Some Observations on MISTY Structure with SPN Round Function

Ruilin Li[1], Bing Sun[1], and Chao Li[1,2]

[1]Department of Mathematics and System Science, Science College,
National University of Defense Technology, Changsha, 410073, China
securitylrl@gmail.com, happy_come@163.com
[2]State Key Laboratory of Information Security, Institute of Software,
Chinese Academy of Sciences, Beijing, 100190, China
lichao_nudt@sina.com

Abstract. MISTY structure is a kind of block cipher structure that can provide provable security against differential and linear cryptanalysis. In this paper, we present some distinguishing properties of MISTY structure with SPN round function. We first show the existence of 6-round integral distinguishers when the linear transformation in the diffusion layer is binary. Then we discuss how to characterize 5/6/7-round impossible differentials through the matrix-based method. According to our analysis, the distinguishing bounds on the block cipher p-Camellia which is proposed at Africacrypt 2010 can be improved.

Keywords: Block ciphers, Block cipher structures, MISTY, SPN, Distinguisher, Integral, Impossible differential

1 Introduction

1.1 Backgrounds and Related Works

High-level structures play an essential role in designing block ciphers. There are many well-known block cipher structures, such as Feistel structure, SPN structure, MISTY structure, Lai-Massay structure, etc. Besides the overall structure, the form of the round function is another important ingredient that should be considered. Since most of the current block cipher structures could provide the security against differential cryptanalysis [3] (DC) and linear cryptanalysis [14] (LC), offer pseudo-randomness and super pseudo-randomness [13], choosing which kind of round function becomes a key step in the designment of a secure cryptographic algorithm. 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, including Camellia, SMS4, CLEFIA, etc. adopt such kind of round functions.

In [4], a new kind of generalized unbalanced Feistel network structure with n sub-blocks, called n-cell GF-NLFSR, was proposed with provable security against DC and LC. Later in [20], n-cell GF-NLFSR with SPN round function was shown to be practical secure against DC by using a similar approach as [9]. Especially when $n = 2$ and $n = 4$, two new block ciphers called p-Camellia and p-SMS4, which adopt GF-NLFSR as the overall structure while choose the components of the block cipher Camellia and SMS4 as the corresponding round functions, are proposed, and their security against LC as well as many other cryptanalytic methods are discussed.

In fact, when $n = 2$, GF-NLFSR is reduced to a classic block cipher structure, the so-called MISTY structure [15], which was introduced by Matsui and recommended as an alternative scheme of Feistel structure, due to its provable security against DC and LC. In [5], Gilbert and Minier formalize the MISTY structure as the L-scheme and referred the dual structure as the R-scheme and provide the proof of (super) pseudo-randomness. Besides providing provable security, 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 [16], and meanwhile, as the basic low-level structure of the round function and the component in block ciphers MISTY1 [16], MISTY2, and KASUMI [19].

1.2 Main Results and Outline of This Paper

For n-cell GF-NLFSR, [11] and [17] demonstrate some distinguishing properties: there exists n^2-round integral distinguisher [8] and $(n^2 + n - 2)$-round impossible differential distinguisher [2, 7]. When $n = 2$ (the MSITY case), the length of such two distinguishers both correspond to 4-round. But, can these bounds be improved especially when the round function is SPN-type?

In this paper, we present some distinguishing properties of MISTY structure with SPN round function. We show that there always exists 6-round integral distinguisher when the linear transformation in the diffusion layer is binary. Meanwhile, by adopting the matrix based method, we demonstrate how to characterize 5/6/7-round impossible differentials. All of these results can be applied to the block cipher p-Camellia. In [20], the designers of p-Camellia confirm the existence of only 4-round integral distinguisher and impossible differential distinguisher, while using our results, we could detect 6/7-round integral distinguishers and 5/6/7-round impossible differentials, which significantly improve the distinguishing bounds.

