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 Zheng4

1State Key Laboratory of Integrated Services Networks, Xidian University, Xi’an 710071, China
2China Electronic Technology Standardization Institute, Beijing 100076, China
3Shenzhen Institute of Information Technology, Shenzhen 518172, China
4Chongqing 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

Copyright © 2020 Huili Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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 CAST256SP and CAST256SPS, respectively) and MARS-like structure with SP/SPS round function (named MARSSP and MARSSPS, 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 CAST256SP and \((3m - 3)\) rounds impossible differentials in MARSSPS (this result does not require the P layer to be invertible). When the diffusion layer satisfied some special conditions, CAST256SPS had \((m^2 + m - 1)\) rounds impossible differentials and MARSSPS 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.
CAST256-like structures and MARS-like structures with tendencies to construct impossible distinguishers of several linearly independent vectors cannot be zero. Based on former work [15], SPN [20], and MISTY [21] are obtained by ignoring [12], and the longest differential distinguishers of and some important longer impossible differentials are 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 SP 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 CAST256 and CAST256SP, there exists $(m^2 + m - 1)$ rounds impossible differential distinguishers and for MARS and MARS SP, 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 $\Delta_{p}(f(\Delta x)) = f(\Delta x)$, else $\Delta_{p}(\Delta x)$ may have several possible values; in this case, we can choose any one for further discussion, and we will use $\Delta_{p}(\Delta x)$ 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 $(X_{i-1}^{1}, X_{i-1}^{2}, \ldots, X_{i-1}^{m})$ be the input of the $i$-th round, $(X_{i}^{1}, X_{i}^{2}, \ldots, X_{i}^{m})$ and $k_{i}$ be the output and the round key of the $i$-th round, resp $(i = 1, 2, \ldots)$.

$$(X_{i}^{1}, \ldots, X_{i}^{m}) = \text{Round}_{\text{CAST256}}(X_{i-1}^{1}, \ldots, X_{i-1}^{m})$$

is defined as

$$\begin{cases}
X_{i}^{1} = X_{i-1}^{m}, \\
X_{i}^{j} = X_{i-1}^{j}, & 1 \leq j \leq m - 1; \\
X_{i}^{m} = F(k_{i}, X_{i-1}^{1}) \oplus X_{i-1}^{m-1},
\end{cases}$$

(1)

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

### 2.2. Mars-like Structure

An $m$-dataline MARS-like network consists of $r$ rounds; each round is defined as follows.

Let $(X_{i-1}^{1}, X_{i-1}^{2}, \ldots, X_{i-1}^{m})$ be the input of the $i$-th round, $(X_{i}^{1}, X_{i}^{2}, \ldots, X_{i}^{m})$ and $k_{i}$ be the output and the round key of the $i$-th round, resp $(i = 1, 2, \ldots)$.

$$(X_{i}^{1}, \ldots, X_{i}^{m}) = \text{Round}_{\text{MARS}}(X_{i-1}^{1}, \ldots, X_{i-1}^{m})$$

is defined as

$$\begin{cases}
X_{i}^{1} = F(k_{i}, X_{i-1}^{1}) \oplus X_{i-1}^{m}, & 1 \leq j \leq m - 1; \\
X_{i}^{j} = X_{i-1}^{j},
\end{cases}$$

(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 $S_{1}, \ldots, S_{n}: \{0, 1\}^{d} \rightarrow \{0, 1\}^{d}$ be nonlinear bijections, $P: \{0, 1\}^{1} \rightarrow \{0, 1\}^{1}$ be a linear transformation $(there is no limit that $P$ is a bijection), $k = (k_{1}, \ldots, k_{n}) \in \{0, 1\}^{n}$ is the round key, then the round function Round

$$Round_{SP}: \{0, 1\}^{d} \times \{0, 1\}^{n} \rightarrow \{0, 1\}^{d},$$

(4)

of SP network (SPN) is defined by

$$Round_{SP}(x, k) = P(S_{1}(x_{1} \oplus k_{1}), \ldots, S_{n}(x_{n} \oplus k_{n})).$$

(5)

We use CAST256SP (resp. CAST256SPS) to denote CAST256-like structure with SP (resp. SPS) type round function and MARSSP (resp. MARSSPS) for MARS-like structure with SP (resp. SPS) type round function.

