Quantum Distinguishing Attacks against Type-1 Generalized Feistel Ciphers

Gembu Ito and Tetsu Iwata

Nagoya University, Furo-cho, Chikusa-ku, Nagoya 464-8603, Japan
g_itou@echo.nuee.nagoya-u.ac.jp, tetsu.iwata@nagoya-u.jp

Abstract. A generalized Feistel cipher is one of the methods to construct block ciphers, and it has several variants. Dong, Li, and Wang showed quantum distinguishing attacks against the $(2d-1)$-round Type-1 generalized Feistel cipher with quantum chosen-plaintext attacks, where $d \geq 3$, and they also showed key recovery attacks [Dong, Li, Wang. Sci China Inf Sci, 2019, 62(2): 022501].
In this paper, we show a polynomial time quantum distinguishing attack against the $(3d-3)$-round version, i.e., we improve the number of rounds by $(d-2)$. We also show a quantum distinguishing attack against the (d^2-d+1)-round version in the quantum chosen-ciphertext setting. We apply these quantum distinguishing attacks to obtain key recovery attacks against Type-1 generalized Feistel ciphers.

Keywords: Generalized Feistel cipher · Simon's algorithm · Grover search · Quantum cryptanalysis

1 Introduction

Zheng, Matsumoto, and Imai proposed Type-1, Type-2, and Type-3 generalized Feistel ciphers, which are dn-bit block ciphers composed of n-bit round functions, where $d \geq 3$ [ZMI89]. These constructions are suitable for small-scale implementations because the internal round function can be smaller as the number of branches d grows. Several block ciphers are based on this construction, e.g., we see CAST-256 [AG99] and MAME [YWO+07] (Type-1), CLEFIA [SSA+07] and RC6 [RRSY98] (Type-2), and MARS [BCD+99] (Type-3).

The seminal work of Shor's algorithm [Sho97] shows that a wide class of public key cryptosystems can be broken once quantum computers are developed. On the other hand, for symmetric key cryptosystems, Kuwakado and Morii showed that the impact of the development of quantum computers is also significant. Specifically, Kuwakado and Morii presented a quantum distinguishing attack against the 3-round Feistel cipher, where the adversary can make quantum superposition queries [KM10]. Feistel cipher with 3 rounds is known to be secure in the classical setting [LR88], and hence the result proves that the security significantly changes in the quantum setting. They used Simon's algorithm [Sim97] that finds a secret cycle-period in polynomial-time. Since then, many quantum attacks using Simon's algorithm have been proposed. Examples include a key

recovery attack against Even-Mansour cipher [KM12], forgery attacks on various MACs [KLLN16], cryptanalysis of AEZ [Bon17], and distinguishing attacks against Type-1 and Type-2 generalized Feistel ciphers [DLW19]. Furthermore, Leander and May [LM17] showed a key recovery attack against FX construction by combining Grover search [Gro96] and Simon's algorithm. Given these examples, it is important to evaluate the impact of quantum attacks on symmetric cryptosystems.

In the classical setting, Zheng et al. showed that the $(2d-1)$-round Type-1 generalized Feistel cipher is secure against chosen-plaintext attacks [ZMI89]. See also the analyses by Moriai and Vaudenay [MV00], and by Hoang and Rogaway [HR10]. On the other hand, in the quantum setting, Dong, Li, and Wang showed a distinguishing attack against the $(2d-1)$-round version with quantum chosen-plaintext attacks by using Simon's algorithm [DLW19]. They also showed a key recovery attack against the (d^2-d+2)-round version in time $O(2^{(\frac{d^2}{2}-\frac{3d}{2}+2)\cdot\frac{k}{2}})$ by using the $(2d-1)$-round distinguisher, where k is the key length of the internal round function.

In this paper, we continue the work of Dong, Li, and Wang [DLW19] to evaluate the security of Type-1 generalized Feistel cipher against quantum attacks.

- First, we show a polynomial time distinguishing attack against the $(3d-3)$-round version. This improves the number of rounds by $(d-2)$. Our idea is to shift the position of α_b, which is a constant used to define a period, so that the period is preserved for longer rounds. It turns out that the idea is simple, but still effective to improve the number of rounds that we can attack.
- Next, assuming that we are in the quantum chosen-ciphertext setting, we show a distinguishing attack against the (d^2-d+1)-round version. The number of rounds is significantly larger than the above, and this follows the intuition in the classical setting where the diffusion of Type-1 generalized Feistel cipher in the decryption direction is slow, which is pointed out in [MV00].
- Finally, we consider key recovery attacks by using the distinguishers. With the $(3d-3)$-round distinguisher, base on Dong et al.'s key recovery attack, we obtain a key recovery attack against the d^2-round version in time $O(2^{(\frac{d^2}{2}-\frac{3d}{2}+2)\cdot\frac{k}{2}})$.

