Impossible Differential Cryptanalysis on Lai-Massey Scheme

Rui Guo and Chenhui Jin

The Lai-Massey scheme, proposed by Vaudenay, is a modified structure in the International Data Encryption Algorithm cipher. A family of block ciphers, named FOX, were built on the Lai-Massey scheme. Impossible differential cryptanalysis is a powerful technique used to recover the secret key of block ciphers. This paper studies the impossible differential cryptanalysis of the Lai-Massey scheme with affine orthomorphism for the first time. Firstly, we prove that there always exist 4-round impossible differentials of a Lai-Massey cipher having a bijective F-function. Such 4-round impossible differentials can be used to help find 4-round impossible differentials of FOX64 and FOX128. Moreover, we give some sufficient conditions to characterize the existence of 5- , 6- , and 7-round impossible differentials of Lai-Massey ciphers having a substitution-permutation (SP) F-function, and we observe that if Lai-Massey ciphers having an SP F-function use the same diffusion layer and orthomorphism as a FOX64, then there are indeed 5- and 6-round impossible differentials. These results indicate that both the diffusion layer and orthomorphism should be chosen carefully so as to make the Lai-Massey cipher secure against impossible differential cryptanalysis.

Keywords: Lai-Massey scheme, FOX cipher, impossible differentials analysis.

I. Introduction

1. Background

Nowadays, the most powerful known attacks on block ciphers are differential cryptanalysis [1] and linear cryptanalysis [2]. These attacks have been efficiently applied to many known ciphers. Therefore, many block cipher structures with a provable security against differential cryptanalysis and linear cryptanalysis have been studied [3]–[8]. However, a provable security against differential cryptanalysis and linear cryptanalysis is not enough to prove the security of block ciphers, because other different cryptanalyses may be applied in the future. For instance, the 3-round Feistel structure, whose round functions are bijective, has a provable security against differential cryptanalysis and linear cryptanalysis [9], but there exists a 5-round impossible differential characteristic, which means that impossible differential cryptanalysis [10] may be much more powerful than differential cryptanalysis and linear cryptanalysis. Thus, it is necessary to evaluate the ability of each block cipher to resist also impossible differential cryptanalysis.

Impossible differential cryptanalysis, proposed by Biham and Knudsen, is one of the most popular cryptanalytic tools for use against block ciphers. The main idea behind impossible differential cryptanalysis is to use an impossible differential that shows that a particular differential characteristic can not occur for the correct key, which means that if these differential characteristics are satisfied under the tested key, then it cannot be the correct one. Moreover, impossible differential cryptanalysis has shown its superiority over differential cryptanalysis in many block ciphers, such as International Data Encryption Algorithm (IDEA) [11], Skipjack [12], AES [13],

Manuscript received Dec. 24, 2013; revised May 18, 2014; accepted July 23, 2014.

This work was supported by the National Natural Science Foundation of China (No. 61272488).

Rui Guo (corresponding author, guorui201@sohu.com) and Chenhui Jin (jinchenhui @126.com) are with the Department of Information Security, the School of Information Science and Technology Institute, Zhengzhou, China.

http://dx.doi.org/10.4218/etrij.14.0113.1335

FOX family [14], and so on.

Obtaining the longest impossible differential is the key step of impossible differential cryptanalysis, and several methods have made use of the miss-in-the-middle method to do just that. Another method used to obtain the longest impossible differential is the u-method [15] proposed by Kim and others. Although the u-method can be used, in general, to find impossible differentials of various block ciphers, information relating to block ciphers is often lost in the process and hence some longer impossible differentials cannot be found by this method. Luo and others extended the idea of the u-method and proposed a more general method; namely, the UID-method [16]. The UID-method removes some limitations of the u-method and harnesses more inconsistent conditions to evaluate impossible differentials. Wu and others [17] introduced a novel tool to search impossible differentials for word-oriented block ciphers with bijective S-boxes. This tool generalizes both the u-method and the UID-method. However, those methods are so general that some information is often lost during calculating the impossible differentials. Hence, once again, some longer impossible differentials cannot be found by using those methods.

In this paper, we mainly focus on impossible differential cryptanalysis of the Lai-Massey cipher (The block ciphers are defined by iterating the Lai-Massey scheme [18]) with affine orthomorphism. The Lai-Massey scheme was originally derived from the IDEA [19] cipher. In 2004, instancing the Lai-Massey scheme's F-function with an SPS structure and orthomorphism [20] as $or(x,y)=(y,x\oplus y)$, Junod and Vaudenay designed the FOX [21] family of block ciphers, also named "IDEA NXT." Thus far, existing analysis results indicate that the FOX family of ciphers is secure enough from such attacks as differential cryptanalysis [14]–[22], integral attacks [23], fault attacks [24], and so on [21]. Moreover, Yun and others introduced the notion of a quasi-Feistel network [25], which is a generalization of the Feistel network and contains the Lai-Massey scheme as an instance. They proved that the Lai-Massey scheme and Feistel structure have the same pseudorandom properties [26] and decorrelation property [27]; however, they didn't precisely present the ability of the Lai-Massey cipher to resist linear and differential cryptanalysis; integral attacks; statistical attacks; slide and related-key attacks; and so on. This paper firstly evaluates the Lai-Massey cipher's ability to resist impossible differential cryptanalysis. By carefully analyzing the properties of the linear transformations, we found that the existence of impossible differentials in a Lai-Massey cipher is not only related to the diffusion layer of the F-function but also strongly related to the orthomorphism. Compared with the Feistel cipher [28], our results indicate that Lai-Massey cipher is much more powerful to resist impossible differential cryptanalysis.

2. Contribution and Outline

The contribution of this paper presents the original evaluation on the impossible differentials of Lai-Massey ciphers for the first time. Firstly, we prove that 4-round impossible differential always exist if the F-function is bijective. Secondly, we give some sufficient conditions to characterize the existence of 5-, 6-, and 7-round impossible differentials of Lai-Massey ciphers having a substitution-permutation (SP) F-function and observe that if the Lai-Massey ciphers having an SP F-function use the same diffusion layer and orthomorphism as a FOX64, then there are indeed 5- and 6-round impossible differentials.

This paper is organized as follows. In Section II, we will describe the Lai-Massey scheme along with some preliminaries. The existence of the impossible differentials of the Lai-Massey cipher having either an SP or an SPS F-function will be discussed in Section III. Section IV concludes this paper.

II. Preliminaries

1. Lai-Massey Scheme

Definition 1 [18]. Let $(G, +)$ be a group. If $\sigma : G \to G$ and $x \to \sigma(x) - x$ are both permutations, then σ is an orthomorphism on G.

Definition 2 [18]. Let $(G, +)$ be a group. Given r F-functions, $f_1, \ldots, f_r$, and an orthomorphism on G, σ; we can define an r-round Lai-Massey cipher that is a permutation on G^2 and that is denoted as

$$\begin{aligned}&\mathrm{LM}\ (f_1, \ldots, f_r)(x_0, y_0)\\ &\quad = \mathrm{LM}\ [f_2, \ldots, f_r][\sigma(x_0 + f_1(x_0 - y_0)), y_0 + f_1(x_0 - y_0)].\end{aligned}$$

Its round functions are defined as

$$(x_{i+1}, y_{i+1}) = (\sigma(x_i + f_i(x_i - y_i)),\ y_i + f_i(x_i - y_i)),$$

where $(x_{i+1}, y_{i+1}) \in G \times G$ denotes the output of the ith round of the Lai-Massey cipher.

