From Camellia to p-Camellia: 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. At AFRICACRYPT 2010, a parallelized version of the block cipher Camellia, called p-Camellia, was proposed. The high level structure of p-Camellia is MISTY-type, while the round function is SPN-type. In this paper, some structural properties of p-Camellia are observed. It is shown that compared with Camellia, p-Camellia seems to be more likely to suffer from integral cryptanalysis, which has been confirmed by the existence of huge 6-round and 7-round integrals. Following this comes an interesting result that, for any block cipher with MISTY structure and SPN round function, if the linear transformation in the diffusion layer is binary, then there always exists 6-round integrals. Moreover, inspired from a recent work [10], many 5, 6, and 7 rounds impossible differentials in p-Camellia could be obtained. It should be emphasized that, the techniques from [10] could be generalized to analyze impossible differentials of MISTY structure with SPN round function.

Keywords: Block ciphers, Camellia, p-Camellia, Feistel, MISTY, SPN, Structural properties

1 Introduction

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, generalized unbalanced Feistel structure, and etc.. In [4], a kind of generalized unbalanced Feistel structure with n sub-blocks, called n-cell GF-NLFSR, was proposed with property that $n+1$-round could provide provable security against differential cryptanalysis [3] (DC) and linear cryptanalysis [13] (LC). This kind of structure was carefully reevaluated in [11] and [16], where it was shown that there exist n^2-round integral distinguisher and n^2+n-2-round impossible differential distinguisher.

When $n=2$, GF-NLFSR is reduced to a classic block cipher structure, the so-called MISTY structure [14]. MISTY structure was firstly introduced by Matsui as an alternative scheme of Feistel structure. In [5], Gilbert and Minier formalized the MISTY structure as the L-scheme and referred the dual structure as the R-scheme. The advantage of MISTY structure is that it can provide provable security against DC and LC, offer pseudorandomness and superpseudorandomness, and meanwhile 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 [15], and meanwhile, as the basic low-level structure of the round function and the component in block ciphers MISTY1 [15], MISTY2, and KASUMI [19].

At AFRICACRYPT 2010, MISTY structure with SPN round function was shown to be practical secure against DC and LC by using a similar approach as [9]. Based on this theory, a new block cipher p-Camellia [20], which is a parallelized version of Camellia [1], was proposed, and its security against many other cryptanalytic methods are also discussed.

In this paper, some observations on the structural properties of p-Camellia, or more generally, MISTY structure with SPN round function, are observed. These structural properties include integrals [8] and impossible differentials [2, 7]. It is known that there exist 4-round integrals [18] and 8-round impossible differentials [17] in Camellia. We show that, compared with Camellia, p-Camellia seems to be more likely to suffer from integral cryptanalysis, which has been confirmed by the existence of huge 6 and 7-round integrals. Following this comes an interesting result that, for any block cipher employing MISTY structure and SPN round function, if the linear transformation in the diffusion layer is binary, then there always exists 6-round integrals. Moreover, inspired from a recent work [10], we also obtain many 5, 6, and 7 rounds impossible differentials in p-Camellia. We point out that the techniques from [10] could be generalized to analyze the impossible differentials of MISTY structure with SPN round function.

The outline of this paper is as follows: some preliminaries are introduced in Section 2. Section 3 shows the existence of 6 and 7 rounds integrals, Section 4 presents an interesting results on 6-round integrals 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 and applies the results to p-Camellia. And finally, Section 5 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 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 substitution layer is a non-linear bijective transformation on $\mathbb{F}_{2^d}^n$ defined by n parallel S-boxes on $\mathbb{F}_{2^d}$, and *they are not necessary to be identical in different rounds*. The diffusion layer employs an invertible linear transformation

