Hindawi
Security and Communication Networks
Volume 2020, Article ID 8828504, 9 pages
https://doi.org/10.1155/2020/8828504

Research Article

Impossible Differential Distinguishers of Two Generalized Feistel Structures

Huili Wang,[1,2] Wenping Ma,[1] Lang Liao,[3] Yushan Li,[4] and Linfeng Zheng[4]

[1] *State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China*
[2] *China Electronic Technology Standardization Institute, Beijing 100076, China*
[3] *Shenzhen Institute of Information Technology, Shenzhen 518172, China*
[4] *Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

Correspondence should be addressed to Huili Wang; wanghuili163e@163.com

Received 7 May 2020; Revised 4 August 2020; Accepted 9 September 2020; Published 22 September 2020

Academic Editor: Luxing Yang

Generalized Feistel structures are widely used in the design of block ciphers. In this paper, we focused on retrieving impossible differentials for two kinds of generalized Feistel structures: CAST256-like structure with Substitution-Permutation (SP) or Substitution-Permutation-Substitution (SPS) round functions (named $\text{CAST256}_{\text{SP}}$ and $\text{CAST256}_{\text{SPS}}$, respectively) and MARS-like structure with SP/SPS round function (named MARS_{SP} and MARS_{SPS}, respectively). Known results show that for bijective round function, CAST256-like structures and MARS-like structures have (m^2-1) and $(2m-1)$ rounds impossible differentials, respectively. By our observation, there existed (m^2+m) rounds impossible differentials in $\text{CAST256}_{\text{SP}}$ and $(3m-3)$ rounds impossible differentials in MARS_{SPS} (this result does not require the P layer to be invertible). When the diffusion layer satisfied some special conditions, $\text{CAST256}_{\text{SPS}}$ had (m^2+m-1) rounds impossible differentials and MARS_{SPS} had $(3m-3)$ rounds impossible differentials.

1. Introduction

The architecture is one of the most important parts of a block cipher. It will directly affect the implementation performance and the round number. Among them, SP structure [1], Feistel structure [2], and generalized Feistel structure [3] are the most often used architectures. The SP structure is a simple and clear block cipher model which is designed to implement Shannon's suggestions of confusion and diffusion. This architecture was adopted by the famous block cipher AES [1]. Besides, many block ciphers, including Camellia, E2, and CLEFIA [4–6] adopt such kind of round functions. Except for the SP structure, the Feistel structure is another important structure, and there are a lot of block ciphers employing this architecture, such as DES, GOST, E2, and Camellia [2, 4, 6, 7]. In [3], Nyberg first introduced generalized Feistel structures. The generalized Feistel structures are generalized forms of the classical Feistel cipher. These structures reserve some advantages of the classical Feistel cipher such as encryption-decryption similarity and flexibility in the design of round functions. A large number of ciphers like CAST256, MARS, CLEFIA [5, 8, 9], etc. use these structures as their architectures.

Impossible differential cryptanalysis was first proposed by Knudsen [10] and Biham et al. [11]. This cryptanalysis uses impossible differentials to discard the wrong keys. This cryptanalysis has been used to attack Skipjack, AES, Camellia, ARIA [11–14], etc. and get many good results. The key step of impossible differential cryptanalysis is to find the longest impossible differentials [15]. For generalized Feistel structures, since only part of the data was processed in each round, there always exist long rounds impossible differentials, and this makes these ciphers vulnerable to impossible differential cryptanalysis.

Since the powerful efficiencies of impossible differential cryptanalysis, many experts work on finding impossible differential distinguisher for several block cipher structures, and lots of remarkable results are achieved. In

[16], u-method was provided by Kim et al. to find impossible differentials of block ciphers structures and was later extended by Bouillaguet et al. [17]; this method uses the inconsistencies of the elements in set u to find impossible differentials. It is worthwhile for the declaration that several longest impossible differentials of some famous block cipher structures are obtained by this method. As is mentioned in [16], for m-dataline CAST256-like structure and m-dataline MARS-like structure, existed the longest round number of impossible differentials are m^2 and $2m$ respectively. However, u-method is too general and some important longer impossible differentials are ignored [12], and the longest differential distinguishers of several architectures like GF-NLFSR [18, 19], Feistel ciphers [15], SPN [20], and MISTY [21] are obtained by other methods. In [22], a new automatic method was proposed to find more impossible differentials.

It is well known that nonzero linear combinations of several linearly independent vectors cannot be zero. Based on this matter of fact, we present some new inconsistencies to construct impossible distinguishers of CAST256-like structures and MARS-like structures with SP and SPS round function. To our knowledge, the best result is m-dataline CAST256-like cipher has m^2 rounds impossible differential distinguisher and m-dataline MARS-like cipher has $2m$ rounds impossible differential distinguisher. Our results show that for m-dataline $\text{CAST256}_{\text{SP}}$ and $\text{CAST256}_{\text{SPS}}$, there exists $(m^2 + m - 1)$ rounds impossible differential distinguishers and for MARS_{SP} and MARS_{SPS}, there exists $(3m - 3)$ rounds impossible differential distinguishers.

This paper is organized as follows: Section 2 introduces some preliminaries. Section 3 focuses on finding impossible differential distinguisher of m-dataline CAST256-like structures with SP/SPS round function. Section 4 works on finding impossible differential distinguisher of m-dataline MARS-like structures with SP/SPS round function. Section 5 concludes this paper.

2. Guidelines for Manuscript Preparation

Throughout this paper, we will use the symbols, described in Table 1.

It is well known that if f is a linear bijection, then $\Delta_f(\Delta x) = f(\Delta x)$, else $\Delta_f(\Delta x)$ may have several possible values; in this case, we can choose any one for further discussion, and we will use $\Delta_f^{(i)}(\Delta x)$ to distinguish them.

Next, we will first describe these two structures, and then lay out some basic definitions and notations.

2.1. CAST256-like Structure. An m-dataline CAST256-like network consists of r rounds, each round is defined as follows.

Let $(X_1^{i-1}, X_2^{i-1}, \ldots, X_m^{i-1})$ be the input of the i-th round, $(X_1^i, X_2^i, \ldots, X_m^i)$ and k_i be the output and the round key of the -th round, resp $(i = 1, 2, \ldots)$.

