Quantum Chosen-Ciphertext Attacks against Feistel Ciphers

Gembu Ito
Nagoya University

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

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

<table>
<thead>
<tr>
<th>Rounds</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic</td>
<td>CPA insecure</td>
<td>CPA secure [LR88]</td>
<td>CCA secure [LR88]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CCA insecure</td>
<td></td>
</tr>
</tbody>
</table>

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

Overview

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

<table>
<thead>
<tr>
<th>Rounds</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic</td>
<td>CPA insecure</td>
<td>CPA secure [LR88]</td>
<td>CCA secure [LR88]</td>
</tr>
<tr>
<td>Quantum</td>
<td>QCPA insecure [KM10]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

---

Overview

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

<table>
<thead>
<tr>
<th>Rounds</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic</td>
<td>CPA insecure</td>
<td>CPA secure [LR88]</td>
<td>CCA secure [LR88]</td>
</tr>
<tr>
<td></td>
<td>CCA insecure</td>
<td>CPA secure [LR88]</td>
<td>CCA secure [LR88]</td>
</tr>
<tr>
<td>Quantum</td>
<td>QCPA insecure [KM10]</td>
<td>QCCA insecure</td>
<td>QCCA insecure</td>
</tr>
</tbody>
</table>
Overview

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

<table>
<thead>
<tr>
<th>Rounds</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic</td>
<td>CPA insecure</td>
<td>CPA secure [LR88]</td>
<td>CCA secure [LR88]</td>
</tr>
<tr>
<td>Quantum</td>
<td>QCPA insecure [KM10]</td>
<td>QCCA insecure</td>
<td></td>
</tr>
</tbody>
</table>

- 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
  $$b_{i+1} \leftarrow a_i \oplus F_{K_i}(b_i), \quad a_{i+1} \leftarrow b_i$$
- $F_{K_i}$ 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 Diagram](image1)

![Feistel-FK Diagram](image2)
Main Tool: Simon’s algorithm [Sim97]

Problem

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

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

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

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

---

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]
  - ...

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 $\Pi \in \text{Perm}(n)$, 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 $\Pi$
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

$$f^O: \{0,1\} \times \{0,1\}^{n/2} \rightarrow \{0,1\}^{n/2}$$

$$(\beta || x) \mapsto c \oplus \alpha_\beta$$
Quantum Distinguisher against 3-round Feistel-F [KM10]

- $F_3$ does not contribute to $f^O$
- Orange line and $\alpha \beta$ cancel each other
Quantum Distinguisher against 3-round Feistel-F [KM10]
Quantum Distinguisher against 3-round Feistel-F [KM10]

- $f^O$ has a period $s = (1 \parallel F_1(\alpha_0) \oplus F_1(\alpha_1))$

\[
f^O(\beta \parallel x) = F_2 \left( x \oplus F_1(\alpha_\beta) \right)
= F_2 \left( x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1) \oplus F_1(\alpha_\beta \oplus 1) \right)
= f^O(\beta \oplus 1 \parallel x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1))
\]
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]

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

\[
\mathcal{O} : \{0,1\} \times \{0,1\}^{n/2} \rightarrow \{0,1\}^{n/2}
\]

\[(\beta \parallel x) \mapsto b \oplus \alpha_\beta\]
Quantum Distinguisher against 4-round Feistel-F

- $F_4$ has no effect
- Last $F_1$ does not contribute to $f^O$
Quantum Distinguisher against 4-round Feistel-F
Quantum Distinguisher against 4-round Feistel-F
Quantum Distinguisher against 4-round Feistel-F

\[ f^O(\beta \parallel x) \]
Quantum Distinguisher against 4-round Feistel-F

- Computation after $Z_{\beta\|x}$ does not depend on $\beta, x$
- $Z_{\beta\|x}$ has a period $s = (1 \parallel F_1(\alpha_0) \oplus F_1(\alpha_1))$
Quantum Distinguisher against 4-round Feistel-F

- $\alpha_\beta$ 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

- $\alpha_\beta$ 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 $\beta, x$
Quantum Distinguisher against 4-round Feistel-F