The outline of this paper is as follows: some preliminaries are introduced in Section 2. Section 3 presents an interesting result on 6-round integral distinguishers of MISTY structure with SPN round function that employs a binary diffusion matrix. Section 4 studies the impossible differentials properties of MISTY structure with SPN round function. Section 5 applies these results to p-Camellia. And finally, Section 6 concludes this paper.

2 Preliminaries

2.1 MISTY Structure

Consider any block cipher that employs a MISTY structure, see Fig. 1 (Left). Let (L_{i-1}, R_{i-1}) be the $2dn$-bit input in the i-th round, then the output is defined by

$$\begin{cases} L_i = R_{i-1}, \\ R_i = R_{i-1} \oplus F(L_{i-1}, K_i), \end{cases}$$

where $F(\cdot, \cdot)$ is the round function and K_i is the round key. Note that 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 $P = (L_0, R_0)$, then after iterating the above round transformation r times, the ciphertext is defined as (R_r, L_r).

Block ciphers with MISTY structure can be further categorized into different groups according to the definition of the round function F. For instance, the round function of the block cipher

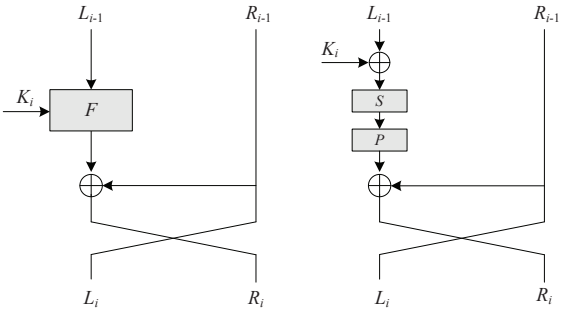

Fig. 1. MISTY Structure (Left) and MISTY Structure with SPN Round Function (Right)

MISTY2 adopts a recursive structure, where the round function itself uses another small MISTY structure. While the block cipher p-Camellia employs MISTY structure with SPN round function.

In this paper, we focus on block ciphers with MISTY structure and SPN round function, see Fig.1 (Right). More precisely, the round function 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 simply by the exclusive OR (XOR) of the round-key and the input. The substitution layer is a non-linear bijective transformation on $\mathbb{F}_{2^d}^n$ defined by n parallel S-boxs on $\mathbb{F}_{2^d}$, i.e. $S(\cdot) = (s_1(\cdot), s_2(\cdot), \ldots, s_n(\cdot))$. The diffusion layer employs an invertible linear transformation P defined over $\mathbb{F}_{2^d}^{n\times n}$. In the following sections, we will denote such a kind of block cipher by $\mathcal{E}$, and further denote 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 denote the j-th column vector of P, and $P_i^{(r)}$ to denote the i-th row vector of P.

Aided by Fig. 2, some useful notations used throughout this paper are given: X_i and Y_i denote the input and output variable of the $(i+1)$-th round function, K_{i+1} denote the $(i+1)$-th round-key, i.e. $Y_{i+1} = F(X_i \oplus K_{i+1})$. Z_i denote the intermediate variable after the confusion layer in the round function, i.e. $Z_i = S(X_i \oplus K_{i+1})$ and $Y_i = P(Z_i)$.

2.2 Known Results

Let $X = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{2^d}^n$ be an n-word state with each word being d-bit, ΔX be the difference of X and X', where the difference is the XOR difference, i.e., $\Delta X = X \oplus X'$. Given a MISTY structure, let $(\alpha_1, \alpha_2) \to (\beta_1, \beta_2)$ denote a possible differential with (α_1, α_2) (resp. (β_1, β_2)) the input (resp. output) difference, and let $(\alpha_1, \alpha_2) \nrightarrow (\beta_1, \beta_2)$ represent an impossible differential.

The following definition is needed for integral distinguishers.

