Journal of Universal Computer Science, vol. 19, no. 16 (2013), 2453-2471
submitted: 15/7/13, accepted: 27/9/13, appeared: 1/10/13 © J.UCS

Observations of Skipjack-like Structure with SP/SPS Round Function

Ting Cui
(Information Science and Technology Institute, Zhengzhou, China
cuiting_1209@hotmail.com)

Chenhui Jin
(Information Science and Technology Institute, Zhengzhou, China
jinchenhui@126.com)

Guoshuang Zhang
(Science and Technology on Information Assurance Laboratory, Beijing, China
guoshuang_zhang@sina.com)

Abstract: Impossible differential cryptanalysis is an important tool for evaluating the security level of a block cipher, and the key step of this cryptanalysis is to find the longest impossible differential. This paper focuses on retrieving impossible differentials for m-cell Skipjack-like structure with SP/SPS round function (named $Skipjack_{SP}$ and $Skipjack_{SPS}$ resp.). Up to now, known longest impossible differentials in m-cell Skipjack-like structures is m^2 rounds. In this paper, we provide some new m^2 rounds impossible differentials for these two structures. Further, we prove that if P layer is chosen from binary matrices, we can always retrieve $m^2 + 1$ rounds impossible differentials for these two structures, and $m^2 + 2$ rounds impossible differentials for $Skipjack_{SP}$. Moreover, if P layer satisfies some satiable conditions, we may further obtain $m^2 + 2$ rounds impossible differential for $Skipjack_{SPS}$. Our results show that we should choose P layer carefully when employing these two structures.

Key Words: block Cipher, Skipjack-like structure, permutation layer, impossible differential
Category: SD E.3, SD C.2.0, SD D.4.6

1 Introduction

The architecture is one of the most important parts of block ciphers. It will directly affect the implementation performance and the choice of round number. Architectures of block ciphers could be roughly classified by SP structure [Daemen, Rijmen (2002)], Feistel structure [Standard (1999)] and generalized Feistel structure [Nyberg (1996)]. The SP structure is a simple and clear block cipher model which is designed to implement Shannon's suggestions of confusion and diffusion. This architecture is adopted by the famous block cipher AES [Daemen, Rijmen (2002)]. As well, many block ciphers, including Camellia, E2, CLEFIA [Aoki et al. (2001), Kanda et al. (1998), Shirai et al. (2007)] etc. adopt such kind of round function. Except for the SP structure, the Feistel structure is another important structure since it provides flexibility in the design of round function. There are a lot of block ciphers employ this architecture, such as DES, E2, Camellia [Standard (1999), Kanda et al. (1998), Aoki et al. (2001)] etc.

As we know, modern ciphers usually adopt 128-bit (or longer) data length. If we construct a 128-bit block cipher with the Feistel structure, we need to find a 64-bit round function. However, to construct 64-bit round function is not as easy as the 32-bit round function, and the 64-bit round function will bring extra cost in implementation, either. In [Nyberg (1996)], Nyberg introduced generalized Feistel structures. The generalized Feistel structures are generalized forms of the classical Feistel structure. These structures reserve some advantages of classical Feistel cipher such as flexibility in the design of round functions, and could be implemented easily by adopting slight round functions. Large series of ciphers like Skipjack [Biham et al. (1999)], CAST256 [Adams (1999)], MARS [Burwick (1998)], CLEFIA [Shirai et al. (2007)] etc. use these structures as their architectures. Among them, the block cipher Skipjack using two types of rounds, called Rule A and Rule B. Within the Skipjack cipher, the data block is divided into four subblocks, and eight rounds of Rule A and eight rounds of Rule B are applied alternatively until the full 32 rounds are achieved. In order to measure the security level of Skipjack, people often consider Rule A or Rule B independently [Pudovkina (2009)][Kim et al. (2010)][Sung et al. (2000)], and in this paper, we will also treat Rule A as the Skipjack-like structure.

Impossible differential cryptanalysis was first proposed by Knudsen [Knudsen (1998)] and Biham [Biham et al. (1999)]. This cryptanalysis uses impossible differentials to discard the wrong keys. It has been used to attack Skipjack, AES, Camellia, ARIA, E2 [Biham et al. (1999)], [Lu et al. (2008)], [Wu and Zhang et al. (2007)], [Liu et al. (2012)], [Bai et al. (2012)], [Wei et al. (2012)] etc. and produced many good results. The key step of impossible differential cryptanalysis is to find the longest impossible differentials [Wei et al. (2010)]. For generalized Feistel structures, since only part of the data is processed in each round, there always exist long round impossible differentials. This makes these ciphers vulnerable to impossible differential cryptanalysis.

In light of the powerful efficiencies of impossible differential cryptanalysis, many experts work on finding impossible differential distinguishers for block cipher structures, and lots of wonderful results are achieved. In [Kim et al. (2003)], $\mathcal{U}$-methods were provided by Kim et al. to find impossible differentials of block ciphers structures. This method uses the inconsistencies of the elements in the specially defined set $\mathcal{U}$ to find impossible differentials. Later in [Luo et al. (2009)], Yiyuan Luo et.al. proposed the UID method, which can find longer impossible differential distinguishers than the $\mathcal{U}$-method. However, these two methods consider only the overall structure of block ciphers, hence some longer impossible differentials which caused by round functions are ignored. For instance, Li et al. [Li et al. (2010)] and Wu et al. [Wu et al. (2009)] investigated a new kind of generalized Feistel network called n-cell GF-NLFSR, the results explain that for n-cell GF-NLFSR, there exists n^2+n-2 rounds impossible differential distinguishers, which significantly improve the result obtained by the $\mathcal{U}$-method. Furthermore, some elaborate criteria based on the diffusion layer for finding impossible differentials are proposed recently. Wei et al. [Wei et al. (2010)] provided several impossible differential distinguishers for classical Feistel ciphers with SP and SPS round function. Li et al. [Li et al. (2011)] proposed methods to find impossible differentials for SPN ciphers. And in [Li et al. (2012)], Li et al. investigated impossible differentials of MISTY structure with SP-based round function. And recently, Wu et al [Wu and Wang(2012)] proposed a new method to find impossible differentials.

Inspired by the previous work, this paper presents some new inconsistencies to construct impossible differential distinguishers of Skipjack-like structures with SP and SPS round function. To our knowledge, existed longest impossible differential in m-cell Skipjack-like cipher is m^2 rounds. And in this paper, we find new m^2 rounds impossible differentials of $Skipjack_{SP}/Skipjack_{SPS}$, and also some m^2+1 /m^2+2 rounds impossible differentials from $Skipjack_{SP}$ and $Skipjack_{SPS}$.

This paper is organized as below: [Section 2] introduces some preliminaries. [Section 3] presents the differential properties of Skipjack-like structure and its decryption structure. [Section 4] focuses on finding impossible differential distinguisher of m-cell Skipjack-like structures with SP and SPS round function. [Section 5] concludes this paper.

2 Preliminaries

2.1 Notations

Throughout this paper, we will use the following symbols.

$\oplus$: XOR operation;

$w(X)$: the number of nonzero components of vector X;

$|$: matrices concatenation;

E : the identity matrix;

Δx : the XOR difference of x and x';

$\Delta_f(\Delta x)$[1]: the output difference of f when the input difference is Δx.

[1] It is well known that if f is a linear bijection, then $\Delta_f(\Delta x) = f(\Delta x)$, and when f is a non-linear bijection, $\Delta_f(\Delta x)$ may have several values, in this case, we can choose any one for further discussion, and if necessary, we will use $\Delta_f^{(i)}(\Delta x)$ to distinguish them.

