Security Evaluation of MISTY Structure with SPN Round Function

Ruilin Li[1], Chao Li[1,2], Jinshu Su[2], and Bing Sun[1,3]

[1]Department of Mathematics and System Science, Science College,
National University of Defense Technology, Changsha, 410073, China
securitylrl@gmail.com
[2]College of Computer, National University of Defense Technology,
Changsha, 410073, China
[3]State Key Laboratory of Information Security, Institute of Software,
Chinese Academy of Sciences, Beijing, 100190, China

Abstract. This paper deals with the security of MISTY structure with SPN round function. We study the lower bound of the number of active s-boxes for differential and linear characteristics of such block cipher construction. Previous result shows that the differential bound is consistent with the case of Feistel structure with SPN round function, yet the situation changes when considering the linear bound. We carefully revisit such issue, and prove that the same bound in fact could be obtained for linear characteristic. This result combined with the previous one thus demonstrates a similar practical secure level for both Feistel and MISTY structures. Besides, we also discuss the resistance of MISTY structure with SPN round function against other kinds of cryptanalytic approaches including the integral cryptanalysis and impossible differential cryptanalysis. We confirm the existence of 6-round integral distinguishers when the linear transformation of the round function employs a binary matrix (i.e., the element in the matrix is either 0 or 1), and briefly describe how to characterize 5/6/7-round impossible differentials through the matrix-based method.

Keywords: Block ciphers, MISTY structure, SPN, Practical security, Differential cryptanalysis, Linear cryptanalysis, Integral cryptanalysis, Impossible differential cryptanalysis

1 Introduction

1.1 Backgrounds

Differential cryptanalysis [7] (DC) and linear cryptanalysis [27] (LC) are the two most powerful known attacks on block ciphers. Accordingly, for a new proposed algorithm, the designers should evaluate its security against DC and LC, or even prove its resistance against these two attacks. In general, there are two strategies for achieving this goal. The first one is the *provable secure* approach, and the second one is the *practical secure* approach. The provable secure approach[1] is introduced in [32, 31], where the concepts of differential [23] and linear hull [31] are used to prove an upper bound of maximum differential (linear) probability. This bound should be sufficiently low in order to make the whole cipher be theoretically invulnerable to DC and LC. This condition is

[1] Note that, for some ciphers, see e.g. [3, 4], the theory of decorrelation [41] can provide a tool for the proof of provable security against DC and LC.

usually achieved by imposing a (relative hard) restriction on the round function. Another approach is the practical secure approach [19], which concentrates on the differential characteristic and linear characteristics, other than the differential and linear hull. According to this approach, if the upper bound of the maximum differential and linear characteristic probabilities are less than (usually) the security threshold, the whole cipher is said to be practically secure against DC and LC.

High-level structures play an essential role in designing block ciphers resisting DC and LC. There are many well-known block cipher structures, including SPN structure, Feistel structure, MISTY structure, Lai-Massey structure, etc. Since most of these block cipher structures can provide their provable security proofs against DC and LC based on some assumptions of the round function, choosing which kind of round function becomes a key step in the design of a secure block cipher. SPN-type round functions attract more attentions in recent years, since they can provide good performance, and meanwhile without lost of security. Many block ciphers, such as Camellia, CLEFIA, SMS4, etc. adopt such kind of round functions.

1.2 Related Works

Both provable and practical approaches have been widely adopted to demonstrate the security of various block cipher structures. For instance, using the idea of provable security, the upper bound of differential and linear hull probabilities for Feiste structure are obtained in [2, 32, 31], and the result for SPN structure are shown in [15, 16, 33]. While using the notation of practical security, the upper bound of probabilities of differential and linear characteristic of Feistel ciphers are obtained in [19].

It is believed that for most block cipher structures, if the round function is SPN-type, the maximum probability of differential and linear characteristic can usually be converted to the least number of active differential and linear s-boxes. Thus when considering the practical security aspects, the method of counting (or providing the lower bound of) the number of active s-boxes becomes a well used technique. For SPN structure, this approach had been formalized as the *wide trail strategy* [10], which is widely used in many block cipher designs [11, 12, 34]. For Feistel structure with SPN round function, a similar result is obtained by Kanda in [22], followed by some advanced results using the technique of *diffusion switching mechanism* to avoid the *difference cancellation* as shown in [36–38]. Recently, many results are also obtained for generalized Feistel structureswith SPN round function, see e.g. [8, 42, 35, 39].

MISTY structure is another well-known block cipher structure that is introduced by Matsui in [29] and is recommended as an alternative scheme of Feistel structure, due to its provable security against DC and LC. In [13], Gilbert and Minier formalize the standard MISTY structure as the L-scheme and refer the dual structure as the R-scheme and provide the proof of (super) pseudo-randomness. Another advantage of MISTY structure is that it allow parallel computations in the encryption direction. Due to this, MISTY structure has been chosen as the underlying high-level structure of the block cipher MISTY2 [30], and meanwhile, as the basic low-level structure of the round function and the component in block ciphers MISTY1 [30], MISTY2, and KASUMI [40].

1.3 Main Results and Outline of This Paper

This paper mainly concentrates the practical security of MISTY structure when the round function is SPN-type. Let $\mathcal{B}_d$ (resp. $\mathcal{B}_l$) be the differential (resp. linear) branch number of the linear transformation. Previous result [44] shows that the number of differential active s-boxes in $4r$ rounds is at least $\mathcal{B}_d \times r + \lfloor r/2 \rfloor$. This lower bound for differential characteristic is consistent with the case of Feistel structure with SPN round function [22]. However, as the authors mentioned, the situation changes when considering the linear characteristic.

We carefully revisit such issue, and prove that the same bound in fact could be obtained for linear characteristic. That is to say the number of active s-boxes in any linear characteristic over $4r$ rounds is at least $\mathcal{B}_l \times r + \lfloor r/2 \rfloor$. This result combined with the previous one thus demonstrate a similar practical secure level for both Feistel and MISTY structures. Besides, we also discuss the resistance of MISTY structure with SPN round function against other kinds of cryptanalytic approaches including the integral cryptanalysis and the impossible differential cryptanalysis. We confirm the existence of 6-round integral distinguishers when the linear transformation of the round function employs a binary matrix, and briefly describe how to characterize 5/6/7-round impossible differentials through the matrix-based method.

All of the above results can be applied to the block cipher p-Camellia that is proposed in [44]. For instance, the least number of active s-boxes for 16-round linear characteristic can be improved from 15 to 22, which demonstrates the practical resistance of p-Camellia against LC. Meanwhile, 6/7-round integral distinguishers and 5/6/7-round impossible differentials can be constructed (previous known results are only 4-round), which significantly improve the distinguishing bounds of p-Camellia (See Appendix A).

The outline of this paper is as follows: some preliminaries are introduced in Section 2. Section 3 revisits the practical security of MISTY structure with SPN round function against DC and LC. Section 4 discusses the resistance of such block cipher construction against other kinds of cryptanalytic approaches including the integral cryptanalysis and impossible differential cryptanalysis. Finally, Section 5 concludes this paper.

2 Preliminaries

2.1 Notations

Let $X = (x_1, x_2, \ldots, x_n), Y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_{2^d}^n$, where d and n are some integers, then the following notations are used throughout this paper.

ΔX : difference of X and X', $\Delta X = X \oplus X'$
ΓY : mask value of Y
$X \oplus Y$: bitwise exclusive-OR (XOR) of X and Y
$Y \cdot \Gamma Y$: parity of bitwise product Y and ΓY
$X \| Y$: concatenation of X and Y

2.2 MISTY Structure

Consider any block cipher that employs a MISTY structure (see Fig.1). Let (X_{i-1}, X_i) be the input of the i-th round, then the output is (X_i, X_{i+1}) satisfying

$$X_{i+1} = F\left(X_{i-1}, K_i\right) \oplus X_i,$$

where $F(\cdot,\cdot)$ is the round function and K_i is the round key. In order to make MISTY structure invertible, for any fixed round key K_i, $F(\cdot, K_i)$ must be bijective. Assume the plaintext is (X_0, X_1), then after iterating the above round transformation r times, the ciphertext is defined as (X_{r+1}, X_r).

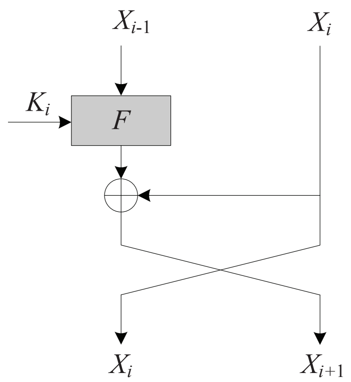

Fig. 1. The i-th round of MISTY structure

In this paper, we focus on MISTY structure with SPN round function, that is $F(X,K) = P(S(X \oplus K))$, where the input X is first XORed with the round key K known as the *round key addition layer*, and then the result is fed into a *substitution layer* defined as a non-linear bijective transformation S over $\mathbb{F}_{2^d}^n$ by n parallel S-boxs on $\mathbb{F}_{2^d}$, followed by a *diffusion layer* which employs an invertible linear transformation P defined over $\mathbb{F}_{2^d}^{n\times n}$. More precisely,

$$S : \mathbb{F}_{2^d}^n \to \mathbb{F}_{2^d}^n \ , X = (x_1, x_2, \dots, x_n) \mapsto Z = S(X) = (s_1(x_1), s_2(x_2), \dots, s_n(x_n)),$$
$$P : \mathbb{F}_{2^d}^n \to \mathbb{F}_{2^d}^n \ , Z = (z_1, z_2, \dots, z_n) \mapsto Y = P(Z) = (y_1, y_2, \dots, y_n).$$

In the following sections, we will use X_{i-1} (resp. Y_{i-1}) to denote the input (resp. output) of the i-th round function, i.e. $Y_{i-1} = F(X_{i-1} \oplus K_i)$. Let Z_{i-1} denote the intermediate variable after the substitution layer in the i-th round function, thus $Z_{i-1} = S(X_{i-1} \oplus K_i)$ and $Y_{i-1} = P(Z_{i-1})$.

