Quantum Attacks on Lai-Massey Structure*

Shuping Mao[1,2], Tingting Guo[1,2], Peng Wang[1,2(✉)] and Lei Hu[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering, CAS
[2] School of Cyber Security, University of Chinese Academy of Sciences
w.rocking@gmail.com

Abstract. Aaram Yun et al. considered that Lai-Massey structure has the same security as Feistel structure. However, Luo et al. showed that 3-round Lai-Massey structure can resist quantum attacks of Simon's algorithm, which is different from Feistel structure. We give quantum attacks against a typical Lai-Massey structure. The result shows that there exists a quantum CPA distinguisher against 3-round Lai-Massey structure and a quantum CCA distinguisher against 4-round Lai-Massey Structure, which is the same as Feistel structure. We extend the attack on Lai-Massey structure to quasi-Feistel structure. We show that if the combiner of quasi-Feistel structure is linear, there exists a quantum CPA distinguisher against 3-round balanced quasi-Feistel structure and a quantum CCA distinguisher against 4-round balanced quasi-Feistel Structure.

Keywords: Quantum attacks · Lai-Massey structure · Quasi-Feistel structure.

1 Introduction

Quantum attacks With the rapid development of quantum computers, the security of classic algorithms has been challenged. Shor [31] found that both the large number decomposition problem and the discrete logarithm problem have quantum polynomial-time algorithms, which pose a serious threat to RSA and other mainstream asymmetric crypto algorithms. In symmetric cryptography, it has always been considered that the biggest threat comes from Grover's quantum search algorithm [12]. It can reduce the complexity of k bits exhaustive algorithm to $O\left(2^{k/2}\right)$.

In his seminal paper, Simon [32] answered the question of how to find the period of a periodic function in $O(n)$ quantum queries. Many structures and the most widely used modes of operation for authentication and authenticated encryption were attacked by using Simon's algorithm. For example, the attacks of 3-round [21], 4-round [17] Feistel structures, 3-round MISTY-L structure, 3-round MISTY-R structure [29], Even-Mansour structure, LRW structure, CBC-MAC, PMAC, GMAC, GCM, and OCB [19].

Leander and May combined Simon's Algorithm with Gover's algorithm, giving a quantum key-recovery attack on FX-construction [24], which caused a quantum CPA attack on 5-round Feistel structure [8], quantum CCA attack on 7-round Feistel-KF structure and 9-round Feistel-FK structure [17].

* Supported by the NSFC of China (61732021) and the National Key RD Program of China (2018YFB0803801 and 2018YFA0704704).

Lai-Massey Structure IDEA algorithm [22,23] was designed by Lai and Massey. Vaudenay [35] generalized the structure adopted by IDEA algorithm and proposed the Lai-Massey structure. Lai-Massey structure uses general addition and subtraction operations in a finite abelian group G and has an orthomorphism permutation $\sigma : G \to G$. σ has the orthomorphism property: σ and $x \mapsto \sigma(x) - x$ are both permutations. Based on Lai-Massey structure, FOX [18] (also known as "IDEA NXT") was produced. FOX uses XOR operation instead of general addition and subtraction operations, and it reifies σ as $\sigma\left(x_L, x_R\right) = \left(x_R, x_L \oplus x_R\right)$. In this paper, we attack the instantiated Lai-Massey structure used in FOX. The ith-round of Lai-Massey structure is shown in Figure 1.

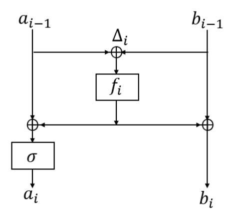

Fig. 1. The ith-round of Lai-Massey structure

Let $\mathrm{LM}_i(a_{i-1}, b_{i-1}) = (\sigma(a_{i-1} \oplus f_i(\Delta_i)), b_{i-1} \oplus f_i(\Delta_i))$, $\mathrm{LM}'_i(a_{i-1}, b_{i-1}) = (a_{i-1} \oplus f_i(\Delta_i), b_{i-1} \oplus f_i(\Delta_i))$. Then r-round Lai-Massey structure can be written as:

$$\mathrm{F}_{\mathrm{rLM}} \overset{\mathrm{def}}{=} (a_r, b_r) = \mathrm{LM}'_r \circ \mathrm{LM}_{r-1} \circ \cdots \circ \mathrm{LM}_1.$$

3-round and 4-round Lai-Massey structures are proven to be secure against chosen-plaintext attacks (CPAs) and chosen-ciphertext attacks (CCAs), respectively by Vaudenay et al. [35], like Feistel structure [9]. Luo, et al. [27] proved that 3 rounds (4 rounds) are necessary for CPA secure (CCA secure). Sui et al. [34] proved that 4-round Lai-Massey structure is CCA secure even if the adversary extra access to two internal rounds. Luo, et al. [28] proved beyond-birthday-bound for the CCA-security of many-round Lai-Massey scheme. Attacks like integral attacks [38,37], impossible differential cryptanalysis [39,7,13], collision-integral attacks [36], fault attacks [25], differential cryptanalysis [10,11], linear cryptanalysis [10], all-subkeys recovery attacks [16], imprimitivity attacks [3] were applied to block ciphers with Lai-Massey structure.

Quasi-Feistel structure Feistel structure is one of the most important block-cipher structures. Many block ciphers are designed by this scheme like DES [33], FEAL [30], SKIPJACK [1] and SIMON [4]. Michael Luby and Charles Rackoff [26] proved that 3-round Feistel structure is CPA secure, and 4-round Feistel structure is CCA secure if round functions are independent random functions. Zhang Liting et al. [41] extended those conclusions and proved that $k+1$ rounds **u**nbalanced **F**eistel **n**etworks with **c**ontracting functions(UFN-C) is CPA secure, $k+2$ rounds UFN-C is CCA secure.

In [40], Aaram Yun et.al proposed quasi-Feistel structure and proved that Feistel structure and Lai-Massey structure are quasi-Feistel structures. They shown that the birthday security of $(2b-1)$-round and $(3b-2)$-round unbalanced quasi-Feistel ciphers with b branches against CPA and CCA attacks respectively.

In [29], Luo, et al. shown that 3-round Lai-Massey structure can resist the attacks of Simon's algorithm in quantum, which is different from Feistel structure. This leads to natural questions:

Do Lai-Massey structure and Feistel structure have the same number of rounds that can be attacked in quantum? Can the attacks be extended to quasi-Feistel structures?

Our Contributions The contributions of this paper are listed as follows:

1. We show a quantum CPA distinguisher against 3-round Lai-Massey structure and a quantum CCA distinguisher against 4-round Lai-Massey structure with $O(n)$ quantum queries, where the input length of Lai-Massey structure is $2n$ bits. So Lai-Massey structure and Feistel structure have the same number of rounds that can be attacked efficiently in quantum, this makes it possible for quasi-Feistel structures to have similar security strength in quantum.
2. we give a quantum Grover-meet-Simon attack on 4-round Lai-Massey structure with $O(n2^{m/2})$ quantum queries, where m is the length of the key k_4 of the fourth round function f_4.
3. We extend the quantum attack on Lai-Massey structure to quasi-Feistel structure. We show that 3-rounds (4-round) balanced quasi-Feistel structure including Feistel structure and Lai-Massey structure with linear combiners can be attacked with $O(n)$ quantum queries in quantum CPA (CCA).

2 Preliminaries

2.1 Notation

Let $\mathcal{X}$ be a finite set. Let $\mathsf{Perm}(\mathcal{X})$ be the set of all permutations on $\mathcal{X}$. Let $x \stackrel{\$}{\leftarrow} \mathcal{X}$ denote selecting an element x from the set $\mathcal{X}$ uniformly and randomly. Let $\pi \stackrel{\$}{\leftarrow} \mathsf{Perm}(\mathcal{X})$ be a random permutation on $\mathcal{X}$. $\mathcal{X}^k$ denotes the set of all k-tuples of elements from $\mathcal{X}$. A block cipher keyed by K is a function $E_K \in \mathsf{Perm}(\mathcal{X})$. We call the input and output of E_K as plaintext and ciphertext respectively. Let $\mathrm{Func}(\mathcal{X}, \mathcal{Y})$ be the set of all functions $f : \mathcal{X} \to \mathcal{Y}$. We write $\mathrm{Func}(\mathcal{X}) \stackrel{\text{def}}{=} \mathrm{Func}(\mathcal{X}, \mathcal{X})$.

Let $\mathcal{A}$ be an adversary. Let $\mathcal{A}^{f(\cdot)} \Rightarrow b$ (resp. $\mathcal{A}^{f(\odot)} \Rightarrow b$) denote an algorithm performs classical queries (resp. quantum queries) to oracle f and outputs b.

2.2 Pseudo-random Permutation

In this paper, we consider the adversary $\mathcal{A}$ making **c**hosen-**p**laintext **a**ttack (CPA), i.e., $\mathcal{A}$ queries with plaintexts and get corresponding ciphertexts, or **c**hosen-**c**iphertext **a**ttack (CCA), i.e., $\mathcal{A}$ queries with plaintexts or ciphertexts and get corresponding ciphertexts or plaintexts. Let PRP-CPA and PRP-CPA denote the **p**seudo-**r**andom **p**ermutation

(PRP) security under CPA and CCA respectively. Let qPRP-CPA and qPRP-CPA denote the quantum PRP security under CPA and CCA respectively. We put the formal definitions as follows.

Definition 1. *(PRP-CPA/qPRP-CPA) Let $E : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ be a family of permutations indexed by the elements in $\mathcal{K}$, $g : \mathcal{X} \to \mathcal{X}$. Let $\mathcal{A}$ be a adversary. The PRP-CPA/qPRP-CPA advantage of $\mathcal{A}$ is defined as:*

$$\mathbf{Adv}_E^{\textit{prp-cpa/qprp-cpa}}(\mathcal{A}) = \left| \Pr_{K \xleftarrow{\$} \mathcal{K}} \left[\mathcal{A}^{E_K(*)} \Rightarrow 1 \right] - \Pr_{g \xleftarrow{\$} \mathsf{Perm}(\mathcal{X})} \left[\mathcal{A}^{g(*)} \Rightarrow 1 \right] \right|,$$

where we replace the $*$ symbol by $\cdot$ (classical) or $\odot$ (quantum).

Definition 2. *(PRP-CCA/qPRP-CCA) Let $E : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ be a family of permutations indexed by the elements in $\mathcal{K}$, $g : \mathcal{X} \to \mathcal{X}$. Let $\mathcal{A}$ be a adversary. The PRP-CCA/qPRP-CCA advantage of $\mathcal{A}$ is defined as:*

$$\mathbf{Adv}_E^{\textit{prp-cca/qprp-cca}}(\mathcal{A}) = \left| \Pr_{K \xleftarrow{\$} \mathcal{K}} \left[\mathcal{A}^{E_K(*), E_K^{-1}(*)} \Rightarrow 1 \right] - \Pr_{g \xleftarrow{\$} \mathsf{Perm}(\mathcal{X})} \left[\mathcal{A}^{g(*), g^{-1}(*)} \Rightarrow 1 \right] \right|,$$

where we replace the $*$ symbol by $\cdot$ (classical) or $\odot$ (quantum).

2.3 Quantum Algorithms

In this section, we present some quantum algorithms that will be applied in our attacks.

Simon's Algorithm Simon's algorithm is a quantum algorithm to recover the period of a periodic function with polynomial queries. It solves the Simon's problem.
Simon's problem [32] Given a Boolean function $f : \{0,1\}^n \to \{0,1\}^m$, $x, y \in \{0,1\}^n$. x, y satisfied the condition $[f(x) = f(y)] \Leftrightarrow [x \oplus y \in \{0^n, s\}]$, s is non-zero and $s \in \{0,1\}^n$, the goal is to find s.
The steps of Simon's algorithm: [32]

1. Initialize the state of $2n$ qubits to $|0\rangle^{\otimes n}|0\rangle^{\otimes m}$;
2. Apply Hadamard transformation $H^{\otimes n}$ to the first n qubits to obtain quantum superposition $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|0\rangle^{\otimes m}$;
3. A quantum query to the function f maps this to the state: $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle$;
4. Measure the last m qubits to get the output z of $f(x)$, and the first n qubits collapse to $\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle)$;
5. Apply the Hadamard transform to the first n quantum again $H^{\otimes n}$, we can get $\frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{y \cdot z} (1 + (-1)^{y \cdot s}) |y\rangle$. If $y \cdot s = 1$ then the amplitude of $|y\rangle$ is 0. So measuring the state in the computational basis yields a random vector y such that $y \cdot s = 0$, which means that y must be orthogonal to s.

By repeating this step $O(n)$ times, $n-1$ independent vectors y orthogonal to s can be obtained with high probability, then we can recover s with high probability by using linear algebra.