$(X_1^i, \ldots, X_m^i) = \text{Round}_{\text{CAST256}}(X_1^{i-1}, \ldots, X_m^{i-1})$ is defined as

$$\begin{cases} X_1^i = X_m^{i-1}, \\ X_{j+1}^i = X_j^{i-1}, \quad 1 \le j \le m-1; \\ X_m^i = F\left(k_i, X_m^{i-1}\right) \oplus X_{m-1}^{i-1}, \end{cases} \tag{1}$$

where F is the round function (Figure 1 describes one round of 4-dataline CAST256-like network).

2.2. Mars-like Structure. An m-daaline MARS-like network consists of r rounds; each round is defined as follows.

Let $(X_1^{i-1}, X_2^{i-1}, \ldots, X_m^{i-1})$ be the input of the i-th round, $(X_1^i, X_2^i, \ldots, X_m^i)$ and k_i be the output and the round key of the -th round, resp $(i = 1, 2, \ldots)$.

$(X_1^i, \ldots, X_m^i) = \text{Round}_{\text{MARS}}(X_1^{i-1}, \ldots, X_m^{i-1})$ is defined as

$$\begin{cases} X_j^i = F\left(k_i, X_1^{i-1}\right) \oplus X_{j+1}^{i-1}, \quad 1 \le j \le m-1; \\ X_m^i = X_1^{i-1}, \end{cases} \tag{2}$$

where F is the round function (Figure 2 describes one round of 4-dataline CAST256-like network).

2.3. Notations. According to the definition of round function f, these two cipher structures can be classified into many substructures. Major round functions under study are based on SP structure and SPS structure, which are two basic structures of modern ciphers.

Definition 1 (See [1]) (SP network). Let $S_1, \ldots, S_n$:$\{0,1\}^d \longrightarrow \{0,1\}^d$be nonlinear bijections, P

$$\{0,1\}^{\text{nd}} \longrightarrow \{0,1\}^{\text{nd}} \tag{3}$$

be a linear transformation (*there is no limit that P is a bijection*), $k = (k_1, \ldots, k_n) \in \{0,1\}^{\text{nd}}$ is the round key, then the round function Round_{sp}

$$\{0,1\}^{\text{nd}} \times \{0,1\}^{\text{nd}} \longrightarrow \{0,1\}^{\text{nd}}, \tag{4}$$

of SP *network* (*SPN*) is defined by

$$\text{Round}_{\text{SP}}(x,k) = P\left(S_1(x_1 \oplus k_1), \ldots, S_n(x_n \oplus k_n)\right). \tag{5}$$

We use $\text{CAST256}_{\text{SP}}$ (resp. $\text{CAST256}_{\text{SPS}}$) to denote CAST256-like structure with SP(resp. SPS) type round function and MARS_{SP} (resp. MARS_{SPS}) for MARS-like structure with SP(resp. SPS) type round function.

Definition 2 (See [15]). (χ – function) χ: $F_{2^d}^n \longrightarrow F_2^n$ is defined as

$$\chi(x_1, \ldots, x_n) = (\theta(x_1), \ldots, \theta(x_n)) \tag{6}$$

where θ: $F_{2^d} \longrightarrow F_2$ is defined by

$$\theta(x) = \begin{cases} 1, & \text{if } x \ne 0; \\ 0, & \text{if } x = 0. \end{cases} \tag{7}$$

Let $X = (x_1, \ldots, x_n)$, function χ_s: $F_{2^d}^n \longrightarrow F_2$ is defined by $\chi_S(X) = \theta(x_S)$.

Table 1: Symbols.

$\oplus$	XOR operation
Δx	The XOR difference of x and x'
$\omega(X)$	The number of nonzero components of vector X
$\Delta_f(\Delta x)$	The output difference of f when the given input difference is Δx
$\vert$	Matrices concatenation
$g^{\circ} f(x)$	Composition of function f and g, i.e., $g(f(x))$
$M_{(i)}$	The i-th column of matrix $M = (M_{i,j})_{n\times n}$
$e_{i_1,\ldots,i_r}$	Vector with nonzero values only in the $i_1,\ldots,i_r$-th components
$\mathbf{0}$	n-dimension zero vector
U	Uncertain difference

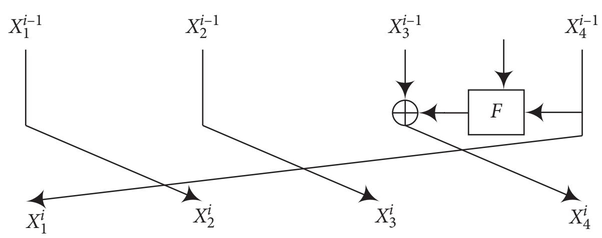

Figure 1: One round of 4-dataline CAST256-like structure.

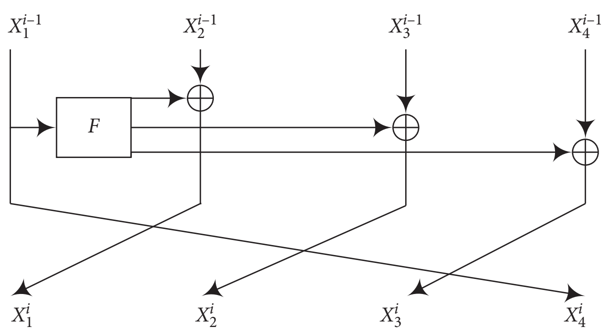

Figure 2: One round of 4-dataline MARS-like structure.

Definition 3 (φ − *function*). Let $1 \le r \le n$; then φ_r: $F_{2^d}^n \longrightarrow F_{2^d}$ is defined as $\varphi_r(x_1,\ldots,x_n) = x_r$.

Definition 4 (See [1]) (differential branch number). Let $f(x) = Mx$ be a linear mapping, where M is a matrix over $GF(2^d)$. Then the differential branch number of f is defined by

$$\mathrm{Br}(f) = \min_{x\neq 0}\{w(x) + w(M\times x)\}. \quad (8)$$

3. Impossible Differential Distinguishers of Cast256-like Structure

3.1. Two Important Differential Characteristics of CAST256-like Structure

Lemma 1 (See [23]). *For the m-dataline CAST256-like structure, any nontrivial differential characteristic of the round function must be with the following form:*

$$\left(\Delta X_1^i,\ldots,\Delta X_{m-1}^i,\Delta X_m^i\right) \longrightarrow \left(\Delta X_m^i,\Delta X_1^i,\ldots,\Delta X_{m-2}^i,\Delta y\oplus X_{m-1}^i\right). \quad (9)$$

And Δy denotes the output difference of the round function. From Lemma 1, we have.