  With the (d^2-d+1)-round distinguisher in the decryption direction, we obtain an r-round key recovery attack in time $O(2^{\frac{(r-(d^2-d+1))k}{2}})$, which is better than the one with $(3d-3)$-round distinguisher when $d>3$.

It is interesting to note that our $(3d-3)$-round distinguisher outperforms the classical provable security result, i.e., there are examples where a block cipher is provably secure in the classical sense with r rounds, and there is a matching quantum distinguishing attack that breaks the r-round version, but our result shows an example that a quantum attack can break much more rounds than r.

A summary of key recovery attacks is shown in Table 1.

Table 1. Key Recovery Attacks against Type-1 Generalized Feistel Cipher

Distinguisher	Round	Complexity (log)
$2d-1$ [DLW19]	$r \geq d^2-d+2$	$(\frac{1}{2}d^2-\frac{3}{2}d+2)\cdot\frac{k}{2}+\frac{(r-d^2+d-2)k}{2}$
$3d-3$ [Ours]	$r \geq d^2$	$(\frac{1}{2}d^2-\frac{3}{2}d+2)\cdot\frac{k}{2}+\frac{(r-d^2)k}{2}$
d^2-d+1 [Ours]	$r \geq d^2-d+1$	$\frac{(r-(d^2-d+1))k}{2}$

Paper Outline. This paper is organized as follows: Section 2 describes preliminaries. Section 3 introduces previous work. Section 4 presents our $(3d-3)$-round quantum distinguisher against Type-1 generalized Feistel cipher. In Sect. 5, we show the (d^2-d+1)-round quantum distinguisher by using the quantum decryption oracle. Section 6 presents key recovery attacks against Type-1 generalized Feistel cipher by using our quantum distinguishers. We conclude the paper in Sect. 7

2 Preliminaries

2.1 Notation

For a positive integer n, let $\{0,1\}^n$ be the set of all strings of n bits. Let $\mathrm{Perm}(n)$ be the set of all permutations on $\{0,1\}^n$, and let $\mathrm{Func}(n)$ be the set of all function from $\{0,1\}^n$ to $\{0,1\}^n$. For vectors a and b of the same dimension, we denote their inner product by $a \cdot b$. In this paper, e denotes Napier's number.

2.2 Type-1 Generalized Feistel Ciphers

In this section, we describe Type-1 generalized Feistel ciphers [ZMI89]. In Type-1 generalized Feistel cipher, we divide the dn-bit state into d branches, where $d \geq 3$ and each branch constitutes an n-bit sub-block. Let Φ_r denote the encryption algorithm of the r-round Type-1 generalized Feistel cipher, and Φ_r^{-1} denote its decryption algorithm. Let $R_1, R_2, \ldots, R_r \in \mathrm{Func}(n)$ be the keyed round functions of Φ_r. We assume that the function R_i takes a k-bit key k_i as input (thus the total key length of Φ_r is rk bits). Φ_r takes a plaintext $(x_0^0, x_1^0, \ldots, x_{d-1}^0) \in (\{0,1\}^n)^d$ as input, and outputs a ciphertext $(x_0^r, x_1^r, \ldots, x_{d-1}^r) \in (\{0,1\}^n)^d$, where the i-th round is defined as

$$(x_0^{i-1}, x_1^{i-1}, \ldots, x_{d-1}^{i-1}) \mapsto (R_i(x_0^{i-1}) \oplus x_1^{i-1}, x_2^{i-1}, x_3^{i-1}, \ldots, x_{d-1}^{i-1}, x_0^{i-1}).$$

The decryption is defined in an obvious way. Figure 1 shows the i-th round of Type-1 generalized Feistel cipher.

2.3 Simon's Algorithm

Here we review Simon's algorithm [Sim97] that is the basis of our distinguishers. Simon's algorithm can solve the following problem efficiently.