For $f : \{0,1\}^n \to \{0,1\}^n$ and $f(x \oplus s) = f(x)$, Kaplan [19] define:

$$\varepsilon(f,s) = \max_{t \in \{0,1\}^n \setminus \{0,s\}} \mathrm{Pr}_x[f(x) = f(x \oplus t)].$$

ε represents max probability of unwanted additional collisions that $f(x) = f(x \oplus t)$ where $t \notin \{0,1\}^n \setminus \{0,s\}$. The following theorem shows that Simon's algorithm can succeed even with additional collisions.

Theorem 1. *[19] If $m = n$ and $\varepsilon(f,s) \le p_0 < 1$, then Simon's algorithm returns s with cn queries, with probability at least $1 - \left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$.*

Guo et al. [14] shows Simon's conclusion holds for $m \neq n$ as well.

Grover's Algorithm Grover's Algorithm can find a marked element from a set with an acceleration of the square root compared to classical computing. It solves the Grover's problem.

Grover's problem Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$. Find a marked element x_0 from $\{0,1\}^n$ such that $f(x_0) = 1$.

The steps of Grover's Algorithm [12]:

1. Initializing a n-bit register $|0\rangle^{\otimes n}$.
2. Apply Hadamard transformation $H^{\otimes n}$ to the first register to obtain quantum superposition $H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle = |\varphi\rangle$.
3. Construct an Oracle $\mathcal{O} : |x\rangle \xrightarrow{\mathcal{O}} (-1)^{f(x)}|x\rangle$, if x is the correct state then $f(x) = 1$, otherwise $f(x) = 0$.
4. Apply Grover iteration for $R \approx \frac{\pi}{4}\sqrt{2^n}$ times: $[(2|\varphi\rangle\langle\varphi| - I)\mathcal{O}]^R|\varphi\rangle \approx |x_0\rangle$.
5. Return x_0.

Grover-meet-Simon Algorithm In 2017, Leander and May [24] combined Grover's algorithm with Simon's algorithm to attack FX construction [20]. Their main idea is to construct a function with two inputs based on FX, say $f(u,x)$. When the first input u equals to a special value k, the function has a hidden period s such that $f(k,x) = f(k, x \oplus s)$ for all x. Their combined algorithm use Grover's algorithm to search k, by running many independent Simon's algorithms to check whether the function is periodic or not, and recover both k and s in the end. The attack only costs $\mathcal{O}(2^{m/2}(m+n))$ quantum queries to FX, which is much less than the proved security up to $2^{\frac{m+n}{2}}$ queries [20], where m is the bit length of u, which is the key length of the underlying block cipher and n is the bit length of s, which is the block size.

3 Quantum Attacks on Lai-Massey Structures

3.1 Quantum Chosen-Plaintext Attack Against 3-round Lai-Massey Structure

Figure 2 shows the 3-round Lai-Massey Structure, where f_1, f_2, f_3 are round functions and $\sigma(x_L, x_R) = (x_R, x_L \oplus x_R)$. We define $[a, b] \in \{0,1\}^n$, where a, b represent the highest $n/2$ bits and the lowest $n/2$ bits respectively. Let $x_i, y_i \in \{0,1\}^{n/2}, i = 1, 2, 3, 4$. The inputs of 3-round Lai-Massey structure can be written as $[x_1, x_2]$, $[x_3, x_4]$, the outputs can be written as $[y_1, y_2]$,$[y_3, y_4]$. a_i, b_i and $\Delta_i, i = 1, 2, 3$ are intermediate parameters as shown in Figure 2.

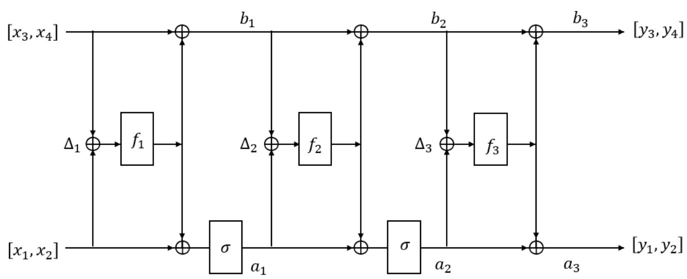

Fig. 2. 3-round Lai-Massey structure

Theorem 2. *If $f_i, i = 1, 2, 3$ are random functions, we can construct a quantum CPA distinguisher against 3-round Lai-Massey structure with $\sigma(x_L, x_R) = (x_R, x_L \oplus x_R)$ in $O(n)$ quantum queries by using Simon's algorithm.*

We first give some lemmas before proving Theorem 2. To attack 3-round Lai-Massey structure with Simon's algorithm, we will find a periodic function. Due to the complex structure of Lai-Massey, first we write the values of intermediate parameters.

For the 3-round Lai-Massey structure shown in the figure 2, the intermediate parameters are as follows

$$
\begin{aligned}
a_1 =& [x_2 \oplus f_{1R}(\Delta), x_1 \oplus x_2 \oplus f_{1L}(\Delta_1) \oplus f_{1R}(\Delta_1)], \\
b_1 =& [x_3 \oplus f_{1L}(\Delta_1), x_4 \oplus f_{1R}(\Delta_1)], \\
a_2 =& [x_1 \oplus x_2 \oplus f_{1L}(\Delta_1) \oplus f_{1R}(\Delta_1) \oplus f_{2R}(\Delta_2), \\
& x_1 \oplus f_{1L}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{2R}(\Delta_2)], \\
b_2 =& [x_3 \oplus f_{1L}(\Delta_1) \oplus f_{2L}(\Delta_2), x_4 \oplus f_{1R}(\Delta_1) \oplus f_{2R}(\Delta_2)], \\
a_3 =& [y_1, y_2] \\
=& [x_1 \oplus x_2 \oplus f_{1L}(\Delta_1) \oplus f_{1R}(\Delta_1) \oplus f_{2R}(\Delta_2) \oplus f_{3L}(\Delta_3), \\
& x_1 \oplus f_{1L}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{2R}(\Delta_2) \oplus f_{3R}(\Delta_3)] \\
b_3 =& [y_3, y_4] \\
=& [x_3 \oplus f_{1L}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{3L}(\Delta_3), x_4 \oplus f_{1R}(\Delta_1) \oplus f_{2R}(\Delta_2) \oplus f_{3R}(\Delta_3)],
\end{aligned}
$$

where

$$\begin{aligned}\Delta_1 =& [x_1 \oplus x_3, x_2 \oplus x_4],\\ \Delta_2 =& [x_2 \oplus x_3 \oplus f_{1L}(\Delta_1) \oplus f_{1R}(\Delta_1), x_1 \oplus x_2 \oplus x_4 \oplus f_{1L}(\Delta_1)],\\ \Delta_3 =& [x_1 \oplus x_2 \oplus x_3 \oplus f_{1R}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{2R}(\Delta_2),\\ & x_1 \oplus x_4 \oplus f_{1L}(\Delta_1) \oplus f_{1R}(\Delta_1) \oplus f_{2L}(\Delta_2)].\end{aligned}$$

Lemma 1. *Let $x, x' \in \{0,1\}^{n/2}, b \in \{0,1\}$ and α_0, α_1 be arbitrary two fixed different numbers in $\{0,1\}^{n/2}$. Let $([x_1^{\alpha_b}, x_2^{\alpha_b}], [x_3^{\alpha_b}, x_4^{\alpha_b}]) \overset{def}{=} ([x \oplus \alpha_b, x'], [x, x' \oplus \alpha_b])$ being the input of 3-round Lai-Massey structure with corresponding output $([y_1^{\alpha_b}, y_2^{\alpha_b}], [y_3^{\alpha_b}, y_4^{\alpha_b}])$. We can construct a periodic function g_1 from 3-round Lai-Massey structure with period $s = f_1[\alpha_0, \alpha_0] \oplus f_1[\alpha_1, \alpha_1]$ by letting*

$$\begin{aligned} g_1 : \{0,1\}^n \to& \{0,1\}^{n/2}\\ [x, x'] \mapsto& x_1^{\alpha_0} \oplus x_2^{\alpha_0} \oplus x_3^{\alpha_0} \oplus y_1^{\alpha_0} \oplus y_3^{\alpha_0} \oplus x_1^{\alpha_1} \oplus x_2^{\alpha_1} \oplus x_3^{\alpha_1} \oplus y_1^{\alpha_1} \oplus y_3^{\alpha_1}\\ g_1([x, x']) =& f_{1R}[\alpha_0, \alpha_0] \oplus f_{2L}(\Delta_2^{\alpha_0}([x, x'])) \oplus f_{2R}(\Delta_2^{\alpha_0}([x, x']))\\ & \oplus f_{1R}[\alpha_1, \alpha_1] \oplus f_{2L}(\Delta_2^{\alpha_1}([x, x'])) \oplus f_{2R}(\Delta_2^{\alpha_1}([x, x'])), \end{aligned} \tag{1}$$

where $\Delta_2^{\alpha_b}([x, x'])$ denotes the value of intermediate parameter Δ_2 when the input of 3-round Lai-Massey structure is $([x_1^{\alpha_b}, x_2^{\alpha_b}], [x_3^{\alpha_b}, x_4^{\alpha_b}])$ and

$$\Delta_2^{\alpha_b}([x, x']) = [x' \oplus x \oplus f_{1L}[\alpha_b, \alpha_b] \oplus f_{1R}[\alpha_b, \alpha_b], x \oplus f_{1L}[\alpha_b, \alpha_b]].$$

Proof. we show that g_1 is obviously a periodic function.

(a) $\Delta_2^{\alpha_b}([x, x']) = \Delta_2^{\alpha_b \oplus 1}([x, x'] \oplus s)$ holds for all $x, x' \in \{0,1\}^{n/2}$.
(b) $g_1([x, x'])$ has a period s deriving from (a). □

Proof. (Proof of Theorem 2) Now we have a periodic function g_1 with period $s = f_1[\alpha_0, \alpha_0] \oplus f_1[\alpha_1, \alpha_1]$. Actually, other t's ($t \neq s$) may occur due to collisions, which may lead to misjudgments. Theorem 1 guarantees that Simon's algorithm can still succeed with probability $1 - \left(2\left(\frac{3}{4}\right)^c\right)^n$ if $\varepsilon(f, s) \leq p_0 < 1$. For 3-round Lai-Massey structure, the following certificate $\varepsilon(g_1, s) < \frac{1}{2}$:

Assuming $\varepsilon(g_1, s) \geq \frac{1}{2}$, then there is at least one $t \notin \{0, s\}$ such that $\Pr[g_1([x, x']) = g_1([x, x'] \oplus t]) \geq 1/2$. We denote f_{2L} or f_{2R} as f_{2*}. From equation (1) we have $\Pr\{f_{2*}[x' \oplus x \oplus u', x \oplus v'] = f_{2*}[x' \oplus t_R \oplus x \oplus t_L \oplus u', x \oplus t_L \oplus v']\} \geq \frac{1}{2}$, where u', v' are some parameters. That is, if $\varepsilon(g_1, s) \geq \frac{1}{2}$, then the probability that the permutation $f_{2*}[x' \oplus x \oplus u, x \oplus v]$ has a collision is greater than $\frac{1}{2}$. For different m_1, m_2, $\Pr\{f_{2*}[m_1' \oplus m_1 \oplus u, m_1 \oplus v] = f_{2*}[m_2\prime \oplus m_2 \oplus u, m_2 \oplus v]\} = \frac{1}{2^n}$, which is contradictory. Therefore $\varepsilon(g_1, s) < \frac{1}{2}$.

let $\mathcal{A}$ be an adversary, we write 3-round Lai-Massey structure as 3LM. For 3-round Lai-Massey structure, we can construct a period function g_1 with period s, and $g_1([x, x']) = g_1([x, x'] \oplus s)$. In the first query we ask x, and then we ask $x \oplus s$. If $\mathcal{A}$ is asking about 3-round Lai-Massey structure, then the outputs are the same. If $\mathcal{A}$ is asking about random permutation, then the outputs are different. So $\mathbf{Adv}_{\text{3LM}}^{\text{qprp-cpa}}(\mathcal{A}) = 1 - \left(2\left(\frac{3}{4}\right)^c\right)^n - \frac{1}{2^{n/2}}$. If we choose $c \geq 3/(1 - p_0)$, the error decreases exponentially with n. So if $c \geq 6$, $\mathbf{Adv}_{\text{3LM}}^{\text{qprp-cpa}}(\mathcal{A}) = 1 - \frac{1}{2^{n/2}}$. □

3.2 Quantum Chosen-Ciphertext Attack Against 4 round Lai-Massey Structure

For 4-round Lai-Massey Structure, let f_1, f_2, f_3, f_4 be round functions and $\sigma(x_L, x_R) = (x_R, x_L \oplus x_R)$. Let $x_i, y_i, n_i, z_i, x'_i \in \{0,1\}^{n/2}$, $i = 1,2,3,4$. To attack 4-round Lai-Massey Structure in CCA model, our attack strategy is as follows.