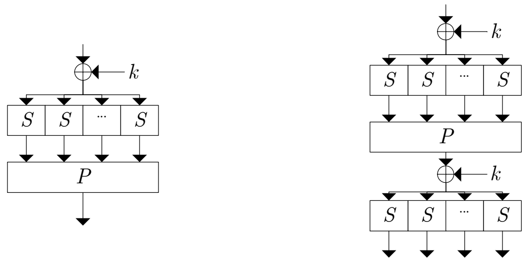

Figure 1: SP and SPS type round function.

$g \circ f$:	composition of function f and g, i.e. $g \circ f(x) = g(f(x))$;
$M_{(k)}$:	the k-th column of matrix $M_{n\times n}$;
$e_{\{i_1,\cdots,i_r\}}$:	vector with nonzero values only in the $i_1,\cdots,i_r$-th components;
e_{i_k} :	the i_k-th component of $e_{\{i_1,\cdots,i_r\}}$;
$\varepsilon_{\{u_1,\cdots,u_q\}}$:	vector with same nonzero values only in the $u_1,\cdots,u_q$-th components;
P^{-1} :	the inverse matrix of P;
$P_{i,j}$:	the (i,j)-entry of matrix P.

Definition 1 [Daemen, Rijmen (2002)]. (SP network) Let $S_1,\cdots,S_d : \{0,1\}^n \rightarrow \{0,1\}^n$ be non-linear **bijections**, $P : F_{2^n}^d \rightarrow F_{2^n}^d$ is a linear bijection, $k = (k_1,\cdots,k_d)$ is the round key, then the round function $Round_{SP} : F_{2^n}^d \times F_{2^n}^d \rightarrow F_{2^n}^d$ of SP network (SPN) is defined by

$$Round_{SP}(x,k) = P(S_1(x_1 \oplus k_1),\cdots,S_d(x_d \oplus k_d)).$$

SP and SPS networks are two basic structures of modern ciphers, and many ciphers employ these structure in their round functions [Aoki et al. (2001)], [Kanda et al. (1998)],[Shirai et al. (2007)],[Kim et al. (2003)],[Li et al. (2010)], [Wu et al. (2009)],[Wu and Wang(2012)]. [Fig.1] describes the SP and SPS round function.

Definition 2 [Shirai et al. (2002)]. (χ-function & θ-function) $\chi : F_{2^m}^d \rightarrow F_2^d$ is defined by

$$\chi(x_1,\cdots,x_d) = (\theta(x_1),\cdots,\theta(x_d)),$$

where $\theta : F_{2^m} \rightarrow F_2$ is defined by $\theta(x) = \begin{cases} 1, if\ x \neq 0; \\ 0, if\ x = 0. \end{cases}$, function $\chi_s : F_{2^m}^d \rightarrow F_2$ is defined by $\chi_s(X) = \theta(x_s)$ for any $X = (x_1,\cdots,x_d)$

As mentioned in [Shirai et al. (2002)], when S is a bijection, we have $\chi(\Delta_S(X)) = \chi(X)$.

Definition 3 [Daemen, Rijmen (2002)]. (differential branch number) Let $f(x) = Px$ be a linear mapping, where P is a $d \times d$ matrix over F_{2^n}, then

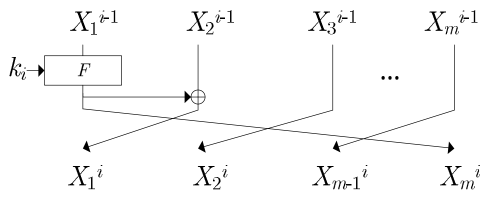

Figure 2: m-cell Skipjack-like Structure.

the differential branch number of f is defined by

$$D_f = \min_{x \neq 0}\{w(x) + w(P \times x)\}.$$

Definition 4. (binary diffusion layer) A linear bijection $f{:}F_{2^n}^d \to F_{2^n}^d$ is defined as a binary diffusion layer, if f could be represented by a $d \times d$ binary matrix, i.e.

$$f(x) = P_{d \times d} \times x.$$

2.2 Skipjack-like Structure

An m-cell Skipjack-like network consists of r rounds, each round is defined as follows.

Let $(X_1^{i-1}, X_2^{i-1}, \cdots, X_m^{i-1})$ be the input to the i-th($i \geq 1$) round, $(X_1^i, X_2^i, \cdots, X_m^i)$ and k_i be the output and the round key of the i-th round, resp.

$(X_1^i, X_2^i, \cdots, X_m^i) = Round(X_1^{i-1}, X_2^{i-1}, \cdots, X_m^{i-1})$ is defined as:

$$\begin{cases} X_1^i = F(k_i, X_1^{i-1}) \oplus X_2^{i-1}; \\ X_j^i = X_{j+1}^{i-1}, \;\; 2 \leq j \leq m-1; \\ X_m^i = F(k_i, X_1^{i-1}). \end{cases}$$

where F is the round function ([Fig.2] describes one round of m-cell Skipjack-like network).

Remark 1. The decrypt operation of m-cell Skipjack-like network is

$$\begin{cases} X_1^{i-1} = F^{-1}(k_i, X_m^i); \\ X_2^{i-1} = X_1^i \oplus X_m^i; \\ X_j^{i-1} = X_{j-1}^i, \quad 3 \leq j \leq m. \end{cases}$$

Later in this paper, we use $Skipjack_{SP}$ ($Skipjack_{SPS}$ resp.) to denote m-cell Skipjack-like network who employs SP (SPS resp.) type round function. In these two round functions, all parameters are as illustrated in Definition 1.

3 Two Properties of Skipjack-like Structure

In this section, we will study the differential propagation properties of Skipjack-like structure.

Lemma 1. For the m-cell Skipjack-like structure, any non-trivial differential of the round function is with the following form

$$(\Delta x_1, \cdots, \Delta x_{m-1}, \Delta x_m) \rightarrow (\Delta_F(\Delta x_1) \oplus \Delta x_2, \Delta x_3, \cdots, \Delta x_{m-1}, \Delta_F(\Delta x_1)).$$

Lemma 2. If m-cell Skipjack-like structure satisfies $(\Delta X_1^0, \cdots, \Delta X_m^0) = (0, \cdots, 0, \Delta x)$, then we have $\Delta X_m^m = \Delta_F(\Delta x)$ and $\Delta X_m^{m+1} = \Delta_{F^2}(\Delta x)$.

Proof. See [Tab.1].

Table 1: $2m-2$ rounds differential trail of m-cell Skipjack-like structure from encryption direction

Round/Diff	0	0	$\cdots$	0	Δx
1	0	0	$\cdots$	Δx	0
$\cdots$			$\cdots$	0	0
$m-2$	0	Δx	$\cdots$	0	0
$m-1$	Δx	0	$\cdots$	0	0
m	$\Delta_F(\Delta x)$	0	$\cdots$	0	$\Delta_F(\Delta x)$
$m+1$	$\Delta_{F^2}(\Delta x)$	0	$\cdots$	$\Delta_F(\Delta x)$	$\Delta_{F^2}(\Delta x)$
$m+2$	$\Delta_{F^3}(\Delta x)$	0	$\cdots$	$\Delta_{F^2}(\Delta x)$	$\Delta_{F^3}(\Delta x)$
$\cdots$					
$2m-3$	$\Delta_{F^{m-2}}(\Delta x)$	0	$\cdots$	$\Delta_{F^{m-3}}(\Delta x)$	$\Delta_{F^{m-2}}(\Delta x)$
$2m-2$	$\Delta_{F^{m-1}}(\Delta x)$	$\Delta_F(\Delta x)$	$\cdots$	$\Delta_{F^{m-2}}(\Delta x)$	$\Delta_{F^{m-1}}(\Delta x)$

Lemma 3. Let $s < m-2$, if the output difference of m-1 round m-cell Skipjack-like structure is $(\Delta X_1^{m-1}, \cdots, \Delta X_m^{m-1}) = (0, \cdots, 0, \Delta z_1, \cdots, \Delta z_s, \Delta y)$, then we have $(\Delta X_1^0, \cdots, \Delta X_m^0) = (0, \cdots, 0, \Delta_1, \cdots, \Delta_s, \Delta z_s \oplus \Delta_{F^{-1}}(\Delta y), \Delta y)$, where $\Delta_1, \Delta_2, \cdots, \Delta_s$ denotes some uncertain value.