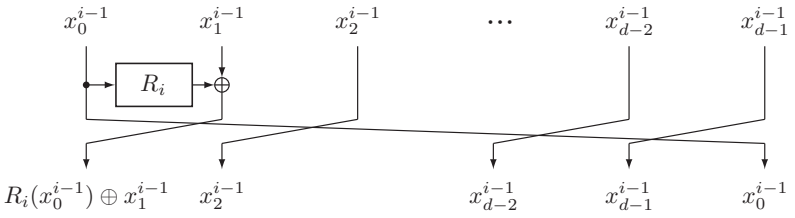

Fig. 1. The i-th round of Type-1 generalized Feistel cipher

Problem 1. Given a function $f : \{0,1\}^n \to \{0,1\}^n$ that has a non-zero period $s \in \{0,1\}^n$ such that

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

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

We need $O(2^{n/2})$ queries to find s in the classical setting. On the other hand, Simon's algorithm can find s with $O(n)$ quantum queries.

We explain how Simon's algorithm works. We assume that we have access to the quantum oracle U_f, which is defined as $U_f |x\rangle |z\rangle = |x\rangle |z \oplus f(x)\rangle$. For an n-qubit state $|x\rangle$, Hadamard transformation $H^{\otimes n}$ is defined as $H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$. Simon proposed a circuit $\mathcal{S}_f$ that computes a vector that is orthogonal to s for a periodic function f, which is defined as $\mathcal{S}_f = (H^{\otimes n} \otimes I_n) \cdot U_f \cdot (H^{\otimes n} \otimes I_n)$ and works as follows.

$$\begin{aligned}
\mathcal{S}_f |0^n\rangle |0^n\rangle &= (H^{\otimes n} \otimes I_n) \cdot U_f \cdot (H^{\otimes n} \otimes I_n) |0^n\rangle |0^n\rangle \\
&= (H^{\otimes n} \otimes I_n) \cdot U_f \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |0^n\rangle \\
&= (H^{\otimes n} \otimes I_n) \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle \\
&= \frac{1}{2^n} \sum_{x,y} (-1)^{x \cdot y} |y\rangle |f(x)\rangle \qquad (1)
\end{aligned}$$

If f satisfies $f(x) = f(x') \Leftrightarrow x' = x \oplus s$, then (1) can be rearranged as

$$\frac{1}{2^n} \sum_{x \in V, y} ((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}) |y\rangle |f(x)\rangle ,$$

where V is a linear subspace of $\{0,1\}^n$ of dimension $(n-1)$ that partitions $\{0,1\}^n$ into cosets V and $V + s$. The vector y such that $y \cdot s \equiv 1 \pmod 2$ satisfies $(-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y} = 0$. Therefore, the vector y that we obtain by measuring $\mathcal{S}_f |0^n\rangle |0^n\rangle$ satisfies $y \cdot s \equiv 0 \pmod 2$. By repeating this measurement for $O(n)$ times, we obtain $(n-1)$ linearly independent vectors that are all orthogonal to s with a high probability. Then we can recover s by solving the system of linear equations with $O(n^3)$ classical steps.

2.4 Qunatum Distinguisher based on Simon's Algorithm

Next, we introduce a quantum distinguisher based on Simon's algorithm. We follow the approach of Kaplan et al. [KLLN16] and Santoli and Schaffner [SS17], and the formalization by Ito et al. [IHM+19]. To recover s with Simon's algorithm, the function f has to satisfy $f(x) = f(x') \Leftrightarrow x' = x \oplus s$. However, for distinguishers, the condition can be relaxed.

In more detail, suppose that we are given an oracle $\mathcal{O} : \{0,1\}^n \to \{0,1\}^n$, which is either an encryption algorithm $E_K \in \mathrm{Perm}(n)$ or a random permutation $\mathit{\Pi} \in \mathrm{Perm}(n)$, and our goal is to distinguish the two cases. We assume that the quantum oracles $U_{\mathcal{O}}$ and $U_{\mathcal{O}^{-1}}$ are given. The distinguisher in [IHM+19] can be applied to a function $f^{\mathcal{O}} : \{0,1\}^\ell \to \{0,1\}^m$, where there exists a non-zero period s when $\mathcal{O} = E_K$, i.e., $f^{\mathcal{O}}$ such that $f^{E_K}(x) = f^{E_K}(x \oplus s)$ holds for all x. We expect that, with a high probability, $f^{\mathit{\Pi}}$ does not have any period. The distinguisher works as follow.

1. Prepare an empty set $\mathcal{Y}$.
2. Measure the first ℓ qubits of $\mathcal{S}_{f^{\mathcal{O}}} |0^{\ell+m}\rangle$ and add the obtained vector y to $\mathcal{Y}$ for η times.
3. Calculate the dimension d of the vector space spanned by $\mathcal{Y}$.
4. If $d = \ell$, then output $\mathcal{O} = \mathit{\Pi}$, otherwise output $\mathcal{O} = E_K$.