- Query the 4-round Lai- Massey structure with inputs $([x_1, x_2], [x_3, x_4])$s and get corresponding outputs $([y_1, y_2], [y_3, y_4])$s;
- Xor $([y_1, y_2], [y_3, y_4])$s with $([n_1, n_2], [n_3, n_4])$ and get $([z_3, z_4], [z_1, z_2])$;
- Query the inverse of 4-round Lai- Massey structure with inputs $([z_1, z_2], [z_3, z_4])$s and get corresponding outputs $([x'_1, x'_2], [x'_3, x'_4])$s;
- Construct a periodic function g_2 based on x'_1, x'_2, x'_3, x'_4s.
- Apply the periodicity of g_2 to distinguish 4-round Lai-Massey structure from a random permutation.

Let a_i, b_i, a'_i, b'_i and $\Delta_i, \Delta'_i, i = 1,2,3,4$ be intermediate parameters as shown in Figure.3. In the following, we show the formulation.

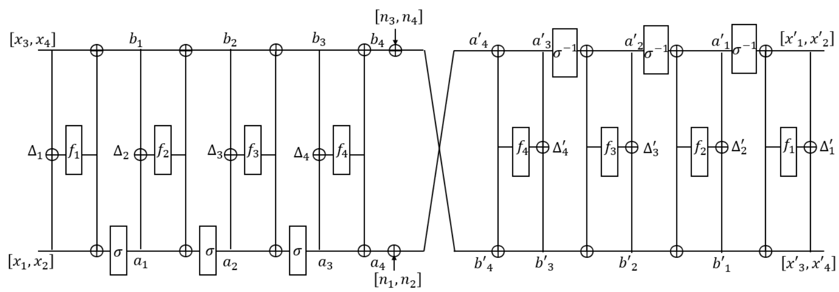

Fig. 3. The encryption and decryption process of 4-round Lai-Massey structure

Theorem 3. *If $f_i, i = 1,2,3,4$ are random functions, we can construct a quantum CCA distinguisher against 4-round Lai-Massey Structure with $\sigma(x_L, x_R) = (x_R, x_L \oplus x_R)$ in $O(n)$ quantum queries by using Simon's algorithm.*

We first give a lemma before proving Theorem 3. To show a quantum CCA distinguisher against 4-round Lai-Massey Structure with Simon's algorithm, we will find a periodic function based the function showed in Figture.3.

Intermediate parameters $a_i, b_i, \Delta_j, i = 1,2; j = 1,2,3$ are the same as Section 3.1. Intermediate parameters $a_3, b_3, a_4, b_4, \Delta_4$ are shown as follows. Other intermediate parameters $a'_i, b'_i, \Delta'_i, i = 1,2,3,4$ with respect to $[z_1, z_2], [z_3, z_4]$ are showed in in Appendix A.

$$\begin{aligned} a_3 =& [x_1 \oplus f_{1L}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{2R}(\Delta_2) \oplus f_{3R}(\Delta_3), \\ & x_2 \oplus f_{1R}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{3L}(\Delta_3) \oplus f_{3R}(\Delta_3)], \end{aligned}$$

$$
\begin{aligned}
b_3 =& [x_3 \oplus f_{1L}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{3L}(\Delta_3), x_4 \oplus f_{1R}(\Delta_1) \oplus f_{2R}(\Delta_2) \oplus f_{3R}(\Delta_3)],\\
a_4 =& [y_1, y_2]\\
=& [x_1 \oplus f_{1L}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{2R}(\Delta_2) \oplus f_{3R}(\Delta_3) \oplus f_{4L}(\Delta_4),\\
& x_2 \oplus f_{1R}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{3R}(\Delta_3) \oplus f_{3L}(\Delta_3) \oplus f_{4R}(\Delta_4)],\\
b_4 =& [y_3, y_4]\\
=& [x_3 \oplus f_{1L}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{3L}(\Delta_3) \oplus f_{4L}(\Delta_4),\\
& x_4 \oplus f_{1R}(\Delta_1) \oplus f_{2R}(\Delta_2) \oplus f_{3R}(\Delta_3) \oplus f_{4R}(\Delta_4)].
\end{aligned}
$$

where

$$
\begin{aligned}
\Delta_4 =& [x_1 \oplus x_3 \oplus f_{2R}(\Delta_2) \oplus f_{3L}(\Delta_3) \oplus f_{3R}(\Delta_3),\\
& x_2 \oplus x_4 \oplus f_{2L}(\Delta_2) \oplus f_{2R}(\Delta_2) \oplus f_{3L}(\Delta_3)].
\end{aligned}
$$

Let $n_1 \oplus n_3 = 0, n_2 \oplus n_4 = 0$. After the whole process of 4-round Lai-Massey structure shown in the Figure 3, the outputs $[x'_1, x'_2], [x'_3, x'_4]$ can be expressed with $[x_1, x_2], [x_3, x_4]$:

$$
\begin{aligned}
x'_1 =& x_1 \oplus n_1 \oplus f_{1L}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{2R}(\Delta_2) \oplus f_{3R}(\Delta_3) \oplus\\
& f_{1L}(\Delta'_1) \oplus f_{2L}(\Delta'_2) \oplus f_{2R}(\Delta'_2) \oplus f_{3R}(\Delta'_3),\\
x'_2 =& x_2 \oplus n_2 \oplus f_{1R}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{3R}(\Delta_3) \oplus f_{3L}(\Delta_3) \oplus\\
& f_{1R}(\Delta'_1) \oplus f_{2L}(\Delta'_2) \oplus f_{3R}(\Delta'_3) \oplus f_{3L}(\Delta'_3),\\
x'_3 =& x_3 \oplus n_3 \oplus f_{1L}(\Delta_1) \oplus f_{2L}(\Delta_2) \oplus f_{3L}(\Delta_3) \oplus f_{1L}(\Delta'_1) \oplus f_{2L}(\Delta'_2) \oplus f_{3L}(\Delta'_3),\\
x'_4 =& x_4 \oplus n_4 \oplus f_{1R}(\Delta_1) \oplus f_{2R}(\Delta_2) \oplus f_{3R}(\Delta_3) \oplus f_{1R}(\Delta'_1) \oplus f_{2R}(\Delta'_2) \oplus f_{3R}(\Delta'_3),
\end{aligned}
$$

where

$$
\begin{aligned}
\Delta'_3 =& \Delta_3 \oplus [n_2, n_1 \oplus n_4],\\
\Delta'_2 =& \Delta_2 \oplus [f_{3R}(\Delta_3) \oplus f_{3R}(\Delta'_3) \oplus n_2 \oplus n_3,\\
& f_{3L}(\Delta_3) \oplus f_{3R}(\Delta_3) \oplus f_{3L}(\Delta'_3) \oplus f_{3R}(\Delta'_3) \oplus n_1],\\
\Delta'_1 =& \Delta_1 \oplus [f_{2R}(\Delta_2) \oplus f_{3R}(\Delta_3) \oplus f_{3L}(\Delta_3) \oplus f_{2R}(\Delta'_2) \oplus f_{3L}(\Delta'_3) \oplus f_{3R}(\Delta'_3),\\
& f_{2R}(\Delta_2) \oplus f_{2L}(\Delta_2) \oplus f_{3L}(\Delta_3) \oplus f_{2L}(\Delta'_2) \oplus f_{2R}(\Delta'_2) \oplus f_{3L}(\Delta'_3)].
\end{aligned}
$$

Lemma 2. *Let $x, x' \in \{0,1\}^{n/2}, b \in \{0,1\}$ and α_0, α_1 be arbitrary two fixed different numbers in $\{0,1\}^{n/2}$. Let $([x_1^{\alpha_b}, x_2^{\alpha_b}], [x_3^{\alpha_b}, x_4^{\alpha_b}]) \overset{def}{=} ([x \oplus \alpha_b, x'], [x, x' \oplus \alpha_b])$ being the input of the function in Figure.3 based on 4-round Lai-Massey structure and its inverse with corresponding output $([{x'_1}^{\alpha_b}, {x'_2}^{\alpha_b}], [{x'_3}^{\alpha_b}, {x'_4}^{\alpha_b}])$ when $n_1 = n_2 = n_3 = n_4 = \alpha_0 \oplus \alpha_1$. We an construct a periodic function g_2 from 4-round Lai-Massey structure with period $s = f_1[\alpha_0, \alpha_0] \oplus f_1[\alpha_1, \alpha_1]$ by letting*

$$
\begin{aligned}
g_2 : \{0,1\}^n \to& \{0,1\}^{n/2}\\
[x, x'] \mapsto& {x'_1}^{\alpha_0} \oplus {x'_3}^{\alpha_0} \oplus {x'_1}^{\alpha_1} \oplus {x'_3}^{\alpha_1}\\
g_2([x, x']) =& f_{2R}(\Delta_2^{\alpha_0}([x, x'])) \oplus f_{2R}\left({\Delta'_2}^{\alpha_0}([x, x'])\right) \oplus f_{2R}(\Delta_2^{\alpha_1}([x, x'])) \oplus
\end{aligned}
$$

$$f_{2R}\left({\Delta'_2}^{\alpha_1}([x,x'])\right) \oplus f_{3R}\left(\Delta_3^{\alpha_0}([x,x'])\right) \oplus f_{3R}\left({\Delta'_3}^{\alpha_0}([x,x'])\right) \oplus$$
$$f_{3R}\left(\Delta_3^{\alpha_1}([x,x'])\right) \oplus f_{3R}\left({\Delta'_3}^{\alpha_1}([x,x'])\right) \oplus f_{3L}\left(\Delta_3^{\alpha_0}([x,x'])\right) \oplus$$
$$f_{3L}\left({\Delta'_3}^{\alpha_0}([x,x'])\right) \oplus f_{3L}\left(\Delta_3^{\alpha_1}([x,x'])\right) \oplus f_{3L}\left({\Delta'_3}^{\alpha_1}([x,x'])\right) \oplus$$
$$\alpha_0 \oplus \alpha_1,$$

where $\Delta_2^{\alpha_b}([x,x'])$, ${\Delta'_2}^{\alpha_b}([x,x'])$, $\Delta_3^{\alpha_b}([x,x'])$, *and* ${\Delta'_3}^{\alpha_b}([x,x'])$ *denote the values of intermediate parameters* $\Delta_2, \Delta'_2, \Delta_3$, *and* Δ'_3 *respectively when the input of the function in Figure.3 is* $([x_1^{\alpha_b}, x_2^{\alpha_b}], [x_3^{\alpha_b}, x_4^{\alpha_b}])$.

Proof. For $i = 2, 3$, we let

$$h_i([x,x'])$$
$$\stackrel{\text{def}}{=} f_i\left(\Delta_i^{\alpha_0}([x,x'])\right) \oplus f_i\left({\Delta'_i}^{\alpha_0}([x,x'])\right) \oplus f_i\left(\Delta_i^{\alpha_1}([x,x'])\right) \oplus f_i\left({\Delta'_i}^{\alpha_1}([x,x'])\right).$$

Then we will clearly show that g_2 is a periodic function step by step.