It is worth noting that we will neglect the effect of the round key addition layer when considering the provable or practical security evaluation of block ciphers, since in these situations we assume that the round-key consists of independent and uniform random bits and is bitwise XORed with the data, i.e. $Y = F(X \oplus K) \doteq F(X) = P(S(X))$. One can discriminate those situations according to the context.

2.3 Definitions

In this subsection, we give some definitions used in the following sections.

Definition 1. *Given $\Delta x, \Delta z, \Gamma x, \Gamma z \in \mathbb{F}_2^d$, the differential and linear probabilities of each s-box are defined as*

$$DP^{s_i}(\Delta x \to \Delta z) = \frac{\#\{x \in \mathbb{F}_2^d | s_i(x) \oplus s_i(x \oplus \Delta x) = \Delta z\}}{2^d}$$
$$LP^{s_i}(\Gamma z \to \Gamma x) = \left(2 \times \frac{\#\{x \in \mathbb{F}_2^d | x \cdot \Gamma x = s_i(x) \cdot \Gamma z\}}{2^d} - 1\right)^2$$

Definition 2. *The maximum differential and linear probability of s-boxes are defined as:*

$$p_s = \max_i \max_{\Delta x \neq 0, \Delta z} DP^{s_i}(\Delta x \to \Delta z)$$
$$q_s = \max_i \max_{\Gamma x, \Gamma z \neq 0} LP^{s_i}(\Gamma z \to \Gamma x)$$

Thus, p_s (resp. *q_s*) *is the upper bound of the maximum of differential* (resp. *linear*) *probabilities for all s-boxes.*

Definition 3. *A differential active s-box is defined as an s-box whose input difference is non-zero. Similarly, a linear active s-box is defined as an s-box whose output mask value is non-zero. Note that if the s-box is bijective, then such s-box given a non-zero output difference* (resp. *input mask value*) *is also a differential* (resp. *linear*) *active s-box.*

Definition 4. *Let $X = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{2^d}^n$, then the bundle weight of X is defined by*

$$H_w(X) = \#\{i | x_i \neq 0\}.$$

For convenience, given a linear transformation $P : \mathbb{F}_{2^d}^n \to \mathbb{F}_{2^d}^n$, we will simply use P to denote its matrix representation and P^T to denote the transpose of P. Then the differential/linear branch number [9, 12] is defined as follows:

Definition 5. *The differential branch number of P is defined as*

$$\mathcal{B}_d = \min_{\Delta X \neq 0} \left(H_w(\Delta X) + H_w(P \cdot \Delta X) \right).$$

Definition 6. *The linear branch number of P is defined as*

$$\mathcal{B}_l = \min_{\Gamma Y \neq 0} (H_w(\Gamma Y) + H_w(P^T \cdot \Gamma Y)).$$

3 Practical Security Evaluation Against DC and LC

To evaluate the practical security of Feistel ciphers with SPN round function against DC and LC, Kanda presents the following result, which implies that clarifying the upper bound of the maximum differential (resp. linear) characteristic probability is equivalent to showing the lower bound of minimum number of differential (resp. linear) active s-boxes. In general [2], this result can be applied to many other kinds of block cipher constructions.

Proposition 1. [3] *Assume Feistel ciphers with SPN round function, let $\mathcal{D}^{(r)}$ and $\mathcal{L}^{(r)}$ be the minimum number of active s-boxes over any r-round differential and linear characteristics, then r-round differential and linear characteristic probability $p_d^{(r)}$ and $p_l^{(r)}$ satisfy the following relationship:*

$$p_d^{(r)} \leq p_s^{\mathcal{D}^{(r)}} \quad \text{and} \quad p_l^{(r)} \leq q_s^{\mathcal{L}^{(r)}}.$$

[2] For a counterexample, one can refer the kind of unbalanced Feistel structure with contracting MDS diffusion as shown in [8].

[3] This proposition is presented as Definition 8 and Definition 10 in [22].

Kanda also demonstrates that for Feistel ciphers with SPN round function, if the linear transformation is bijective, the cipher can be transformed into a Feistel cipher with PSN round function. Thus, according to the duality [5, 28] between DC and LC of Feistel structure, one only needs to give the lower bound of the number of active s-boxes for differential characteristic.

However, Kanda's approach cannot be extended to the case of MISTY structure with SPN round function due to the fact that MISTY structure and its dual structure is not the same. Thus we must study the lower bound of minimum number of active s-boxes for differential and linear characteristics respectively. For convenience, we will still use $\mathcal{D}^{(r)}$ and $\mathcal{L}^{(r)}$ to represent be the minimum number of differential and linear active s-boxes over r-round MISTY structure with SPN round function.

3.1 Lower Bound of the Number of Differential Active S-boxes

In this subsection, we just list the result for the lower bound of then number of differential active s-boxes over $4r$-round MISTY structure with SPN round function. Remind that in [44], MISTY structure is referred as 2-cell GF-NLFSR.

Proposition 2. [44] *The minimum number of differential active s-boxes for* $4r$*-round* 2*-cell GF-NLFSR cipher with SPN round function satisfies*

$$\mathcal{D}^{(4r)} \geq \mathcal{B}_d \times r + \lfloor r/2 \rfloor.$$

Note that this differential bound is consistent with the case of Feistel structure with SPN round function.

3.2 Lower Bound of the Number of Linear Active S-boxes

In this subsection, we revisit the practical security of MISTY structure with SPN round function against LC. Previous result[4] only gives a lower bound of the number of linear active s-boxes for some consecutive rounds when $\mathcal{B}_l = 5$, and the bound is far from tight. We present a new bound for the general case by carefully studying the relationship of the mask values between different rounds.

To this end, the propagation rule of the mask value should be investigated. As discussed in [5, 28], for Feistel structure, there exists a duality between differential characteristic and linear characteristic. For MISTY structure, this duality can be described as shown in Fig. 2. Thus, for differential characteristic, we have $\Delta Y_{i-1} = \Delta X_i \oplus \Delta X_{i+1}$, where $i \geq 1$, while for linear characteristic, we have $\Gamma X_i = \Gamma Y_{i-2} \oplus \Gamma Y_{i-1}$, where $i \geq 2$.

Note that for MISTY structure with SPN round function, the minimum number of linear active s-boxes over r-round is defined by

$$\mathcal{L}^{(r)} = \min_{(\Gamma Y_0, \Gamma Y_1, \ldots, \Gamma Y_{r+1}) \neq (0,0,\ldots,0)} \sum_{i=0}^{r-1} H_w(\Gamma Z_i).$$

We first present the following lemma.

[4] This result is obtained in [44], where MISTY structure is referred as 2-cell GF-NLFSR. It is shown that, when $\mathcal{B}_l = 5$, the lower bound of the number of linear active s-boxes is 3 for 4 rounds, 7 for 8 rounds, 11 for 12 rounds and 15 for 16 rounds.

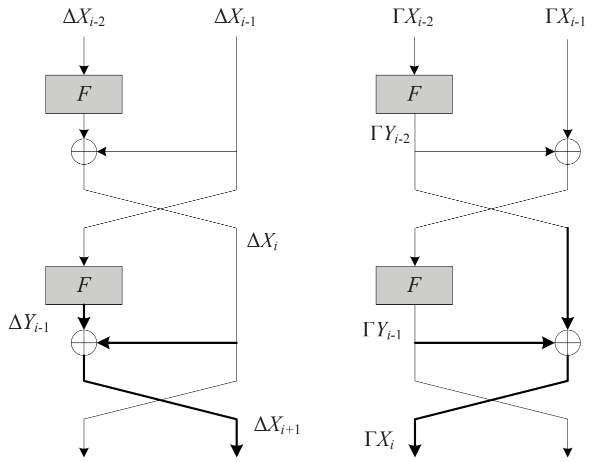

Fig. 2. MISTY structure (Left) and its Dual structure (Right)

Lemma 1. *Let ΓX_{i-1}, and $\Gamma Y_{i-1} \neq 0$ be the mask value of the input X_{i-1} and output Y_{i-1} in the i-th round, where $i \geq 1$ then*

$$H_w(P^T \cdot \Gamma X_{i-1}) + H_w(P^T \cdot \Gamma Y_{i-1}) \geq \mathcal{B}_l.$$

Proof. Let Z_{i-1} be the intermediate value after the substitution layer in the i-th round and ΓZ_{i-1} be the mask value of Z_{i-1}, then $Z_{i-1} = S(X_{i-1})$ and $Y_{i-1} = P \cdot Z_{i-1}$.

Assume $X_{i-1} = P \cdot V_{i-1}$, then $\Gamma V_{i-1} = P^T \cdot \Gamma X_{i-1}$. Further from $Y_{i-1} = P \cdot Z_{i-1}$, we get $\Gamma Z_{i-1} = P^T \cdot \Gamma Y_{i-1}$, thus

$$\begin{aligned} & H_w(P^T \cdot \Gamma X_{i-1}) + H_w(P^T \cdot \Gamma Y_{i-1}) \\ =\; & H_w(\Gamma V_{i-1}) + H_w(\Gamma Z_{i-1}) \\ =\; & H_w(\Gamma V_{i-1}) + H_w(\Gamma X_{i-1}) \\ \geq\; & \mathcal{B}_l. \end{aligned}$$

□

To further facilitate our proof, we introduce the following useful definition.

