Research Article

Revisiting Impossible Differential Distinguishers of Two Generalized Feistel Structures

Xuan Shen,1 Lei Cheng,2 Bing Sun,2 and Jun He3

1College of Information and Communication, National University of Defense Technology, Wuhan 430010, China
2College of Liberal Arts and Sciences, National University of Defense Technology, Changsha 410073, China

Correspondence should be addressed to Jun He; hejun17c@nudt.edu.cn

Received 27 February 2021; Accepted 19 May 2021; Published 1 June 2021

Academic Editor: Stelvio Cimato

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

Impossible differential attack is one of the most effective cryptanalytic methods for block ciphers. Its key step is to construct impossible differential distinguishers as long as possible. In this paper, we mainly focus on constructing longer impossible differential distinguishers for two kinds of generalized Feistel structures which are \( m \)-dataline CAST256-like and MARS-like structures. When their round function takes Substitution Permutation (SP) and Substitution Permutation Substitution (SPS) types, they are called CAST256 SP/CAST256SPS and MARS SP/MARSSPS, respectively. For CAST256 SP/CAST256SPS, the best known result for the length of the impossible differential distinguisher was \( \frac{m^2 + m}{m^2 + m - 1} \) rounds, respectively. With the help of the linear layer \( P \), we can construct \( \frac{m^2 + m + \Lambda_0}{m^2 + m + \Lambda_1} \) rounds impossible differential distinguishers, where \( \Lambda_0 \) and \( \Lambda_1 \) are non-negative numbers if \( P \) satisfies some restricted conditions. For MARS SP, the best known result for the length of the impossible differential distinguisher was \( 3m - 1 \) rounds. We can construct \( 3m \)-round impossible differential distinguishers which are 1 round longer than before. To our knowledge, the results in this paper are the best for the two kinds of generalized Feistel structures.

1. Introduction

Block ciphers are significant elements to construct symmetric cryptographic schemes. To design a block cipher, a proper structure needs to be selected carefully. Popular structures for designing block ciphers are Substitution Permutation Network (SPN) structures [1], Feistel structures [2], and generalized Feistel structures [3]. Since the encryption and decryption of generalized Feistel structures share the same round functions and similar structures, it makes the implementation more flexible and economical. Generalized Feistel structures have many types such as CAST256-like structure [4], MARS-like structure [5], and so on. At the same time, many famous block ciphers take generalized Feistel structures as their architectures, for example, CAST256 [6], MARS [7], and SMS4 [8].

Many effective methods were proposed for evaluating the security of block ciphers in the past decades. Among them, impossible differential attack is one of the most effective methods. It was independently proposed by Knudsen [9] and Biham et al. [10]. So far, impossible differential attack has given exciting works for AES [11], Camellia [12], SMS4 [8], etc. Impossible differential attack has two steps. The first one is to construct an impossible differential distinguisher as long as possible. The second one is to exploit the distinguisher to recover the master key. Thus, constructing long impossible differentials is the core step to make this attack. So far, the most popular method to construct impossible differentials is the miss-in-the-middle method [10]. It obtains contradictions from the middle differences which are encrypted and decrypted with probability 1 for the input difference and the output difference, respectively. If the middle differences cannot be matched with each other, the impossible differential distinguisher is constructed. Moreover, some automatic methods were proposed to construct impossible differentials with the help of computers [13–16].

As far as we know, many works paid attention to constructing impossible differential distinguishers of \( m \)-dataline CAST256-like and MARS-like structures. For \( m \)-dataline CAST256-like structure, when the round
function is any bijective transformation, \( m^2 \)-round impossible differentials were presented by the \( U \) method in [13]. Furthermore, when the round function takes SP type, 19/20-round impossible differentials of \((m = 4)\)-dataline CAST256-like structure were constructed in [17]. Very recently, when the round function takes SP type and SPS type, there existed \((m^2 + m)/(m^2 + m - 1)\)-round impossible differentials, respectively [18].

For \( m \)-dataline MARS-like structure, when the round function is any bijective transformation, (\( 2m - 1 \))-round impossible differentials were presented by the \( U \) method in [13]. This result was improved to (\( 3m - 1 \))-round in [19]. Furthermore, when the round function takes SP type, \( 3m \)-round impossible differentials were found in [5]. Very recently, when the round function takes SPS type, (\( 3m - 3 \))-round impossible differentials were constructed for some constrained linear layer \( P \) [18].

Known results on impossible differentials of \( m \)-dataline CAST256-like and MARS-like structures are presented in Table 1.

\[
\begin{align*}
\Lambda_0 &= \min\{R - 2, m - 3\}, \\
\Lambda_1 &= \min\{R - 3, m - 3\},
\end{align*}
\]

In this paper, we mainly study the impossible differential distinguishers of \( m \)-dataline CAST256-like and MARS-like structures. For these two structures, we construct longer impossible differential distinguishers with the details of the linear transformation \( P \). Note that \( m \geq 4 \) and the linear transformation \( P \) is a bijective mapping throughout this paper. Moreover, \( R \) denotes the primitive index of \( P \). Our contributions are presented below.

1. For \( m \)-dataline CAST256-like structure, when the round function takes SP type (namely, CAST256SP), the previous best result was presented in [18]. They showed that \((m^2 + m)/(m^2 + m - 1)\)-round impossible differentials were constructed for \( B(P) > 2 \), where \( B(P) \) denotes the differential branch number of \( P \). In this paper, we firstly remove the restricted condition and give \((m^2 + m)/(m^2 + m - 1)\)-round impossible differentials for any bijective \( P \). It expands the range of the linear layer \( P \). Furthermore, if \( P \) satisfies the condition that \( R \geq 2 \), \((\Lambda_0 = \min\{R - 2, m - 3\})\)-round impossible differentials are constructed. To satisfy the condition \( R \geq 2 \), some specific linear transformations \( P \) are also presented.