Proposition 1. *Let* (ΔX) *be one round differential characteristic of m-dataline CAST256-like structure, then the following equations hold with probability 1.*

(1) $\Delta X_k^i = \Delta X_{k-1}^{i-1}$ *for* $2 \le k \le m-1$

(2) $\Delta X_1^i = \Delta X_m^{i-1}$

(3) $\Delta X_m^{i-1} = \Delta_F(\Delta X_m^{i-1})\oplus\Delta X_{m-1}^{i-1}$

Proposition 1 can be verified directly from Lemma 1. In the following, we concentrate on two special differences which will help us to find the impossible differentials.

Observation 1. Let $1 \le k_0 \le m-2$ and $(\Delta X_1^{i-1},\ldots,\Delta X_m^{i-1}) \longrightarrow (\Delta X_1^i,\ldots,\Delta X_m^i)$ be the same as in the previous observation, if $\Delta X_k^{i-1} = \begin{cases} O, & k \ne k_0 \\ \alpha, & k = k_0 \end{cases}$, then

$$\Delta X_k^i = \begin{cases} O, & k \ne k_0+1, \\ \alpha, & k = k_0+1. \end{cases} \quad (10)$$

Observation 2. Let $1 \le k_0 \le m-2$ and $(\Delta X_1^{i+m},\ldots,\Delta X_m^{i+m})$ be the output difference of the $(i+m)$ round, if $\Delta X_j^{i+m} = \begin{cases} O, & j \le k_0; \\ U, & k_0 \le j \le m-2; \\ \Delta, & j = m-1; \\ \alpha, & j = m. \end{cases}$, then

$$\Delta X_j^i = \begin{cases} O, & j \le k_0 - 1; \\ U, & k_0 - 1 \le j \le m-2; \\ \Delta\oplus\Delta_F(\alpha), & j = m-1; \\ \alpha, & j = m. \end{cases} \quad (11)$$

We can conclude the following Lemma.

Lemma 2. *For the m-dataline CAST256-like structure, there exists a rounds differential characteristic*

$$(\alpha, O, \ldots, O) \xrightarrow{(2m-1)\text{-round}} (U, \ldots, U, \Delta_{F^2}(\alpha), \Delta_F(\alpha), U) \xrightarrow{1\text{-round}} (U, \ldots, U, \Delta_{F^2}(\alpha), U). \tag{12}$$

from encryption direction and an $m(m-1)$ rounds differential characteristic

$$\left(U, \ldots, U, \bigoplus_{k=1}^{m-1} \Delta_F^{(k)}(\alpha), \alpha\right) \xleftarrow{m(m-1)\text{-round}} (O, \ldots, O, \alpha), \tag{13}$$

from the decryption direction, both with probability 1.

Proof. If the input difference is chosen as $(\Delta X_1^0, \ldots, \Delta X_m^0) = (\alpha, O, \ldots, O)$, according to Observation 1,

$$\left(\Delta X_1^{m-2}, \ldots, \Delta X_m^{m-2}\right) = (O, \ldots, O, \alpha, O). \tag{14}$$

Applying Proposition 1 repeatedly, the following equations must hold

$$\begin{aligned}
\Delta X_{m-1}^{m-1} &= \Delta X_{m-2}^{m-2} = O,\\
\Delta X_m^{m-1} &= \Delta_F\left(\Delta X_m^{m-2}\right) \oplus \Delta X_{m-1}^{m-2} = \alpha,\\
\Delta X_{m-1}^{m} &= \Delta X_{m-2}^{m-1} = \Delta X_{m-3}^{m-2} = O,\\
\Delta X_m^{m} &= \Delta_F\left(\Delta X_m^{m-1}\right) \oplus \Delta X_{m-1}^{m-1} = \Delta_F(\alpha).
\end{aligned} \tag{15}$$

Then we arrive to

$$\begin{aligned}
\Delta X_1^{m+2} &= \Delta X_m^{m+1} = \Delta_F\left(\Delta X_m^{m}\right) \oplus \Delta X_{m-1}^{m} = \Delta_{F^2}(\alpha),\\
\Delta X_{m-1}^{2m-1} &= \Delta X_1^{m+1} = \Delta_F(\alpha),\\
\Delta X_{m-2}^{2m-1} &= \Delta X_{m-1}^{2m} = \Delta X_1^{m+2} = \Delta_{F^2}(\alpha),
\end{aligned} \tag{16}$$

which implies the differential

$$(\alpha, O, \ldots, O) \xrightarrow{(2m-1)\text{-round}} (U, \ldots, U, \Delta_{F^2}(\alpha), \Delta_F(\alpha), U) \xrightarrow{1\text{-round}} (U, \ldots, U, \Delta_{F^2}(\alpha), U) \tag{17}$$

exists.

From the decryption direction, if the output difference is set as $(O, \ldots, O, \alpha)$, then by Observation 2, after m rounds decryption, the input difference (from the encryption direction) is $(O, \ldots, O, \Delta_F(\alpha), \alpha)$, and applying Observation $(2m-2)$ times, we may clarify this Lemma (in Tables 2 and 3, we listed the whole procedure).

3.2. Impossible Differentials for CAST256-like Structure with SP/SPS Round Function

Theorem 1. *Assume A is the permutation layer of $CAST256_{SP}$, where A is a $n \times n$ matrix over $GF(2^d)$. Let $\Omega_1 = i_1, \ldots, i_x$, $\Omega_2 = j_1, \ldots, j_y \subseteq 1, 2, \ldots, n$, if $A_{i_1}, \ldots, A_{i_x}$, $A_{j_1}, \ldots, A_{j_y}$ are linearly independent, then for any n-dimension vector e_{Ω_1}, e_{Ω_2},*

$$\left(e_{\Omega_1}, O, \ldots, O\right) \longrightarrow \left(O, \ldots, O, e_{\Omega_2}\right) \tag{18}$$

is an $m^2 + m - 1$ rounds impossible differential of $CAST256_{SP}$.