Definition 7. *For MISTY structure with SPN round function, let $O_r = (Y_i, Y_{i+1}, \ldots, Y_{i+r-1})$ be the output of the $(i+1)$-th, $(i+2)$-th, $\ldots$, $(i+r)$-th round functions, and $\Gamma O_r = (\Gamma Y_i, \Gamma Y_{i+1}, \ldots, \Gamma Y_{i+r-1})$ be the corresponding mask value of O_r, then the truncated form (or pattern) of ΓO_r is defined by a binary sequence $(a_i, a_{i+1}, \ldots, a_{i+r-1})$, where $a_{i+j} = 0$ if $\Gamma Y_{i+j} = 0$, and $a_{i+j} = 1$ if $\Gamma Y_{i+j} \neq 0$, where $j = 0, 1, \ldots, r-1$. Similarly, the truncated form (or pattern) of the mask value of the input X_i, and the intermediate value Z_i of the round function can also be defined.*

Lemma 2. *The minimum number of linear active s-boxes in any three consecutive rounds satisfies $\mathcal{L}^{(3)} \geq 2$.*

Proof. Without loss of generality, let's consider the first three rounds. We can divide the minimum number of linear active s-boxes into $2^3 - 1 = 7$ cases (the trivial (all zero) pattern is out of considering) according to the patterns of the output mask values.

Table 1. The minimum number of linear active s-boxes in 3-round

(a_0, a_1, a_2)	minimum number of linear active s-boxes
(0,1,1)	$\mathcal{L}_1^{(3)} \geq \mathcal{B}_l$
(1,0,1)	$\mathcal{L}_2^{(3)} \geq \mathcal{B}_l$
(1,1,1)	$\mathcal{L}_3^{(3)} \geq \mathcal{B}_l$
(1,1,0)	$\mathcal{L}_4^{(3)} \geq 2$

Table 2. The minimum number of linear active s-boxes in 4-round

(a_0, a_1, a_2, a_3)	minimum number of linear active s-boxes
(0,1,1,0)	$\mathcal{L}_1^{(4)} \geq \mathcal{B}_l$
(0,1,1,1)	$\mathcal{L}_2^{(4)} \geq \mathcal{B}_l + 1$
(1,0,1,1)	$\mathcal{L}_3^{(4)} \geq \mathcal{B}_l + 1$
(1,1,1,0)	$\mathcal{L}_4^{(4)} \geq \mathcal{B}_l$
(1,1,1,1)	$\mathcal{L}_5^{(4)} \geq \mathcal{B}_l + 1$
(1,1,0,1)	$\mathcal{L}_6^{(4)} \geq \mathcal{B}_l + 1$

Note that if $(a_0, a_1, a_2) \in \{(0,0,1), (0,1,0), (1,0,0)\}$, then it is an impossible pattern, thus we only need to consider $7 - 3 = 4$ possible patterns, whose corresponding linear bounds are listed in Table 1. The details are explained as follows:

If $(a_0, a_1, a_2) = (1,1,1)$, according to Lemma 1,

$$\begin{aligned}
&H_w(\Gamma Z_0) + H_w(\Gamma Z_1) + H_w(\Gamma Z_2) \\
&= H_w(P^T \cdot \Gamma Y_0) + H_w(P^T \cdot \Gamma Y_1) + H_w(P^T \cdot \Gamma Y_2) \\
&\geq H_w(P^T \cdot (\Gamma Y_0 \oplus \Gamma Y_1)) + H_w(P^T \cdot \Gamma Y_2) \\
&= H_w(P^T \cdot \Gamma X_2) + H_w(P^T \cdot \Gamma Y_2) \\
&\geq B_l,
\end{aligned}$$

thus $\mathcal{L}_3^{(3)} \geq \mathcal{B}_l$.

Similarly, if $(a_0, a_1, a_2) = (0,1,1)$ or $(1,0,1)$, we can obtain $\mathcal{L}_1^{(3)} \geq B_l$ and $\mathcal{L}_2^{(3)} \geq B_l$. While $(a_0, a_1, a_2) = (1,1,0)$, $H_w(\Gamma Z_0) + H_w(\Gamma Z_1) \geq 1 + 1 = 2$, thus $\mathcal{L}_4^{(3)} \geq 2$.

In total, we have $\mathcal{L}^{(3)} \geq 2$. □

Lemma 3. *The minimum number of linear active s-boxes in any four consecutive rounds satisfies* $\mathcal{L}^{(4)} \geq \mathcal{B}_l$.

Proof. Similarly, let's consider the first four rounds. Now that any three consecutive round has only 4 possible patterns, thus in total we need only to study $4 \times 2 = 8$ possible patterns by adding one round after the first three rounds, among which two patterns $(1,0,1,0)$ and $(1,1,0,0)$ are impossible, due to the impossibility of the sub-patterns $(0,1,0)$ and $(1,0,0)$. For those $8 - 2 = 6$ possible patterns, the corresponding bounds are listed in Table 2.

In fact, these bounds can be directly obtained based on the 3-round case.

(1) If $(a_0, a_1, a_2, a_3) = (0,1,1,0)$, then $\mathcal{L}_1^{(4)} = \mathcal{L}_1^{(3)} \geq \mathcal{B}_l$.

(2) If $(a_0, a_1, a_2, a_3) = (0, 1, 1, 1)$, then $\mathcal{L}_2^{(4)} \geq \mathcal{L}_1^{(3)} + 1 \geq \mathcal{B}_l + 1$.
(3) If $(a_0, a_1, a_2, a_3) = (1, 0, 1, 1)$, then $\mathcal{L}_3^{(4)} \geq \mathcal{L}_2^{(3)} + 1 \geq \mathcal{B}_l + 1$.
(4) If $(a_0, a_1, a_2, a_3) = (1, 1, 1, 0)$, then $\mathcal{L}_4^{(4)} = \mathcal{L}_3^{(3)} \geq \mathcal{B}_l$.
(5) If $(a_0, a_1, a_2, a_3) = (1, 1, 1, 1)$, then $\mathcal{L}_5^{(4)} \geq \mathcal{L}_3^{(3)} + 1 \geq \mathcal{B}_l + 1$.
(6) If $(a_0, a_1, a_2, a_3) = (1, 1, 0, 1)$, then $\mathcal{L}_6^{(4)} \geq 1 + \mathcal{L}_2^{(3)} \geq \mathcal{B}_l + 1$.

In total, we have $\mathcal{L}^{(4)} \geq \mathcal{B}_l$. □

Using a similar technique as shown in Lemma 3, we can obtain the minimum number of linear active s-boxes in any six consecutive rounds.

Table 3. The minimum number of linear active s-boxes in 6-round

$(a_0, a_1, a_2, a_3, a_4, a_5)$	minimum number of linear active s-boxes
(0,1,1,0,1,1)	$\mathcal{L}_1^{(6)} \geq 2 \times \mathcal{B}_l$
(0,1,1,1,0,1)	$\mathcal{L}_2^{(6)} \geq 2 \times \mathcal{B}_l$
(0,1,1,1,1,0)	$\mathcal{L}_3^{(6)} \geq \mathcal{B}_l + 2$
(0,1,1,1,1,1)	$\mathcal{L}_4^{(6)} \geq 2 \times \mathcal{B}_l$
(1,0,1,1,0,1)	$\mathcal{L}_5^{(6)} \geq 2 \times \mathcal{B}_l$
(1,0,1,1,1,0)	$\mathcal{L}_6^{(6)} \geq \mathcal{B}_l + 2$
(1,0,1,1,1,1)	$\mathcal{L}_7^{(6)} \geq 2 \times \mathcal{B}_l$
(1,1,0,1,1,0)	$\mathcal{L}_8^{(6)} \geq \mathcal{B}_l + 2$
(1,1,0,1,1,1)	$\mathcal{L}_9^{(6)} \geq \mathcal{B}_l + 3$
(1,1,1,0,1,1)	$\mathcal{L}_{10}^{(6)} \geq 2 \times \mathcal{B}_l$
(1,1,1,1,0,1)	$\mathcal{L}_{11}^{(6)} \geq 2 \times \mathcal{B}_l$
(1,1,1,1,1,0)	$\mathcal{L}_{12}^{(6)} \geq \mathcal{B}_l + 2$
(1,1,1,1,1,1)	$\mathcal{L}_{13}^{(6)} \geq 2 \times \mathcal{B}_l$

Lemma 4. *The minimum number of linear active s-boxes in any six consecutive rounds satisfies* $\mathcal{L}^{(6)} \geq \mathcal{B}_l + 2$.

Proof. The six-round encryption can be treated as a concatenation of two three-round encryptions, thus we have to consider $4 \times 4 = 16$ cases, among which three patterns $(1, 0, 1, 0, 1, 1)$, $(1, 1, 0, 0, 1, 1)$ and $(1, 1, 0, 1, 0, 1)$ are impossible, due to the impossible sub-patterns $(0, 1, 0)$, $(1, 0, 0)$ and $(0, 1, 0)$.

The bounds for the other 13 patterns are listed in Table 3, based on which one can deduce that $\mathcal{L}^{(6)} \geq \mathcal{B}_l + 2$. □

Lemma 5. *The minimum number of linear active s-boxes in any eight consecutive rounds satisfies* $\mathcal{L}^{(8)} \geq 2 \times \mathcal{B}_l + 1$.

Proof. From Table 2, $\mathcal{L}^{(4)} \geq \mathcal{B}_l$ if and only if the corresponding pattern

$$(a_0, a_1, a_2, a_3) = (0, 1, 1, 0) \quad \text{or} \quad (1, 1, 1, 0).$$

And in the other cases, $\mathcal{L}^{(4)} \geq \mathcal{B}_l + 1$.

Let's discuss how the above two patterns can be concatenated to form a 8-round pattern. The process can be divided into the following four cases:

(1) $(a_0, a_1, \ldots, a_7) = (\underline{0,1,1,0}, \underline{0,1,1,0}) = (0,1,\underline{1,0,0},1,1,0)$.

This is an impossible pattern since the sub-pattern $(1,0,0)$ is impossible.

(2) $(a_0, a_1, \ldots, a_7) = (\underline{0,1,1,0}, \underline{1,1,1,0}) = (\underline{0,1,1}, \underline{0,1,1}, \underline{1,0})$.

