Impossible Differential Cryptanalysis on Feistel Ciphers with SP and SPS Round Functions

Yuechuan Wei[1], Ping Li[2], Bing Sun[2], and Chao Li[1,2,3]

[1] School of Computer Science, National University of Defense Technology,
Changsha, China, 410073

[2] Science College of National University of Defense Technology,
Changsha, China, 410073

[3] State Key Laboratory of Information Security, Chinese Academy of Sciences,
Beijing, China, 100049

wych004@163.com, leave17@gmail.com, happy_come@163.com,
lichao_nudt@sina.com

Abstract. Impossible differential cryptanalysis is well known to be effective in analyzing the security of block ciphers. Known result shows that there always exists 5-round impossible differentials of a Feistel cipher with bijective round function. However, if more details of the round function are known, the result could be improved. This paper mainly studies the impossible differentials of Feistel ciphers with both SP and SPS round functions where the linear transformation P is defined over $\mathbb{F}_2^{n\times n}$. For Feistel ciphers with SP round functions, any column of $P \oplus P^{-1}$ whose Hamming weight is greater than 1 corresponds to some 6-round impossible differentials. The existence of some 7-round impossible differentials can be determined by counting the times that 1 appears at some special positions of P and P^{-1}. Some 8-round impossible differentials can be found by computing the rank of some sub-matrix of P. Impossible differentials of Camellia found by these techniques are well consistent with previously known results. For Feistel ciphers with SPS round functions, by determining the rank of some sub-matrix of P, 6-round impossible differentials can be found, which improves the results on E2 by one round. These results tell that when designing a Feistel cipher with SP or SPS round function where the diffusion layer is selected from $\mathbb{F}_2^{n\times n}$, the linear transformation should be chosen carefully to make the cipher secure against impossible differential cryptanalysis.

Keywords: Block cipher, Feistel cipher, Impossible differential.

1 Introduction

Impossible differential cryptanalysis, proposed by Biham and Knudsen, was first applied to the cipher DEAL [7] and later to Skipjack [8]. The main idea is to specify a differential with probability zero over some rounds of the cipher. Then one can derive the right keys by discarding the wrong keys which lead to the impossible differential. Impossible differential cryptanalysis has been applied to AES, Camellia, MISTY1 and so on with very good results [10–16].

J. Zhou and M. Yung (Eds.): ACNS 2010, LNCS 6123, pp. 105–122, 2010.

The key step of impossible differential cryptanalysis is to retrieve the longest impossible differential. The main technique is miss-in-the-middle [8, 9], namely to find two differential characteristics with probability 1 from encryption and decryption directions, and connect them together. When there are some inconsistencies, their combination is the impossible differential that we are looking for. Once the impossible differential is found, it can be used to distinguish the cipher from a random permutation. In [17], Kim *et al.* introduced the $\mathcal{U}$-method to find impossible differentials of various block ciphers. However, $\mathcal{U}$-method is so general that some information is often lost during calculating the impossible differentials. Some longer impossible differentials cannot be found by using the $\mathcal{U}$-method.

The class of block ciphers considered in this paper is Feistel cipher with SP and SPS round functions whose diffusion layers can be represented by matrices over $\mathbb{F}_2$. These structures are worth being looked at since they are so popular that they have been employed by many famous ciphers, including Camellia, E2 and so on. For Feistel structure, 5-round impossible differential always exists if the round function is bijective [7]. However, if more details of the round function are taken into consideration, we can prove the existence of impossible differentials over more than 5 rounds. By carefully analyzing the properties of the linear transformations, we found that the existence of impossible differentials in a cipher is strongly related to the properties of the diffusion layer P. We should emphasize that the idea of exploiting incomplete diffusion of the round function is not new. Impossible differential for 7 rounds of DES is shown in [9], 8-round impossible differential for Camellia has been used in the previous attacks [11].

The contribution of this paper is an improvement of the original judgement about the impossible differential for Feistel cipher. Instead of searching by experience and intuition, some sufficient conditions are given to characterize the existence of 6/7/8-round impossible differentials of Feistel cipher with SP round functions and 6-round impossible differential of Feistel cipher with SPS round functions. One can discover these impossible differentials just by observing the linear transformation. All of these kinds of impossible differentials cannot be found by $\mathcal{U}$-method. As examples, 6-round impossible differential of E2 is found while previously known round of impossible differentials of E2 is 5 [3]. 8-round impossible differentials of Camellia found by this technique are well consistent with [11].

The paper is organized as follows: Feistel structure and χ-function are described in Section 2. In Section 3 and Section 4, we discuss the existence of impossible differentials of Feistel ciphers with SP and SPS round functions, respectively. Section 5 concludes this paper.

2 Preliminaries

In this section, we describe Feistel structure firstly, and then give the definition and properties of χ-function.

2.1 Feistel Structure

A Feistel network consists of r rounds, each of which is defined as follows. Denote by (L, R) the $2n$-bit input, set $\alpha_0 = L$ and $\beta_0 = R$, let $(\alpha_{i-1}, \beta_{i-1})$ be the input to the i-th round, (α_i, β_i) and k_i be the output and the round key of the i-th round, respectively. Then $(\alpha_i, \beta_i) = Round(\alpha_{i-1}, \beta_{i-1})$ is defined as:

$$\begin{cases} \alpha_i = \beta_{i-1}, \\ \beta_i = f(\beta_{i-1}, k_i) \oplus \alpha_{i-1}, \end{cases}$$

where f is the round function and in this paper, we always assume that $f(\beta_{i-1}, k_i) = f(\beta_{i-1} \oplus k_i)$. After iterating $Round$ r times, the ciphertext (C_L, C_R) is defined as (β_r, α_r). According to the definition of round function f, Feistel cipher can be fractionized to many branch structures. Major round functions under study are based on SP structure and SPS structure (See Fig. 1).

The former structure has one nonlinear transformation layer, and one linear transformation layer. Examples of these ciphers are DES [4], Camellia [5]. The later structure consist of 1st nonlinear transformation layer, linear transformation layer, and 2nd nonlinear transformation layer. Example of this kind of cipher is E2 [1].

This paper focuses on the above two kinds of Feistel ciphers with following nonlinear transformation S and linear transformation P. $S : \mathbb{F}_{2^t}^n \to \mathbb{F}_{2^t}^n$ is defined as $S(x_1, x_2, \ldots, x_n) = (S_1(x_1), S_2(x_2), \ldots, S_n(x_n))$, where $S_i (1 \le i \le n)$ are nonlinear bijective mappings on $\mathbb{F}_{2^t}$. P is an invertible linear transformation defined over $\mathbb{F}_2^{n \times n}$.