Proof. According to Lemma 2, we have $\Delta X_{m-1}^{2m-1} = \Delta_F(\Omega_1) = \Delta_{P\circ S}(e_{\Omega_1})$ from the encryption direction and $\Delta X_{m-1}^{2m-1} = \oplus_{k=1}^{m-1} \Delta_F^{(k)}(\Omega_2) = \oplus_{k=1}^{m-1} \Delta_{P\circ S}^{(k)}(\Omega_2)$ from the decryption direction.

By the definition of e_{Ω_1}, we get

$$\Delta_{P\circ S}\left(e_{\Omega_1}\right) = \Delta_P\left(\Delta_S\left(e_{\Omega_1}\right)\right) = \bigoplus_{u=1}^{x} \varphi_u\left(\Delta_S\left(e_{\Omega_1}\right)\right) \times A_{(i_u)}. \tag{19}$$

Similarly,

$$\bigoplus_{k=1}^{m-1} \Delta_{P\circ S}\left(e_{\Omega_2}\right) = \bigoplus_{k=1}^{m-1} \Delta_P\left(\Delta_S^{(k)}\left(e_{\Omega_2}\right)\right) = P \bigoplus_{k=1}^{m-1} \Delta_S^{(k)}\left(e_{\Omega_2}\right) = A \times \left(\bigoplus_{k=1}^{m-1} \Delta_S^{(k)}\left(e_{\Omega_2}\right)\right) = \bigoplus_{v=1}^{y} \varphi_v\left(\bigoplus_{k=1}^{m-1} \Delta_S^{(k)}\left(e_{\Omega_2}\right)\right) \times A_{(j_v)}. \tag{20}$$

Since $A_{i_1}, \ldots, A_{i_x}$, $A_{j_1}, \ldots, A_{j_y}$ are linearly independent and $\Delta_S(e_{i_u}) \neq 0$, we have

$$\left(\bigoplus_{u=1}^{x} \varphi_u\left(\Delta_S\left(e_{\Omega}\right)\right) \times A_{(i_u)}\right) \oplus \left(\bigoplus_{v=1}^{y} \varphi_v\left(\bigoplus_{k=1}^{m-1} \Delta_S^{(k)}\left(e_{\Omega_2}\right)\right) \times A_{(j_v)}\right) \neq 0. \tag{21}$$

This indicates $\Delta_{P\circ S}(e_{\Omega_1}) \neq \oplus_{k=1}^{m-1} \Delta_{P\circ S}^{k}(e_{\Omega_2})$, which means $(e_{\Omega_1}, O, \ldots, O) \longrightarrow (O, \ldots, O, e_{\Omega_2})$ is an $(m^2 + m - 1)$ rounds impossible differential of $CAST256_{SP}$.

For most designs of permutation layer, we can easily find these $i_1, \ldots, i_x$, $j_1, \ldots, j_y$, which satisfy the condition of Theorem 1.

Corollary 1. *Assume A is the diffusion layer of $CAST256_{SP}$, if A is a $n \times n$ invertible matrix, $\Omega_1 = i_1, \ldots, i_x$, $j_1, \ldots, j_y \subseteq 1, 2, \ldots, n$ and $\Omega_1 \cap \Omega_2 = \varnothing$, then for any n-dimension vector e_{Ω_1}, e_{Ω_2}, $(e_{\Omega_1}, O, \ldots, O) \longrightarrow (O, \ldots, O, e_{\Omega_2})$ is an $(m^2 + m - 1)$ rounds impossible differential of $CAST256_{SP}$.*

TABLE 2: $(2m-1)$ rounds differential characteristics of the m-dataline CAST256-like structure from the encryption direction.

Round/output diff↓	α	O	O	...	OOtextbf0	
1	O	α	O	...	O	O
...				...		
$m-1$	O	O	O	...	O	α
m	α	O	O	...	O	$\Delta_F(\alpha)$
$m+1$	$\Delta_F(\alpha)$	α	O	...	O	$\Delta_{F^2}(\alpha)$
...				...		
$2m-1$	**U**	**U**	**U**	...	$\Delta_F(\alpha)$	α
$2m$	**U**	**U**	**U**	...	$\Delta_{F^2}(\alpha)$	**U**

TABLE 3: $m(m-1)$ rounds differential characteristics of the m-dataline CAST256-like structure from the decryption direction.

1	**U**	**U**	**U**	...	$\oplus_{k=1}^{m-1}\Delta_F^{(k)}(\alpha)$	α
2	α	**U**	**U**	...	**U**	$\oplus_{k=1}^{m-2}\Delta_F^{(k)}(\alpha)$
...				...		
$m(m-3)+1$	O	O	O	...	$\oplus_{k=1}^{2}\Delta_F^{(k)}(\alpha)$	α
...				...		
$m(m-2)+1$	O	O	O	...	$\Delta_F^{(1)}(\alpha)$	α
...				...		
$m(m-1)$	O	O	O	...	α	O
Round/input diff↑	O	O	O		O	α

By considering the $2m$ rounds differential proposed in Lemma 2, we can find an m^2+m round impossible differential. And the result is concluded as follows.

Theorem 2. *Assume $n\times n$ matrix A is the permutation layer of CAST256$_{SP}$ and $Br(A)>2$, then for any n-dimension vector α, if $w(\alpha)=1$, then $(\alpha,O,\ldots,O)\longrightarrow(O,O,\ldots,\alpha)$ is an (m^2+m) rounds impossible differential of CAST256$_{SP}$.*

Proof. Let the input and output difference of (m^2+m-1) rounds CAST256$_{\mathrm{SP}}$ be $(\alpha,O,\ldots,O)$ and $(O,\ldots,O,\alpha)$, respectively. By Lemma 2, we can conclude that from the encryption direction, the difference of the 2nd left most branch of $2m$ round is $\Delta_{P^\circ S^\circ P^\circ S}(\alpha)$, while from the decryption direction, this difference is $\oplus_{k=1}^{m-1}\Delta_{P^\circ S}^{(k)}(\alpha)$.

If differential $(\alpha,O,\ldots,O)\overset{m(m-1)\text{-round}}{\longleftarrow}(O,\ldots,O,\alpha)$ is possible, then equation is possible; then equation

$$\Delta_{P^\circ S^\circ P^\circ S}(\alpha)\oplus\left(\bigoplus_{k=1}^{m-1}\Delta_{P^\circ S}^{(k)}(\alpha)\right)=A\times\left(\Delta_{S^\circ P^\circ S}(\alpha)\oplus\left(\oplus_{k=1}^{m-1}\Delta_S^{(k)}(\alpha)\right)\right)=0 \tag{22}$$

is possible.

