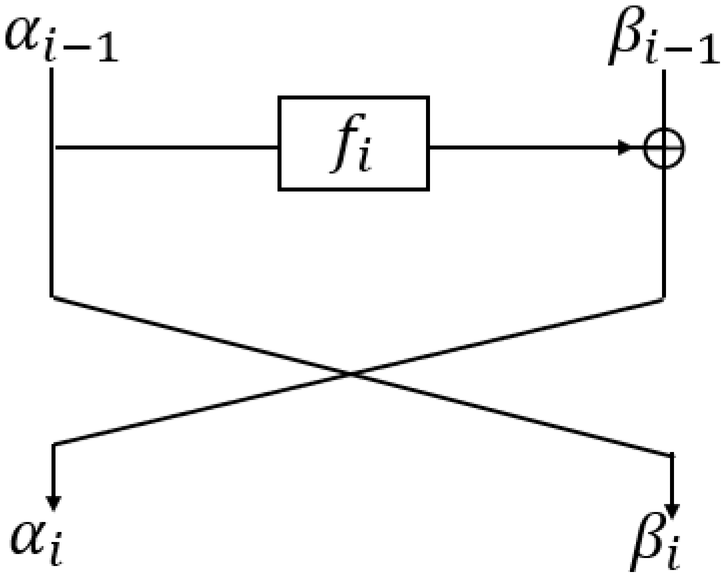
Quantum Attacks on Lai-Massey Structure

Shuping Mao, Tingting Guo, Peng Wang, Lei Hu

State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing, China

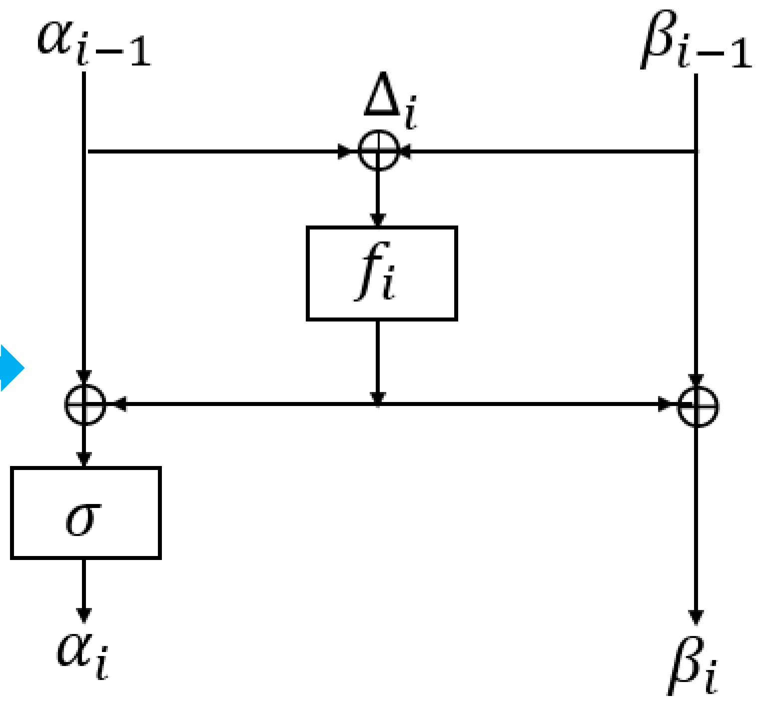
PQCrypto, September 28–30, 2022



Feistel structure

the same security

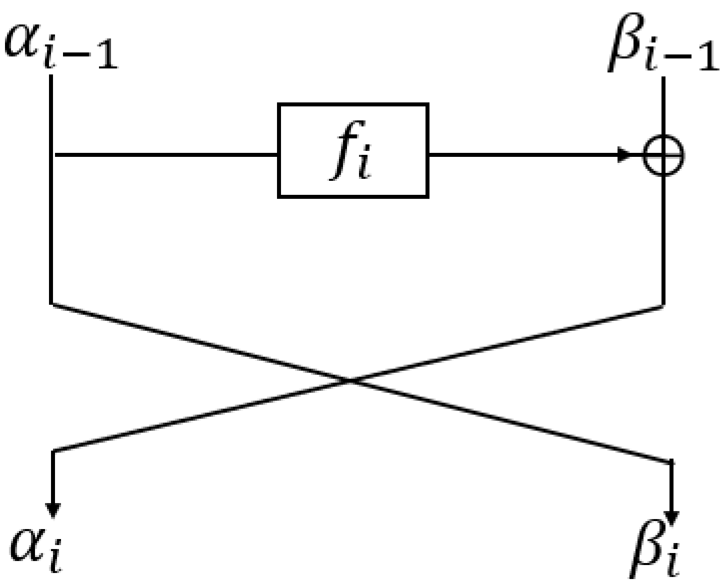
In classical



Lai-Massey structure

quasi-Feistel structure

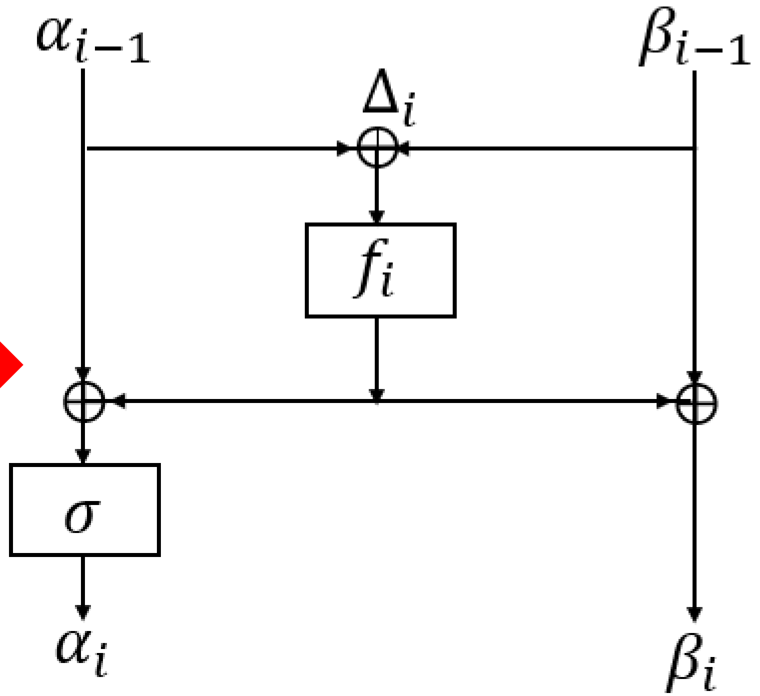
Aaram Yun et al.



Feistel structure

different security

In quantum?



Lai-Massey structure

Gembu Ito: 3 rounds Feistel structure can be attacked by using Simon's algorithm in quantum

?

?

?