#### Definition 2 (See [15]) ($\chi$-function)

$\chi_{i}: F_{2}^{n} \rightarrow F_{2}^{n}$ is defined as

$$\chi(x_{1}, \ldots, x_{n}) = (\theta(x_{1}), \ldots, \theta(x_{n}))$$

(6)

where $\theta: F_{2}^{n} \rightarrow F_{2}$ is defined by

$$\theta(x) = \begin{cases}
1, & if x \neq 0; \\
0, & if x = 0.
\end{cases}$$

(7)

Let $X = (x_{1}, \ldots, x_{n})$, function $\chi_{i}: F_{2}^{n} \rightarrow F_{2}$ is defined by $\chi_{i}(X) = \theta(x_{i})$.  

---

**Table 1.**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F$</td>
<td>Round function</td>
</tr>
<tr>
<td>$S_{i}$</td>
<td>Nonlinear bijections</td>
</tr>
<tr>
<td>$P$</td>
<td>Linear transformation</td>
</tr>
<tr>
<td>$k$</td>
<td>Round key</td>
</tr>
<tr>
<td>$\Delta_{p}$</td>
<td>Difference operator</td>
</tr>
</tbody>
</table>

---

**Figure 1.**

Diagram of CAST256-like network.

**Figure 2.**

Diagram of CAST256SP (resp. CAST256SPS) network.
Table 1: Symbols.

<table>
<thead>
<tr>
<th>Φ</th>
<th>XOR operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Δx</td>
<td>The XOR difference of x and x'</td>
</tr>
<tr>
<td>ω(X)</td>
<td>The number of nonzero components of vector X</td>
</tr>
<tr>
<td>Δf(Δx)</td>
<td>The output difference of f when the given input difference is Δx</td>
</tr>
<tr>
<td></td>
<td>Matrices concatenation</td>
</tr>
<tr>
<td></td>
<td>Composition of function f and g, i.e., g(f(x))</td>
</tr>
<tr>
<td></td>
<td>The i-th column of matrix M = (M_i)_join</td>
</tr>
<tr>
<td></td>
<td>Vector with nonzero values only in the i_1, i_2-th components</td>
</tr>
<tr>
<td></td>
<td>n-dimensional zero vector</td>
</tr>
<tr>
<td></td>
<td>Uncertain difference</td>
</tr>
</tbody>
</table>

(ΔX^i_1, ..., ΔX^i_{m-1}, ΔX^i_m) → (ΔX^i_m, ΔX^i_1, ..., ΔX^i_{m-2}, Δy ^ X^i_{m-1}).  \tag{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. ΔX^k_k = ΔX^k_{k-1} for 2 ≤ k ≤ m - 1
2. ΔX^1_1 = ΔX^1_{m-1}
3. ΔX^m_m = Δ_f(ΔX^m_{m-1})aksiΔX^m_{m-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 ≤ k_0 ≤ m - 2 and (ΔX^j_{i-1}, ..., ΔX^i_m) → (ΔX^j_{i}, ..., ΔX^i_{m}) be the same as in the previous observation, if ΔX^j_{i} = \begin{cases} O, & k \neq k_0 \\ a, & k = k_0 \end{cases}, then

\[ ΔX^j_{i} = \begin{cases} O, & k \neq k_0 + 1 \\ a, & k = k_0 + 1 \end{cases}. \tag{10} \]

Observation 2. Let 1 ≤ k_0 ≤ m - 2 and (ΔX^j_{i+m}, ..., ΔX^i_{m}) be the output difference of the (i + m) round, if

\[ ΔX^j_{i+m} = \begin{cases} O, & j \leq k_0; \\ U, & k_0 \leq j \leq m - 2; \\ Δ, & j = m - 1; \\ a, & j = m. \end{cases} \tag{11} \]

We can conclude the following Lemma.

