RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: CRYP-R09

Quantum Chosen-Ciphertext Attacks against Feistel Ciphers

Gembu Ito

Nagoya University

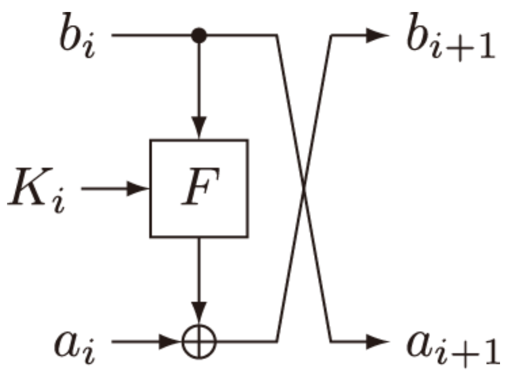
Joint work with Akinori Hosoyamada, Ryutaroh Matsumoto, Yu Sasaki and Tetsu Iwata

#RSAC

Overview

- 3-round Feistel construction is a PRP, 4-round is an SPRP [LR88]

Rounds	2	3	4
Classic	CPA insecure	CPA secure [LR88] CCA insecure	CCA secure [LR88]



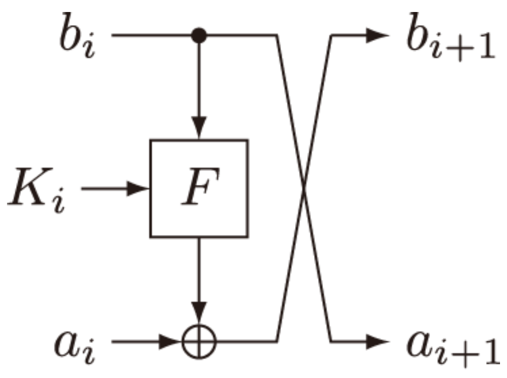
- insecure: efficient distinguishing attacks
- secure: indistinguishable from a random permutation

[LR88] Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput. 1988.

Overview

- **3-round** Feistel construction is **not secure** against **quantum CPAs** [KM10]

Rounds	2	3	4
Classic	CPA insecure	CPA secure [LR88] CCA insecure	CCA secure [LR88]
Quantum		QCPA insecure [KM10]	



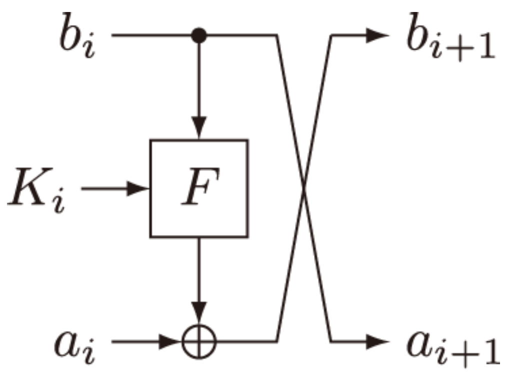
- insecure: efficient distinguishing attacks
- secure: indistinguishable from a random permutation

[KM10] Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. ISIT 2010.

Overview

- **4-round** Feistel construction is **not secure** against **quantum CCAs**

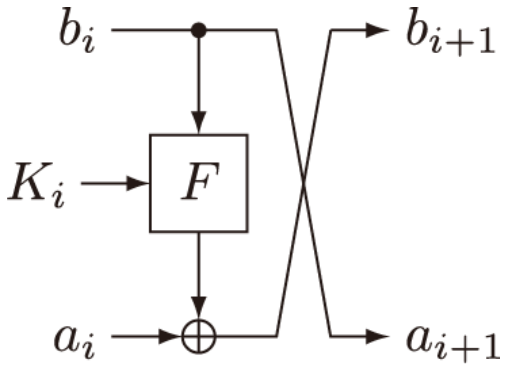
Rounds	2	3	4
Classic	CPA insecure	CPA secure [LR88] CCA insecure	CCA secure [LR88]
Quantum		QCPA insecure [KM10]	QCCA insecure



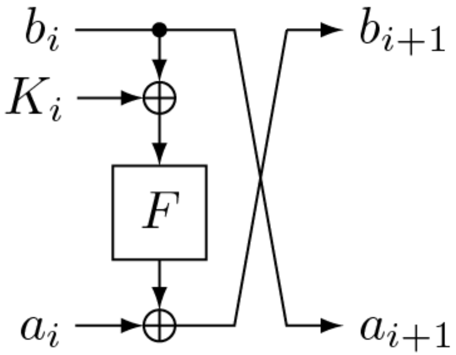
Overview

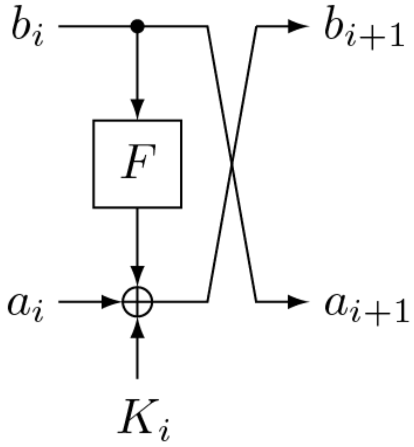
- **4-round** Feistel construction is **not secure** against **quantum CCAs**

Rounds	2	3	4
Classic	CPA insecure	CPA secure [LR88] CCA insecure	CCA secure [LR88]
Quantum		QCPA insecure [KM10]	QCCA insecure



- Extend to practical designs of Feistel ciphers (including key recovery attacks)





Outline

1. Introduction
2. Previous Quantum Distinguisher
3. Quantum CCAs against Feistel Constructions
   - Quantum Distinguisher against 4-round Feistel Constructions
   - Formalization of Quantum Distinguishers
   - Quantum CCAs against Practical Designs of Feistel Constructions
4. Concluding Remarks

Outline

1. Introduction
2. Previous Quantum Distinguisher
3. Quantum CCAs against Feistel Constructions
   - Quantum Distinguisher against 4-round Feistel Constructions
   - Formalization of Quantum Distinguishers
   - Quantum CCAs against Practical Designs of Feistel Constructions
4. Concluding Remarks

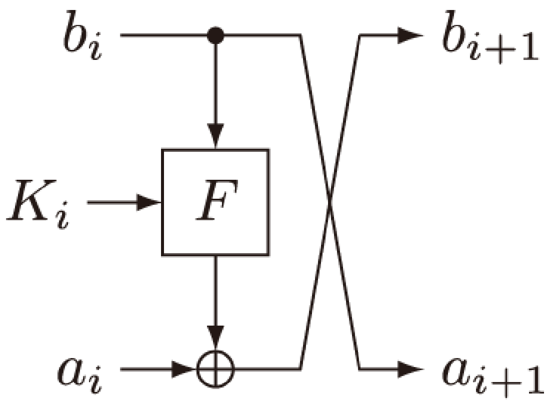
Feistel Ciphers

Feistel-F Construction

- n-bit state is divided into $n/2$-bit halves a_i and b_i, then

$$b_{i+1} \leftarrow a_i \oplus F_{K_i}(b_i), \qquad a_{i+1} \leftarrow b_i$$

- F_{K_i} is a keyed function taking a subkey K_i as input



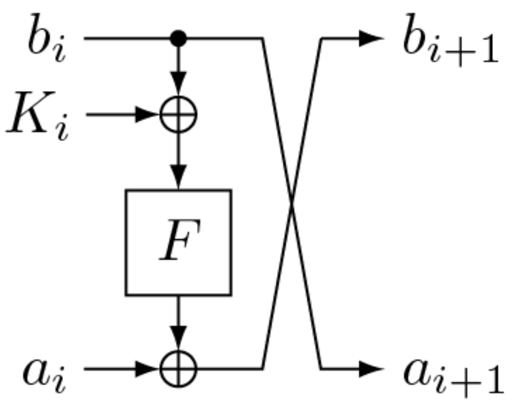
Practical Designs of Feistel Ciphers

Feistel-KF Construction

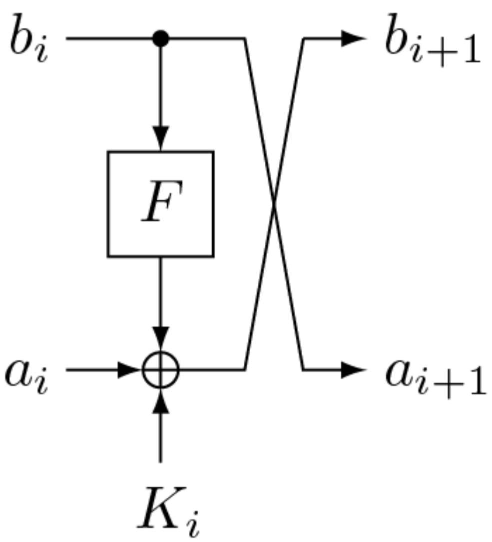
- DES, Camellia

Feistel-FK Construction

- Piccolo, SIMON, Simeck



Feistel-KF



Feistel-FK

Main Tool: Simon's algorithm [Sim97]

Problem

Given $f: \{0,1\}^n \to \{0,1\}^n$ such that there exists a non-zero period s with

$$f(x) = f(x') \Leftrightarrow x' = x \oplus s$$

for any distinct $x, x' \in \{0,1\}^n$, the goal is to find s

- $O(2^{n/2})$ queries in the classical setting
- **Simon's algorithm** [Sim97] can find s with $\boldsymbol{O(n)}$ **quantum queries**

[Sim97] Simon, D.R.: On the power of quantum computation. SIAM J. Comput. 26(5),1474–1483 (1997)

Main Tool: Simon's algorithm [Sim97]

- Many polynomial-time attacks using Simon's algorithm
  - 3-round Feistel construction [KM10]
  - Even-Mansour [KM12]
  - LRW, various MACs, and CAESAR candidates [KLL+16]
  - AEZ [Bon17]
  - …

[KM12] H. Kuwakado and M. Morii. Security on the Quantum-Type Even-Mansour Cipher. ISITA 2012.

[KLL+16] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Breaking Symmetric Cryptosystems using Quantum Period Finding. CRYPTO 2016.

[Bon17] Bonnetain, X.: Quantum Key-Recovery on Full AEZ. SAC 2017.