In this paper, let group $G = \{0, 1\}^n$. We define the group operation + as the bit-wise exclusive OR ⊕. Then, the round function can be rewritten as

$$(x_{i+1}, y_{i+1}) = (\sigma[x_i \oplus f_i(x_i \oplus y_i]),\ y_i \oplus f_i(x_i \oplus y_i)).$$

In particular, to ensure the similarity of encryption and decryption of the Lai-Massey cipher, the σ in the last round is always omitted.

2. Description of FOX

FOX is a family of block ciphers designed by Junod and Vaudenay in 2004, which is the result of a joint project with the company MediaCrypt AG in Switzerland. FOX adopts a modified structure of the Lai-Massey Scheme, which can be proven to have sound pseudorandom properties in the Luby-Rackoff paradigm, as well as having decorrelation in hesitance properties. FOX has two versions, both have a variable number of rounds, the exact number of which being dependent upon key sizes. The first one, FOX64/*k*/*r*, has a 64-bit block size with a variable key length — a multiple of 8 and up to 256 bits. The second, FOX128/*k*/*r*, uses a 128-bit block size with variable key length and round number. The original FOX design suggests these two ciphers should be iterated for 16 rounds. The round function of FOX uses a substitution-permutation-substitution (SPS) structure with three layers of sub-key addition. The key schedule of FOX is very complex as it uses the round function as a compress function to generate sub-keys from the master key. Here, we give only a brief description of the F-function, *f*, of FOX64, for further details we refer you to [21].

The round function, *f*, comprises three main parts: a substitution part, denoted *sigma*4; a diffusion part, denoted *mu*4; and a round key addition part. Let f: $\{0, 1\}^{32} \times \{0, 1\}^{64} \rightarrow \{0, 1\}^{32}$, for a 32-bit input $x \in \{0, 1\}^{32}$ and a 64-bit round key $k = k_0 || k_1$, we have

$$f(x, k) = sigma4(mu4(sigma4(x \oplus k_0)) \oplus k_1) \oplus k_0.$$

The substitution transformation *sigma*4: $\{0, 1\}^{32} \rightarrow \{0, 1\}^{32}$ comprises four parallel applications of a nonlinear bijective S-box for different input bytes. The linear permutation transformation *mu*4: $[GF(256)]^4 \rightarrow [GF(256)]^4$ considers an input (x_0, x_1, x_2, x_3) as a column vector $(x_0, x_1, x_2, x_3)^T$ over $[GF(256)]^4$ and multiplies it with a maximum distance separable (MDS) matrix to output a column vector of the same size. The branch number of the MDS matrix is five. The MDS matrix is defined as follows:

$$\begin{pmatrix} 1 & 1 & Z & \alpha \\ 1 & Z & \alpha & 1 \\ Z & \alpha & 1 & 1 \\ \alpha & 1 & Z & 1 \end{pmatrix},$$

where $Z = \alpha^{-1} \oplus 1$ and α is a root of the irreducible polynomial $m(x) = x^8 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^4 \oplus x^3 \oplus 1$ over *GF*(2).

Moreover, the σ transformation used in FOX64 is the linear orthomorphism $or(a, b) = (b, a \oplus b)$, which satisfies the following properties.

Property 1 [21]. The orthomorphsim $or(x, y) = (y, x \oplus y)$ and its inverse transformation $io(x, y) = (x \oplus y, x)$ have the following properties:

- $or^2(x, y) = io(x, y),\ \ io^2(x, y) = or(x, y).$
- $io(x, y) \oplus or(x, y) \oplus (x, y) = (0, 0).$
- $or(x, y) = (x, y)$ if and only if $(x, y) = (0, 0).$
- $or^3(x, y) = (x, y)$.

3. Notation and Definitions

Throughout this paper, we use the following notations:

- *GF*(*q*) denotes a Galois field with *q* elements.
- #*T* denotes a cardinal number of the set *T*.
- $f \circ g$ or *fg* denotes a composite function of *f* and *g*.
- $A_{i,j}$ denotes the element in the *i*th row and *j*th column of matrix *A*.
- $\Delta f(\Delta X)$ denotes the output difference of the input difference, ΔX, for the F-function *f*.
- $\Delta S(\Delta X)$ denotes the output difference of the input difference ΔX for the nonlinear transform layer *S*.

In this section, we give the definition and properties of the χ-function and then give the definition of the Hamming weight.

Definition 3 (χ-function). For $m \geq 1$, let δ: $GF(2^m) \rightarrow GF(2)$, $\chi: (GF(2^m))^n \rightarrow (GF(2))^n$, and $\chi_i: (GF(2^m))^n \rightarrow GF(2)$, for $1 \leq i \leq n$, then define

$$\delta(x) = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \neq 0, \end{cases}$$

$$\chi(x_1, \ldots, x_n) = \delta(x_1), \ldots, \delta(x_n),$$

and

$$\chi_i(x_1, \ldots, x_n) = \delta(x_i).$$

Therefore, for $X \in (GF(2^m))^n$, $\chi_i(X) = 1$ means that there is some non-zero value at the *i*th position. Let $e_i \in (GF(2^m))^n$ be a vector such that $\chi_i(e_i) = E_i$, where $E_i \in (GF(2))^n$ is a vector whose *i*th component is one, while other [$e_j = 0$ ($j \neq i$)] components are zero. The χ-function adheres to the following properties outlined in Property 2:

Property 2 [28].

A. For any difference $\Delta X \in (GF(2^m))^n$, we have $\chi(\Delta S(\Delta X)) = \chi(\Delta X).$

B. Let $P = (p_1, \ldots, p_n)$, where p_i is the *i*th column vector of diffusion layer *P*, then if $\Delta X = e_i$, we have

$$\chi(P \circ \Delta S(e_i)) = \chi(P(e_i)) = \chi(p_i).$$

C. Let $X = (x_1, \ldots, x_n)$, $Y = (y_1, \ldots, y_n)$, $1 \leq i \leq n.$ if $x_i = 0$, then $\chi_i(X \oplus Y) = \chi_i(Y) = \delta(y_i)$.

Definition 4 [28]. Let $X = (x_1, \ldots, x_n) \in (GF(2^m))^n$, then define the number of nonzero components in X by $w(X) = \#\{i \mid x_i \neq 0, 1 \le i \le n\}$.

In this paper, we only consider the Lai-Massey scheme with affine orthomorphism $\sigma : \{0, 1\}^n \rightarrow \{0, 1\}^n$, let $\tau = \sigma \oplus I$ (I denotes the identical transformation), then $\sigma\tau = \tau\sigma$, and we can list the properties of σ and τ as follows:

Property 3.

(1) $(\sigma^2 \oplus I)\tau^{-1} = \tau$; (2) $(\tau^2 \oplus I)\sigma^{-1} = \sigma$;

(3) $(\sigma^{-1} \oplus I)\tau^{-1}\sigma = I$; (4) $\sigma^2 \oplus \sigma \oplus I \oplus \tau^2 = \sigma$.