Lemma 2. For the m-dataline CAST256-like structure, there exists a rounds differential characteristic
(\(a, O, \ldots, O\)) \(\rightarrow\) \((2m - 1)\)-round \((U, \ldots, U, \Delta_{F_1}(a), \Delta_{F_2}(a), U)\) \(\rightarrow\) \(1\)-round \((U, \ldots, U, \Delta_{F_1}(a), U)\). (12)

\[
\begin{align*}
\Delta x_{m-1}^{m-1} &= \Delta x_{m-2}^{m-2} = O, \\
\Delta x_{m-1}^{m-1} &= \Delta x_{m-2}^{m-2} = O,
\end{align*}
\]

Then we arrive to
\[
\begin{align*}
\Delta x_{m-2}^{m} &= \Delta x_{m-1}^{m} = \Delta x_{m-2}^{m} = \Delta F(a), \\
\Delta x_{m-2}^{m} &= \Delta x_{m-1}^{m} = \Delta x_{m-2}^{m} = \Delta F(a),
\end{align*}
\]

which implies the differential
\[
(a, O, \ldots, O) \rightarrow (\alpha, \ldots, \alpha, O, e),
\]

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 \((O, \ldots, O, \Delta F(a), \alpha)\), 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, where \(A\) is a \(n \times n\) matrix over \(GF(2^d)\). Let \(\Omega_1 = i_1, \ldots, i_s\), \(\Omega_2 = j_1, \ldots, j_r\), \(1 \leq i_1 \leq \ldots \leq s\), \(1 \leq j_1 \leq \ldots \leq r\). If \(A_{i_1}, \ldots, A_{i_s}, A_{j_1}, \ldots, A_{j_r}\) are linearly independent, then for any \(n\)-dimension vector \(e_{\Omega_1}, e_{\Omega_2}\),

\[
\begin{align*}
\Delta_{SP}(e_{\Omega_1}) &= \Delta_{SP}(e_{\Omega_2}) = 0, \\
\Delta_{SP}^{m-1}(e_{\Omega_1}) &= \Delta_{SP}^{m-1}(e_{\Omega_2}) = 0,
\end{align*}
\]

Since \(A_{i_1}, \ldots, A_{i_s}, A_{j_1}, \ldots, A_{j_r}\) are linearly independent and \(\Delta_S(e_{\Omega_1}) \neq 0\), we have

\[
\begin{align*}
\frac{\phi_y(e_{\Omega_1})}{\phi_y(e_{\Omega_2})} \left( \Delta_{SP}^{m-1}(e_{\Omega_1}) \right) &\neq 0, \\
\frac{\phi_y(e_{\Omega_1})}{\phi_y(e_{\Omega_2})} \left( \Delta_{SP}^{m-1}(e_{\Omega_1}) \right) &\neq 0.
\end{align*}
\]

This indicates \(\Delta_{SP}(e_{\Omega_1}) \neq \Delta_{SP}(e_{\Omega_2})\), which means \((e_{\Omega_1}, O, \ldots, O) \rightarrow (O, \ldots, O, e_{\Omega_1})\) is an \((m^2 + m - 1)\) rounds impossible differential of CAST256.

**Corollary 1.** Assume \(A\) is the diffusion layer of CAST256, if \(A\) is an \(n \times n\) invertible matrix, \(\Omega_1 = i_1, \ldots, i_s\), \(j_1, \ldots, j_r\), \(1 \leq i_1 \leq \ldots \leq s\), \(1 \leq j_1 \leq \ldots \leq r\), and \(\Omega_1 \cap \Omega_2 = \emptyset\), then for any \(n\)-dimension vector \(e_{\Omega_1}, e_{\Omega_2}, (O, O, \ldots, O) \rightarrow (O, O, \ldots, O)\) is an \((m^2 + m - 1)\) rounds impossible differential of CAST256.
Table 2: (2m−1) rounds differential characteristics of the m-dataine CAST256-like structure from the encryption direction.