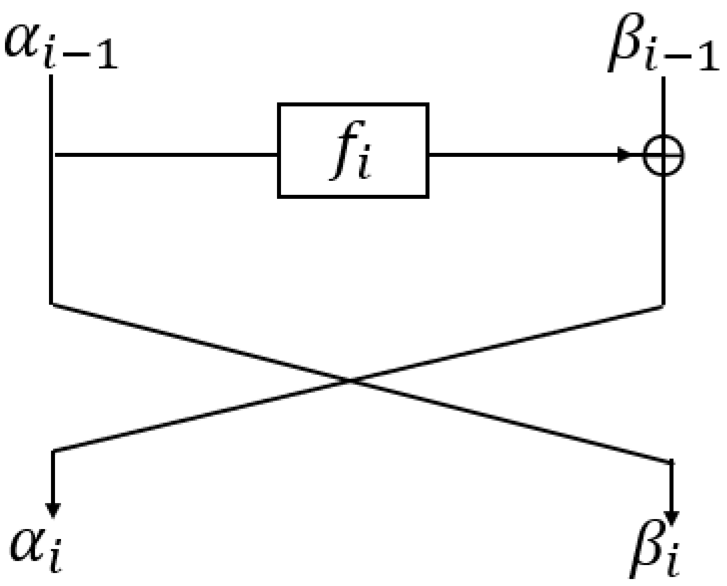
quasi-Feistel structure in quantum

Luo et al. : 3-round Lai-Massey structure can resist quantum attacks of Simon's algorithm

Question:

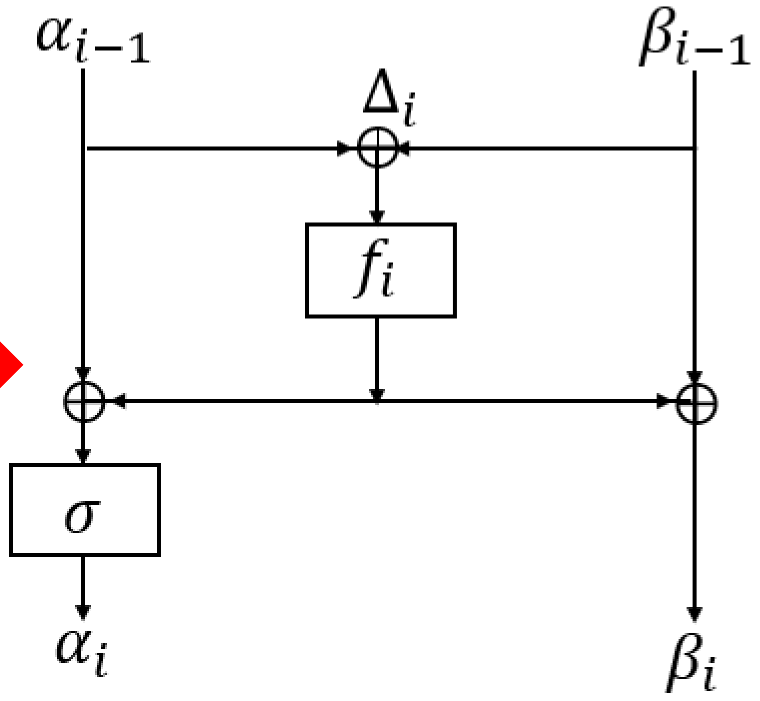
- Do Lai-Massey structure and Feistel structure have the same number of rounds that can be attacked in quantum?

- Can the attacks be extended to quasi-Feistel structures?



Feistel structure

different security ? In quantum



Lai-Massey structure

Gembu Ito: 3 rounds Feistel can be attacked by using Simon's algorithm in quantum

?

?

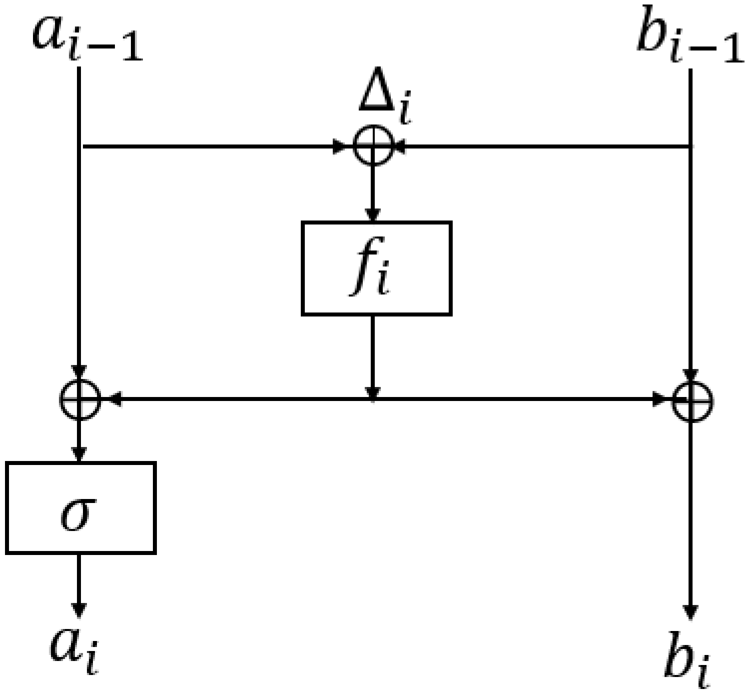
?

quasi-Feistel structure in quantum

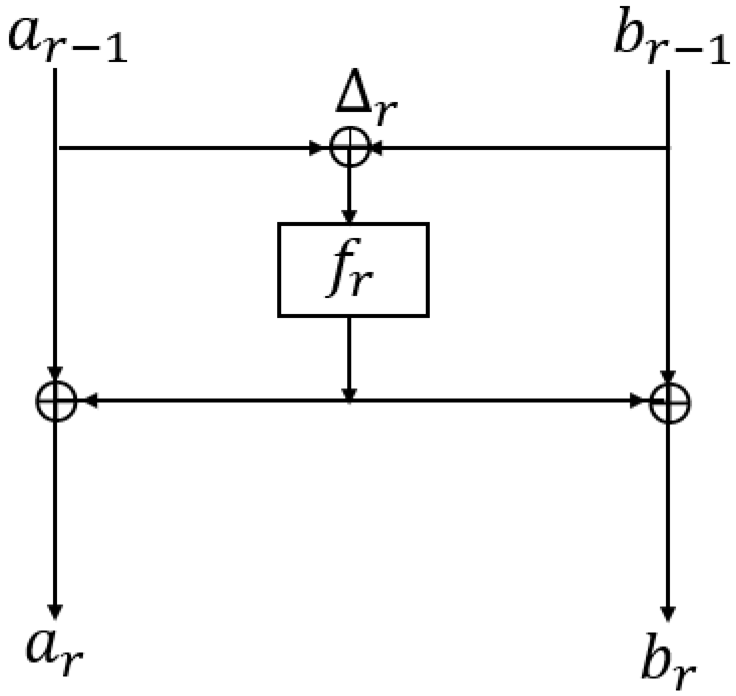
Luo et al. : 3-round Lai-Massey structure can resist quantum attacks of Simon's algorithm

