# Quantum Chosen-Ciphertext Attacks against Feistal Ciphers

Eleena Gupta

Indian Institute of Science, Bangalore

April 28, 2023

# Feistal Cipher

Feistal network is a Block Cipher with

- Input: $n$ bit state divided into two $n/2$ bit halves, $a_i$ and $b_i$.
- Key scheduling algorithm: From secret key $K$ of $l$-bits derive $l'$-bit "subkeys" $K_1, K_2, .., K_r$ for $r$ rounds.
- Round function: defined for each subkey:

$$F_{K_i} : \{0,1\}^{n/2} \times \{0,1\}^{l'} \rightarrow \{0,1\}^{n/2}$$

The state is updated iteratively in each round as

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

This is *Feistal-F* construction.

# Feistal Cipher

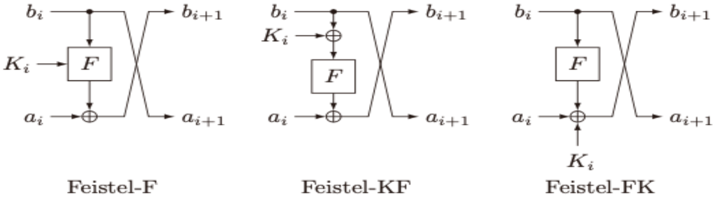
$F_{K_i}$ is a PRF which requires significant implementation costs. More practical versions are where each subkey $K_i \in \{0,1\}^{n/2}$, and $F_{K_i}$ is defined as

- *Feistal-KF*: $F_{K_i}(b_i) := F(K_i \oplus b_i)$, where $F$ is a public function (not a PRF), and

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

- *Feistal-FK*: $F_{K_i}(b_i) := F(b_i) \oplus K_i$,

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



# Classical Attacks

When $F_{K_i}$ is a PRF, there exists efficient attacks against:

- 2-round Feistal Cipher against chosen-plaintext attacks (CPA).
- 3-round Feistal Cipher against chosen-ciphertext attacks (CCA).

# Classical Attacks

When $F_{K_i}$ is a PRF, there exists efficient attacks against:

- 2-round Feistal Cipher against chosen-plaintext attacks (CPA).
- 3-round Feistal Cipher against chosen-ciphertext attacks (CCA).

3-round and 4-round Feistel ciphers are PRPs up to $O(2^{n/4})$ queries against CPAs and CCAs, respectively, hence secure.

Security changes under quantum attacks where superposition queries can be made.

# Quantum Attacks

- Grover's key search : $O(\sqrt{n})$ for an $n$ bit key
- Simon's Algorithm : detects a secret cycle-period in polynomial time of the output size.
  - Distinguisher : distinguish Feistel-cipher from a random permutation or the right key from the wrong key guesses.
  - Key recovery : cycle-period used for key recovery.

# Simon's Algorithm

*Problem statement* Given a periodic function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ with period $s \in \{0,1\}^n \backslash \{0^n\}$ such that for any $x \in \{0,1\}^n$, we have $f(x \oplus s) = f(x)$. Find the period $s$.

- Assume that Simon's algorithm has access to the quantum oracle $U_f$ which is defined as:

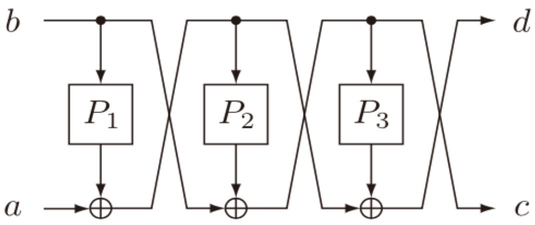
$$U_f|x\rangle|z\rangle = |x\rangle|z \oplus f(x)\rangle$$

- Use a circuit $S_f = (H^{\otimes n} \otimes I_n) \cdot U_f \cdot (H^{\otimes n} \otimes I_n)$ to compute vectors $y_i$ orthogonal to $s$ i.e. $y \cdot s = 0(mod2)$
- It solves the problem using *one* oracle query, and $O(n^2)$ other operations.