To be convenient, we simply denote $P = (p_{i,j})_{1 \le i,j \le n} = (p_1, \ldots, p_n)$, $P^{-1} = (q_{i,j})_{1 \le i,j \le n} = (q_1, \ldots, q_n)$, where p_i and q_i are the i-th columns of P and P^{-1}, respectively. $\mathcal{E}$ denotes a Feistel cipher with SP round function. $\mathcal{D}$ denotes a Feistel cipher with SPS round function. Brief descriptions of Camellia, SNAKE(2) and E2 are presented in Appendix A.

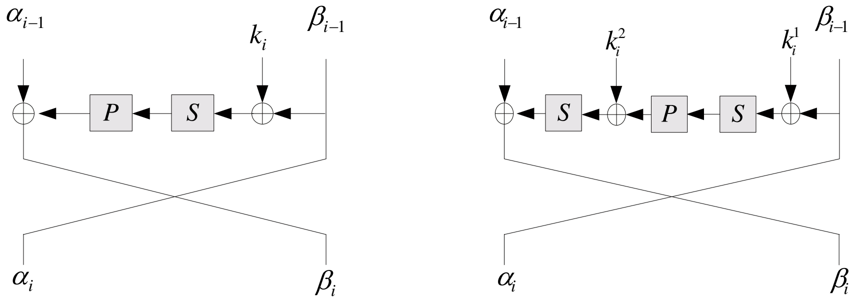

Fig. 1. Feistel Ciphers with SP and SPS Round Function

Proposition 1. *If the round function of a Feistel cipher is bijective, then* $(x, 0) \nrightarrow (0, x)$ *is a* 5*-round impossible differential of the cipher, where* $x \neq 0$.

The above proposition is pointed out by Knudsen. As described in Fig. 2, the output difference of the 3rd round function should be $x \oplus x = 0$, while the input difference is non-zero, which indicates a contradiction since f is bijective.

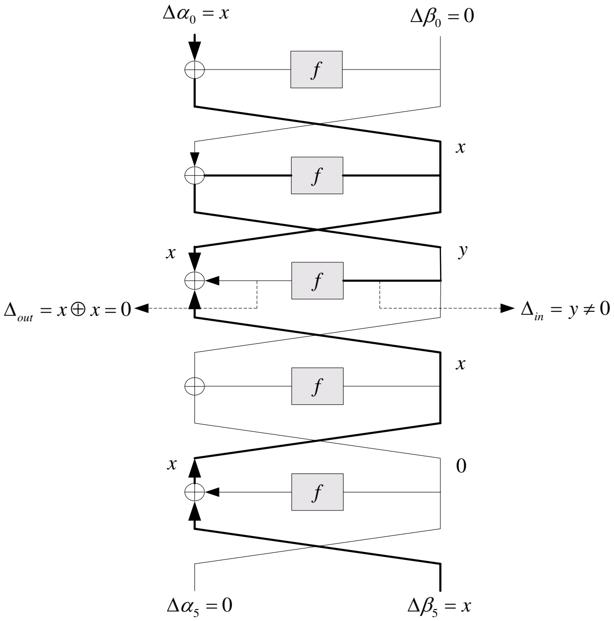

Fig. 2. 5-round Impossible Differential of Feistel Structure

2.2 χ-Function

In this section, we first give the definition of χ-function that maps any element of $\mathbb{F}_{2^t}^n$ to $\mathbb{F}_2^n$, and then discuss basic properties of χ-function.

Definition 1. ***(χ-Function)*** *Let $\theta : \mathbb{F}_{2^t} \to \mathbb{F}_2$ be defined as*

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

Then $\chi : \mathbb{F}_{2^t}^n \to \mathbb{F}_2^n$ is defined as

$$\chi(x_1, x_2, \ldots, x_n) = (\theta(x_1), \theta(x_2), \ldots, \theta(x_n)),$$

while $\chi_s : \mathbb{F}_{2^t}^n \to \mathbb{F}_2$ is defined as

$$\chi_s(x_1, x_2, \ldots, x_n) = \theta(x_s).$$

The χ-function is well used in truncated differential cryptanalysis, when we only consider whether there is a difference or not while the concrete value of the difference is out of consideration. If $\chi_s(\Delta X) = 1$ ($\Delta X \in \mathbb{F}_{2^t}^n$), it means that there is some non-zero difference at the s position.

For convenience, let $E_i \in \mathbb{F}_2^n$ be a vector whose i-th component is 1 while other components are 0, and e_i is any one of the vectors such that $\chi(e_i) = E_i$. For nonlinear transform layer S, we denote $S(X) \oplus S(X \oplus \Delta X)$ by $S(\Delta X)$.

Property 1. (1) For any difference $\Delta X \in \mathbb{F}_{2^t}^n$,

$$\chi(S(\Delta X)) = \chi(\Delta X);$$

(2) Let $P = (p_1, \ldots, p_n)$ where p_i is the i-th column of P, if $\Delta X = e_i$, then

$$\chi(P \circ S(\Delta X)) = \chi(P(\Delta X)) = p_i;$$

(3) Let $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_n)$, respectively, if $x_s = 0$, then

$$\chi_s(X \oplus Y) = \chi_s(Y).$$

Definition 2. ***(Hamming Weight)*** *Let $\mathbb{F}_q$ be a finite field with q elements, $X = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$. Then the Hamming Weight of X is defined as the number of non-zero components of X:*

$$w(X) = |\{i | x_i \neq 0, 1 \leq i \leq n\}|.$$

3 Analysis of Round-Reduced Feistel Cipher with *SP* Structure

By carefully analyzing the properties of the linear transformations and taking the χ-function into consideration, some sufficient conditions will be given which characterize the existence of 6/7/8-round impossible differentials of Feistel cipher with SP round functions (Notice that Feistel cipher with this structure is denoted by $\mathcal{E}$).

To apply the miss-in-the-middle technique effectively, we concentrate on differentials with the form $(e_i, 0) \rightarrow (0, e_j)$, i.e. both the Hamming weight of input difference and out difference are 1.

3.1 Analysis of 6-Round Feistel Cipher with *SP* Structure

Let (α_r, β_r) be the output of the r-th round, and Y_r and Z_r be the outputs of S-Box layer and P layer of the r-th round, respectively. In the following, impossibility of some differential $(e_i, 0) \rightarrow (0, e_j)$ will be proved given that some special properties of the linear transformation P are satisfied.