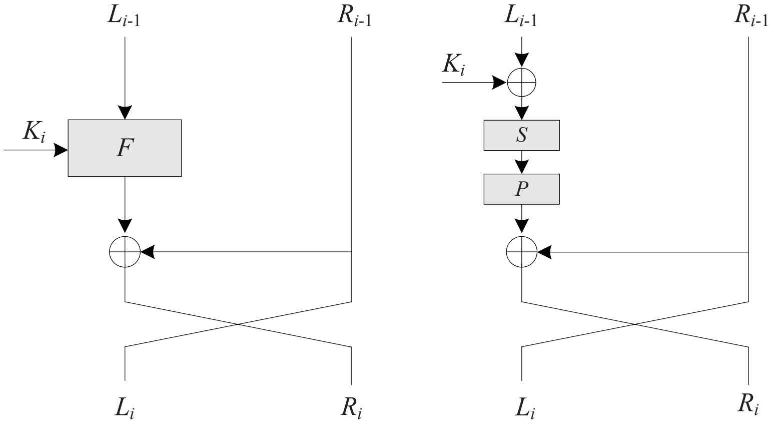

Fig. 1. MISTY Structure (Left) and MISTY Structure with SPN Round Function (Right)

$P = (P_{i,j})_{n\times n}$ defined over $\mathbb{F}_{2^d}^{n\times n}$. The round key addition layer is defined simply by the exclusive OR (XOR) of the round-key and the input.

2.2 Notations and Known Results

Let $X = (x_1, x_2, \dots, x_n) \in \mathbb{F}_{2^d}^n$ 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., $\Delta X = X \oplus X'$. Further, $(\alpha_1, \alpha_2) \rightarrow (\beta_1, \beta_2)$ is used to denote a possible differential with (α_1, α_2) (resp. (β_1, β_2)) the input (resp. output) difference. Similarly, $(\alpha_1, \alpha_2) \nrightarrow (\beta_1, \beta_2)$ represents an impossible differential. Moreover, the following definitions are 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* $0 \le i < j \le 2^b - 1$, $a_i \neq a_j$. *We use* **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* **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* **B** *to denote the balanced set.*

Refer to Fig. 2, 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 a 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.

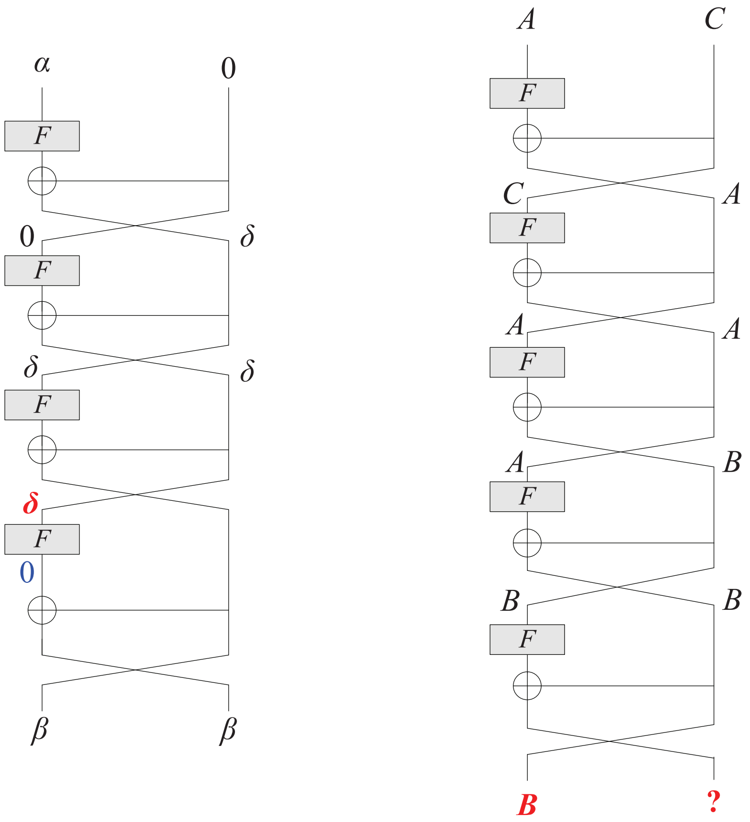

Fig. 2. Impossible differentials (Left) and integrals (Right) of MISTY structure

2.3 Brief Description of p-Camellia

p-Camellia[1], a paralleled version of Camellia, 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.