2. For \( m \)-dataline CAST256-like structure, when the round function takes SPS type (namely, CAST256SPS), the previous best result was also presented in [18]. They showed that \((m^2 + m - 1)/(m^2 + m - 2)\)-round impossible differentials were constructed for \( R \geq 2 \). In this paper, if \( P \) satisfies some conditions, \((\Lambda_1 + 1 = \min\{R - 3, m - 3\} + 1)\)-round impossible differentials are constructed. Moreover, some specific linear transformations \( P \) are presented for satisfying the restricted conditions.

3. For \( m \)-dataline MARS-like structure, when the round function takes SPS type (namely, MARSSP), the previous best result of MARSSP was also presented in [19]. They showed that \((3m - 1)/(3m - 3)\)-round impossible differentials were constructed with \( P \) satisfying the bijective condition. In this paper, if \( P \) has 0 element in the diagonal line, we can construct \( 3m \)-round impossible differentials which are 1 round longer than those in [19].

This paper is organized as follows. In Section 2, we give some notations and definitions that will be used in this paper. Then, with the help of \( P \), we construct longer impossible differential distinguishers of \( m \)-dataline CAST256-like and MARS-like structures in Sections 3 and 4, respectively. Finally, Section 5 concludes this paper.

### 2. Preliminary

#### 2.1. Notations

In this section, we give some notations used in this paper (Table 2). Note that all vectors used in our paper are column vectors and \( X_0 \) is the most significant element for a vector \( X = (X_0, X_1, \ldots, X_{n-2}, X_{n-1}) \), where \( X_i \) is defined by the \( i \)-th element of \( X \).

It should be pointed out that when \( F \) is a nonlinear bijective function, \( \Delta_f(\Delta X) \) has many possible output difference values when the input difference \( \Delta X \neq 0 \). Thus, if some \( \Delta_f(\Delta X) \) XORed each other, take \( \Delta_f^0(\Delta X) \) to distinguish them, where \( l \geq 1 \). For example,

\[
\Delta_f(\Delta X) \oplus \Delta_f(\Delta X) = \Delta_f^1(\Delta X) \oplus \Delta_f^2(\Delta X) = \delta_{\Lambda_0}^{\Lambda_1} \Delta_f^0(\Delta X),
\]

in addition, similar to the definition of \( \Delta_f(\Delta X) \), \( \Delta_f(\Delta X) \) is defined by the output difference that \( \Delta X \) propagates after continuous \( t \) rounds of \( F \).

#### 2.2. Definitions

**Definition 1** (SP networks) (see [1]). Let \( S_{0,1}, \ldots, S_{n-1} : \{0, 1\}^d \rightarrow \{0, 1\}^d \) be nonlinear bijections, \( P : F\rightarrow F' \) be the bijective linear layer, and \( k = (k_0, k_1, \ldots, k_{n-1}) \in \{0, 1\}^d \) be the round key. Then, the round function \( \text{Round}_{SP} : \{0, 1\}^d \times \{0, 1\}^d \rightarrow \{0, 1\}^d \) is defined by

\[
\text{Round}_{SP}(x, k) = P(S(x \oplus k), \ldots, S_{n-1}(x_{n-1} \oplus k_{n-1})).
\]
In this paper, the round functions of \( m \)-dataline CAST256-like and MARS-like structures take SP type and SPS type.

**Definition 2** (Hamming weight) (see [20]). Let \( x \) be an \( n \)-dimension vector, and the Hamming weight of \( x \) is defined by

\[
H(x) = \#\{i | x_i \neq 0, i = 0, 1, \ldots, n - 1\}. \tag{5}
\]

According to the definition, \( H(x) = 0 \) is equivalent to \( x = 0 \). It implies that \( H(x) \geq 1 \) when \( x \neq 0 \). Furthermore, \( H(x) = 1 \) is equivalent to \( x = e_i \) for some \( i \).

**Definition 3** (differential branch number) (see [1]). 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

\[
B(f) = \min_{x \neq 0} \{ H(x) + H(Mx) \}. \tag{6}
\]

Note that if \( f \) is a bijective linear mapping, according to the definition, \( B(f) \geq 2 \).

**Definition 4** (characteristic matrix) (see [20]). For \( P = (p_{i,j}) \in F_{2^n}^{2^n} \), denote \( Z \) as the integer ring, and the characteristic matrix of \( P \) is defined as \( P^* = (p_{i,j}^*) \in Z^{m \times n} \), where

\[
p_{i,j}^* = \begin{cases} 0, & p_{i,j} = 0, \\ 1, & p_{i,j} \neq 0. \end{cases} \tag{7}
\]

According to the definition of characteristic matrix, for an SPN cipher, \( p_{i,j}^* = 0 \) means that the \( i \)-th output block of one-round function is independent of the \( j \)-th input block. Generally, let \( (P^*)^j = (q_{i,j})_{m \times n} \) then, \( q_{i,j} = 0 \) means that the \( i \)-th output block of the \( t \)-round SPN cipher is independent of the \( j \)-th input block.

For a matrix \( M, M > 0 \) means that all elements of \( M \) are positive.

**Definition 5** (primitive index of linear transformation) (see [20]). The primitive index of the linear transformation \( P \) is defined as

\[
R = \min \{ t | (P^*)^t > 0, t \in Z^+ \}. \tag{8}
\]

According to the above definition, if \( R \geq 2 \), there exists at least one 0 element in \( (P^*)^t \) for \( 1 \leq t \leq R - 1 \).

3. Revisiting Impossible Differential Distinguishers of \( m \)-Dataline CAST256-Like Structure

In this section, the brief description of \( m \)-dataline CAST256-like structure is first presented. Moreover, the differential propagation rules are investigated from the encryption and decryption directions. Furthermore, when the round function takes SP type and SPS type, respectively, longer impossible differential distinguishers will be constructed for some linear layers \( P \).