Proof. We only prove (3); the proof of the others is a trivial exercise. Due to the fact that σ^{-1} is also an affine orthomorphism [20] and $\tau = \sigma \oplus I$, we have $(\sigma^{-1} \oplus I)\tau^{-1}\sigma = \sigma^{-1}(\sigma \oplus I)\tau^{-1}\sigma = I$. ■

III. Impossible Differentials Analysis of the Iterative Lai-Massey Scheme

By comprehensively analyzing the properties of the diffusion layer and the σ transformation on the Lai-Massey ciphers, some sufficient conditions will be presented that characterize the existence of 4-round impossible differentials of a Lai-Massey cipher having a bijective F-function and that characterize the existence of 5-, 6-, and 7-round impossible differentials of a Lai-Massey cipher having an SP F-function. Let Δ_i (i = 1, 2, … , r) denote the input difference of the ith round. Using the miss-in-the-middle technique, we try to find the impossible differential of a Lai-Massey cipher and obtain several results as follows.

1. Analysis on 4-Round Lai-Massey Cipher Having a Bijective F-function

Proposition 1. Let the F-function of a Lai-Massey cipher be bijective, then $(\tau^{-1}(\alpha), \tau^{-1}(\alpha)) \nrightarrow (\sigma^2(\alpha), \sigma(\alpha))$ is a 4-round impossible differential of the cipher, where $\alpha \neq 0$.

Proof. As described in Fig. 1, from the encryption direction, if $\Delta_1 = (\tau^{-1}(\alpha), \tau^{-1}(\alpha))$, then $\Delta_2 = (\sigma\tau^{-1}(\alpha), \tau^{-1}(\alpha))$ and $\Delta_3 = (\sigma^2\tau^{-1}(\alpha) \oplus \sigma(\beta), \tau^{-1}(\alpha) \oplus \beta)$, where $\sigma\tau^{-1}(\alpha) \oplus \tau^{-1}(\alpha) = \alpha$ and $\beta = \Delta f_2(\alpha)$ are the input difference and output difference of f_2, respectively. Moreover, due to the fact that the F-function is bijective and α is nonzero, we have $\beta \neq 0$. By Property 3, we know that

$$\begin{aligned} &\sigma^2\tau^{-1}(\alpha) \oplus \sigma(\beta) \oplus \tau^{-1}(\alpha) \oplus \beta \\ &= (\sigma^2 \oplus I)\tau^{-1}(\alpha) \oplus \tau(\beta) \\ &= \tau(\alpha) \oplus \tau(\beta), \end{aligned}$$

which is the input difference of the third F-function, f_3.

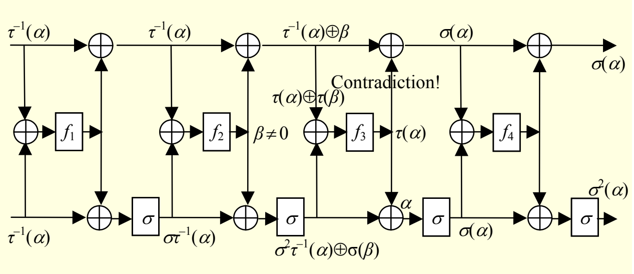


Fig. 1. Impossible differential of 4-round Lai-Massey cipher having a bijective round function.

From the decryption direction, if the output difference of the fourth round is $(\sigma^2(\alpha), \sigma(\alpha))$, then $\Delta_4 = (\sigma(\alpha), \sigma(\alpha))$, and the input difference of f_3 is $\alpha \oplus \sigma(\alpha) = \tau(\alpha)$. Therefore, by $\beta \neq 0$, $\tau(\alpha) \oplus \tau(\beta) = \tau(\alpha)$ is a contradiction. Hence, $(\tau^{-1}(\alpha), \tau^{-1}(\alpha)) \nrightarrow (\sigma^2(\alpha), \sigma(\alpha))$ is a 4-round impossible differential. ■

From Proposition 1, we can obtain a new kind of impossible differential of a 4-round FOX cipher as the following corollary.

Corollary 1. Let $or(x, y) = (y, x \oplus y)$, then we have the following:

- If $\alpha \in \{0, 1\}^{32} \setminus \{0\}$, then $(\alpha, \alpha) \nrightarrow (or(\alpha), \alpha)$ is a 4-round impossible differential of FOX64.
- If $\alpha \in \{0, 1\}^{32} \setminus \{0\}$ and $\beta \in \{0, 1\}^{32}$, then $(\alpha, \alpha, \beta, \beta) \nrightarrow (or(\alpha), \alpha, or(\beta), \beta)$ is a 4-round impossible differential of FOX128.

In [14], Wu proved that $(0a0a, 0a0a) \nrightarrow (bcbd, bcbd)$ is a 4-round impossible differential of FOX64, where each a, b, c, and d denote one byte, and $a \neq 0$. In addition, they presented a chosen plaintexts impossible differential cryptanalysis of the FOX64. In Corollary 1, the only requirement is that $\alpha \neq 0$, which implies that perhaps we can present a distinct known plaintexts attack on FOX, which is a more realistic model. Moreover, for a Feistel scheme, if the F-function is bijective, then it will have a 5-round impossible differential. In Proposition 1, we know that the Lai-Massey scheme only has a 4-round impossible differential if the F-function is bijective.

2. Analysis on 5-Round Lai-Massey Cipher Having an SP Round Function

From now on, let σ_M and τ_M denote the corresponding matrix of the linear transformation σ and τ, respectively.

Proposition 2. Let $\phi = P^{-1}\sigma^{-1}P$, $\varphi = P^{-1}(\tau \oplus \sigma^{-1})$, for $1 \le I \le n$. If there exists $1 \le j \neq i \le n$ such that $\chi_j(\tau(e_i)) = 0$ and either $\chi_j(\phi(e_i)) = 0$, $\chi_j(\varphi(e_i)) = 1$ or $\chi_j(\phi(e_i)) = 1$, $\chi_j(\varphi(e_i)) = 0$, then $(e_i, e_i) \nrightarrow (\tau^{-1}\sigma^2(e_i), \tau^{-1}\sigma(e_i))$ is a 5-round impossible differential of the Lai-Massey cipher having an SP structure.

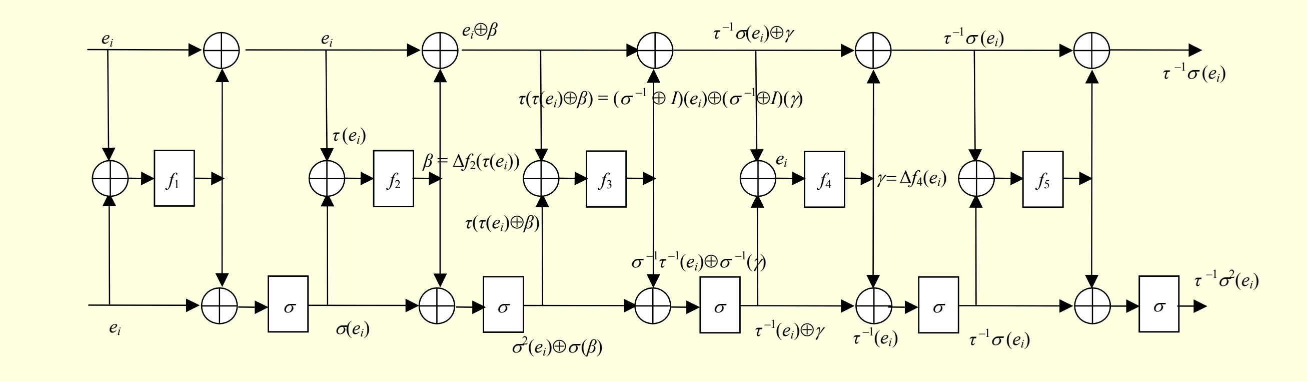

e_i
e_i
$e_i\oplus\beta$
$\tau^{-1}\sigma(e_i)\oplus\gamma$
$\tau^{-1}\sigma(e_i)$
$\tau^{-1}\sigma(e_i)$
$\tau(\tau(e_i)\oplus\beta)=(\sigma^{-1}\oplus I)(e_i)\oplus(\sigma^{-1}\oplus I)(\gamma)$
$\tau(e_i)$
f_1
f_2
$\beta=\Delta f_2(\tau(e_i))$
f_3
e_i
f_4
$\gamma=\Delta f_4(e_i)$
f_5
$\tau(\tau(e_i)\oplus\beta)$
$\sigma^{-1}\tau^{-1}(e_i)\oplus\sigma^{-1}(\gamma)$
$\tau^{-1}\sigma^2(e_i)$
e_i
σ
$\sigma(e_i)$
σ
$\sigma^2(e_i)\oplus\sigma(\beta)$
σ
$\tau^{-1}(e_i)\oplus\gamma$
$\tau^{-1}(e_i)$
σ
$\tau^{-1}\sigma(e_i)$
σ