Outline

1. Introduction
2. Previous Quantum Distinguisher
3. Quantum CCAs against Feistel Constructions
   - Quantum Distinguisher against 4-round Feistel Constructions
   - Formalization of Quantum Distinguishers
   - Quantum CCAs against Practical Designs of Feistel Constructions
4. Concluding Remarks

Overview of the Distinguisher

- Given an oracle O which is $O = E_K$ or a random permutation $\Pi \in \mathrm{Perm}(n)$, distinguish the two cases
  – The adversary can make superposition queries to O

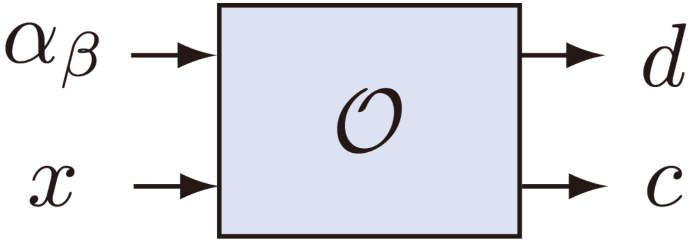
Distinguisher

1. Construct a function f^O that
   – has a period s when O is E_K, and
   – does not have any period when O is Π
2. Check if f^O has a period or not by using Simon's algorithm

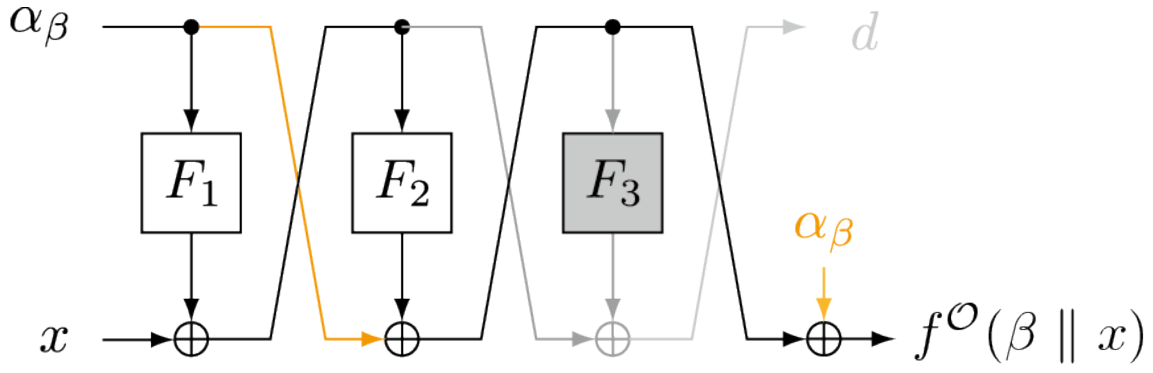
Quantum Distinguisher against 3-round Feistel-F [KM10]

- $\alpha_0, \alpha_1 \in \{0,1\}^{n/2}$: arbitrary distinct constants

$$f^{O}: \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$$
$$(\beta \parallel x) \qquad \mapsto c \oplus \alpha_\beta$$

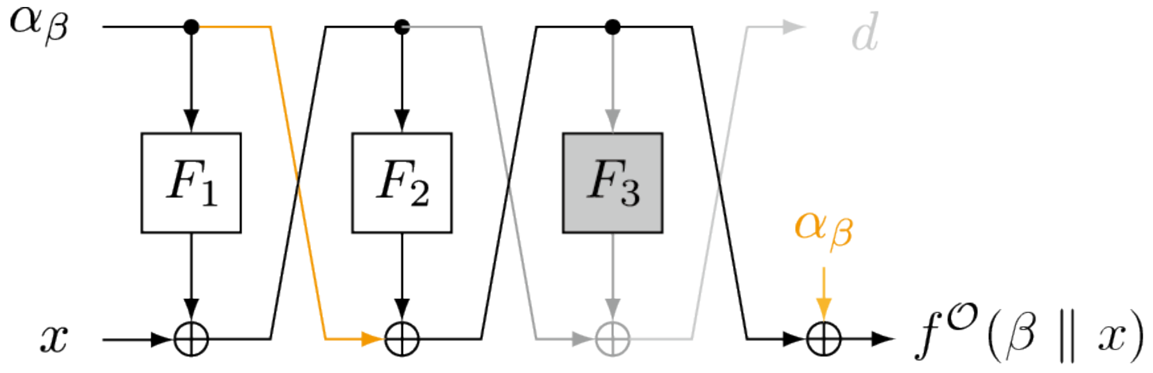


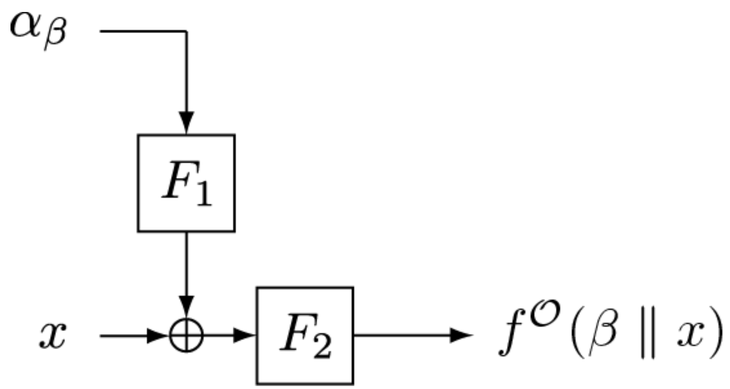
Quantum Distinguisher against 3-round Feistel-F [KM10]



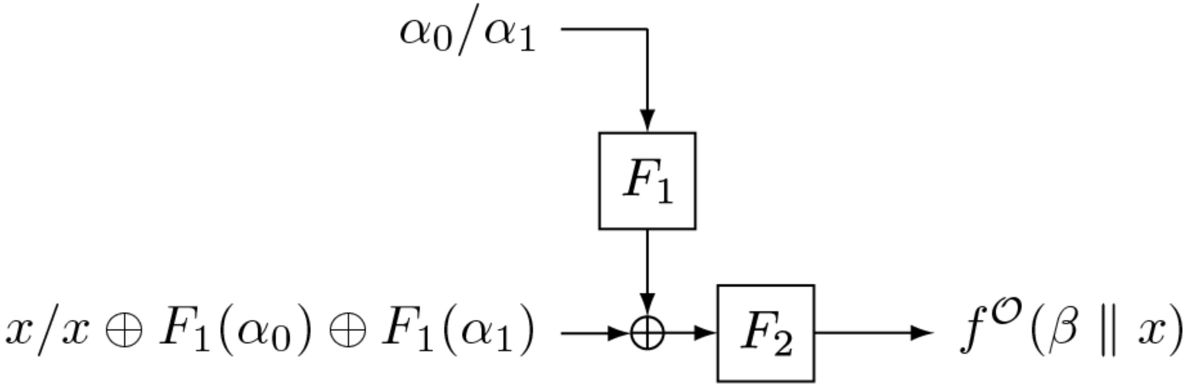
- F_3 does not contribute to f^O
- Orange line and α_β cancel each other

Quantum Distinguisher against 3-round Feistel-F [KM10]





Quantum Distinguisher against 3-round Feistel-F [KM10]



- f^O has a period $\boldsymbol{s} = \left(\mathbf{1} \parallel \boldsymbol{F_1}(\boldsymbol{\alpha_0}) \oplus \boldsymbol{F_1}(\boldsymbol{\alpha_1})\right)$

$$\begin{aligned} f^O(\beta \parallel x) &= F_2\left(x \oplus F_1\left(\alpha_\beta\right)\right) \\ &= F_2\left(x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1) \oplus F_1\left(\alpha_{\beta\oplus 1}\right)\right) \\ &= f^O\left(\beta \oplus 1 \parallel x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1)\right) \end{aligned}$$

Key Recovery Attacks

- Distinguisher can be extended to key recovery attacks
- Key recovery attacks against Feistel-KF [HS18,DW17]
  - Combining Grover search [Gro96] and the distinguisher
  - Leander and May developed this technique [LM17]

[HS18] Hosoyamada, A., Sasaki, Y.: Quantum Demiric-Selçuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions. SCN 2018.

[DW17] Dong, X., Wang, X.: Quantum key-recovery attack on Feistel structures. IACR Cryptology ePrint Archive 2017.

[Gro96] Grover, L.K.: A fast quantum mechanical algorithm for database search. STOC 1996.

[LM17] Leander, G., May, A.: Grover meets Simon - Quantumly attacking the FX-construction. ASIACRYPT 2017.

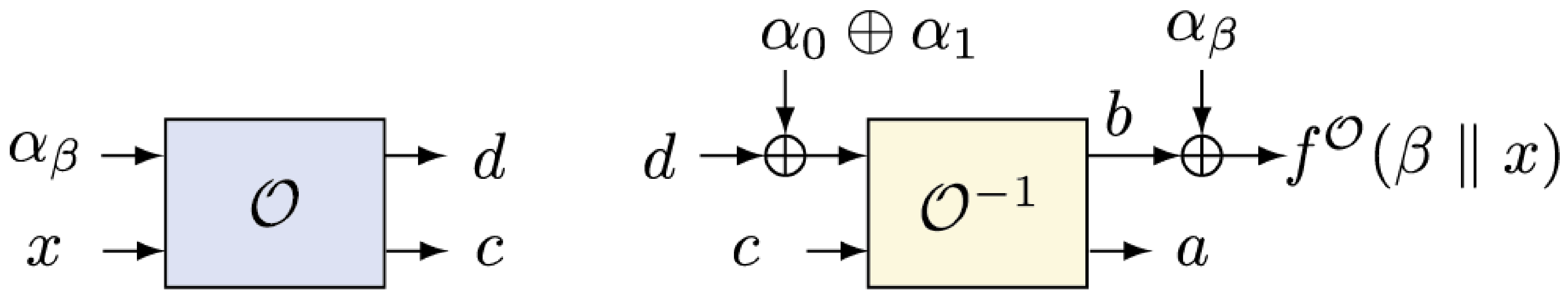
Outline

1. Introduction
2. Previous Quantum Distinguisher
3. Quantum CCAs against Feistel Constructions
   – Quantum Distinguisher against 4-round Feistel Constructions
   – Formalization of Quantum Distinguishers
   – Quantum CCAs against Practical Designs of Feistel Constructions
4. Concluding Remarks

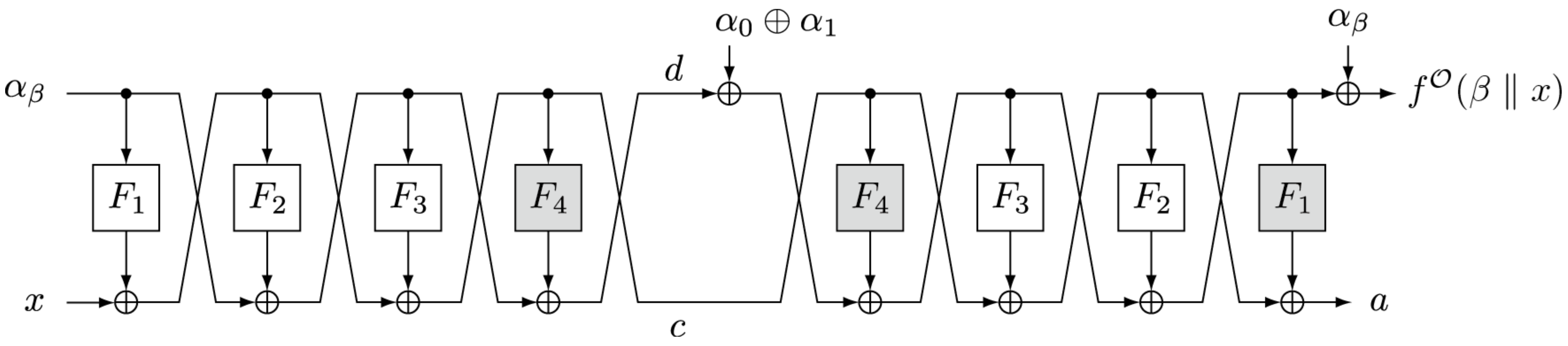
Quantum Distinguisher against 4-round Feistel-F

- $\alpha_0, \alpha_1 \in \{0,1\}^{n/2}$: arbitrary distinct constants

$$f^{O}: \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$$
$$(\beta \parallel x) \qquad \mapsto b \oplus \alpha_\beta$$