3.1. \( m \)-Dataline CAST256-Like Structure. An \( m \)-dataline CAST256-like structure consists of \( r \) rounds, and each round is depicted in Figure 1. Let \( (X_0^{i-1}, X_1^{i-1}, \ldots, X_{m-1}^{i-1}) \) be the input of the \( i \)-th round and \( (X_0^i, X_1^i, \ldots, X_{m-1}^i) \) and \( K^i \) be the output and the round key of the \( i \)-th round, respectively. One-round encryption is defined by

\[
\begin{align*}
X_0^i &= X_{m-1}^{i-1}, \\
X_j^i &= X_{j-1}^{i-1}, & 1 \leq j \leq m - 2, \\
X_{m-1}^i &= F(X_{m-2}^{i-1} @ K^{i-1}) @ X_{m-2}^{i-1},
\end{align*} \tag{9}
\]

where \( F \) is the round function and \( X_{m-2}^j \in F_{2^n}, 0 \leq j \leq m - 1, i \geq 1 \).

To construct impossible differentials, one-round differential propagations from the encryption and decryption directions need to be studied. They are described as follows.

**Proposition 1.** Let \( \Delta X_0^{i-1} \) and \( \Delta X_i^j \) be the \( i \)-th round input difference and output difference of \( m \)-dataline CAST256-like structure. From the encryption direction, one-round differential propagation is given below:

\[
\begin{align*}
\Delta X_0^i &= \Delta X_{m-1}^{i-1}, \\
\Delta X_j^i &= \Delta X_{j-1}^{i-1}, & 1 \leq j \leq m - 2, \\
\Delta X_{m-1}^i &= \Delta F(\Delta X_{m-2}^{i-1} @ \Delta X_{m-2}^{i-1}).
\end{align*} \tag{10}
\]

From the decryption direction, one-round differential propagation is given below:
According to the encryption process of $m$-dataline CAST256-like structure, the above proposition can be proved. In the encryption direction, the input difference $(\alpha, O, O, \ldots, O, O)$ is encrypted $(3m - 3)$ rounds with probability 1 as described in Table 3. Moreover, in the decryption direction, the output difference $(O, O, \ldots, O, O, \beta)$ is decrypted $m(m - 1)$ rounds with probability 1. The differential characteristic is given in Table 4.

From Tables 3 and 4, the following proposition can be obtained.

**Proposition 2.** For $m$-dataline CAST256-like structure, after encrypting $2m + r (0 \leq r \leq m - 3)$ rounds with the input difference $(\alpha, O, O, \ldots, O, O)$, the following differential holds with probability 1:

\[
(\alpha, O, O, \ldots, O, O) \overset{2m + r}{\rightarrow} (?, ?, \ldots, ?, ?, \Delta_{P^{-1}}(\alpha), ?).
\]

(12)

Likewise, after decrypting $m(m - 1)$ rounds with the output difference $(O, O, \ldots, O, O, \beta)$, the following differential holds with probability 1:

\[
(O, O, \ldots, O, O, \beta) \overset{m(m-1)}{\rightarrow} (?, ?, \ldots, ?, ?, \Delta_P^{(0)}(\beta), ?).
\]

(13)

### 3.2. Constructing Impossible Differential Distinguishers of $m$-Dateline CAST256-Like Structure with SP-Type Round Function

When the round function $F$ of $m$-dataline CAST-like structure is made up of SP type, we exploit the details of the linear layer $P$ to construct longer impossible differential distinguishers. Firstly, two lemmas are presented as follows.

**Lemma 1.** If $G$ is a bijective mapping, $\Delta_G(\alpha) = O$ if and only if $\alpha = \Delta$.

### Table 3: $(3m - 3)$-round differential characteristic of $m$-dataline CAST256-like structure from the encryption direction.

<table>
<thead>
<tr>
<th>Round</th>
<th>$\alpha$</th>
<th>$O$</th>
<th>$O$</th>
<th>$O$</th>
<th>$O$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\Delta_1$</td>
<td>$\Delta_2$</td>
<td>$\Delta_3$</td>
<td>$\Delta_4$</td>
<td>$\Delta_5$</td>
</tr>
<tr>
<td>2</td>
<td>$\Delta_1$</td>
<td>$\Delta_2$</td>
<td>$\Delta_3$</td>
<td>$\Delta_4$</td>
<td>$\Delta_5$</td>
</tr>
<tr>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
</tr>
<tr>
<td>$m - 1$</td>
<td>$\Delta_1$</td>
<td>$\Delta_2$</td>
<td>$\Delta_3$</td>
<td>$\Delta_4$</td>
<td>$\Delta_5$</td>
</tr>
<tr>
<td>$m + 1$</td>
<td>$\Delta_1$</td>
<td>$\Delta_2$</td>
<td>$\Delta_3$</td>
<td>$\Delta_4$</td>
<td>$\Delta_5$</td>
</tr>
</tbody>
</table>

### Table 4: $m(m - 1)$-round differential characteristic of $m$-dataline CAST256-like structure from the decryption direction.