(a) $\Delta_2^{\alpha_b}([x,x']) = \Delta_2^{\alpha_b \oplus 1}([x,x'] \oplus s)$ holds for all $x, x' \in \{0,1\}^{n/2}$ the same as Lemma.1.
(b) $\Delta_3^{\alpha_b}([x,x']) = {\Delta'_3}^{\alpha_b \oplus 1}([x,x'] \oplus s)$ holds for all $x, x' \in \{0,1\}^{n/2}$. We have

$$\begin{aligned}\Delta_3^{\alpha_b}([x,x']) = [&x' \oplus \alpha_b \oplus f_{1R}[\alpha_b,\alpha_b] \oplus f_{2L}(\Delta_2^{\alpha_b}([x,x'])) \oplus f_{2R}(\Delta_2^{\alpha_b}([x,x'])),\\ &x \oplus x' \oplus f_{1L}[\alpha_b,\alpha_b] \oplus f_{1R}[\alpha_b,\alpha_b] \oplus f_{2L}(\Delta_2^{\alpha_b}([x,x']))],\\ {\Delta'_3}^{\alpha_b}([x,x']) = \Delta_3^{\alpha_b}&([x,x']) \oplus [\alpha_0 \oplus \alpha_1, 0].\end{aligned}$$

Thus we get $\Delta_3^{\alpha_b}([x,x']) = {\Delta'_3}^{\alpha_b \oplus 1}([x,x'] \oplus s)$ deriving from (a).
(c) $h_3([x,x'])$ has a period s deriving from (b).
(d) ${\Delta'_2}^{\alpha_b}([x,x']) = {\Delta'_2}^{\alpha_b \oplus 1}([x,x'] \oplus s)$ holds for all $x, x' \in \{0,1\}^{n/2}$. We have

$$\begin{aligned}{\Delta'_2}^{\alpha_b}([x,x']) =& \Delta_2^{\alpha_b}([x,x']) \oplus [f_{3R}\left(\Delta_3^{\alpha_b}([x,x'])\right) \oplus f_{3R}\left({\Delta'_3}^{\alpha_b}([x,x'])\right),\\ & f_{3L}\left(\Delta_3^{\alpha_b}([x,x'])\right) \oplus f_{3L}\left({\Delta'_3}^{\alpha_b}([x,x'])\right) \oplus f_{3R}\left(\Delta_3^{\alpha_b}([x,x'])\right)\\ & \oplus f_{3R}\left({\Delta'_3}^{\alpha_b}([x,x'])\right) \oplus \alpha_0 \oplus \alpha_1].\end{aligned}$$

Thus ${\Delta'_2}^{\alpha_b}([x,x']) = {\Delta'_2}^{\alpha_b \oplus 1}([x,x'] \oplus s)$ deriving from (a) and (b).
(e) $h_2([x,x'])$ has a period s deriving from (d).
(f) $g_2([x,x'])$ has a period s. We have

$$g_2([x,x']) = h_{2R}([x,x']) \oplus h_{3R}([x,x']) \oplus h_{3L}([x,x']) \oplus \alpha_0 \oplus \alpha_1.$$

Thus we get $g_2([x,x'])$ has a period s deriving from (c) and (e). □

Proof. (Proof of Theorem 3) When the period is not unique, that is, Simon's algorithm satisfies the approximate commitment, there is $\varepsilon(g_2, s) < \frac{1}{2}$, the probability of getting the correct s is at least $1 - \left(2\left(\frac{3}{4}\right)^c\right)^n$.

let $\mathcal{A}$ be an Adversary, we write 4-round Lai-Massey structure as 4LM. Similar to the proof of Theorem 2, We have $\mathbf{Adv}_{\text{4LM}}^{\text{qprp-cpa}}(\mathcal{A}) = 1 - \left(2\left(\frac{3}{4}\right)^c\right)^n - \frac{1}{2^{n/2}}$. If we choose $c \geq 6$, $\mathbf{Adv}_{\text{4LM}}^{\text{qprp-cpa}}(\mathcal{A}) = 1 - \frac{1}{2^{n/2}}$. □

3.3 Quantum Key-recovery Attack on 4-round Lai-Massey Structure

Figure 4 shows the 4-round Lai-Massey Structure, where f_1, f_2, f_3, f_4 are round functions and $\sigma(x_L, x_R) = (x_R, x_L \oplus x_R)$. a_i, b_i and $\Delta_i, i = 1, 2, 3, 4$ are intermediate parameters as shown in Figure 4. Let $x_i, y_i, z_i \in \{0,1\}^{n/2}, i = 1, 2, 3, 4$. Let the inputs of 4-round Lai-Massey Structure be $[x_1, x_2], [x_3, x_4]$, the outputs be $[z_1, z_2], [z_3, z_4]$, and the immediate parameters after 3-round Lai-Massey be $[y_1, y_2], [y_3, y_4]$.

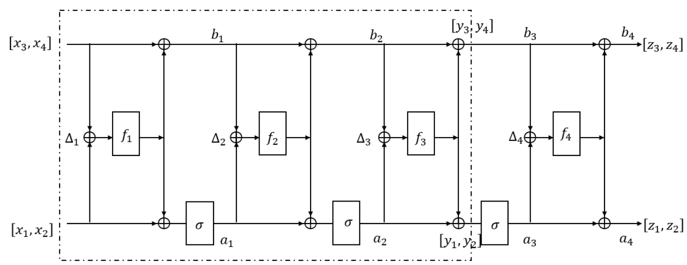

Fig. 4. 4-round Lai-Massey structure

To recover the partial key of 4-round Lai-Massey structure in CPA model, our strategy is as follows.

- Query the 4-round Lai- Massey structure with inputs $([x_1, x_2], [x_3, x_4])$s and get corresponding outputs $([z_1, z_2], [z_3, z_4])$s;
- Guess the key k_4 of f_4 as k;
- Given the value of the outputs $([z_1, z_2], [z_3, z_4])$s of 4-round Lai- Massey structure and key k, compute the value of immediate parameters after 3-round Lai-Massey $([y_1, y_2], [y_3, y_4])$s as $([y_1(k), y_2(k)], [y_3(k), y_4(k)])$s through the reverse of the last round Lai-Massey;
- Construct function $g_3(k, \cdot)$ based on $x_1, x_2, x_3, x_4, y_1(k), y_2(k), y_3(k), y_4(k)$s the same as $g1$ in Lemma 1 when attacking 3-round Lai-Massey.
- If $g_3(k, \cdot)$ is a periodic function, then k is the correct key k_4 of f_4; Or it doesn't hold by the randomness of f_4.

Thus we can recover key k_4 and $g_3(k_4, \cdot)$ is a periodic function. However, when replacing above 4-round Lai- Massey structure with random permutation, g_3 isn't a periodic any more. So we can distinguish 4-round Lai-Massey Structure from a random permutation. In the following, we show the formulation.

Theorem 4. *If $f_i, i = 1, 2, 3, 4$ are random functions, the length of the key k_4 of f_4 is m bits. We can give a quantum Grover-meet-Simon attack on 4-round Lai- Massey structure with $\sigma(x_L, x_R) = (x_R, x_L \oplus x_R)$ with $O(n2^{m/2})$ quantum queries in quantum CPA.*

We first give a lemma before proving Theorem 4.

Lemma 3. *If $f_i, i = 1, 2, 3, 4$ are random functions, the length of the key k_4 of f_4 is m bits. Let $x, x' \in \{0,1\}^{n/2}, b \in \{0,1\}$ and α_0, α_1 be arbitrary two fixed different numbers in $\{0,1\}^{n/2}$. Let $([x_1^{\alpha_b}, x_2^{\alpha_b}], [x_3^{\alpha_b}, x_4^{\alpha_b}]) \overset{def}{=} ([x \oplus \alpha_b, x'], [x, x' \oplus \alpha_b])$ being the input of 4-round Lai-Massey structure with corresponding output $([z_1^{\alpha_b}, z_2^{\alpha_b}], [z_3^{\alpha_b}, z_4^{\alpha_b}])$. And let $([y_1^{\alpha_b}(k), y_2^{\alpha_b}(k)], [y_3^{\alpha_b}(k), y_4^{\alpha_b}(k)])$ be the immediate parameters when reverse the last round of 4-round Lai-Massey with a guessed key k of f_4. We construct a function g_3 from 4-round Lai-Massey structure by letting*

$$
\begin{aligned}
g_3 : \{0,1\}^m \times \{0,1\}^n \to & \{0,1\}^{n/2} \\
k, [x, x'] \mapsto & x_1^{\alpha_0} \oplus x_2^{\alpha_0} \oplus x_3^{\alpha_0} \oplus y_1^{\alpha_0}(k) \oplus y_3^{\alpha_0}(k) \oplus \\
& x_1^{\alpha_1} \oplus x_2^{\alpha_1} \oplus x_3^{\alpha_1} \oplus y_1^{\alpha_1}(k) \oplus y_3^{\alpha_1}(k) \\
g_3(k, [x, x']) = & z_1^{\alpha_0} \oplus z_2^{\alpha_0} \oplus z_3^{\alpha_0} \oplus f_{4R}([z_1^{\alpha_0} \oplus z_3^{\alpha_0}, z_2^{\alpha_0} \oplus z_4^{\alpha_0}]) \\
& \oplus z_1^{\alpha_1} \oplus z_2^{\alpha_1} \oplus z_3^{\alpha_1} \oplus f_{4R}([z_1^{\alpha_1} \oplus z_3^{\alpha_1}, z_2^{\alpha_1} \oplus z_4^{\alpha_1}]) \\
& \oplus \alpha_0 \oplus \alpha_1 .
\end{aligned}
$$

Then $g_3(k_4, \cdot)$ is a periodic function with period $s = f_1[\alpha_0, \alpha_0] \oplus f_1[\alpha_1, \alpha_1]$ in its second component.

It is obviously that $g_3(k_4, [x, x']) = g_1([x, x'])$. By Lemma 1 we get the Lemma 3.

Proof. (Proof of Theorem 4) Given quantum oracle to g_3 , k_4 and $f_1[\alpha_0, \alpha_0] \oplus f_1[\alpha_1, \alpha_1]$ could be computed with $O(n^2)$ qubits and about $2^{n/2}$ quantum queries. The details are provided in Appendix B. And Theorem 4 is proved. □

4 Lai-Massey and Quasi-Feistel structures

4.1 Quasi-Feistel structure

Aaram Yun et.al [40] proposed the notion of quasi-Feistel structure, which is an extension of Feistel structure and Lai-Massey structure. Combiner is an important notion in quasi-Feistel structure, we briefly recall the definitions.

Definition 3. *[40](Combiner) A function $\Gamma : \mathcal{X} \times \mathcal{X} \times \mathcal{Y} \to \mathcal{X}$ is a combiner over $(\mathcal{X}, \mathcal{Y})$, if for $y \in \mathcal{X}, z \in \mathcal{Y}$, $x \mapsto \Gamma(x, y, z)$ is a permutation, and for $x \in \mathcal{X}, z \in \mathcal{Y}$, $y \mapsto \Gamma(x, y, z)$ is a permutation. We denote $\Gamma[[x \star y \mid z]] \overset{def}{=} \Gamma(x, y, z)$.*

Definition 4. *[40](b-branched, r-round quasi-Feistel structure) Let $b > 1$ and $r \geq 1$ be fixed integers, and fix a b-combiner Γ over $\mathcal{X}$. Suppose that $P, Q : \mathcal{X}^b \to \mathcal{X}^b$ are permutations. Given r functions $f_1, \ldots, f_r : \mathcal{X}^{b-1} \to \mathcal{X}$, we define a function $\Psi = \Psi_{P,Q}^{b,r}(f_1, \ldots, f_r) : \mathcal{X}^b \to \mathcal{X}^b$ as follows; for $x = (x_1, x_2, ..., x_b) \in \mathcal{X}^b$,we compute $y = \Psi(x)$ by*

1. $(z_0, z_1, \ldots, z_{b-1}) \leftarrow P(x)$,
2. $z_{i+b-1} \leftarrow \Gamma\left[\left[z_{i-1} \star f_i\left(z_i \cdots z_{i+b-2}\right) \mid z_i \cdots z_{i+b-2}\right]\right]$ *for* $i = 1, \ldots, r$.
3. $y \leftarrow Q^{-1}\left(z_r, z_{r+1}, \ldots, z_{r+b-1}\right)$.

Then Ψ is a permutation. For integer $b > 1$, we call Ψ a b-branched, r-round quasi-Feistel permutation for $f_1, \ldots, f_r$ with respect to (P, Q, Γ). If $\Psi^{b,r} : \mathrm{Func}\left(\mathcal{X}^{b-1}, \mathcal{X}\right)^r \to \mathrm{Perm}\left(\mathcal{X}^b\right)$. We call Ψ a b-branched, r-round quasi-Feistel structure for $f_1, \ldots, f_r$ with respect to (P, Q, Γ).

Note 1. Quasi-Feistel structure is *balanced* when $b = 2$, and *unbalanced* when $b > 2$. In our subsequent discussion, Feistel and Lai-Massey structures are both under the condition of $b = 2$.

Aaram Yun et.al [40] showed that Feistel and Lai-Massey structures are quasi-Feistel structures with different combiners when $b = 2$. The Lai-Massey structure version they used is given by Vaudenay [35].

Lemma 4. *[40] (Unbalanced) Feistel structure is a special case of the quasi-Feistel structure, and the combiner is $\Gamma[[x \star y \mid z]] = x \oplus y$.*

Lemma 5. *[40] Lai-Massey structure is an instance of the quasi-Feistel structure. Let G be a finite abelian group, $\sigma : G \to G$. The underlying set $\mathcal{X}$ is the group G. $\tau(x) = \sigma(x) - x$. The combiner is $\Gamma[[x \star y \mid z]] = z + \tau(z - x + y + \tau^{-1}(z - x))$.*

4.2 Lai-Massey and Quasi-Feistel structures

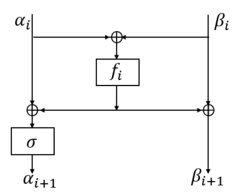

Fig. 5. The ith-round of Lai-Massey structure

First we write the combiner of Lai-Massey structure with $\sigma(x_L, x_R) = (x_R, x_L \oplus x_R)$. Note that our notation is slightly different from the above in order to match the definition of quasi-Feistel (Figure 5).