Fig. 2. Impossible differential of 5-round Lai-Massey cipher having an SP round function.

Proof. As described in Fig. 2, if the input difference is (e_i, e_i), then the input difference of f_2 will be $\sigma(e_i)\oplus e_i=\tau(e_i)$. Let $\beta=P\Delta S(\tau(e_i))$ denote the output difference of f_2, then $\Delta_3=(\sigma^2(e_i)\oplus\sigma(\beta),\ e_i\oplus\beta)$, and the input difference of f_3 is

$$\sigma^2(e_i)\oplus\sigma(\beta)\oplus e_i\oplus\beta=\tau(\tau(e_i)\oplus\beta).$$

Then, $\Delta_5=(\tau^{-1}\sigma(e_i),\ \tau^{-1}\sigma(e_i))$, and the input difference of f_4 is $\tau^{-1}(e_i)\oplus\tau^{-1}\sigma(e_i)=\tau^{-1}(\sigma\oplus I)(e_i)=e_i$. Let $\gamma=P\Delta S(e_i)$ denote the output difference of f_4, then $\Delta_4=(\tau^{-1}(e_i)\oplus\gamma,\ \tau^{-1}\sigma(e_i)\oplus\gamma)$, from which we know that the input difference of f_3 is

$$\begin{aligned}&\sigma^{-1}\tau^{-1}(e_i)\oplus\sigma^{-1}(\gamma)\oplus\tau^{-1}\sigma(e_i)\oplus\gamma\\&=(\sigma^{-1}\oplus I)(e_i)\oplus(\sigma^{-1}\oplus I)(\gamma).\end{aligned}$$

Thus, the following equation holds:

$$\tau(\tau(e_i)\oplus\beta)=(\sigma^{-1}\oplus I)(e_i)\oplus(\sigma^{-1}\oplus I)(\gamma);\text{ namely,}$$

$$\tau P\Delta S(\tau(e_i))=(\sigma^{-1}\oplus I)P\Delta S(e_i)\oplus(\tau^2\oplus\sigma^{-1}\oplus I)(e_i),$$

which implies that $\Delta S(\tau(e_i))=\phi\Delta S(e_i)\oplus\varphi(e_i)$,

where $\varphi=P^{-1}\tau^{-1}(\tau^2\oplus\sigma^{-1}\oplus I)=P^{-1}(\tau\oplus\sigma^{-1})$ and $\phi=P^{-1}\tau^{-1}(\sigma^{-1}\oplus I)P=P^{-1}\sigma^{-1}P$. Moreover, we have $\chi(\Delta S(\tau(e_i)))=\chi(\phi\Delta S(e_i)\oplus\varphi(e_i))$.

From Property 2, we know $\chi(\Delta S(\tau(e_i)))=\chi(\tau(e_i))$. If there exists $1\le j\ne i\le n$ such that either $\chi_j(\phi(e_i))=0$, $\chi_j(\varphi(e_i))=1$ or $\chi_j(\phi(e_i))=1$, $\chi_j(\varphi(e_i))=0$, then we have $\chi_j(\phi\Delta S(e_i)\oplus\varphi(e_i))=1$. Meanwhile, if $\chi_{j\ne i}(\tau(e_i))=0$, then this is a contradiction. Thus, $(e_i,\ e_i)\nrightarrow(\tau^{-1}\sigma^2(e_i),\ \tau^{-1}\sigma(e_i))$ is a 5-round impossible differential. ■

The following example implies that if the Lai-Massey ciphers having an SP structure use the same σ function and diffusion layer P as FOX64, then they will have a 5-round impossible differential.

Example 1. By the definition and property of the orthomorphism *or* in FOX64, we have

$$or_M=\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&1&0\\0&1&0&1\end{pmatrix},\qquad io_M=\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix},$$

$$P=\begin{pmatrix}1&1&1&\alpha\\1&Z&\alpha&1\\Z&\alpha&1&1\\\alpha&1&Z&1\end{pmatrix},\qquad P^{-1}=\begin{pmatrix}a&c&d&e\\a&d&e&c\\a&e&c&d\\b&a&a&a\end{pmatrix},$$

where $Z=\alpha^{-1}\oplus 1$, and a, b, c, and d are four distinct nonzero elements in $GF(2^8)$.

From Proposition 2, here $\phi=P^{-1}or_M(io_M\oplus I)P=P^{-1}io_MP$, $\varphi=P^{-1}or_M(or_M\oplus io_M\oplus I)=0$, and

$$P^{-1}io_MP=\begin{pmatrix}a&c&d&e\\a&d&e&c\\a&e&c&d\\b&a&a&a\end{pmatrix}\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}\begin{pmatrix}1&1&1&\alpha\\1&Z&\alpha&1\\Z&\alpha&1&1\\\alpha&1&Z&1\end{pmatrix}$$

$$=\begin{pmatrix}a&c&d&e\\a&d&e&c\\a&e&c&d\\b&a&a&a\end{pmatrix}\begin{pmatrix}1\oplus Z&1\oplus\alpha&0&1\oplus\alpha\\1\oplus\alpha&1\oplus Z&Z\oplus\alpha&0\\1&1&1&\alpha\\1&Z&\alpha&1\end{pmatrix}$$

$$=\begin{pmatrix}*&*&*&*\\*&*&*&*\\*&*&*&*\\*&*&a(1\oplus Z)&*\end{pmatrix}.$$

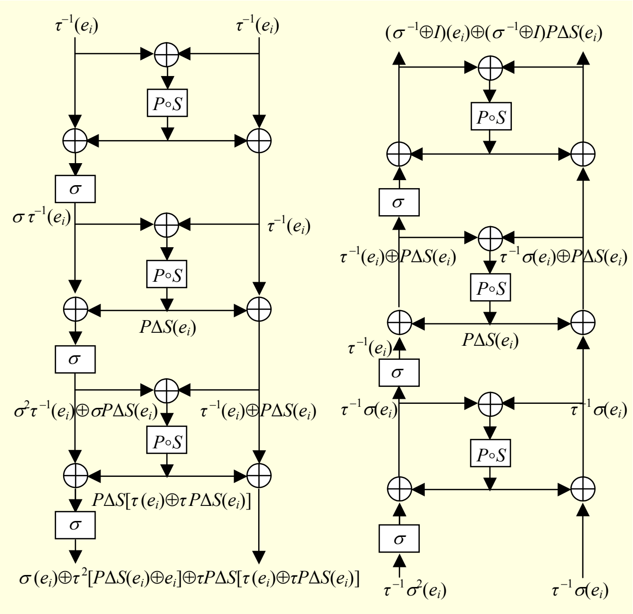
So, $\chi_4(\tau(e_3))=0$, $\chi_4(\phi(e_3))=a(1\oplus Z)\ne 0$, and $\chi_4(\varphi(e_3))=0$. Thus, $(e_3,\ e_3)\nrightarrow(e_3,\ io(e_3))$ is a 5-round impossible differential.