<table>
<thead>
<tr>
<th>Round</th>
<th>$O$</th>
<th>$O$</th>
<th>$O$</th>
<th>$O$</th>
<th>$\beta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\Delta_1$</td>
<td>$\Delta_2$</td>
<td>$\Delta_3$</td>
<td>$\Delta_4$</td>
<td>$\Delta_5$</td>
</tr>
<tr>
<td>2</td>
<td>$\Delta_1$</td>
<td>$\Delta_2$</td>
<td>$\Delta_3$</td>
<td>$\Delta_4$</td>
<td>$\Delta_5$</td>
</tr>
<tr>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
<td>$\ldots$</td>
</tr>
<tr>
<td>$m - 1$</td>
<td>$\Delta_1$</td>
<td>$\Delta_2$</td>
<td>$\Delta_3$</td>
<td>$\Delta_4$</td>
<td>$\Delta_5$</td>
</tr>
<tr>
<td>$m$</td>
<td>$\Delta_1$</td>
<td>$\Delta_2$</td>
<td>$\Delta_3$</td>
<td>$\Delta_4$</td>
<td>$\Delta_5$</td>
</tr>
</tbody>
</table>

(14)

Since $G$ is bijective, according to the bijective property, Lemma 1 can be easily proved. It also means that $\alpha \neq O$, $\Delta_G(\alpha) \neq O$. Especially, for $S$ layer in SP type and SPS type which is a nonlinear bijective mapping, it does not change the nonzero difference positions for the differential propagation according to Lemma 1. It also implies that $H(\Delta_S(\alpha)) = H(\alpha)$.

**Lemma 2.** For $S$ layer in SP type and SPS type, if $t \geq 1$ and

\[
\phi_{t+1}^{(t)}(e_t) \neq O,
\]

the equation $\phi_{t+1}^{(t)}(e_t) = e_t$ holds.

**Proof.** Firstly, we recall the definition of $e_t$. It denotes that only the $t$-th element of $n$-dimension vector $e$ is nonzero and the others are zero. According to Lemma 1 and $\phi_{t+1}^{(t)}(e_t) \neq O$,

\[
\phi_{t+1}^{(t)}(e_t) = e_t.
\]

(15)

According to Lemma 2, for $H(\alpha) = 1 \equiv \alpha = e_i$, when $\phi_{t+1}^{(t)}(\Delta_S^{(i)}(\alpha)) \neq O$, the following equation holds:

\[
H(\phi_{t+1}^{(t)}(\Delta_S^{(i)}(\alpha))) = H(\alpha) = 1.
\]

(16)

**Theorem 1.** For $m$-dataline CAST256-like structure with SP-type round function, if $H(\alpha) = H(\beta) = 1$, we can
construct \( (m^2 + m) \)-round impossible differential distinguishers for any bijective linear layer \( P \) as follows:

\[
(a, O, O, \ldots, O, O) \rightarrow m^2 + m \ (O, O, \ldots, O, O, \beta).
\]

(17)

**Proof.** From the encryption and decryption directions, the differential with the input \((a, O, O, \ldots, O, O)\) and the output \((O, O, \ldots, O, O, \beta)\) propagates \(2m + m(m-1)\) rounds, respectively. According to Proposition 2, if the differential is possible, the following equation must hold:

\[
\Delta_{P^2}(a) = \Phi_{l=1}^{m-1} \Delta_F(\beta).
\]

Taking \( F = P \circ S \) into consideration, the above equation becomes

\[
\Delta_{P \circ S \circ P, S}(a) = \Phi_{l=1}^{m-1} \Delta_F(\beta).
\]

(19)

Since \( P \) is a linear bijective mapping,

\[
P(\Delta_{P, S \circ P, S}(a)) = P(\Phi_{l=1}^{m-1} \Delta_F(\beta)) \Longleftrightarrow \Delta_{S \circ P, S}(a) = \Phi_{l=1}^{m-1} \Delta_F(\beta).
\]

(20)

For the left part of equation (20),

\[
H(\Delta_{S, P, S}(a)) = H(\Delta_{P, S}(a)) \geq B(P) - H(\Delta_S(a)).
\]

(21)

Since \( H(\Delta_S(a)) = H(\alpha) = 1 \) and \( B(P) \geq 2 \),

\[
H(\Delta_{S, P, S}(a)) \geq B(P) - H(\Delta_S(a)) = B(P) - H(\alpha) \geq 1.
\]

(22)

Case 1: when \( H(\Delta_{S, P, S}(a)) > 1 \), note that \( H(\Phi_{l=1}^{m-1} \Delta_F(\beta)) = H(\beta) = 1 \) according to Lemma 2, and the left and right parts of equation (20) have different Hamming weights. So, equation (20) does not hold.

Case 2: when \( H(\Delta_{S, P, S}(a)) = 1 \), assume that \( \Delta_{S, P, S}(a) = \epsilon_j \). Take \( \beta = \epsilon_i \), where \( j \neq i \). According to Lemma 2, \( \Phi_{l=1}^{m-1} \Delta_F(\beta) = \epsilon_i \neq \epsilon_j \). The left and right parts of equation (20) could not match each other. So, equation (20) does not hold.

Therefore, combined with the above two cases, equation (20) does not hold. It means that the middle differences could not match each other, and the \((2m + m(m-1)) = m^2 + m\)-round differential is impossible.

In [18], \((m^2 + m)\)-round impossible differential distinguishers were also constructed, but the linear layer \( P \) is restricted to that satisfying the condition \( B(P) > 2 \). However, in Theorem 1, the restricted condition of \( P \) is removed and it is expanded to any bijective linear layer.

To construct longer impossible differential distinguishers, we need to exploit the details of the linear layer \( P \). When the primitive index of the linear layer \( P \) satisfies \( R \geq 2 \), the following theorem is given.