Proposition 2. *For linear transformation P, let $P \oplus P^{-1} = (\gamma_1, \gamma_2, \ldots, \gamma_n)$, where γ_i is the i-th column of $P \oplus P^{-1}$. If there exists an i, $1 \leq i \leq n$, such that $w(\gamma_i) \geq 2$, then for any j, $1 \leq j \leq n$, $(e_i, 0) \rightarrow (0, e_j)$ is a 6-round impossible differential of $\mathcal{E}$.*

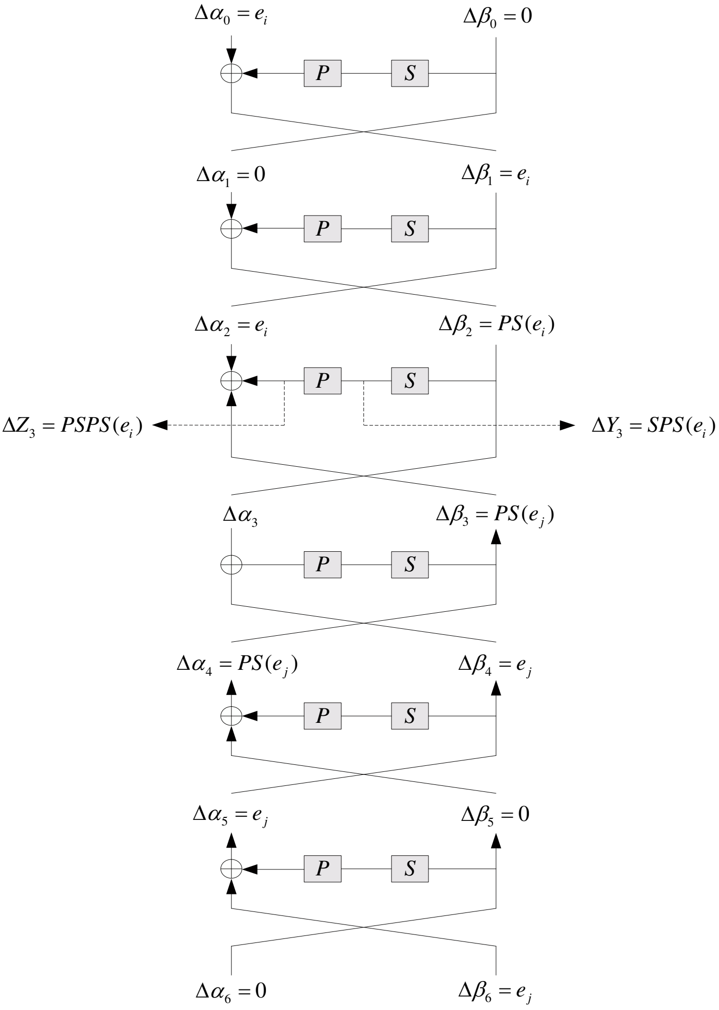

Fig. 3. 6-round Impossible Differential of Feistel-SP

Proof. Fig. 3 describes the 6-round impossible differential. From the encryption direction, if the input difference is

$$\Delta(\alpha_0, \beta_0) = (e_i, 0),$$

the differences of the output of the 1st and 2nd rounds can be calculated as follows:

$$\Delta(\alpha_1, \beta_1) = (0, e_i),$$
$$\Delta(\alpha_2, \beta_2) = (e_i, P \circ S(e_i)).$$

Accordingly, in the third round,

$$\Delta Y_3 = S \circ P \circ S(e_i),$$
$$\Delta Z_3 = P \circ S \circ P \circ S(e_i).$$

From the decryption direction, if the output difference (the 6-th round) is

$$\Delta(\alpha_6, \beta_6) = (0, e_j),$$

the differences of the output of the 5-th and 4-th rounds are

$$\Delta(\alpha_5, \beta_5) = (e_j, 0),$$
$$\Delta(\alpha_4, \beta_4) = (P \circ S(e_j), e_j).$$

According to the Feistel structure,

$$\Delta\alpha_4 = \Delta\beta_3 = \Delta Z_3 \oplus \Delta\alpha_2 = \Delta Z_3 \oplus \Delta\beta_1,$$

the following equation must hold:

$$P \circ S(e_j) = \Delta\alpha_4 = \Delta Z_3 \oplus \Delta\beta_1 = P \circ S \circ P \circ S(e_i) \oplus e_i,$$

which implies that

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

and

$$\chi(S(e_j)) = \chi\left(S \circ P \circ S(e_i) \oplus P^{-1}(e_i)\right).$$

From Property 1,

$$\chi(S(e_j)) = \chi(e_j) = E_j.$$

If $w(p_i \oplus q_i) \geq 2$, which implies that p_i and q_i differ at least 2 positions, say $p_{t_1,i} = 0$, $q_{t_1,i} = 1$ and $p_{t_2,i} = 1$, $q_{t_2,i} = 0$. Thus

$$\chi_{t_1}(S \circ P \circ S(e_i) \oplus P^{-1}(e_i)) = \chi_{t_1}(P^{-1}(e_i)) = 1,$$
$$\chi_{t_2}(S \circ P \circ S(e_i) \oplus P^{-1}(e_i)) = \chi_{t_2}(S \circ P \circ S(e_i)) = 1,$$

which implies that $w(\chi(S \circ P \circ S(e_i) \oplus P^{-1}(e_i))) \geq 2$, and this is contradicted with $\chi(S(e_j)) = E_j$ whose Hamming weight is 1. Thus $(e_i, 0) \rightarrow (0, e_j)$ is a 6-round impossible differential. □

Example 1. (6-Round Impossible Differential of Camellia) By careful computation, we have:

$$P \oplus P^{-1} = \begin{pmatrix} 1&1&0&0&0&0&0&0 \\ 0&1&1&0&0&0&0&0 \\ 0&0&1&1&0&0&0&0 \\ 1&0&0&1&0&0&0&0 \\ 0&0&0&0&1&1&0&0 \\ 0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&1&1 \\ 0&0&0&0&1&0&0&1 \end{pmatrix} = (\gamma_1, \gamma_2, \ldots, \gamma_8).$$

Since for any $1 \leq i \leq 8$, $w(\gamma_i) = 2$, according to Proposition 2, for any $1 \leq i, j \leq 8$, $(e_i, 0) \to (0, e_j)$ is a 6-round differential of Camellia.

3.2 Analysis of 7-Round Feistel Cipher with *SP* Structure

The 7-round Feistel ciphers with SP round functions can be analyzed similarly.