Proof. See [Tab.2].

Lemma 4. Let the output difference of m-cell Skipjack-like structure be

$$(\Delta X_1^{m(m-1)+1}, \cdots, \Delta X_m^{m(m-1)+1}) = (\Delta y, 0, \cdots, 0),$$

then we have $\Delta X_2^{m-1} = \Delta y$ and $\Delta X_m^0 = \bigoplus_{i=1}^{m-1} \Delta_{F^{-1}}^{(i)}(\Delta y)$.

Table 2: $m-1$ rounds differential trail of m-cell Skipjack-like structure from decrypt direction

Round	**Differential**
0	$(0,\cdots,0,\Delta_1,\cdots,\Delta_s,\Delta_{F^{-1}}(\Delta y)\oplus\Delta z_s,\Delta y)$
	$\uparrow$
$\vdots$	$\vdots$
	$\uparrow$
$m-s-3$	$(0,\Delta_1,\Delta_2,\cdots,\Delta_s,\Delta_{F^{-1}}(\Delta y)\oplus\Delta z_s,\Delta y,0,\cdots,0)$
	$\uparrow$
$m-s-2$	$(\Delta_1,\Delta_2,\cdots,\Delta_s,\Delta_{F^{-1}}(\Delta y)\oplus\Delta z_s,\Delta y,0,\cdots,0)$
	$\uparrow$
$\vdots$	$\vdots$
	$\uparrow$
$m-3$	$(\Delta'_s,\Delta_{F^{-1}}(\Delta y)\oplus\Delta z_s,\Delta y,0,\cdots,0,\Delta z_1,\cdots,\Delta z_{s-1})$
	$\uparrow$
$m-2$	$(\Delta_{F^{-1}}(\Delta y),\Delta y,0,\cdots,0,\Delta z_1,\Delta z_2,\cdots,\Delta z_s)$
	$\uparrow$
$m-1$	$(0,\cdots,0,\Delta z_1,\Delta z_2,\cdots,\Delta z_s,\Delta y)$

Proof. Firstly, according to Lemma 2,

$$(\Delta X_1^{(m-1)^2+1},\cdots,\Delta X_m^{(m-1)^2+1})=(0,\cdots,0,\Delta y),$$

Then by iteratively applying Lemma 3 $(m-2)$ times,

$$(\Delta X_1^m,\Delta X_2^m,\cdots,\Delta X_m^m)=(0,\Delta_1,\cdots,\Delta_{m-3},\bigoplus_{i=1}^{m-2}\Delta_{F^{-1}}^{(i)}(\Delta y),\Delta y).$$

According to Lemma 1, we have

$$(\Delta X_1^{m-1},\cdots,\Delta X_m^{m-1})=(\Delta_{F^{-1}}^{(m-1)}(\Delta y),\Delta y,\Delta_1,\cdots,\Delta_{m-3},\bigoplus_{i=1}^{m-2}\Delta_{F^{-1}}^{(i)}(\Delta y)),$$

thus

$$\Delta X_m^0=\Delta X_{m-1}^1=\cdots=\Delta X_2^{m-2}=\bigoplus_{i=1}^{m-1}\Delta_{F^{-1}}^{(i)}(\Delta y).$$

We summarize the main results of this section in [Fig.3]. And in the next section, we will take advantage of them to find impossible differentials.

$$\begin{aligned}
&(0, \cdots, 0, \Delta x)\\
&\downarrow \mathtt{m-round}\\
&\Delta X_m^m = \Delta_F(\Delta x)\\
&\downarrow \mathtt{1-round}\\
&\Delta X_m^{m+1} = \Delta_{F^2}(\Delta x)\\
&\downarrow \mathtt{(m-3)-round}\\
&\Delta X_2^{2m-2} = \Delta_F(\Delta x)\\
&\\
&\Delta X_m^0 = \bigoplus_{i=1}^{m-1} \Delta_{F^{-1}}^{(i)}(\Delta y)\\
&\uparrow \mathtt{(m-1)-round}\\
&\Delta X_2^{m-1} = \Delta y\\
&\uparrow \mathtt{[(m-1)^2+1]-round}\\
&(\Delta y, 0, \cdots, 0)
\end{aligned}$$

Figure 3: Two differential properties of m-cell Skipjack-like structure.

4 $m^2/m^2+1/m^2+2$ Rounds Impossible Differential of $Skipjack_{SP}/Skipjack_{SPS}$

In Asiacrypt00, J. Sung conjectured that for m-cell *Skipjack*-like structure, there is no impossible differential longer than $m^2 - 1$ [Sung et al. (2000)], and this conjecture was claimed being proved in the rump of FSE09 [Pudovkina (2009)]. However, in [Kim et al. (2010)], m^2 rounds impossible differential

$$(0, \alpha, 0, \cdots, 0) \to (\beta, \beta, 0, \cdots, 0)$$

was founded, hence the conjecture results mentioned in [Sung et al. (2000)] and [Pudovkina (2009)] was disproved. In this section, more details of the round function are taken into consideration, we can find some new $m^2/\ m^2+1/\ m^2+2$ rounds impossible differentials of $Skipjack_{SP}$ and $Skipjack_{SPS}$ structure.

Note: Throughout this paper, we always assume that S layers are consist of bijective S-boxes.

4.1 m^2 Rounds Impossible Differential of $Skipjack_{SP}/Skipjack_{SPS}$

Theorem 1(m^2 rounds impossible differential of $Skipjack_{SP}$ $/Skipjack_{SPS}$). Let P be the diffusion layer of an m-cell $Skipjack_{SP}/Skipjack_{SPS}$, if the branch number of P is D_P, then for any $\alpha, \beta \in F_{2^n}^d \backslash \{0\}$ satisfying $w(\alpha) + w(\beta) < D_P$,

$(0, \cdots, 0, \alpha) \to (\beta, 0, \cdots, 0)$ is an m^2 rounds impossible differential of m-cell $Skipjack_{SP}/Skipjack_{SPS}$.

Proof. Let the m^2 rounds differential of $Skipjack_{SP}$ ($Skipjack_{SPS}$, resp.) be $(0, \cdots, 0, \alpha) \to (\beta, 0, \cdots, 0)$, we have these two relations from encrypt and decrypt directions:

$$\Delta X_2^{2m-2} = \Delta_F(\alpha) = \Delta_{P \circ S}(\alpha)$$

$$(\Delta X_2^{2m-2} = \Delta_F(\alpha) = \Delta_{S \circ P \circ S}(\alpha), resp.)$$

and

$$\Delta X_2^{2m-2} = \beta.$$

Assume $(0, \cdots, 0, \alpha) \to (\beta, 0, \cdots, 0)$ is an m^2 rounds possible differential, then

$$\beta = \Delta_{P \circ S}(\alpha) = P \times \Delta_S(\alpha).$$

$$(\Delta_{S^{-1}}(\beta) = \Delta_{P \circ S}(\alpha) = P \times \Delta_S(\alpha), resp.)$$

According to Definition 3, we have

$$w(P \times \Delta_S(\alpha)) + w(\Delta_S(\alpha)) = w(\beta) + w(\alpha) \geq D_P,$$

$$(w(P \times \Delta_S(\alpha)) + w(\Delta_S(\alpha)) = w(\Delta_{S^{-1}}(\beta)) + w(\alpha) = w(\beta) + w(\alpha) \geq D_P, resp.)$$

which leads to a contradiction. Thus $(0, \cdots, 0, \alpha) \not\to (\beta, 0, \cdots, 0)$ is an m^2 rounds impossible differential of $Skipjack_{SP}$($Skipjack_{SPS}$, resp.).