<table>
<thead>
<tr>
<th>Round/output diff_{i}</th>
<th>α</th>
<th>O</th>
<th>O</th>
<th>O</th>
<th>OOtexbf0</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>O</td>
<td>α</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m−1</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>α</td>
</tr>
<tr>
<td>m</td>
<td>α</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>Δ_{f}(α)</td>
</tr>
<tr>
<td>m+1</td>
<td>Δ_{f}(α)</td>
<td>α</td>
<td>O</td>
<td>O</td>
<td>Δ_{φ}(α)</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2m−1</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>Δ_{φ}(α)</td>
<td>α</td>
</tr>
<tr>
<td>2m</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>Δ_{φ}(α)</td>
<td>U</td>
</tr>
</tbody>
</table>

Table 3: m(m−1) rounds differential characteristics of the m-dataine CAST256-like structure from the decryption direction.

<table>
<thead>
<tr>
<th>1</th>
<th>U</th>
<th>U</th>
<th>U</th>
<th>...</th>
<th>θ_{k=1}^{m−2}Δ_{f}^{(k)}(α)</th>
<th>α</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>α</td>
<td>U</td>
<td>U</td>
<td>...</td>
<td>U</td>
<td>θ_{k=1}^{m−2}Δ_{f}^{(k)}(α)</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m(m−3)+1</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>...</td>
<td>θ_{k=1}^{m−1}Δ_{f}^{(k)}(α)</td>
<td>α</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m(m−2)+1</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>...</td>
<td>Δ_{φ}^{(1)}(α)</td>
<td>α</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m(m−1)</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>...</td>
<td>α</td>
<td>O</td>
</tr>
</tbody>
</table>

| Round/input diff | O | O | O | O |

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 × n matrix A is the permutation layer of CAST256_{SPS} and Br(A) > 2, then for any n-dimensional vector α, if w(α) = 1, then (α, O, O, ..., O) → (O, O, ..., O) is an (m^2 + m) rounds impossible differential of CAST256_{SPS}.

Proof. Let the input and output difference of (m^2 + m − 1) rounds CAST256_{SPS} be (α, O, O, ..., O) and (O, O, ..., O), respectively. By Lemma 2, we can conclude that from the encryption direction, this difference is θ_{k=1}^{m−1}Δ_{PS}^{(k)}(α).

If differential (α, O, O, ..., O) \( m(m−1) \)-round \( O, O, ..., O \), is possible, then equation is possible; hence equation

\[
Δ_{PS}^{(k)}(α)θ_{k=1}^{m−1}Δ_{PS}^{(k)}(α) = A × Δ_{PS}^{(k)}(α)θ_{k=1}^{m−1}Δ_{PS}^{(k)}(α) = 0
\]

(22)

is possible.

Since for any 1 \( k \leq m−1 \), \( χ(Δ_{PS}^{(k)}(α)) = χ(α) \), so \( w(Δ_{PS}^{(k)}(α)) ≥ Br(A) + w(Δ_{PS}(α)) > 1 \); thus, \( Δ_{PS}^{(k)}(α)θ_{k=1}^{m−1}Δ_{PS}^{(k)}(α) \), which means that (α, O, O, ..., O) → (O, O, ..., O) is an \( m^2 + m \) rounds impossible differential.

For CAST256_{SPS}, we have similar results.

Theorem 3. Assume n×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 \( 1 \leq i, j \leq n \), such that \( A_{ij} ≠ 0 \) and \( A_{ji} = 0 \). Let the input and output difference of \( (m^2 + m − 1) \) rounds CAST256_{SPS} be \( (e_1, O, O, ..., O) \) and \( (O, O, ..., O, e_j) \), respectively. Since \( ΔX_{2m−1}^{m−1} = ΔF(e_i) = e_{φ(i)}^{m−1}Δ_{F}^{(k)}(e_i) \) and \( F = S'PS \), we have

\[
Δ_{SPS}^{m−1}(e_i) = ΔS(ΔF(ΔS(e_i))) = ΔS(ΔF(ΔS(e_i))) = ΔS(φ_{i}(ΔS(e_i)) × A_{ij}),
\]