**Theorem 2.** For \( m \)-dataline CAST256-like structure with \( SP \)-type round function, if \( R \geq 2 \) and \( H(\alpha) = H(\beta) = 1 \), \( L \)-round impossible differential distinguishers \((a, O, O, \ldots, O, O, O, O, \beta) \) could be constructed, where

\[
L = m^2 + m + \min[R - 2, m - 3].
\]

(23)

**Proof.** To prove this theorem, we compare \( R \) with \( m - 1 \) for two cases.

Case 1: when \( 2 \leq R \leq m - 1 \), \( \min[R - 2, m - 3] = R - 2 \). From the encryption and decryption directions, the differential with the input \((a, O, O, \ldots, O, O)\) and the output \((O, O, \ldots, O, O, \beta)\) propagates \(2m + R - 2\) and \(m(m-1)\) rounds, respectively. According to Proposition 2, if the differential is possible,

\[
\Delta_{P^R}(a) = \Phi_{l=1}^{m-1} \Delta_F(\beta).
\]

(24)

Taking \( F = P \circ S \) into consideration, the above equation becomes

\[
\Delta_{S, \{P \circ S, \ldots, P \circ S\}}(a) = \Phi_{l=1}^{m-1} \Delta_F(\beta).
\]

(25)

Since \( P \) is a linear bijective mapping,

\[
\Delta_{S, \{P \circ S, \ldots, P \circ S\}}(a) = \Phi_{l=1}^{m-1} \Delta_S(\beta).
\]

(26)

In the left part of equation (26), there exists at least one 0 element in the matrix \((P^*)^{-1} = (q_{i,j})_{ij}\). Assume that \( q_{i,j} = 0 \), and when we take \( \alpha = e_j \), the \( i \)-th element of \( \Delta_{S, \{P \circ S, \ldots, P \circ S\}}(a) \) must be 0.

In the right part of equation (26), since \( H(\beta) = 1 \), we take \( \beta = e_i \). According to Lemma 2, \( \Phi_{l=1}^{m-1} \Delta_S(\beta) = e_i \). So, the \( i \)-th element of \( \Phi_{l=1}^{m-1} \Delta_S(\beta) \) is not equal to 0. Therefore, equation (26) cannot hold. In this case, we can construct \((2m + R - 2 + m(m-1)) = m^2 + m + R - 2\)-round impossible differential distinguishers.

Case 2: when \( R > m - 1 \), \( \min[R - 2, m - 3] = m - 3 \). From the encryption and decryption directions, the differential with the input \((a, O, O, \ldots, O, \beta)\) and the output \((O, O, \ldots, O, O, \beta)\) propagates \(3m - 3\) and \(m(m-1)\) rounds, respectively. According to Proposition 2, if the differential is possible,

\[
\Delta_{P^{m-1}}(a) = \Phi_{l=1}^{m-1} \Delta_F(\beta).
\]

(27)

Taking \( F = P \circ S \) into consideration, the above equation becomes

\[
\Delta_{S, \{P \circ S, \ldots, P \circ S\}}(a) = \Phi_{l=1}^{m-1} \Delta_F(\beta).
\]

(28)

Since \( P \) is a linear bijective mapping,

\[
\Delta_{S, \{P \circ S, \ldots, P \circ S\}}(a) = \Phi_{l=1}^{m-1} \Delta_S(\beta).
\]

(29)
In the left part of equation (29), since \( R > (m - 1) \), there exists at least one 0 element in the matrix \((P^{r})^{m-2} = (d_{ij})_{\text{non}}\). Assume that \( d_{ij} = 0 \), and when we take \( \alpha = e_{j} \), the \( i \)-th element of \( \Delta_s. (P \circ S \circ \ldots \circ P \circ S) \) \((a)\) must be 0.

In the right part of equation (29), it is similar to Case 1. Thus, if we take \( \beta = e_{i} \), the \( i \)-th element of \( \Phi^{n-1}_{\text{non}} A \{0\} (\beta) \) is not equal to 0.

Therefore, equation (29) does not hold. In this case, we can construct \((3m - 3 + m(m - 1) = m^2 + 2m - 3)\)-round impossible differentials.

Combined with the above two cases, we can construct \(L\)-round impossible differential distinguishers, where

\[
L = \begin{cases} 
    m^2 + m + R - 2, & 2 \leq R \leq m - 1, \\
    m^2 + m + m - 3, & R > m - 1. 
\end{cases} \tag{30}
\]

It is equivalent to \( L = m^2 + m + \min\{R - 2, m - 3\} \).

In [18], \((m^2 + m)\)-round impossible differential distinguishers were constructed. According to Theorem 2, we can construct \((m^2 + m + \min\{R - 2, m - 3\})\)-round impossible differentials which are \( \Lambda_{0} = \min\{R - 2, m - 3\} \) rounds longer than before. The restricted condition \( R \geq 2 \) can be satisfied easily. We present some specific linear transformations \( P \) satisfying the condition. For example, we first present \(MC\) of Skinny block cipher [21] below:

\[
P_{MC} = \begin{pmatrix} 
1 & 0 & 1 \\
1 & 0 & 0 \\
0 & 1 & 1 \\
1 & 0 & 1 
\end{pmatrix}. \tag{31}
\]

With the definition of \( R \), we calculate \( R = 3 \) for \( P_{MC} \). According to Theorem 2, if the linear transformation \( P \) takes \( P_{MC} \) and \( m \geq 4 \), \( \Lambda_{0} = \min\{R - 2, m - 3\} = 1 \). Therefore, we can construct \((m^2 + m + 1)\)-round impossible differential distinguishers for \(m\)-dataloader CAST256-like structure with SP-type round function. They are \((\Lambda_{0} = 1)\) round longer than those in [18]. Moreover, we present another example. For the linear transformation of Skinny block cipher which is \(SR \circ MC\), it is given below:

\[
P_{Skinny} = \begin{pmatrix} 
1000000000100100 \\
0100000000100100 \\
0010000010000001 \\
0001000001000001 \\
0000100000100001 \\
0000010000010001 \\
0000001000001001 \\
0000000100001001 \\
0000000010001001 \\
0000000001001001 \\
0000000000101001 \\
0000000000011001 \\
0000000000001100 \\
0000000000000110 \\
0000000000000011 \\
0000000000000001 
\end{pmatrix}_{16 \times 16}. \tag{32}
\]

We calculate \( R = 6 \) for \(P_{Skinny}\). According to Theorem 2, if the linear transformation \( P \) takes \(P_{Skinny}\) and \( m \geq 7 \), \( \Lambda_{0} = \min\{R - 2, m - 3\} = 4 \). Therefore, we can construct \((m^2 + m + 4)\)-round impossible differential distinguishers. They are \((\Lambda_{0} = 4)\) rounds longer than those in [18].

