Pseudorandomness Analysis of the Lai-Massey Scheme

Yiyuan Luo[1], Xuejia Lai[1], Zheng Gong[2] and Zhongming Wu[1]

[1] Department of Computer Science and Engineering, Shanghai Jiaotong University, China. luoyiyuan@sjtu.edu.cn
[2] Faculty of EEMCS University of Twente. z.gong@utwente.nl

Abstract. At Asiacrypt'99, Vaudenay modified the structure in the IDEA cipher to a new scheme, which they called as the Lai-Massey scheme. It is proved that 3-round Lai-Massey scheme is sufficient for pseudorandomness and 4-round Lai-Massey scheme is sufficient for strong pseudorandomness. But the author didn't point out whether three rounds and four rounds are necessary for the pseudorandomness and strong pseudorandomness of the Lai-Massey Scheme. In this paper we find a two-round pseudorandomness distinguisher and a three-round strong pseudorandomness distinguisher, thus prove that three rounds is necessary for the pseudorandomness and four rounds is necessary for the strong pseudorandomness.

1 Introduction

The notion of *pseudorandom permutation* was formally discussed by Luby and Rackoff [6], which referred to the functions that cannot be distinguished from a uniformly random permutation in polynomial time bound. Pseudorandom permutations are often used to describe the idealized abstractions of block ciphers, which play an important role in symmetric key cryptography. Well-designed block ciphers, such as DES and AES, are often assumed to be a pseudorandom permutation in the literature. Furthermore, one can explicitly modeling the underlying blockcipher as a pseudorandom permutation to enable the formal analysis of a blockcipher-based construction. The construction could be an encryption scheme (e.g., DES, IDEA[4], FOX[3]), a message authentication code (e.g., CBC-MAC) and so on.

The security of pseudorandom permutations can be classified as pseudorandomness and strong pseudorandomness. The pseudorandom permutations can be interpreted as block ciphers that are secure against an adaptive chosen-plaintext attack. That is to say, the adversary can only access the encryption oracle during the attack. The strong pseudorandom permutations can be interpreted as block ciphers that are secure against an adaptive chosen-ciphertext attack. A strong pseudorandom permutation should be indistinguishable from a uniformly random permutation, even if the distinguisher is given oracle accesses to both the encryption and decryption oracles during the attack.

Motivated by the Feistel network, Luby and Rackoff [6] provided a generic construction for strong pseudorandom permutations. They proved that 3-round Feistel network can be used to construct a pseudorandom permutation from a pseudorandom function, and 4-round Feistel network can construct a strong pseudorandom permutation from a pseudorandom function. Later many works focus on alternative structures that also have the pseudorandomness and the strong pseudorandomness properties[7, 9–13].

At Asiacrypt'99, Vaudenay [14] provided the other method to construct (strong) pseudorandom permutations. Since this new method uses a structure which is similar to the block cipher IDEA [4, 5], so it is called *the Lai-Massey scheme*. Moreover, a new family of block ciphers, which is named the *FOX* (also known as *IDEA-NXT*) [3], was built on the Lai-Massey scheme. It is proved that 3-round Lai-Massey scheme is sufficient to construct a pseudorandom permutation from a pseudorandom function, and 4-round Lai-Massey scheme is sufficient to construct a strong pseudorandom permutation from a pseudorandom function. But it is unknown that whether 3 rounds and 4 rounds are necessary for the pseudorandomness and strong pseudorandomness property of the Lai-Massey scheme .

Our Contribution. In this work, we first present two concrete attacks on the 2-round pseudorandomness and 3-round strong pseudorandomness of Lai-Massey scheme, respectively. Combined our new distinguishable attacks with Vaudenay's theorems , we formally prove that 3 rounds is not only sufficient, but also necessary for the pseudorandomness of the Lai-Massey scheme, while 4 rounds is not only sufficient, but also necessary for the strong pseudorandomness of the Lai-Massey scheme.

Organization. The remainder of this paper is organized as follows. In Section 2 we describe the formal definitions of (strong) pseudorandom permutations and two methods to construct them, including the Feistel structure and the Lai-Massey scheme. We reanalyze the pseudorandomness of the Lai-Massey scheme in Section 3, and the strong pseudorandomness in Section 4. Finally we draw a conclusion in Section 5.

2 Preliminaries

In this section, at first the formal definition of the pseudorandom and strong pseudorandom permutations are reviewed, then two methods of construct pseudorandom and strong pseudorandom permutations from pseudorandom functions, which are the Feistel network and Lai-Massey scheme are described.

2.1 Pseudorandom and Strong Pseudorandom Permutatoions

Definition 1. *Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be an efficient, keyed permutation. We say F is a pseudorandom permutation if for all probabilistic polynomial-time distinguishers D, there exists a negligible function $\epsilon(n)$ such that:*

$$|Pr[D^{F_k}(1^n) = 1] - Pr[D^P(1^n) = 1]| \leq \epsilon(n)$$

where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and P is chosen uniformly at random from the set of permutations mapping n-bit strings to n-bit strings.