In this situation,

$$\mathcal{L}_1^{(8)} \geq \mathcal{L}_1^{(3)} + \mathcal{L}_1^{(3)} + 1 \geq 2 \times \mathcal{B}_l + 1.$$

(3) $(a_0, a_1, \ldots, a_7) = (\underline{1,1,1,0}, \underline{1,1,1,0}) = (\underline{1,1,1}, \underline{0,1,1}, \underline{1,0})$.

In this situation,

$$\mathcal{L}_1^{(8)} \geq \mathcal{L}_3^{(3)} + \mathcal{L}_1^{(3)} + 1 \geq 2 \times \mathcal{B}_l + 1.$$

(4) $(a_0, a_1, \ldots, a_7) = (\underline{1,1,1,0}, \underline{0,1,1,0}) = (1,1,\underline{1,0,0},1,1,0)$.

This is an impossible pattern since the sub-pattern $(1,0,0)$ is impossible.

From (1)(2)(3)(4), we get $\mathcal{L}^{(8)} \geq 2 \times \mathcal{B}_l + 1$ for these two possible patterns. While for all the other possible patterns, we have $\mathcal{L}^{(8)} \geq \mathcal{B}_l + (\mathcal{B}_l + 1) = 2 \times \mathcal{B}_l + 1$, which ends the proof. □

Lemma 6. *The minimum number of linear active s-boxes in any twelve consecutive rounds satisfies* $\mathcal{L}^{(12)} \geq 3 \times \mathcal{B}_l + 1$.

Proof. The lower bound of the linear active s-boxes in any twelve consecutive rounds can be deduced as follow:

$$\begin{aligned} \mathcal{L}^{(12)} &\geq \max\{4 \times \mathcal{L}^{(3)}, 2 \times \mathcal{L}^{(6)}, \mathcal{L}^{(8)} + \mathcal{L}^{(4)}\} \\ &\geq \max\{8, 2 \times \mathcal{B}_l + 4, 3 \times \mathcal{B}_l + 1\} \\ &\geq 3 \times \mathcal{B}_l + 1. \end{aligned}$$
□

Now we have obtained the lower bound of the linear active s-boxes for consecutive 4, 8, and 12 rounds. In general, we can obtain the follow theorem:

Theorem 1. *The minimum number of linear active s-boxes for* $4r$*-round MISTY structure with SPN round function satisfies*

$$\mathcal{L}^{(4r)} \geq \mathcal{B}_l \times r + \lfloor r/2 \rfloor.$$

Proof. From Lemma 3 and Lemma 5, we have $\mathcal{L}^{(4)} \geq \mathcal{B}_l$ and $\mathcal{L}^{(8)} \geq 2\mathcal{B}_l + 1$. Note that $\mathrm{lcm}(4,8) = 8$, thus we let $4r = 4r - 8m + 8m$, where $m \geq 0$ is an integer. Let $m = \lfloor r/2 \rfloor$, then $r - 2m \geq 0$. Now we get

$$\begin{aligned} \mathcal{L}^{(4r)} &= \mathcal{L}^{(4r-8m+8m)} \\ &\geq \mathcal{L}^{(4(r-2m))} + \mathcal{L}^{(8m)} \\ &\geq \mathcal{B}_l \times (r - 2m) + (2\mathcal{B}_l + 1) \times m \\ &= \mathcal{B}_l \times r + m \\ &= \mathcal{B}_l \times r + \lfloor r/2 \rfloor. \end{aligned}$$
□

Remark 1. Theorem 1 shows that the practical secure bound against LC for MISTY structure with SPN round function is also consistent with the case of Feistel structure with SPN round function. Thus both MISTY and Feistel structures possess a similar practical secure level from the viewpoint of resisting DC and LC.

From Theorem 1, we can revisit the practical security of p-Camellia against LC. The maximum differential probability of the s-box is $p_s = 2^{-6}$ and the linear branch number of the linear transformation is $\mathcal{B}_l = 5$, thus $\mathcal{L}^{(16)} \geq 4 \times 5 + 2 = 22$ which implies that the 16-round linear characteristic probability $p_l^{(16)} \leq \left(2^{-6}\right)^{22} = 2^{-132} < 2^{-128}$. This follows that the full round (18-round) p-Camellia is practically secure against LC.

4 Resistance to Other Attacks

There are several cryptanalytic approaches that should be considered other than DC and LC when designing a secure block cipher. In this section, we discuss the resistance of MISTY structure with SPN round function against integral cryptanalysis [21] and impossible differential cryptanalysis [6, 20]. We confirm the existence of 6-round integral distinguishers when the linear transformation of the round function employs binary matrix, and describe how to characterize 5/6/7-round impossible differentials through the matrix-based method [17, 18, 24, 26, 43].

4.1 Notations and Known Results

In the following subsections, for convenience, we will denote MISTY structure with SPN round function as introduced in Section 2 by $\mathcal{E}$, the diffusion matrix of $\mathcal{E}$ by $P = (p_{i,j})_{n\times n}$ and its inversion by $P^{-1} = (q_{i,j})_{n\times n}$. We will also use P_j to represent the j-th column vector of P, and $P_i^{(r)}$ to represent the i-th row vector of P.

Notations for Integral Distinguisher A set $\{a_i | a_i \in \mathbb{F}_{2^d}, 0 \leq i \leq 2^d - 1\}$ is *active*, if for any $0 \leq i < j \leq 2^d - 1$, $a_i \neq a_j$. A set $\{a_i | a_i \in \mathbb{F}_{2^d}, 0 \leq i \leq 2^d - 1\}$ is *passive* or *constant*, if for any $0 < i \leq 2^d - 1$, $a_i = a_0$. A set $\{a_i | a_i \in \mathbb{F}_{2^d}, 0 \leq i \leq 2^d - 1\}$ is *balanced*, if the bit-wise *XOR*-sum of all elements of the set is 0, that is $\bigoplus_{i=0}^{2^d-1} a_i = 0$.

We use **A** to denote a active set, **C** to denote a passive or constant set, and **B** to denote a balanced set. Sometimes we will use the letter "**D**" to represent an unknown word, but with the property that all **D**'s have the same value in the distinguisher.

Notations for Impossible Differential For MISTY structure, we will use $(\alpha_1, \alpha_2) \to (\beta_1, \beta_2)$ to denote a possible differential, where (α_1, α_2) (resp. (β_1, β_2)) is the input (resp. output) difference, and use $(\alpha_1, \alpha_2) \nrightarrow (\beta_1, \beta_2)$ to represent an impossible differential.

Known Results Due to the bijective property of the round function, for any block cipher with MISTY structure, there always exists a 4-round impossible differential $(\alpha, 0) \nrightarrow (\beta, \beta)$, where $\alpha, \beta \in \mathbb{F}_{2^d}^n$ be any non-zero values and 5-round integral distinguisher $(A, C) \to (B, ?)$, where A, B, and C denote an active state, a balanced state, and a passive state [21]. The question mark ? denotes an unknown state, i.e. the sum of values at this position couldn't be predicted.

4.2 Integral Distinguishers

Let's further consider the block cipher $\mathcal{E}$ with additional property that the diffusion layer employs a binary invertible matrix $P \in \mathbb{F}_2^{n\times n}$. The main result of this subsection is to confirm the existence of 6-round integral distinguishers for such a kind of block cipher.

A Simple Notation To describe these distinguishers more clearly, we simplify the notations for "balanced" and "unknown" states. From now on, the number "0" will be used to denote a balanced state, and "1" will be used to denote a unknown state with the property that if there are several "1"s in the distinguishers, they are of the same value.

For example, assume $n = 8$, and consider the following integral distinguisher

$$((C,C,C,C,C,C,C,C),(C,C,A,C,C,C,C,C)) \to ((D,B,D,D,B,D,D,B),(?,?,?,?,?,?,?,?))$$

Then within the above notation, such distinguisher can be simply denoted as

$$(L_C, R_3) \to ((1,0,1,1,0,1,1,0),?),$$

where L_C denotes that the left half is fixed to a constant, while R_3 represents that the third component of the right half of the input is active. The main convenience is to represent (D,B,D,D,B,D,D,B) simply by $(1,0,1,1,0,1,1,0)$.

6-Round Integral Distinguishers To confirm the existence of 6-round integral distinguisher of $\mathcal{E}$ when the linear transformation employs binary matrix, the following lemma is needed. Let's use $X_{i,l}$ to denote the l-th component of X_i.

Lemma 7. *Let $(X_0, X_1) = ((c,c,\ldots,c),(c,\ldots,c,x,c,\ldots,c)) \in \mathbb{F}_{2^d}^n \times \mathbb{F}_{2^d}^n$ be the input of $\mathcal{E}$, where $x \in \mathbb{F}_{2^d}$ is a variable in the j-th position of the right part of the input, and all c's are constants in $\mathbb{F}_{2^d}$ and they are not necessary to be identical. Assume the intermediate values after application of the non-linear transformations S in the $(i+1)$-th round is $Z_i = (Z_{i,1}, Z_{i,2}, \ldots, Z_{i,n})$. If x takes all values in $\mathbb{F}_{2^d}$, then*

- *if $p_{j,j} = 0$, we have for any $0 \le i \le 4$, $1 \le t \le n$, $Z_{i,t}$ is balanced.*
- *if $p_{j,j} = 1$, we have for $i = 0,1,2$, $1 \le t \le n$, $Z_{i,t}$ is balanced, while for $i = 3,4$, and $1 \le t \le n, t \ne j$, $Z_{i,t}$ is balanced.*

Proof. Let $(X_0, X_1) = ((c,c,\ldots,c),(c,\ldots,c,x,c,\ldots,c)) \in \mathbb{F}_{2^d}^n \times \mathbb{F}_{2^d}^n$ be the input of $\mathcal{E}$, where $x \in \mathbb{F}_{2^d}$ is a variable in the j-th position of the right part of the input, and all c's are constants in $\mathbb{F}_{2^d}$, then from the encryption procedure, we have

$$X_2 = (c,\ldots,c,x\oplus c,c,\ldots,c),$$

from which it's easy to show the balanced property for each word of Z_0, Z_1 and Z_2.