In brief, combined with Theorem 1 and Theorem 2, for \(m\)-dataloader CAST256-like structure with SP-type round function, the results on the impossible differential distinguishers have been improved. Especially, when \( R > 2 \), we can construct longer impossible differentials. \( \square \)

### 3.3. Constructing Impossible Differential Distinguishers of \(m\)-Dataloader CAST256-Like Structure with SP-Type Round Function

For \(m\)-dataloader CAST256-like structure with SP-type round function, \((m^2 + m - 1)\)-round impossible differential distinguishers were constructed for \(R \geq 2 \) [18]. In this section, we will construct longer impossible differential distinguishers with the details of \(P\). We present the following theorem as follows.
Theorem 3. For m-dataline CAST256-like structure with SPS-type round function, if \( R \geq 3 \), \( \exists P(t) = e_i \) and \( 0 = q_{i,j} \in (P^*)^{(\min(R,m)-1)} \), we can construct \( L \)-round impossible differential distinguishers \( (a, O, O, \ldots, O, O) \rightarrow (O, O, \ldots, O, O, \beta) \), where \( H(a) = H(\beta) = 1 \) and
\[
L = m^2 + m + \min(R - 3, m - 3).
\]

**Proof.** To prove this theorem, we compare \( R \) with \( m \) for two cases.

Case 1: when \( 3 \leq R \leq m \), \( \min(R - 3, m - 3) = R - 3 \). From the encryption and decryption directions, the differential with the input \((a, O, O, \ldots, O, O)\) and the output \((O, O, \ldots, O, O, \beta)\) propagates \( 2m + R - 3 \) and \( m(m - 1) \) rounds, respectively. According to Proposition 2, if the differential is possible,
\[
\Delta_{P^{m-1}}(a) = \Theta_{\pi}^{-1} \Delta_F(\beta).
\]
Taking \( F = S \circ P \circ S \) into consideration, the above equation becomes
\[
\Delta_{[S \circ P \circ S \ldots S \circ P \circ S]}(a) = \Theta_{\pi}^{-1} \Delta_{S \circ P \circ S}(\beta). \tag{35}
\]
In the left part of equation (35), there exists at least one 0 element in the matrix \((P^*)^{\beta-1} = (q_{i,j})_{m \times m} \). Assume that \( q_{i,j} = 0 \), and when we take \( a = e_i \), the \( i \)-th element of \( \Delta_{[S \circ P \circ S \ldots S \circ P \circ S]}(a) \) must be 0.

In the right part of equation (35), when one column of \( P \) is \( e_i \), assume that the \( t \)-th column of \( P \) is \( e_i \), i.e., \( P(t) = e_i \), taking \( \beta = e_i \) and \( \Delta_{S \circ P \circ S}(\beta) = \Delta_{S \circ P \circ S}(e_i) = \Delta_{S \circ P}(e_i) = \Delta_S(\pi)(e_i) = e_i \). Furthermore, according to Lemma 2,
\[
\Theta_{\pi}^{-1} \Delta_{S \circ P \circ S}(e_i) = \Theta_{\pi}^{-1} \Delta_{S \circ P \circ S}(e_i) = e_i. \tag{36}
\]
So, the \( i \)-th element of \( \Theta_{\pi}^{-1} \Delta_{S \circ P \circ S}(\beta) \) is not equal to 0. Therefore, equation (35) does not hold. In this case, we can construct \( (2m + R - 3 + m(m - 1) = m^2 + m + R - 3) \)-round impossible differential distinguishers.

Case 2: when \( R > m \), \( \min(R - 3, m - 3) = m - 3 \). From the encryption and decryption directions, the differential with the input \((a, O, O, \ldots, O, O)\) and the output \((O, O, \ldots, O, O, \beta)\) propagates \( 3m - 3 \) and \( m(m - 1) \) rounds, respectively. According to Proposition 2, if the differential is possible,
\[
\Delta_{P^{m-1}}(a) = \Theta_{\pi}^{-1} \Delta_F(\beta). \tag{37}
\]
Taking \( F = S \circ P \circ S \) into consideration, the above equation becomes
\[
\Delta_{[S \circ P \circ S \ldots S \circ P \circ S]}(a) = \Theta_{\pi}^{-1} \Delta_{S \circ P \circ S}(\beta). \tag{38}
\]
In the left part of equation (38), since \( R > m \), there exists at least one 0 element in the matrix \((P^*)^{\beta-1} \). It is similar to Case 1, and we can construct \( (3m - 3 + m^2 - m = m^2 + 2m - 3) \)-round impossible differential distinguishers.

Combined with the above two cases, we can construct \( L \)-round impossible differential distinguishers, where
\[
L = \begin{cases} 
  m^2 + m + R - 3, & 3 \leq R \leq m, \\
  m^2 + m + m - 3, & R > m. \end{cases} \tag{39}
\]
It is equivalent to \( L = m^2 + m + \min(R - 3, m - 3) \).