In fact, a pseudorandom permutation is also a length-preserving pseudorandom function, since a length-preserving random function f looks identical to a random permutation unless a distinct pair of values x and y are found for which $f(x) = f(y)$, where in such a case the function cannot be a permutation. However, the probability of finding such points x, y using a polynomial number of queries is negligible due to the birthday bound.

If F is an efficient pseudorandom permutation then cryptographic schemes based on F might require honest parties to compute the inverse F_k^{-1} in addition to the permutation F_k itself. This potentially introduces new security concerns that are not covered by the fact that F is pseudorandom. In such a case, we may need to impose the stronger requirement that F_k be indistinguishable from a random permutation even if the distinguisher is given oracle access to the inverse of the permutation. If F has this property, we call it a strong pseudorandom permutation. Formally:

Definition 2. *Let $F : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ be an efficient, keyed permutation. We say F is a strong pseudorandom permutation if for all probabilistic polynomial-time distinguishers D, there exists a negligible function $\epsilon(n)$ such that:*

$$|Pr[D^{F_k, F_k^{-1}}(1^n) = 1] - Pr[D^{P, P^{-1}}(1^n) = 1]| \leq \epsilon(n)$$

where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and P is chosen uniformly at random from the set of permutations mapping n-bit strings to n-bit strings.

2.2 The Feistel and the Lai-Massey Schemes

The Feistel network is the most popular structure which many modern symmetric block ciphers are based on, such as DES, Blowfish, Twofish, RC5 etc. Luby and Rackoff analyzed the Feistel network and proved that if the round function is a pseudorandom function, then 3 rounds is sufficient to make the block cipher a pseudorandom permutation, while 4 rounds is sufficient to make it a strong pseudorandom permutation. A Feistel network operates in a series of rounds. The input to the ith round is a string of length $2n$ which is divided into two n-bit halves L_{i-1} and R_{i-1}. The output of the ith round will be the $2n$-bit string (L_i, R_i) where

$$L_i = R_{i-1} \quad \text{and} \quad R_i = L_{i-1} \oplus F_i(R_{i-1})$$

for some efficiently-computable(but not necessarily invertible) round function F_i mapping n-bit inputs to n-bit outputs. At last the left half and the right half of the last round outputs are swaped. Here we denote LR_r as r-round $2n$-bit Feistel network, where $F_i, 1 \leq i \leq r$ are independent uniform distribution random functions from $\{0,1\}^n$ to $\{0,1\}^n$. The 3-round Feistel network LR_3 is described in Fig. 1. The following result is proved[2]:

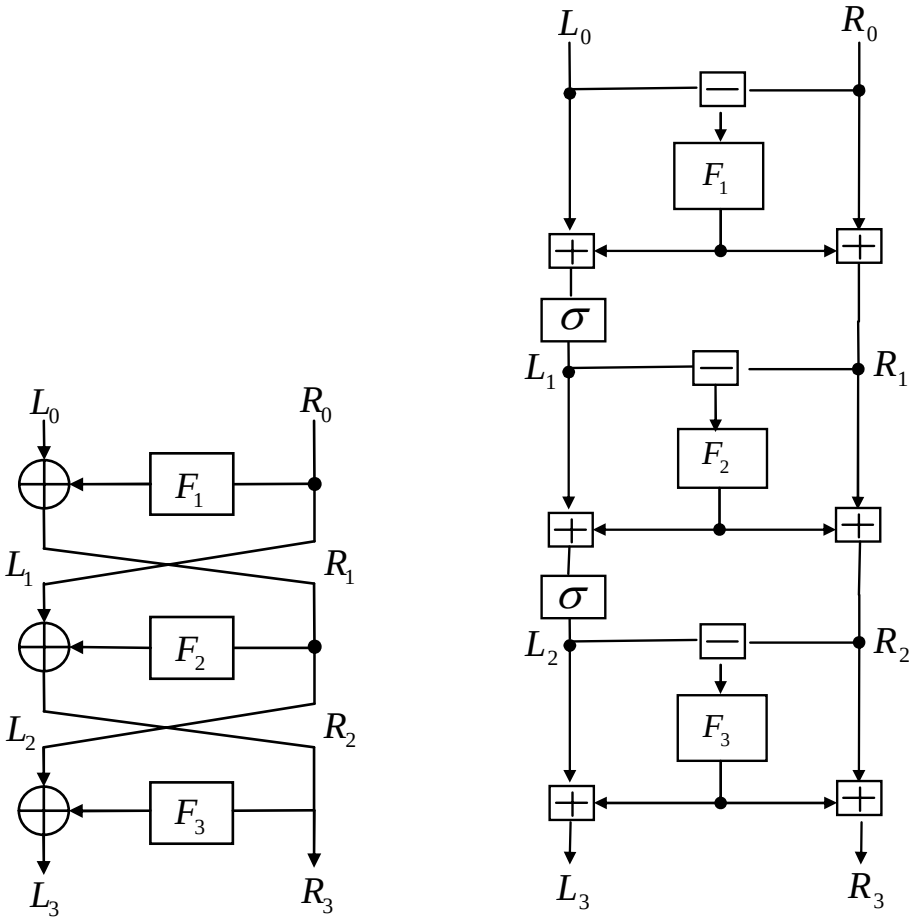

Fig. 1. The 3-round Feistel Structure LR_3 and 3-round Lai-Massey Scheme LM_3.

Theorem 1. *If F_1, F_2, F_3 are independent psuedorandom functions from $\{0,1\}^n$ to $\{0,1\}^n$, then LR_3 is a pseudorandom permutation that maps $2n$-bit strings to $2n$-bit strings.*

LR_3 is not strongly pseudorandom, this will be explained later. Fortunately, adding a fourth round does yield a strong pseudorandom permutation[2, 6].

Theorem 2. *If F_1, F_2, F_3, F_4 are independent psuedorandom functions from $\{0,1\}^n$ to $\{0,1\}^n$, then LR_4 is a strong pseudorandom permutation that maps $2n$-bit strings to $2n$-bit strings.*

The Lai-Massey scheme show in Fig.1 is a modification of the block cipher IDEA. Let $(G, +)$ be a group. Given r functions $F_1, \ldots, F_r$ and an orthomorphism[1] permutation σ on G. r-round Lai-Massey scheme LM_r which is a permutation

on G^2 is defined as follows. The input to the ith round is (L_{i-1}, R_{i-1}) where $L_{i-1}, R_{i-1} \in G$. The output of the ith round is (L_i, R_i), such that

$$L_i = \sigma(L_{i-1} + F_i(L_{i-1} - R_{i-1}))$$
$$R_i = R_{i-1} + F_i(L_{i-1} - R_{i-1})$$

where the σ permutation is omitted in the last round. The 3-round Lai-Massey scheme is described in Fig.1.

In [14] the following theorem was stated:

Theorem 3. *Let F_1, F_2, F_3 be three independent pseudorandom functions from $\{0,1\}^{2n}$ to $\{0,1\}^{2n}$, Let σ be an orthomorphism on $\{0,1\}^{2n}$. For any distinguisher D limited to q encryption or decryption oracle queries between the three-round Lai-Massey permutation LM_3 built from F_1, F_2, F_3 and a random permutation P with a uniform distribution, the advantage of D is*

$$|Pr[D^{LM_3} = 1] - Pr[D^P = 1]| \leq q(q-1)(2^{-2n} + 2^{-4n}).$$

3 Pseudorandomness of The Lai-Massey Scheme

In[14], the pseudorandomness of Lai-Massey permutation is independent of arbitrary group G and the orthomorphism σ, so it is enough to find a distinguisher for a special group and orthomorphism.

It is easy to exploit that 2-round Lai-Massey scheme can not be pseudorandom from the following case which is defined in block cipher FOX [3]. Assume that group $(G, +)$ is $(\{0,1\}^{2n}, \oplus)$. Let the orthomorphism σ be $\sigma(x, y) = (y, x \oplus y)$ where $x, y \in (\{0,1\}^{2n}, \oplus)$. Let $\oplus$ denote the bitwise exclusive or operation(xor). A distinguisher can distinguish LM_2 from a uniformly random permutation P with an overwhelming probability, which is described as follows.

Distinguisher D can access to the oracle $\mathcal{O}$ where $\mathcal{O}$ is LM_2 or P.

1. D selects a message m_1 where $|m_1| = 4n$ and $m_1 = (A_1, A_2, A_3, A_4)$(this is shown in Fig.2), then he makes the query m_1 to $\mathcal{O}$, and receives $c_1 = (C_1, C_2, C_3, C_4)$.
2. D queries m_2 where $|m_2| = 4n$ and $m_2 = (A_1 \oplus \delta_1, A_2 \oplus \delta_2, A_3 \oplus \delta_1, A_4 \oplus \delta_2)$ to $\mathcal{O}$, and receives $c_2 = (C_1', C_2', C_3', C_4')$.
3. If $C_1' \oplus C_3' = C_1 \oplus C_3 \oplus \delta_1 \oplus \delta_2$ and $C_2' \oplus C_4' = C_2 \oplus C_4 \oplus \delta_1$, outputs 1, otherwise outputs 0.