Theorem 5. *The r-round Lai-Massey structure with $\sigma(x_L, x_R) = (x_R, x_L \oplus x_R)$ can be written as:*

$$\alpha_1 \leftarrow [x_1, x_2], \beta_1 \leftarrow [x_3, x_4].$$
$$\alpha_{i+1} \leftarrow [\alpha_{iR} \oplus f_{iR}(\alpha_i \oplus \beta_i), \alpha_{iL} \oplus \alpha_{iR} \oplus f_{iL}(\alpha_i \oplus \beta_i) \oplus f_{iR}(\alpha_i \oplus \beta_i)],$$
$$\beta_{i+1} \leftarrow [\beta_{iL} \oplus f_{iL}(\alpha_i \oplus \beta_i), \beta_{iR} \oplus f_{iR}(\alpha_i \oplus \beta_i)], i = 1...r,$$
$$y_L \leftarrow \alpha_{r+1}, y_R \leftarrow \beta_{r+1},$$
Return $y = (y_L, y_R)$.

The combiner of Lai-Massey structure is $\Gamma[[x \star y \mid z]] = \sigma(x) \oplus \sigma^{-1}(y) \oplus \sigma^{-1}(z)$.

Proof. Let $x = \alpha_{i-1} \oplus \beta_{i-1}, y = f_i(\alpha_i \oplus \beta_i), z_i = \alpha_i \oplus \beta_i, z_{i+1} = \alpha_{i+1} \oplus \beta_{i+1}$. Then $\alpha_{i+1} \oplus \beta_{i+1} = [\alpha_{iR} \oplus \beta_{iL} \oplus f_{iL}(\alpha_i \oplus \beta_i) \oplus f_{iR}(\alpha_i \oplus \beta_i), \alpha_{iL} \oplus \alpha_{iR} \oplus \beta_{iR} \oplus f_{iL}(\alpha_i \oplus \beta_i)]$. Similarly, we can get $\alpha_i \oplus \beta_i$, which means that

$$\begin{aligned} z_{i+1} =& [x_L \oplus \alpha_{i-1R} \oplus f_{i-1R}(\alpha_{i-1} \oplus \beta_{i-1}) \oplus y_L \oplus y_R, \\ & \alpha_{i-1L} \oplus \beta_{i-1R} \oplus f_{i-1L}(\alpha_{i-1} \oplus \beta_{i-1}) \oplus f_{i-1R}(\alpha_{i-1} \oplus \beta_{i-1}) \oplus y_L] \\ =& [z_{iL} \oplus z_{iR} \oplus x_R \oplus y_L \oplus y_R, z_{iL} \oplus x_L \oplus x_R \oplus y_L]. \end{aligned}$$

Hence, we may define the combiner by

$$\Gamma[[x \star y \mid z]] = [z_L \oplus z_R \oplus x_R \oplus y_L \oplus y_R, z_L \oplus x_L \oplus x_R \oplus y_L] = \sigma(x) \oplus \sigma^{-1}(y) \oplus \sigma^{-1}(z).$$

We can see that $x \mapsto \Gamma[[x \star y \mid z]]$ and $y \mapsto \Gamma[[x \star y \mid z]]$ are permutations. We give the following equivalent description of Lai-Massey structure: given the input $x = (\alpha_1, \beta_1)$.

Let $H(x, y) = \left(\sigma^{-1}(x) \oplus y, x \oplus y\right)$ and we can compute $(z_0, z_1) = H(\alpha_1, \beta_1)$. We calculate $z_2, ..., z_{r+1}$ by

$$z_{i+1} = \sigma(z_{i-1}) \oplus \sigma^{-1}(f_i(z_i)) \oplus \sigma^{-1}(z_i) = \Gamma[[z_{i-1} \star f_i(z_i) \mid z_i]].$$

We compute the output $(\alpha_{r+1}, \beta_{r+1})$ by $(\alpha_{r+1}, \beta_{r+1}) = H^{-1}(z_r, z_{r+1})$. $\square$

The result of Theorem 5 is consistent with Lemma 5.

5 Quantum attacks against Quasi-Feistel structures

Since Feistel structure and Lai-Massey structure are quasi-Feistel structures, a problem of much interest is whether it is possible to directly perform quantum attacks on quasi-Feistel structures. Here we consider $b = 2$. The ith-round of quasi-Feistel structure is shown in Figure 6.

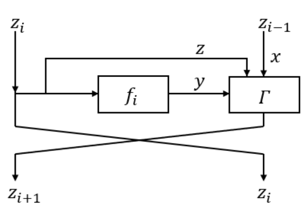

Fig. 6. ith-round of quasi-Feistel structure with $b = 2$.

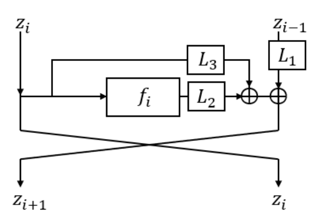

Fig. 7. ith-round of quasi-Feistel structure with linear combiner and $b = 2$.

We only consider the case where the combiner Γ of quasi-Feistel structure is linear. Let A be a matrix of linear transformation. Then we write

$$\Gamma(x, y, z) = A \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = [\, A_1 \;\; A_2 \;\; A_3 \,] \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} \overset{\text{def}}{=} L_1(x) \oplus L_2(y) \oplus L_3(z),$$

According to Definition 3, L_1, L_2 are reversible. The ith-round of quasi-Feistel structure with linear combiner and $b = 2$ is shown in Figure 7.

5.1 Quantum Chosen-Plaintext Attack Against 3-round quasi-Feistel Structure

Figure 8 shows the 3-round quasi-Feistel Structure with linear combiner and $b = 2$, where f_1, f_2, f_3 are round functions. For $b = 2$, the inputs are z_0, z_1 and the outputs are z_3, z_4 as we shown in Definition 4.

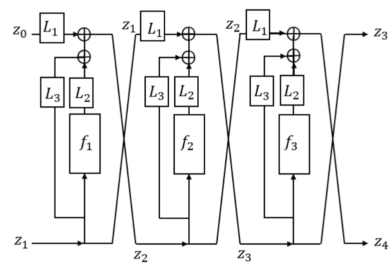

Fig. 8. 3-round quasi-Feistel structure with linear combiner and $b = 2$

Theorem 6. *If $f_i, i = 1, 2, 3$ are random functions, we can construct a quantum CPA distinguisher against 3-round balanced quasi-Feistel Structure in $O(n)$ queries by using Simon's algorithm.*

Proof. For inputs z_0, z_1, $z_i = L_1(z_{i-2}) \oplus L_2(f_{i-1}(z_{i-1})) \oplus L_3(z_{i-1}), i = 2, 3, 4$. let $z_0 = x$, $z_1 = \alpha_b$. We have

$$z_2^{\alpha_b}(x) = L_1(x) \oplus L_2(f_1(\alpha_b)) \oplus L_3(\alpha_b) = L_1[x \oplus L_1^{-1}L_2(f_1(\alpha_b)) \oplus L_1^{-1}L_3(\alpha_b)],$$

Then $z_3^{\alpha_b}(x) = L_1(\alpha_b) \oplus L_2(f_2(z_2^{\alpha_b})) \oplus L_3(z_2^{\alpha_b})$.

Lemma 6. *Let $x \in \{0,1\}^n, b \in \{0,1\}$ and α_0, α_1 be arbitrary two fixed different numbers in $\{0,1\}^n$. Let $(z_0^{\alpha_b}, z_1^{\alpha_b}) \overset{def}{=} (x, \alpha_b)$ being the input of 3-round balanced quasi-Feistel structure with corresponding output $(z_3^{\alpha_b}, z_4^{\alpha_b})$. We can construct a periodic function g_4 from 3-round balanced quasi-Feistel structure with period $s = L_1^{-1}L_2(f_1(\alpha_0)) \oplus L_1^{-1}L_2(f_1(\alpha_1)) \oplus L_1^{-1}L_3(\alpha_0) \oplus L_1^{-1}L_3(\alpha_1)$ by letting*

$$\begin{aligned} g_4 : \{0,1\}^n \to & \{0,1\}^n \\ x \mapsto & z_3^{\alpha_0}(x) \oplus z_3^{\alpha_1}(x) \\ g_4(x) = & L_1(\alpha_0) \oplus L_2(f_2(z_2^{\alpha_0}(x))) \oplus L_3(z_2^{\alpha_0}(x)) \oplus \\ & L_1(\alpha_1) \oplus L_2(f_2(z_2^{\alpha_1}(x))) \oplus L_3(z_2^{\alpha_1}(x)), \end{aligned}$$

where $z_2^{\alpha_b}(x)$ denotes the value of z_2 when the input of 3-round balanced quasi-Feistel structure is $(z_0^{\alpha_b}, z_1^{\alpha_b})$.

Proof. we show that g_4 is obviously a periodic function.

(a) $z_2^{\alpha_b}(x) = z_2^{\alpha_b \oplus 1}(x \oplus s)$ holds for all $x \in \{0,1\}^n$.
(b) $g_4(x)$ has a period s deriving from (a). □

When the period is not unique, that is, Simon's algorithm satisfies the approximate commitment, there is $\varepsilon(g_4, s) < \frac{1}{2}$, the probability of getting the correct s is at least $1 - \left(2\left(\frac{3}{4}\right)^c\right)^n$. Let A be an Adversary, we write 3-round balanced quasi-Feistel structure as 3qF. We have $\mathbf{Adv}_{\text{3qF}}^{\text{qprp-cpa}}(\mathcal{A}) = 1 - \left(2\left(\frac{3}{4}\right)^c\right)^n - \frac{1}{2^n}$. If we choose $c \geq 6$, $\mathbf{Adv}_{\text{3qF}}^{\text{qprp-cpa}}(\mathcal{A}) = 1 - \frac{1}{2^n}$. □

5.2 Quantum Chosen-Ciphertext Attack Against 4-round quasi-Feistel Structure

Figure 9 shows the attack progress of 4-round quasi-Feistel Structure with linear combiner and $b = 2$, where f_1, f_2, f_3, f_4 are round functions. $z_i, z_i', i = 0, ..., 4$ follow the definition in Definition 4.

Let the inputs of the encryption process be z_0, z_1, and the outputs be z_4, z_5. Let the inputs of the decryption process be z_4', z_5', and the outputs be z_0', z_1'. $z_4' = z_4 \oplus m_1$ and $z_5' = z_5 \oplus m_5$, where $m_j, j = 1, 2$ and z_i have the same length.

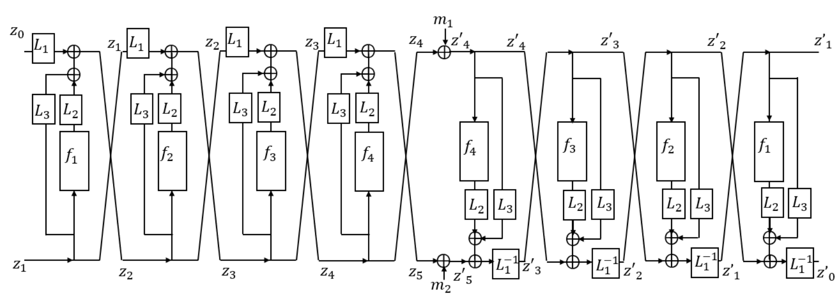

Fig. 9. The encryption and decryption progress of 4-round quasi-Feistel structure with linear combiner and $b = 2$

Theorem 7. *If $f_i, i = 1, 2, 3$ are random functions, 4-round balanced quasi-Feistel Structure can be attacked in $O(n)$ queries by using Simon's algorithm in quantum CCA.*

Proof. For the encryption process we have

$$z_i = L_1(z_{i-2}) \oplus L_2(f_{i-1}(z_{i-1})) \oplus L_3(z_{i-1}), i = 2, 3, 4, 5.$$

And for the decryption process we have

$$z_j' = L_1^{-1}[z_{j+2}' \oplus L_2(f_{j+1}(z_{j+1}')) \oplus L_3(z_{j+1}')], j = 0, 1, 2, 3.$$

Let $m_1 = 0$. Let $m_2 = L_1L_1(\alpha_0) \oplus L_1L_1(\alpha_1)$. So we can get

$$\begin{aligned}
z_3' =& z_3 \oplus L_1(\alpha_0 \oplus \alpha_1),\\
z_2' =& z_2 \oplus L_1^{-1}L_2(f_3(z_3) \oplus f_3(z_3')) \oplus L_1^{-1}L_3L_1(\alpha_0 \oplus \alpha_1),\\
z_1' =& z_1 \oplus L_1^{-1}L_2(f_2(z_2) \oplus f_2(z_2')) \oplus L_1^{-1}L_3L_1^{-1}L_2(f_3(z_3) \oplus f_3(z_3'))\oplus\\
&\alpha_0 \oplus \alpha_1 \oplus L_1^{-1}L_3L_1^{-1}L_3L_1(\alpha_0 \oplus \alpha_1).
\end{aligned}$$