Quantum Attacks on Lai-Massey Structures

r-round Lai-Massey structure: $(a_r, b_r) = \mathrm{LM}'_r \circ \mathrm{LM}_{r-1} \circ \cdots \circ \mathrm{LM}_1$



The ith-round of Lai-Massey structure (LM_i)



The rth-round of Lai-Massey structure (LM'_r)

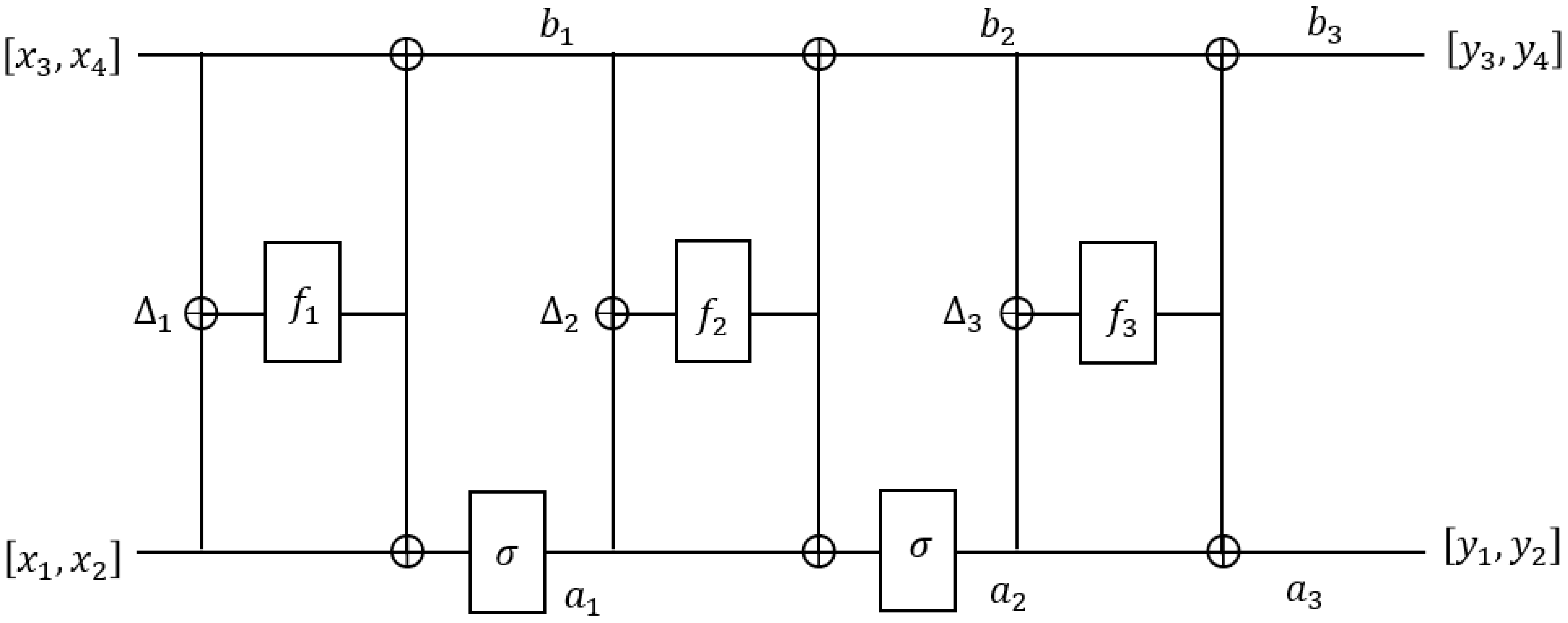
σ has the orthomorphism property: σ and $x \mapsto \sigma(x) - x$ are both permutations.

The instantiated Lai-Massey structure used in **FOX**:

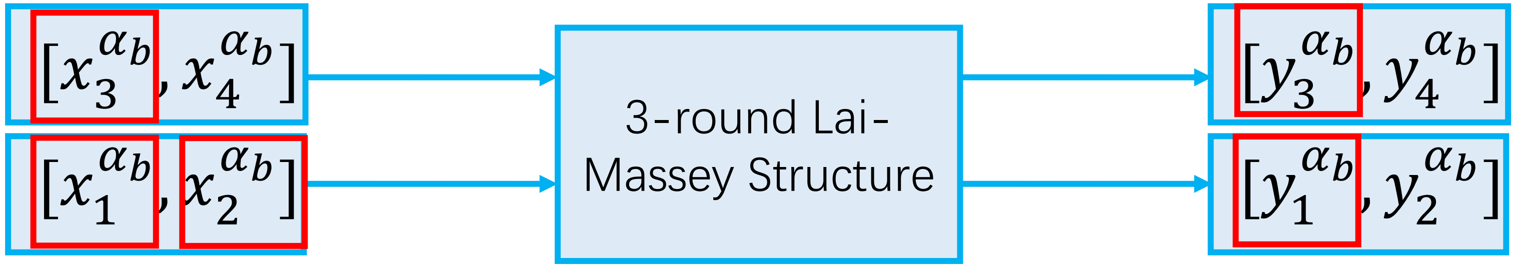
$$\sigma(x_L, x_R) = (x_R, x_L \oplus x_R)$$

$[a, b] \in \{0,1\}^n$: a, b represent the highest $n/2$ bits and the lowest $n/2$ bits respectively

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



- Let $x, x' \in \{0,1\}^{n/2}$. $([x_1^{\alpha_b}, x_2^{\alpha_b}], [x_3^{\alpha_b}, x_4^{\alpha_b}]) \overset{\text{def}}{=} ([x \oplus \alpha_b, x'], [x, x' \oplus \alpha_b])$.