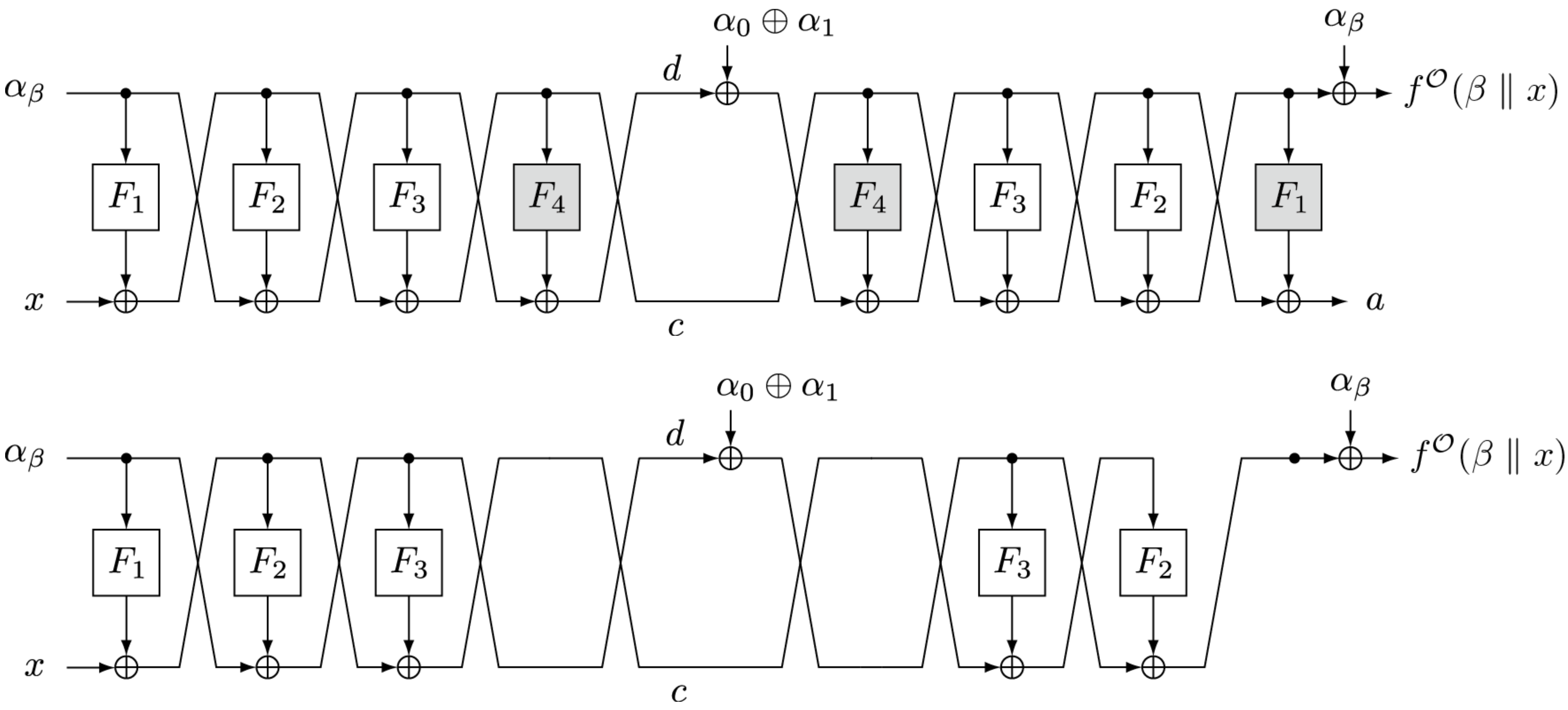


Quantum Distinguisher against 4-round Feistel-F

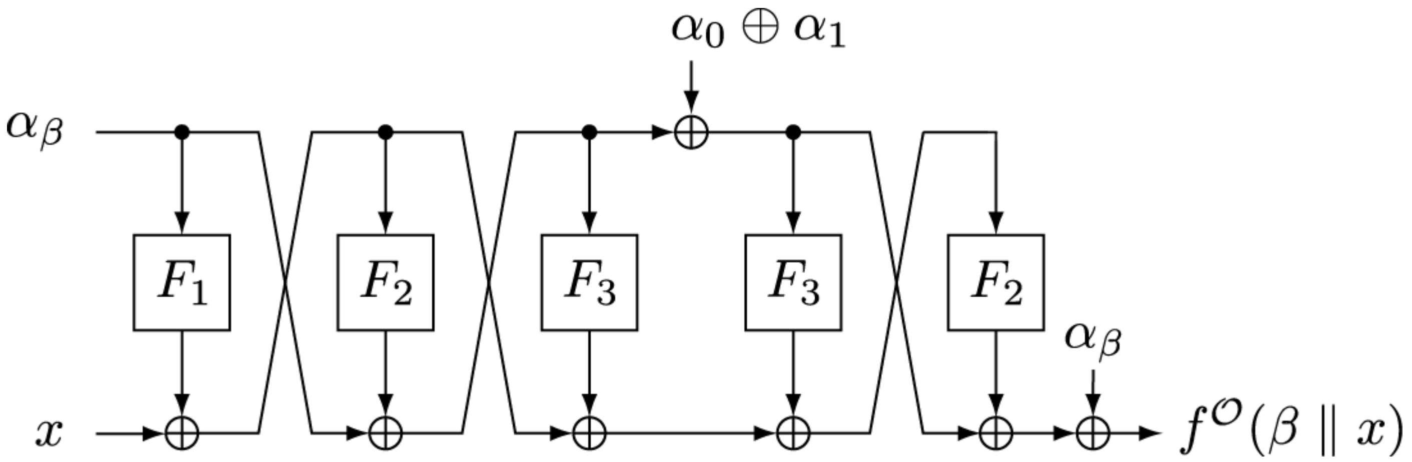


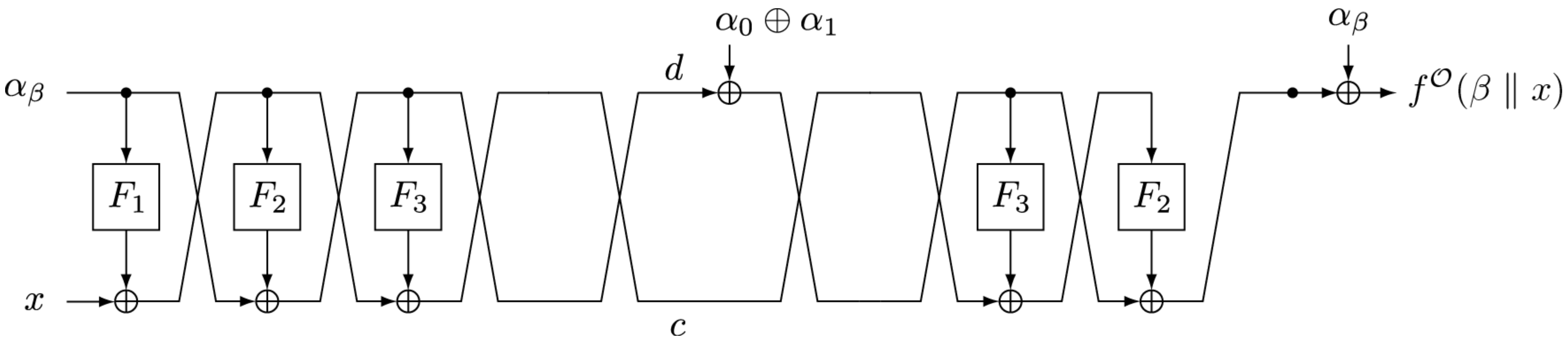
- F_4 has no effect
- Last F_1 does not contribute to $f^{\mathcal{O}}$