If D outputs 1, then $\mathcal{O}$ is LM_2, otherwise is P. The advantage of D is

$$Adv(D) = |Pr[D^{LM_2} = 1] - Pr[D^P = 1]| = 1 - \frac{1}{2^{2n}}.$$

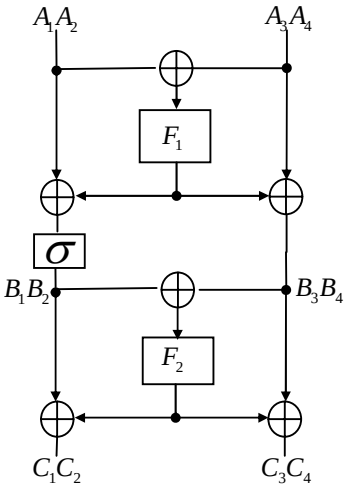

Fig. 2. Two-round FOX-style Lai-Massey Scheme. $\sigma(x, y) = (y, x \oplus y)$, $\oplus$ means the bitwise exclusive or operation(xor).

Thus we get the following corollary.

Corollary 1 *The r-round Lai-Massey scheme LM_r is pseudorandom if and only if $r \geq 3$.*

4 Strong Pseudorandomness of The Lai-Massey Scheme

If a permutation P has the strong pseudorandomness property, then it is indistinguishable from a random permutation even if the distinguisher is given oracle access to the inverses of the permutation. This security notation is reasonable since there exist chose plaintext and chosen ciphertext attackers in practice. Of course, any strong pseudorandom permutation is also a pseudorandom permutation. Vaudenay proved that four rounds Lai-Massey scheme is sufficient for strong pseudorandomness. In [14], the following theorem has been stated.

Theorem 4. *Let F_1, F_2, F_3, F_4 be four independent pseudorandom functions from $\{0,1\}^{2n}$ to $\{0,1\}^{2n}$, Let σ be an orthomorphism on $\{0,1\}^{2n}$. For any distinguisher D limited to q encryption or decryption oracle queries between the four-round Lai-Massey permutation LM_4 built from F_1, F_2, F_3, F_4 and a random permutation P with a uniform distribution, the advantage of D is*

$$|Pr[D^{LM_4, LM_4^{-1}} = 1] - Pr[D^{P,P^{-1}} = 1]| \leq q(q-1)(2^{-2n} + 2^{-4n}).$$

[1] An orthomorphism σ on a group $(G, +)$ is a permutation $x \to \sigma(x)$ on G such that $x \to \sigma(x) - x$ is also a permutation.

This theorem shows that a 4-round random Lai-Massey scheme with an orthomorphism is sufficient as a strong pseudorandom permutation when it is used less than 2^n times. Is 3 rounds also enough to implement the strong pseudorandomness property? In the next part we will show the answer is no. We find a distinguisher that can distinguish the 3-round random Lai-Massey permutation from a random permutation with an overwhelming probability. Our analysis is similar to the analysis of Feistel schemes. In Luby and Rackoff's well known paper[6], they proved that 3-round and 4-round Feistel permutation is sufficient to implement pseudorandomness and strong pseudorandomness. Later many people realize that 3-round Feistel is not strong pseudorandomness, this question is even left as an exercise in [2]. In [9], Moriai and Vaudenay find a 3-round distinguisher which needs 2 encryption queries and 2 decryption queries. In fact, there exist a distinguisher only needs 2 encryption queries and 1 decryption queries. In the following, we first describe how to distinguish 3-round Feistel Schemes with 3 oracle queries. Based on this method, we find a 3-round Lai-Massey distinguisher, which prove that 4-round is sufficient and necessary for the strong pseudorandomness of Lai-Massey scheme.

4.1 Three-Round Distinguishers of the Feistel Scheme

In Luby and Rackoff's origin work, 3-round Feistel permutation was sufficient for pseudorandomness, and they presented the 2-round pseudorandomness distinguisher. But they didn't give the 3-round strong pseudorandomness distinguisher. Later Patarin gave a distinguisher for the strong pseudorandomness with 3 rounds[11] which involved four oracle queries. Patarin's distinguisher is described as follows:

Patarin's distinguisher with four oracle queries.

Distinguisher D can access to oracles $(\mathcal{O}, \mathcal{O}^{-1})$ where $(\mathcal{O}, \mathcal{O}^{-1})$ is (LR_3, LR_3^{-1}) or (P, P^{-1}).

1. D selects a message m_1 where $|m_1| = 2n$ and $m_1 = (a, b)$, then he makes the query m_1 to $\mathcal{O}$, and receives $c_1 = (x, y)$.
2. D queries m_2 where $|m_2| = 2n$ and $m_2 = (a \oplus \delta, b)$ to $\mathcal{O}$, and receives $c_2 = (x', y')$.
3. D queries $(x \oplus \delta, y)$ to $\mathcal{O}^{-1}$ and receives $m_1' = (a_1', b_1')$.
4. D queries $(x' \oplus \delta, y')$ to $\mathcal{O}^{-1}$ and receives $m_2' = (a_2', b_2')$.
5. If $b_1' = b_2'$ outputs 1, otherwise outputs 0.