It is easily to see from Theorem 1 that for an m-cell $Skipjack_{SP}$ /$Skipjack_{SPS}$ structure, we can always find m^2 rounds impossible differential. Actually, the impossible differential showed in Theorem 1 is based on the inconsistence of the P layer: *branch number bounds the minimum weight of P layers differential(i.e. the number of nonzero n-bit words in a differential), when the weight of a differential is less than the lower bound, this differential is impossible.* Furthermore, this kind of inconsistence could be extended as below.

Theorem 2(m^2 rounds impossible differential of $Skipjack_{SP}$ /$Skipjack_{SPS}$). Let P be the diffusion layer of an m-cell $Skipjack_{SP}$ /$Skipjack_{SPS}$, if $P_{(i_1)}, \cdots, P_{(i_s)}, E_{(j_1)}, \cdots, E_{(j_t)}$ are linearly independent, then

$$(0, \cdots, 0, e_{\{i_1, \cdots, i_s\}}) \to (e_{\{j_1, \cdots, j_t\}}, 0, \cdots, 0)$$

is an m^2 rounds impossible differential of m-cell $Skipjack_{SP}$ /$Skipjack_{SPS}$.

Proof. According to Theorem 1, we only need to prove $e_{\{j_1, \cdots, j_t\}} = P \times \Delta_S(e_{\{i_1, \cdots, i_s\}})$ ($\Delta_{S^{-1}}(e_{\{j_1, \cdots, j_t\}}) = P \times \Delta_S(e_{\{i_1, \cdots, i_s\}})$.resp.) is impossible.

$$e_{\{j_1, \cdots, j_t\}} = P \times \Delta_S(e_{\{i_1, \cdots, i_s\}}) \Leftrightarrow (P|E) \times \begin{pmatrix} \Delta_S(e_{\{i_1, \cdots, i_s\}}) \\ e_{\{j_1, \cdots, j_t\}} \end{pmatrix} = 0,$$

$$(\Delta_{S^{-1}}(e_{\{j_1,\cdots,j_t\}}) = P\times\Delta_S(e_{\{i_1,\cdots,i_s\}}) \Leftrightarrow (P|E)\times\begin{pmatrix}\Delta_S(e_{\{i_1,\cdots,i_s\}})\\ \Delta_{S^{-1}}(e_{\{j_1,\cdots,j_t\}})\end{pmatrix} = 0.resp.)$$

which could be rewritten as

$$\left(\overset{s}{\underset{k=1}{\oplus}} \Delta_S(e_{i_k}) \times P_{(i_k)}\right) \oplus \left(\overset{t}{\underset{r=1}{\oplus}} e_{j_r} \times E_{(j_r)}\right) = 0.$$

$$(\left(\overset{s}{\underset{k=1}{\oplus}} \Delta_S(e_{i_k}) \times P_{(i_k)}\right) \oplus \left(\overset{t}{\underset{r=1}{\oplus}} \Delta_{S^{-1}}(e_{j_r}) \times E_{(j_r)}\right) = 0, resp.)$$

Since $P_{(i_1)}, \cdots, P_{(i_s)}, E_{(j_1)}, \cdots, E_{(j_t)}$ are linearly independent and $e_{i_1,\cdots,i_s}$, $e_{j_1,\cdots,j_t}$ are nonzero, this equation is impossible. Thus we obtain this theorem.

In the next, we will concentrate in the P layers which are binary matrices, the reason we study {0,1}-matrices is because they are faster to compute than MDS transforms, another reason is that in hardware implementation, they will take up less space and thus allow for more compact implementation. Also, they have been employed by many famous ciphers, including Camellia [Aoki et al. (2001)], E2 [Kanda et al. (1998)] and so on. When the P layer is chosen as a binary matrix, Theorem 2 shows a simpler form as below.

Corollary 1. If diffusion layer $P_{d\times d}$ is a nonsingular matrix over a finite field F, then there always exists $1 \le i, j \le d$ such that

$$(0, \cdots, 0, e_{\{i\}}) \to (e_{\{j\}}, 0, \cdots, 0)$$

is an m^2 rounds impossible differential of $Skipjack_{SP}/Skipjack_{SPS}$.

Proof. By Theorem 2, we only need to give the existence of i, j such that $P_{(i)}$ and $E_{(j)}$ are linearly independent, we launch a contradiction method here. If $P_{(i)}$ and $E_{(j)}$ are linearly dependent for any $1 \le i \le d$, then for any $i' \ne i$, $P_{(i')}$ and $E_{(j)}$ are linearly independent (otherwise $P_{d\times d}$ is singular).

Existing results show that m^2 rounds impossible differential $(0, \alpha, 0, \cdots, 0) \to (\beta, \beta, 0, \cdots, 0)$ is the longest impossible differential [Kim et al. (2010)]. Analysis above indicates that we may obtain some new impossible differentials of $Skipjack_{SP}$ /$Skipjack_{SPS}$ by checking the linearly independent vectors in $(P|E)$.

4.2 $m^2 + 1$ Rounds Impossible Differential of $Skipjack_{SP}/Skipjack_{SPS}$

In this section, we will focus on retrieving longer impossible differentials for $Skipjack_{SP}$ and $Skipjack_{SPS}$ whose diffusion layer P are defined by binary matrices.

Theorem 3 (m^2+1 rounds impossible differential of $Skipjack_{SP}$ $/Skipjack_{SPS}$). Let P be a diffusion layer of an m-cell $Skipjack_{SP}$ $/Skipjack_{SPS}$. If there exist $\{i_1, i_2, \cdots, i_s\}$, $\{j_1, j_2, \cdots, j_t\} \subseteq \{1, 2, \cdots, d\}$ and $1 \le p \le d$ such that $\sum_{r=1}^{s} w(P_{p,i_r}) = 1$ and $\sum_{r=1}^{t} w(P^{-1}_{p,j_r}) = 0$, then

$$(0, \cdots, 0, e_{\{i_1,\cdots,i_s\}}) \to (e_{\{j_1,\cdots,j_t\}}, 0, \cdots, 0)$$

is an m^2+1 rounds impossible differential of m-cell $Skipjack_{SP}$ $/Skipjack_{SPS}$.