Proposition 3. *For linear transformation P, if there exists a triplet (i, j, k) such that the multiset $\{p_{k,i}, p_{k,j}, q_{k,i}, q_{k,j}\}$ is equal to $\{1, 0, 0, 0\}$, then $(e_i, 0) \to (0, e_j)$ is a 7-round impossible differential of $\mathcal{E}$.*

Proof. Let $\Delta(\alpha_0, \beta_0) = (e_i, 0)$ and $\Delta(\alpha_7, \beta_7) = (0, e_j)$, respectively. Then by analyzing the propagation of $\Delta(\alpha_0, \beta_0)$ and $\Delta(\alpha_7, \beta_7)$ from the encryption and decryption directions, respectively, we have (see Fig. 4)

$$\begin{aligned}
\Delta(\alpha_1, \beta_1) &= (0, e_i), \\
\Delta(\alpha_2, \beta_2) &= (e_i, P \circ S(e_i)), \\
\Delta Z_3 &= P \circ S \circ P \circ S(e_i), \\
\Delta(\alpha_6, \beta_6) &= (e_j, 0), \\
\Delta(\alpha_5, \beta_5) &= (P \circ S(e_j), e_j), \\
\Delta Z_5 &= P \circ S \circ P \circ S(e_j).
\end{aligned}$$

Since

$$\Delta\alpha_2 \oplus \Delta Z_3 = \Delta\beta_3 = \Delta\alpha_4 = \Delta\beta_5 \oplus \Delta Z_5,$$

thus

$$e_i \oplus P \circ S \circ P \circ S(e_i) = e_j \oplus P \circ S \circ P \circ S(e_j),$$

from which we have

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

Let $\rho_1 = \chi(P^{-1}(e_i))$, $\rho_2 = \chi(P^{-1}(e_j))$, $\rho_3 = \chi(S \circ P \circ S(e_i))$, $\rho_4 = \chi(S \circ P \circ S(e_j))$. According to Property 1, the following equations hold:

$$\begin{aligned}
\rho_1 &= q_i, \\
\rho_2 &= q_j, \\
\rho_3 &= p_i, \\
\rho_4 &= p_j.
\end{aligned}$$

Assume that there exists some t, such that $\{\rho_{1,t}, \rho_{2,t}, \rho_{3,t}, \rho_{4,t}\} = \{1, 0, 0, 0\}$, say $\rho_{1,t} = 1$, and $\rho_{2,t} = \rho_{3,t} = \rho_{4,t} = 0$, then

$$\chi_t(P^{-1}(e_i) \oplus P^{-1}(e_j)) = 1,$$

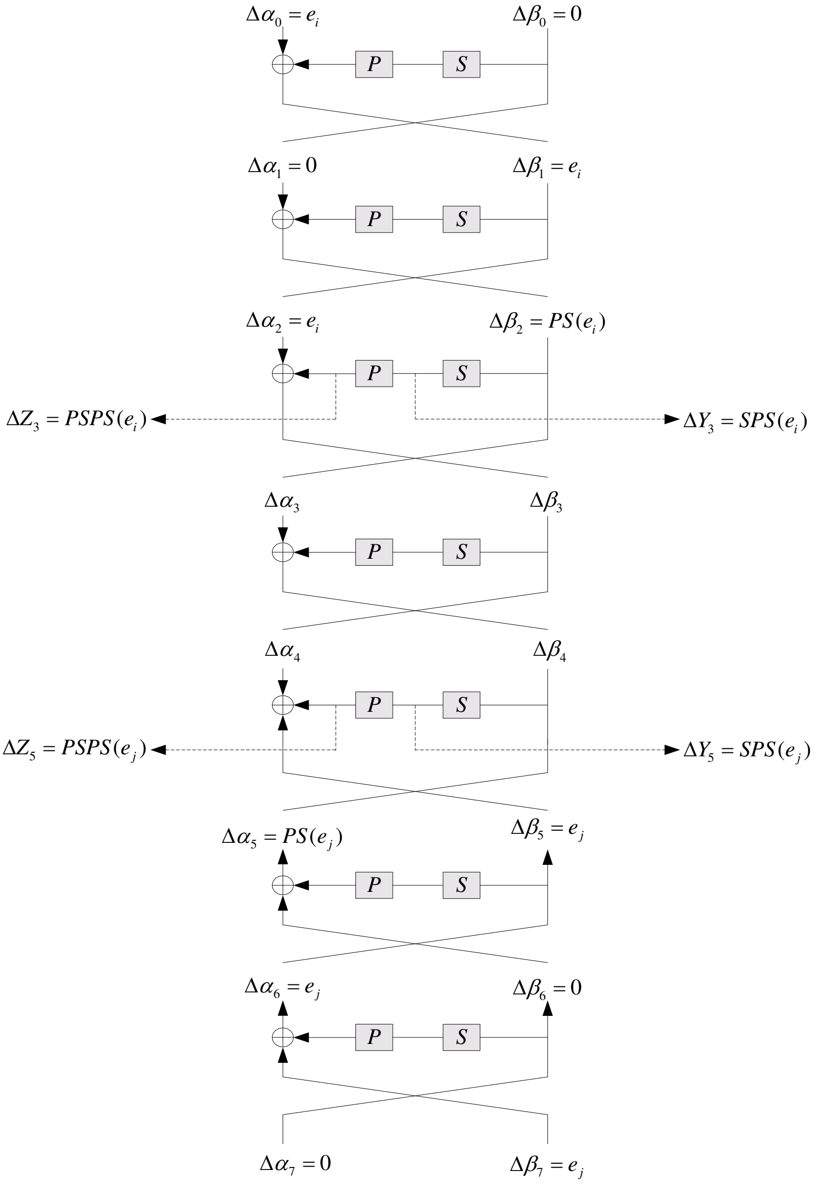

Fig. 4. 7-round Impossible Differential of Feistel-SP

and

$$\chi_t\left((S \circ P \circ S(e_i)) \oplus (S \circ P \circ S(e_j))\right) = 0,$$

which is a contradiction. Thus the above Proposition holds. □

Example 2. (7-Round Impossible Differentials of Camellia) By the definition of Camellia, we can determine $P = (p_{i,j})_{1\leq i,j\leq 8}$ and $P^{-1} = (q_{i,j})_{1\leq i,j\leq 8}$ as follows:

$$P = \begin{pmatrix} \underline{\mathbf{1}} & 0 & 1 & 1 & \underline{\mathbf{0}} & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & \underline{\mathbf{0}} & 1 & 1 & 1 & 1 & \underline{\mathbf{0}} & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \qquad P^{-1} = \begin{pmatrix} \underline{\mathbf{0}} & 1 & 1 & 1 & \underline{\mathbf{0}} & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & \underline{\mathbf{0}} & 1 & 1 & 1 & 1 & \underline{\mathbf{1}} & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Since $p_{1,1} = 1$, $p_{1,5} = q_{1,1} = q_{1,5} = 0$, $(e_1, 0) \to (0, e_5)$ is a 7-round impossible differential of Camellia; Similarly, $(e_2, 0) \to (0, e_7)$ is another 7-round impossible differential of Camellia since $q_{7,7} = 1$, $p_{7,2} = p_{7,7} = q_{7,2} = 0$.