In [18], \( (m^2 + m - 1) \)-round impossible differential distinguishers were constructed. According to Theorem 3, we can construct \( (\Lambda_1 + 1 = \min(R - 3, m - 3) + 1 = \min(R - 2, m - 2) \) \) rounds longer than before. Moreover, we present a specific linear transformation \( P \) satisfying the restricted condition in Theorem 3. For \( P_{\text{Skinny}} \) which is described in Section 3.2, we calculate \( R = 6 \). \( P_{\text{Skinny}}^* \) and \( (P_{\text{Skinny}}^*)^{\beta-1} = (P_{\text{Skinny}}^*)^2 \) are given below, respectively.

\[
\begin{array}{cccccccccccc}
10000000000000100100 & 2872225376481152 \\
01000000000000101000 & 2287322587642115 \\
00100000001000000100 & 7228532248765211 \\
00010000000101000000 & 8722253264871521 \\
100000000000000000 & 152112132250130 \\
010000000000000000 & 1152112253220013 \\
001000000000000000 & 2115211225323001 \\
000100000000000000 & 521121122531300 \\
000000000000000000 & 3212112124322110 \\
000010000000000000 & 2321111222430211 \\
000000100000000000 & 123211132241021 \\
000000001000000000 & 2123121143221102 \\
100000000000000000 & 173212324361140 \\
010000000000000000 & 2173212364430114 \\
001000000000000000 & 3217321236444011 \\
000100000000000000 & 7321232143641401 \\
000000000000000100 & \end{array} \tag{40}
\]

When \( m \geq 6 \) and \( (P_{\text{Skinny}}^*)^{\beta-1} = (P_{\text{Skinny}}^*)^2 \), we can find that the 4-th column of \( P_{\text{Skinny}} \) is \( e_9 \) and \( 0 = q_{9,12} \in (P_{\text{Skinny}}^*)^2 \). Therefore, \( P_{\text{Skinny}} \) satisfies the restricted condition in Theorem 3. Moreover, \( (\Lambda_1 + 1 = \min(R - 2, m - 2) = 4 \) Thus, for \( m \)-dataline CAST256-like structure with SPS-type round function, if \( P \) takes \( P_{\text{Skinny}} \) and \( m \geq 6 \), we can construct 4-round impossible differentials longer than those in [18].
4. Revisiting Impossible Differential Distinguishers of \( m \)-Dataline MARS-Like Structure

In this section, we first introduce \( m \)-dataline MARS-like structure and present the differential propagation rules from the encryption and decryption directions. Then, when the round function takes SPS type, \( 3m \)-round impossible differential distinguishers will be constructed. It should be pointed out that \( m \geq 4 \) and \( m \) should be even number in this section.

4.1. \( m \)-Dataline MARS-Like Structure. An \( m \)-dataline MARS-like structure consists of \( r \) rounds, and each round is depicted in Figure 2.

Let \((X^0_0, X^1_1, \ldots, X^{m-1}_{m-1})\) be the input of the \( i \)-th round and \((X^0_i, X^1_i, \ldots, X^{m-1}_{m-1})\) and \(K^{i-1}\) be the output and the round key of the \( i \)-th round, respectively. One-round encryption is defined by

\[
\begin{align*}
X^i_j &= F(X^0_j \oplus K^{i-1}) \oplus X^{i-1}_{j+1}, \quad 0 \leq j \leq m - 2, \\
X^{m-1}_i &= X^0_i,
\end{align*}
\]

(41)

where \( F \) is the round function and \( X^{i-1}_j \in F_{2^m}, 0 \leq j \leq m - 1, \ i \geq 1 \).

4.2. Constructing Impossible Differential Distinguishers of \( m \)-Dataline MARS-Like Structure with SPS-Type Round Function. To construct impossible differentials, one-round differential propagations from the encryption and decryption directions need to be studied. They are described as follows.

**Proposition 3.** Let \( \Delta X^{i-1}_j \) and \( \Delta X^i_j \) be the \( i \)-th round input difference and output difference of \( m \)-dataline MARS-like structure. From the encryption direction, one-round differential propagation is presented below:

\[
\begin{align*}
\Delta X^i_j &= \Delta F(\Delta X^{i-1}_j) \oplus \Delta X^{i-1}_{j+1}, \quad 0 \leq j \leq m - 2, \\
\Delta X^i_{m-1} &= \Delta X^{i-1}_0.
\end{align*}
\]

(42)

From the decryption direction, one-round differential propagation is presented below:

\[
\begin{align*}
\Delta X^{i-1}_0 &= \Delta X^i_{m-1}, \\
\Delta X^i_j &= \Delta F(\Delta X^{i-1}_{m-1}) \oplus \Delta X^{i-1}_{j-1}, \quad 1 \leq j \leq m - 1.
\end{align*}
\]

(43)

According to the encryption process of MARS-like structure, the above proposition can be proved. Moreover, from the encryption direction, the input difference \((O, O, \ldots, O, O, 0) (a \in F^m_{2^m}, a \neq O)\) is encrypted \( 3m/2 \) rounds with probability 1 as described in Table 5. In this table, \( a_0 \in \Delta F(a), a_1 \in \Delta F(a_0 \oplus a_0 \oplus \cdots \oplus a_{i-1}) \), \( i \geq 1 \), \( A = a_0 \oplus a_0 \oplus \cdots \oplus a_{m/2} \). Similarly, from the decryption direction, the output difference \((a, O, O, \ldots, O, O)\) is decrypted \( 3m/2 \) rounds with probability 1 as described in Table 6. In this case, \( b_0 \in \Delta F(a), b_1 \in \Delta F(b_0 \oplus b_1 \oplus \cdots \oplus b_{m/2}) \).