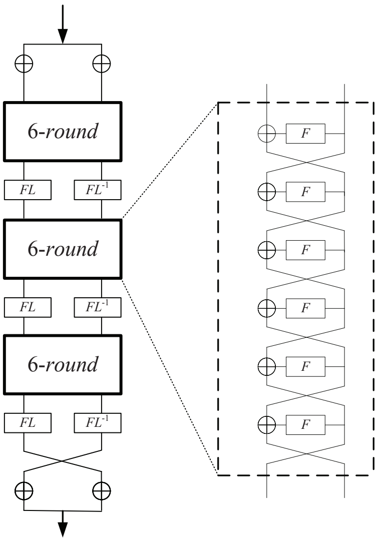

Fig. 3. Description of Camellia

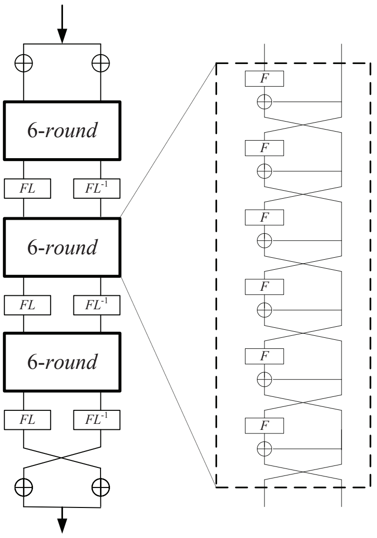

Fig. 4. Description of p-Camellia

The round function 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.

Aided by Fig.5, some useful notations used throughout this paper are given: Let X_i and Y_i be the input and output variable of the $i+1$-th round function, K_{i+1} be the $i+1$-th round-key, i.e., $Y_{i+1} = F(X_i \oplus K_{i+1})$. Let Z_i be the intermediate variable after the confusion layer in the round function, i.e., $Z_i = S(X_i \oplus K_{i+1})$ and $Y_i = P(Z_i)$.

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

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

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

[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. Meanwhile, in the following sections, we always assume that the left and right part of the output in the last round of reduced-round p-Camellia are not swapped.

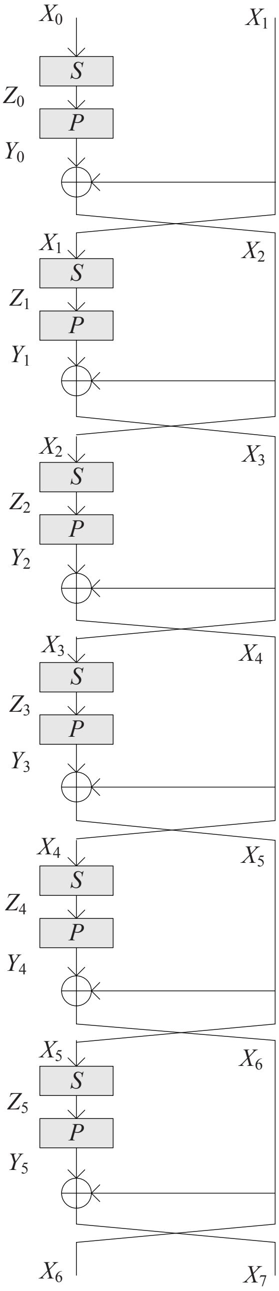

Fig. 5. 6-Round MSITY structure with SPN round function (The round-key addition layer is omitted).