(23)

For \( A_{ij} ≠ 0 \), we have \( χ_{i}(A_{ij}) ≠ 0 \), since S layer is parallel bijections and \( φ_i(e_i) ≠ 0 \), we may obtain \( φ_i(ΔS(e_i)) ≠ 0 \), so \( φ_i(ΔS(e_i)) × A_{ij} = 0 \). And for \( χ_{i}(A_{ij}) ≠ 0 \), we have

\[
χ_{i}(φ_i(ΔS(e_i))) × A_{ij} = χ_{i}(φ_i(ΔS(e_i)) × A_{ij}) = 1,
\]

(24)

so we conclude

\[
χ_{i}(ΔS(φ_i(ΔS(e_i)) × A_{ij})) = χ_{i}(φ_i(ΔS(e_i)) × A_{ij}) = 1.
\]

(25)

For \( A_{ij} = 0 \), we have \( χ_{i}(A_{ij}) = 0 \), which implies \( χ_{i}(φ_i(ΔS(e_i)) × A_{ij}) = 0 \); thus, the two equations below hold:

\[
χ_i(ΔS(φ_i(ΔS(e_i)) × A_{ij})) = 0,
\]

(26)

\[
χ_i(ΔS(φ_i(ΔS(e_i)) × A_{ij})) = 0.
\]

This means \( ΔX_{2m−1}^{m−1} = ΔS(φ_i(ΔS(e_i)) × A_{ij}) = ΔX_{m−1}^{m−1} \), which leads contradiction. This implies \( e_i, O, ..., O, e_j \) is an \( (m^2 + m − 1) \) rounds impossible differential of CAST256_{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 CAST256_{SPS}, where A is a n×n binary matrix with rank(A) ≥ 2; then for some 1 ≤ i, j ≤ n, there exists \( (m^2 + m − 1) \) rounds impossible differential \( (e_i, O, O, ..., O) → (O, O, ..., O, e_j) \), where rank(A) denotes the rank of matrix A.

Proof. Since rank(A) ≥ 2, we know there exist some \( 1 ≤ i, j ≤ n \), such that \( A_{ij} ≠ 0 \) and \( A_{ji} ≠ A_{ij} \). This means

\[
\begin{align*}
\text{or } A_{ij} & = 0, & A_{ij} & = 1
\end{align*}
\]

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 \( (\Delta X_1, \ldots, \Delta X_{m-1}, \Delta X_m) \rightarrow (\Delta X'_1 \oplus \Delta y, \ldots, \Delta X'_{m-1} \oplus \Delta y, \Delta X'_m) \), and \( \Delta y \) denotes the output difference of the round function.

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

\[
(\Delta x, \ldots, \Delta x, \Delta t_1, \ldots, \Delta t_{m-r}) \rightarrow (\Delta x \oplus \Delta, \ldots, \Delta x \oplus \Delta, \Delta t_1 \oplus \Delta, \ldots, \Delta t_{m-r} \oplus \Delta, \Delta x),
\]

where \( \Delta = \Delta_f(\Delta x) \).

Observation 4. Let \( 1 \leq k_0 \leq m - 1 \) and \( (\Delta X_1', \ldots, \Delta X_m') \rightarrow (\Delta X_1'', \ldots, \Delta X_m'') \) be the same as in the previous propositions; following this, if

\[
\Delta X_k^{i+1} = \begin{cases} O, & k \neq k_0; \\ \alpha, & k = k_0, \end{cases}
\]

then

\[
\Delta X_k^i = \begin{cases} O, & k \neq k_0 + 1; \\ \alpha, & k = k_0 + 1. \end{cases}
\]

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 \( (O, \ldots, O, a) \rightarrow (2m-3)\text{round}(A, A, U, \ldots, U, U) \) from encryption direction and an m rounds differential characteristic \( (a, \Delta_f(a), \Delta_f(a), \ldots, \Delta_f(a)) \rightarrow (a, O, \ldots, O) \) from the decryption direction, both with probability 1, where denotes one fixed difference and denotes some uncertain difference(s).