Let $FP_3$ be the encryption algorithm with $F_{K_i}$ as random permutations $P_i$.
Input : $(a, b) \in (\{0,1\}^{n/2})^2$
Output : $(c, d) \in (\{0,1\}^{n/2})^2$

$$c = b \oplus P_2(a \oplus P_1(b))$$

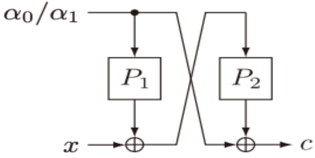
$$d = a \oplus P_1(b) \oplus P_3(b \oplus P_2(a \oplus P_1(b)))$$



# Quantum Distinguisher

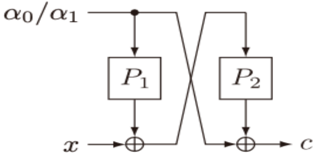
## Against the 3-round Feistal Cipher

Let the plaintext $(a, b) = (x, \alpha_\beta)$ where , $\beta \in \{0, 1\}$ and $x, \alpha_0, \alpha_1 \in \{0, 1\}^{n/2}$.




$$c \oplus \alpha_\beta = P_2(x \oplus P_1(\alpha_\beta))$$

Let the plaintext $(a, b) = (x, \alpha_\beta)$ where , $\beta \in \{0, 1\}$ and $x, \alpha_0, \alpha_1 \in \{0, 1\}^{n/2}$.




$$c \oplus \alpha_\beta = P_2(x \oplus P_1(\alpha_\beta))$$

Construct a function as:

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

If $\mathcal{O}$ is FP3, then,

$$f^{\mathcal{O}}(\beta || x) = P_2(x \oplus P_1(\alpha_\beta))$$

with a period $s = 1||(P_1(\alpha_0) \oplus P_1(\alpha_1))$.

# Quantum Distinguisher

## Against the 3-round Feistal Cipher

Apply Simon's algorithm to $f^{\mathcal{O}}$ and recover the period $s$.

- Randomly choose $\beta \in \{0, 1\}$ and $z \in \{0, 1\}^{n/2}$,
- Compute $f^{\mathcal{O}}(\beta||z)$ and $f^{\mathcal{O}}((\beta||z) \oplus s)$,
- If both are equal then output, "$\mathcal{O}$ is FP3."
- Else, $\mathcal{O}$ is $\Pi$.

If $\mathcal{O}$ is $\Pi$, Simon's algorithm return some random string $s'$, and the probability of $f^{\mathcal{O}}(\beta||z)$ and $f^{\mathcal{O}}((\beta||z) \oplus s)$ is about $2^{-n/2}$. Therefore, we can distinguish correctly in $O(n)$ queries.

This is a Quantum chosen-plaintext attack combining 3-round Feistal Cipher quantum distinguisher with the Grover search.

*Attack Idea*: Given the quantum encryption oracle of the $r$-round Feistal-KF construction, run the following procedures,

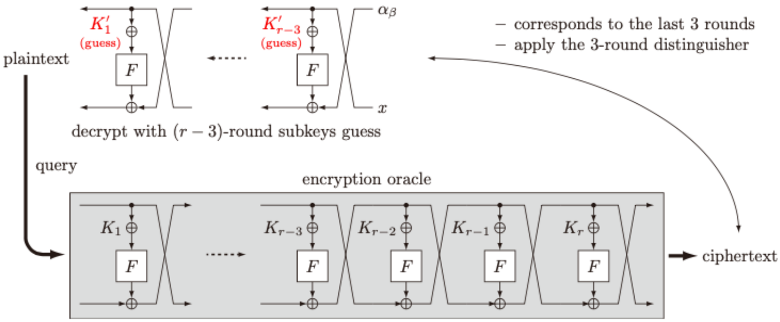



**Fig. 5.** Construction of $\mathcal{E}$ in the key recovery attack against the $r$-round Feistel-KF construction. The ciphertext corresponds to the output of the 3-round Feistel-KF construction which takes $(K_{r-2}, K_{r-1}, K_r)$ as subkeys and $(x, \alpha_\beta)$ as input.

# Key Recovery Attacks

## Against the Fiestal-KF Construction

1. Implement a quantum circuit $\mathcal{E}$ :
   - Input: subkeys of the first $(r-3)$ rounds and intermediate state value after the first $(r-3)$ rounds
   - Decrypt first $(r-3)$ rounds and compute the plaintext.
   - query the plaintext to the encryption oracle ( corresponds to the 3-round Fesital-KF)
   - return oracle output
2. Guess the first $(r-3)$ rounds subkeys, ( Grover). For each guess check its correctness as,
3. Apply the 3-round distinguisher to $\mathcal{E}$.
   1. Distinguisher $\rightarrow$ Random permutation $\implies$ wrong guess.
   2. Otherwise, the guess is correct.