If D outputs 1, then $(\mathcal{O}, \mathcal{O}^{-1})$ is (LR_3, LR_3^{-1}), otherwise is (P, P^{-1}). The advantage of D is

$$Adv(D) = |Pr[D^{LR_3, LR_3^{-1}} = 1] - Pr[D^{P, P^{-1}} = 1]| = 1 - \frac{1}{2^n}.$$

In fact, there exist a distinguisher can distinguish the 3-round strong pseudorandomness with an overwhelming probability with 3 oracle queries. The distinguisher is described as follows:

Distinguisher with three oracle queries.

Distinguisher D can access to oracles $(\mathcal{O}, \mathcal{O}^{-1})$ where $(\mathcal{O}, \mathcal{O}^{-1})$ is (LR_3, LR_3^{-1}) or (P, P^{-1}).

1. D selects a message m_1 where $|m_1| = 2n$ and $m_1 = (a, b)$, then he makes the query m_1 to $\mathcal{O}$, and receives $c_1 = (x, y)$.
2. D queries m_2 where $|m_2| = 2n$ and $m_2 = (a \oplus \delta, b)$ to $\mathcal{O}$, and receives $c_2 = (x', y')$.
3. D queries $(x' \oplus \delta, y')$ to $\mathcal{O}^{-1}$ and receives $m_1' = (a_1', b_1')$.
4. If $b_1' = b \oplus y \oplus y'$ outputs 1, otherwise outputs 0.

Following the Feistel encryption procedure, we have

$$x = a \oplus f_1 \oplus f_3, \quad \text{where } f_1 = F_1(b) \text{ and } f_3 = F_3(b \oplus F_2(a \oplus F_1(b)))$$
$$y = b \oplus f_2, \quad \text{where } f_2 = F_2(a \oplus F_1(b))$$

and

$$x' = a \oplus \delta \oplus f_1 \oplus f_3', \quad \text{where } f_3' = F_3(b \oplus F_2(a \oplus \delta \oplus F_1(b)))$$
$$y' = b \oplus f_2', \quad \text{where } f_2 = F_2(a \oplus \delta \oplus F_1(b))$$

So $f_2 \oplus f_2' = y \oplus y'$, and the right part of the inverse permutation of $(x' \oplus \delta, y')$ is

$$\begin{aligned} b' &= y' \oplus F_2(x' \oplus \delta \oplus f_3') \\ &= y' \oplus F_2(a \oplus f_1) \\ &= b \oplus f_2' \oplus f_2 \\ &= b \oplus y \oplus y'. \end{aligned}$$

So the above distinguisher succeeds and the advantage of the distinguisher is:

$$Adv(D) = |Pr[D^{LR_3, LR_3^{-1}} = 1] - Pr[D^{P, P^{-1}} = 1]| = 1 - \frac{1}{2^n}.$$

It is worthwhile to give some thought to this distinguish method. The first step is to make an encryption query m_1 and receive the ciphertext c_1, and then is to make an encryption query m_2 and receive the ciphertext c_2 such that the input of F_1 remains the same as the first query. Next the ciphertext c_2 is modified to c_3 and then is sent to the decryption oracle to receive the plaintext m_3, while the input of F_3 remains the same as the second encryption query and the input of F_2 remains the same as the first encryption query. At last if there are some relationships between m_3 and m_1, c_1, m_2, c_2, c_3, then the 3-round Feistel permutation can be distinguished from a uniform random permutation.

4.2 Distinguishability of Three-Round Lai-Massey Scheme

To prove that four-round Lai-Massey scheme is necessary for strong pseudorandomness, it must be pointed out that there exists a 3-round strong pseudorandomness distinguisher. In[14], the strong pseudorandomness of Lai-Massey permutation is independent of arbitrary group G and the orthomorphism σ, so it is enough to find a distinguisher for a special group and orthomorphism. Here the group G is $(\{0,1\}^{2n}, \oplus)$ and orthomorphism σ is $\sigma(x,y) = (y, x \oplus y)$ where $x, y \in (\{0,1\}^{2n}, \oplus)$ and $\oplus$ denotes the operation bitwise exclusive or(xor), just defined as the block cipher FOX[3].

The distinguisher of 3-round Feistel network provides the motivation for distinguishing the 3-round Lai-Massey permutation by the similar method. But the distinguisher in this case is more complex.