Since for any $1\le k\le m-1$, $\chi(\Delta_S^{(k)}(\alpha))=\chi(\alpha)$, so $w(\oplus_{k=1}^{m-1}\Delta_S^{(k)}(\alpha))$ is at most 1. We also notice $w(\Delta_{S^\circ P^\circ S}(\alpha))\ge\mathrm{Br}(A)-w(\Delta_s(\alpha))>1$; thus, $\Delta_{S^\circ P^\circ S}(\alpha)\oplus(\oplus_{k=1}^{m-1}\Delta_S^{(k)}(\alpha))$, which means that $(\alpha,O,\ldots,O)\longrightarrow(O,O,\ldots,\alpha)$ is an (m^2+m) rounds impossible differential.

For CAST256$_{\mathrm{SPS}}$, we have similar results.

Theorem 3. *Assume $n\times n$ matrix A is the diffusion layer of CAST256$_{SPS}$, if A has entry "0", then there exists (m^2+m-1) rounds impossible differentials of CAST256$_{SPS}$.*

Proof. Without loss of generality, we can assume that there exists $1\le i,l,j\le n$, such that $A_{l,i}\ne0$ and $A_{l,i}=0$. Let the input and output difference of (m^2+m-1) rounds CAST256$_{\mathrm{SPS}}$ be $(e_i,O,\ldots,O)$ and $(O,\ldots,O,e_j)$, respectively. Since $\Delta X_{m-1}^{2m-1}=\Delta_F(e_i)=\oplus_{k=1}^{m-1}\Delta_F^{(k)}(e_j)$ and $F=S^\circ P^\circ S$, we have

$$\begin{aligned}\Delta_{S^\circ P^\circ S}(e_i)&=\Delta_S(\Delta_P(\Delta_S(e_i)))=\Delta_S(A\times(\Delta_S(e_i)))\\&=\Delta_S\big(\varphi_i(\Delta_S(e_i))\times A_{(i)}\big),\\\bigoplus_{k=1}^{m-1}\Delta_{S^\circ P^\circ S}^{(k)}\big(e_j\big)&=\bigoplus_{k=1}^{m-1}\Delta_S^{(k)}\Big(\varphi_j\big(\Delta_S^{(k)}\big(e_j\big)\big)\times A_{(j)}\Big).\end{aligned} \tag{23}$$

For $A_{l,i}\ne0$, we have $\chi_l(A_{(i)})\ne0$, since S layer are parallel bijections and $\varphi_i(e_i)\ne0$, we may obtain $\varphi_i(\Delta_S(e_i))\ne0$, so $\chi(\varphi_i(\Delta_S(e_i))\times A_{(i)})=\chi(A_{(i)})$. And for $\chi_l(A_{(i)}\ne0)$, we have

$$\chi_l(\varphi_i(\Delta_S(e_i)))\times A_{(i)}=\chi_l\big(A_{(i)}\big)=1, \tag{24}$$

so we conclude

$$\chi_l(\Delta_{S^\circ P^\circ S}(e_i))=\chi_l\big(\Delta_S\big(\varphi_i(\Delta_S(e_i))\times A_{(i)}\big)\big)=\chi_l\big(\varphi_i(\Delta_S(e_i))\times A_{(i)}\big)=1. \tag{25}$$

For $A_{l,i}=0$, we have $\chi_l(A_{(i)})=0$, which implies $\chi_l(\varphi_j(\Delta_S^{(k)}(e_j))\times A_{(j)})=0$; thus, the two equations below hold:

$$\begin{aligned}&\chi_l\Big(\Delta_S^{(k)}\Big(\varphi_j\Big(\Delta_S^{(k)}\big(e_j\big)\Big)\times A_{(j)}\Big)\Big)=0,\\&\chi_l\left(\bigoplus_{k=1}^{m-1}\Delta_S^{(k)}\Big(\varphi_j\Big(\Delta_S^{(k)}\big(e_j\big)\Big)\times A_{(j)}\Big)\right)=0.\end{aligned} \tag{26}$$

This means $\Delta X_{m-1}^{2m-1}=\Delta_{S^\circ P^\circ S}(e_i)\ne\oplus_{k=1}^{m-1}\Delta_{S^\circ P^\circ S}\ (e_j)=\Delta X_{m-1}^{2m-1}$, which leads contradiction. This implies $(e_i,O,\ldots,O)\longrightarrow(O,\ldots O,e_j)$ is an (m^2+m-1) rounds impossible differential of CAST256$_{\mathrm{SPS}}$.

Now we consider a special case, when permutation layer is designed as a binary matrix.

Corollary 2. *Assume A is the permutation layer of CAST 256$_{SPS}$, where A is a $n\times n$ binary matrix with $\mathrm{rank}(A)\ge2$; then for some $1\le i,j\le n$, there exists (m^2+m-1) rounds impossible differential $(e_i,O,\ldots,O)\longrightarrow(O,\ldots O,e_j)$, where $\mathrm{rank}(A)$ denotes the rank of matrix A.*

Proof. Since $\mathrm{rank}(A)\ge2$, we know there exist some $1\le i,j,l\le n$, such that $A_{(i)}\ne A_{(j)}$ and $A_{l,i}\ne A_{l,j}$. This means $\begin{cases}A_{l,i}=1\\A_{l,j}=0\end{cases}$ or $\begin{cases}A_{l,i}=0\\A_{l,j}=1\end{cases}$. Thus, by Theorem 3, we can conclude the result.

Corollary 2 indicates that for binary permutation layer, if its rank exceeds 2, then we can find such impossible differentials. Obviously, this condition is compatible for almost every design.

4. Impossible Differential Distinguishers of MARS-like Structure

4.1. Two Important Differential Characteristics of MARS-like Structure. The following lemma is trivial.

Lemma 3. *For the m-dataline MARS-like cipher, any nontrivial differential characteristic of the round function must be with the form* $(\Delta X_1^i, \ldots, \Delta X_{m-1}^i, \ \Delta X_m^i) \longrightarrow (\Delta X_2^i \oplus \Delta y, \ldots, \Delta X_m^i \oplus \Delta y, \Delta X_1^i)$, *and* Δy *denotes the output difference of the round function.*

From Lemma 3, we can verify the properties as below.