Quantum Distinguisher against 4-round Feistel-F

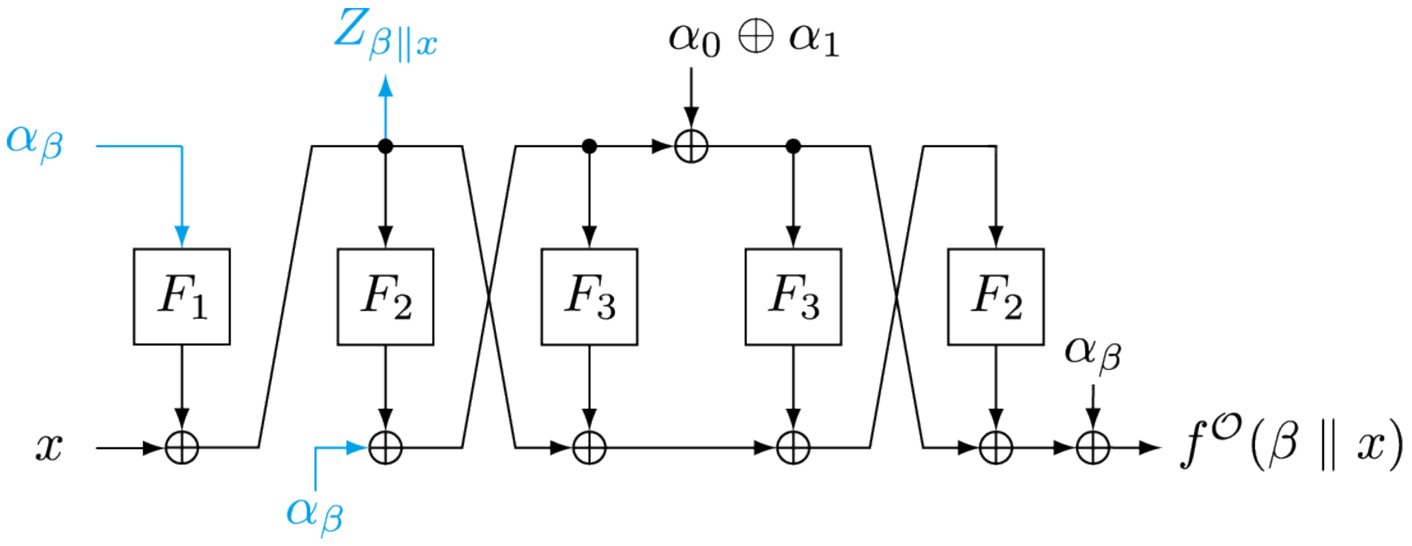


Quantum Distinguisher against 4-round Feistel-F

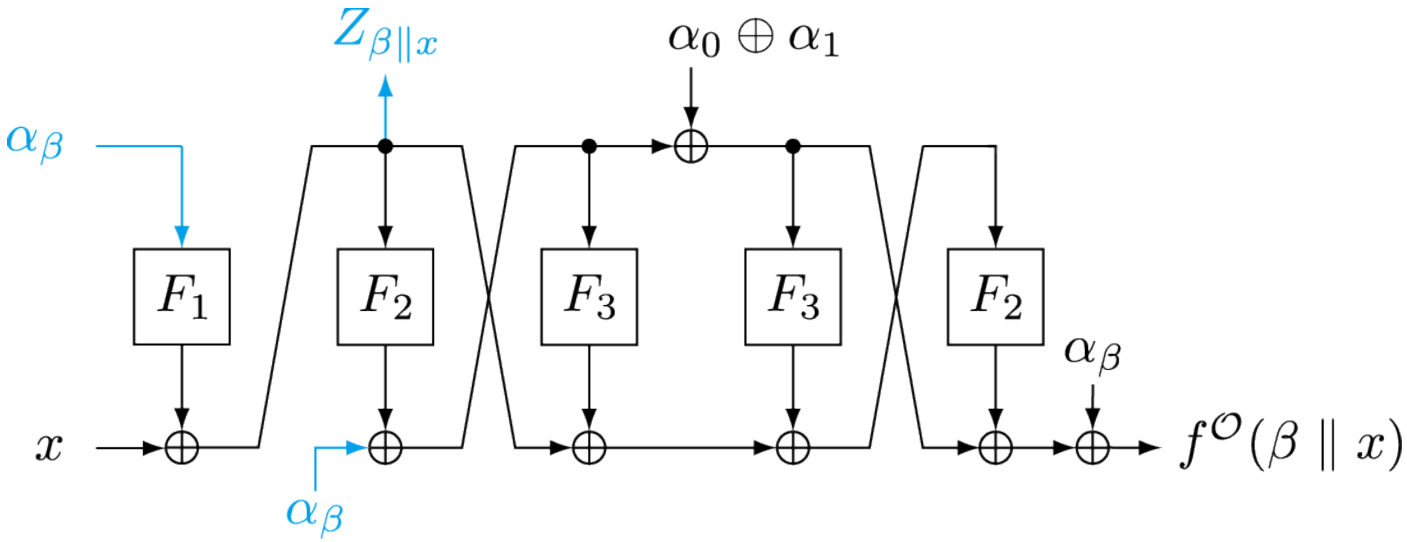




Quantum Distinguisher against 4-round Feistel-F

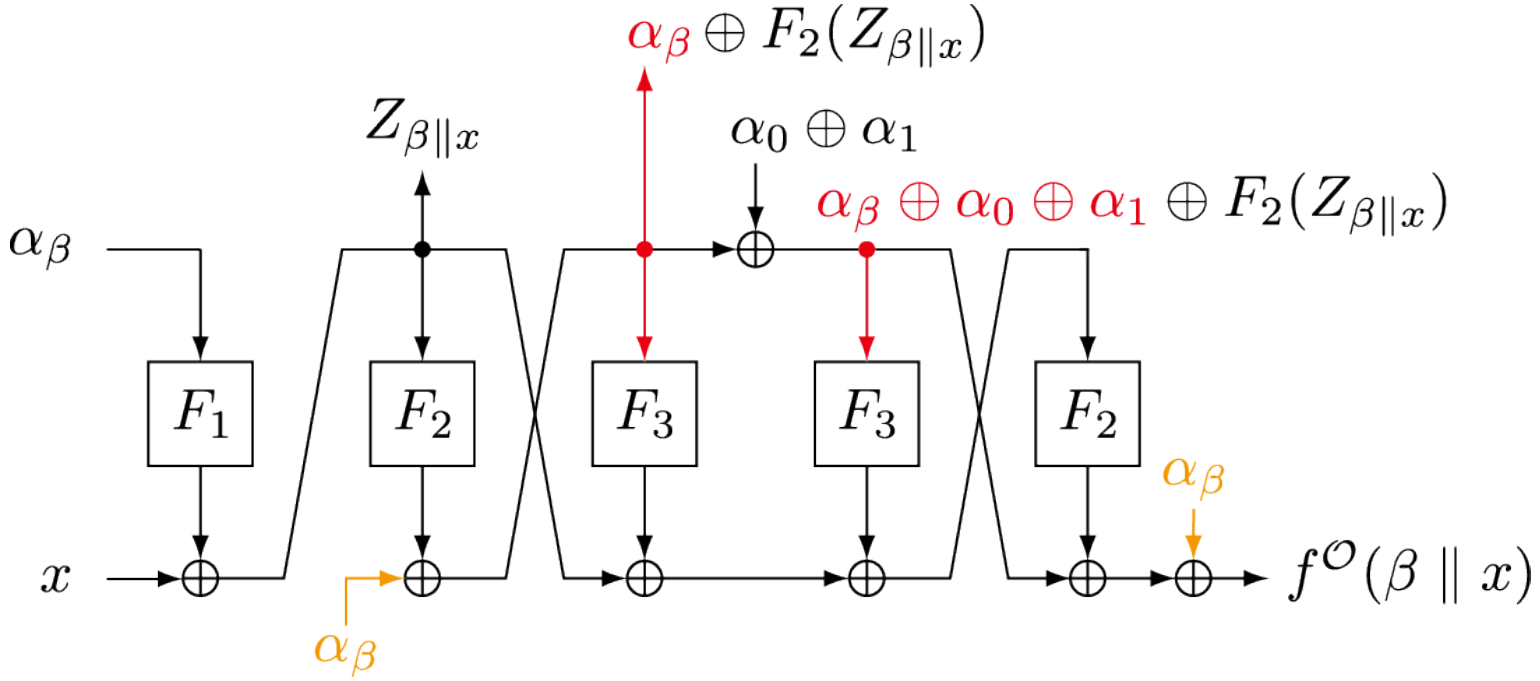


Quantum Distinguisher against 4-round Feistel-F



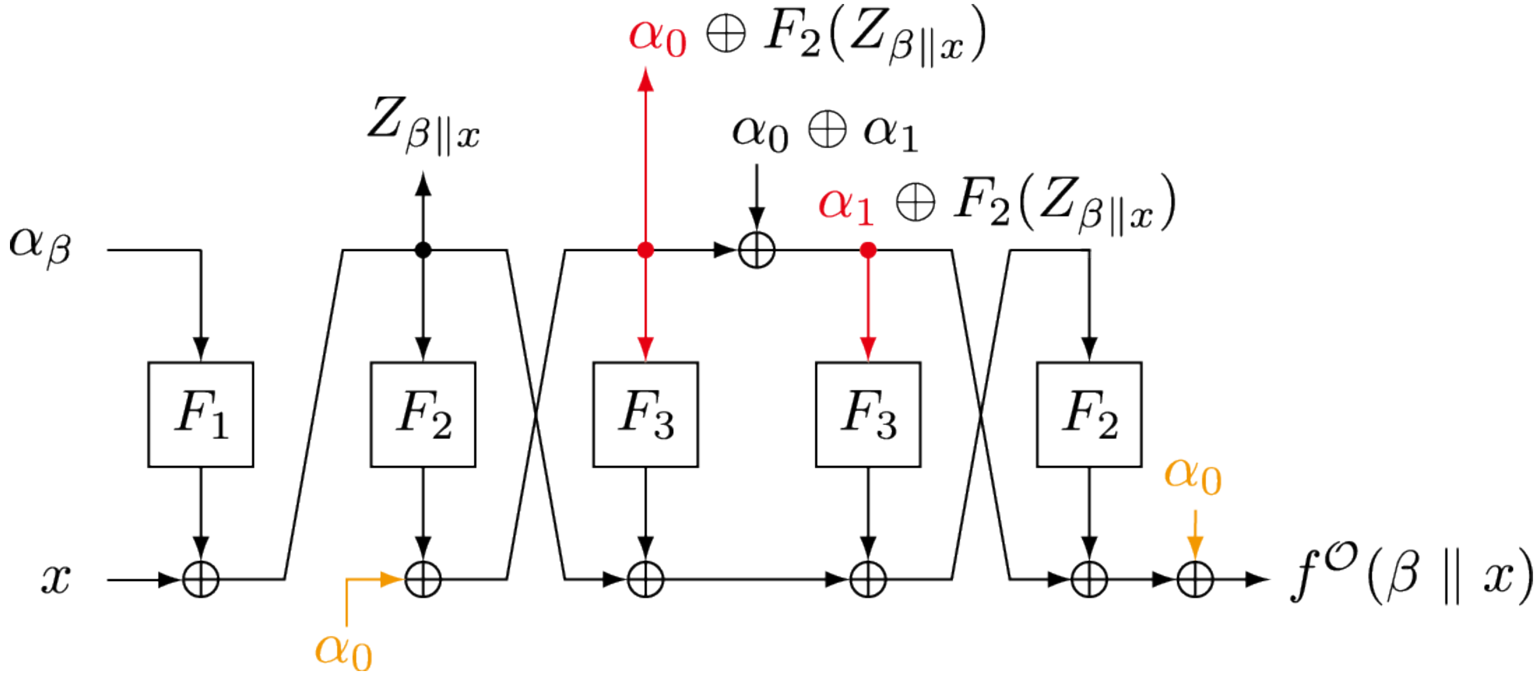
- Computation after $Z_{\beta\|x}$ does not depend on β, x
- $Z_{\beta\|x}$ has a period $s = \left(1 \| F_1(\alpha_0) \oplus F_1(\alpha_1)\right)$

Quantum Distinguisher against 4-round Feistel-F



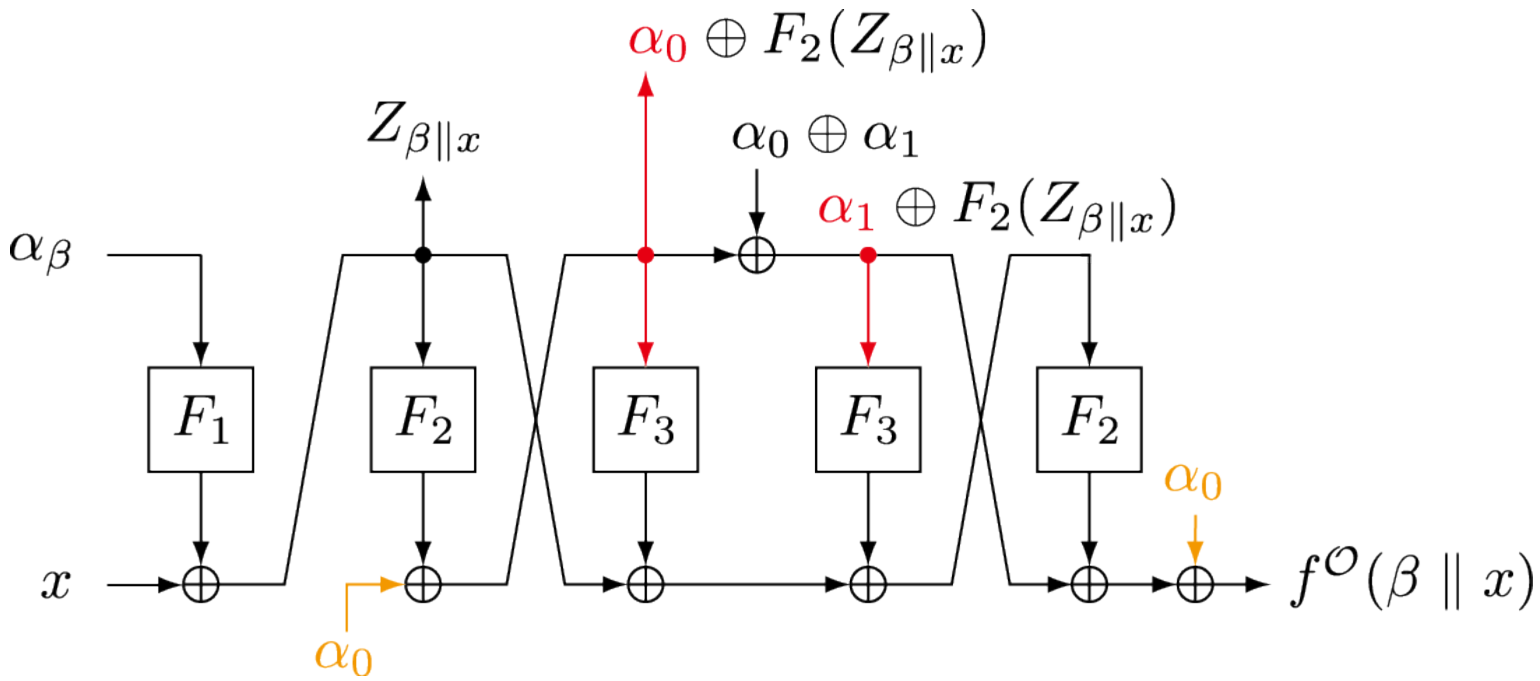
- α_β cancels each other
- $\{\alpha_0, \alpha_0 \oplus \alpha_0 \oplus \alpha_1\} = \{\alpha_1, \alpha_1 \oplus \alpha_0 \oplus \alpha_1\} = \{\alpha_0, \alpha_1\}$

Quantum Distinguisher against 4-round Feistel-F



- α_β cancels each other
- $\{\alpha_0, \alpha_0 \oplus \alpha_0 \oplus \alpha_1\} = \{\alpha_1, \alpha_1 \oplus \alpha_0 \oplus \alpha_1\} = \{\alpha_0, \alpha_1\}$
- Computation after $Z_{\beta\|x}$ does not depend on β, x