Proposition 2. Let \( (\Delta X_1', \ldots, \Delta X_{m-1}'', \Delta X'_m) \rightarrow (\Delta X_1''', \ldots, \Delta X_m''') \) be one round differential characteristic of m-dataline MARS-like structure, then we have

1. \( \Delta X_j^{j+1} = \Delta X_j' \oplus \Delta_f(\Delta X_j') \) for \( 1 \leq j \leq m - 1 \)
2. \( \Delta X_m^{m+1} = \Delta X_1'' \)

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

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

From the decryption direction, if the output difference is chosen as \( (\Delta X_1'', \Delta X_2'', \ldots, \Delta X_m'') = (a, O, \ldots, O) \), then by Observation 4, we have \( (\Delta X_1', \Delta X_2', \ldots, \Delta X_m') = (O, \ldots, O, a) \). According to Proposition 2, we may obtain \( (\Delta X_1', \Delta X_2', \ldots, \Delta X_m') = (a, \Delta_f(a), \Delta_f(a), \ldots, \Delta_f(a)) \) (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 \( \text{Col}(x, M) \) is defined as \( \text{Col}(x, M) = \{M(x) \mid x \neq 0, 1 \leq i \leq t \} \). the characteristic function of \( \text{Col}(x, M) \) is defined as

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

The pattern of \( \text{Col}(x, M) \) is defined as

\[
\text{Pat}(\text{Col}(x, M)) = \{\chi(M \times y) : y = (y_1, \ldots, y_t)^T, y_i \in GF(2^d), \chi(y) = x\}.
\]

Theorem 4. Assume \( n \times n \) matrix \( A \) over \( GF(2^d) \) is the permutation layer of MARSSp, if there exists nonzero \( n \)-dimension vector \( \Delta x \) over \( GF(2^d) \) such that \( \text{Ch}(\text{Col}((\chi(\Delta x) \mid \chi(\Delta x)), (A \mid E))) = 1 \) then \( (0, \ldots, 0, y) \rightarrow (\Delta x, 0, \ldots, 0) \) is a \( (3m - 3) \) rounds impossible differential of MARSSp, 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 \( \Delta_i = \Delta_{i,j}(\Delta_{i-1}, a) \) for \( 1 \leq i \leq m-1 \) and \( \Delta_0 = \Delta_{i,j}(a) \).

<table>
<thead>
<tr>
<th>Round/output diff ( \Delta )</th>
<th>O</th>
<th>O</th>
<th>...</th>
<th>O</th>
<th>( \alpha )</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( m-1 )</td>
<td>( \alpha )</td>
<td>O</td>
<td>O</td>
<td>...</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>( m )</td>
<td>( \delta_{\alpha} )</td>
<td>( \delta_0 )</td>
<td>...</td>
<td>( \delta_1 )</td>
<td>( \delta_2 )</td>
<td>( \alpha )</td>
</tr>
<tr>
<td>( m+1 )</td>
<td>( \delta_1 )</td>
<td>( \delta_1 )</td>
<td>...</td>
<td>( \delta_1 )</td>
<td>( U )</td>
<td>( \delta_0 )</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( 2m-3 )</td>
<td>( \delta_{m-3} )</td>
<td>( \delta_{m-3} )</td>
<td>...</td>
<td>( U )</td>
<td>( U )</td>
<td>( \delta_{m-4} )</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Round/input diff ( \Delta )</th>
<th>( \alpha )</th>
<th>O</th>
<th>O</th>
<th>...</th>
<th>O</th>
<th>O</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( m-1 )</td>
<td>O</td>
<td>( \alpha )</td>
<td>O</td>
<td>...</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>( m )</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>...</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
\Delta X_1^{m-3} &= \Delta x, \\
\Delta X_2^{m-3} &= \Delta_{p,s}(\Delta x) = \Delta_x \times \Delta_x, \\
\end{align*}
\]

from the decryption direction.

