eds., vol. 8479. Springer, 2014, pp. 271–288. [Online]. Available: https://doi.org/10.1007/978-3-319-07536-5_17

[16] B. Sun, Z. Liu, V. Rijmen, R. Li, L. Cheng, Q. Wang, H. AlKhzaimi, and C. Li, "Links among impossible differential, integral and zero correlation linear cryptanalysis," in *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, ser. Lecture Notes in Computer Science, R. Gennaro and M. Robshaw, Eds., vol. 9215. Springer, 2015, pp. 95–115. [Online]. Available: https://doi.org/10.1007/978-3-662-47989-6_5

[17] 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 52nd Annual Design Automation Conference, San Francisco, CA, USA, June 7-11, 2015.* ACM, 2015, pp. 175:1–175:6. [Online]. Available: https://doi.org/10.1145/2744769.2747946

[18] G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong, "The simeck family of lightweight block ciphers," in *Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings*, ser. Lecture Notes in Computer Science, T. Güneysu and H. Handschuh, Eds., vol. 9293. Springer, 2015, pp. 307–329. [Online]. Available: https://doi.org/10.1007/978-3-662-48324-4_16

[19] W. Diffie and G. Ledin, "SMS4 encryption algorithm for wireless networks," *IACR Cryptol. ePrint Arch.*, p. 329, 2008. [Online]. Available: http://eprint.iacr.org/2008/329

[20] C. Burwick, D. Coppersmith, E. D'Avignon, R. Gen-

naro, S. Halevi, C. Jutla, S. M. Matyas, L. O'Connor, M. Peyravian, D. Safford, and N. Zunic, "The MARS encryption algorithm," 1999.

[21] K. Nyberg, "Generalized feistel networks," in *Advances in Cryptology - ASIACRYPT '96, International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, November 3-7, 1996, Proceedings*, ser. Lecture Notes in Computer Science, K. Kim and T. Matsumoto, Eds., vol. 1163. Springer, 1996, pp. 91–104. [Online]. Available: https://doi.org/10.1007/BFb0034838

[22] T. Shirai and K. Araki, "On generalized feistel structures using the diffusion switching mechanism," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 91-A, no. 8, pp. 2120–2129, 2008. [Online]. Available: https://doi.org/10.1093/ietfec/e91-a.8.2120

[23] Y. Zheng, T. Matsumoto, and H. Imai, "On the construction of block ciphers provably secure and not relying on any unproved hypotheses," in *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, ser. Lecture Notes in Computer Science, G. Brassard, Ed., vol. 435. Springer, 1989, pp. 461–480. [Online]. Available: https://doi.org/10.1007/0-387-34805-0_42

[24] S. Vaudenay, "On the lai-massey scheme," in *Advances in Cryptology - ASIACRYPT '99, International Conference on the Theory and Applications of Cryptology and Information Security, Singapore, November 14-18, 1999, Proceedings*, ser. Lecture Notes in Computer Science, K. Lam, E. Okamoto, and C. Xing, Eds., vol. 1716. Springer, 1999, pp. 8–19. [Online]. Available: https://doi.org/10.1007/978-3-540-48000-6_2

[25] X. Lai and J. L. Massey, "A proposal for a new block encryption standard," in *Advances in Cryptology - EUROCRYPT '90, Workshop on the Theory and Application of of Cryptographic Techniques, Aarhus, Denmark, May 21-24, 1990, Proceedings*, ser. Lecture Notes in Computer Science, I. Damgård, Ed., vol. 473. Springer, 1990, pp. 389–404. [Online]. Available: https://doi.org/10.1007/3-540-46877-3_35

[26] J. J. Nakahara, V. Rijmen, B. Preneel, and J. Vandewalle, "The MESH block ciphers," in *Information Security Applications, 4th International Workshop, WISA 2003, Jeju Island, Korea, August 25-27, 2003, Revised Papers*, ser. Lecture Notes in Computer Science, K. Chae and M. Yung, Eds., vol. 2908. Springer, 2003, pp. 458–473. [Online]. Available: https://doi.org/10.1007/978-3-540-24591-9_34