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

$$P = \begin{pmatrix} 1&0&1&1&0&1&1&1 \\ 1&1&0&1&1&0&1&1 \\ 1&1&1&0&1&1&0&1 \\ 0&1&1&1&1&1&1&0 \\ 1&1&0&0&0&1&1&1 \\ 0&1&1&0&1&0&1&1 \\ 0&0&1&1&1&1&0&1 \\ 1&0&0&1&1&1&1&0 \end{pmatrix}.$$

In the following sections, we will use $P_i^{(r)}$ to denote the i-th row vector of P. Also, as discussed in many literatures, we only consider p-Camellia without the FL/FL^{-1} transformation.

3 Integrals of Reduced-Round p-Camellia

From [20], there exists 4-round integrals $(A, C) \to (S_0, S_1)$, where $S_0 \oplus S_1$ is active. In fact, as shown in [8], there always exists 5-round integrals $(A, C) \to (B, ?)$ for MISTY structure. In this section, we demonstrate some 6 and 7-round integrals in p-Camellia. All of these distinguishers have been verified experimentally. Note that, these integrals are found by *counting methods*, which has been successfully used to find 3-round integrals [12] of the block cipher ARIA and reduced-round higher-order differentials [6] of Camellia.

3.1 6-round Integrals in p-Camellia

We first present the following two lemmas, whose proofs can be found in the appendixes. Basing these two lemmas, two kinds of 6-round integral distinguishers could be obtained.

Lemma 1. [2] *Let $(X_0, X_1) = ((c, c, c, c, c, c, c, c), (c, c, c, c, x, c, c, c))$ be the input of p-Camellia, where $x \in \mathbb{F}_{2^8}$ is a variable, and all c's are constants in $\mathbb{F}_{2^8}$ 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 $Z_i = (Z_{i,1}, Z_{i,2}, \ldots, Z_{i,8})$. If x takes all values in $\mathbb{F}_{2^8}$, then for any $0 \le i \le 4$, $1 \le j \le 8$, $Z_{i,j}$ is a balanced byte.*

Lemma 2. [3] *Let $(X_0, X_1) = ((c, c, c, c, c, c, c, c), (x, c, c, c, c, c, c, c))$ be the input of p-Camellia, where $x \in \mathbb{F}_{2^8}$ is a variable, and all c's are constants in $\mathbb{F}_{2^8}$ 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 $Z_i = (Z_{i,1}, Z_{i,2}, \ldots, Z_{i,8})$. If x takes all values in $\mathbb{F}_{2^8}$, then for $i = 0, 1, 2$, $1 \le j \le 8$, $Z_{i,j}$ is a balanced byte, while for $i = 3, 4$, and $2 \le j \le 8$, $Z_{i,j}$ is a balanced byte.*

[2] A similar result could be obtained when the variable x appears at the sixth, seventh or eighth position of the right part.

[3] A similar result could also be obtained when the variable x appears at the second, third or fourth position of the right part.

Proposition 1. *There exist the following kind of* 6*-round integral distinguishers in p-Camellia:*

- $((C,C,C,C,C,C,C,C),(C,C,C,C,A,C,C,C)) \to ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$
- $((C,C,C,C,C,C,C,C),(C,C,C,C,C,A,C,C)) \to ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$
- $((C,C,C,C,C,C,C,C),(C,C,C,C,C,C,A,C)) \to ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$
- $((C,C,C,C,C,C,C,C),(C,C,C,C,C,C,C,A)) \to ((B,B,B,B,B,B,B,B),(?,?,?,?,?,?,?,?))$.

Proof. We just give the proof for the first distinguisher, all the other proofs are similar.