Proof. Let m^2+1 rounds differential of $Skipjack_{SP}$ $/Skipjack_{SPS}$ be

$$(0, \cdots, 0, e_{\{i_1,\cdots,i_s\}}) \to (e_{\{j_1,\cdots,j_t\}}, 0, \cdots, 0)$$

From the encryption direction, we have

$$\Delta X_m^m = \Delta_{P\circ S}(e_{\{i_1,\cdots,i_s\}}) = P \times \Delta_S(e_{\{i_1,\cdots,i_s\}}) \quad = \bigoplus_{k=1}^{s} \left(\Delta_S(e_{i_k}) \times P_{(i_k)}\right)$$

$$(\Delta X_m^m = \Delta_{S\circ P\circ S}(e_{\{i_1,\cdots,i_s\}}) = \Delta_S \left[P \times \Delta_S(e_{\{i_1,\cdots,i_s\}})\right]$$

$$= \Delta_S \left[\bigoplus_{k=1}^{s} \left(\Delta_S(e_{i_k}) \times P_{(i_k)}\right)\right], resp.)$$

Hence

$$\chi_p(\Delta X_m^m) = \chi_p \left[\bigoplus_{r=1}^{s} \left(\Delta_S(e_{i_r}) \times P_{(i_r)}\right)\right] = \theta \left[\bigoplus_{r=1}^{s} \left(\Delta_S(e_{i_r}) \times P_{p,i_r}\right)\right]$$

$$(\chi_p(\Delta X_m^m) = \chi_p \left[\Delta_S \left(\bigoplus_{k=1}^{s} \left(\Delta_S(e_{i_k}) \times P_{(i_k)}\right)\right)\right]$$

$$= \theta \left[\bigoplus_{r=1}^{s} \left(\Delta_S(e_{i_r}) \times P_{p,i_r}\right)\right], resp.)$$

Notice $\sum_{r=1}^{s} w(P_{p,i_r}) = 1$, and for any $1 \le r \le s$, there holds $\Delta_S(e_{i_r}) \ne 0$, then $\chi_p(\Delta X_m^m) = 1$

From the decrypt direction,

$$\Delta X_m^m = \bigoplus_{l=1}^{m-1} \Delta^{(l)}_{(P\circ S)^{-1}}(e_{\{j_1,\cdots,j_t\}}) = \bigoplus_{l=1}^{m-1} \Delta^{(l)}_{S^{-1}} \left[P^{-1} \times (e_{\{j_1,\cdots,j_t\}})\right]$$
$$= \bigoplus_{l=1}^{m-1} \Delta^{(l)}_{S^{-1}} \left[\bigoplus_{k=1}^{t} \left(e_{j_k} \times P^{-1}_{(j_k)}\right)\right]$$

$(\Delta X_m^m = \overset{m-1}{\underset{l=1}{\oplus}} \Delta^{(l)}_{(S\circ P\circ S)^{-1}}(e_{\{j_1,\cdots,j_t\}}) = \overset{m-1}{\underset{l=1}{\oplus}} \Delta^{(l)}_{S^{-1}}\left(P^{-1}\times \Delta_{S^{-1}}(e_{\{j_1,\cdots,j_t\}})\right)$
$= \overset{m-1}{\underset{l=1}{\oplus}} \Delta^{(l)}_{S^{-1}}(\overset{t}{\underset{k=1}{\oplus}} \Delta_{S^{-1}}(e_{j_k})\times P^{-1}_{(j_k)}), resp.)$ Hence

$$\chi_p(\Delta X_m^m) = \chi_p\left[\overset{m-1}{\underset{l=1}{\oplus}} \Delta^{(l)}_{S^{-1}}(\overset{t}{\underset{k=1}{\oplus}} e_{j_k}\times P^{-1}_{(j_k)})\right] = \theta\left(\overset{m-1}{\underset{l=1}{\oplus}} \Delta^{(l)}_{S^{-1}}\left[\overset{t}{\underset{k=1}{\oplus}}\left(e_{j_k}P^{-1}_{p,j_k}\right)\right]\right).$$

$$\begin{aligned}(\chi_p(\Delta X_m^m) &= \chi_p\left[\overset{m-1}{\underset{l=1}{\oplus}} \Delta^{(l)}_{S^{-1}}(\overset{t}{\underset{k=1}{\oplus}} \Delta^{(l)}_{S^{-1}}(e_{j_k})\times P^{-1}_{(j_k)})\right]\\ &= \theta\left[\overset{m-1}{\underset{l=1}{\oplus}} \Delta^{(l)}_{S^{-1}}(\overset{t}{\underset{k=1}{\oplus}} \Delta^{(l)}_{S^{-1}}(e_{j_k})\, P^{-1}_{p,j_k})\right], resp.)\end{aligned}$$

And for $\sum\limits_{r=1}^{t} w(P^{-1}_{p,j_r}) = 0$, we have

$$\chi_p(\Delta X_m^m) = 0$$

which leads a contradiction. Thus $(0,\cdots,0,e_{\{i_1,\cdots,i_s\}}) \rightarrow (e_{\{j_1,\cdots,j_t\}},0,\cdots,0)$ is an m^2+1 rounds impossible differential.

It is worthwhile for declare that when the P layer employs a binary matrix, the condition of Theorem 3 is satisfiable, which means we can always find m^2+1 rounds impossible differentials. And we will illustrate it in Corollary 2.

Corollary 2. Given an m-cell $Skipjack_{SP}$ /$Skipjack_{SPS}$ with diffusion layer $P_{d\times d}$, if P is a binary matrix, then we can always find m^2+1 rounds impossible differential.

Proof. By Cramer's rule, P^{-1} is also a binary matrix. Then by Theorem 3, we only need to prove that there always exist $1 \le i,j,p \le d$, such that $P_{p,i} = 1$ and $P^{-1}_{p,j} = 0$.

Let $1 \le p_1 < p_2 \le d$, then there exist $1 \le i_1, i_2 \le d$ such that $P_{p_1,i_1} = 1$ and $P_{p_2,i_2} = 1$ (otherwise P will be singular).

If $P^{-1}_{p_1,j} = 0$ for some $1 \le j \le d$, then we have $P_{p_1,i_1} = 1$ and $P^{-1}_{p_1,j} = 0$;

If $P^{-1}_{p_1,j} = 1$ for any $1 \le j \le d$, then there exists some j_0, such that $P^{-1}_{p_2,j_0} = 0$ (otherwise the p_1-th and p_2-th rows of P^{-1} are both $(1,1,\cdots 1)$, which indicates P is singular). Thus we have $P_{p_2,i_2} = 1$ and $P^{-1}_{p_2,j_0} = 0$.

4.3 m^2+2 Rounds Impossible Differential of $Skipjack_{SP}$/$Skipjack_{SPS}$

Theorem 4 (m^2+2 rounds impossible differential of $Skipjack_{SP}$).Let binary matrix $P_{d\times d}$ be the diffusion layer of m-cell $Skipjack_{SP}$. For some $1 \le j_1, j_2 \le d$, if

(1) $P_{v_1,j_1}, P_{v_2,j_1}, \cdots, P_{v_p,j_1}$ are all the nonzero entries of $P_{(i)}$;
(2) $P_{u_1,j_2}, P_{u_2,j_2}, \cdots, P_{u_q,j_2}$ are all the nonzero entries of $P_{(j_2)}$;
(3) $P_{(v_1)}, P_{(v_2)}, \cdots, P_{(v_p)}, E_{(j_2)}$ are linearly independent.
then $(0, \cdots, 0, e_{\{j_1\}}) \to (\varepsilon_{\{u_1,\cdots,u_q\}}, 0, \cdots, 0)$ is an m^2+2 rounds impossible differential of $Skipjack_{SP}$. Moreover, we can always find such j_1 and j_2.

Proof. We will prove the first result by finding contradiction.

Since from the encryption direction,

$$\Delta X_m^{m+1} = \Delta_{P\circ S\circ P\circ S}(e_{\{j_1\}}) = P \times \Delta_S(P_{(j_1)} \times \Delta_S(e_{j_1}))$$

let $\Delta_S(P_{(j_1)} \times \Delta_S(e_{j_1})) = \alpha$, then by (1), the nonzero values of α are only occur in the $v_1, v_2, \cdots, v_p$ -th components.