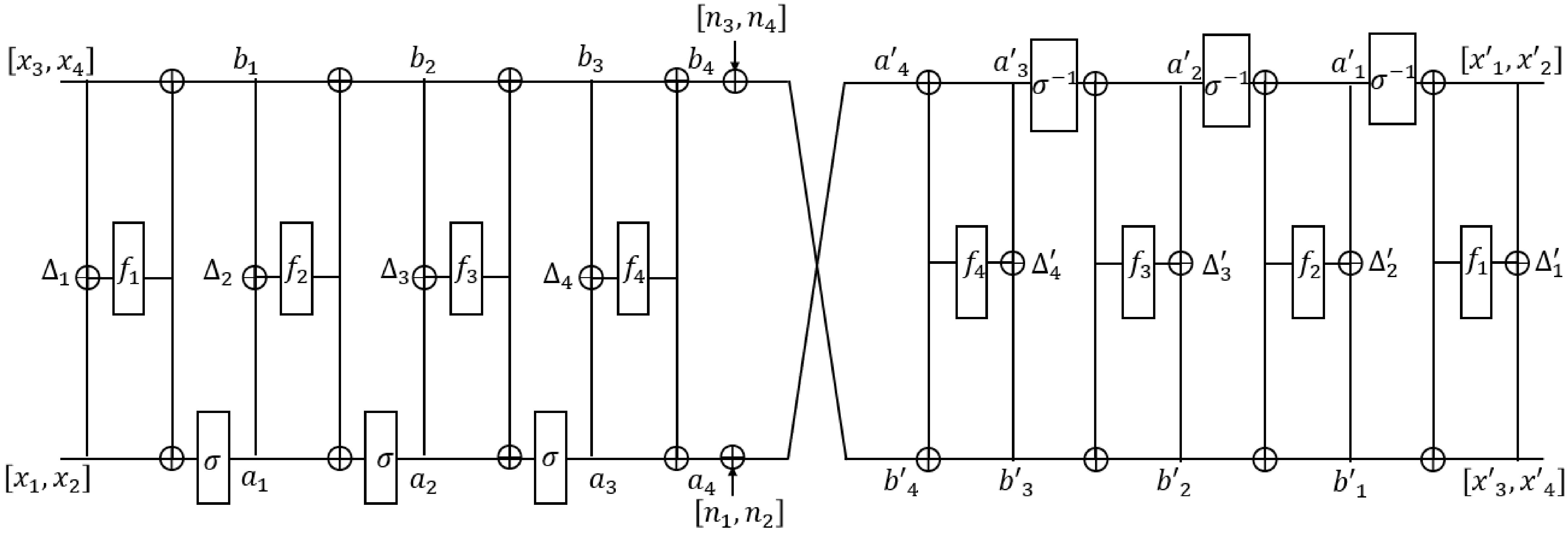


- We can construct a periodic function g_1 with period $s = f_1[\alpha_0, \alpha_0] \oplus f_1[\alpha_1, \alpha_1]$ by letting

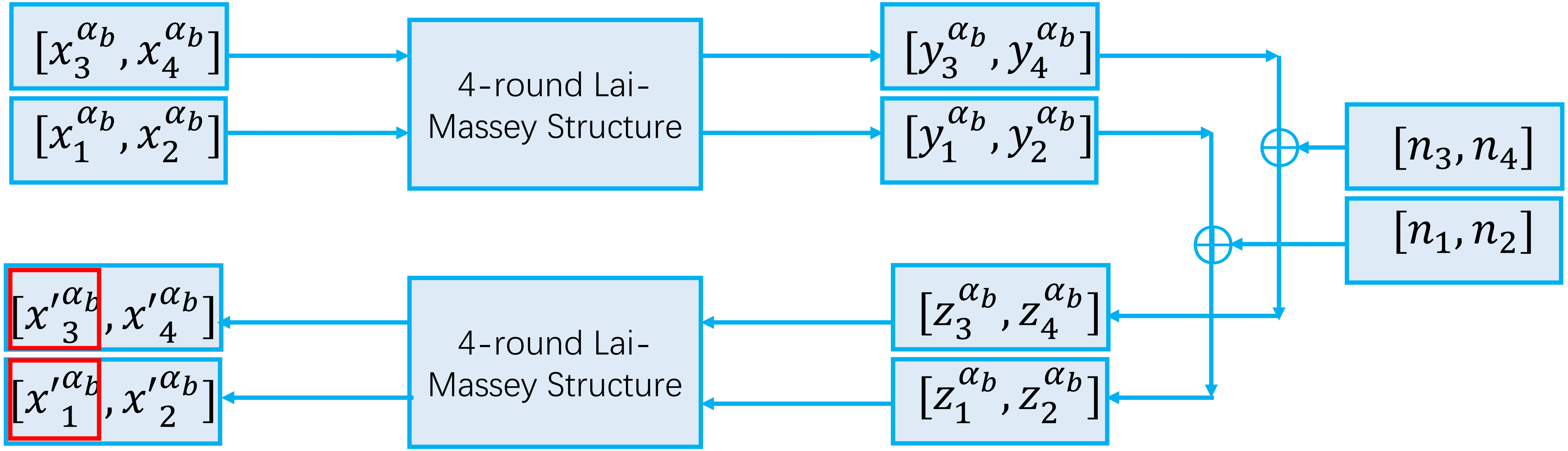
$$g_1 \mapsto x_1^{\alpha_0} \oplus x_2^{\alpha_0} \oplus x_3^{\alpha_0} \oplus y_1^{\alpha_0} \oplus y_3^{\alpha_0} \oplus \\ x_1^{\alpha_1} \oplus x_2^{\alpha_1} \oplus x_3^{\alpha_1} \oplus y_1^{\alpha_1} \oplus y_3^{\alpha_1}$$

- we can construct a quantum CPA distinguisher by using Simon' algorithm in $O(n)$ quantum queries.

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



- Let $x, x' \in \{0,1\}^{n/2}$. $([x_1^{\alpha_b}, x_2^{\alpha_b}], [x_3^{\alpha_b}, x_4^{\alpha_b}]) \overset{\text{def}}{=} ([x \oplus \alpha_b, x'], [x, x' \oplus \alpha_b])$.