Definition 1. *A set* $\{a_i | a_i \in \mathbb{F}_{2^b}, 0 \le i \le 2^b - 1\}$ *is* active, *if for any* $0 \le i < j \le 2^b - 1$, $a_i \ne a_j$. *We use* $\mathbf{A}$ *to denote the active set.*

Definition 2. *A set* $\{a_i | a_i \in \mathbb{F}_{2^b}, 0 \le i \le 2^b - 1\}$ *is* passive *or* constant, *if for any* $0 < i \le 2^b - 1$, $a_i = a_0$. *We use* $\mathbf{C}$ *to denote the passive set.*

Definition 3. *A set* $\{a_i | a_i \in \mathbb{F}_{2^b}, 0 \le i \le 2^b - 1\}$ *is* balanced, *if the* XOR*-sum of all element of the set is* 0, *that is* $\bigoplus_{i=0}^{2^b-1} a_i = 0$. *We use* $\mathbf{B}$ *to denote the balanced set.*

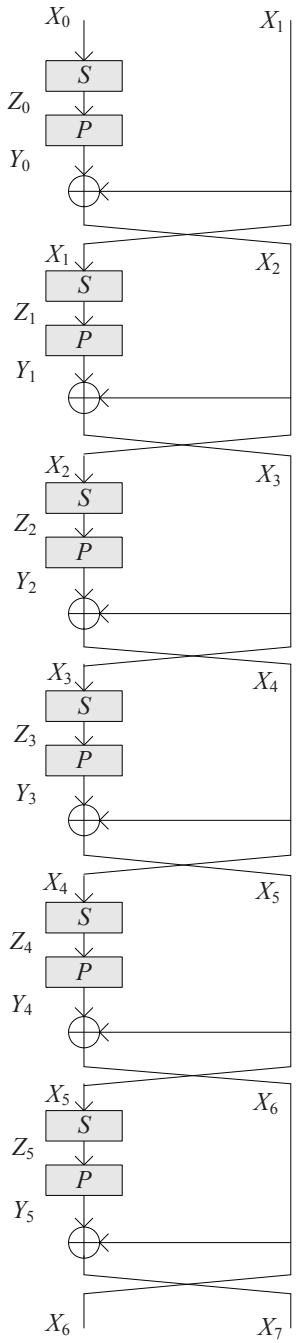

Fig. 2. MSITY structure with SPN round function (The round-key addition layer is omitted).

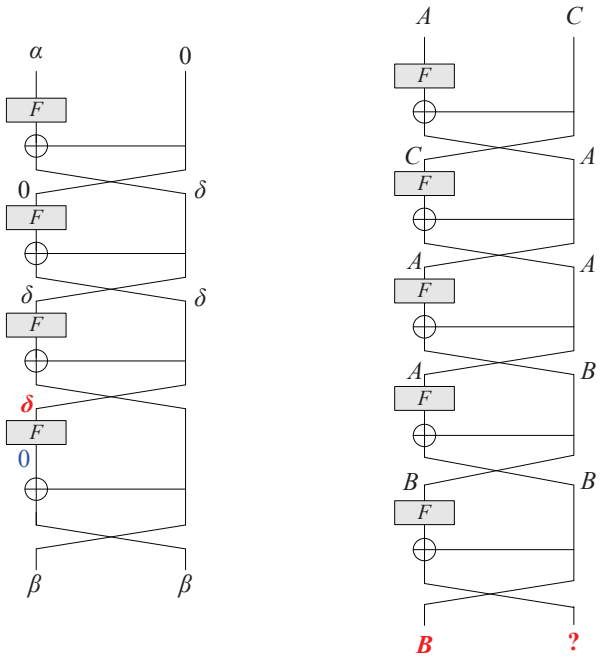

Fig. 3. Impossible differentials (Left) and integrals (Right) of MISTY structure

Refer to Fig. 3, due to the bijective property of the round function, for any block cipher with MISTY structure, there always exists 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 [8] $(A, C) \rightarrow (B, ?)$, where A, B, and C denotes an active state, a balanced state, and a passive state. The question mark ? denotes an unknown state, i.e., the sum of values at this position couldn't be predicted.