Proposition 2. *Let* $(\Delta X_1^i, \ldots, \Delta X_{m-1}^i, \ \Delta X_m^i) \longrightarrow (\Delta X_2^i \oplus \Delta y, \ldots, \Delta X_m^i \oplus \Delta y, \Delta X_1^i)$ *be one round differential characteristic of m-dataline MARS-like structure, then we have*

(1) $\Delta X_j^{i+1} = \Delta X_{j+1}^i \oplus \Delta_F(\Delta X_1^i)$ *for* $1 \le j \le m-1$

(2) $\Delta X_m^{i+1} = \Delta X_1^i$

Observation 3. Let $1 \le r \le m-1$, then for the m-dataline MARS-like structure, there exists the following 1 round differential characteristic with probability 1:

$$(\Delta x, \ldots, \Delta x, \Delta t_1, \ldots, \Delta t_{m-r}) \longrightarrow (\Delta x \oplus \Delta, \ldots, \Delta x \oplus \Delta, \Delta t_1 \oplus \Delta, \ldots, \Delta t_{m-r} \oplus \Delta, \Delta x), \quad (27)$$

where $\Delta = \Delta_F(\Delta x)$.

Observation 4. Let $1 \le k_0 \le m-1$ and $(\Delta X_1^i, \ldots, \Delta X_m^i) \longrightarrow (\Delta X_1^{i+1}, \ldots, \Delta X_m^{i+1})$ be the same as in the previous propositions; following this, if

$$\Delta X_k^{i+1} = \begin{cases} O, & k \ne k_0; \\ \alpha, & k = k_0, \end{cases} \quad (28)$$

then

$$\Delta X_k^{i} = \begin{cases} O, & k \ne k_0+1; \\ \alpha, & k = k_0+1. \end{cases} \quad (29)$$

Based on these two Observations, we can conclude the Lemma below.

Lemma 4. *For the m-dataline MARS-like structure, there exists a* $(2m-3)$ *rounds differential characteristic* $(O, \ldots, O, \alpha) \longrightarrow^{(2m-3)round} (A, A, U, \ldots, U, U)$ *from encryption direction and an m rounds differential characteristic* $(\alpha, \Delta_F(\alpha), \Delta_F(\alpha), \ldots, \Delta_F(\alpha)) \overset{mround}{\longleftarrow} (\alpha, O, \ldots, O)$ *from the decryption direction, both with probability 1, where denotes one fixed difference and denotes some uncertain difference(s).*

Proof. Let $(\Delta X_1^0, \ldots, \Delta X_m^0) = (O, \ldots, O, \alpha)$ be the input difference, then according to Proposition 3, after $(m-1)$ rounds cascade, the output difference is turned into $(\Delta X_1^{m-1}, \ldots, \Delta X_m^{m-1}) = (\alpha, O, \ldots, O)$, then by Proposition 2, it holds $\Delta X_1^m = \cdots = \Delta X_{m-1}^m$ applying Proposition 3 recursively, we have $\Delta X_1^{2m-3} = \Delta X_2^{2m-3}$.

From the decryption direction, if the output difference is chosen as $(\Delta X_1^m, \Delta X_2^m, \ldots, \Delta X_m^m) = (\alpha, O, \ldots, O)$, then by Observation 4, we have $(\Delta X_1^1, \Delta X_2^1, \ldots, \Delta X_m^1) = (O, \ldots, O, \alpha)$. According to Proposition 2, we may obtain $(\Delta X_1^0, \Delta X_2^0, \ldots, \Delta X_m^0) = (\alpha, \Delta_F(\alpha), \Delta_F(\alpha), \ldots, \Delta_F(\alpha))$ (in Tables 4 and 5, we listed the whole procedure).

4.2. Retrieving Impossible Differential for MARS-Like Structure with SP/SPS Round Function. Before we start this section, we will introduce the definition of collect set.

Definition 5. (*collect set*) Let M be an $s \times t$ matrix over $GF(2^d)$, $x = (x_1, \ldots, x_t)$ is a binary vector. Then the *collect set* $\mathrm{Col}(x, M)$ is defined as $\mathrm{Col}(x, M) = \{M_{(i)}: x_i \ne 0, 1 \le i \le t\}$, the *characteristic function* of $\mathrm{Col}(x, M)$ is defined as

$$\mathrm{Ch}(\mathrm{Col}(x, M)) = \begin{cases} 1, & \text{the vectors in } \mathrm{Col}(x, M) \text{ are linearly independent;} \\ 0, & \text{the vectors in } \mathrm{Col}(x, M) \text{ are linearly dependent.} \end{cases} \quad (30)$$

The *pattern* of $\mathrm{Col}(x, M)$ is defined as

$$\mathrm{Pat}(\mathrm{Col}(x, M)) = \left\{\chi(M \times y): \ y = (y_1, \ldots, y_t)^T, y_i \in GF\left(2^d\right), \chi(y) = x\right\}. \quad (31)$$

Theorem 4. *Assume* $n \times n$ *matrix* A *over* $GF(2^d)$ *is the permutation layer of* $MARS_{SP}$, *if there exists nonzero n-dimension vector* Δx *over* $GF(2^d)$ *such that* $Ch(Col((\chi(\Delta x) \mid \chi(\Delta x)), (A \mid E))) = 1$ *then* $(0, \ldots, 0, y) \longrightarrow (\Delta x, 0, \ldots, 0)$ *is a* $(3m-3)$ *rounds impossible differential of* $MARS_{SP}$, *where y represents any nonzero vector.*

Proof. By Lemma 4 we have

Table 4: The (2m-3) rounds differential characteristics of the m-dataline MARS-like structure from the encryption direction $\Delta_i = \Delta_F(\Delta_{i-1} \oplus \Delta_{i-1})$ for $1 \le i \le m-1$ and $\Delta_0 = \Delta_0 = \Delta_F(\alpha)$.

Round/output diff↓	O	O	...	O	α	O
1						
...			...			
$m-1$	α	O	...	O	O	O
m	Δ_0	Δ_0	...	Δ_0	Δ_0	α
$m+1$	Δ_1	Δ_1	...	Δ_1	**U**	Δ_0
...			...			
$2m-3$	Δ_{m-3}	Δ_{m-3}	...	**U**	**U**	Δ_{m-4}

Table 5: m rounds differential characteristics of the m-dataline MARS-like structure from the decryption direction.