3.3 Analysis of 8-Round Feistel Cipher with *SP* Structure

Let $\Delta(\alpha_0, \beta_0) = (e_i, 0)$, $\Delta(\alpha_8, \beta_8) = (0, e_j)$. Then from the encryption direction, we have (see Fig. 5):

$$\begin{aligned} &\Delta(\alpha_1, \beta_1) = (0, e_i), \\ &\Delta(\alpha_2, \beta_2) = (e_i, P \circ S(e_i)), \\ &\Delta(\alpha_3, \beta_3) = (P \circ S(e_i), e_i \oplus P \circ S \circ P \circ S(e_i)), \\ &\Delta Z_4 = P \circ S(e_i \oplus P \circ S \circ P \circ S(e_i)), \end{aligned}$$

and while analyzing from the decryption direction, we have

$$\begin{aligned} &\Delta(\alpha_7, \beta_7) = (e_j, 0), \\ &\Delta(\alpha_6, \beta_6) = (P \circ S(e_j), e_j), \\ &\Delta(\alpha_5, \beta_5) = (e_j \oplus P \circ S \circ P \circ S(e_j), P \circ S(e_j)). \end{aligned}$$

Since

$$\Delta\beta_2 \oplus \Delta Z_4 = \Delta\alpha_3 \oplus \Delta Z_4 = \Delta\beta_4 = \Delta\alpha_5,$$

the following equation holds

$$P \circ S(e_i) \oplus P \circ S(e_i \oplus P \circ S \circ P \circ S(e_i)) = e_j \oplus P \circ S \circ P \circ S(e_j),$$

which implies that

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

Let $U_{i,j} = \{t | p_{t,j} = q_{t,j} = 0, t \neq i\} = \{t_1, \ldots, t_u\}$, thus for any $t \in U_{i,j}$,

$$\chi_t \left(P^{-1}(e_j) \oplus S \circ P \circ S(e_j) \oplus S(e_i)\right) = 0,$$

which tells that

$$\chi_t(e_i \oplus P \circ S \circ P \circ S(e_i)) = 0.$$

and now, we have the following Proposition:

Proposition 4. *For any i and j, let*

$$\begin{aligned} U_{i,j} &= \{t | p_{t,j} = q_{t,j} = 0, t \neq i\} = \{t_1, \ldots, t_u\}, \\ V_i \ &= \{r | p_{r,i} = 1\} = \{r_1, \ldots, r_v\}, \end{aligned}$$

and

$$M_{i,j} = (p_{t_a, r_b})_{u \times v} = (m_1, \ldots, m_v).$$

If $U_{i,j} \neq \emptyset$, $V_i \neq \emptyset$, and there exists an s, $1 \leq s \leq v$, such that

$$\text{rank}\{m_1, \ldots, m_v\} = \text{rank}\{\{m_1, \ldots, m_v\} \setminus \{m_s\}\} + 1,$$

then $(e_i, 0) \to (0, e_j)$ is an 8-round impossible differential of $\mathcal{E}$.

Proof. Let $\eta = e_i \oplus P \circ S \circ P \circ S(e_i)$, $\lambda = S \circ P \circ S(e_i)$. Then

$$\chi_t(\lambda) = \begin{cases} 1 & \text{if } t \in V_i, \\ 0 & \text{if } t \notin V_i. \end{cases}$$

Accordingly, $\chi_t(\lambda) \neq 0$ holds if and only if when $\lambda_t \neq 0$. Thus

$$\eta = e_i \oplus (p_{r_1}, \ldots, p_{r_v})(\lambda_{r_1}, \ldots, \lambda_{r_v})^{\mathrm{T}},$$

where $r_1 < \cdots < r_v$, $r_k \in V_i (1 \leq k \leq v)$ and p_{r_k} is the r_k-th column of P.

By the definition of $U_{i,j}$, we have

$$\eta_t = 0 \qquad \text{if} \qquad t \in U_{i,j},$$

thus

$$\begin{pmatrix} p_{t_1,r_1} & \cdots & p_{t_1,r_v} \\ \vdots & & \vdots \\ p_{t_u,r_1} & \cdots & p_{t_u,r_v} \end{pmatrix} \begin{pmatrix} \lambda_{r_1} \\ \vdots \\ \lambda_{r_v} \end{pmatrix} \triangleq (M_{i,j})_{u,v} \tilde{\lambda} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

where $t_k \in U_{i,j}$, $r_k \in V_i$ and $\lambda_{r_k} \neq 0$.

The above equation can be described as

$$(m_1, \ldots, m_{s-1}, m_{s+1}, \ldots, m_v)(\lambda_1, \ldots, \ldots, \lambda_v)^{\mathrm{T}} = \lambda_s m_s,$$

from linear algebra, the equation has solutions if and only if

$$\text{rank}\{\{m_1, \ldots, m_v\} \setminus \{m_s\}\} = \text{rank}\{m_1, \ldots, \lambda_s m_s, \ldots, m_v\}.$$

Since $\mathrm{rank}\{m_1, \ldots, m_v\} = \mathrm{rank}\{\{m_1, \ldots, m_v\} \setminus \{m_s\}\} + 1$, if $(M_{i,j})_{u,v}\tilde{\lambda} = 0$ has a solution $\tilde{\lambda} = (\lambda_1, \ldots, \lambda_v)$, λ_s must be 0 which is a contradiction. □

For most cases, especially when $n = 4$ or $n = 8$, $|U_{i,j}| = u \leq 2$. According to Proposition 4, the case that $u = 1$ and $u = 2$ can be characterized as follows:

Proposition 5. *Let $U_{i,j}$ and V_i defined as in Proposition 4, and*

$$M_{i,j} = (p_{t_a, r_b})_{u \times v} = \begin{pmatrix} l_1 \\ \vdots \\ l_u \end{pmatrix}.$$

(1) *If $u = 1$ and $w(l_1) = 1$, then $(e_i, 0) \to (0, e_j)$ is an 8-round impossible differential of $\mathcal{E}$.*
(2) *If $u = 2$ and $w(l_1 \oplus l_2) = 1$, then $(e_i, 0) \to (0, e_j)$ is an 8-round impossible differential of $\mathcal{E}$.*