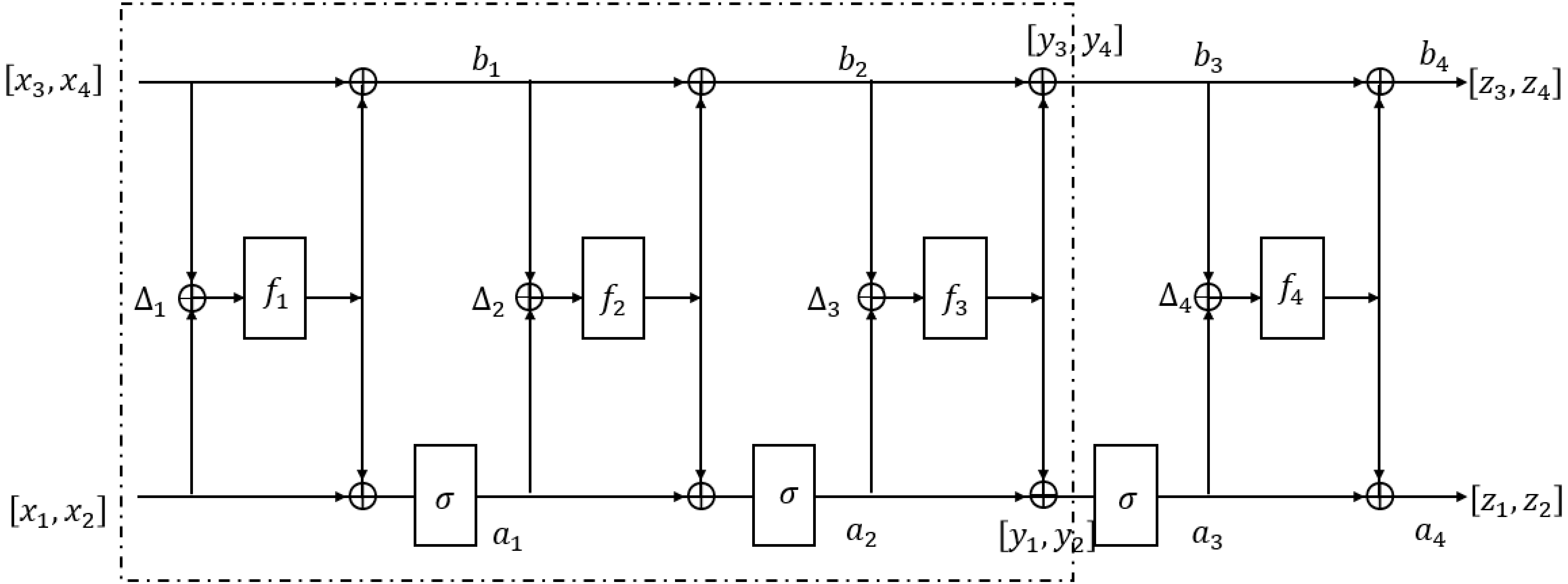
Let $n_1 = n_2 = n_3 = n_4 = \alpha_0 \oplus \alpha_1$

- We can construct a periodic function g_2 with period $s = f_1[\alpha_0, \alpha_0] \oplus f_1[\alpha_1, \alpha_1]$ by letting

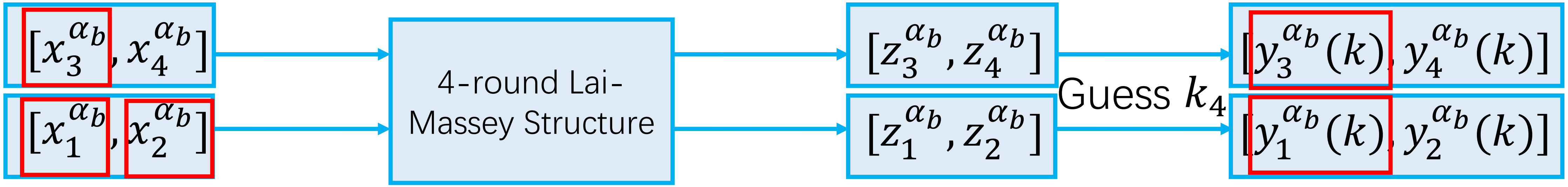
$$g_2 \mapsto x_1'^{\alpha_0} \oplus x_3'^{\alpha_0} \oplus x_1'^{\alpha_1} \oplus x_3'^{\alpha_1}$$

- we can construct a quantum CCA distinguisher by using Simon' algorithm in $O(n)$ quantum queries.

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



- Let $x, x' \in \{0,1\}^{n/2}$. $([x_1^{\alpha_b}, x_2^{\alpha_b}], [x_3^{\alpha_b}, x_4^{\alpha_b}]) \stackrel{\text{def}}{=} ([x \oplus \alpha_b, x'], [x, x' \oplus \alpha_b])$.

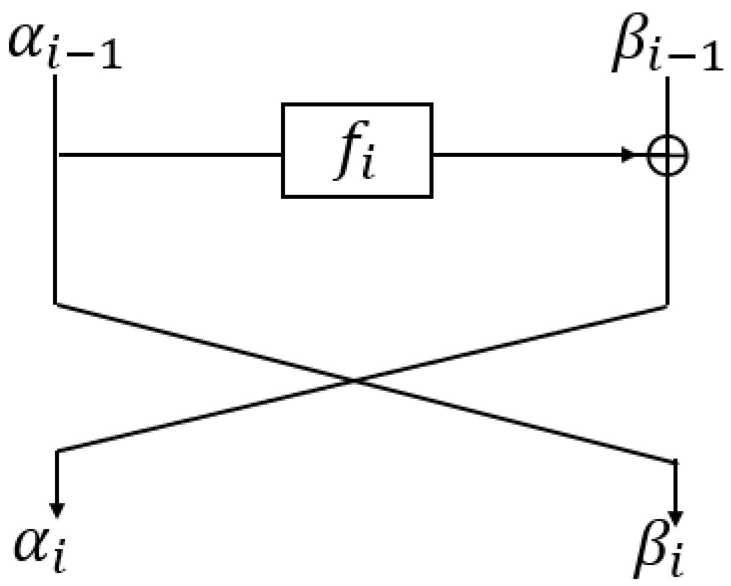


- We can construct a periodic function g_3 by letting

$$g_3 \mapsto x_1^{\alpha_0} \oplus x_2^{\alpha_0} \oplus x_3^{\alpha_0} \oplus y_1^{\alpha_0}(k) \oplus y_3^{\alpha_0}(k) \oplus \\ x_1^{\alpha_1} \oplus x_2^{\alpha_1} \oplus x_3^{\alpha_1} \oplus y_1^{\alpha_1}(k) \oplus y_3^{\alpha_1}(k)$$

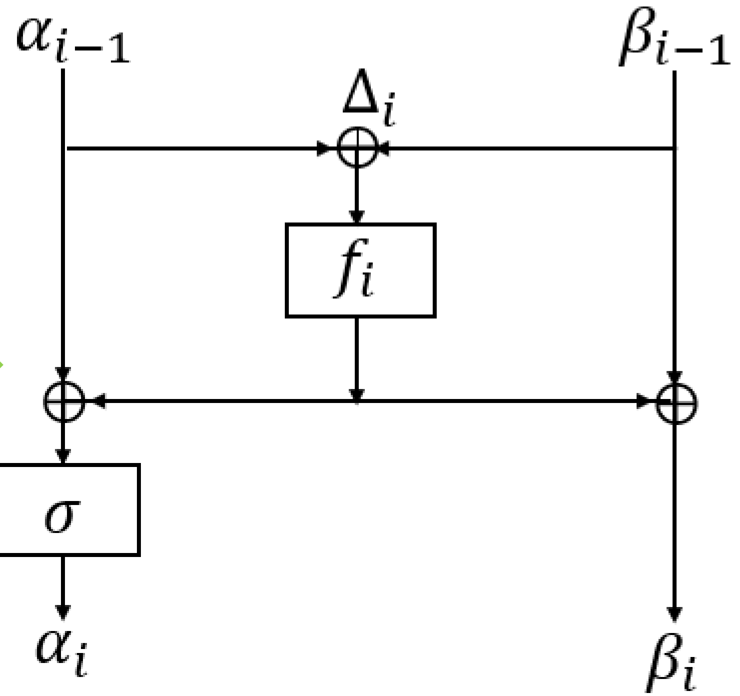
Then g_3 is a periodic function with period $s = f_1[\alpha_0, \alpha_0] \oplus f_1[\alpha_1, \alpha_1]$ if k guessed right.