Theorem 5. *Let F_1, F_2, F_3 be three independent pseudorandom functions from $\{0,1\}^{2n}$ to $\{0,1\}^{2n}$, Let σ be an orthomorphism on $\{0,1\}^{2n}$ such that $\sigma(x,y) = (y, x \oplus y)$ where $x, y \in \{0,1\}^n$ and $\oplus$ denotes the bit operation exclusive or. Then the three-round Lai-Massey permutation LM_3 built from F_1, F_2, F_3 and σ is not strong pseudorandomness.*

Proof. It is required to find a distinguisher D such that can access to oracles $(\mathcal{O}, \mathcal{O}^{-1})$ where $(\mathcal{O}, \mathcal{O}^{-1})$ is (LM_3, LM_3^{-1}) or (P, P^{-1}) and distinguish the two scenarios. The following distinguisher can distinguish three-round Lai-Massey permutation from a uniform random permutation.

1. D selects a message m_1 where $|m_1| = 4n$ and $m_1 = (A_1, A_2, A_3, A_4)$, then he makes the query m_1 to $\mathcal{O}$, and receives $c_1 = (D_1, D_2, D_3, D_4)$.
2. D queries m_2 where $|m_2| = 4n$ and $m_2 = (A_1 \oplus \delta_1, A_2 \oplus \delta_2, A_3 \oplus \delta_1, A_4 \oplus \delta_2)$ to $\mathcal{O}$, and receives $c_2 = (D'_1, D'_2, D'_3, D'_4)$.
3. D queries $(D'_1 \oplus \delta_2, D'_2 \oplus \delta_1 \oplus \delta_2, D'_3 \oplus \delta_2, D'_4 \oplus \delta_1 \oplus \delta_2)$ to $\mathcal{O}^{-1}$ and receives $m_3 = (a_1, a_2, a_3, a_4)$.
4. If $a_1 \oplus a_3 = A_1 \oplus A_3 \oplus D_1 \oplus D_2 \oplus D_3 \oplus D_4 \oplus D'_1 \oplus D'_2 \oplus D'_3 \oplus D'_4$ and $a_2 \oplus a_4 = A_2 \oplus A_4 \oplus D_1 \oplus D_3 \oplus D'_1 \oplus D'_3$, then outputs 1, otherwise outputs 0.

For the first encryption oracle query (A_1, A_2, A_3, A_4), we can calculate the output of three-round Lai-Massey permutation by the encryption procedure as follows:

The input of the first round function is (A_1, A_2, A_3, A_4), if we define $F_1(A_1 \oplus A_3, A_2 \oplus A_4) = f_1 \parallel f_2$, where $\parallel$ means the concatenation, then the output of the first round function is

$$
\begin{aligned}
B_1 &= A_2 \oplus f_2 \\
B_2 &= A_1 \oplus A_2 \oplus f_1 \oplus f_2 \\
B_3 &= A_3 \oplus f_1 \\
B_4 &= A_4 \oplus f_2
\end{aligned}
$$

Let $F_2(B_1 \oplus B_3, B_2 \oplus B_4) = F_2(A_2 \oplus A_3 \oplus f_1 \oplus f_2, A_1 \oplus A_2 \oplus A_4 \oplus f_1) = g_1 \parallel g_2$, then the output of the second round function is

$$\begin{aligned} C_1 &= A_1 \oplus A_2 \oplus f_1 \oplus f_2 \oplus g_2 \\ C_2 &= A_1 \oplus f_1 \oplus g_1 \oplus g_2 \\ C_3 &= A_3 \oplus f_1 \oplus g_1 \\ C_4 &= A_4 \oplus f_2 \oplus g_2 \end{aligned}$$

Let $F_3(C_1 \oplus C_3, C_2 \oplus C_4) = F_3(A_1 \oplus A_2 \oplus A_3 \oplus f_2 \oplus g_1 \oplus g_2, A_1 \oplus A_4 \oplus f_1 \oplus f_2 \oplus g_1) = h_1 \parallel h_2$, the output of the third round function without the σ transform is

$$D_1 = A_1 \oplus A_2 \oplus f_1 \oplus f_2 \oplus g_2 \oplus h_1 \tag{1}$$
$$D_2 = A_1 \oplus f_1 \oplus g_1 \oplus g_2 \oplus h_2 \tag{2}$$
$$D_3 = A_3 \oplus f_1 \oplus g_1 \oplus h_1 \tag{3}$$
$$D_4 = A_4 \oplus f_2 \oplus g_2 \oplus h_2 \tag{4}$$

If xoring the equation (1) and (3), and the equation (2) and (4), one can obtain the following equation:

$$f_2 \oplus g_1 \oplus g_2 = D_1 \oplus D_3 \oplus A_1 \oplus A_2 \oplus A_3 \tag{5}$$
$$f_1 \oplus f_2 \oplus g_1 = D_2 \oplus D_4 \oplus A_1 \oplus A_4 \tag{6}$$