Lemma 7. *Let $x \in \{0,1\}^n, b \in \{0,1\}$ and α_0, α_1 be arbitrary two fixed different numbers in $\{0,1\}^n$. Let $(z_0^{\alpha_b}, z_1^{\alpha_b}) \overset{def}{=} (x, \alpha_b)$ being the input of the function in Figure.9 based on 4-round balanced quasi-Feistel structure and its inverse with corresponding output $({z'}_0^{\alpha_b}, {z'}_1^{\alpha_b})$ when $m_1 = 0, m_2 = L_1L_1(\alpha_0) \oplus L_1L_1(\alpha_1)$. We an construct a periodic function g_5 from 4-round round balanced quasi-Feistel structure with period $s = L_1^{-1}L_2(f_1(\alpha_0)) \oplus L_1^{-1}L_2(f_1(\alpha_1)) \oplus L_1^{-1}L_3(\alpha_0) \oplus L_1^{-1}L_3(\alpha_1)$ by letting*

$$\begin{aligned}
g_5 : \{0,1\}^n \to& \{0,1\}^n\\
x \mapsto& {z'}_1^{\alpha_0}(x) \oplus {z'}_1^{\alpha_1}(x) \oplus \alpha_0 \oplus \alpha_1\\
g_5(x) =& L_1^{-1}L_2(f_2(z_2^{\alpha_0}(x)) \oplus f_2({z'}_2^{\alpha_0}(x)) \oplus f_2(z_2^{\alpha_1}(x)) \oplus f_2({z'}_2^{\alpha_1}(x)))\oplus\\
& L_1^{-1}L_3L_1^{-1}L_2(f_3(z_3^{\alpha_0}(x)) \oplus f_3({z'}_3^{\alpha_0}(x)) \oplus f_3(z_3^{\alpha_1}(x)) \oplus f_3({z'}_3^{\alpha_1}(x))),
\end{aligned}$$

where $z_2^{\alpha_b}(x), {z'}_2^{\alpha_b}(x), z_3^{\alpha_b}(x)$, and ${z'}_3^{\alpha_b}(x)$ denote the values of intermediate parameters z_2, z_2', z_3, and z_3' respectively when the input of the function in Figure.9 is $({z'}_0^{\alpha_b}, {z'}_1^{\alpha_b})$.

Proof. For $i = 2, 3$, we let $h_i'(x) \overset{\text{def}}{=} f_i(z_i^{\alpha_0}(x)) \oplus f_i\left({z'}_i^{\alpha_0}(x)\right) \oplus f_i(z_i^{\alpha_1}(x)) \oplus f_i\left({z'}_i^{\alpha_1}(x)\right)$. Then we will clearly show that g_5 is a periodic function step by step.

(a) $z_2^{\alpha_b}(x) = z_2^{\alpha_{b\oplus 1}}(x \oplus s)$ holds for all $x \in \{0,1\}^n$ the same as Lemma.6.
(b) $z_3^{\alpha_b}(x) = {z'}_3^{\alpha_{b\oplus 1}}(x \oplus s)$ holds for all $x \in \{0,1\}^n$. We have

$$\begin{aligned}
z_3^{\alpha_b}(x) &= L_1(\alpha_b) \oplus L_2(f_2(z_2^{\alpha_b})) \oplus L_3(z_2^{\alpha_b}),\\
{z'}_3^{\alpha_b}(x) &= L_1(\alpha_{b\oplus 1}) \oplus L_2(f_2(z_2^{\alpha_b})) \oplus L_3(z_2^{\alpha_b}).
\end{aligned}$$

Thus we get $z_3^{\alpha_b}(x) = {z'}_3^{\alpha_{b\oplus 1}}(x \oplus s)$ deriving from (a).
(c) $h_3'(x)$ has a period s deriving from (b).
(d) ${z'}_2^{\alpha_b}(x) = {z'}_2^{\alpha_{b\oplus 1}}(x \oplus s)$ holds for all $x \in \{0,1\}^n$. We have

$${z'}_2^{\alpha_b}(x) = z_2^{\alpha_b}(x) \oplus L_1^{-1}L_2(f_3(z_3^{\alpha_b}(x)) \oplus f_3({z'}_3^{\alpha_b}(x))) \oplus L_1^{-1}L_3L_1(\alpha_0 \oplus \alpha_1).$$

Thus ${z'}_2^{\alpha_b}(x) = {z'}_2^{\alpha_{b\oplus 1}}(x \oplus s)$ deriving from (a) and (b).
(e) $h_2'(x)$ has a period s deriving from (d).
(f) $g_5(x)$ has a period s. We have $g_5(x) = L_1^{-1}L_2(h_2'(x)) \oplus L_1^{-1}L_3L_1^{-1}L_2(h_3'(x))$. Thus we get $g_5(x)$ has a period s deriving from (c) and (e). □

Proof. (Proof of Theorem 7) Now we have $g_5(x) = g_5(x \oplus s)$ with period $s = L_1^{-1}L_2(f_1(\alpha_0)) \oplus L_1^{-1}L_2(f_1(\alpha_1)) \oplus L_1^{-1}L_3(\alpha_0) \oplus L_1^{-1}L_3(\alpha_1)$. When the period is not unique, that is, Simon's algorithm satisfies the approximate commitment, there is $\varepsilon(g_5, s) < \frac{1}{2}$, the probability of getting the correct s is at least $1 - \left(2\left(\frac{3}{4}\right)^c\right)^n$. Let A be an Adversary, we write 4-round balanced quasi-Feistel structure as 4qF. We have $\mathbf{Adv}_{4\text{qF}}^{\text{qprp-cpa}}(\mathcal{A}) = 1 - \left(2\left(\frac{3}{4}\right)^c\right)^n - \frac{1}{2^n}$. If we choose $c \geq 6$, $\mathbf{Adv}_{4\text{qF}}^{\text{qprp-cpa}}(\mathcal{A}) = 1 - \frac{1}{2^n}$. □

6 Conclusion and Discussion

There has been a discussion about whether the security of Lai-Massey structure and Feistel structure are the same. Aaram Yun et.al [40] proved that Feistel structure and Lai-Massey structure are quasi-Feistel structures and proved the birthday security of $(2b-1)$ and $(3b-2)$-round unbalanced quasi-Feistel networks with b branches against CPA and CCA attacks in classical. In [29], Luo, et al. shown that 3-round Lai-Massey structure can resist the attacks of Simon's algorithm in quantum, which is different from Feistel structure. According to Luo, this means that Lai-Massey structure and Feistel structure have a different number of rounds for CPA attacks in quantum, which also means that quasi-Feistel structures do not have similar security strength in quantum.

We first give quantum attacks on Lai-Massey structure used in FOX. We show that 3-round Lai-Massey structure can be attacked by using Simon's algorithm in $O(n)$ quantum queries against quantum CPA attacks, which is the same as Feistel structure. Then we give quantum CCA attacks on 4-round Lai-Massey structure, $O(n)$ quantum queries are sufficient to distinguish 4-round Lai-Massey structure from random permutation, which is the same as Feistel structure too. This makes us realize that quasi-Feistel structures may have similar security strength in quantum. So we give quantum attacks on quasi-Feistel structures and show that 3-round (4-round) balanced quasi-Feistel structure with linear combiners can be attacked with $O(n)$ quantum queries in quantum CPA(CCA).

For Lai-Massey structure, the version given by Vaudenay [35] used general operations in a finite group, and the version given by FOX [18] used XOR operation. In both versions, the operation used in σ and the remainder of Lai-Massey structure are the same. We consider that σ and the remainder of Lai-Massey structure use different operations, i.e., we use XOR operation in σ and general operations in the remainder of Lai-Massey structure. A problem of much interest is whether different operations can improve the security of Lai-Massey structure. If the security can be improved, another problem has been whether it is possible to resist quantum attacks as shown in [2].

Here we use quantum attacks that can make superposition queries. Quantum attacks work with classical queries and offline quantum computations can be further considered, as Bonnetain et.al did in [5].

Hosoyamada and Iwata [15] show that 4-round Feistel structure against sufficient qCPAs. More precisely, they prove that 4-round Feistel structure is secure up to $O(2^{n/3})$ quantum queries if the input length is $2n$ bits. We guess that the quantum security bound of 4-round Lai-Massey structure maybe $O(2^{n/3})$, too. But this still needs to be proved in the future.

Acknowledgement Many thanks to the reviewers for their constructive comments during the review process. One of reviewers pointed out that the combiner Γ of balanced quasi-Feistel structure in section 5 does not need to be all linear. After our verification, only L_1 needs to be linear. Specifically, if the combiner of quasi-Feistel structure is like $\Gamma(x,y,z) = L_1(x) \oplus F(y,z)$, where L_1 is linear and F is a function, there exists a quantum CPA distinguisher against 3-round balanced quasi-Feistel structure and a quantum CCA distinguisher against 4-round balanced quasi-Feistel Structure.

References

1. Skipjack and kea algorithm specifications. Tech. rep. (May 1998) 2
2. Alagic, G., Russell, A.: Quantum-secure symmetric-key cryptography based on hidden shifts. In: EUROCRYPT 2017, Proceedings, Part III. LNCS, vol. 10212, pp. 65–93 (2017), https://doi.org/10.1007/978-3-319-56617-7_3 18
3. Aragona, R., Civino, R.: On invariant subspaces in the Lai–Massey scheme and a primitivity reduction. Mediterranean Journal of Mathematics **18**(4), 1–14 (2021) 2
4. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK families of lightweight block ciphers. IACR Cryptol. ePrint Arch. p. 404 (2013), http://eprint.iacr.org/2013/404 2
5. Bonnetain, X., Hosoyamada, A., Naya-Plasencia, M., Sasaki, Y., Schrottenloher, A.: Quantum attacks without superposition queries: The offline simon's algorithm. In: ASIACRYPT 2019, Proceedings, Part I. LNCS, vol. 11921, pp. 552–583 (2019), https://doi.org/10.1007/978-3-030-34578-5_20 18
6. Brassard, G., Høyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. arXiv: Quantum Physics (2000) 25
7. Derbez, P.: Note on impossible differential attacks. In: FSE 2016. LNCS, vol. 9783, pp. 416–427. Springer (2016), https://doi.org/10.1007/978-3-662-52993-5_21 2
8. Dong, X., Wang, X.: Quantum key-recovery attack on Feistel structures. Sci. China Inf. Sci. **61**(10), 102501:1–102501:7 (2018), https://doi.org/10.1007/s11432-017-9468-y 1
9. Feistel, H.: Cryptography and computer privacy. Scientific American **228**(5), 15–23 (1973) 2
10. Fu, L., Jin, C.: Differential and linear provable security of Lai-Massey scheme (in chinese) (2013) 2
11. Fu, L., Jin, C.: Practical security evaluation against differential and linear cryptanalyses for the Lai-Massey scheme with an SPS f-function. KSII Trans. Internet Inf. Syst. **8**(10), 3624–3637 (2014), https://doi.org/10.3837/tiis.2014.10.020 2
12. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, 1996. pp. 212–219. ACM (1996), https://doi.org/10.1145/237814.237866 1, 5
13. Guo, R., Jin, C.: Impossible differential cryptanalysis on Lai-Massey scheme. Etri Journal **36**(6), 1032–1040 (2014) 2
14. Guo, T., Wang, P., Hu, L., Ye, D.: Attacks on beyond-birthday-bound macs in the quantum setting. In: PQCrypto 2021. vol. 12841, pp. 421–441. Springer (2021), https://doi.org/10.1007/978-3-030-81293-5_22 5
15. Hosoyamada, A., Iwata, T.: 4-round luby-rackoff construction is a qPRP: Tight quantum security bound. Cryptology ePrint Archive, Report 2019/243 (2019), https://ia.cr/2019/243 18
16. Isobe, T., Shibutani, K.: Improved all-subkeys recovery attacks on FOX, KATAN and SHACAL-2 block ciphers. In: FSE 2014. LNCS, vol. 8540, pp. 104–126. Springer (2014), https://doi.org/10.1007/978-3-662-46706-0_6 2
17. Ito, G., Hosoyamada, A., Matsumoto, R., Sasaki, Y., Iwata, T.: Quantum chosen-ciphertext attacks against Feistel ciphers. In: CT-RSA 2019, Proceedings. LNCS, vol. 11405, pp. 391–411. Springer (2019), https://doi.org/10.1007/978-3-030-12612-4_20 1
18. Junod, P., Vaudenay, S.: FOX : A new family of block ciphers. In: SAC 2004. LNCS, vol. 3357, pp. 114–129. Springer (2004), https://doi.org/10.1007/978-3-540-30564-4_8 2, 18

19. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: CRYPTO 2016. vol. 9815, pp. 207–237. Springer (2016), https://doi.org/10.1007/978-3-662-53008-5_8 1, 5
20. Kilian, J., Rogaway, P.: How to protect DES against exhaustive key search. In: CRYPTO '96. pp. 252–267 (1996), https://doi.org/10.1007/3-540-68697-5_20 5
21. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: ISIT 2010, Proceedings. pp. 2682–2685. IEEE (2010), https://doi.org/10.1109/ISIT.2010.5513654 1
22. Lai, X.: On the design and security of block ciphers. Ph.D. thesis, ETH Zurich, Zürich, Switzerland (1992), https://d-nb.info/920912710 2
23. Lai, X., Massey, J.L.: A proposal for a new block encryption standard. In: EUROCRYPT '90, Proceedings. LNCS, vol. 473, pp. 389–404. Springer (1990), https://doi.org/10.1007/3-540-46877-3_35 2
24. Leander, G., May, A.: Grover meets simon - quantumly attacking the fx-construction. In: ASIACRYPT 2017, Proceedings, Part II. LNCS, vol. 10625, pp. 161–178. Springer (2017), https://doi.org/10.1007/978-3-319-70697-9_6 1, 5, 25, 26
25. Li, R., You, J., Sun, B., Li, C.: Fault analysis study of the block cipher FOX64. Multim. Tools Appl. **63**(3), 691–708 (2013), https://doi.org/10.1007/s11042-011-0895-x 2
26. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput. **17**(2), 373–386 (1988), https://doi.org/10.1137/0217022 2
27. Luo, Y., Lai, X., Gong, Z.: Pseudorandomness analysis of the (extended) Lai-Massey scheme. Inf. Process. Lett. **111**(2), 90–96 (2010), https://doi.org/10.1016/j.ipl.2010.10.012 2
28. Luo, Y., Lai, X., Hu, J.: The pseudorandomness of many-round Lai-Massey scheme. J. Inf. Sci. Eng. **31**(3), 1085–1096 (2015), http://www.iis.sinica.edu.tw/page/jise/2015/201505_17.html 2
29. Luo, Y., Yan, H., Wang, L., Hu, H., Lai, X.: Study on block cipher structures against simon's quantum algorithm (in chinese). Journal of Cryptologic Research **6**(5), 561–573 (2019) 1, 3, 18
30. Miyaguchi, S.: The FEAL-8 cryptosystem and a call for attack. In: CRYPTO '89, Proceedings. LNCS, vol. 435, pp. 624–627. Springer (1989), https://doi.org/10.1007/0-387-34805-0_59 2
31. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science, 1994. pp. 124–134. IEEE Computer Society (1994), https://doi.org/10.1109/SFCS.1994.365700 1
32. Simon, D.R.: On the power of quantum computation. SIAM J. Comput. **26**(5), 1474–1483 (1997), https://doi.org/10.1137/S0097539796298637 1, 4
33. U.S. Department of Commerce/National Institute of Standards, Technology: Data encryption standard (des) (1977) 2
34. Sui, H., Wu, W., Zhang, L.: Round security of the Lai-Massey structure (in chinese). Journal of Cryptologic Research **1**, 28–40 (2014) 2
35. Vaudenay, S.: On the Lai-Massey scheme. In: ASIACRYPT '99, Proceedings. LNCS, vol. 1716, pp. 8–19. Springer (1999), https://doi.org/10.1007/978-3-540-48000-6_2 2, 13, 18
36. Wu, W., Wei, H.: Collision-integral attack of reduced-round FOX (in chinese). Acta Electronica Sinica (2005) 2
37. Wu, W., Zhang, W., Feng, D.: Improved integral cryptanalysis of FOX block cipher. IACR Cryptol. ePrint Arch. p. 292 (2005), http://eprint.iacr.org/2005/292 2

38. Wu, W., Zhang, W., Feng, D.: Integral cryptanalysis of reduced FOX block cipher. In: ICISC 2005. LNCS, vol. 3935, pp. 229–241. Springer (2005), https://doi.org/10.1007/11734727_20 2
39. Wu, Z., Lai, X., Zhu, B., Luo, Y.: Impossible differential cryptanalysis of FOX. IACR Cryptol. ePrint Arch. p. 357 (2009), http://eprint.iacr.org/2009/357 2
40. Yun, A., Park, J.H., Lee, J.: On Lai-Massey and quasi-Feistel ciphers. Des. Codes Cryptogr. **58**(1), 45–72 (2011), https://doi.org/10.1007/s10623-010-9386-8 2, 12, 13, 18
41. Zhang, L., Wu, W.: Pseudorandomness and super pseudorandomness on the unbalanced Feistel networks with contracting functions (in chinese). CHINESE JOURNAL OF COMPU TERS **32**(7), 1320–1330 (2009) 2

A Intermediate Parameters in the Decryption Process of 4-round Lai-Massey Structure in Section 3.2

For the decryption process of 4-round Lai-Massey structure shown in the figure 3, we write the inputs as $[z_1, z_2], [z_3, z_4]$ and the outputs as $[x'_1, x'_2], [x'_3, x'_4]$. Intermediate parameters are as follows.

$$
\begin{aligned}
a'_4 =&[z_1, z_2], b'_4 = [z_3, z_4],\\
a'_3 =&[z_1 \oplus f_{4L}(\Delta'_4), z_2 \oplus f_{4R}(\Delta'_4)], b'_3 = [z_3 \oplus f_{4L}(\Delta'_4), z_4 \oplus f_{4R}(\Delta'_4)],\\
a'_2 =&[z_1 \oplus z_2 \oplus f_{3L}(\Delta'_3) \oplus f_{4L}(\Delta'_4) \oplus f_{4R}(\Delta'_4), z_1 \oplus f_{3R}(\Delta'_3) \oplus f_{4L}(\Delta'_4)],\\
b'_2 =&[z_3 \oplus f_{3L}(\Delta'_3) \oplus f_{4L}(\Delta'_4), z_4 \oplus f_{3R}(\Delta'_3) \oplus f_{4R}(\Delta'_4)],\\
a'_1 =&[z_2 \oplus f_{2L}(\Delta'_2) \oplus f_{3L}(\Delta'_3) \oplus f_{3R}(\Delta'_3) \oplus f_{4R}(\Delta'_4),\\
&z_1 \oplus z_2 \oplus f_{2R}(\Delta'_2) \oplus f_{3L}(\Delta'_3) \oplus f_{4L}(\Delta'_4) \oplus f_{4R}(\Delta'_4)],\\
b'_1 =&[z_3 \oplus f_{2L}(\Delta'_2) \oplus f_{3L}(\Delta'_3) \oplus f_{4L}(\Delta'_4), z_4 \oplus f_{2R}(\Delta'_2) \oplus f_{3R}(\Delta'_3) \oplus f_{4R}(\Delta'_4)],
\end{aligned}
$$

where

$$
\begin{aligned}
\Delta'_4 =&[z_1 \oplus z_3, z_2 \oplus z_4],\\
\Delta'_3 =&[z_1 \oplus z_2 \oplus z_3 \oplus f_{4R}(\Delta'_4), z_1 \oplus z_4 \oplus f_{4L}(\Delta'_4) \oplus f_{4R}(\Delta'_4)],\\
\Delta'_2 =&[z_2 \oplus z_3 \oplus f_{3R}(\Delta'_3) \oplus f_{4L}(\Delta'_4) \oplus f_{4R}(\Delta'_4),\\
&z_1 \oplus z_2 \oplus z_4 \oplus f_{3L}(\Delta'_3) \oplus f_{3R}(\Delta'_3) \oplus f_{4L}(\Delta'_4)],\\
\Delta'_1 =&[z_1 \oplus z_3 \oplus f_{2R}(\Delta'_2) \oplus f_{3L}(\Delta'_3) \oplus f_{3R}(\Delta'_3),\\
&z_2 \oplus z_4 \oplus f_{2L}(\Delta'_2) \oplus f_{2R}(\Delta'_2) \oplus f_{3L}(\Delta'_3)].
\end{aligned}
$$

Proof. Let $a'_4 = [z_1, z_2], b'_4 = [z_3, z_4]$. Intermediate parameters $a_i, b_i, \Delta_j, i = 1, 2, 3, 4$ are the same as section 3.1 and section 3.2.

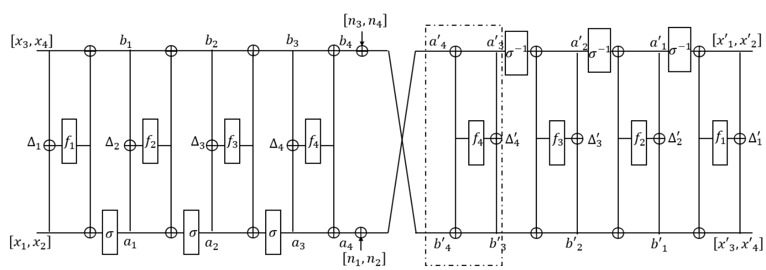

Fig. 10. The fourth round of the decryption progress of 4-round Lai-Massey structure

Lemma 8. *For the fourth round of the decryption progress of 4-round Lai-Massey structure (Figure 10), intermediate parameters Δ'_4, a'_3, b'_3 can be expressed as:*

$$\Delta'_4 =[z_1 \oplus z_3, z_2 \oplus z_4],$$

$$a_3' = [z_1 \oplus f_{4L}(\Delta_4'), z_2 \oplus f_{4R}(\Delta_4')],$$
$$b_3' = [z_3 \oplus f_{4L}(\Delta_4'), z_4 \oplus f_{4R}(\Delta_4')].$$

Proof. According to the decryption progress of 4-round Lai-Massey structure, we can get the following system of equations

$$\begin{cases} \Delta_4' = a_3' \oplus b_3', \\ a_3' \oplus f_4(\Delta_4') = a_4', \\ b_3' \oplus f_4(\Delta_4') = b_4'. \end{cases}$$

Solving the system of equations gives the result.

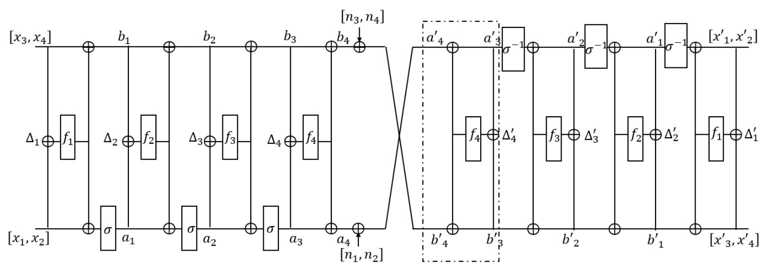

Fig. 11. The third round of the decryption progress of 4-round Lai-Massey structure

Lemma 9. *For the third round of the decryption progress of 4-round Lai-Massey structure (Figure 11), intermediate parameters Δ_3', a_2', b_2' can be expressed as:*

$$\Delta_3' = a_2' \oplus b_2' = [z_1 \oplus z_2 \oplus z_3 \oplus f_{4R}(\Delta_4'), z_1 \oplus z_4 \oplus f_{4L}(\Delta_4') \oplus f_{4R}(\Delta_4')],$$
$$a_2' = [z_1 \oplus z_2 \oplus f_{3L}(\Delta_3') \oplus f_{4L}(\Delta_4') \oplus f_{4R}(\Delta_4'), z_1 \oplus f_{3R}(\Delta_3') \oplus f_{4L}(\Delta_4')],$$
$$b_2' = [z_3 \oplus f_{3L}(\Delta_3') \oplus f_{4L}(\Delta_4'), z_4 \oplus f_{3R}(\Delta_3') \oplus f_{4R}(\Delta_4')].$$

Proof. According to the decryption progress of 4-round Lai-Massey structure, we can get the following system of equations

$$\begin{cases} \Delta_3' = a_2' \oplus b_2', \\ a_3' = [a_{2R}' \oplus f_{3R}(\Delta_3'), a_{2L}' \oplus a_{2R}' \oplus f_{3L}(\Delta_3') \oplus f_{3R}(\Delta_3')], \\ b_3' = [b_{2L}' \oplus f_{3L}(\Delta_3'), b_{2R}' \oplus f_{3R}(\Delta_3')]. \end{cases}$$

From Lemma 8 we can get:

$$\begin{cases} a_{2R}' \oplus f_{3R}(\Delta_3') = z_1 \oplus f_{4L}(\Delta_4'), \\ a_{2L}' \oplus a_{2R}' \oplus f_{3L}(\Delta_3') \oplus f_{3R}(\Delta_3') = z_2 \oplus f_{4R}(\Delta_4'), \\ b_{2L}' \oplus f_{3L}(\Delta_3') = z_3 \oplus f_{4L}(\Delta_4'), \\ b_{2R}' \oplus f_{3R}(\Delta_3') = z_4 \oplus f_{4R}(\Delta_4'). \end{cases}$$

Solving the system of equations gives the result.