The cases for Z_3 and Z_4 are a little involved, in fact, we can calculate them as follows:

$$\begin{aligned} Z_3 &= S(X_3 \oplus K_4) \\ &= S(Y_1 \oplus Y_0 \oplus X_1 \oplus K_4) \\ &= S(P(Z_1) \oplus X_1 \oplus C'), \end{aligned} \tag{1}$$

where $C' = Y_0 \oplus K_4 = P(S(X_0 \oplus K_1)) \oplus K_4$ is some dn-bit unknown constant.

$$\begin{aligned} Z_4 &= S(X_4 \oplus K_5) \\ &= S(Y_2 \oplus Y_1 \oplus Y_0 \oplus X_1 \oplus K_5) \\ &= S(P(Z_2) \oplus P(Z_1) \oplus X_1 \oplus C''), \end{aligned} \tag{2}$$

where $C'' = Y_0 \oplus K_5 = P(S(X_0 \oplus K_1)) \oplus K_5$ is some dn-bit unknown constant.

Note that

$$Z_1 = S(X_1 \oplus K_2) = (c, \ldots, c, s_j(x \oplus k_{2,j}), c, \ldots, c) \triangleq (c, \ldots, c, z_{1,j}, c, \ldots, c), \tag{3}$$

and

$$Z_2 = S(X_2 \oplus K_3) = (c, \ldots, c, s_j(x \oplus c \oplus k_{3,j}), c, \ldots, c) \triangleq (c, \ldots, c, z_{2,j}, c, \ldots, c). \tag{4}$$

Let $[X]_t$ represent the t-th component of X. Below will deal with the cases for Z_3 and Z_4 according to the value of $p_{j,j}$.

The Case for Z_3. If $p_{j,j} = 0$, then according to Eq. (3), the t-th ($1 \le t \le n$) component of $P(Z_1) \oplus X_1$ has the following form:

$$[P(Z_1) \oplus X_1]_t = \begin{cases} c \text{ or } z_{1,j} \oplus c, & \text{if } t \neq j \\ x \oplus c, & \text{if } t = j \end{cases}$$

Since $z_{1,j} = s_j(x \oplus k_{2,j})$, according to Eq.(1), each component of Z_3 is balanced.

While if $p_{j,j} = 1$, the t-th ($1 \le t \le n$) component of $P(Z_1) \oplus X_1$ has the following form:

$$[P(Z_1) \oplus X_1]_t = \begin{cases} c \text{ or } z_{1,j} \oplus c, & \text{if } t \neq j \\ z_{1,j} \oplus x \oplus c, & \text{if } t = j \end{cases}$$

Since $z_{1,j} = s_j(x \oplus k_{2,j})$, according to Eq. (1), each component of Z_3, except the j-th one, is balanced.

The Case for Z_4. If $p_{j,j} = 0$, then according to Eq. (4), the t-th ($1 \le t \le n$) component of $P(Z_2) \oplus P(Z_1) \oplus X_1$ has the following form:

$$[P(Z_2) \oplus P(Z_1) \oplus X_1]_t = \begin{cases} c \text{ or } z_{1,j} \oplus z_{2,j} \oplus c, & \text{if } t \neq j \\ x \oplus c, & \text{if } t = j \end{cases}$$

Since $z_{1,j} \oplus z_{2,j} = s_j(x \oplus c \oplus k_{2,j}) \oplus s_j(x \oplus k_{3,j})$ represents the output difference of the S-box $s_j(\cdot)$, each possible value of $z_{1,j} \oplus z_{2,j}$ appears even times. According to Eq.(2), each component of Z_4 is balanced.

Similarly, if $p_{j,j} = 1$, then the t-th ($1 \le t \le n$) component of $P(Z_2) \oplus P(Z_1) \oplus X_1$ has the following form:

$$[P(Z_2) \oplus P(Z_1) \oplus X_1]_t = \begin{cases} c \text{ or } z_{1,j} \oplus z_{2,j} \oplus c, & \text{if } t \neq j \\ z_{1,j} \oplus z_{2,j} \oplus x \oplus c, & \text{if } t = j \end{cases}$$

Since $z_{1,j} \oplus z_{2,j} = s_j(x \oplus c \oplus k_{2,j}) \oplus s_j(x \oplus k_{3,j})$, according to Eq.(2), each component of Z_4, except the j-th one, is balanced. □

Now let's define the multiplication between a binary value a and a binary vector $V = (v_1, v_2, \ldots, v_n)$ by $a \cdot V = (a \cdot v_1, a \cdot v_2, \ldots, a \cdot v_n)$, where $a \cdot v_i$ means the multiplication of the two binary variables, then based on the above lemma, the following theorem can be obtained.

Theorem 2. *If the diffusion matrix of $\mathcal{E}$ is a binary invertible matrix P, then there always exists 6-round integral distinguisher in $\mathcal{E}$ of the following form:*

$$(L_C, R_j) \to (p_{j,j} \cdot P_j^T, ?),$$

where P_j^T denotes the transpose of P_j.

Proof. Let the input of 6-round $\mathcal{E}$ be

$$(X_0, X_1) = ((c, c, \ldots, c), (c, \ldots, c, x, c, \ldots, c)),$$

where the active position is j, then according to the encryption procedure, the l-th component of the left output, $1 \le l \le n$, after 6 rounds is

$$\begin{aligned} X_{6,l} &= Y_{4,l} \oplus Y_{3,l} \oplus Y_{2,l} \oplus Y_{1,l} \oplus Y_{0,l} \oplus X_{1,l} \\ &= P_l^{(r)} \cdot (Z_4 \oplus Z_3 \oplus Z_2 \oplus Z_1 \oplus Z_0) \oplus X_{1,l}. \end{aligned}$$

Let's further divide the proof into the following two cases:

Case 1: $p_{j,j} = 0$. In this situation, Lemma 1 tells that each component of Z_0, Z_1, Z_2, Z_3 and Z_4 is balanced, thus $X_{6,l}$ is balanced.

Case 2: $p_{j,j} = 1$. In this situation, Lemma 1 shows that each component of Z_0, Z_1 and Z_2 is balanced, and meanwhile, for $1 \le t \le n, t \ne j$, $Z_{3,t}$ and $Z_{4,t}$ are also balanced. Thus

$$\begin{aligned} \bigoplus_{x \in \mathbb{F}_{2^d}} X_{6,l} &= \bigoplus_{x \in \mathbb{F}_{2^d}} \left(P_l^{(r)} \cdot (Z_4 \oplus Z_3 \oplus Z_2 \oplus Z_1 \oplus Z_0) \oplus X_{1,l}\right) \\ &= \bigoplus_{x \in \mathbb{F}_{2^d}} P_l^{(r)} \cdot (Z_4 \oplus Z_3) \\ &= \bigoplus_{x \in \mathbb{F}_{2^d}} \bigoplus_{t=1}^{n} p_{l,t} \cdot (Z_{4,t} \oplus Z_{3,t}) \\ &= \bigoplus_{x \in \mathbb{F}_{2^d}} p_{l,j} \cdot (Z_{4,j} \oplus Z_{3,j}) \end{aligned} \tag{5}$$

From the definition of P, $p_{l,j} = 0$ will imply that for these positions l, $X_{6,l}$ are balanced.

Now the index $1 \le l \le n$ such that $p_{l,j} = 1$ should be considered. In these situations, $p_{l,j} = 1$, and Eq.(5) becomes

$$\bigoplus_{x \in \mathbb{F}_{2^d}} X_{6,l} = \bigoplus_{x \in \mathbb{F}_{2^d}} (Z_{4,j} \oplus Z_{3,j}).$$

Thus, the sum of $X_{6,l}$ are all equal to the sum of $Z_{4,j} \oplus Z_{3,j}$. From the calculation of $Z_{4,j}$ and $Z_{3,j}$ as described in the proof of Lemma 7, the sum of $Z_{4,j} \oplus Z_{3,j}$ over $x \in \mathbb{F}_{2^d}$ is indeed only dependent on the constants of the inputs corresponding to the passive components and the unknown round-keys. □

4.3 Impossible Differentials

The matrix-based method has been utilized to find the impossible differentials of SPN ciphers [24] as well as Feistel ciphers with SP or SPS round function [43]. This technique concentrates on the property of the matrix in the diffusion layer, and can apply the theory of linear algebra to detect truncated impossible differentials. Motivated by this approach, in this subsection, we discuss how to characterize the impossible differentials of $\mathcal{E}$. Remind that the diffusion matrix of $\mathcal{E}$ is $P = (p_{i,j})_{n\times n}$ and its inversion is $P^{-1} = (q_{i,j})_{n\times n}$.

As will be shown later, the process for finding impossible differentials of $\mathcal{E}$ resembles at a large extent the case of SPN ciphers, and all proofs of the proposed criteria are similar as that of [24], thus the details are omitted. For consistency, we use the same notations as in [24]. Particulary, we use e_j to denote an n-word state with the j-th position being non-zero and all other positions being zero.

Assume the input difference of $\mathcal{E}$ is $(\alpha, 0)$ with $\alpha \neq 0$, then according to the encryption procedure, the output differences in the first h_1 rounds, where $h_1 = 1, 2, 3, 4$, can be described as

$$\begin{array}{lcr}
(\quad \alpha & , & 0 \quad) \\
(\quad 0 & , & P \circ S(\alpha) \quad) \\
(\quad P \circ S(\alpha) & , & P \circ S(\alpha) \quad) \\
(\quad P \circ S(\alpha) & , & P \circ S \circ P \circ S(\alpha) \oplus P \circ S(\alpha)) \\
(P \circ S \circ P \circ S(\alpha) \oplus P \circ S(\alpha) & , & ? \quad)
\end{array}$$

where ? denotes some unknown difference that is not considered by us.