By using a similar method, the ciphertext of the second encryption oracle query $(A_1 \oplus \delta_1, A_2 \oplus \delta_2, A_3 \oplus \delta_1, A_4 \oplus \delta_2)$ is

$$\begin{aligned} D'_1 &= A_1 \oplus A_2 \oplus f_1 \oplus f_2 \oplus g'_2 \oplus h'_1 \oplus \delta_1 \oplus \delta_2 \\ D'_2 &= A_1 \oplus f_1 \oplus g'_1 \oplus g'_2 \oplus h'_2 \oplus \delta_1 \\ D'_3 &= A_3 \oplus f_1 \oplus g'_1 \oplus h'_1 \oplus \delta_1 \\ D'_4 &= A_4 \oplus f_2 \oplus g'_2 \oplus h'_2 \oplus \delta_2 \end{aligned}$$

where $F_2(A_2 \oplus A_3 \oplus f_1 \oplus f_2 \oplus \delta_1 \oplus \delta_2, A_1 \oplus A_4 \oplus f_1 \oplus \delta_1) = g'_1 \parallel g'_2$ and $F_3(A_1 \oplus A_2 \oplus A_3 \oplus f_2 \oplus g'_1 \oplus g'_2 \oplus \delta_2, A_1 \oplus A_4 \oplus f_1 \oplus f_2 \oplus g'_1 \oplus \delta_1 \oplus \delta_2) = h'_1 \parallel h'_2$.

Thus we have

$$f_2 \oplus g'_1 \oplus g'_2 = D'_1 \oplus D'_3 \oplus A_1 \oplus A_2 \oplus A_3 \oplus \delta_2 \tag{7}$$
$$f_1 \oplus f_2 \oplus g'_1 = D'_2 \oplus D'_4 \oplus A_1 \oplus A_4 \oplus \delta_1 \oplus \delta_2 \tag{8}$$

The decryption of $(d_1, d_2, d_3, d_4) = (D'_1 \oplus \delta_2, D'_2 \oplus \delta_1 \oplus \delta_2, D'_3 \oplus \delta_2, D'_4 \oplus \delta_1 \oplus \delta_2)$ is (a_1, a_2, a_3, a_4), following the decryption procedure, the output of the third round function without the σ transform is (d_1, d_2, d_3, d_4), since $F_3(d_1 \oplus d_3, d_2 \oplus d_4) = h'_1 \parallel h'_2$, the input of the third round function is:

$$\begin{aligned} c_1 &= A_1 \oplus A_2 \oplus f_1 \oplus f_2 \oplus g'_2 \oplus \delta_1 \\ c_2 &= A_1 \oplus f_1 \oplus g'_1 \oplus g'_2 \oplus \delta_1 \oplus \delta_2 \\ c_3 &= A_3 \oplus f_1 \oplus g'_1 \oplus \delta_2 \\ c_4 &= A_4 \oplus f_2 \oplus g'_2 \oplus \delta_1 \end{aligned}$$

Then the input to the function F_2 is $(c_1 \oplus c_2 \oplus c_3, c_1 \oplus c_4) = (A_2 \oplus A_3 \oplus f_1 \oplus f_2, A_1 \oplus A_2 \oplus A_4 \oplus f_1)$ and so $F_2(c_1 \oplus c_2 \oplus c_3, c_1 \oplus c_4) = g_1 \parallel g_2$. And the input of the second round function is

$$\begin{aligned} b_1 &= A_2 \oplus f_2 \oplus g_1 \oplus g_1' \oplus \delta_1 \oplus \delta_2 \\ b_2 &= A_1 \oplus A_2 \oplus f_1 \oplus f_2 \oplus g_2 \oplus g_2' \oplus \delta_1 \\ b_3 &= A_3 \oplus f_1 \oplus g_1 \oplus g_1' \oplus \delta_1 \oplus \delta_2 \\ b_4 &= A_4 \oplus f_2 \oplus g_2 \oplus g_2' \oplus \delta_1 \end{aligned}$$

Since the input of the first round function is (a_1, a_2, a_3, a_4), we can deduce the following equation:

$$\begin{aligned} a_1 \oplus a_3 &= b_1 \oplus b_2 \oplus b_3 = A_1 \oplus A_3 \oplus g_2 \oplus g_2' \oplus \delta_1 \\ a_2 \oplus a_4 &= b_1 \oplus b_4 = A_2 \oplus A_4 \oplus g_1 \oplus g_1' \oplus g_2 \oplus g_2' \oplus \delta_2 \end{aligned}$$

According to equation (5), (6), (7) and (8),

$$\begin{aligned} g_2 \oplus g_2' &= D_1 \oplus D_2 \oplus D_3 \oplus D_4 \oplus D_1' \oplus D_2' \oplus D_3' \oplus D_4' \oplus \delta_1 \\ g_1 \oplus g_2 \oplus g_1' \oplus g_2' &= D_1 \oplus D_3 \oplus D_1' \oplus D_3' \oplus \delta_2 \end{aligned}$$