Let
$$(X_0, X_1) = ((c,c,c,c,c,c,c,c),(c,c,c,c,x,c,c,c)),$$
then according to the encryption procedure,
$$\begin{aligned} X_{6,i} &= Y_{4,i} \oplus Y_{3,i} \oplus Y_{2,i} \oplus Y_{1,i} \oplus Y_{0,i} \oplus X_{1,i} \\ &= P_i^{(r)} \cdot (Z_4 \oplus Z_3 \oplus Z_2 \oplus Z_1 \oplus Z_0) \oplus X_{1,i}. \end{aligned}$$

Lemma 1 tells that each byte of Z_0, Z_1, Z_2, Z_3 and Z_4 is balanced, thus $X_{6,i}$ is balanced. □

Proposition 2. *There exist the following kind of* 6*-round integral distinguishers in p-Camellia:*

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

where, the letter "D" also represents some unknown byte, but with the property that all D's have the same value in each distinguisher.

Proof. Similarly, we will give the proof for the first distinguisher.

Let
$$(X_0, X_1) = ((c,c,c,c,c,c,c,c),(x,c,c,c,c,c,c,c)),$$
then according to the encryption procedure,
$$\begin{aligned} X_{6,i} &= Y_{4,i} \oplus Y_{3,i} \oplus Y_{2,i} \oplus Y_{1,i} \oplus Y_{0,i} \oplus X_{1,i} \\ &= P_i^{(r)} \cdot (Z_4 \oplus Z_3 \oplus Z_2 \oplus Z_1 \oplus Z_0) \oplus X_{1,i}. \end{aligned}$$

Lemma 2 shows that each byte of Z_0, Z_1 and Z_2 is balanced, and meanwhile, for $2 \leq j \leq 8$, $Z_{3,j}$ and $Z_{4,j}$ are also balanced. Thus
$$\begin{aligned} \bigoplus_{x\in\mathbb{F}_{2^8}} X_{6,i} &= \bigoplus_{x\in\mathbb{F}_{2^8}} \Big(P_i^{(r)} \cdot (Z_4 \oplus Z_3 \oplus Z_2 \oplus Z_1 \oplus Z_0) \oplus X_{1,i}\Big) \\ &= \bigoplus_{x\in\mathbb{F}_{2^8}} P_i^{(r)} \cdot (Z_4 \oplus Z_3) \\ &= \bigoplus_{x\in\mathbb{F}_{2^8}} \bigoplus_{j=1}^{8} p_{i,j} \cdot (Z_{4,j} \oplus Z_{3,j}) \\ &= \bigoplus_{x\in\mathbb{F}_{2^8}} p_{i,1} \cdot (Z_{4,1} \oplus Z_{3,1}) \qquad (1) \end{aligned}$$

From the definition of P, $p_{4,1} = p_{6,1} = p_{7,1} = 0$, which implies that for these positions $i = 4, 6, 7$, $X_{6,i}$ are balanced.

Now the case $1 \leq i \leq 8$ with $i \neq 4, 6, 7$ should be considered. In these situations, $p_{i,1} = 1$, and Eq.(1) becomes

$$\bigoplus_{x \in \mathbb{F}_{2^8}} X_{6,i} = \bigoplus_{x \in \mathbb{F}_{2^8}} (Z_{4,1} \oplus Z_{3,1}).$$

Thus, for any position i, the sum of $X_{6,i}$ are all equal to the sum of $Z_{4,1} \oplus Z_{3,1}$. From the calculation of $Z_{4,1}$ and $Z_{3,1}$ as described in the proof of Lemma 2, the sum of $Z_{4,1} \oplus Z_{3,1}$ over $x \in \mathbb{F}_{2^8}$ is indeed only dependent with the constants of the inputs corresponding to the passive bytes. □

Remark 1. The above two kinds of 6-round integrals presented in Proposition 1 and Proposition 2 contains only one active byte. However, using a similar technique, other kinds of integrals, which contains two, three or more active bytes could be obtained. For instance, consider 6-round p-Camellia, assume the left part of the input is a constant, and the right part of the input includes two active bytes (the active position indexes could be chosen arbitrary), then each byte of the left part of the output is balanced.

3.2 7-round Integrals in p-Camellia

In this sub-section, we present the following 7-round integral distinguishers of p-Camellia. The proof is also based on counting methods and the detail is omitted.