Similarly, assume the output difference of $\mathcal{E}$ is (β, β) with $\beta \neq 0$, then from the decryption direction, the output differences in the last h_2 rounds, where $h_2 = 1, 2, 3$, can be described as

$$\begin{array}{lcr}
(\ S^{-1} \circ P^{-1} \circ S^{-1} \circ P^{-1}(\beta) & , & S^{-1} \circ P^{-1}(\beta)) \\
(\quad S^{-1} \circ P^{-1}(\beta) & , & 0 \quad) \\
(\quad 0 & , & \beta \quad) \\
(\quad \beta & , & \beta \quad)
\end{array}$$

The above two evolutional properties of the differences are very useful for our study on the impossible differentials of MISTY structure with SPN round function.

5-round Impossible Differentials If we choose $h_1 = 3$ and $h_2 = 2$, and let $\alpha = e_i$, $\beta = e_j$, then we can use the following equation

$$P \circ S(e_i) = S^{-1} \circ P^{-1}(e_j) \tag{6}$$

to present a criterion to characterize 5-round impossible differentials of $\mathcal{E}$.

Proposition 3. *If there exists a $k \in \{1, 2, \ldots, n\}$, such that $H_w(p_{k,i}, q_{k,j}) = 1$, then $(e_i, 0) \nrightarrow (e_j, e_j)$ is a 5-round impossible differential of $\mathcal{E}$.*

6-round Impossible Differentials If we choose $h_1 = 3$ and $h_2 = 3$, and let $\alpha = e_i$, $\beta = e_j$, then the following equation

$$S^{-1} \circ P^{-1} \circ S^{-1} \circ P^{-1}(e_j) = P \circ S(e_i) \tag{7}$$

could be used to analyze the case of 6-round impossible differentials of $\mathcal{E}$. The criteria can be further divided into the following cases:

Proposition 4. *For any $1 \le i, j \le n$, let $U_i = \{r|p_{r,i} = 0\} = \{r_1, r_2, \ldots, r_u\}$, $V_j = \{t|q_{t,j} \neq 0\} = \{t_1, t_2, \ldots, t_v\}$, and*

$$M_{i,j} = (q_{r_a,t_b})_{u\times v} = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_u \end{pmatrix},$$

where each m_a is the a-th row vector of $M_{i,j}$, $a = 1, 2, \ldots, u$. If $U_i, V_j \neq \emptyset$, and there exists an $l \in \{1, 2, \ldots, u\}$, such that $H_w(m_l) = 1$, then $(e_i, 0) \nrightarrow (e_j, e_j)$ is a 4-round impossible differential of $\mathcal{E}$.

Proposition 5. *For any $1 \le i, j \le n$, let $U_i = \{r|p_{r,i} = 0\} = \{r_1, r_2, \ldots, r_u\}$, $V_j = \{t|q_{t,j} \neq 0\} = \{t_1, t_2, \ldots, t_v\}$ and*

$$M_{i,j} = (q_{r_a,t_b})_{u\times v} = (m_1, m_2, \ldots, m_v),$$

where each m_b is the b-th column vector of $M_{i,j}$, $b = 1, 2, \ldots, v$. If $U_i, V_j \neq \emptyset$, and there exists an $l \in \{1, 2, \ldots, v\}$, such that $\mathrm{rank}\{\{m_1, m_2, \ldots, m_v\}\backslash\{m_l\}\} < \mathrm{rank}\{m_1, m_2, \ldots, m_v\}$, *then $(e_i, 0) \nrightarrow (e_j, e_j)$ is a 6-round impossible differential of $\mathcal{E}$.*

Proposition 6. *For any $1 \le i, j \le n$, let $U_i = \{r|p_{r,i} = 0\} = \{r_1, r_2, \ldots, r_u\}$, $W_i = \{s|p_{s,i} \neq 0\} = \{s_1, s_2, \ldots, s_w\}$, $V_j = \{t|q_{t,j} \neq 0\} = \{t_1, t_2, \ldots, t_v\}$, and*

$$M_{i,j} = (q_{r_a,t_b})_{u\times v} = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_u \end{pmatrix},\ M'_{i,j} = (q_{s_a,t_b})_{w\times v} = \begin{pmatrix} m'_1 \\ m'_2 \\ \vdots \\ m'_w \end{pmatrix},$$

where each m_a (resp. m'_a) *denotes the a-th row vector of $M_{i,j}$* (resp. $M'_{i,j}$). *If $U_i, W_i, V_j \neq \emptyset$, and there exists an $l \in \{1, 2, \ldots, w\}$, such that* $\mathrm{rank}\{m_1, m_2, \ldots, m_u, m'_l\} = \mathrm{rank}\{m_1, m_2, \ldots, m_u\}$, *then $(e_i, 0) \nrightarrow (e_j, e_j)$ is a 6-round impossible differential of $\mathcal{E}$.*

We remind here that, if $\alpha = e_i$, $\beta = P(e_j)$, then Eq.(7) becomes the following

$$S^{-1} \circ P^{-1} \circ S^{-1}(e_j) = P \circ S(e_i) \tag{8}$$

based on which, finding 6-round impossible differentials of the form $(e_i, e_i) \nrightarrow (P(e_j), P(e_j))$ could be degenerated into the 5-round impossible differentials.

Proposition 7. *If there exists a $k \in \{1, 2, \ldots, n\}$, such that $H_w(p_{k,i}, q_{k,j}) = 1$, then $(e_i, 0) \nrightarrow (P(e_j), P(e_j))$ is a 6-round impossible differential of $\mathcal{E}$.*

7-Round Impossible Differentials If we choose $h_1 = 4$ and $h_2 = 3$, then the following equation

$$P \circ S \circ P \circ S(\alpha) \oplus P \circ S(\alpha) = S^{-1} \circ P^{-1} \circ S^{-1} \circ P^{-1}(\beta),$$

which is equivalent to

$$P^{-1} \circ S^{-1} \circ P^{-1} \circ S^{-1} \circ P^{-1}(\beta) = S \circ P \circ S(\alpha) \oplus S(\alpha) \tag{9}$$

could be used to analyze 7-round impossible differentials of $\mathcal{E}$. Let $\alpha = e_i$ and $\beta = P(e_j)$, the 7-round case could be degenerated into the 6-round case as follow

$$P^{-1} \circ S^{-1} \circ P^{-1} \circ S^{-1}(e_j) = S \circ P \circ S(e_i) \oplus S(e_i), \tag{10}$$

based on which, we can obtain similar criteria as [24] but with slight modification.

Proposition 8. *For any* $1 \leq i, j \leq n$, *let* $U_i = \{r \neq i | p_{r,i} = 0\} = \{r_1, r_2, \ldots, r_u\}$, $V_j = \{t | q_{t,j} \neq 0\} = \{t_1, t_2, \ldots, t_v\}$, *and*

$$M_{i,j} = (q_{r_a,t_b})_{u \times v} = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_u \end{pmatrix},$$

where each m_a *denotes the* a*-th row vector of* M_{ij}, $a = 1, 2, \ldots, u$. *If* $U_i, V_j \neq \emptyset$, *and there exists an* $l \in \{1, 2, \ldots, u\}$, *such that* $H_w(m_l) = 1$, *then* $(e_i, 0) \nrightarrow (P(e_j), P(e_j))$ *is a* 7*-round impossible differential of* $\mathcal{E}$.

Proposition 9. *For any* $1 \leq i, j \leq n$, *let* $U_i = \{r \neq i | p_{r,i} = 0\} = \{r_1, r_2, \ldots, r_u\}$, $V_j = \{t | q_{t,j} \neq 0\} = \{t_1, t_2, \ldots, t_v\}$, *and*

$$M_{i,j} = (q_{r_a,t_b})_{u \times v} = (m_1, m_2, \ldots, m_v),$$

where each m_b *is the* b*-th column vector of* $M_{i,j}$, $b = 1, 2, \ldots, v$. *If* $U_i, V_j \neq \emptyset$, *and there exists an* $l \in \{1, 2, \ldots, v\}$, *such that* $\mathrm{rank}\{\{m_1, m_2, \ldots, m_v\} \backslash \{m_l\}\} < \mathrm{rank}\{m_1, m_2, \ldots, m_v\}$, *then* $(e_i, 0) \nrightarrow (P(e_j), P(e_j))$ *is a* 7*-round impossible differential of* $\mathcal{E}$.

Proposition 10. *For any* $1 \leq i, j \leq n$, *let* $U_i = \{r \neq i | p_{r,i} = 0\} = \{r_1, r_2, \ldots, r_u\}$, $W_i = \{s \neq i | p_{s,i} \neq 0\} \cup \{i | p_{i,i} = 0\} = \{s_1, s_2, \ldots, s_w\}$, $V_j = \{t | q_{t,j} \neq 0\} = \{t_1, t_2, \ldots, t_v\}$, *and*

$$M_{i,j} = (q_{r_a,t_b})_{u \times v} = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_u \end{pmatrix}, \quad M'_{i,j} = (q_{r_a,t_b})_{w \times v} = \begin{pmatrix} m'_1 \\ m'_2 \\ \vdots \\ m'_w \end{pmatrix},$$

where each m_a (resp. m'_a) *denotes the* a*-th row vector of* $M_{i,j}$ (resp. $M'_{i,j}$). *If* $U_i, W_i, V_j \neq \emptyset$, *and there exists an* $l \in \{1, 2, \ldots, w\}$, *such that* $\mathrm{rank}\{m_1, m_2, \ldots, m_u, m'_l\} = \mathrm{rank}\{m_1, m_2, \ldots, m_u\}$, *then* $(e_i, 0) \nrightarrow (P(e_j), P(e_j))$ *is a* 7*-round impossible differential of* $\mathcal{E}$.

5 Conclusion

This paper revisits the practical security evaluation of MISTY structure with SPN round function against linear cryptanalysis. We unify the lower bound of the number of active s-boxes for both differential and linear characteristics. This demonstrates a similar secure level for both MISTY structure and Feistel structure from the viewpoint of resisting DC and LC.