Example 3. (8-Round Impossible Differentials of Camellia) We verify $(e_2, 0) \to (0, e_2)$ is an 8-round impossible differential. From the linear transformation of Camellia we have,

$$P = \begin{pmatrix} 1&0&1&1&0&1&1&1 \\ 1&1&0&1&1&0&1&1 \\ 1&1&1&0&1&1&0&1 \\ 0&1&1&1&1&1&1&0 \\ 1&1&0&0&0&1&1&1 \\ 0&1&1&0&1&0&1&1 \\ 0&\underline{\mathbf{0}}&\underline{\mathbf{1}}&\underline{\mathbf{1}}&\underline{\mathbf{1}}&\underline{\mathbf{1}}&0&1 \\ 1&\underline{\mathbf{0}}&\underline{\mathbf{0}}&\underline{\mathbf{1}}&\underline{\mathbf{1}}&\underline{\mathbf{1}}&1&0 \end{pmatrix} \qquad P^{-1} = \begin{pmatrix} 0&1&1&1&0&1&1&1 \\ 1&0&1&1&1&0&1&1 \\ 1&1&0&1&1&1&0&1 \\ 1&1&1&0&1&1&1&0 \\ 1&1&0&0&1&0&1&1 \\ 0&1&1&0&1&1&0&1 \\ 0&\underline{\mathbf{0}}&1&1&1&1&1&0 \\ 1&\underline{\mathbf{0}}&0&1&0&1&1&1 \end{pmatrix}.$$

Since $p_{7,2} = q_{7,2} = 0$, $p_{8,2} = q_{8,2} = 0$,

$$U_{2,2} = \{7, 8\}.$$

Since $p_{2,2} = p_{3,2} = p_{4,2} = p_{5,2} = p_{6,2} = 1$, we have

$$V_2 = \{2, 3, 4, 5, 6\},$$

Thus $M_{2,2}$ is a sub-matrix of P

$$M_{2,2} = \begin{pmatrix} 0&1&1&1&1 \\ 0&0&1&1&1 \end{pmatrix}.$$

Since,

$$2 = \mathrm{rank} M_{2,2} = \mathrm{rank}\{M_{2,2} \setminus \{l_2\}\} + 1,$$

we know that $(e_2, 0) \to (0, e_2)$ is an 8-round impossible differential of Camellia which is consistent with [11].

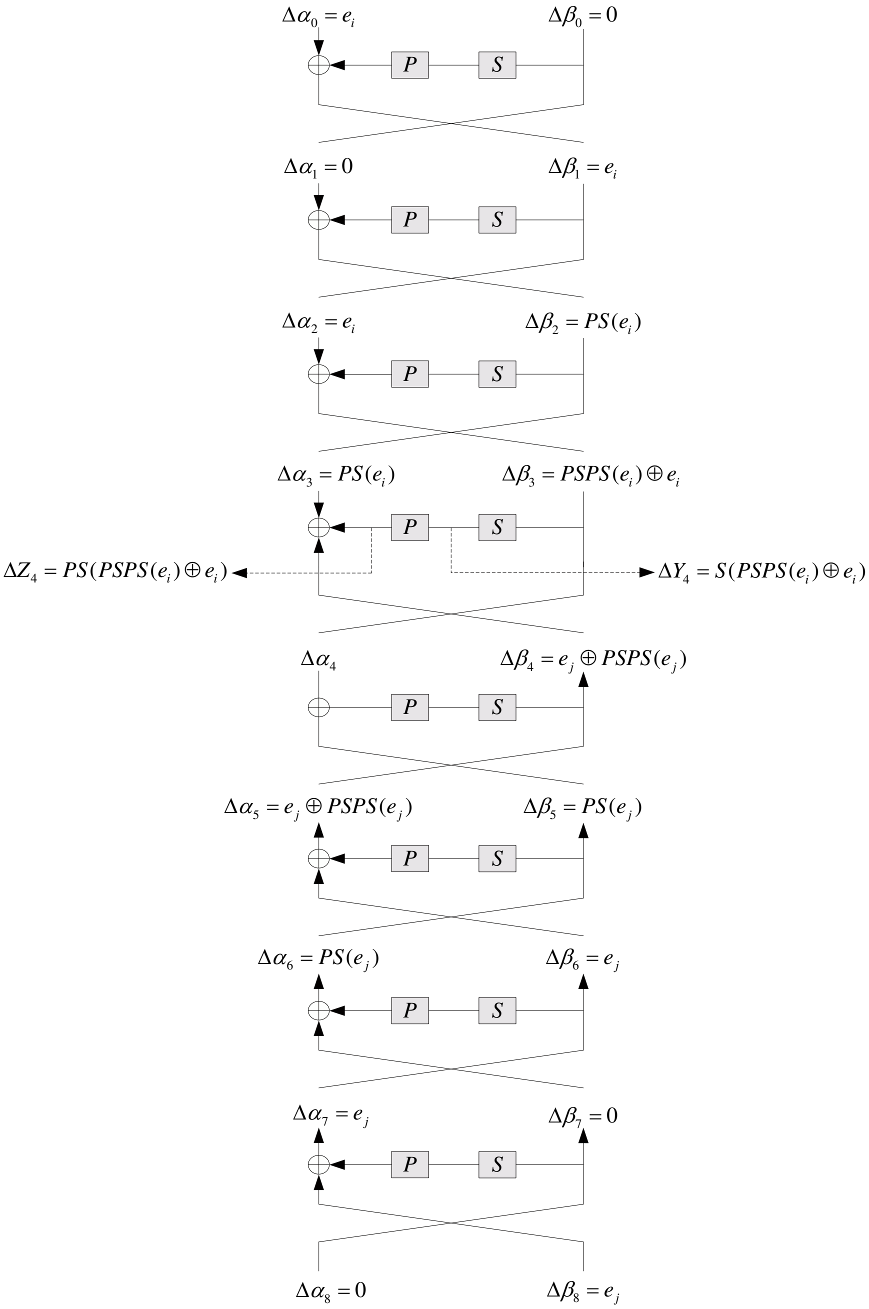
$\Delta\alpha_0 = e_i$
$\Delta\beta_0 = 0$
P
S
$\Delta\alpha_1 = 0$
$\Delta\beta_1 = e_i$
P
S
$\Delta\alpha_2 = e_i$
$\Delta\beta_2 = PS(e_i)$
P
S
$\Delta\alpha_3 = PS(e_i)$
$\Delta\beta_3 = PSPS(e_i) \oplus e_i$
P
S
$\Delta Z_4 = PS(PSPS(e_i) \oplus e_i)$
$\Delta Y_4 = S(PSPS(e_i) \oplus e_i)$
$\Delta\alpha_4$
$\Delta\beta_4 = e_j \oplus PSPS(e_j)$
P
S
$\Delta\alpha_5 = e_j \oplus PSPS(e_j)$
$\Delta\beta_5 = PS(e_j)$
P
S
$\Delta\alpha_6 = PS(e_j)$
$\Delta\beta_6 = e_j$
P
S
$\Delta\alpha_7 = e_j$
$\Delta\beta_7 = 0$
P
S
$\Delta\alpha_8 = 0$
$\Delta\beta_8 = e_j$