3. Analysis on 6-Round Lai-Massey Scheme Having an SP Round Function

Proposition 3. For $1\le i\le n$, let

$$\begin{aligned}\Omega_i=\{k\mid&[(\tau_M)_{k,i}=0,\ (\tau_M\circ P)_{k,i}\ne 0]\\&\vee[(\tau_M)_{k,i}\ne 0,\ (\tau_M\circ P)_{k,i}=0]\},\end{aligned}$$

$$\Lambda_i=\{k\mid\phi_{k,i}=0\},\quad\Gamma_i=\{k\mid\varphi_{k,i}\ne 0\},\quad n_1=\#(\Omega_i\cap\Lambda_i),$$



$\tau^{-1}(e_i)$
$\tau^{-1}(e_i)$
$P\circ S$
σ
$\sigma\tau^{-1}(e_i)$
$\tau^{-1}(e_i)$
$P\circ S$
$P\Delta S(e_i)$
σ
$\sigma^2\tau^{-1}(e_i)\oplus\sigma P\Delta S(e_i)$
$\tau^{-1}(e_i)\oplus P\Delta S(e_i)$
$P\circ S$
$P\Delta S[\tau(e_i)\oplus\tau P\Delta S(e_i)]$
σ
$\sigma(e_i)\oplus\tau^2[P\Delta S(e_i)\oplus e_i]\oplus\tau P\Delta S[\tau(e_i)\oplus\tau P\Delta S(e_i)]$
$(\sigma^{-1}\oplus I)(e_i)\oplus(\sigma^{-1}\oplus I)P\Delta S(e_i)$
$P\circ S$
σ
$\tau^{-1}(e_i)\oplus P\Delta S(e_i)$
$\tau^{-1}\sigma(e_i)\oplus P\Delta S(e_i)$
$P\circ S$
$P\Delta S(e_i)$
$\tau^{-1}(e_i)$
σ
$\tau^{-1}\sigma(e_i)$
$\tau^{-1}\sigma(e_i)$
$P\circ S$
σ
$\tau^{-1}\sigma^2(e_i)$
$\tau^{-1}\sigma(e_i)$

Fig. 3. Impossible differential of 6-round Lai-Massey cipher having an SP round function.

and $n_2 = \#\Gamma_i$, where $\phi = P^{-1}(\tau_M^{-1}\sigma_M^{-1} \oplus \sigma_M)$ and $\varphi = P^{-1}(\sigma_M^{-1} \oplus \tau_M)P$. If $n_1 > n_2$, then $(\tau^{-1}(e_i), \tau^{-1}(e_i)) \not\rightarrow (\sigma^2(e_i), \sigma(e_i))$ is a 6-round impossible differential of a Lai-Massey cipher having an SP structure.

Proof. As described in Fig. 3 and similar to Proposition 2, when $\Delta_1 = (\tau^{-1}(e_i), \tau^{-1}(e_i))$, we conclude that the input difference of f_4 is

$$\begin{aligned}&\sigma^3\tau^{-1}(e_i) \oplus \sigma^2 P\Delta S(e_i) \oplus \sigma P\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)]\\ &\oplus P\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)] \oplus \tau^{-1}(e_i) \oplus P\Delta S(e_i)\\ &\quad = \sigma(e_i) \oplus \tau^2[P\Delta S(e_i) \oplus e_i]\\ &\qquad \oplus \tau P\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)].\end{aligned}$$

From the decryption direction, if the output difference of the sixth round is $(\sigma^2(e_i), \sigma(e_i))$, then $\Delta_6 = (\tau^{-1}(e_i) \oplus P\Delta S(e_i), \tau^{-1}\sigma(e_i) \oplus P\Delta S(e_i))$. Therefore, the input difference of f_4 is

$$\begin{aligned}&\sigma^{-2}\tau^{-1}\sigma(e_i) \oplus \sigma^{-1}P\Delta S(e_i) \oplus \tau^{-1}\sigma(e_i) \oplus P\Delta S(e_i)\\ &\quad = (\sigma^{-2} \oplus I)\tau^{-1}\sigma(e_i) \oplus (\sigma^{-1} \oplus I)P\Delta S(e_i)\\ &\quad = (\sigma^{-1} \oplus I)(e_i) \oplus (\sigma^{-1} \oplus I)P\Delta S(e_i).\end{aligned}$$

Thus, the following equation holds:

$$\begin{aligned}&\sigma(e_i) \oplus \tau^2[P\Delta S(e_i) \oplus e_i] \oplus \tau P\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)]\\ &\quad = (\sigma^{-1} \oplus I)(e_i) \oplus (\sigma^{-1} \oplus I)P\Delta S(e_i).\end{aligned}$$

Accordingly,

$$\begin{aligned}&\tau P\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)]\\ &\quad = (\sigma^{-1} \oplus I \oplus \sigma \oplus \tau^2)(e_i) \oplus (\sigma^{-1} \oplus I \oplus \tau^2)P\Delta S(e_i).\end{aligned}$$

Thus, we obtain

$$\begin{aligned}&\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)] \oplus P^{-1}(\tau^{-1}\sigma^{-1} \oplus \sigma)(e_i)\\ &\quad = P^{-1}(\sigma^{-1} \oplus \tau)P\Delta S(e_i).\end{aligned}$$

For $1 \le i \le n$ and a linear transformation P, let

$$\begin{aligned}\Omega_i = \{k \mid &[(\tau_M)_{k,i} = 0,\ (\tau_M \circ P)_{k,i} \ne 0]\\ &\vee [(\tau_M)_{k,i} \ne 0,\ (\tau_M \circ P)_{k,i} = 0]\},\end{aligned}$$

$$\Lambda_i = \{k \mid \phi_{k,i} = 0\},\quad \Gamma_i = \{k \mid \varphi_{k,i} \ne 0\},\ n_1 = \#(\Omega_i \cap \Lambda_i),$$

$$n_2 = \#\Gamma_i,\quad \phi = P^{-1}(\tau_M^{-1}\sigma_M^{-1} \oplus \sigma_M),$$

and

$$\varphi = P^{-1}(\sigma_M^{-1} \oplus \tau_M)P.$$

Assume that there exist $k_1, \ldots, k_{n_1} \in \Omega_i \cap \Lambda_i$. Since $k_1, \ldots, k_{n_1} \in \Lambda_i$, for any $k_j (1 \le j \le n_1)$, we have $\chi_{k_j}(P^{-1}(\tau^{-1}\sigma^{-1} \oplus \sigma)(e_i)) = \chi_{k_j}(\phi(e_i)) = 0$, by Property 2-A, then

$$\begin{aligned}&\chi_{k_j}(\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)] \oplus P^{-1}(\tau^{-1}\sigma^{-1} \oplus \sigma)(e_i))\\ &\quad = \chi_{k_j}(\Delta S(\tau(e_i) \oplus \tau P\Delta S(e_i)))\\ &\quad = \chi_{k_j}(\tau(e_i) \oplus \tau P\Delta S(e_i)).\end{aligned}$$