Quantum Distinguisher against 4-round Feistel-F



- $Z_{\beta\|x}$ has a period $s = \left(1 \| F_1(\alpha_0) \oplus F_1(\alpha_1)\right)$ since

$$\begin{aligned} Z_{(0\|x)\oplus s} &= x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1) \oplus F_1(\alpha_1) \\ &= x \oplus F_1\,(\alpha_0\,) \\ &= Z_{(0\|x)} \end{aligned}$$

Relaxing Simon's Algorithm

- We know that $f(x) = f(x') \Leftarrow x' = x \oplus s$
- $f(x) = f(x') \Rightarrow x' = x \oplus s$ may or may not hold
- We formalize a sufficient condition
  to eliminate the need to prove it

Relaxing Simon's Algorithm

- Simon's Algorithm uses the circuit S_f that returns a vector y_i that is orthogonal to all periods $s_1, s_2, \ldots$
- To recover s from $y_1, y_2, \ldots, f$ has to satisfy

$$f(x) = f(x') \Rightarrow x' = x \oplus s$$

Relaxing Simon's Algorithm

- In distinguisher
  - If f has a period s, we obtain $y_i \cdot s \equiv 0 \pmod 2$ (**other periods can exist**) $\Rightarrow$ **dimension** of the space spanned by $y_1, y_2, \ldots$ is **at most $\boldsymbol{n} - \mathbf{1}$**
  - If f doesn't have a period, y_i can take any value of $\{0,1\}^n$ $\Rightarrow$ **dimension** can reach $\boldsymbol{n}$

[SS17] Santoli, T., Schaffner, C.: Using Simon's algorithm to attack symmetric-key cryptographic primitives. Quantum Information & Computation 2017.

Relaxing Simon's Algorithm

- In distinguisher
  - If f has a period s, we obtain $y_i \cdot s \equiv 0 \pmod 2$ (**other periods can exist**) ⇒ **dimension** of the space spanned by $y_1, y_2, \ldots$ is **at most $\boldsymbol{n} - 1$**
  - If f doesn't have a period, y_i can take any value of $\{0,1\}^n$ ⇒ **dimension** can reach $\boldsymbol{n}$
- Checking the dimension of the space spanned by $y_1, y_2, \ldots$
- Similar observation is pointed out in [SS17]
  - We formalized a sufficient condition

[SS17] Santoli, T., Schaffner, C.: Using Simon's algorithm to attack symmetric-key cryptographic primitives. Quantum Information & Computation 2017.

Relaxing Simon's Algorithm

- $\epsilon_f^\pi = \max_{t \in \{0,1\}^l \setminus \{0^l\}} \Pr_x[f^\pi(x) = f^\pi(x \oplus x)]$ (π is a fixed permutation)
- $\mathrm{irr}_f^\delta = \{\pi \in \mathrm{Perm}(n) \mid \epsilon_f^\pi > 1 - \delta\}$ (δ is a small constant $0 \leq \delta < 1$)
- Checking the dimension of the space spanned by $y_1, y_2, \ldots, y_\eta$
- Success probability is at least

$$1 - \frac{2^l}{e^{\delta\eta/2}} - \Pr_\Pi[\Pi \in \mathrm{irr}_f^\delta]$$

[SS17] Santoli, T., Schaffner, C.: Using Simon's algorithm to attack symmetric-key cryptographic primitives. Quantum Information & Computation 2017.

Outline

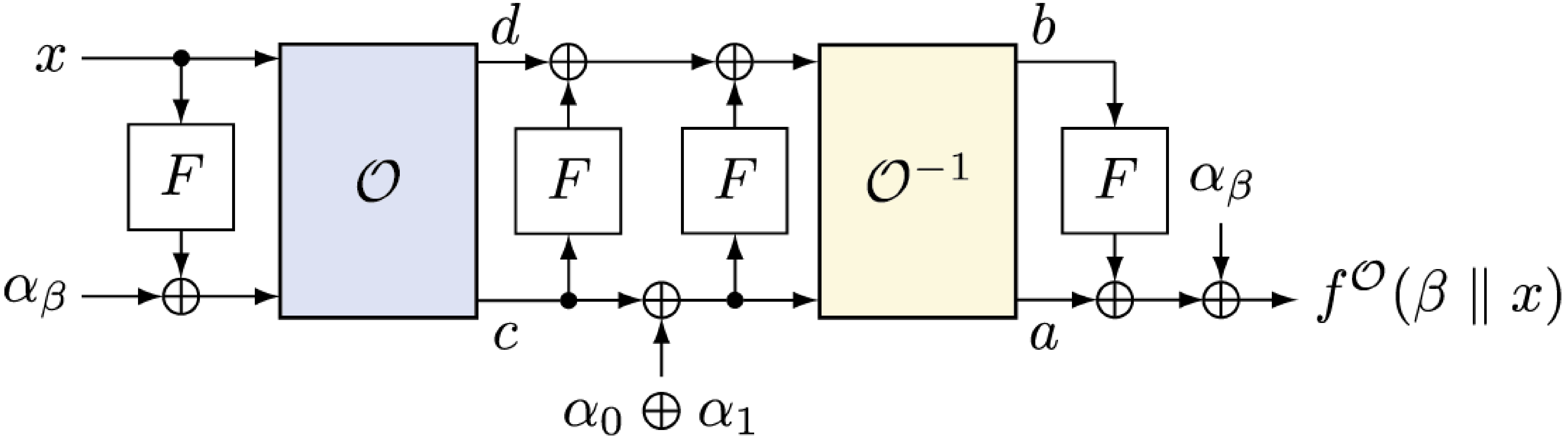
1. Introduction
2. Previous Quantum Distinguisher
3. Quantum CCAs against Feistel Constructions
   - Quantum Distinguisher against 4-round Feistel Constructions
   - Formalization of Quantum Distinguishers
   - Quantum CCAs against Practical Designs of Feistel Constructions
4. Concluding Remarks

Quantum Attacks against Practical Designs

- The same distinguishing attack against Feistel-F can be used against Feistel-KF
- Extend to quantum distinguishing attacks against 6-round Feistel-FK
- Key recovery attacks against 7-round Feistel-KF and 9-round Feistel-FK

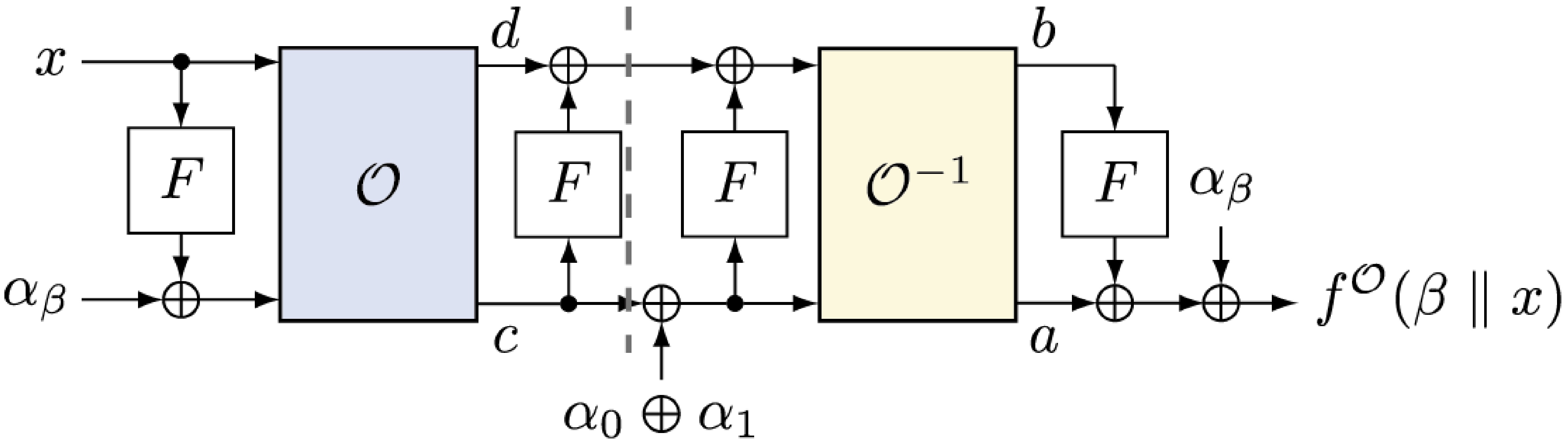
Quantum Distinguisher against 6-round Feistel-FK

$$f^{O}: \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$$
$$(\beta \parallel x) \mapsto a \oplus F(b) \oplus \alpha_\beta$$

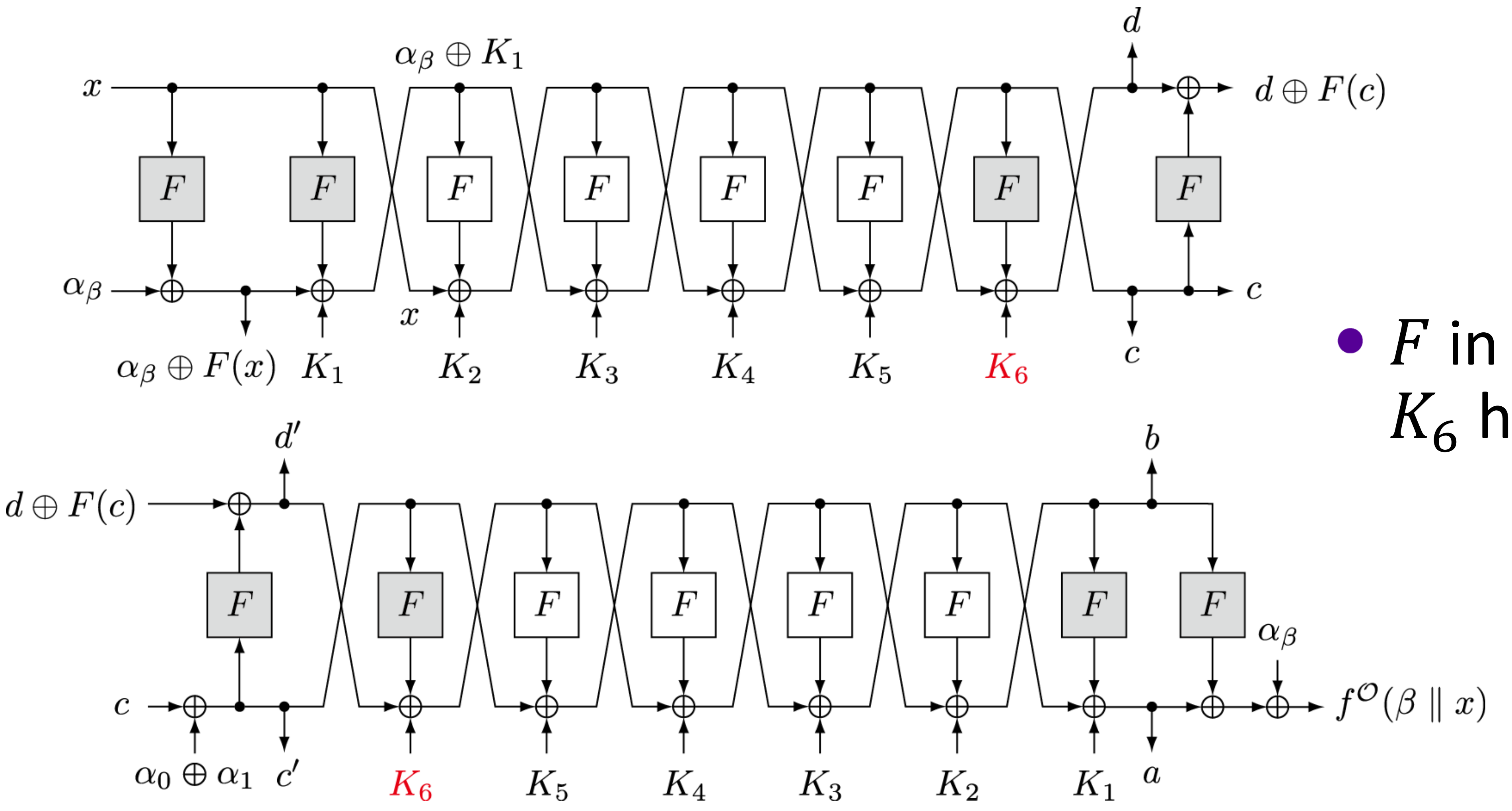


Quantum Distinguisher against 6-round Feistel-FK

$$f^{O}: \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$$
$$(\beta \parallel x) \mapsto a \oplus F(b) \oplus \alpha_\beta$$