By (2), we have

$$P \times e_{\{j_2\}} = e_{j_2} \cdot P_{(j_2)}$$

Since P is a binary matrix, then all the nonzero components in $e_{j_2} \cdot P_{(j_2)}$ are of the same value, which indicates $e_j \cdot P_{(j)}$ could be represented by $\varepsilon_{\{u_1,\cdots,u_q\}}$. We denote the nonzero value of $\varepsilon_{\{u_1,\cdots,u_q\}}$ by $const'$, then

$$P^{-1} \times \varepsilon_{\{u_1,\cdots,u_q\}} = const' \times E_{(j_2)}$$

Hence from the decrypt direction,

$$\Delta X_m^{m+1} = \overset{m-1}{\underset{l=1}{\oplus}} \Delta^{(l)}_{S^{-1}\circ P^{-1}}(\varepsilon_{\{u_1,\cdots,u_q\}}) = \overset{m-1}{\underset{l=1}{\oplus}} \Delta^{(l)}_{S^{-1}}(P^{-1} \times \varepsilon_{\{u_1,\cdots,u_q\}})$$

$$= \overset{m-1}{\underset{l=1}{\oplus}} \Delta^{(l)}_{S^{-1}}(const' \times E_{(j_2)}) \overset{\Delta}{=} const \times E_{(j_2)}$$

Assume $(0, \cdots, 0, e_{\{j_1\}}) \to (\varepsilon_{\{u_1,\cdots,u_q\}}, 0, \cdots, 0)$ is possible, then $P \times \alpha = const \times E_{(j_2)}$, which could be represented as $\overset{p}{\underset{k=1}{\oplus}} \alpha_{v_k} \times P_{(v_k)} \oplus const \times E_{(j_2)} = 0$. However, by (3), $P_{(v_1)}, P_{(v_2)}, \cdots, P_{(v_p)}, E_{(j_2)}$ are linearly independent, Thus we get the contradiction and end the first proof.

Next, we will show how to find such j_1 and j_2.

Since binary matrix P is invertible, then there exists some $1 \le j_1 \le d$, such that we can find entry 0 in $P_{(j_1)}$, let

$$\{v_1, v_2, \cdots, v_p\} = \{t : P_{t,j_1} \ne 0, 1 \le t \le d\},$$

Accordingly,

$$rank(P_{(v_1)}, P_{(v_2)}, \cdots, P_{(v_p)}) = p < d.$$

If for any $1 \le k \le d$, $P_{(v_1)}, P_{(v_2)}, \cdots, P_{(v_p)}, E_{(k)}$ are linearly dependent, since $P_{(v_1)}, P_{(v_2)}, \cdots, P_{(v_p)}$ are linearly independent, then we can assume

$$E_{(k)} = \overset{p}{\underset{l=1}{\oplus}} x_{k,l} \times P_{(v_l)},$$

which implies

$$E = \left(E_{(1)}, E_{(2)}, \cdots, E_{(d)}\right) = \left(P_{(v_1)}, P_{(v_2)}, \cdots, P_{(v_p)}\right) \times \begin{pmatrix} x_{1,1} & x_{2,1} & \cdots & x_{d,1} \\ x_{1,2} & x_{2,2} & & x_{d,2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{1,p} & x_{2,p} & \cdots & x_{d,p} \end{pmatrix},$$

thus

$$d = rank(E) = rank(\left(P_{(v_1)}, P_{(v_2)}, \cdots, P_{(v_p)}\right) \times \begin{pmatrix} x_{1,1} & x_{2,1} & & x_{d,1} \\ x_{1,2} & x_{2,2} & & x_{d,2} \\ \vdots & \vdots & \ddots & \\ x_{1,p} & x_{2,p} & & x_{d,p} \end{pmatrix}) \le p.$$

This leads a contradiction, hence we can find some $1 \le j_2 \le d$, such that $P_{(v_1)}, P_{(v_2)}, \cdots, P_{(v_p)}, E_{(j_2)}$ are linearly independent. Thus we constructed such j_1 and j_2.

Example 1. Given $d = 8, n = 8, m = 4$, we employ the diffusion layer of Camellia [Aoki et al. (2001)] as the P layer(see Appendix 1.), we choose $i = 5$ and $j = 1$, $v_1 = 2, v_2 = 3, v_3 = 4, v_4 = 6, v_5 = 7, v_6 = 8$, and we notice that $P_{(2)}, P_{(3)}, P_{(4)}, P_{(6)}, P_{(7)}, P_{(8)}, E_{(1)}$ are linearly independent, hence $(0, \cdots, 0, e_{\{5\}}) \to (\varepsilon_{\{1,2,3,5,8\}}, 0, \cdots, 0)$ is an 18 rounds impossible differential of $Skipjack_{SP}$ /$Skipjack_{SPS}$.

Theorem 5($m^2 + 2$ rounds impossible differential of $Skipjack_{SP/SPS}$). Let matrix $P_{d\times d}$ be the diffusion layer of m-cell $Skipjack_{SP/SPS}$. $\{u_1, \cdots, u_p\}$, $\{v_1, \cdots, v_q\}$, $\{i_1, \cdots, i_s\}$, $\{j_1, \cdots, j_t\}$ are subsets of $\{1, \cdots, d\}$, and

$$k \notin \{u_1, \cdots, u_p\} \cup \{v_1, \cdots, v_q\}.$$

If:

(1) $P_{(u_1)}, P_{(u_2)}, \cdots, P_{(u_p)}$,$E_{(v_1)}, E_{(v_2)}, \cdots, E_{(v_q)}$ are linearly independent;
(2) $P_{k,i_1} = P_{k,i_2} = \cdots = P_{k,i_s} = 0$;
(3) $P^{-1}_{k,j_1} = P^{-1}_{k,j_2} = \cdots = P^{-1}_{k,j_t} = 0$.

then

$$(0, \cdots, 0, e_{\{i_1,\cdots,i_s\}}) \to (e_{\{j_1,\cdots,j_t\}}, 0, \cdots, 0)$$

is an $m^2 + 2$ rounds impossible differential of m-cell $Skipjack_{SP}$.

Proof. From the encryption direction, we have

$$\Delta X_m^{m+1} = \Delta_{P\circ S\circ P\circ S}(e_{\{i_1,\cdots,i_s\}}) = P \times \Delta_S \left[\overset{s}{\underset{r=1}{\oplus}} (\Delta_S(e_{i_r}) \times P_{(i_r)}) \right]$$

$$(\Delta X_m^{m+1} = \Delta_{(S\circ P\circ S)\circ(S\circ P\circ S)}(e_{\{i_1,\cdots,i_s\}})$$
$$= \Delta_S\left(P\times\Delta_{S\circ S}\left[\overset{s}{\underset{r=1}{\oplus}}(\Delta_S(e_{i_r})\times P_{(i_r)})\right]\right), resp.).$$

Let

$$\Delta_S\left[\overset{s}{\underset{r=1}{\oplus}}(\Delta_S(e_{i_r})\times P_{(i_r)})\right]=\alpha$$

$$(\Delta_{S\circ S}\left[\overset{s}{\underset{r=1}{\oplus}}(\Delta_S(e_{i_r})\times P_{(i_r)})\right]=\alpha, resp.),$$

then

$$\chi\left(\alpha\right)=\chi\left[\overset{s}{\underset{r=1}{\oplus}}\left(P_{(i_r)}\times\Delta_S(e_{i_r})\right)\right]$$