$Z_{\beta||x}$ has a period $s = 1$ since

$Z_{\beta||x} \oplus s = Z_{\beta||x}$

$Z_{0||x} \oplus s = x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1)$

$(Z_{0||x}) \oplus s = x \oplus F_1(\alpha_0) \oplus F_1(\alpha_1)$
Relaxing Simon’s Algorithm

- We know that $f(x) = f(x') \iff x' = x \oplus s$
- $f(x) = f(x') \Rightarrow x' = x \oplus s$ 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 $s_1, s_2, ...$
- To recover $s$ from $y_1, y_2, ..., f$ 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)
    ⇒ **dimension** of the space spanned by $y_1, y_2, ...$ is **at most** $n - 1$
  – If $f$ doesn’t have a period, $y_i$ can take any value of $\{0,1\}^n$
    ⇒ **dimension** can reach $n$

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)
    \[ \Rightarrow \text{dimension} \text{ of the space spanned by } y_1, y_2, \ldots \text{ is at most } n - 1 \]
  - If \( f \) doesn’t have a period, \( y_i \) can take any value of \( \{0,1\}^n \)
    \[ \Rightarrow \text{dimension} \text{ can reach } n \]

- 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

Relaxing Simon’s Algorithm

\[ \varepsilon_f^{\pi} = \max_{t \in \{0,1\}^l \setminus \{0^l\}} \Pr[f^\pi(x) = f^\pi(x \oplus x)] \quad (\pi \text{ is a fixed permutation}) \]

\[ \text{irr}_f^{\delta} = \{\pi \in \text{Perm}(n) \mid \varepsilon_f^{\pi} > 1 - \delta\} \quad (\delta \text{ is a small constant } 0 \leq \delta < 1) \]

- Checking the dimension of the space spanned by \( y_1, y_2, \ldots, y_\eta \)
- Success probability is at least

\[
1 - \frac{2^l}{e^{\delta \eta/2}} - \Pr[\Pi \in \text{irr}_f^{\delta}]\]

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

\[ f^O : \{0,1\} \times \{0,1\}^{n/2} \rightarrow \{0,1\}^{n/2} \]

\[(\beta \parallel x) \mapsto a \oplus F(b) \oplus \alpha_\beta\]
Quantum Distinguisher against 6-round Feistel-FK

\[ f^O : \{0,1\} \times \{0,1\}^{n/2} \rightarrow \{0,1\}^{n/2} \]
\[ (\beta \parallel x) \mapsto a \oplus F(b) \oplus \alpha_\beta \]
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 $\alpha_\beta$ with $\alpha_\beta \oplus K_1$
  - Replace $F_i(x)$ with $F(x) \oplus K_{i+1}$

\[ s = (1 \parallel F(\alpha_0 \oplus K_1) \oplus F(\alpha_1 \oplus K_1)) \]
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.
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

\[ \frac{46}{49} \]
Key Recovery Attacks

- Combining Grover search and the distinguisher

<table>
<thead>
<tr>
<th>Construction</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>7-round Feistel-KF</td>
<td>Recover $7n/2$-bit key with $O(2^{(r-4)n/4}) = O(2^{3n/4})$ (CCAs)</td>
</tr>
<tr>
<td>9-round Feistel-FK</td>
<td>Recover $9n/2$-bit key with $O(2^{(r-6)n/4}) = O(2^{3n/4})$ (CCAs)</td>
</tr>
<tr>
<td>8-round Feistel-FK</td>
<td>Recover $8n/2$-bit key with $O(2^{(r-5)n/4}) = O(2^{3n/4})$ (CPAs)</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Rounds</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic</td>
<td>CPA secure [LR88]</td>
<td>CCA secure [LR88]</td>
</tr>
<tr>
<td>Quantum</td>
<td>QCPA insecure [KM10]</td>
<td>QCCA insecure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Construction</th>
<th>Feistel-KF</th>
<th>Feistel-FK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distinguish</td>
<td>4-round</td>
<td>6-round</td>
</tr>
<tr>
<td>Key Recovery</td>
<td>7-round</td>
<td>9-round (and 8-round QCPA)</td>
</tr>
</tbody>
</table>

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