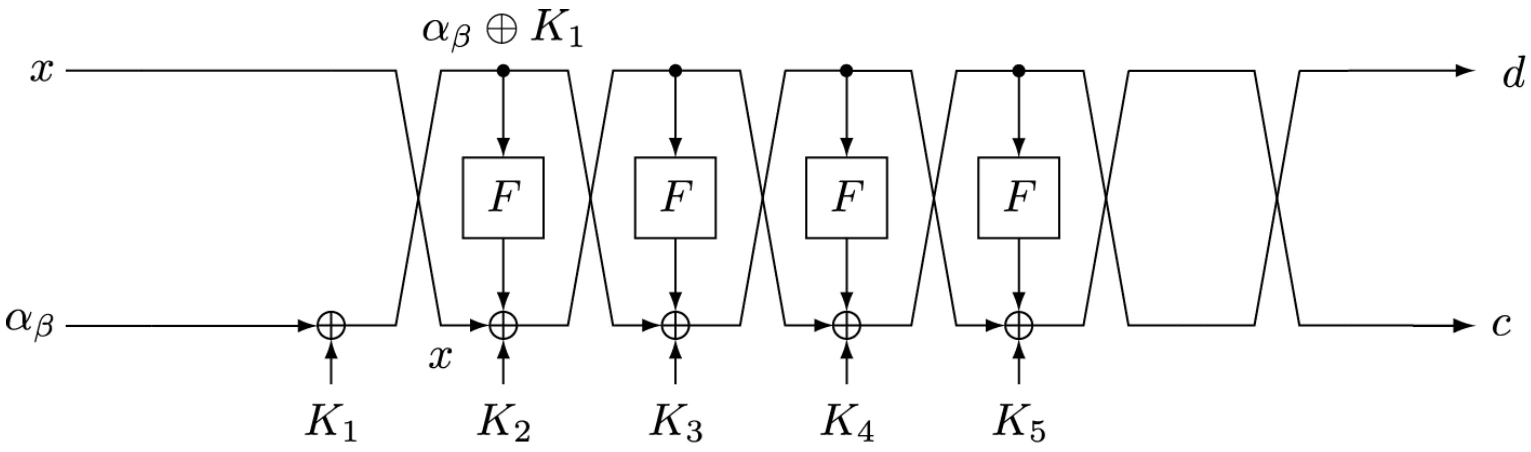


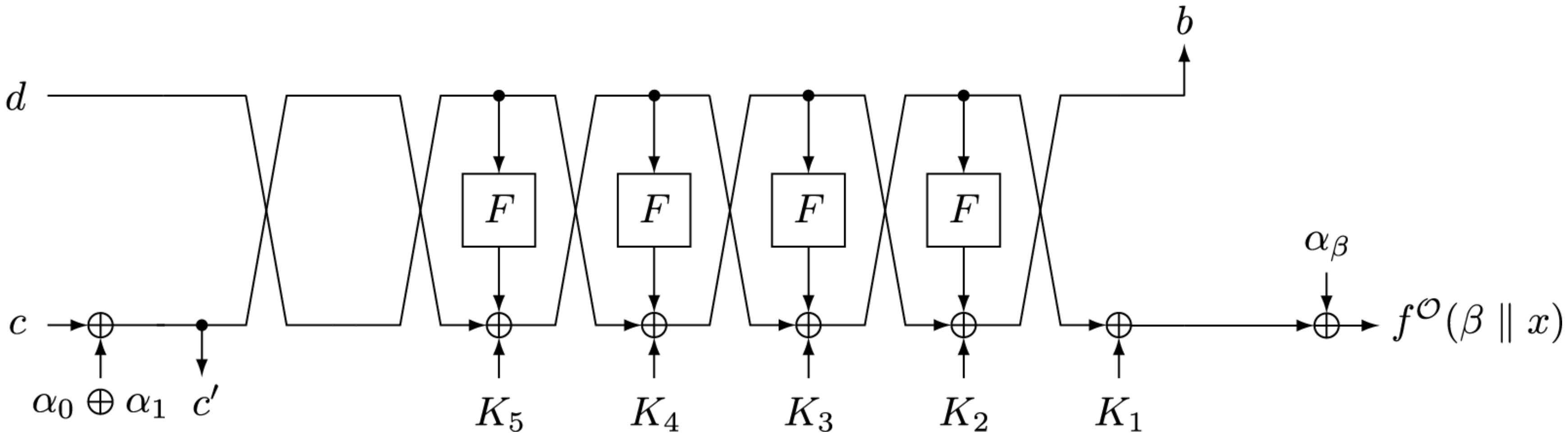
Quantum Distinguisher against 6-round Feistel-FK



- F in gray and K_6 has no effect

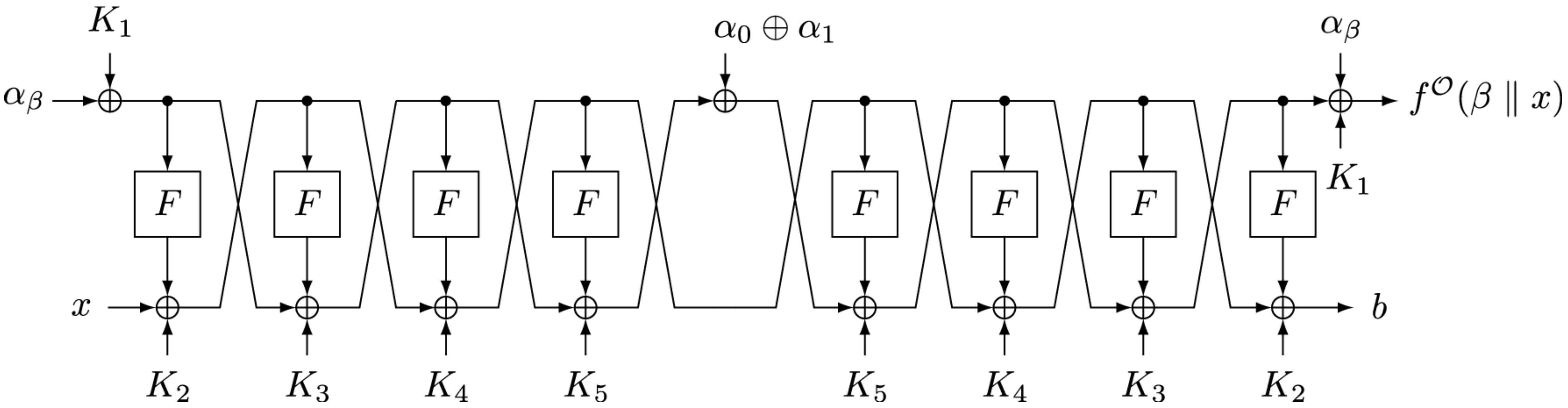
Quantum Distinguisher against 6-round Feistel-FK





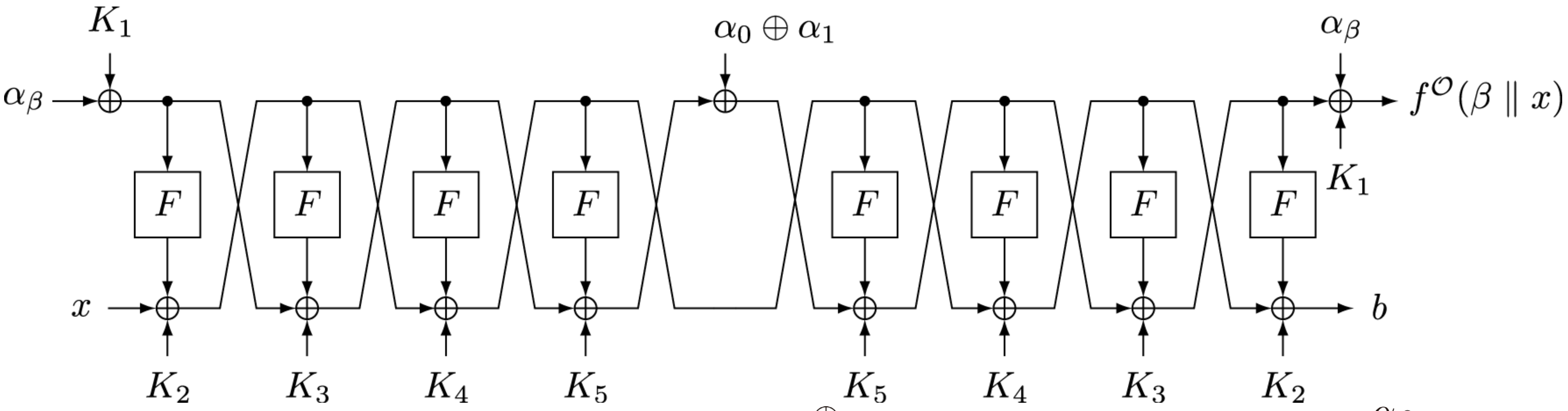
- Connect 2 figures

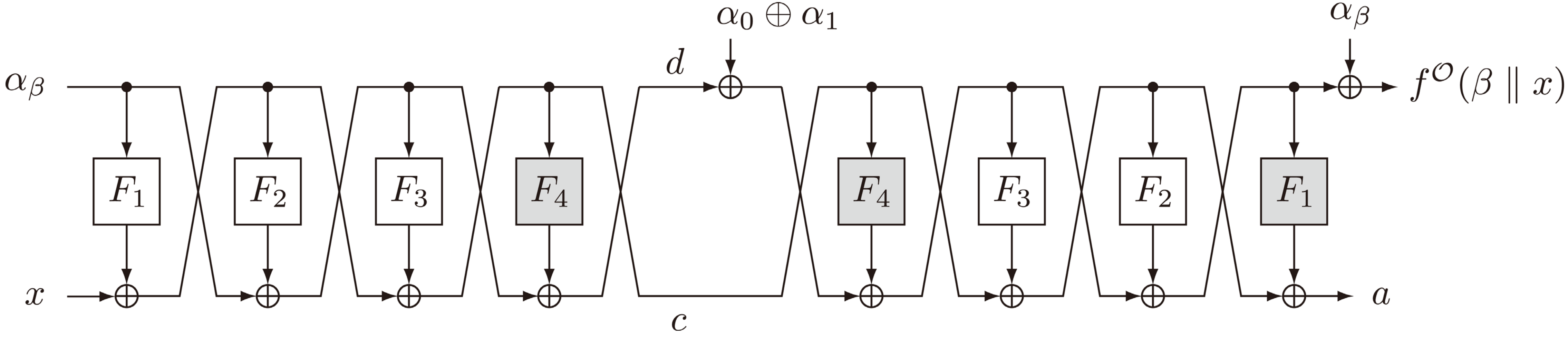
Quantum Distinguisher against 6-round Feistel-FK