Proposition 3. *There exist the following kind of 7-round integral distinguishers in p-Camellia:*

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

where "$A_i \| A_j \| A_k$" denotes an active state over the corresponding three bytes (i, j, k), the letter "D" have the same meanings as described in Proposition 2.

4 Further Results on Integrals of MISTY Structure with SPN Round Function

This section focuses on 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, i.e., $P \in \mathbb{F}_2^{n \times n}$. 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.

Within these notations, the following 6-round integral distinguisher of p-Camellia

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

can be simply denoted as

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

where R_i represents that the i-th component of the right half of the input is active, while L_C denotes that the left half is fixed to a constant. The main convenience is to denote (D,B,D,D,B,D,D,B) by $(1,0,1,1,0,1,1,0)$.

In general, by adopting the technique in Section 3, we have the following result:

Proposition 4. *For any block cipher with* MISTY *structure and* SPN *round function, let the diffusion matrix be a binary matrix P, then there always exists the following kind of* 6*-round integral distinguisher:*

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

where P_j is the j-th column vector of P, and P_j^T denotes the transpose of P_j.

5 Impossible Differentials of MISTY Structure with SPN Round Function with Application to p-Camellia

As shown in [20], there exists 4-round impossible differential $(\alpha, 0) \nrightarrow (\beta, \beta)$ in p-Camellia, where $\alpha \neq 0$ and $\beta \neq 0$. Moreover, the designers confirmed that they didn't find impossible differentials with more than 4 rounds.

In this section, we briefly describe how to adopt the technique from [10] to study the impossible differential properties of any block ciphers with MISTY structure and SPN round function. And then apply these criteria to detect reduced-round impossible differentials in p-Camellia. Now let's 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 $P^{-1} = (q_{i,j})_{n\times n}$.

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

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

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

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

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.

5.1 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 5. *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 $\mathcal{E}$.*

5.2 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 6. *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 7. *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 8. *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* $\text{rank}\{m_1, m_2, \ldots, m_u, m'_l\} = \text{rank}\{m_1, m_2, \ldots, m_u\}$, *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 9. *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 $\mathcal{E}$.*

5.3 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 5.2 but with *slight modifications*.

Proposition 10. *For any $1 \leq i, j \leq n$, let $U_i = \{r \neq i | p_{r,i} = 0\} = \{r_1, r_2, \ldots, r_u\}$, $V_j = \{t | q_{t,j} \neq 0\} = \{t_1, t_2, \ldots, t_v\}$, 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 11. *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_i *is the* i*-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* $(e_i, 0) \not\twoheadrightarrow (P(e_j), P(e_j))$ *is a* 7*-round impossible differential of* $\mathcal{E}$*.*

Proposition 12. *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_i (resp. m'_i) *denotes the* i*-th row vector of* $M_{i,j}$ (resp. $M'_{i,j}$)*. If* $U_i, W_i, V_j \neq \emptyset$*, 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* $(e_i, 0) \not\twoheadrightarrow (P(e_j), P(e_j))$ *is a* 7*-round impossible differential of* $\mathcal{E}$*.*

5.4 Applications to p-Camellia

Since the linear transformation P of p-Camellia and its inversion P^{-1} are defined by

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

we can use the results from Section 5.1 $\sim$ 5.3 to find the following 5, 6, and 7 rounds impossible differentials in p-Camellia.

5-round Impossible Differentials of p-Camellia From Proposition 5, for any $1 \leq i,j \leq 8$, $(e_i, 0) \not\twoheadrightarrow (e_j, e_j)$ 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 6, 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 7.

Case 3. Table 2 shows 6-round impossible differentials of p-Camellia found by Proposition 8.

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

Case 4. From Proposition 9, for any $1 \le i, j \le 8$, $(e_i, 0) \nrightarrow (P(e_j), P(e_j))$ is a 6-round impossible differential of p-Camellia.