Fig. 5. 8-round Impossible Differential of Feistel-SP

Example 4. (8-Round Impossible Differentials of SNAKE(2)) SNAKE(2) is equivalent to Feistel structure with SP round function by adding a P^{-1} in the beginning and a P in the end. By the definition of SNAKE(2), we describe P and P^{-1} as follows:

$$P = \begin{pmatrix} 1\,1\,1\,1 \\ 1\,0\,0\,\underline{\mathbf{0}} \\ 1\,1\,0\,0 \\ 1\,1\,1\,0 \end{pmatrix} \qquad P^{-1} = \begin{pmatrix} 0\,1\,0\,0 \\ 0\,1\,1\,\underline{\mathbf{0}} \\ 0\,0\,1\,1 \\ 1\,0\,0\,1 \end{pmatrix}.$$

Hence,

$$U_{4,4} = \{2\},\ V_4 = \{1\},\ \text{and}\ M_{4,4} = \{1\}.$$

Since $w(l_1) = 1$, $(e_4, 0) \to (0, e_4)$ is an 8-round impossible differential of SP part of SNAKE(2). Therefore, $(P(e_4), 0) \to (0, P(e_4))$ is an 8-round impossible differential of SNAKE(2).

4 Analysis of 6-Round Feistel Cipher with *SPS* Structure

By using the same techniques that are used in analyzing 8-round Feistel ciphers with SP round functions, a characterization for the existence of 6-round of Feistel cipher with SPS round functions (Notice that Feistel cipher with this structure is denoted by $\mathcal{D}$) can be given as follows, and the details of the proof are omitted.

Proposition 6. *For any i and j, let*

$$\begin{aligned} U_{i,j} &= \{t | p_{t,j} = 0, t \neq i\} = \{t_1, \ldots, t_u\}, \\ V_i &= \{r | p_{r,i} = 1\} = \{r_1, \ldots, r_v\}, \end{aligned}$$

and

$$M_{i,j} = (p_{t_a, r_b})_{u \times v} = (m_1, \ldots, m_v).$$

If $U_{i,j} \neq \emptyset$, $V_i \neq \emptyset$, and there exists an s, $1 \leq s \leq v$, such that

$$\text{rank}\{m_1, \ldots, m_v\} = \text{rank}\{\{m_1, \ldots, m_v\} \setminus \{m_s\}\} + 1,$$

then $(e_i, 0) \to (0, e_j)$ is a 6-round impossible differential of $\mathcal{D}$.

Proposition 7. *Let $U_{i,j}$ and V_i be defined as in Proposition 6, and*

$$M_{i,j} = (p_{t_a, r_b})_{u \times v} = \begin{pmatrix} l_1 \\ \vdots \\ l_u \end{pmatrix}.$$

(1) *If $u = 1$ and $w(l_1) = 1$, then $(e_i, 0) \to (0, e_j)$ is a 6-round impossible differential of $\mathcal{D}$.*

(2) *If* $u = 2$ *and* $w(l_1 \oplus l_2) = 1$*, then* $(e_i, 0) \rightarrow (0, e_j)$ *is a* 6*-round impossible differential of* $\mathcal{D}$*.*

Example 5. (6-Round Impossible Differentials of E2) Since the permutation BRL after the 2nd nonlinear transformation layer of E2 is a byte-transposition, the structure is equivalent to an SPS structure, where the linear transformation $P^{'}$ is defined as:

$$P^{'} = BRL \circ P = \begin{pmatrix} 1\,0\,1\,1\,0\,1\,1\,1 \\ 1\,1\,0\,1\,1\,0\,1\,1 \\ 1\,1\,1\,0\,1\,1\,0\,1 \\ 1\,1\,0\,1\,1\,1\,0\,0 \\ 1\,1\,1\,0\,0\,1\,1\,0 \\ 0\,1\,1\,1\,0\,0\,1\,1 \\ 1\,0\,1\,1\,1\,0\,0\,1 \\ 0\,1\,1\,1\,1\,1\,1\,0 \end{pmatrix}.$$

We have

$$U_{1,3} = \{2, 4\}, \quad V_1 = \{1, 2, 3, 4, 5, 7\},$$

hence,

$$M_{1,3} = \begin{pmatrix} 1\,1\,0\,1\,1\,1 \\ 1\,1\,0\,1\,1\,0 \end{pmatrix}.$$

Since,

$$w(l_1 \oplus l_2) = 1,$$

$(e_1, 0) \rightarrow (0, e_3)$ is a 6-round impossible differential of E2, whereas only 5-round impossible differentials were previously known[3].

5 Conclusion

In this paper, we propose impossible differential cryptanalysis on Feistel ciphers with SP and SPS round functions. Both 6/7/8-round impossible differentials of Feistel cipher with SP round functions and 6-round impossible differential of Feistel cipher with SPS round functions can be judged by verifying some properties of linear transformations. The former result that 5-round impossible differential exists when round function is bijective is improved. Since we know a lot about Feistel cipher against impossible differential cryptanalysis, the properties presented in this paper should be considered when designing a block cipher.

Acknowledgements

The authors would like to thank Vincent Rijmen and Ruilin Li for their helpful comments and corrections that improved the quality of the paper. We are also grateful to the anonymous referees for their valuable remarks.

This work is supported by the Natural Science Foundation of China (No: 60803156) and the open research fund of State Key Laboratory of Information Security (No: 01– 07).