By (2), $\chi_k\left(\alpha\right)=\theta\left[\overset{s}{\underset{r=1}{\oplus}}\left(\Delta_S(e_{i_r})\times P_{k,i_r}\right)\right]=0.$

From the decryption direction, we have

$$\Delta X_m^{m+1}=\beta=\overset{m-1}{\underset{l=1}{\oplus}}\Delta^{(l)}_{S^{-1}\circ P^{-1}}(e_{\{j_1,\cdots,j_t\}})=\overset{m-1}{\underset{l=1}{\oplus}}\Delta^{(l)}_{S^{-1}}\left[\overset{t}{\underset{r=1}{\oplus}}(e_{j_r}\times P^{-1}_{(j_r)})\right],$$

$$(\Delta X_m^{m+1}=\beta=\overset{m-1}{\underset{l=1}{\oplus}}\Delta^{(l)}_{S^{-1}\circ P^{-1}\circ S^{-1}}(e_{\{j_1,\cdots,j_t\}})$$
$$=\overset{m-1}{\underset{l=1}{\oplus}}\Delta^{(l)}_{S^{-1}}\left[\overset{t}{\underset{r=1}{\oplus}}\left(\Delta^{(l)}_{S^{-1}}\left(e_{j_r}\right)\times P^{-1}_{(j_r)}\right)\right], resp.),$$

Let

$$\gamma=\overset{t}{\underset{r=1}{\oplus}}\left(e_{j_r}\times P^{-1}_{(j_r)}\right),$$

$$(\gamma=\overset{t}{\underset{r=1}{\oplus}}\left(\Delta^{(l)}_{S^{-1}}\left(e_{j_r}\right)\times P^{-1}_{(j_r)}\right), resp.),$$

hence

$$\chi_k\left(\gamma\right)=\theta\left[\overset{t}{\underset{r=1}{\oplus}}\left(e_{j_r}\times P^{-1}_{k,j_r}\right)\right]$$

$$(\chi_k\left(\gamma\right)=\theta\left[\overset{t}{\underset{r=1}{\oplus}}\left(\Delta^{(l)}_{S^{-1}}\left(e_{j_r}\right)\times P^{-1}_{k,j_r}\right)\right], resp.).$$

Then by (3), we have $\chi_k\left(\beta\right)=\chi_k\left[\overset{m-1}{\underset{l=1}{\oplus}}\Delta_{S^{-1}}(\gamma)\right]=0.$

If $(0,\cdots,0,e_{\{i_1,\cdots,i_s\}})\rightarrow(e_{\{j_1,\cdots,j_t\}},0,\cdots,0)$ is possible, then there exists nonzero α,β satisfying

$$(P|E)\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=0,$$

$$((P|E)\begin{pmatrix}\alpha\\ \Delta_{S^{-1}}(\beta)\end{pmatrix}=0, resp)$$

which implies

$$\left(\overset{p}{\underset{k=1}{\oplus}} \alpha_{u_k} \times P_{(u_k)}\right) \oplus \left(\overset{q}{\underset{k=1}{\oplus}} \beta_{v_k} \times E_{(v_k)}\right) = 0.$$

$$(\left(\overset{p}{\underset{k=1}{\oplus}} \alpha_{u_k} \times P_{(u_k)}\right) \oplus \left(\overset{q}{\underset{k=1}{\oplus}} \left(\Delta_{S^{-1}}(\beta)\right)_{v_k} \times E_{(v_k)}\right) = 0, resp.)$$

However, from (1) we have $P_{(u_1)}, P_{(u_2)}, \cdots, P_{(u_p)}$, $E_{(v_1)}, E_{(v_2)}, \cdots, E_{(v_q)}$ are linearly independent, any nonzero α, β cannot hold this formula. Thus

$$(0, \cdots, 0, e_{\{i_1,\cdots,i_s\}}) \to (e_{\{j_1,\cdots,j_t\}}, 0, \cdots, 0)$$

is an $m^2 + 2$ rounds impossible differential.

Example 2. Given $n = 8, d = 16, m = 4$, we employ the matrix representation of the linear layer of AES[1] as the P layer(see Appendix 2.), we choose $p = q = s = t = 1$, $u_1 = 1, v_1 = 1, i_1 = 1, j_1 = 1, k = 2$, since $P_{(1)}, E_{(1)}$ are linearly independent and $P_{2,1} = P^{-1}_{2,1} = 0$, thus $(0, \cdots, 0, e_{\{1\}}) \to (e_{\{1\}}, 0, \cdots, 0)$ is a 18 rounds impossible differential of $Skipjack_{SP}$ /$Skipjack_{SPS}$

5 Conclusion

In this paper, we work on finding impossible differential distinguishers for Skipjack structure with SP/SPS round function.

Previous result indicates that the longest impossible differentials in m-cell Skipjack-like structures is m^2 rounds ($(0, \alpha, 0, \cdots, 0) \to (\beta, \beta, 0, \cdots, 0)$). In this paper, we find some new m^2 rounds impossible differentials for $Skipjack_{SP}$ /$Skipjack_{SPS}$ which are derived from the impossible differentials of the P layer. Our results show that if the P layer is designed as a binary matrix, we can always retrieve $m^2 + 1$ rounds impossible differentials for $Skipjack_{SP}$ and $Skipjack_{SPS}$, and also $m^2 + 2$ rounds impossible differentials for $Skipjack_{SP}$. Moreover, if P layer satisfies some special conditions (we can judge these conditions in real time), we may further obtain $m^2 + 2$ rounds impossible differential for $Skipjack_{SPS}$.

Since $Skipjack_{SP}$ /$Skipjack_{SPS}$ is not a real cipher, we failed in launching a key-recovery attack on it. However, our results can still be treated as a security measurement of generalized Feistel family ciphers. We believe that these longer impossible differentials constructed in our paper are caused by the sparsity of the P layer. These results indicate that when employing $Skipjack_{SP}$ or $Skipjack_{SPS}$ structure, we should choose P layer carefully.

Acknowledgment

We appreciate the anonymous referees for their valuable comments. The work in this paper is supported by: the Natural Science Foundation of China (Grant

No:61272488, 61272041, 61202491), the Foundation of Science and Technology on Information Assurance Laboratory(Grant No. KJ-13-007)

References

[Adams (1999)] Adams, C.: "The CAST-256 encryption algorithm"; (1999).

[Aoki et al. (2001)] Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: "Camellia: A 128-bit Block Cipher Suitable for Multiple Platforms." SAC 2000, Springer, Heidelberg (2001), 39-56.

[Bai et al. (2012)] Bai, D. X, and Li, L.B.: "New Impossible Differential Attacks on Camellia"; Information Security Practice and Experience, Springer, Heidelberg(2012), 80-96.

[Biham et al. (1999)] Biham, E., Biryukov, A., and Shamir, A.: "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials"; Advances in CryptologyEurocrypt99, Springer, Heidelberg(1999),12-23.

[Burwick (1998)] Burwick, C., et al.: "MARS-a candidate cipher for AES", NIST AES Proposal 268 (1998). `http://www.encryption.de/docs/Mars.pdf`

[Daemen, Rijmen (2002)] Daemen, J., Rijmen, V.: "The Design of Rijndael. AES-The Advanced Encryption Standard"; Springer, Heidelberg (2002).

[Kanda et al. (1998)] Kanda, M., Moriai, S., Aoki, K. et al. :"E2-a Candidate Cipher for AES; In Proceedings from the First Advanced Encryption Standard Candidate Conference, National Institute of Standards and Technology (NIST). (1998)

[Kim et al. (2003)] Kim, J., et al.: "Impossible Fifferential Cryptanalysis for Block Cipher Structures"; Progress in Cryptology-INDOCRYPT 2003, Springer, Heidelberg(2003), 82-96.