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

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

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

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

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 5.3, $(e_i, 0) \nrightarrow (P(e_j), P(e_j))$ is a 7-round impossible differential of p-Camellia, where i, j are chosen from Table 1 and Table 2.

6 Conclusion

This paper observes some structural properties of MISTY structure with SPN round function. And Table 3 lists the comparison between Camellia and p-Camellia from the viewpoint of the integral and impossible differential. The main difference is due to the underlying structure changing from Feistel to MISTY, and meanwhile some properties of the linear transformations in the SPN round function. This remind us that, the cryptographic properties of MISTY structure should be carefully studied, especially when the round function is implemented with SPN-type round functions.

Table 3. Comparisons between Camellia and p-Camellia

	Integral	Impossible Differential	Ref.
Camellia	4-round	8-round	[17, 18]
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. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. EUROCRYPT 1993, LNCS 765, pp. 386–397, Springer, 1993.
14. Mitsuru Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. FSE 1996, LNCS 1039, pp. 205–218, Springer, 1996.
15. Mitsuru Matsui. New block encryption algorithm MISTY. FSE 1997, LNCS 1267, pp. 54–68, Springer, 1997.
16. 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.

17. Wenling Wu, Wentao Zhang and Dengguo Feng. Impossible differential cryptanalysis of reduced-round ARIA and Camellia. Journal of Compute Science and Technology 22(3): 449–456, Springer, 2007.
18. Yongjin Yeom, Sangwoo Park, and Iljun Kim. On the security of Camellia against the square attack. FSE 2002, LNCS 2365, pp. 89–99, Springer, 2002.
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. According to the encryption procedure as shown in Fig 5, we have

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

from which it's easy to show the balanced property for each byte of Z_0, Z_1 and Z_2. Below will deal with the cases for Z_3 and Z_4.

A.1 Proof for the balanced property of $Z_{3,j}$.

We have

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

where $C' = Y_0 \oplus K_4 = P(S(X_0 \oplus K_1)) \oplus K_4$ is some 64-bit unknown constant.

Noting that

$$X_1 = (c, c, c, c, x, c, c, c),$$

we will get

$$Z_1 = S(X_1 \oplus K_2) = (c, c, c, c, s_2(x \oplus k_{2,5}), c, c, c) \triangleq (c, c, c, c, z_{1,4}, c, c, c),$$

and

$$P(Z_1) = (c,\ z_{1,4} \oplus c,\ z_{1,4} \oplus c,\ z_{1,4} \oplus c,\ c,\ z_{1,4} \oplus c,\ z_{1,4} \oplus c,\ z_{1,4} \oplus c).$$

Thus,

$$P(Z_1) \oplus X_1 = (c,\ z_{1,4} \oplus c,\ z_{1,4} \oplus c,\ z_{1,4} \oplus c,\ x \oplus c,\ z_{1,4} \oplus c,\ z_{1,4} \oplus c,\ z_{1,4} \oplus c).$$

Since $z_{1,4} = s_2(x \oplus k_{2,5})$, according to Eq.(7), each byte of Z_3 is balanced.

A.2 Proof for the balanced property of $Z_{4,j}$.

We have

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

where $C'' = Y_0 \oplus K_5 = P(S(X_0 \oplus K_1)) \oplus K_5$ is some 64-bit unknown constant.