- We can give a quantum Grover-meet-Simon attack with $O(n2^{m/2})$ quantum queries in quantum CPA.



The same security

In quantum



Feistel structure

Lai-Massey structure

Gembu Ito: 3/4 rounds Feistel can be attacked by using Simon's algorithm in quantum

?

quasi-Feistel structure in quantum

Our: 3/4 rounds Lai-Massey structure can be attacked by using Simon's algorithm in quantum

Quantum Attacks against Quasi-Feistel structures

Quasi-Feistel structures

Combiner:

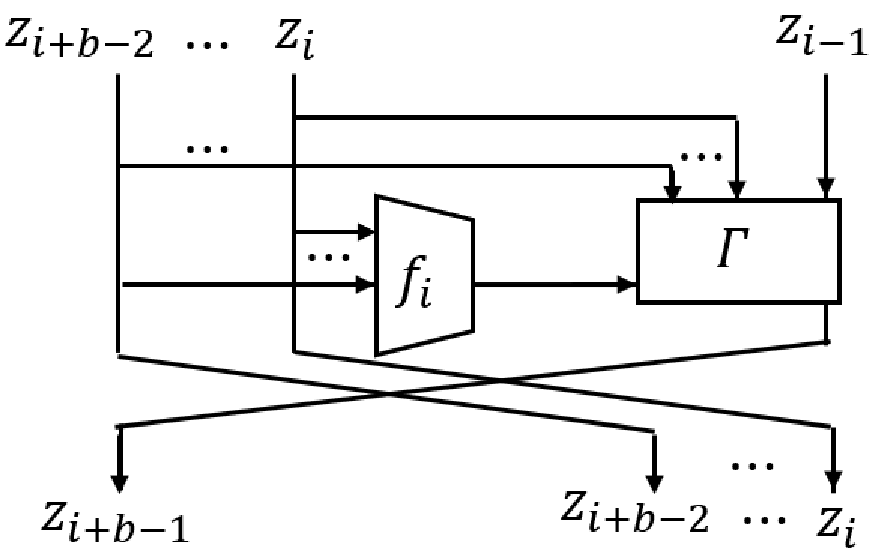
A function $\Gamma: \mathcal{X} \times \mathcal{X} \times \mathcal{Y} \to \mathcal{X}$ is a combiner over $(\mathcal{X}, \mathcal{Y})$, if

- 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.

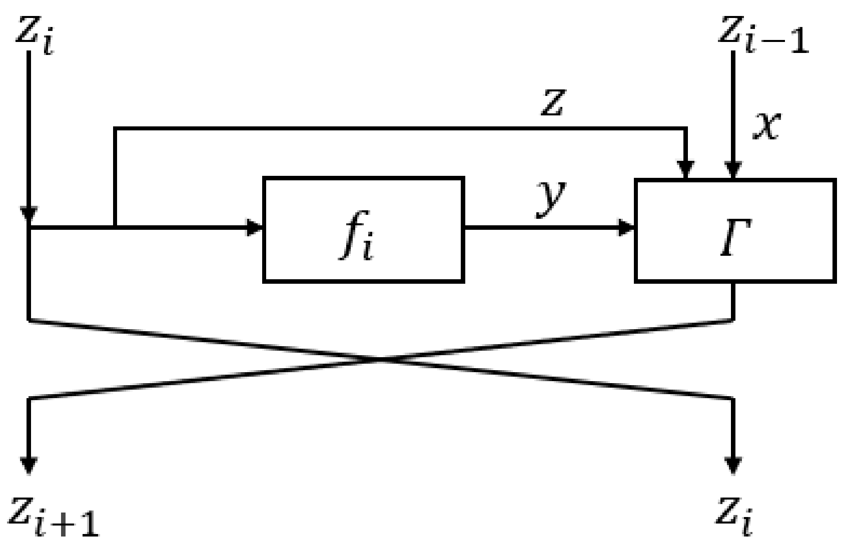
We denote $\Gamma[[x \star y \mid z]] \stackrel{\text{def}}{=} \Gamma(x, y, z)$.

- Feistel structure： $\Gamma\left[\left[x \star y \mid z\right]\right] = x \oplus y$
- Our Lai-Massey structure： $\Gamma\left[\left[x \star y \mid z\right]\right] = \sigma(x) \oplus \sigma^{-1}(y) \oplus \sigma^{-1}(\mathrm{z})$

b-branched, r-round quasi-Feistel structure:

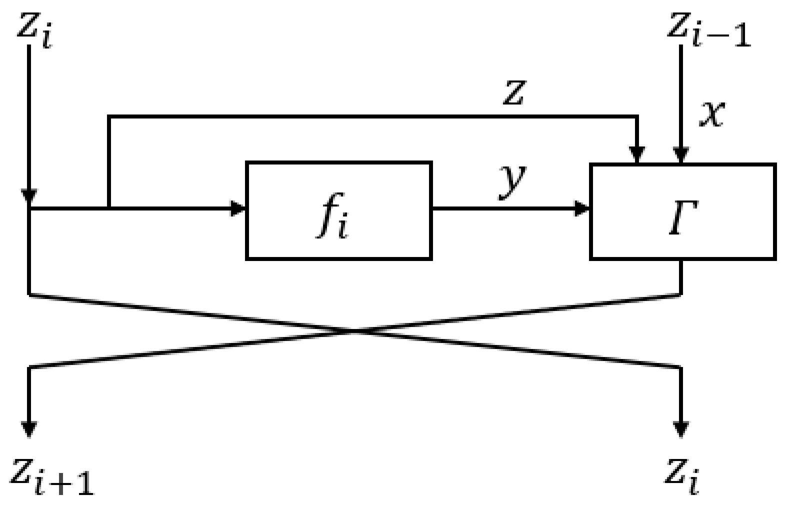


ith-round of quasi-Feistel structure

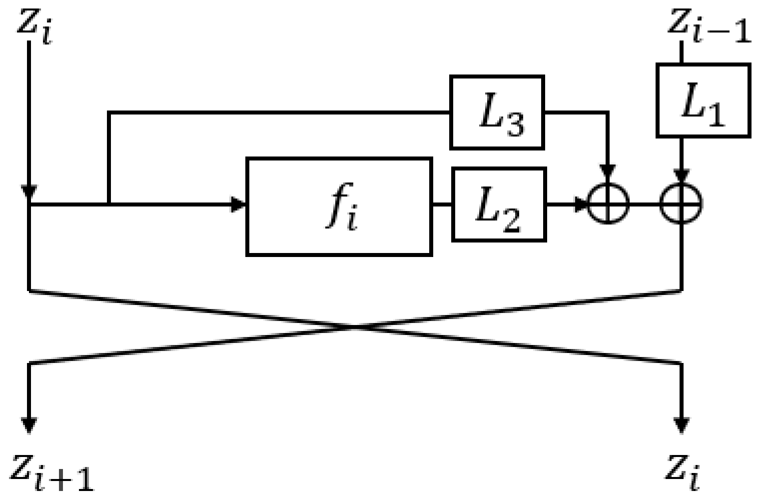


ith-round of balanced quasi-Feistel structure

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

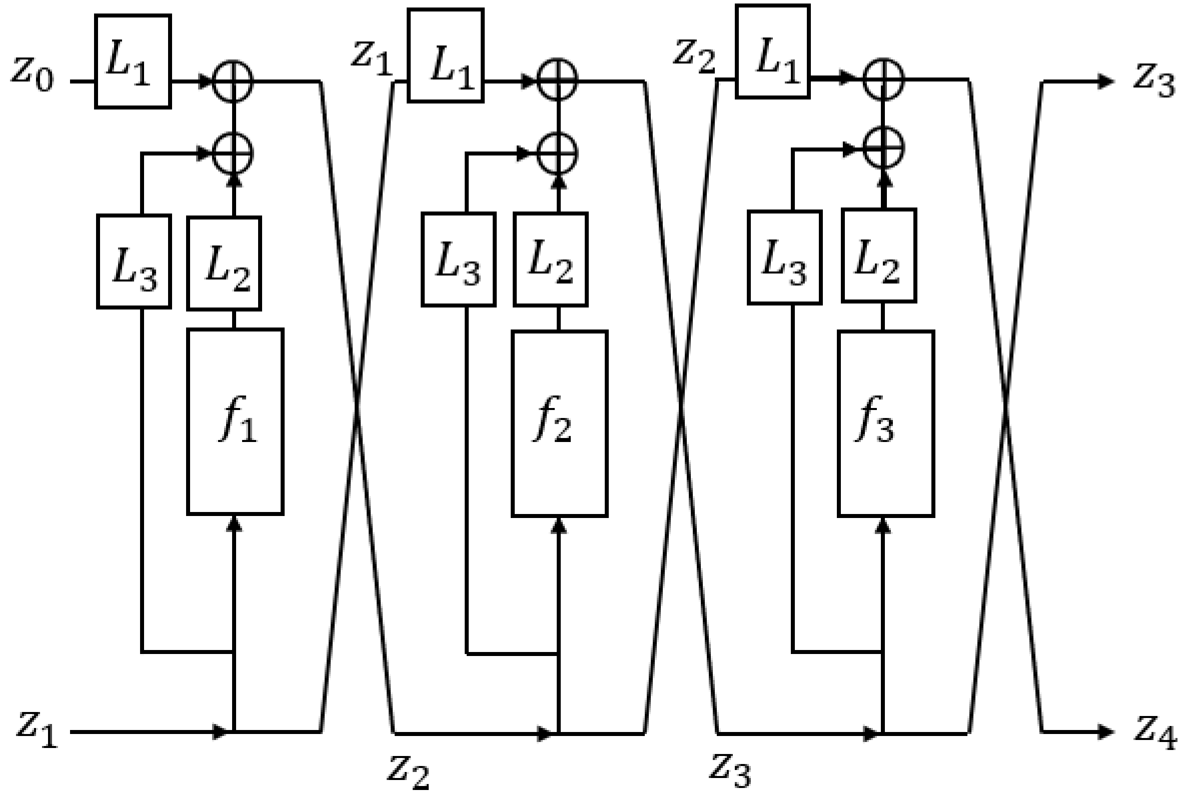


ith-round of balanced quasi-Feistel structure

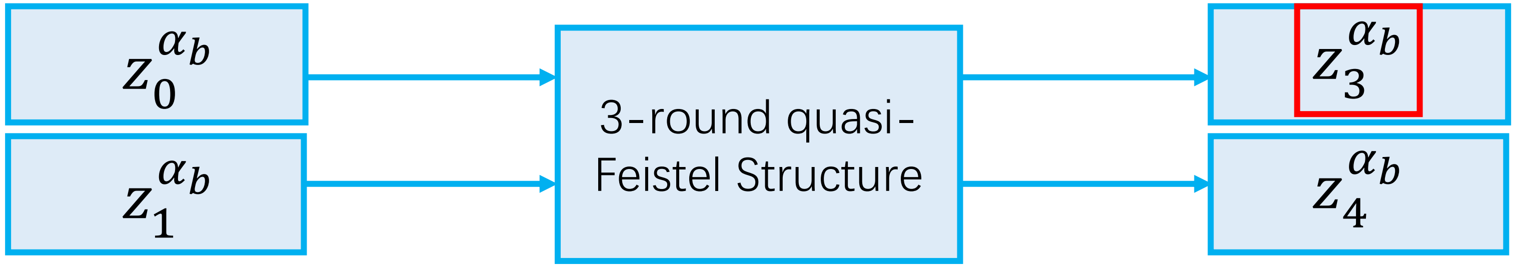


ith-round of balanced quasi-Feistel structure with linear combiner

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



- Let $x \in \{0,1\}^n$. $(z_0^{\alpha_b}, z_1^{\alpha_b}) \overset{\text{def}}{=} (x, \alpha_b)$.