[27] P. Junod and S. Vaudenay, "FOX : A new family of block ciphers," in *Selected Areas in Cryptography, 11th International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004, Revised Selected Papers*, ser. Lecture Notes in Computer Science, H. Handschuh and M. A. Hasan, Eds., vol. 3357. Springer, 2004, pp. 114–129. [Online]. Available: https://doi.org/10.1007/978-3-540-30564-4_8

[28] Y. Luo, X. Lai, Z. Wu, and G. Gong, "A unified method for finding impossible differentials of block cipher structures," *Inf. Sci.*, vol. 263, pp. 211–220, 2014. [Online]. Available: https://doi.org/10.1016/j.ins.2013.08.051

[29] J. Lu, "Attacking reduced-round versions of the SMS4 block cipher in the chinese WAPI standard," in *Information and Communications Security, 9th International Conference, ICICS 2007, Zhengzhou, China, December 12-15, 2007, Proceedings*, ser. Lecture Notes in Computer Science, S. Qing, H. Imai, and G. Wang, Eds., vol. 4861. Springer, 2007, pp. 306–318. [Online]. Available: https://doi.org/10.1007/978-3-540-77048-0_24

[30] L. Cheng, B. Sun, and C. Li, "Revised cryptanalysis for SMS4," *Sci. China Inf. Sci.*, vol. 60, no. 12, p. 122101, 2017. [Online]. Available: https://doi.org/10.1007/s11432-016-0477-8

[31] L. R. Knudsen, "DEAL – A 128-bit Block Cipher," Department of Informatics, University of Bergen,

Norway, Tech. Rep., 1998.

Jiajie LIU received the B.E. and the M.E. degrees from the National University of Defense Technology, in 2016 and 2018, respectively. He is currently a PH.D. student with the National University of Defense Technology. His current research interests include the cryptography, especially structural cryptanalysis and provable security of symmetric primitives.

Bing Sun received the B.E. degree from the Airforce Engineering University of China in 2003, and the M.E. and Ph.D. degrees from the National University of Defense Technology, in 2005 and 2009, respectively. He is currently an Associate Professor with the National University of Defense Technology. His current research interests include the cryptography, especially cryptanalysis of symmetric primitives. He received the best paper awards from ACISP 2010.

Guoqiang Liu received the Ph.D.degree in Information Engineering University. He is currently an Associate Professor with the National University of Defense Technology. His research interests include design and cryptanalysis of block ciphers.

Xinfeng Dong received the B.E. degree from SiChuan University of China in 2008, and the M.E. degrees from Southwest Communications Institute of China in 2011. He is currently an senior researcher with the CETC and UESTC. His current research interests include the cryptography.

Li Liu received the PhD degree in information and communication engineering from the National University of Defense Technology, China, in 2012. She is currently a professor with the College of System Engineering. She has held visiting appointments at the University of Waterloo, Canada, at the Chinese University of Hong Kong, and at the University of Oulu, Finland. Her current research interests include computer vision, pattern recognition, and machine learning. Her papers have currently more than 7,800 citations in Google Scholar.

Hua Zhang is an associate professor with the Institute of Information Engineering, Chinese Academy of Sciences. He received the Ph.D. degrees in computer science from the School of Computer Science and Technology, Tianjin University, Tianjin, China in 2015. His research interests include computer vision, multi media, and machine learning.

Chao Li received the B.S. degree in mathematics from the University of Information Engineering, China in 1987, the M.S. degree in mathematics from the University of Science and Technology of China in 1990, the Ph.D. degree in engineering from the National University of Defense Technology, China in 2002. He is now a professor with the National University of Defense Technology. His research interests are cryptography, coding theory and information security.