Noting that

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

we will get

$$Z_2 = S(X_2 \oplus K_3) = (c, c, c, c, s_2(x \oplus c \oplus k_{3,5}), c, c, c) \triangleq (c, c, c, c, z_{2,4}, c, c, c),$$

and

$$P(Z_2) = (c,\ z_{2,4} \oplus c,\ z_{2,4} \oplus c,\ z_{2,4} \oplus c,\ c,\ z_{2,4} \oplus c,\ z_{2,4} \oplus c,\ z_{2,4} \oplus c).$$

Thus, $P(Z_2) \oplus P(Z_1) \oplus X_1$ becomes

$$(c,\ z_{1,4} \oplus z_{2,4} \oplus c,\ z_{1,4} \oplus z_{2,4} \oplus c,\ z_{1,4} \oplus z_{2,4} \oplus c,\ x \oplus c, z_{1,4} \oplus z_{2,4} \oplus c,\ z_{1,4} \oplus z_{2,4} \oplus c,\ z_{1,4} \oplus z_{2,4} \oplus c).$$

Since $z_{1,4} \oplus z_{2,4} = s_2(x \oplus c \oplus k_{2,5}) \oplus s_2(x \oplus k_{3,5})$ represents the output difference of the S-box $s_2(\cdot)$, each possible value of $z_{1,4} \oplus z_{2,4}$ appears even times. According to Eq.(8), each byte of Z_4 is balanced. □

B Proof of Lemma 2

Proof. According to the encryption procedure as shown in Fig 5, we have

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

from which it's also easy to show the balanced property for each byte of Z_0, Z_1 and Z_2. Now the case for Z_3 and Z_4 is a little involved.

B.1 The Case for $Z_{3,i}$.

As demonstrated in Lemma 1, we have

$$Z_3 = S(X_3 \oplus K_4) = S(P(Z_1) \oplus X_1 \oplus C'). \tag{9}$$

Noting that

$$X_1 = (x, c, c, c, c, c, c, c),$$

we will get

$$Z_1 = S(X_1 \oplus K_2) = (s_1(x \oplus k_{2,1}), c, c, c, c, c, c, c) \triangleq (z_{1,1}, c, c, c, c, c, c, c),$$

and

$$P(Z_1) = (z_{1,1} \oplus c,\ z_{1,1} \oplus c,\ z_{1,1} \oplus c,\ c,\ z_{1,1} \oplus c,\ c,\ c,\ z_{1,1} \oplus c).$$

Thus,

$$P(Z_1) \oplus X_1 = (z_{1,1} \oplus x \oplus c,\ z_{1,1} \oplus c,\ z_{1,1} \oplus c,\ c,\ z_{1,1} \oplus c,\ c,\ c,\ z_{1,1} \oplus c).$$

Since $z_{1,1} = s_1(x \oplus k_{2,1})$, according to Eq.(9), each byte of Z_3, except the first one, is balanced.

B.2 The Case for $Z_{4,i}$.

Similarly, we have

$$Z_4 = S(P(Z_2) \oplus P(Z_1) \oplus X_1 \oplus C''). \tag{10}$$

Noting that

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

we will get

$$Z_2 = S(X_2 \oplus K_3) = (s_1(x \oplus c \oplus k_{3,1}), c, c, c, c, c, c, c) \triangleq (z_{2,1}, c, c, c, c, c, c, c),$$

and

$$P(Z_2) = (z_{2,1} \oplus c,\ z_{2,1} \oplus c,\ z_{2,1} \oplus c,\ c,\ z_{2,1} \oplus c,\ c,\ c,\ z_{2,1} \oplus c).$$

Thus, $P(Z_2) \oplus P(Z_1) \oplus X_1$ becomes

$$(z_{1,1} \oplus z_{2,1} \oplus x \oplus c,\ z_{1,1} \oplus z_{2,1} \oplus c,\ z_{1,1} \oplus z_{2,1} \oplus c,\ c,\ z_{1,1} \oplus z_{2,1} \oplus c,\ c,\ c,\ z_{1,1} \oplus z_{2,1} \oplus c).$$

Since $z_{1,1} \oplus z_{2,1} = s_1(x \oplus k_{2,1}) \oplus s_1(x \oplus c \oplus k_{3,1})$ represents the output difference of $s_2(\cdot)$, each possible value of $z_{1,1} \oplus z_{2,1}$ appears even times. According to Eq.(10), each byte of Z_4, except the first one, is balanced. □