[Kim et al. (2010)] Kim, J., Hong, S., Lim, J.: "Impossible Differential Cryptanalysis Using Matrix Method"; Discrete Mathematics, 310, 5 (2010), 988-1002.

[Knudsen (1998)] Knudsen, L.: "DEAL-a 128-bit block cipher"; complexity 258 (1998): 2. `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.32.7982&rep=rep1&type=pdf`.

[Koo et al. (2006)] Koo, B. W., Jang, H. S., Song, J. H.: "On Constructing of a 32 × 32 Binary Matrix as a Diffusion Layer for a 256-Bit Block Cipher." Information Security and Cryptology C ICISC 2006, Springer, Heidelberg(2006), 51-64.

[Li et al. (2010)] Li, R., et al.: "Cryptanalysis of a Generalized Unbalanced Feistel Network Structure"; Information Security and Privacy, Springer, Heidelberg(2010), 1-18.

[Li et al. (2011)] Li, R. L., Sun, B., Li, C.: "Impossible Differential Cryptanalysis of SPN Ciphers"; IET Information Security, 5, 2 (2011), 111-120.

[Li et al. (2012)] Li, R. L., et al.: "Security evaluation of MISTY structure with SPN round function." Computers & Mathematics with Applications (2012).

[Liu et al. (2012)] Liu, Y., et al.: "Impossible Differential Attacks on Reduced-Round LBlock"; Information Security Practice and Experience, Springer, Heidelberg(2012), 97-108.

[Lu et al. (2008)] Lu, J., et al.: "New Impossible Differential Attacks on AES"; Progress in Cryptology-INDOCRYPT 2008, Springer, Heidelberg(2008), 279-293.

[Luo et al. (2009)] Luo, Y.Y., et al.: A Unified Method for Finding Impossible Differentials of Block Cipher Structures; Cryptology ePrint Archive: Report 2009/627. `https://eprint.iacr.org/2009/627.pdf`

[Nyberg (1996)] Nyberg, K.: "Generalized Feistel Networks"; Advances in CryptologyASIACRYPT'96, Springer Berlin (1996), 91-104.

[Pudovkina (2009)] Pudovkina, M.: On Impossible Truncated Differentials of Generalized Feistel and Skipjack Ciphers; FSE 2009 rump session(2009). `http://fse2009rump.cr.yp.to/e31bba5d1227eac5ef0daa6bcbf66f27.pdf`.

[Shirai et al. (2002)] Shirai, T., Kanamaru, S., Abe, G.: "Improved Upper Bounds of Differential and Linear Characteristic Probability for Camellia"; Fast Software Encryption, Springer, Heidelberg(2002), 128-142.
[Shirai et al. (2007)] Shirai, T. et al.: "The 128-bit Block Cipher CLEFIA"; Fast Software Encryption2007, Springer, Heidelberg(2007), 181-195.
[Standard (1999)] Standard, N. F.: "Data Encryption Standard (DES) "; Federal Information Processing Standards Publication (1999).
[Sung et al. (2000)] Sung, J., et al.: "Provable Security for the Skipjack-like Structure Against Differential Cryptanalysis and Linear Cryptanalysis"; Advances in CryptologyASIACRYPT 2000, Springer, Heidelberg(2000), 274-288.
[Wang et al. (2005)] Wang, N. P., et al.: "The Differential Provable Security Analysis of a Kind of Unbalanced Feistel Networks"; Journal of Electronics and Information Technology, 27,6 (2005), 870-873.
[Wei et al. (2010)] Wei, Y. C., et al.: "Impossible Differential Cryptanalysis on Feistel Ciphers with SP and SPS Round Functions"; Applied Cryptography and Network Security, Springer, Heidelberg(2010), 105-122.
[Wei et al. (2012)] Wei, Y. C., et al.: "Impossible Differential Cryptanalysis on Tweaked E2"; Network and System Security, Springer, Heidelberg(2012), 392-404.
[Wu and Zhang et al. (2007)] Wu, W. L., Zhang, W. T., Feng, D. G.: "Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia"; Journal of Computer Science and Technology, 22, 3 (2007), 449-456.
[Wu et al. (2009)] Wu, W. L., et al.: "Security Analysis of the GF-NLFSR Structure and Four-Cell Block Cipher"; Information and Communications Security, Springer, Heidelberg(2009), 17-31.
[Wu and Wang(2012)] Wu, S. B and Wang, M. S.: "Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers", Progress in Cryptology-INDOCRYPT 2012. Springer, Heidelberg(2012), 283-302.

Appendix

Appendix 1

. P layer and it's inversion of Example 1 (the linear layer of Camellia).

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

Appendix 2

P layer and it's inversion of Example 2 (the linear layer of AES).

$$
P = \begin{pmatrix}
2&0&0&0&1&0&0&0&1&0&0&0&3&0&0&0\\
0&1&0&0&0&1&0&0&0&3&0&0&0&2&0&0\\
0&0&1&0&0&0&3&0&0&0&2&0&0&0&1&0\\
0&0&0&3&0&0&0&2&0&0&0&1&0&0&0&1\\
3&0&0&0&2&0&0&0&1&0&0&0&1&0&0&0\\
0&2&0&0&0&1&0&0&0&1&0&0&0&3&0&0\\
0&0&1&0&0&0&1&0&0&0&3&0&0&0&2&0\\
0&0&0&1&0&0&0&3&0&0&0&2&0&0&0&1\\
1&0&0&0&3&0&0&0&2&0&0&0&1&0&0&0\\
0&3&0&0&0&2&0&0&0&1&0&0&0&1&0&0\\
0&0&2&0&0&0&1&0&0&0&1&0&0&0&3&0\\
0&0&0&1&0&0&0&1&0&0&0&3&0&0&0&2\\
1&0&0&0&1&0&0&0&3&0&0&0&2&0&0&0\\
0&1&0&0&0&3&0&0&0&2&0&0&0&1&0&0\\
0&0&3&0&0&0&2&0&0&0&1&0&0&0&1&0\\
0&0&0&2&0&0&0&1&0&0&0&1&0&0&0&3
\end{pmatrix},
$$

$$
P^{-1} = \begin{pmatrix}
e&0&0&0&9&0&0&0&d&0&0&0&b&0&0&0\\
0&b&0&0&0&e&0&0&0&9&0&0&0&d&0&0\\
0&0&d&0&0&0&b&0&0&0&e&0&0&0&9&0\\
0&0&0&9&0&0&0&d&0&0&0&b&0&0&0&e\\
b&0&0&0&e&0&0&0&9&0&0&0&d&0&0&0\\
0&d&0&0&0&b&0&0&0&e&0&0&0&9&0&0\\
0&0&9&0&0&0&d&0&0&0&b&0&0&0&e&0\\
0&0&0&e&0&0&0&9&0&0&0&d&0&0&0&b\\
d&0&0&0&b&0&0&0&e&0&0&0&9&0&0&0\\
0&9&0&0&0&d&0&0&0&b&0&0&0&e&0&0\\
0&0&e&0&0&0&9&0&0&0&d&0&0&0&b&0\\
0&0&0&b&0&0&0&e&0&0&0&9&0&0&0&d\\
9&0&0&0&d&0&0&0&b&0&0&0&e&0&0&0\\
0&e&0&0&0&9&0&0&0&d&0&0&0&b&0&0\\
0&0&b&0&0&0&e&0&0&0&9&0&0&0&d&0\\
0&0&0&d&0&0&0&b&0&0&0&e&0&0&0&9
\end{pmatrix}
$$