Finally, we obtain

$$\begin{aligned} a_1 \oplus a_3 &= A_1 \oplus A_3 \oplus D_1 \oplus D_2 \oplus D_3 \oplus D_4 \oplus D_1' \oplus D_2' \oplus D_3' \oplus D_4' \\ a_2 \oplus a_4 &= A_2 \oplus A_4 \oplus D_1 \oplus D_3 \oplus D_1' \oplus D_3' \end{aligned}$$

Thus the distinguisher succeeds with an overwhelming probability. The advantage of the distinguisher is as follows.

$$|Pr[D^{LM_3, LM_3^{-1}} = 1] - Pr[D^{P, P^{-1}} = 1]| = 1 - 2^{-2n}.$$

So the theorem follows. □

In order to implement the strong pseudorandomness property, it is required to iterated the Lai-Massey round function at least 4 rounds. Combined with previous results, the following corollary follows.

Corollary 2 *The r-round Lai-Massey scheme LM_r is pseudorandom and strongly pseudorandom if and only if $r \geq 3$ and $r \geq 4$ respectively.*

5 Conclusion

We have proven that three rounds and four rounds are not only sufficient, but also necessary to implement the pseudorandomness and strong pseudorandomness of the Lai-Massey scheme. The results are proven under the classical indistinguishability model. Under this model, distinguisher has only access to the input/output of the construction; in particular it does not have access to the

input/output of the internal primitives. Since the indifferentiability model was introduced recently and be used in exploiting if there exist hidden flaws in hash constructions [1, 8]. An interesting future work is to find out that the exact rounds for the Lai-Massey scheme can be secure in the indifferentiability model, where the distinguisher can make oracle queries to all the internal primitives.

References

1. J. S. Coron, J. Patarin, and Y. Seurin. The random oracle model and the ideal cipher model are equivalent. In David Wagner, editor, *Advances in Cryptology - CRYPTO 2008*, LNCS 5157, pp. 1-20. 2008.
2. O. Goldreich. Foundations of Cryptography - Basic Tools. Cambridge University Press, 2001.
3. P. Junod and S. Vaudenay. FOX: a new family of block ciphers. *Selected Areas in Cryptography - SAC 2004*, LNCS 2595, pp.131-146, Springer-Verlag, 2004.
4. X. Lai. On the design and security of block ciphers. *ETH Series in Information Processing*, vol. 1, Hartung-Gorre Verlag, Konstanz, 1992.
5. X. Lai and J. L. Massey. A proposal for a new block encryption standard. *Advances in Cryptology - EUROCRYPT'90*, LNCS 473, pp. 389-404, Springer-Verlag, 1991.
6. M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, vol. 17, no. 2, pp. 373-386, April 1988.
7. U. M. Maurer, A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators, *Advances in Cryptology - EUROCRYPT '92*, LNCS 658, pp. 239-255, Springer-Verlag, Berlin, 1992.
8. U. Maurer, R. Renner, and C. Holenstein. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. *Theory of Cryptography - TCC 2004*, LNCS 2951, pp. 21-39. 2004.
9. Shiho Moriai and Serge Vaudenay. On the Pseudorandomness of Top-Level Schemes of Block Ciphers. *Advances in Cryptology - ASIACRYPT'00*, LNCS 1976, pp. 289-302, Springer-Verlag, 2000.
10. M. Naor and O. Reingold. On the construction of pseudorandom permutations: Luby-Rackoff revisited. *Journal of Cryptology*, vol. 12, no. 1, pp. 29-66, 1999.
11. J. Patarin. How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function. *Advances in Cryptology - EUROCRYPT'92*, LNCS 658, pp. 256-266, Springer-Verlag, 1993.
12. B. Sadeghiyan and J. Pieprzyk, On necessary and sufficient conditions for the construction of super pseudorandom permutations, *Abstracts of ASIACRYPT'91*, LNCS 739, pp. 194-209, Springer-Verlag, 1991.
13. S. Vaudenay. Provable Security for Block Ciphers by Decorrelation. *Theoretical Aspects of Computer Science - STACS'98*, LNCS 1373, pp. 249-275, Springer-Verlag, 1998.
14. S. Vaudenay. On the Lai-Massey Scheme. *Advances in Cryptology - ASIACRYPT'99*, LNCS 1716, pp. 8-19, Springer-Verlag, 1999.
15. Wenling Wu, Wentao Zhang and Dengguo Feng. Integral Cryptanalysis of Reduced FOX Block Cipher. *Information Security and Cryptology - ICISC 2005*, LNCS 3935, pp. 229-241, Springer-Verlag, 2006.