It should be emphasized here that, in the following sections, we will sometimes use the letter "**D**" to represent some unknown state, but with the property that all D's have the same value in the distinguisher.

3 Integrals of MISTY Structure with SPN Round Function

3.1 A Simple Notation

We concentrate block ciphers with MISTY structure and SPN round function as mentioned in Section 2. Let's further consider such block cipher with additional property that the diffusion layer employs a binary invertible matrix P, that is to say, $P \in \mathbb{F}_2^{n \times n}$. The main result of this section is to demonstrate the existence of 6-round integral distinguishers for such a kind of block cipher.

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 there exists the following integral distinguisher

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

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

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

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) by $(1,0,1,1,0,1,1,0)$.

3.2 Six-Round Integral Distinguishers

We first present the following lemma, whose proof can be found in the appendix.

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

Basing this lemma, the existence of six-round integral distinguisher of $\mathcal{E}$ could be proved in the following proposition.

Proposition 1. *Assume 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:*

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

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 (see Fig. 2), the l-th byte 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 byte 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 byte of Z_0, Z_1 and Z_2 is balanced, and meanwhile, for $1 \leq t \leq n, t \neq j$, $Z_{3,t}$ and $Z_{4,t}$ are also balanced. Thus

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

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

Now the index $1 \leq l \leq n$ such that $p_{l,j} = 1$ should be considered. In these situations, $p_{l,j} = 1$, and Eq.(1) 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 1, the sum of $Z_{4,j} \oplus Z_{3,j}$ over $x \in \mathbb{F}_{2^d}$ is indeed only dependent one the constants of the inputs corresponding to the passive bytes and the unknown round-keys. □

4 Impossible Differentials of MISTY Structure with SPN Round Function

In this section, we describe how to adopt the matrix-based method from [10] and [18] to study the impossible differential properties 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, such process resembles at a large extent the case of SPN ciphers, and all proofs of these criteria are similar as that of [10], thus the details are omitted. To facilitate our analysis, we use the same notations as in [10]. 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

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

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

Similarly, assume the 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

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

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

4.1 5-round Impossible Differentials

By adopting the technique in analyzing 3-round impossible differentials as shown in [10], 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

$$P \circ S(e_i) = S^{-1} \circ P^{-1}(e_j) \tag{2}$$

to present a similar criterion to characterize the case of 5-round impossible differentials.

Proposition 2. *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 $\mathcal{E}$.*

4.2 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

$$S^{-1} \circ P^{-1} \circ S^{-1} \circ P^{-1}(e_j) = P \circ S(e_i) \tag{3}$$

could be used to analyze the case of 6-round impossible differentials. The criteria can be further divided into the following cases:

Proposition 3. *For any $1 \leq i, j \leq n$, 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 4. *For any $1 \leq i, j \leq n$, 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 $M_{i,j}$. 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 5. *For any* $1 \leq i, j \leq n$, *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.(3) becomes the following

$$S^{-1} \circ P^{-1} \circ S^{-1}(e_j) = P \circ S(e_i) \tag{4}$$

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 6. *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* $\mathcal{E}$.

4.3 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

$$P^{-1} \circ S^{-1} \circ P^{-1} \circ S^{-1} \circ P^{-1}(\beta) = S \circ P \circ S(\alpha) \oplus S(\alpha), \tag{5}$$

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

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

based on which, we could obtain similar results as in Section 4.2 but with *slight modifications*.