1	α	$\Delta_F(\alpha)$	$\Delta_F(\alpha)$	...	$\Delta_F(\alpha)$	$\Delta_F(\alpha)$
...	O	O	O	...	O	α
$m-1$				...		
m	O	α	O	...	O	O
Round/input diff↑	α	O	O		O	O

$$\begin{cases} \Delta X_1^{2m-3} = \Delta x, \\ \Delta X_2^{2m-3} = \Delta_{P^\circ S}(\Delta x) = A \times \Delta_S(\Delta x), \end{cases} \tag{32}$$

from the decryption direction.

We assume $A \times \Delta_S(\Delta x) = \Delta x$, then

$$(A \mid E) \times \begin{pmatrix} \Delta_S(\Delta x) \\ \Delta x \end{pmatrix} = 0. \tag{33}$$

This indicates $\mathrm{Col}(\chi(\Delta_S(\Delta x)) \mid \chi(\Delta x), A \mid E)$ are linearly dependent, which is contradictory with $Ch(\mathrm{Col}((\chi(\Delta x) \mid \chi(\Delta x)), (A \mid E))) = 1$. So $A \times \Delta_S(\Delta x) \neq \Delta x$, i.e., $\Delta X_1^i \neq \Delta X_2^i$. However, by Lemma 4, we have from the encryption direction, and this leads to a contradiction. Thus $(O, \ldots, O, y) \longrightarrow (\Delta x, O, \ldots, O)$ is an impossible differential of $\mathrm{MARS_{SP}}$.

Corollary 3. *Assume $n \times n$ matrix A over $GF(2^d)$ is the permutation layer of $MARS_{SP}$, if the branch number of A is $Br(A)$, then for any nonzero n-dimension vector Δx over such that $w(\Delta x) < (D_A/2)$, then $(O, \ldots, O, y) \longrightarrow (\Delta x, O, \ldots, O)$ is a $(3m-3)$ rounds impossible differential of $MARS_{SP}$, where y represents any nonzero vector.*

Proof. According to Definition 4, for any $w(\Delta x) < (\mathrm{Br}(A)/2)$, $w(A \times \Delta_S(\Delta x)) \ge \mathrm{Br}(A) - w(\Delta x) > (\mathrm{Br}(A)/2)$ which implies $A \times \Delta_S(\Delta x) \neq \Delta x$; thus, $(O, \ldots, O, y) \longrightarrow (\Delta x, O, \ldots, O)$ is an impossible differential of $\mathrm{MARS_{SP}}$.

Theorem 5. *Assume $n \times n$ matrix A over $GF(2^d)$ is the permutation layer of $MARS_{SPS}$, if there exists nonzero n-dimension vector Δx over $GF(2^d)$ such that $\chi(\Delta x) \notin Pat(Col(\chi(\Delta x), A))$ then $(O, \ldots, O, y) \longrightarrow (\Delta x, O, \ldots, O)$ is an $(3m-3)$ rounds impossible differential of $MARS_{SPS}$, where y represents any nonzero vector.*

Proof. By Lemma 4 we have,

$$\begin{cases} \Delta X_1^i = \Delta x, \\ \Delta X_2^i = \Delta_{S^\circ P^\circ S}(\Delta x) = \Delta_S(A \times \Delta_S(\Delta x)), \end{cases} \tag{34}$$

from the decryption direction.

Since $\chi(\Delta_S(A \times (\Delta_S(\Delta x)))) = \chi(A \times (\Delta_S(\Delta x))) \in \mathrm{Pat}(\mathrm{Col}(\chi(\Delta x), A))$ and $\chi(\Delta x) \notin \mathrm{Pat}(\mathrm{Col}(\chi(\Delta x), A))$, we can conclude $\Delta X_1^{2m-3} \neq \Delta X_2^{2m-3}$. Thus, $(O, \ldots, O, y) \longrightarrow (\Delta x, O, \ldots, O)$ is a $(3m-3)$ rounds impossible differential of $\mathrm{MARS_{SPS}}$.

According to Theorem 5, the case that the binary matrix employment is characterized as follows.

Corollary 4. *Assume $n \times n$ binary matrix A is the diffusion layer of $MARS_{SPS}$, if exists $1 \le i_1 < i_2 \le n$ and $1 \le j_1 < j_2 \le n$, such that $\{i_1, i_2\} \neq \{j_1, j_2\}$ and*

$$\begin{cases} A_{i_1,j_1} = 0, \\ A_{i_1,j_2} \neq 0, \\ A_{i_2,j_1} \neq 0, \\ A_{i_2,j_2} = 0, \end{cases} \tag{35}$$

then for any e_{j_1,j_2} and nonzero vector y, $(O, \ldots, O, y) \longrightarrow (e_{j_1,j_2}, O, \ldots, O)$ is a $(3m-3)$ rounds impossible differential of $MARS_{SPS}$.

Proof. We have

$$\varphi_i\left(A \times \left(\Delta_S\left(e_{j_1,j_2}\right)\right)\right) = \bigoplus_{k=1}^{n} A_{i,k} \times \varphi_k\left(\Delta_S\left(e_{j_1,j_2}\right)\right) = \bigoplus_{k \in \{j_1,j_2\}} A_{i,k} \times \varphi_k\left(\Delta_S\left(e_{j_1,j_2}\right)\right). \tag{36}$$

Which tells $\chi_{i_1}(\Delta_S(A \times (\Delta_S(\Delta x)))) = \chi_{i_2}(\Delta_S(A \times (\Delta_S(\Delta x)))) = 1$. However, by the definition of $e_{\{j_1,j_2\}}$, we have www and $\{i_1, i_2\} \neq \{j_1, j_2\}$. Thus, $\chi(e_{\{j_1,j_2\}}) \notin \mathrm{Pat}(\mathrm{Col}(\chi(e_{\{j_1,j_2\}}), A))$.

Compared with other designs, binary diffusion layer has an obvious advantage in implementation and thus is a very common design, and for this case, the conditions of Corollary 4 are satiable for most of the time.