Meanwhile, the resistance of MISTY structure with SPN round function against other kinds of cryptanalytic approaches such as integral and impossible differential cryptanalysis are also studied. The existence of 6-round integral distinguisher is confirmed when the diffusion layer employs a binary invertible matrix, and the criteria for characterizing 5/6/7-round impossible differentials are described. These results will benefit us to understand the security level of MISTY structure.

Acknowledgment

The work in this paper is supported by the National Natural Science Foundation of China (No: 61070215, 61103192), the Program for Changjiang Scholars and Innovative Research Team in University of Ministry of Education of China (No: IRT1012), and the Fund for Creative Research Groups of the Natural Science Foundation of Hunan Province, China (No: 11FH002).

References

1. Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: a 128-Bit block cipher suitable for multiple platforms – design and analysis. SAC 2000, LNCS 2012, pp. 39–56, Springer, 2001.
2. Kazumaro Aoki, and Kazuo Ohta. Strict evaluation of the maximum average of differential probability and the maxumum average of linear probability. IEICE Trans. Fundamentals E80-A(1), pp. 2–8, 1997.
3. Thomas Baignères and Matthieu Finiasz. Dial C for Cipher. SAC 2006, LNCS 4356, pp. 76–95, Springer, 2007.
4. Thomas Baignères and Matthieu Finiasz. KFC - The Krazy Feistel Cipher. ASIACRYPT 2006, LNCS 4284, pp. 380–395, Springer, 2006.
5. Eli Biham. On Matsui's linear cryptanalysis. EUROCRYPT 1994, LNCS 950, pp. 341–355, Springer, 1995.
6. Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. EUROCRYPT 1999, LNCS 2595, pp.12–23, Springer 1999.
7. Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, Vol 3, pp. 3–72, Springer, 1991.
8. Andrey Bogdanov. On unbalanced Feistel networks with contracting MDS diffusion. Designs, Codes, and Cryptography, 59(1-3), pp. 35–58, Springer, 2011.
9. Joan Daemen. Cipher and hash function design strategies based on linear and differential cryptanalysis, Doctoral Dissertation, March 1995, K.U.Leuven
10. Joan Daemen, Vincent Rijmen. The wide trail design strategy. IMA Cryptography and Coding 2001, LNCS 2260, pp. 222–238, Springer, 2001.
11. Joan Daemen , Lars Ramkilde Knudsen, Vincent Rijmen. The block cipher Square. FSE 1997, LNCS 1267, pp. 149–165, Springer, 1997.
12. Joan Daemen, and Vincent Rijmen. The desigh of Rijndael–AES, the advanced encryption standard. Springer, 2002.
13. Henri Gilbert and Marine Minier. New results on the pseudorandomness of some blockcipher constructions. FSE 2001, LNCS 2355, pp. 248–266, Springer, 2002.
14. Yasuo Hatano, Hiroki Sekine and Toshinobu Kaneko. Higher order diffrential attack of Camellia (II). SAC 2002, LNCS 2595, pp. 129-146, Springer, 2003.
15. Seokhie Hong, Sangjin Lee, Jongin Lim, Jaechul Sung, Donghyeon Cheon, and Inho Cho. Provable security against differential and linear cryptanalysis for the SPN structure. FSE 2000, LNCS 1978, pp. 273–283, Springer, 2001.
16. Ju-Sung Kang, Seokhie Hong, Sangjin Lee, Okyeon Yi, Choonsik Park, Jongin Lim. Practial and Provable Security against Differential and Linear Cryptanalysis for Substitution-Permutation Networks. ETRI Journal, 23(4): 158-167. 2001.
17. Jongsung Kim, Seokhie Hong, Jaechul Sung, Sanjin Lee, Jonggin Lim, and Soohak Sung. Impossible differential cryptanalysis for block cipher structures. INDOCRYPT 2003, LNCS 2904, pp. 82-96, Springer, 2003.
18. Jongsung Kim, Seokhie Hong, Jongin Lim. Impossible differential cryptanalysis using matrix method. Discrete Mathematics, Vol 310, Issue 5, pp. 988–1002, Elsevier, 2010.

19. Lars Ramkilde Knudsen. Pracital secure Feistel ciphers. FSE 1994, LNCS 809, pp. 211–221, Springer, 1994.
20. Lars Ramkilde Knudsen. DEAL – a 128-bit block cipher. Technical Report 151, Department of Informatics, University of Bergen, Norway, Feb. 1998.
21. Lars Ramkilde Knudsen, David Wagner. Integral cryptanalysis. FSE 2002, LNCS 2365, pp. 112–127, Springer, 2002.
22. Masayuki Kanda. Practical security evaluation against differential and linear cryptanalysis for Feistel ciphers with SPN round function. SAC 2000, LNCS 2012, pp. 324–338, Springer, 2001.
23. Xuejia Lai, James L. Massey, Sean Murphy. Markov ciphers and differential cryptanalysis. EUROCRYPT 1991, LNCS 547, pp. 17–38, Springer, 1991.
24. Ruilin Li, Bing Sun, and Chao Li. Impossible differential cryptanalysis of SPN ciphers. IET Information Security, Vol 5, Issue 2, pp. 111–120, 2011. Also avaiable through http://eprint.iacr.org/2010/307.
25. Ping Li, Bing Sun, and Chao Li. Integral cryptanalysis of ARIA. Inscrypt 2009, LNCS 6151, pp. 1–14, Springer, 2010.
26. Yiyuan Luo, Zhongming Wu, Xuejia Lai, Guang Gong. Unified impossible differential cryptanalysis on block cipher structures. Cryptology ePrint Archive, Report 2009/627. Available through: http://eprint.iacr.org/2009/627.
27. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. EUROCRYPT 1993, LNCS 765, pp. 386–397, Springer, 1994.
28. Mitsuru Matsui. On correlation between the order of S-boxes and the strength of DES. EUROCRYPT 1994, LNCS 950, pp. 366–375, Springer, 1995.
29. Mitsuru Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. FSE 1996, LNCS 1039, pp. 205–218, Springer, 1996.
30. Mitsuru Matsui. New block encryption algorithm MISTY. FSE 1997, LNCS 1267, pp. 54–68, Springer, 1997.
31. Kaisa Nyberg. Linear approximation of block ciphers. EUROCRYPT 1994, LNCS 950, pp. 439–444, Springer, 1995.
32. Kaisa Nyberg, and Lars Ramkilde Knudsen. Provable security against a differential attcks. Journal of Cryptology, 8(1), pp. 27–37, Springer, 1995.
33. Sangwoo Park, Soo Hak Sung, Sanjin Lee, and Jongin Lim. Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES. FSE 2003, LNCS 2887, pp. 247–260, Springer, 2003.
34. Vincent Rijmen, Joan Daemon, Bart Preneel, Antoon Bosselaers, and Erik De Win. The cipher SHARK, FSE 1996, LNCS 1039, pp. 99–111, Springer, 1996.
35. Kyoji Shibutani. On the diffusion of generalized Feistel structures regarding differential and linear cryptanalysis. SAC 2010, LNCS 6544, pp. 211–228, Springer, 2011.
36. Taizo Shirai and Kyoji Shibutani. Improving immunity of Feistel ciphers against differential cryptanalysis by using multiple MDS matrices. FSE 2004, LNCS 3017, pp. 260–278, Sorubger, 2004.
37. Taizo Shirai, and Bart Preneel. On Feistel ciphers using optimal diffusion mappings across multiple rounds. ASIACRYPT 2004, LNCS 3329, pp. 1–15, 2004.
38. Taizo Shirai, Kyoji Shibutani. On Feistel structures using a diffusion switching mechanism. FSE 2006, LNCS 4047, pp. 41–56. Springer, 2006.
39. Taizo Shirai, Kiyomichi Araki. On generalized Feistel structures using the diffusion switching mechanism. IEICE Trans. Fundamentals E91-A(8), pp. 2120–2129, 2008.
40. Specification of the 3GPP confidentiality and Integrity algorithm KASUMI. Available through http://www.etsi.org/.
41. Serge Vaudenay. Decorrelation: a theory for block cipher security. Journal of Cryptology, Vol 16, Issue 4, pp. 249–286, Springer, 2003.
42. Wenling Wu, Wentao Zhang, and Dongdai Lin. Security on generalized Feistel scheme with SP round function. Int. J. Network Security, vol. 3, No. 3, pp. 215–224, 2006.

43. Yuechuan Wei, Ping Li, Bing Sun, Chao Li. Impossible differential cryptanalysis on Feistel ciphers with SP and SPS round functions. ACNS 2010, LNCS 6123, pp. 105–122, Springer, 2010.
44. Huihui Yap, Khoongming Khoo, and Axel Poschmann. Parallelizing the Camellia and SMS4 block ciphers. AFRICACRYPT 2010, LNCS 6055, pp. 387–406, Springer, 2010.

A Distinguishing Properties of p-Camellia

A.1 Brief Description of p-Camellia

The block cipher p-Camellia [5] shares the same round function and the FL/FL^{-1} transformation as that of Camellia, except that the high-level structure is modified from Feistel to MISTY. One can refer Fig. 3 and Fig. 4 to compare the difference between Camellia and p-Camellia.