Proposition 7. *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_i *denotes the* i*-th row vector of* M_{ij}. *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 8. *For any* $1 \le i,j \le n$, *let* $U_i = \{r \ne i | p_{r,i} = 0\} = \{r_1, r_2, \ldots, r_u\}$, $V_j = \{t | q_{t,j} \ne 0\} = \{t_1, t_2, \ldots, t_v\}$, *and* $M_{i,j} = (q_{r_a,t_b})_{u\times v} = (m_1, m_2, \ldots, m_v)$, *where each* m_i *is the* i*-th column vector of* $M_{i,j}$. *If* $U_i, V_j \ne \emptyset$, *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 9. *For any* $1 \le i,j \le n$, *let* $U_i = \{r \ne i | p_{r,i} = 0\} = \{r_1, r_2, \ldots, r_u\}$, $W_i = \{s \ne i | p_{s,i} \ne 0\} \cup \{i | p_{i,i} = 0\} = \{s_1, s_2, \ldots, s_w\}$, $V_j = \{t | q_{t,j} \ne 0\} = \{t_1, t_2, \ldots, t_v\}$, *and*

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

where each m_i (resp. m'_i) *denotes the* i*-th row vector of* $M_{i,j}$ (resp. $M'_{i,j}$). *If* $U_i, W_i, V_j \ne \emptyset$, *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 Application to p-Camellia

5.1 Brief Description of p-Camellia

The block cipher p-Camellia[1] 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. 4 and Fig. 5 to compare the difference between Camellia and p-Camellia.

The round function F 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 substitution layer is a non-linear transformation S on $\mathbb{F}_{2^8}^8$ defined by eight parallel S-boxs on $\mathbb{F}_{2^8}$. The diffusion layer is an invertible linear transformation P defined over $\mathbb{F}_2^{8\times 8}$. The round key addition layer is defined simply by the exclusive OR (XOR) of the round-key and the input.

The non-linear transformation in the confusion layer is defined by

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

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

The linear transformation P in the diffusion layer which provides the avalanche effect, and its inversion P^{-1} are defined by the following binary matrices

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

[1] We use the same notations as in [20]. In fact, there is a *slight distinction* between the basic notation for Feistel structure in [1] and as that in [20]. However, this dose not influence our analysis.

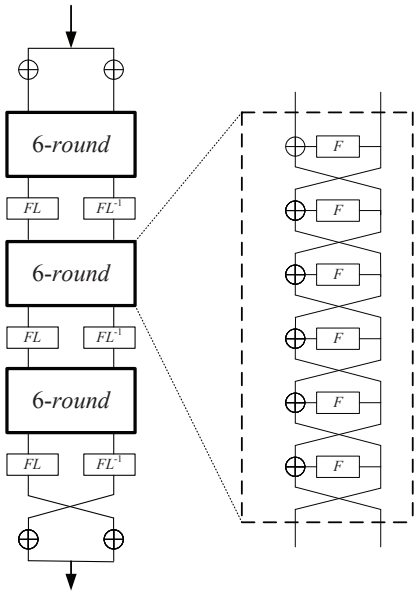

Fig. 4. Description of Camellia

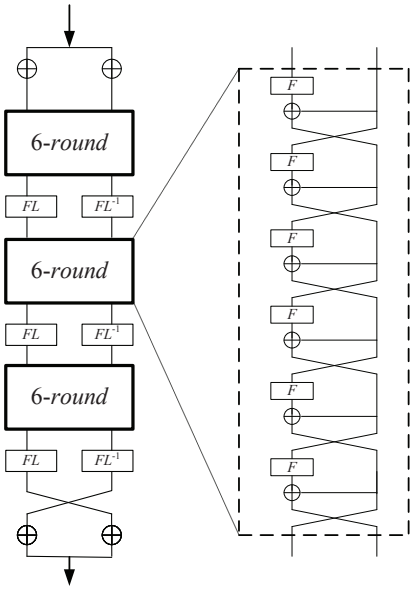

Fig. 5. Description of p-Camellia

Also, as discussed in many literatures for Camellia, we only consider p-Camellia without the FL/FL^{-1} transformation.

5.2 Integral Distinguishers of Reduced-Round p-Camellia

In this subsection, we apply the criterion from Section 3 to find integral distinguishers of reduced-round p-Camellia, all of which have been verified experimentally.

According to Proposition 1, we could obtain the following 8 six-round integral distinguisher.