References

1. NTT-Nippon Telegraph and Telephone Corporation: E2: Efficient Encryption Algorithm, `http://info.isl.ntt.co.jp/e2`
2. Lee, C., Cha, Y.: The Block Cipher: SNAKE with Provable Resistance against DC and LC attacks. In: JW-ISC 1997, pp. 3–17 (1997)
3. Aoki, K., Kanda, M.: Search for Impossible Differential of E2, `http://csrc.nist.gov/encryption/aes/round1/comment`
4. Feistel, H.: Cryptography and Data Security. Scientific American 228(5), 15–23 (1973)
5. Aoki, K., Ichikawa, T., Kanda, M., et al.: Specification of Camellia — a 128–bit Block Cipher. In: Stinson, D.B., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 183–191. Springer, Heidelberg (2001)
6. Duo, L., Li, C., Feng, K.: New Observation on Camellia. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 51–64. Springer, Heidelberg (2006)
7. Knudsen, L.: DEAL — A 128-bit Block Cipher. Technical Report 151, Department of Informatics, University of Bergen, Bergen, Norway (1998)
8. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999)
9. Biham, E., Biryukov, A., Shamir, A.: Miss in the Middle Attacks on IDEA and Khufu. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 124–138. Springer, Heidelberg (1999)
10. Sugita, M., Kobara, K., Imai, H.: Security of Reduced Version of the Block Cipher Camellia against Truncated and Impossible Differential Cryptanalysis. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 193–207. Springer, Heidelberg (2001)
11. Wu, W., Zhang, W., Feng, D.: Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia. Journal of Computer Science and Technology 22(3), 449–456 (2007)
12. Wu, W., Zhang, L., Zhang, W.: Improved Impossible Differential Cryptanalysis of Reduced–Round Camellia. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 442–456. Springer, Heidelberg (2009)
13. Lu, J., Kim, J., Keller, N., et al.: Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1. In: Malkin, T.G. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 370–386. Springer, Heidelberg (2008)
14. Lu, J., Dunkelman, O., Keller, N., et al.: New Impossible Differential Attacks on AES. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 279–293. Springer, Heidelberg (2008)
15. Dunkelman, O., Keller, N.: An Improved Impossible Differential Attack on MISTY1. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 441–454. Springer, Heidelberg (2008)
16. Mala, H., Shakiba, M., Dakhilalian, M., Bagherikaram, G.: New Results on Impossible Differential Cryptanalysis of Reduced-Round Camellia–128. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 281–294. Springer, Heidelberg (2009)
17. Kim, J., Hong, S., Sung, J., Lee, S., Lim, J.: Impossible Differential Cryptanalysis for Block Cipher Structures. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 82–96. Springer, Heidelberg (2003)

A Appendix

A.1 Brief Description of Camellia

Camellia is a Feistel cipher with SP round function and has 18 rounds (for 128-bit keys) or 24 rounds (for 192/256-bit keys). The FL/FL^{-1} function layer is inserted at every 6 rounds. In this paper, we consider Camellia without FL/FL^{-1} function layer. The nonlinear layer S and linear transformation P in the round function of Camellia are represented as follows. For more details, we refer to [5].

$$\begin{gathered} S : \mathbb{F}_{2^8}^8 \rightarrow \mathbb{F}_{2^8}^8 : (x_1, x_2, \ldots, x_8) \rightarrow (y_1, y_2, \ldots, y_8) \\ y_1 = s_1(x_1),\, y_2 = s_2(x_2),\, y_3 = s_3(x_3),\, y_4 = s_4(x_4), \\ y_5 = s_2(x_5),\, y_6 = s_3(x_6),\, y_7 = s_4(x_7),\, y_8 = s_1(x_8), \end{gathered}$$

where s_1, s_2, s_3 and s_4 are 8×8 nonlinear transformations (s-boxes).

$$P : \mathbb{F}_{2^8}^8 \rightarrow \mathbb{F}_{2^8}^8 \colon (y_1, y_2, \ldots, y_8) \rightarrow P(y_1, y_2, \ldots, y_8)$$

$$P = \begin{pmatrix} 1\,0\,1\,1\,0\,1\,1\,1 \\ 1\,1\,0\,1\,1\,0\,1\,1 \\ 1\,1\,1\,0\,1\,1\,0\,1 \\ 0\,1\,1\,1\,1\,1\,1\,0 \\ 1\,1\,0\,0\,0\,1\,1\,1 \\ 0\,1\,1\,0\,1\,0\,1\,1 \\ 0\,0\,1\,1\,1\,1\,0\,1 \\ 1\,0\,0\,1\,1\,1\,1\,0 \end{pmatrix}$$

A.2 Brief Description of SNAKE(2)

SNAKE(1) and SNAKE(2) are Feistel ciphers proposed by Lee and Cha at JW-ISC'97 [2] and this paper concentrates on SNAKE(2) only. Although it employs a PS round function, according to [6], SNAKE(2) is equivalent to a Feistel cipher with SP round function by adding a P^{-1} transformation before the first round and a P transformation after the last round. The nonlinear layer S and linear transformation P in the round function of SNAKE(2) are represented as follows.

$$\begin{gathered} S : \mathbb{F}_{2^8}^4 \rightarrow \mathbb{F}_{2^8}^4 : (x_1, x_2, x_3, x_4) \rightarrow (y_1, y_2, y_3, y_4) \\ y_1 = s(x_1),\, y_2 = s(x_2),\, y_3 = s(x_3),\, y_4 = s(x_4), \end{gathered}$$

where s is an 8×8 nonlinear transformation.

$$P : \mathbb{F}_{2^8}^4 \rightarrow \mathbb{F}_{2^8}^4 \colon (y_1, y_2, y_3, y_4) \rightarrow P(y_1, y_2, y_3, y_4)$$

$$P = \begin{pmatrix} 1\,1\,1\,1 \\ 1\,0\,0\,0 \\ 1\,1\,0\,0 \\ 1\,1\,1\,0 \end{pmatrix}$$

A.3 Brief Description of E2

E2, designed by NTT, is a candidate of AES [1]. It employs Feistel structure with an SPS round function. There is also an initial transformation in the beginning and a final transformation in the end. Another permutation BRL is placed after the 2nd non linear transformation layer. The non-linear layer S and linear transformation P and BRL in the round function of E2 are represented as follows.

$$\begin{aligned} S : \mathbb{F}_{2^8}^8 \rightarrow \mathbb{F}_{2^8}^8 : (x_1, x_2, \ldots, x_8) &\rightarrow (y_1, y_2, \ldots, y_8) \\ y_1 = s(x_1),\, y_2 = s(x_2),\, y_3 &= s(x_3),\, y_4 = s(x_4), \\ y_5 = s(x_5),\, y_6 = s(x_6),\, y_7 &= s(x_7),\, y_8 = s(x_8), \end{aligned}$$

where s is an 8×8 nonlinear transformation.

$$P : \mathbb{F}_{2^8}^8 \rightarrow \mathbb{F}_{2^8}^8\text{: } (y_1, y_2, \ldots, y_8) \rightarrow P(y_1, y_2, \ldots, y_8)$$

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

$$BRL : \mathbb{F}_{2^8}^8 \rightarrow \mathbb{F}_{2^8}^8\text{: } (y_1, y_2, \ldots, y_8) \rightarrow (y_2, y_3, \ldots, y_8, y_1).$$