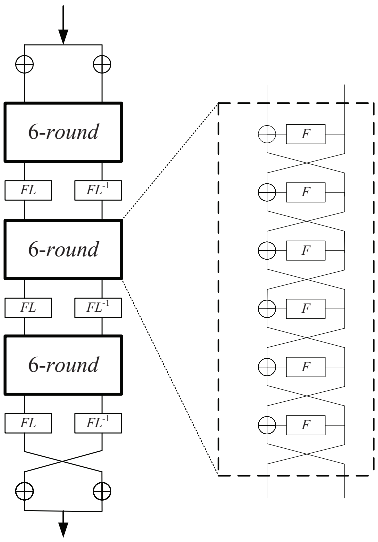

Fig. 3. Description of Camellia

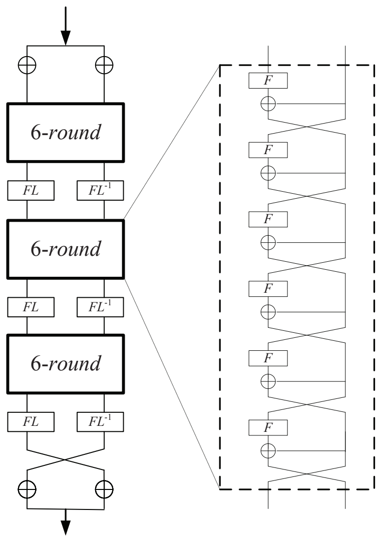

Fig. 4. Description of p-Camellia

The round function of p-Camellia (Camellia) is SPN type. It consists of three layers of operations: a round key addition layer, a substitution layer and a diffusion layer. The round key addition layer is defined by the XOR of the round-key and the input. The substitution layer is a non-linear bijective transformation S over $\mathbb{F}_{2^8}^8$ defined by eight parallel s-boxs on $\mathbb{F}_{2^8}$ as follow:

$$S : \mathbb{F}_{2^8}^8 \to \mathbb{F}_{2^8}^8, \quad S(\cdot) = (s_1(\cdot), s_2(\cdot), s_3(\cdot), s_4(\cdot), s_2(\cdot), s_3(\cdot), s_4(\cdot), s_1(\cdot)),$$

where $s_1(\cdot)$, $s_2(\cdot)$, $s_3(\cdot)$, and $s_4(\cdot)$ are some 8×8 s-boxes.

[5] We use the same notations as in [44]. In fact, there is a *slight distinction* between the basic notation for Feistel structure in [1] and as that in [44]. However, this dose not influence our analysis.

The diffusion layer which provides the avalanche effect employs an invertible linear transformation P defined over $\mathbb{F}_2^{8\times 8}$. P and its inversion P^{-1} are defined by the following binary matrices

$$P = \begin{pmatrix} 1&0&1&1&0&1&1&1 \\ 1&1&0&1&1&0&1&1 \\ 1&1&1&0&1&1&0&1 \\ 0&1&1&1&1&1&1&0 \\ 1&1&0&0&0&1&1&1 \\ 0&1&1&0&1&0&1&1 \\ 0&0&1&1&1&1&0&1 \\ 1&0&0&1&1&1&1&0 \end{pmatrix}, \quad P^{-1} = \begin{pmatrix} 0&1&1&1&0&1&1&1 \\ 1&0&1&1&1&0&1&1 \\ 1&1&0&1&1&1&0&1 \\ 1&1&1&0&1&1&1&0 \\ 1&1&0&0&1&0&1&1 \\ 0&1&1&0&1&1&0&1 \\ 0&0&1&1&1&1&1&0 \\ 1&0&0&1&0&1&1&1 \end{pmatrix}.$$

A.2 Integral Distinguishers of Reduced-Round p-Camellia

We can apply the criterion from Section 4.2 to find the 6-round integral distinguishers of p-Camellia, all of which have been verified experimentally.

6-round Integral Distinguishers of p-Camellia

$$((C,C,C,C,C,C,C,C),(A,C,C,C,C,C,C,C)) \to ((D,D,D,B,D,B,B,D),(?,?,?,?,?,?,?,?))$$
$$((C,C,C,C,C,C,C,C),(C,A,C,C,C,C,C,C)) \to ((B,D,D,D,D,D,B,B),(?,?,?,?,?,?,?,?))$$
$$((C,C,C,C,C,C,C,C),(C,C,A,C,C,C,C,C)) \to ((D,B,D,D,B,D,D,B),(?,?,?,?,?,?,?,?))$$
$$((C,C,C,C,C,C,C,C),(C,C,C,A,C,C,C,C)) \to ((D,D,B,D,B,B,D,D),(?,?,?,?,?,?,?,?))$$
$$((C,C,C,C,C,C,C,C),(C,C,C,C,A,C,C,C)) \to ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$$
$$((C,C,C,C,C,C,C,C),(C,C,C,C,C,A,C,C)) \to ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$$
$$((C,C,C,C,C,C,C,C),(C,C,C,C,C,C,A,C)) \to ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$$
$$((C,C,C,C,C,C,C,C),(C,C,C,C,C,C,C,A)) \to ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$$

Besides the above 6-round integral distinguishers, according to the special arrangement of s-boxes in the substitution layer, we also detect the following 7-round integral distinguishers of p-Camellia *without* the FL/FL^{-1} transformation. The proof can be provided based on the counting methods (see e.g. [14, 25]).

7-round Integral Distinguishers of p-Camellia *without* FL/FL^{-1}

$$((C,C,A_3,A_4,A_5,C,C,C),(C,C,C,C,C,C,C,C)) \to ((D,D,D,B,D,B,B,D),(?,?,?,?,?,?,?,?))$$
$$((A_1,C,C,A_4,C,A_6,C,C),(C,C,C,C,C,C,C,C)) \to ((B,D,D,D,D,D,B,B),(?,?,?,?,?,?,?,?))$$
$$((A_1,A_2,C,C,C,C,A_7,C),(C,C,C,C,C,C,C,C)) \to ((D,B,D,D,B,D,D,B),(?,?,?,?,?,?,?,?))$$
$$((C,A_2,A_3,C,C,C,C,A_8),(C,C,C,C,C,C,C,C)) \to ((D,D,B,D,B,B,D,D),(?,?,?,?,?,?,?,?))$$

where "$A_i \| A_j \| A_k$" denotes an active state of 3-byte with positions being (i,j,k).

A.3 Impossible Differentials of Reduced-Round p-Camellia

According to the definition of P and P^{-1} in the diffusion layer, we can apply the criteria from Section 4.3 to detect reduced-round impossible differentials in p-Camellia.

5-round Impossible Differentials of p-Camellia From Proposition 3, for any $1 \leq i, j \leq 8$, $(e_i, 0) \nrightarrow (e_j, e_j)$ is a 5-round impossible differential of p-Camellia, since we can find a $1 \leq k \leq 8$ such that $p_{k,i} + q_{k,j} = 1$.

6-round Impossible Differentials of p-Camellia

Case 1. From Proposition 4, we do not find 6-round impossible differentials of p-Camellia.

Case 2. Table 4 shows 6-round impossible differentials of p-Camellia found by Proposition 5.

Case 3. Table 5 shows 6-round impossible differentials of p-Camellia found by Proposition 6.

Case 4. From Proposition 7, for any $1 \leq i, j \leq 8$, $(e_i, 0) \nrightarrow (P(e_j), P(e_j))$ is a 6-round impossible differential of p-Camellia.

Table 4. Case 2: 6-round impossible differentials $e_i \nrightarrow e_j$ of p-Camellia

i	j	i	j	i	j	i	j
1	1, 2, 5	2	2, 3, 6	3	3, 4, 7	4	1, 4, 8

Table 5. Case 3: 6-round impossible differentials $e_i \nrightarrow e_j$ of p-Camellia

i	j	i	j	i	j	i	j
1	1, 4, 6, 7	3	2, 3, 5, 8	5	1	7	3
2	1, 2, 7, 8	4	3, 4, 5, 6	6	2	8	4

The following two examples explain the procedure when utilizing Proposition 4 and 5 to detect the 6-round impossible differential $(e_1, 0) \nrightarrow (e_1, e_1)$.

Example 1. Given $i = j = 1$, then $U_1 = \{4, 6, 7\}$, and $V_1 = \{2, 3, 4, 5, 8\}$, thus

$$M_{1,1} = \begin{pmatrix} 1\,1\,0\,1\,\mathbf{0} \\ 1\,1\,0\,1\,\mathbf{1} \\ 0\,1\,1\,1\,\mathbf{0} \end{pmatrix} \triangleq (m_1, m_2, m_3, m_4, m_5).$$

One can verify that

$$\text{rank}\{\{m_1, m_2, m_3, m_4, m_5\} \backslash \{m_5\}\} = 2 < 3 = \text{rank}\{m_1, m_2, \ldots, m_5\},$$

thus $(e_1, 0) \nrightarrow (e_1, e_1)$ is a 6-round impossible differential of p-Camellia.

Example 2. Given $i = j = 1$, then $U_1 = \{4, 6, 7\}$, $W_1 = \{1, 2, 3, 5, 8\}$, and $V_1 = \{2, 3, 4, 5, 8\}$, thus

$$M_{1,1} = \begin{pmatrix} 1\,1\,0\,1\,0 \\ 1\,1\,0\,1\,1 \\ 0\,1\,1\,1\,0 \end{pmatrix} = \begin{pmatrix} m_1 \\ m_2 \\ m_3 \end{pmatrix}, \quad M'_{1,1} = \begin{pmatrix} 1\ 1\ 1\ 0\ 1 \\ \mathbf{0\ 1\ 1\ 1\ 1} \\ 1\ 0\ 1\ 1\ 1 \\ 1\ 0\ 0\ 1\ 1 \\ 0\ 0\ 1\ 0\ 1 \end{pmatrix} = \begin{pmatrix} m'_1 \\ m'_2 \\ m'_3 \\ m'_4 \\ m'_5 \end{pmatrix}.$$

One can see that $m'_2 = m_1 + m_2 + m_3$, thus

$$\text{rank}\{m_1, m_2, m_3, m'_2\} = \text{rank}\{m_1, m_2, m_3\},$$

accordingly, we obtain the same 6-round impossible differential $(e_1, 0) \nrightarrow (e_1, e_1)$.

7-round Impossible Differentials of p-Camellia According to Proposition 8, 9, and 10, $(e_i, 0) \nrightarrow (P(e_j), P(e_j))$ is a 7-round impossible differential of p-Camellia, where i, j are chosen from Table 4 and Table 5.