For $\mathrm{MARS_{SPS}}$, we can tell that if $(\Delta X_1^{3m-3}, .., \Delta X_m^{3m-3}) = (\Delta X, O, \ldots, O)$, then $\Delta X_1^{2m-3} = \Delta x$ and $\Delta X_2^{2m-3} = \Delta_{S^\circ P^\circ S}(\Delta x)$. One can see $\Delta X_1^{2m-3} = \Delta X_2^{2m-3}$ can be represented by $\Delta_S[P(\Delta_S(\Delta x))] = \Delta x$. Notice

$w(\Delta_S[P(\Delta_S(\Delta x))]) = w(P(\Delta_S(\Delta x)))$, we can change "$\text{MARS}_{\text{SP}}$" by "$\text{MARS}_{\text{SPS}}$" in Corollary 3.

Corollary 5. *Assume $n \times n$ matrix A over $GF(2^d)$ is the diffusion layer of $MARS_{SPS}$, if the branch number of A is D_A, then for any nonzero n-dimension vector Δx over $GF(2^d)$ such that $w(\Delta x) < (D_A/2)$, then $(O, \ldots, O, y) \longrightarrow (\Delta x, O, \ldots, O)$ is a $(3m-3)$ rounds impossible differential of $MARS_{SPS}$, where y represents any nonzero n-dimension vector.*

5. Conclusion

Generalized Feistel structures are of great importance in modern block cipher design. Evaluating the strength of these structures can help us in constructing a security cipher. Among all the cryptanalysis technologies, impossible differential cryptanalysis is one of the most powerful attacks. This paper provides an improvement in finding the longest impossible differentials for two generalized Feistel structures named the CAST256-like structure and the MARS-like structure.

This paper bridges some links between impossible differentials and linear transformations. We provide some sufficient conditions on the linear transformations. By our results, people may find the possible longer impossible differentials by verifying some properties of the linear transformations. Thus, the properties we list in this paper should be considered carefully when using these two structures.

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 National Key R&D Program of China (2018YFB0803905).

References

[1] J. Daemen and R. Vincent, "The design of rijndael: AES-the advanced encryption standard," in *Information Security and Cryptography*, Springer, Berlin, Germany, 2002.

[2] Data Encryption Standard, *Federal information processing standards publication 46*, Vol. 23, National Bureau of Standards, US Department of Commerce, Gaithersburg, MY, USA, 1977.

[3] K. Nyberg, "Generalized feistel networks," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Kobe, Japan, pp. 91–104, December 1996.

[4] K. Aoki, T. Ichikawa, M. Kanda et al., "Specification of camellia-a 128-bit block cipher," *Specification Version*, vol. 2, 2000.

[5] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-bit blockcipher clefia," in *Proceedings of the International Workshop on Fast Software Encryption*, Springer, Luxembourg, Luxembourg, pp. 181–195, March 2007.

[6] NTT-Nippon Telegraph, *Telephone Corporation: E2: Efficient Encryption Algorithm*, NTT-Nippon Telegraph, Tokyo, Japan, 1998.

[7] R. Aragona, A. Caranti, and M. Sala, "The group generated by the round functions of a gost-like cipher," *Annali di Matematica Pura ed Applicata (1923)*, vol. 196, no. 1, pp. 1–17, 2017.

[8] C Adams, "The cast-256 encryption algorithm," 1999.

[9] C. Burwick, D. Coppersmith, and E. Davignon, "Mars-a candidate cipher for aes. nist aes proposal," 1999.

[10] L. R. Knudsen, "Deal—a 128-bit block cipher," Technical Report 151, University of Bergen, Department of Informatics, Bergen, Norway, 1998.

[11] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," *Journal of Cryptology*, vol. 18, no. 4, pp. 291–311, 2005.

[12] J. Lu, D. Orr, N. Keller, and J. Kim, "New impossible differential attacks on AES," in *Proceedings of the International Conference on Cryptology in India*, Springer, Kharagpur, India, pp. 279–293, December 2008.

[13] J. Sung, S. Lee, J. Lim, S. Hong, and S. Park, "Provable security for the skipjack-like structure against differential cryptanalysis and linear cryptanalysis," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, Springer, Gold Coast, Australia, pp. 274–288, December 2000.

[14] W.-L. Wu, W.-T. Zhang, and D.-G. Feng, "Impossible differential cryptanalysis of reduced-round aria and camellia," *Journal of Computer Science and Technology*, vol. 22, no. 3, pp. 449–456, 2007.

[15] Y. Wei, P. Li, B. Sun, and C. Li, "Impossible differential cryptanalysis on feistel ciphers with sp and sps round functions," in *Proceedings of the International Conference on Applied Cryptography and Network Security*, Springer, Beijing, China, pp. 105–122, June 2010.

[16] J. Kim, S. Hong, J. Sung, S. Lee, J. Lim, and S. Sung, "Impossible differential cryptanalysis for block cipher structures," in *Proceedings of the International Conference on Cryptology in India*, Springer, New Delhi, India, pp. 82–96, December 2003.

[17] C. Bouillaguet, D. Orr, P.-A. Fouque, and G. Leurent, "New insights on impossible differential cryptanalysis," in *Proceedings of the International Workshop on Selected Areas in Cryptography*, Springer, Toronto, Canada, pp. 243–259, August 2011.

[18] R. Li, B. Sun, C. Li, and L. Qu, "Cryptanalysis of a generalized unbalanced feistel network structure," in *Proceedings of the Australasian Conference on Information Security and Privacy*, Springer, Sydney, Australia, pp. 1–18, July 2010.

[19] W. Wu, L. Zhang, L. Zhang, and W. Zhang, "Security analysis of the GF-NLFSR structure and four-cell block cipher," in *Proceedings of the International Conference on Information and Communications Security*, Springer, Beijing, China, pp. 17–31, December 2009.

[20] R. Li, B. Sun, and C. Li, "Impossible differential cryptanalysis of SPN ciphers," *IET Information Security*, vol. 5, no. 2, pp. 111–120, 2011.

[21] R. Li, C. Li, J. Su, and B. Sun, "Security evaluation of misty structure with SPN round function," *Computers & Mathematics with Applications*, vol. 65, no. 9, pp. 1264–1279, 2013.

[22] S. Wu and M. Wang, "Automatic search of truncated impossible differentials for word-oriented block ciphers," in *Proceedings of the International Conference on Cryptology in India*, Springer, Kolkata, India, pp. 283–302, December 2012.

[23] N. Wang, C. Jin, and Y. Li, "The differential provable security analysis of a kind of unbalanced feistel networks," *Journal of Electronics and Information Technology*, vol. 27, no. 6, pp. 870–873, 2005.