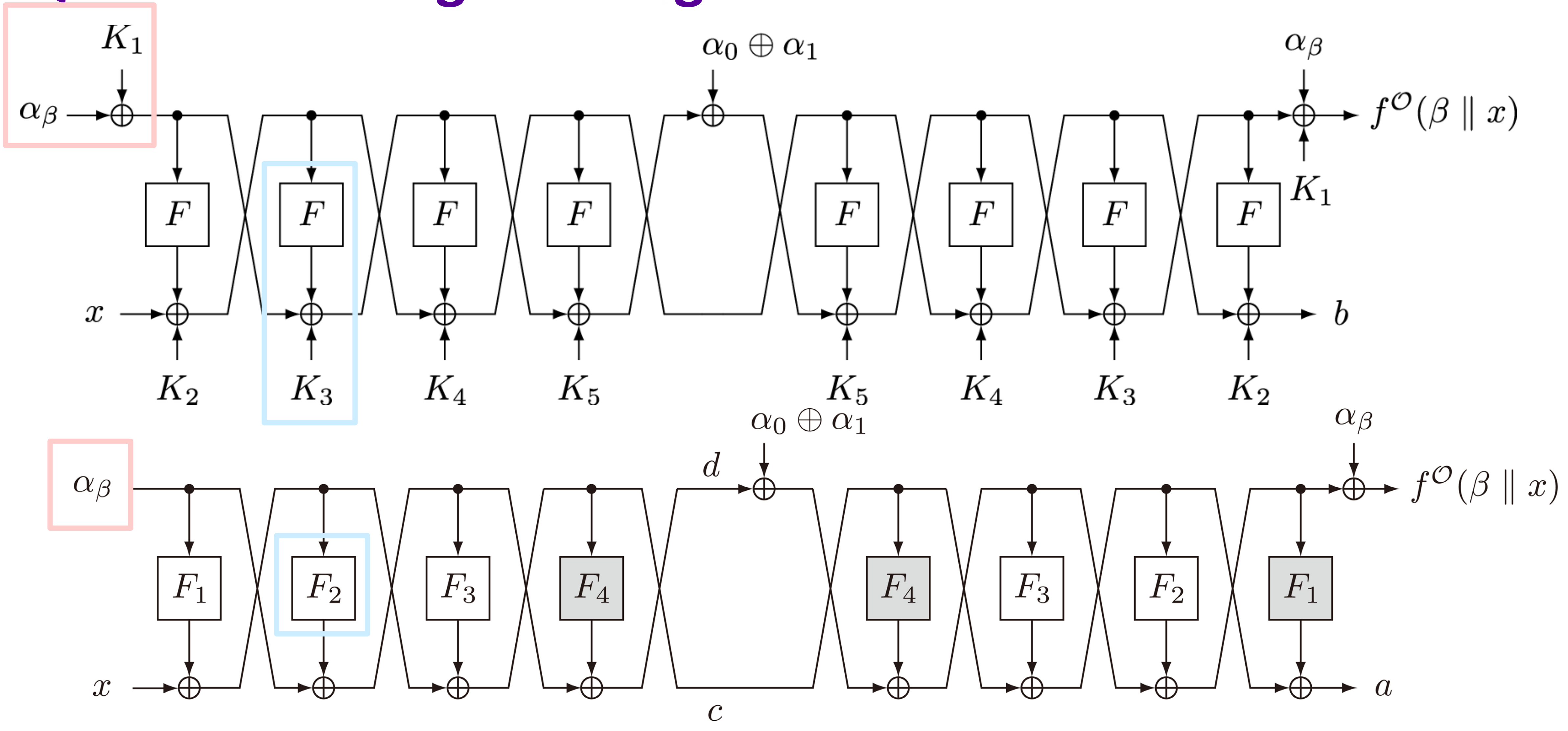
- Almost the same as the 4-round distinguisher

Quantum Distinguisher against 6-round Feistel-FK

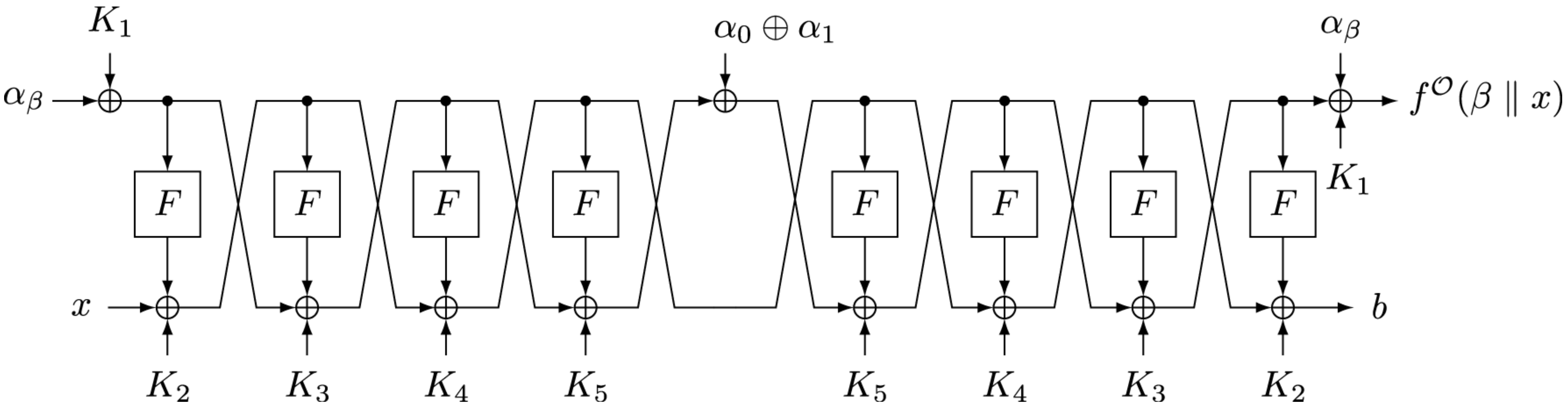




Quantum Distinguisher against 6-round Feistel-FK

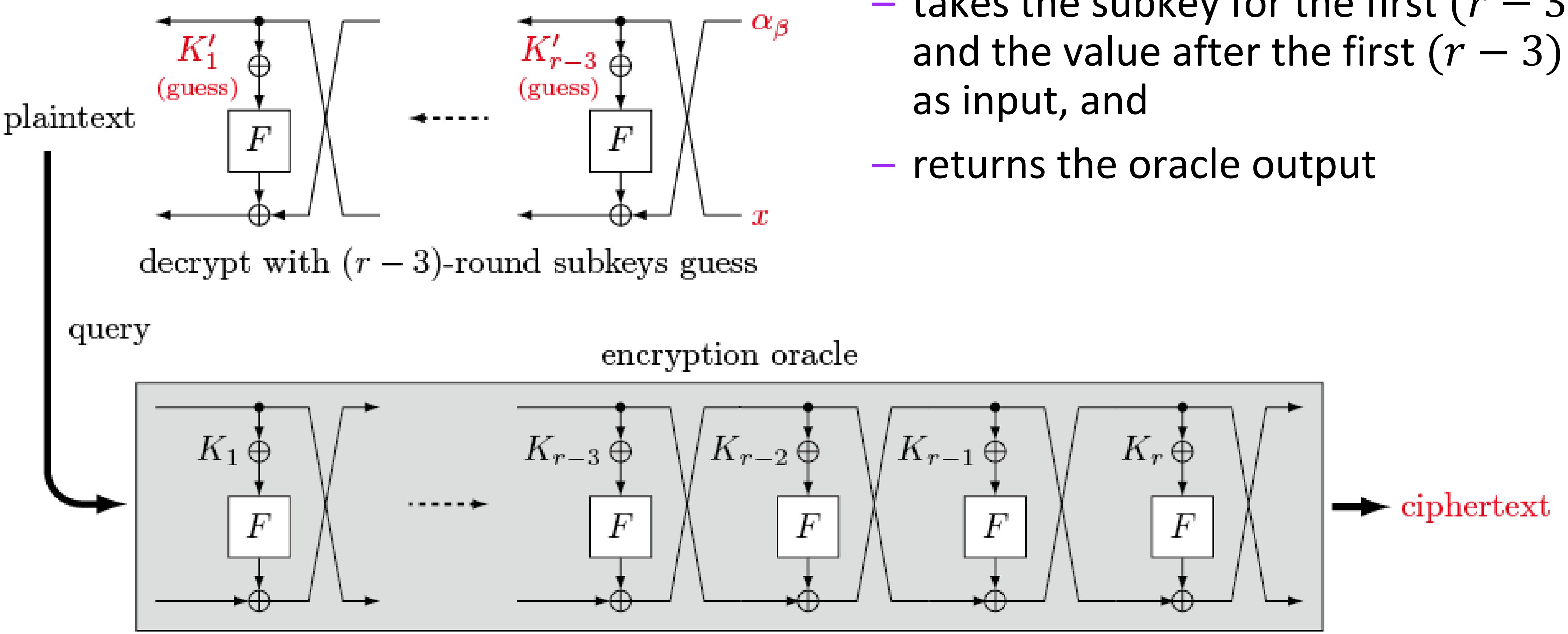


Quantum Distinguisher against 6-round Feistel-FK



- Almost the same as the 4-round distinguisher
  - Replace α_β with $\alpha_\beta \oplus K_1$
  - Replace $F_i(x)$ with $F(x) \oplus K_{i+1}$
- $s = \left(1 \parallel F(\alpha_0 \oplus K_1) \oplus F(\alpha_1 \oplus K_1)\right)$

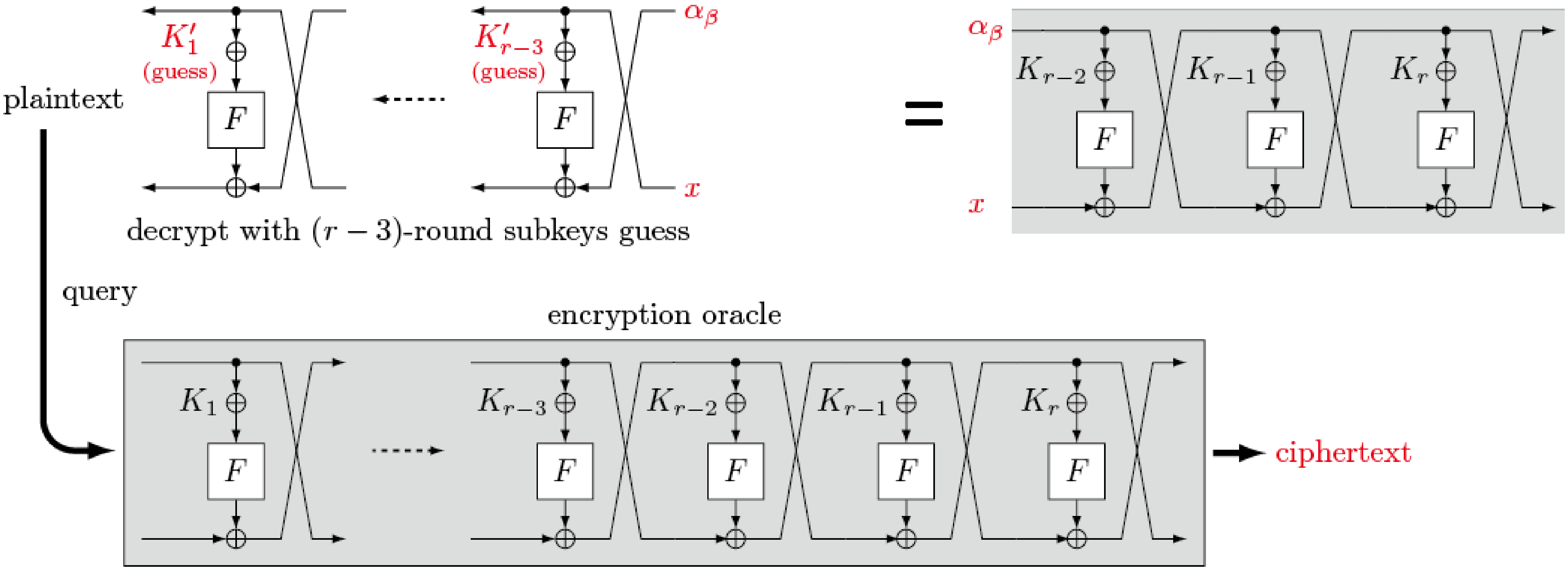
Key Recovery Attacks



1. Implement a quantum circuit $\mathcal{E}$ that
   - takes the subkey for the first $(r-3)$ round and the value after the first $(r-3)$ round as input, and
   - returns the oracle output