Lemma 10. *For the second round of the decryption progress of 4-round Lai-Massey structure, intermediate parameters Δ_2', a_1', b_1' can be expressed as:*

$$\begin{aligned}\Delta_2' =&[z_2 \oplus z_3 \oplus f_{3R}(\Delta_3') \oplus f_{4L}(\Delta_4') \oplus f_{4R}(\Delta_4'),\\ &z_1 \oplus z_2 \oplus z_4 \oplus f_{3L}(\Delta_3') \oplus f_{3R}(\Delta_3') \oplus f_{4L}(\Delta_4')],\\ a_1' =&[z_2 \oplus f_{2L}(\Delta_2') \oplus f_{3L}(\Delta_3') \oplus f_{3R}(\Delta_3') \oplus f_{4R}(\Delta_4'),\\ &z_1 \oplus z_2 \oplus f_{2R}(\Delta_2') \oplus f_{3L}(\Delta_3') \oplus f_{4L}(\Delta_4') \oplus f_{4R}(\Delta_4')],\\ b_1' =&[z_3 \oplus f_{2L}(\Delta_2') \oplus f_{3L}(\Delta_3') \oplus f_{4L}(\Delta_4'), z_4 \oplus f_{2R}(\Delta_2') \oplus f_{3R}(\Delta_3') \oplus f_{4R}(\Delta_4')].\end{aligned}$$

Proof. According to the decryption progress of 4-round Lai-Massey structure, we can get the following system of equations

$$\begin{cases}\Delta_2' = a_1' \oplus b_1',\\ a_2' = [a_{1R}' \oplus f_{2R}(\Delta_2'), a_{1L}' \oplus a_{1R}' \oplus f_{2L}(\Delta_2') \oplus f_{2R}(\Delta_2')],\\ b_2' = [b_{1L}' \oplus f_{2L}(\Delta_2'), b_{1R} \oplus f_{2R}(\Delta_2')].\end{cases}$$

From Lemma 9 we have

$$\begin{cases}a_{1R}' \oplus f_{2R}(\Delta_2') = z_1 \oplus z_2 \oplus f_{3L}(\Delta_3') \oplus f_{4L}(\Delta_4') \oplus f_{4R}(\Delta_4'),\\ a_{1L}' \oplus a_{1R}' \oplus f_{2L}(\Delta_2') \oplus f_{2R}(\Delta_2') = z_1 \oplus f_{3R}(\Delta_3') \oplus f_{4L}(\Delta_4'),\\ b_{1L}' \oplus f_{2L}(\Delta_2') = z_3 \oplus f_{3L}(\Delta_3') \oplus f_{4L}(\Delta_4'),\\ b_{1R}' \oplus f_{2R}(\Delta_2') = z_4 \oplus f_{3R}(\Delta_3') \oplus f_{4R}(\Delta_4').\end{cases}$$

Solving the system of equations gives the result.

Lemma 11. *For the first round of the decryption progress of 4-round Lai-Massey structure, intermediate parameters $\Delta_1', [x_1', x_2'], [x_3', x_4']$ can be expressed as:*

$$\begin{aligned}\Delta_1' =&[z_1 \oplus z_3 \oplus f_{2R}(\Delta_2') \oplus f_{3L}(\Delta_3') \oplus f_{3R}(\Delta_3'),\\ &z_2 \oplus z_4 \oplus f_{2L}(\Delta_2') \oplus f_{2R}(\Delta_2') \oplus f_{3L}(\Delta_3')],\\ [x_1', x_2'] =&[z_1 \oplus f_{1L}(\Delta_1') \oplus f_{2L}(\Delta_2') \oplus f_{2R}(\Delta_2') \oplus f_{3R}(\Delta_3') \oplus f_{4L}(\Delta_4'),\\ &z_2 \oplus f_{1R}(\Delta_1') \oplus f_{2L}(\Delta_2') \oplus f_{3L}(\Delta_3') \oplus f_{3R}(\Delta_3') \oplus f_{4R}(\Delta_4'),\\ [x_3', x_4'] =&[z_3 \oplus f_{1L}(\Delta_1') \oplus f_{2L}(\Delta_2') \oplus f_{3L}(\Delta_3') \oplus f_{4L}(\Delta_4'),\\ &z_4 \oplus f_{1R}(\Delta_1') \oplus f_{2R}(\Delta_2') \oplus f_{3R}(\Delta_3') \oplus f_{4R}(\Delta_4')].\end{aligned}$$

Proof. According to the decryption progress of 4-round Lai-Massey structure, we can get the following system of equations

$$\begin{cases}\Delta_1' = [x_1', x_2'] \oplus [x_3', x_4'],\\ a_1' = [x_2' \oplus f_{1R}(\Delta_1'), x_1' \oplus x_2' \oplus f_{1L}(\Delta_1') \oplus f_{1R}(\Delta_1')],\\ b_1' = b_0' \oplus f_1(\Delta_1') = [x_3' \oplus f_{1L}(\Delta_1'), x_4' \oplus f_{1R}(\Delta_1')].\end{cases}$$

From Lemma 11 we have

$$\begin{cases}x_2' \oplus f_{1R}(\Delta_1') = z_2 \oplus f_{2L}(\Delta_2') \oplus f_{3L}(\Delta_3') \oplus f_{3R}(\Delta_3') \oplus f_{4R}(\Delta_4'),\\ x_1' \oplus x_2' \oplus f_{1L}(\Delta_1') \oplus f_{1R}(\Delta_1') = z_1 \oplus z_2 \oplus f_{2R}(\Delta_2') \oplus f_{3L}(\Delta_3') \oplus f_{4L}(\Delta_4') \oplus f_{4R}(\Delta_4'),\\ x_3' \oplus f_{1L}(\Delta_1') = z_3 \oplus f_{2L}(\Delta_2') \oplus f_{3L}(\Delta_3') \oplus f_{4L}(\Delta_4'),\\ x_4' \oplus f_{1R}(\Delta_1') = z_4 \oplus f_{2R}(\Delta_2') \oplus f_{3R}(\Delta_3') \oplus f_{4R}(\Delta_4').\end{cases}$$

Solving the system of equations gives the result.

B Proof of Theorem 4

Proof. First, we introduce a Theorem and a Lemma for subsequent proofs.

Theorem 8. *[6] (Brassard, Hoyer, Mosca and Tapp). Let $\mathcal{A}$ be any quantum algorithm on q qubits that uses no measurement. Let $\mathcal{B} : \mathbb{F}_2^q \to \{0,1\}$ be a function that classifies outcomes of $\mathcal{A}$ as good or bad. Let $p > 0$ be the initial success probability that a measurement of $\mathcal{A}|0\rangle$ is good. Set $t = \lceil \frac{\pi}{4\theta} \rceil$, where θ is defined via $sin^2(\theta) = p$. Moreover, define the unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_{\mathcal{B}}$, where the operator $S_{\mathcal{B}}$ changes the sign of the good state:*

$$|x\rangle \mapsto \begin{cases} -|x\rangle & \text{if } \mathcal{B}(x) = 1 \\ \ \ |x\rangle & \text{if } \mathcal{B}(x) = 0 \end{cases}$$

while S_0 changes the sign of the amplitude only for the zero state $|0\rangle$. Then after the computation of $Q^t\mathcal{A}|0\rangle$, a measurement yields well with probability a least $\max\{1 - p, p\}$.

Lemma 12. *[24] Any state $|z_i\rangle = (-1)^{\langle u_i, x_i\rangle}|u_i\rangle$ is proper with probability at least $\frac{1}{2}$. Any set of $\ell = 2(n+\sqrt{n})$ states contains at least $n-1$ proper states with probability greater than $\frac{4}{5}$.*

Let U_h be a quantum oracle as $|x_1, ..., x_l, 0\rangle \mapsto |x_1, ..., x_l, h(x_1, ..., x_l)\rangle$. If k_4 guessed right, then $g_3(k_4, [x, x']) = g_3(k_4, [x, x'] \oplus s)$. Let $h : \mathbb{F}_2^m \times \mathbb{F}_2^{n^l} \to \mathbb{F}_2^{(n/2)^l}$ with: $(k, [x_1, x_1'], ..., [x_l, x_l']) \mapsto g_3(k, [x_1, x_1'])||...||g_3(k, [x_l, x_l'])$. Then we can construct the following quantum algorithm $\mathcal{A}$:

1. Initializing a $m + nl + nl/2$-qubit register $|0\rangle^{\otimes m+nl+nl/2}$.
2. Apply Hadamard transformation $H^{\otimes m+nl}$ to the first $m+nl$ qubits to obtain quantum superposition

$$H^{\otimes m+nl}|0\rangle = \frac{1}{\sqrt{2^{m+nl}}} \sum_{k\in\mathbb{F}_2^m, [x_1,x_1'],...,[x_l,x_l']\in\mathbb{F}_2^n} |k\rangle|[x_1, x_1']\rangle...|[x_l, x_l']\rangle|0, ..., 0\rangle.$$

3. Applying U_h:

$$\frac{1}{\sqrt{2^{m+nl}}} \sum_{k\in\mathbb{F}_2^m, [x_1,x_1'],...,[x_l,x_l']\in\mathbb{F}_2^n} |k\rangle|[x_1, x_1']\rangle...|[x_l, x_l']\rangle|h(k, [x_1, x_1'], ..., [x_l, x_l'])\rangle.$$

4. Apply Hadamard transformation to the qubits $|[x_1, x_1']\rangle...|[x_l, x_l']\rangle$:

$$\begin{aligned}|\varphi\rangle =& \frac{1}{\sqrt{2^{m+2nl}}} \sum_{k\in\mathbb{F}_2^m, u_1,...,u_l, [x_1,x_1'],...,[x_l,x_l']\in\mathbb{F}_2^n} |k\rangle(-1)^{\langle u_1, [x_1,x_1']\rangle}|u_1\rangle \cdots (-1)^{\langle u_1, [x_l,x_l']\rangle} \\ & |u_l\rangle|h(k, [x_1, x_1'], ..., [x_l, x_l'])\rangle.\end{aligned}$$

If k_4 is guessed right, the period s will orthogonal to all the $u_i, i = 1...l$. From lemma 12, we choose $l = 2(n + \sqrt{n})$. Then we can construct a classifier $\mathcal{B} : \mathbb{F}_2^{m+nl} \to \{0,1\}$ with a good subspace $|\varphi_1\rangle$ and a bad subspace $|\varphi_0\rangle$ as Definition 5. $|x\rangle$ in the good subspace if $\mathcal{B}(x) = 1$. Let $|\varphi\rangle = |\varphi_1\rangle + |\varphi_0\rangle$. $|\varphi_1\rangle$ is the sum of basis states for which the right k_4. We can check it by whether $g_3(k, [x, x']) = g_3(k, [x, x'] \oplus s)$:

Definition 5. *Let $\tilde{U} = \langle u_1, ..., u_l\rangle$ be the linear span of all u_i. We define Classifier $\mathcal{B} : \mathbb{F}_2^{m+nl} \mapsto \{0,1\}$ which maps $(k, u_1, ..., u_l) \mapsto \{0,1\}$.*

1. *If $\dim(\tilde{U}) \neq n - 1$, output 0. Otherwise compute the unique period s by using Lemma 2 in [24].*
2. *For random $[x, x']$, if $g_3(k, [x, x']) = g_3(k, [x, x'] \oplus s)$, then output 1, otherwise output 0.*

Mearsure $|\varphi\rangle$ and the initial probability of the good state is:

$$p = \Pr[|k\rangle|u_1\rangle...|u_l\rangle \text{ is good}] = \Pr[k = k_4] \cdot \Pr[\mathcal{B}(k, u_1, ..., u_l) = 1 | k = k_4] \approx \frac{1}{2^n}.$$

Set $t = \lceil \frac{\pi}{4\theta} \rceil$, where θ is defined via $sin^2(\theta) = p$. Then $\theta \approx \arcsin(2^{-n/2}) \approx 2^{-n/2}$, $t \approx \lceil \frac{\pi}{4 \times 2^{-n/2}} \rceil \approx 2^{n/2}$. We define the unitary operator $Q = -\mathcal{A} S_0 \mathcal{A}^{-1} S_{\mathcal{B}}$, where the operator $S_{\mathcal{B}}$ changes the sign of the good state:

$$|k\rangle|u_1\rangle...|u_l\rangle \mapsto \begin{cases} -|k\rangle|u_1\rangle...|u_l\rangle & \text{if } B(k, u_1, ..., u_l) = 1 \\ |k\rangle|u_1\rangle...|u_l\rangle & \text{if } B(k, u_1, ..., u_l) = 0. \end{cases}$$

S_0 changes the sign of the amplitude only for the zero state $|0\rangle$. Then after the computation of $Q^t \mathcal{A}|0\rangle$, according to the Theorem 8, a measurement yields good with probability a least $\max\{1 - p, p\} \approx 1 - \frac{1}{2^n}$.