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

\[
(A \mid E) \times \left( \begin{array}{c}
\Delta_x \\
\Delta_x \\
\end{array} \right) = 0. 
\]  

This indicates \( \text{Col}(\chi(\Delta_x(\Delta x))) \mid \chi(\Delta x), A \mid E) = 1 \). So \( A \times \Delta_x(\Delta x) \neq \Delta x \), \( \Delta x_1 \neq \Delta x_2 \).

However, by Lemma 4, we have from the encryption direction, and this leads to a contradiction. Thus \( (O, \ldots, O, y) \rightarrow (\Delta x, O, \ldots, O) \) is an impossible differential of \( \text{MARS}_{sp} \).

Corollary 3. Assume \( n \times n \) matrix \( A \) over \( GF(2^d) \) is the permutation layer of \( \text{MARS}_{sp} \), if the branch number of \( A \) is \( Br(A) \), then for any nonzero \( n \)-dimension vector \( \Delta x \) over such that \( \omega(\Delta x) < (D_A/2) \), then \( (O, \ldots, O, y) \rightarrow (\Delta x, O, \ldots, O) \) is a \( (3m-3) \) rounds impossible differential of \( \text{MARS}_{sp} \).

Proof. According to Definition 4, for any \( \omega(\Delta x) < (Br(A)/2) \), \( \omega(A \times \Delta_x(\Delta x)) \geq (Br(A) - \omega(\Delta x)) > (Br(A)/2) \) which implies \( A \times \Delta_x(\Delta x) \neq \Delta x \); thus, \( (O, \ldots, O, y) \rightarrow (\Delta x, O, \ldots, O) \) is an impossible differential of \( \text{MARS}_{sp} \).

Theorem 5. Assume \( n \times n \) matrix \( A \) over \( GF(2^d) \) is the permutation layer of \( \text{MARS}_{sp} \), if there exists nonzero \( n \)-dimension vector \( \Delta x \) over \( GF(2^d) \) such that \( \chi(\Delta x) \notin \text{Pat}(\chi(\Delta x), A) \) and \( \Delta x \neq \Delta x \) Pat(\( \chi(\Delta x), A) \), we can conclude \( \Delta x_{1}^{m-3} \neq \Delta x_{2}^{m-3} \). Thus, \( (O, \ldots, O, y) \rightarrow (\Delta x, O, \ldots, O) \) is a \( (3m-3) \) rounds impossible differential of \( \text{MARS}_{sp} \).

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 \( \text{MARS}_{sp} \), if exists \( 1 \leq i_1 < i_2 \leq n \) and \( 1 \leq j_1 < j_2 \leq n \), such that \( \{i_1, i_2\} \neq \{j_1, j_2\} \) and

\[
\begin{align*}
A_{i_1, i_2} &= 0, \\
A_{i_1, i_2} &
eq 0, \\
A_{j_1, j_2} &= 0, \\
A_{j_1, j_2} &
eq 0, \\
A_{i_1, j_2} &= 0, \\
A_{i_1, j_2} &
eq 0,
\end{align*}
\]

then for any \( e_{j_1, j_2} \) and nonzero vector \( y \), \( (O, \ldots, O, y) \rightarrow (e_{j_1, j_2}, O, \ldots, O) \) is a \( (3m-3) \) rounds impossible differential of \( \text{MARS}_{sp} \).

Proof. We have

\[
\varphi_i(A \times \Delta_x(e_{j_1, j_2})) = \prod_{k=1}^{n} A_{i_k} \chi^k(\Delta_x(e_{j_1, j_2})) = \prod_{k \in \{i_1, i_2\}} A_{i_k} \chi^k(\Delta_x(e_{j_1, j_2})).
\]
$w(\Delta_x\{P(\Delta_x\{\Delta\})\}) = w(P(\Delta_x\{\Delta\}))$, we can change “MARS$_{SP}$” by “MARS$_{SPS}$” 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 $\Delta_d$, then for any nonzero $n$-dimension vector $\Delta x$ over $GF(2^d)$ such that $w(\Delta x) < (D_d/2)$, 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**