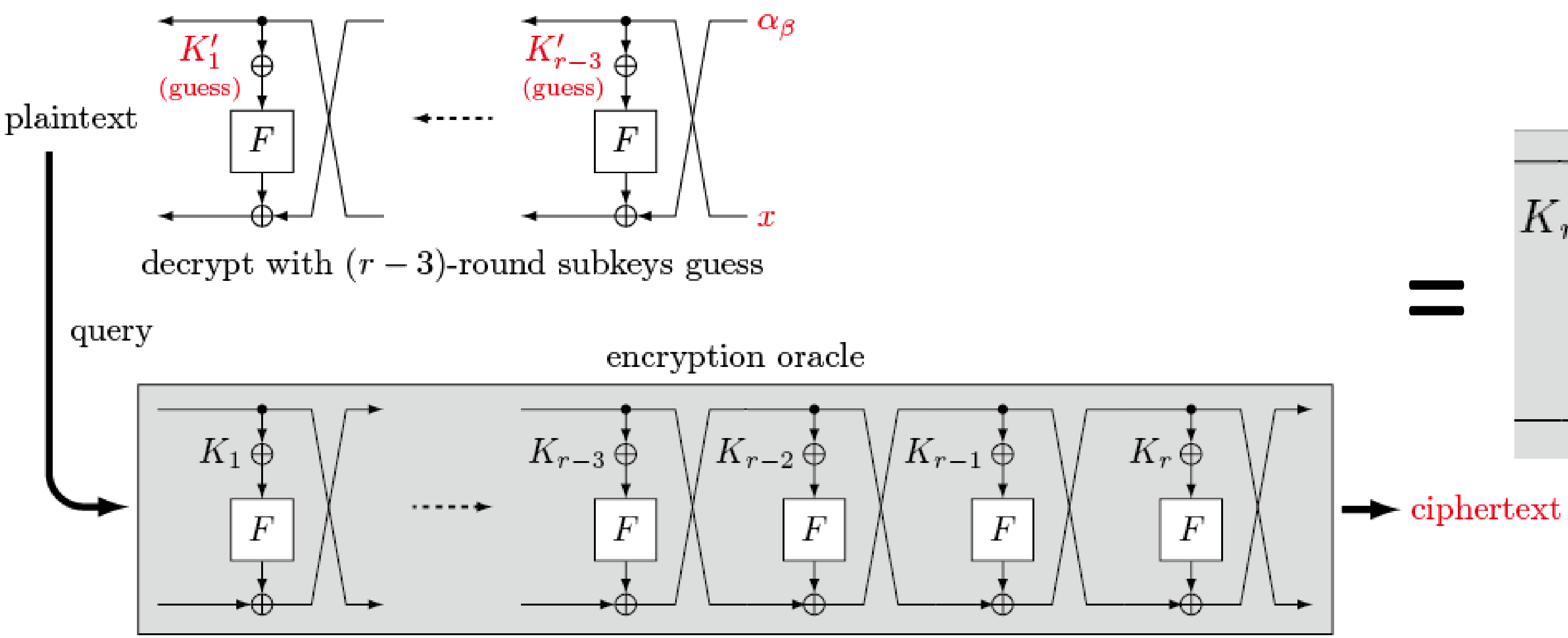
Key Recovery Attacks

- If the guess is correct



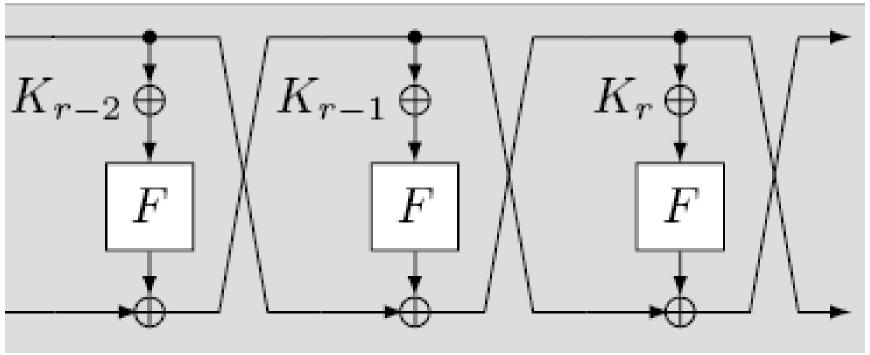
Key Recovery Attacks

2. For each guess, apply the distinguisher to $\mathcal{E}$
3. If the distinguisher returns that "this is a random permutation", then judge the guess is wrong, otherwise the guess is correct.



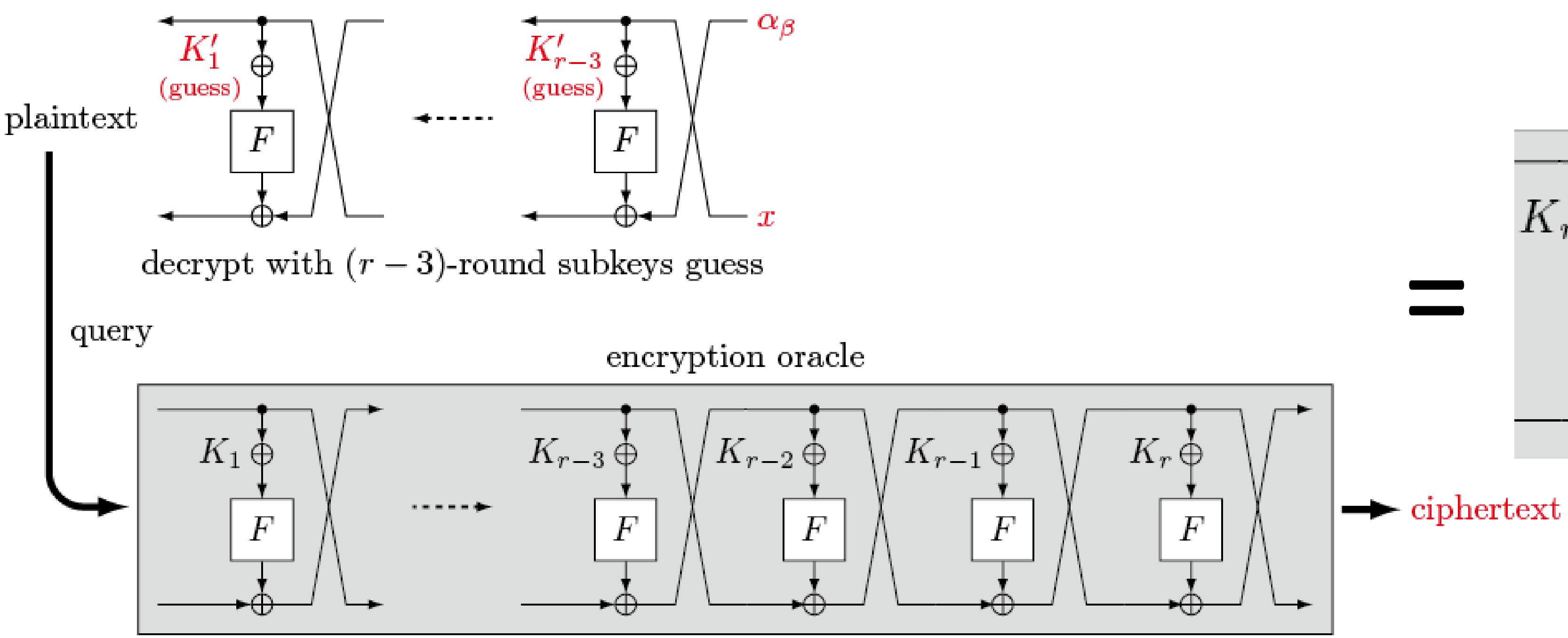
=

If the guess is correct

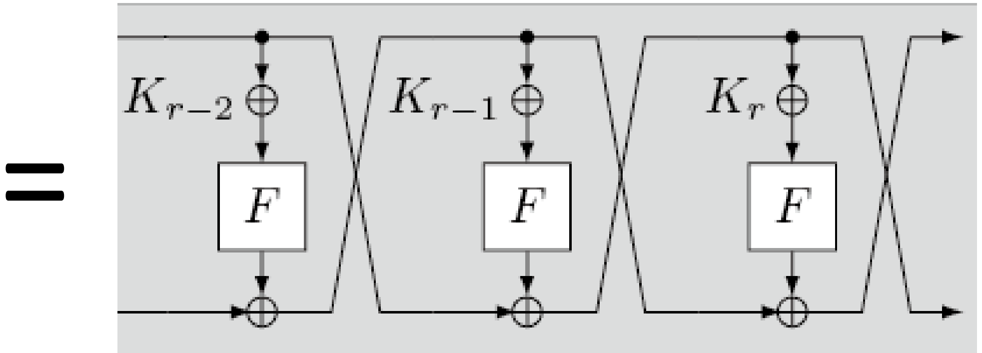


Key Recovery Attacks

- Exhaustive search of the first $(r-3)$ round : $O\left(\sqrt{2^{(r-3)n/2}}\right)$ by Grover search
- 3-round distinguisher : $O(n)$ for each subkeys guess



If the guess is correct



Key Recovery Attacks

- Combining Grover search and the distinguisher

7-round Feistel-KF Construction

- Recover $7n/2$-bit key with $O\left(2^{(r-4)n/4}\right) = O(2^{3n/4})$ (CCAs)

9-round Feistel-FK Construction

- Recover $9n/2$-bit key with $O\left(2^{(r-6)n/4}\right) = O(2^{3n/4})$ (CCAs)

8-round Feistel-FK Construction

- Recover $8n/2$-bit key with $O\left(2^{(r-5)n/4}\right) = O(2^{3n/4})$ (CPAs)

Outline

1. Introduction
2. Previous Quantum Distinguisher
3. Quantum CCAs against Feistel Constructions
   - Quantum Distinguisher against 4-round Feistel Constructions
   - Formalization of Quantum Distinguishers
   - Quantum CCAs against Practical Designs of Feistel Constructions
4. Concluding Remarks

Concluding Remarks

Rounds	3	4
Classic	CPA secure [LR88]	CCA secure [LR88]
Quantum	QCPA insecure [KM10]	QCCA insecure

Construction	Feistel-KF	Feistel-FK
Distinguish	4-round	6-round
Key Recovery	7-round	9-round (and 8-round QCPA)

Open Questions

- Tight bound on the number of rounds that we can attack Feistel-F
- Improving the complexity or extending the number of rounds of the attacks against Feistel-KF and Feistel-FK