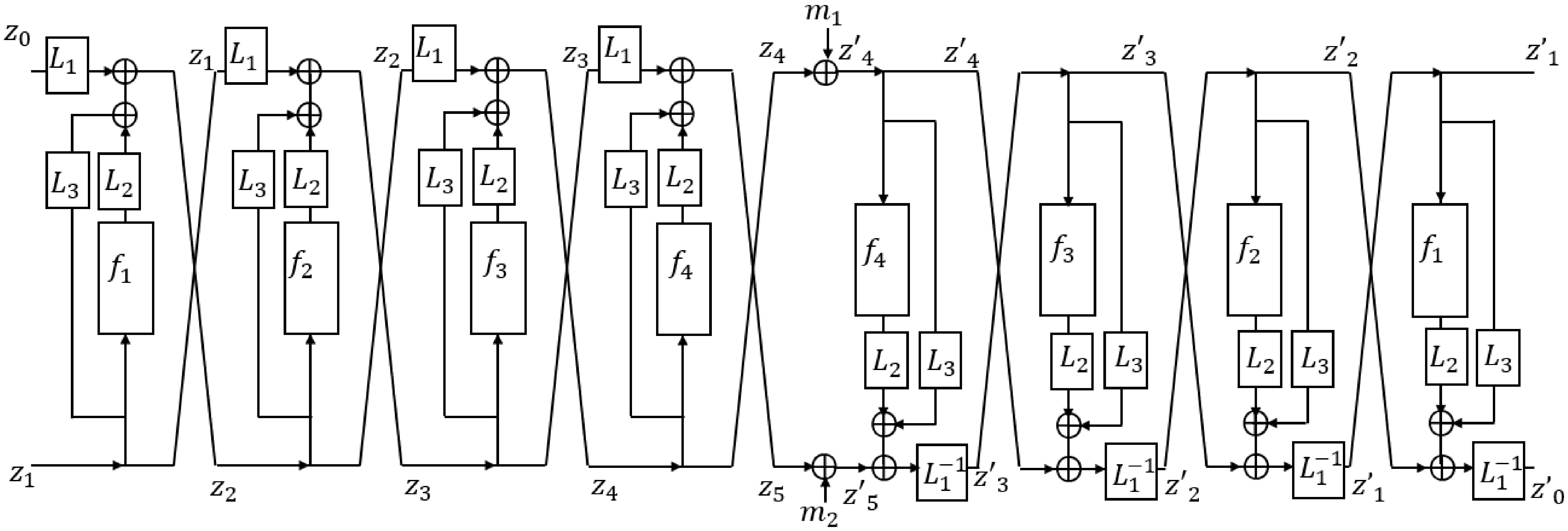


- We can construct a periodic function g_4 with period $s = L_1^{-1}L_2(f_1(\alpha_0)) \oplus L_1^{-1}L_2(f_1(\alpha_1)) \oplus L_1^{-1}L_3(\alpha_0) \oplus L_1^{-1}L_3(\alpha_1)$ by letting

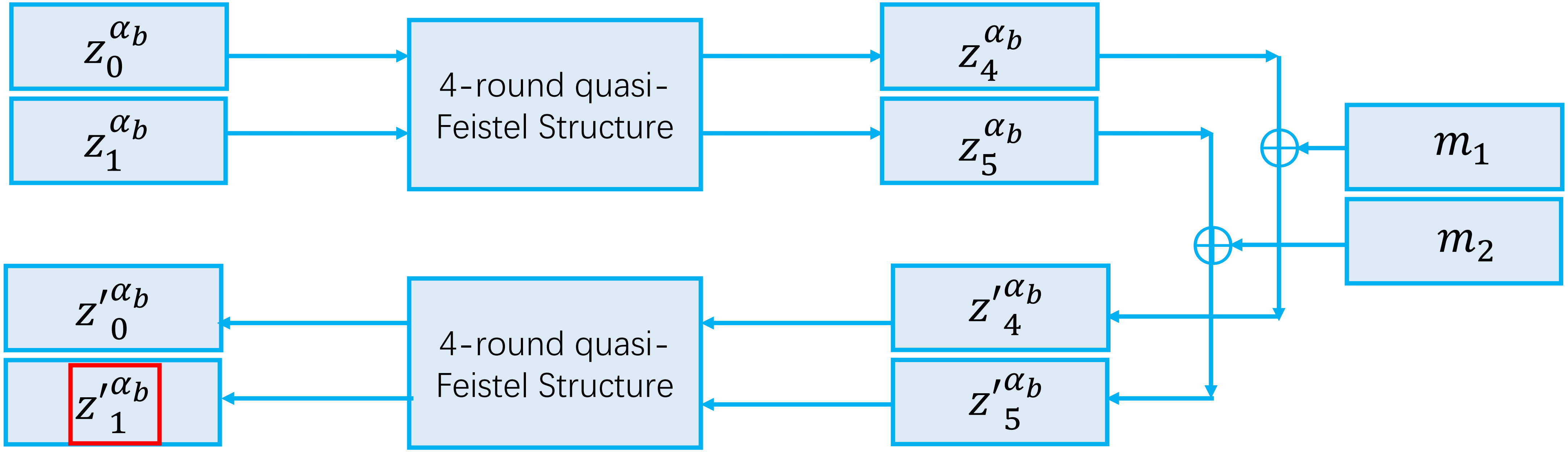
$$g_4 \mapsto z_3^{\alpha_0}(x) \oplus z_3^{\alpha_1}(x)$$

- we can construct a quantum CPA distinguisher by using Simon' algorithm in $O(n)$ quantum queries.

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



- Let $x \in \{0,1\}^n$. $(z_0^{\alpha_b}, z_1^{\alpha_b}) \stackrel{\text{def}}{=} (x, \alpha_b)$.



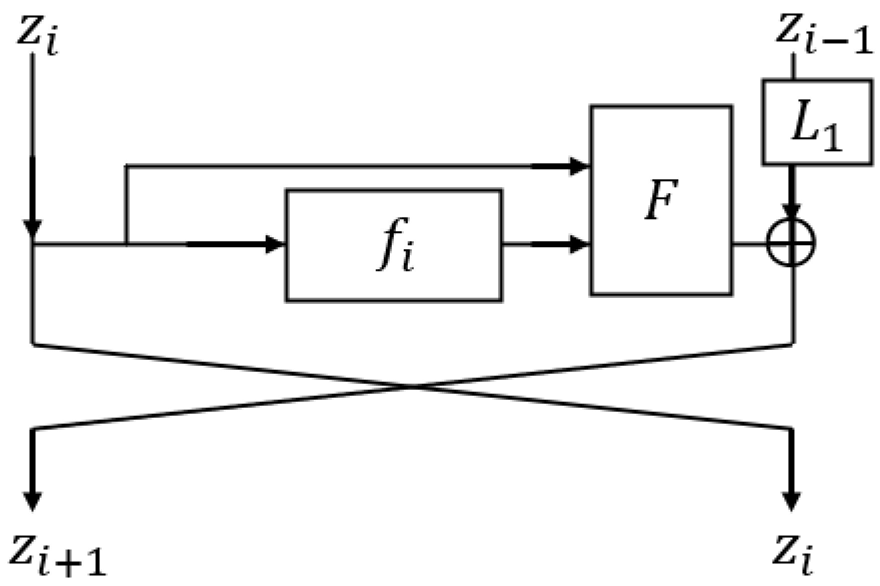
Let $m_1 = 0, m_2 = L_1 L_1(\alpha_0) \oplus L_1 L_1(\alpha_1)$

- We can construct a periodic function g_5 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

$$g_5 \mapsto {z'}_1^{\alpha_0}(x) \oplus {z'}_1^{\alpha_1}(x) \oplus \alpha_0 \oplus \alpha_1$$

- we can construct a quantum CCA distinguisher by using Simon' algorithm in $O(n)$ quantum queries.

Acknowledgement



One of reviewers pointed out that the combiner Γ of balanced quasi-Feistel structure does not need to be all linear.
After our verification, only L_1 needs to be linear.

$$\Gamma[\![x \star y \mid z]\!] = L_1(x) \oplus F(y, z)$$

where L_1 is linear and F is a function.

Thanks