Moreover, due to $k_1, \ldots, k_{n_1} \in \Omega_i$, for any $k_j (1 \le j \le n_1)$, there are

$$\begin{aligned}&\chi_{k_j}(\tau(e_i) \oplus \tau P\Delta S(e_i))\\ &= \begin{cases}\chi_{k_j}((\tau_M)_{k_j,i}(e_i)) = 1 & \text{if } (\tau_M)_{k_j,i} \ne 0 \text{ and } (\tau \circ P)_{k_j,i} = 0,\\ \chi_{k_j}((\tau_M \circ P)_{k_j,i}\Delta S(e_i)) = 1 & \text{if } (\tau_M \circ P)_{k_j,i} \ne 0 \text{ and } \tau_{k_j,i} = 0.\end{cases}\end{aligned}$$

For $1 \le j \le n_1$, we have $\chi_{k_j}(\tau(e_i) \oplus \tau P\Delta S(e_i)) = 1$, which means that $w(\chi(\tau(e_i) \oplus \tau P\Delta S(e_i))) \ge n_1$, so

$$w(\chi(\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)] \oplus P^{-1}(\tau^{-1}\sigma^{-1} \oplus \sigma)(e_i))) \ge n_1.$$

On the other hand, assume that there exist some $k_1, \ldots, k_{n_2} \in \Gamma_i$, by Property 2-B, then

$$\begin{aligned}&w(\chi(P^{-1}(\sigma^{-1} \oplus \tau)P\Delta S(e_i)))\\ &\quad = w(\chi(P^{-1}(\sigma^{-1} \oplus \tau)P(e_i)))\\ &\quad = w(P^{-1}(\sigma^{-1} \oplus \tau)P(e_i))\\ &\quad = n_2.\end{aligned}$$

Hence, if $n_1 > n_2$, then $(\tau^{-1}(e_i), \tau^{-1}(e_i)) \not\rightarrow (\sigma^2(e_i), \sigma(e_i))$ is a 6-round impossible differential. ■

The following example implies that if the Lai-Massey ciphers having an SP structure use the same σ function and diffusion layer as FOX64, then they will have 6-round impossible differentials.

Example 2. Similar to Example 1, by the definition and property of the orthomorphism *or* in FOX64, we have

$\phi = P^{-1}(io_M^{-1}or_M^{-1} \oplus io_M) = P^{-1}or_M$ and $\varphi = P^{-1}(or_M^{-1} \oplus io_M)P = 0$; hence, $n_2 = 0$. Moreover, we have

$$io_M P = \begin{pmatrix} 1\oplus Z & 1\oplus\alpha & 0 & 1\oplus\alpha \\ 1\oplus\alpha & 1\oplus Z & Z\oplus\alpha & 0 \\ 1 & 1 & 1 & \alpha \\ 1 & Z & \alpha & \underline{1} \end{pmatrix}$$

and $$P^{-1}or_M = \begin{pmatrix} d & e & a\oplus d & c\oplus e \\ e & c & a\oplus e & c\oplus d \\ c & d & a\oplus c & d\oplus e \\ a & a & a\oplus b & \underline{0} \end{pmatrix}.$$

We have $(io_M)_{4,4} = 0$, $(io_M P)_{4,4} = 1$, and $\phi_{4,4} = (P^{-1}or_M)_{4,4} = 0$, which implies that $n_1 \geq 1$. Thus, $(or(e_4), or(e_4)) \nrightarrow (io(e_4), or(e_4))$ is a 6-round impossible differential.

4. Analysis on 7-Round Lai-Massey Scheme Having an SP Round Function

Proposition 4. For $1 \leq i, j, k \leq n$, let $\Omega_i = \{k \mid (\sigma_M^{-1}\tau_M)_{k,i} = 0;\ (\sigma_M^{-1}\tau_M P)_{k,i} = 0\}$, $A = P^{-1}\tau_M^{-1}\sigma_M(\sigma_M^{-2} \oplus \sigma_M^{-1} \oplus \sigma_M \oplus \sigma_M^2)$, and $B = P^{-1}\tau_M^{-1}\sigma_M(\sigma_M^{-2} \oplus I \oplus \sigma_M^2)P$. If $\Omega_i \neq \emptyset$ and there exist any $k \in \Omega_i$ such that $\{a_{k,i}, b_{k,i}\} = \{0, 0\}$ and $\chi_k(P^{-1}\sigma P\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)]) = 1$, then $(\tau^{-1}(e_i), \tau^{-1}(e_i)) \nrightarrow (\sigma^2(e_i), \sigma(e_i))$ is a 7-round impossible differential of the Lai-Massey cipher having an SP structure, where $A = (a_{i,j})_{n\times n}$, $B = (b_{i,j})_{n\times n}$, and a_i and b_i denote the ith column vectors of A and B, respectively.

Proof. As described in Fig. 4, from the encryption direction, if $\Delta_1 = (\tau^{-1}(e_i), \tau^{-1}(e_i))$, then the input difference of f_3 is

$$\begin{aligned} &\sigma^2\tau^{-1}(e_i) \oplus \sigma(P\Delta S(e_i)) \oplus \tau^{-1}(e_i) \oplus P\Delta S(e_i) \\ &= \tau(e_i \oplus P\Delta S(e_i)). \end{aligned}$$

Let $\lambda = P\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)]$ denote the output difference of f_3. Accordingly, the input difference of f_4 is

$$\begin{aligned} &\sigma^3\tau^{-1}(e_i) \oplus \sigma^2 P\Delta S(e_i) \oplus \sigma\lambda \oplus \lambda \oplus \tau^{-1}(e_i) \oplus P\Delta S(e_i) \\ &= \sigma(e_i) \oplus \tau^2[P\Delta S(e_i) \oplus e_i] \oplus \tau\lambda. \end{aligned}$$

From the decryption direction, if the output difference of the seventh round is $(\sigma^2(e_i), \sigma(e_i))$, then $\Delta_6 = (\tau^{-1}(e_i) \oplus P\Delta S(e_i), \tau^{-1}\sigma(e_i) \oplus P\Delta S(e_i))$. We denote the output difference of f_5 as $\beta = P\Delta S[\sigma^{-1}\tau(e_i \oplus P\Delta S(e_i))]$. From Property 3, the input difference of f_4 is

$$\begin{aligned} &\sigma^{-1}[\sigma^{-1}\tau^{-1}(e_i) \oplus \sigma^{-1}P\Delta S(e_i) \oplus \beta] \oplus \beta \oplus \tau^{-1}\sigma(e_i) \oplus P\Delta S(e_i) \\ &= (\sigma^{-2}\tau^{-1} \oplus \tau^{-1}\sigma)(e_i) \oplus (\sigma^{-2} \oplus I)P\Delta S(e_i) \oplus (\sigma^{-1} \oplus I)\beta \\ &= [\sigma^{-2} \oplus \sigma^{-1} \oplus I](e_i) \oplus (\sigma^{-2} \oplus I)P\Delta S(e_i) \oplus (\sigma^{-1} \oplus I)\beta. \end{aligned}$$

Thus, the following equation holds:

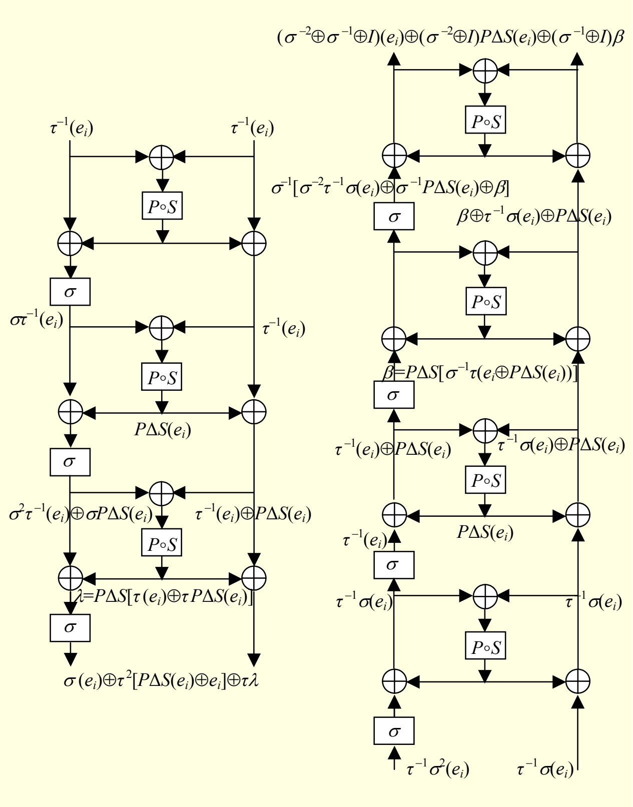

$(\sigma^{-2}\oplus\sigma^{-1}\oplus I)(e_i)\oplus(\sigma^{-2}\oplus I)P\Delta S(e_i)\oplus(\sigma^{-1}\oplus I)\beta$
$\tau^{-1}(e_i)$
$\tau^{-1}(e_i)$
$P\circ S$
σ
$\sigma\tau^{-1}(e_i)$
$\tau^{-1}(e_i)$
$P\Delta S(e_i)$
$\sigma^2\tau^{-1}(e_i)\oplus\sigma P\Delta S(e_i)$
$\tau^{-1}(e_i)\oplus P\Delta S(e_i)$
$\lambda=P\Delta S[\tau(e_i)\oplus\tau P\Delta S(e_i)]$
$\sigma(e_i)\oplus\tau^2[P\Delta S(e_i)\oplus e_i]\oplus\tau\lambda$
$\sigma^{-1}[\sigma^{-2}\tau^{-1}\sigma(e_i)\oplus\sigma^{-1}P\Delta S(e_i)\oplus\beta]$
$\beta\oplus\tau^{-1}\sigma(e_i)\oplus P\Delta S(e_i)$
$\beta=P\Delta S[\sigma^{-1}\tau(e_i\oplus P\Delta S(e_i))]$
$\tau^{-1}(e_i)\oplus P\Delta S(e_i)$
$\tau^{-1}\sigma(e_i)\oplus P\Delta S(e_i)$
$P\Delta S(e_i)$
$\tau^{-1}(e_i)$
$\tau^{-1}\sigma(e_i)$
$\tau^{-1}\sigma(e_i)$
$\tau^{-1}\sigma^2(e_i)$
$\tau^{-1}\sigma(e_i)$

Fig. 4. Impossible differential of 7-round Lai-Massey cipher having an SP round function.

$$\begin{aligned} &\sigma(e_i) \oplus \tau^2[P\Delta S(e_i) \oplus e_i] \oplus \tau\lambda \\ &= (\sigma^{-2} \oplus \sigma^{-1} \oplus I)(e_i) \oplus (\sigma^{-2} \oplus I)P\Delta S(e_i) \oplus (\sigma^{-1} \oplus I)\beta, \end{aligned}$$

which means that

$$\begin{aligned} &\tau\lambda \oplus (\sigma^{-1} \oplus I)\beta \\ &= (\sigma^{-2} \oplus \sigma^{-1} \oplus I \oplus \sigma \oplus \tau^2)(e_i) \oplus (\sigma^{-2} \oplus I \oplus \sigma^2)P\Delta S(e_i) \\ &= (\sigma^{-2} \oplus \sigma^{-1} \oplus \sigma \oplus \sigma^2)(e_i) \oplus (\sigma^{-2} \oplus I \oplus \sigma^2)P\Delta S(e_i) \end{aligned}$$

and

$$\begin{aligned} &\tau P\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)] \oplus \sigma^{-1}\tau P\Delta S[\sigma^{-1}\tau(e_i \oplus P\Delta S(e_i))] \\ &= (\sigma^{-2} \oplus \sigma^{-1} \oplus \sigma \oplus \sigma^2)(e_i) \oplus (\sigma^{-2} \oplus I \oplus \sigma^2)P\Delta S(e_i). \end{aligned}$$

For $1 \leq i, j, k \leq n$ and linear transformation P, let

$$\Omega_i = \{k \mid (\sigma_M^{-1}\tau_M)_{k,i} = 0;\ (\sigma_M^{-1}\tau_M P)_{k,i} = 0\},$$
$$A = P^{-1}\tau_M^{-1}\sigma_M(\sigma_M^{-2} \oplus \sigma_M^{-1} \oplus \sigma_M \oplus \sigma_M^2),$$

and $B = P^{-1}\tau_M^{-1}\sigma_M(\sigma_M^{-2} \oplus I \oplus \sigma_M^2)P$. If $\Omega_i \neq \emptyset$ and there exist any $k \in \Omega_i$ such that $\{a_{k,i}, b_{k,i}\} = \{0, 0\}$, then we have

$$\begin{aligned} &\chi_k(\Delta S[\sigma^{-1}\tau(e_i \oplus P\Delta S(e_i))]) \\ &= \chi_k(A(e_i) \oplus B\Delta S(e_i) \oplus P^{-1}\sigma P\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)]) \\ &= \chi_k(P^{-1}\sigma P\Delta S[\tau(e_i) \oplus \tau P\Delta S(e_i)]). \end{aligned}$$

Here,

$$\begin{aligned}&\chi_k(\Delta S[\sigma^{-1}\tau(e_i \oplus P\Delta S(e_i))])\\&\quad=\chi_k(\sigma^{-1}\tau(e_i \oplus P\Delta S(e_i)))\\&\quad=0,\end{aligned}$$

which contradicts $\chi_k(P^{-1}\sigma P\Delta S[\tau(e_i)\oplus \tau P\Delta S(e_i)])=1$. Therefore, the above proposition holds. ■

Toy Example. Let the σ function be an *or* transformation used in FOX64 and choose a diffusion layer P as follows:

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

Here, $or_M^{-2}\oplus or_M^{-1}\oplus or_M \oplus or_M^{2}=(or_M^{-2}\oplus I\oplus or_M^{2})=0$; thus, $A=B=0$. Moreover, we have

$$io_M P=\begin{pmatrix}0&1&1&1\\1&1&1&0\\0&1&0&1\\\underline{1}&1&0&1\end{pmatrix},\quad or_M P=\begin{pmatrix}\underline{0}&0&1&0\\0&0&1&1\\0&1&1&1\\1&1&1&0\end{pmatrix},$$

and

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

We have $(or_M)_{1,1}=0$, $(or_M P)_{1,1}=0$, and $\{a_{1,1}, b_{1,1}\}=\{0, 0\}$. Moreover, $(io_M)_{4,1}=0$, $(io_M P)_{4,1}=1$, $(P^{-1}orP)_{1,4}=1$, $(P^{-1}orP)_{1,1}=0$, $(P^{-1}orP)_{1,2}=0$, and $(P^{-1}orP)_{1,3}=0$, from which $\chi_1(P^{-1}orP\Delta S[io(e_1)\oplus ioP\Delta S(e_1)])=1$. Thus, $(or(e_1), or(e_1))\not\rightarrow(io(e_1), or(e_1))$ is a 7-round impossible differential of this special Lai-Massey cipher having an SP structure.