If \( (3m/2 + 3m/2 = 3m) \)-round differential \((O, O, \ldots, O, O, a) \rightarrow m (a, O, O, \ldots, O, O)\) is a possible differential, the middle differences need to match each other. Thus, the following equations need to be satisfied:

\[
\begin{align*}
A &= a_1 \oplus a_0 \oplus \cdots \oplus a_{m/2}, \\
B &= b_0 \oplus b_1 \oplus \cdots \oplus b_{m/2}, \\
A &= B \oplus b_{m/2}, \\
A &= B \oplus b_{m/2-1}, \\
A &= B \oplus b_{m/2-3}, \\
&\vdots \\
A &= B \oplus b_2, \\
A \oplus a_0 \oplus a_0 &= B \oplus b_1, \\
A \oplus a_1 &= B \oplus a_0, \\
A \oplus a_2 &= B, \\
&\vdots \\
A \oplus a_{m/2} &= B.
\end{align*}
\]

(44)

Solving the above equations,

\[
\begin{align*}
b_{m/2} &= b_{m/2-1} = \cdots = b_2 = a_2 = \cdots = a_{m/2-1} = a_{m/2} = O, \\
a_0 \oplus b_1 = a_1 \oplus b_0 = a.
\end{align*}
\]

(45)

Since \( F \) is bijective, according to Lemma 1,
Table 6: 3m/2-round differential characteristic of m-dataline MARS-like-like structure from the decryption direction.

<table>
<thead>
<tr>
<th>Round</th>
<th>α</th>
<th>O</th>
<th>O</th>
<th>O</th>
<th>...</th>
<th>O</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>O</td>
<td>α</td>
<td>O</td>
<td>O</td>
<td>...</td>
<td>O</td>
<td>O</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>O</td>
<td>O</td>
<td>O</td>
<td>...</td>
<td>O</td>
<td>α</td>
</tr>
<tr>
<td>m</td>
<td>α</td>
<td>b₀</td>
<td>b₀</td>
<td>b₀</td>
<td>...</td>
<td>b₀</td>
<td>b₀</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>3m/2</td>
<td>B₀b₀</td>
<td>...</td>
<td>B₀b₁</td>
<td>B₀αb₀</td>
<td>B</td>
<td>...</td>
<td>B</td>
</tr>
</tbody>
</table>

\[
\begin{aligned}
\left\{ \begin{array}{l}
\alpha_2 = \Delta_F (a_0 \oplus a_1) = O, \\
\beta_1 = \Delta_F (b_0 \oplus b_1) = O,
\end{array} \right. \\
\left\{ \begin{array}{l}
\alpha_1 = a_0, \\
\beta_1 = b_0.
\end{array} \right.
\end{aligned}
\]  

(46)

Thus,

\[a_0 \oplus b_1 = a_0 \oplus b_0 = a \implies \Delta_F^{(1)} (a) \oplus \Delta_F^{(2)} (a) = a. \]  

(47)

When the round function \( F \) of \( m \)-dataline MARS-like structure takes SPS type, the impossible differential distinguishers can be constructed with the following theorem.

**Theorem 4.** For \( m \)-dataline MARS-like structure with SPS-type round function, if there exists one 0 element in the diagonal line of \( P \), \( 3m \)-round impossible differential distinguishers can be constructed as follows:

\[ (\alpha, O, O, \ldots, O, O) \xrightarrow{3m} (O, O, \ldots, O, O, \alpha), \]  

where \( H(\alpha) = 1 \).

**Proof.** When \( (\alpha, O, O, \ldots, O, O) \xrightarrow{3m} (O, O, \ldots, O, O, \alpha) \) is a \( 3m \)-round possible differential, the following equation needs to be satisfied:

\[ \Delta_F^{(1)} (\alpha) \oplus \Delta_F^{(2)} (\alpha) = a. \]  

(49)

Given that \( F \) takes SPS type, the above equation becomes

\[ \Delta_{SP}^{(1)} (\alpha) \oplus \Delta_{SP}^{(2)} (\alpha) = a. \]  

(50)

Since \( \exists P_{i,j} = 0, P_{i,j} \in P \), we take \( \alpha = e_t, \Delta_e (\alpha) = e_t \), \( \Delta_{SP} (\alpha) = \bar{e}_t \), where \( \bar{e}_t \) denotes that the \( t \)-th element of \( n \)-dimension vector \( e \) is 0 and the others can be arbitrary values. Moreover, \( \Delta_{SP} (\alpha) = \bar{e}_t \). Furthermore, \( \Delta_{SP}^{(1)} (\alpha) \oplus \Delta_{SP}^{(2)} (\alpha) = \bar{e}_t \) which conflicts with \( \alpha = e_t \) in the \( t \)-th element. Therefore, equation (50) does not hold.

In [19], \( (3m−1) \)-round impossible differential distinguishers were constructed for \( m \)-dataline MARS-like structure with SPS-type round function. According to Theorem 4, we can construct 1 round longer than before. Moreover, some specific linear transformations \( P \) satisfying the condition in Theorem 4 are presented. For example, MC of Midori block cipher [22] is described below:

\[
P_{MC} = \begin{pmatrix}
0 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0
\end{pmatrix}_{4 \times 4}.
\]  

(51)

In this matrix, we can observe that \( p_{0,0} = p_{1,1} = p_{2,2} = p_{3,3} = 0 \). Therefore, \( P_{MC} ∗ \) satisfies the restricted condition in Theorem 4. Furthermore, \( P_{MC} \) and \( P_{Smart} \) described in Section 3.2 also satisfy the condition.

\[ \square \]

5. Conclusions

In this paper, we investigated impossible differential distinguishers of \( m \)-dataline CAST256-like structure and \( m \)-dataline MARS-like structure. Longer impossible differentials for them were constructed with the help of the linear transformation \( P \). Moreover, given that the dual relationship between impossible differentials and zero correlation linear hulls which is presented by Sun Bing et al. at CRYPTO 2015, our results may also be applied to construct zero correlation linear hulls of these two structures. In brief, our results not only are useful to improve the impossible differential attack on these two structures from the cryptanalysis view but also provide guidance to select better linear transformation for improving the security from the designer’s view.

Data Availability

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

Conflicts of Interest

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

Acknowledgments

This study was funded by the National Natural Science Foundation of China (nos. 62002370 and 61772545).

References