Proposition 10. *There exist the following kind of* 6*-round integral distinguishers in p-Camellia:*

- $((C,C,C,C,C,C,C,C),(A,C,C,C,C,C,C,C)) \rightarrow ((D,D,D,B,D,B,B,D),(?,?,?,?,?,?,?,?))$
- $((C,C,C,C,C,C,C,C),(C,A,C,C,C,C,C,C)) \rightarrow ((B,D,D,D,D,D,B,B),(?,?,?,?,?,?,?,?))$
- $((C,C,C,C,C,C,C,C),(C,C,A,C,C,C,C,C)) \rightarrow ((D,B,D,D,B,D,D,B),(?,?,?,?,?,?,?,?))$
- $((C,C,C,C,C,C,C,C),(C,C,C,A,C,C,C,C)) \rightarrow ((D,D,B,D,B,B,D,D),(?,?,?,?,?,?,?,?))$
- $((C,C,C,C,C,C,C,C),(C,C,C,C,A,C,C,C)) \rightarrow ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$
- $((C,C,C,C,C,C,C,C),(C,C,C,C,C,A,C,C)) \rightarrow ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$
- $((C,C,C,C,C,C,C,C),(C,C,C,C,C,C,A,C)) \rightarrow ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$
- $((C,C,C,C,C,C,C,C),(C,C,C,C,C,C,C,A)) \rightarrow ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$

Besides the above 6-round integral distinguishers, according to the special arrangement of s-boxs in the confusion layer, we also detect the following 7-round integral distinguishers of p-Camellia. The proof is based on counting methods (see e.g. [6, 12]) and the detail is omitted.

Proposition 11. *There exist the following kind of* 7*-round integral distinguishers in p-Camellia:*

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

where "$A_i \| A_j \| A_k$*" denotes an active state over the corresponding three bytes* (i, j, k)*.*

5.3 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 to detect reduced-round impossible differentials in p-Camellia.

5-round Impossible Differentials of p-Camellia From Proposition 2, 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 3, we do not find 6-round impossible differentials of p-Camellia.

Case 2. Table 1 shows 6-round impossible differentials of p-Camellia found by Proposition 4.

Case 3. Table 2 shows 6-round impossible differentials of p-Camellia found by Proposition 5.

Case 4. From Proposition 6, 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 1. 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 2. 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 From the results in Section 4.3, $(e_i, 0) \nrightarrow (P(e_j), P(e_j))$ is a 7-round impossible differential of p-Camellia, where i, j are chosen from Table 1 and Table 2.

6 Conclusion

This paper presents some distinguishing properties of MISTY structure with SPN round function. The existence of 6-round integral distinguisher is confirmed when the diffusion layer employs a binary invertible matrix, and some criteria for characterizing 5/6/7-round impossible differentials are proposed. Based on these results, we improve the distinguishing bounds on the block cipher p-Camellia, and Table 3 lists the comparison.

Table 3. Comparison of Distinguishers between Camellia and p-Camellia without FL/FL^{-1}

	Integral	Impossible Differential	Ref.
p-Camellia	4-round	4-round	[20]
p-Camellia	7-round	7-round	This Paper

Acknowledgment

The work in this paper is supported by the Natural Science Foundation of China (No: 60803156, 61070215) and the open research fund of State Key Laboratory of Information Security (No: 01-07).