IV. Conclusion

In this paper, we presented an impossible differential cryptanalysis on Lai-Massey ciphers. By comprehensively analyzing the properties of the diffusion layer and the σ function on the Lai-Massey ciphers, we gave some sufficient conditions that characterized the existence of 4-round impossible differentials of Lai-Massey cipher having a bijective F-function and 5-, 6-, 7-round impossible differentials of Lai-Massey ciphers having an SP F-function. These results indicate that both the diffusion layer and the σ function should be chosen carefully so as to make the Lai-Massey cipher secure against impossible differential cryptanalysis, and the propositions presented in this paper should be considered when designing a block cipher. Moreover, the problem of how to suitably design the diffusion layer and σ function of a Lai-Massey scheme so as to resist cryptanalyses is still an open one.

References

[1] E. Biham and A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” *Advances in Cryptology - CRYPTO’90*, *LNCS* 537, Berlin, Germany: Springer-Verlag, 1991, pp. 2–21.

[2] M. Matsui, “Linear Cryptanalysis Method for DES Cipher,” *Advances in Cryptology - EUROCRYPT’93*, *LNCS* 765, Berlin, Germany: Springer-Verlag, 1994, pp. 386–397.

[3] K. Nyberg and L.R. Knudsen, “Provable Security against Differential Cryptanalysis,” *Advances in Cryptology - CRYPTO’92*, *LNCS* 740, Berlin, Germany: Springer-Verlag, 1993, pp. 566–574.

[4] S. Hong et al., *Provable Security against Differential and Linear Cryptanalysis for the SPN Structure*, *FSE’00*, *LNCS* 1978, Berlin, Germany: Springer-Verlag, 2001, pp. 273–283.

[5] S. Hong et al., “Provable Security for 13 Round Skipjack-like Structure,” *Inf. Proc. Lett.*, vol. 82, no. 5, 2002, pp. 243–246.

[6] M. Matsui, *New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis*, *FSE’96*, *LNCS* 1039, Berlin, Germany: Springer-Verlag, 1996, pp. 205–218.

[7] K. Nyberg, “Generalized Feistel Networks,” *Advances in Cryptology - ASIACRYPT’96*, *LNCS* 1163, Berlin, Germany: Springer-Verlag, 1996, pp. 91–104.

[8] J. Sung et al., “Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis,” *Advances in Cryptology - ASIACRYPT’00*, *LNCS* 1976, Berlin, Germany: Springer-Verlag, 2000, pp. 274–288.

[9] K. Aoki and K. Ohta, “Strict Evaluation of the Maximum Average of Differential Probability and the Maximum Average of Linear Probability,” *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, no. 1, 1997, pp. 2–8.

[10] L.R. Knudsen, “DEAL-A 128-bit Block Cipher,” Department Infometrics, University of Bergen, Norway, Technical Report 151, 1998.

[11] E. Biham, A. Biryukov, and A. Shamir, *Miss-in-the-Middle Attacks on IDEA, Khufu, and Khafre*, *Knudsen, FSE’99*. *LNCS* 1636, Berlin, Germany: Springer-Verlag, 1999, pp. 124–138.

[12] E. Biham, A. Biryukov, and A. Shamir, “Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials,” *EUROCRYPT’99*. *LNCS* 1592, Berlin, Germany: Springer-Verlag, 1999, pp. 12–23.

[13] J. Daemen and V. Rijmen, *The Design of Rijndael: AES, Advanced Encryption Standard*, New York, USA: Springer-Verlag, 2002.

[14] Z. Wu et al., “Impossible Differential Cryptanalysis of FOX,” *Proc. Int. Conf., LNCS 6163*, Beijing, China, 2009, pp. 236–249.

[15] J. Kim et al., “Impossible Differential Cryptanalysis for Block Cipher Structures,” *INDOCRYPT* 2003, *LNCS* 2904, Berlin, Germany: Springer-Verlag, 2003, pp. 82–96.

http://dx.doi.org/10.4218/etrij.14.0113.1335

[16] Y. Luo et al., “A Unified Method for Finding Impossible Differentials of Block Cipher Structures,” *Inf. Sci.*, vol. 263, Apr. 1, 2014, pp. 211–220.

[17] S. Wu and M. Wang. “Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers,” *INDOCRYPT* 2012, *LNCS* 7668, Berlin, Germany: Springer-Verlag, 2012, pp. 283–302.

[18] S. Vaudenay, “On the Lai-Massey Scheme,” *Advances in Cryptology-ASIACRYPT’*99, *LNCS* 1716, Berlin, Germany: Springer-Verlag, 1999, pp. 8–19.

[19] X. Lai and J.L. Massey, “A Proposal for a New Block Encryption Standard,” *Advances in Cryptology EUROCRYPT’*90*, LNCS* 473, Berlin, Germany: Springer-Verlag, 1991, pp. 389–404.

[20] L. Mittenthal, “Block Substitutions Using Orthomorphic Mappings,” *Adv. Appl. Math*., vol. 16, no. 1, Mar. 1995, pp. 59–71.

[21] P. Junod and S. Vaudenay, *FOX: A New Family of Block Ciphers*, *Selected Areas in Cryptography-SAC* 2004*, LNCS* 2595, Berlin, Germany: Springer-Verlag, 2004, pp. 131–146.

[22] J. Chen et al., “Differential Collision Attack on Reduced FOX Block Cipher,” *China Commun*., vol. 9, no. 7, 2012, pp. 71–76.

[23] W. Wu, W. Zhang, and D. Feng, “Integral Cryptanalysis of Reduced FOX Block Cipher,” *Information Security and Cryptology*, *LNCS* 3935, Berlin, Germany: Springer-Verlag, 2006, pp. 229–241.

[24] R. Li et al., “Fault Analysis Study of the Block Cipher FOX64,” *Multimedia Tools and Applications*, vol. 63, no. 3, Apr. 2013, pp. 691–708.

[25] A. Yun, J.H. Park, and J. Lee, “On Lai-Massey and Quasi-Feistel Ciphers,” *Design Codes Cryptography*, vol. 58, 2011, pp. 45–72.

[26] M. Luby and C. Rackoff, “How to Construct Pseudorandom Permutations from Pseudorandom Functions,” *SIAM J. Comput*., vol. 17, no. 2, 1988, pp. 373–386.

[27] S. Vaudenay, “Provable Security for Block Ciphers by Decorrelation,” *Proc. Annual Symp. Theoretical Aspects. Comput. Sci*., Paris, France, 1998, pp. 249–275.

[28] Y. Wei et al., “Impossible Differential Cryptanalysis on Feistel Ciphers with SP and SPS Round Functions,” in *Appl. Cryptography Netw. Security*, Berlin, Germany: Springer-Verlag, 2010, pp. 105–122.

Rui Guo received his PhD degree in cryptography from the Information Science and Technology Institute, Zhengzhou, China, in 2014. His research interests include the design and analysis of block ciphers. His works have been published in several journals and cryptology conferences.

Chenhui Jin is a professor at the Information Science and Technology Institute, Zhengzhou, China. His research interests include cryptology and information security.