# Key Recovery Attacks

## Against the Fiestal-KF Construction

Attack complexity:

- Length of first $(r-3)$ round subkeys is $((r-3)n/2)$,
- Grover search in time $O(\sqrt{2^{(r-3)n/2}})$,
- 3-round distinguisher runs in time $O(n)$ for each guess.
- Net running time of attack is $O(\sqrt{2^{(r-3)n/2}}) \times O(poly(n)) = \tilde{O}(2^{(r-3)n/4})$

# Relaxing Simon's Algorithm

Dimension of the space spanned by the vectors $y_1, y_2$.. ( obtained using $S_f$) is

- at most $|s| - 1$ if $f$ has non-zero period $s$,
- else, can reach $|s|$ with high probability.

Hence, distinguish $f$ without computing actual period $s$.

Distinguisher: Let $\mathcal{O} : \{0,1\}^n \rightarrow \{0,1\}^n$ be either an encryption scheme $E_K$ or a random permutation $\Pi$. The goal is to distinguish whether $\mathcal{O} = E_K$ or $\mathcal{O} = \Pi$.

# Relaxing Simon's Algorithm

## Distinguisher Algorithm

Construct a function $f^{\pi} : \{0,1\}^{l} \to \{0,1\}^{m},\ \pi \in Perm(n)$

- has a classical algorithm $\mathcal{A}$ which computes $f^{\pi}(x)$ in time $O(poly(l, m))$.
- For the encryption scheme $E_K$, $f^{E_K}$ has a period $s \in \{0,1\}^{l}$ depending on $K$.
- We expect $f^{\Pi}$ has no period with high probability.

**Algorithm 1** Distinguisher without recovering the period

1. Prepare an empty set $\mathcal{Y}$.
2. For $1 \le i \le \eta$, do:
3. Measure the first $\ell$ qubits of $\mathcal{S}_{f^{\mathcal{O}}} |0^{\ell+m}\rangle$ and add the obtained vector $y$ to $\mathcal{Y}$.
4. End For
5. Calculate the dimension $d$ of the vector space spanned by $\mathcal{Y}$.
6. If $d = \ell$, then output "$\mathcal{O}$ is $\Pi$." If $d < \ell$, output "$\mathcal{O}$ is $E_K$."

A parameter $\epsilon_f^\pi$ to capture the bias of the distribution of $y$ under the condition that random permutation $\Pi$ matches a fixed permutation $\pi$,

$$\epsilon_f^\pi = max_t Pr[f^\pi(x) = f^\pi(x \oplus t)]$$

it is small if $\pi$ is chosen uniformly at random.
A set of irregular permutations is defined for $0 \leq \delta < 1$ as

$$irr_f^\delta = \{\pi \in Perm(n) | \epsilon_f^\pi > 1 - \delta\}$$

The distinguisher failure probability is small if $Pr_\Pi[\Pi \in irr_f^\delta]$ is sufficiently small.

# Relaxing Simon's Algorithm

## Distinguisher Success Probability

A parameter $\epsilon_f^{\pi}$ to capture the bias of the distribution of $y$ under the condition that random permutation $\Pi$ matches a fixed permutation $\pi$,

$$\epsilon_f^{\pi} = max_t Pr[f^{\pi}(x) = f^{\pi}(x \oplus t)]$$

it is small if $\pi$ is chosen uniformly at random.
A set of irregular permutations is defined for $0 \leq \delta < 1$ as

$$irr_f^{\delta} = \{\pi \in Perm(n) | \epsilon_f^{\pi} > 1 - \delta\}$$

The distinguisher failure probability is small if $Pr_{\Pi}[\Pi \in irr_f^{\delta}]$ is sufficiently small.

Theorem: For $O(\eta)$ quantum queries by the distinguisher, it distinguishes $E_K$ from $\Pi$ with probability at least

$$1 - 2^l / e^{\delta\eta/2} - Pr_{\Pi}[\Pi \in irr_f^{\delta}].$$

Thank You!