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. 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.
3. Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, Vol 3, pp. 3–72, 1991.
4. Jiali Choy, Guanhan Chew, Khoongming Khoo, and Huihui Yap. Cryptographic properties and application of a generalized unbalanced Feistel network structure. ACISP 2009, pp. 73–89, Springer, 2009.
5. Henri Gilbert and Marine Minier. New Results on the Pseudorandomness of Some Blockcipher Constructions. FSE 2001, LNCS 2355, pp. 248–266, Springer, 2002.
6. Yasuo Hatano, Hiroki Sekine and Toshinobu Kaneko. Higher order diffrential attack of Camellia (II). SAC 2002, LNCS 2595, pp. 129-146, Springer, 2003.
7. Lars Ramkilde Knudsen. DEAL – a 128-bit block cipher. Technical Report 151, Department of Informatics, University of Bergen, Norway, Feb. 1998.
8. Lars Ramkilde Knudsen, David Wagner. Integral cryptanalysis. FSE 2002, LNCS 2365, pp. 112–127, Springer, 2002.
9. 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.
10. Ruilin Li, Bing Sun, and Chao Li. Impossible differential cryptanalysis of SPN ciphers. Cryptology ePrint Archive, Report 2010/307, available through: http://eprint.iacr.org/2010/307.
11. Ruilin Li, Bing Sun, Chao Li, Longjiang Qu. Cryptanalysis of a generalized unbalanced Feistel network structure. ACISP 2010, LNCS 6168, pp. 1–18, Springer, 2010.
12. Ping Li, Bing Sun, and Chao Li. Integral cryptanalysis of ARIA. Inscrypt 2009, LNCS 6151, pp. 1–14, Springer, 2010.
13. M. Luby and C. Rackoff. How to construct pseudo-random permutations from pseudo-random functions. SIAM Journal on Computing, vol. 17, no. 2, pp. 373C386, 1988.
14. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. EUROCRYPT 1993, LNCS 765, pp. 386–397, Springer, 1993.
15. Mitsuru Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. FSE 1996, LNCS 1039, pp. 205–218, Springer, 1996.
16. Mitsuru Matsui. New block encryption algorithm MISTY. FSE 1997, LNCS 1267, pp. 54–68, Springer, 1997.
17. Wenling Wu, Lei Zhang, Liting Zhang and Wentao Zhang. Security analysis of the GF-NLFSR structure and Four-Cell block cipher. ICICS 2009, LNCS 5927, pp.17–31, Springer-Verlag, 2009.
18. 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.
19. Specification of the 3GPP confidentiality and Integrity algorithm KASUMI. Available through http://www.etsi.org/.
20. Huihui Yap, Khoongming Khoo, and Axel Poschmann. Parallelizing the Camellia and SMS4 block ciphers. AFRICACRYPT 2010, LNCS 6055, pp. 387–406, Springer, 2010.

A Proof of Lemma 1

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 as shown in Fig 2, 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 byte 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:

$$\begin{aligned} Z_3 &= S(X_3 \oplus K_4) \\ &= S(Y_1 \oplus Y_0 \oplus X_1 \oplus K_4) \\ &= S(P(Z_1) \oplus X_1 \oplus C'), \end{aligned} \tag{7}$$

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

$$\begin{aligned} Z_4 &= S(X_4 \oplus K_5) \\ &= S(Y_2 \oplus Y_1 \oplus Y_0 \oplus X_1 \oplus K_5) \\ &= S(P(Z_2) \oplus P(Z_1) \oplus X_1 \oplus C''), \end{aligned} \tag{8}$$

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

$$Z_1 = S(X_1 \oplus K_2) = (c, \ldots, c, s_j(x \oplus k_{2,j}), c, \ldots, c) \triangleq (c, \ldots, c, z_{1,j}, c, \ldots, c), \tag{9}$$

and

$$Z_2 = S(X_2 \oplus K_3) = (c, \ldots, c, s_j(x \oplus c \oplus k_{3,j}), c, \ldots, c) \triangleq (c, \ldots, c, z_{2,j}, c, \ldots, c). \tag{10}$$

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. (9), 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.(7), each byte 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. (7), each byte of Z_3, except the j-th one, is balanced.

The Case for Z_4. If $p_{j,j} = 0$, then according to Eq. (10), the t-th ($1 \leq t \leq n$) 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.(8), each byte of Z_4 is balanced.

Similarly, if $p_{j,j} = 1$, then the t-th ($1 \leq t \leq n$) 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.(8), each byte of Z_4, except the j-th one, is balanced. □