If $f^{\mathcal{O}}$ has the period s, the obtained vector y is orthogonal to s. Therefore the dimension d of the vector space spanned by $\mathcal{Y}$ is at most $\ell - 1$. On the other hand, if $f^{\mathcal{O}}$ has no period, the dimension can reach ℓ. Thus we can distinguish the two cases by checking the dimension.

This distinguisher fails only if $\mathcal{O} = \mathit{\Pi}$ and the dimension of the vector space spanned by $\mathcal{Y}$ is less than ℓ. To analyze the success probability of the distinguisher, define a parameter ϵ_f^π as

$$\epsilon_f^\pi = \max_{t \in \{0,1\}^\ell \setminus \{0^\ell\}} \Pr_x \left[f^\pi(x) = f^\pi(x \oplus t) \right],$$

where $\pi \in \mathrm{Perm}(n)$ is a fixed permutation. This parameter shows how the dimension of y is biased when $\mathit{\Pi} = \pi$. If this parameter is large (i.e., there exists t that is close to a period), then with a high probability, the vector space spanned by $\mathcal{Y}$ is orthogonal to t. Thus, we take a small constant $0 \le \delta < 1$ arbitrarily, and we say that a permutation π is irregular if $\epsilon_f^\pi > 1 - \delta$. In addition, define the set of the irregular permutations irr_f^δ as

$$\mathsf{irr}_f^\delta = \{\pi \in \mathrm{Perm}(n) \mid \epsilon_f^\pi > 1 - \delta\}.$$

The following theorem was proved.

Theorem 1 ([IHM+19]). *Let ℓ and m be positive integers that are $O(n)$. Assume that we have a quantum circuit with $O(poly(\ell, m))$ qubits which computes $f^{\mathcal{O}} : \{0,1\}^\ell \to \{0,1\}^m$ by making $O(1)$ queries to $\mathcal{O}$, and runs in time $T(\ell, m)$.*

The distinguisher makes $O(\eta)$ quantum queries, and distinguishes E_K from Π with probability at least

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

This shows that the distinguisher succeeds if $\Pr_{\Pi}[\Pi \in \mathsf{irr}_f^\delta]$ is a small value.

2.5 Combining Grover Search and Distinguishers

Leander and May combined Grover search and Simon's algorithm to show a key recovery attack against FX constructions [LM17]. Hosoyamada and Sasaki [HS18], and Dong and Wang [DW18] showed key recovery attacks against Feistel ciphers by using this combining technique.

Grover Search. Grover search provides a quadratic speed up on unsorted-database search [Gro96]. Let N be the number of elements in the database, and assume that there exists only one target element. In the classical setting, we can find the target element in time $O(N)$. However, in the quantum setting, Grover's algorithm can find it in time $O(\sqrt{N})$.

This algorithm was generalized later as quantum amplitude amplification by Brassard et al. as in the following theorem.

Theorem 2 ([BHMT02]). *Let $\mathcal{A}$ be any quantum algorithm on q qubits that uses no measurement. Let $\mathcal{B} : \{0,1\}^q \to \{0,1\}$ 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 $m = \lfloor \pi/4\theta_p \rfloor$, where θ_p is defined so that $\sin^2(\theta_p) = p$ and $0 < \theta_p \leq \pi/2$. Moreover, define the unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_{\mathcal{B}}$, where the operator $S_{\mathcal{B}}$ conditionally changes the sign of the amplitudes of the good states,*

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

while the operate S_0 changes the sign of the amplitude if and only if the state is the zero state $|0\rangle$. Then, after the computation of $Q^m\mathcal{A}|0\rangle$, a measurement is good with probability at least $\max\{1-p, p\}$.

Key Recovery Attack against FX Constructions. FX construction by Killian and Rogaway is a way to extend the key length of a block cipher [KR96, KR01]. Let E be an n-bit block cipher that takes an m-bit key k_0 as input. FX construction under two additional n-bit keys k_1, k_2 is described as

$$\mathrm{Enc}(x) = E_{k_0}(x \oplus k_1) \oplus k_2.$$

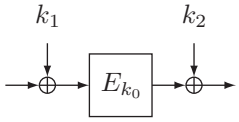

Fig. 2. FX construction

Figure 2 shows FX construction.

Leander and May constructed a function $f(k, x)$ that is defined as

$$f(k, x) = \mathrm{Enc}(x) \oplus E_k(x) = E_{k_0}(x \oplus k_1) \oplus k_2 \oplus E_k(x).$$

If $k = k_0$, $f(k, x)$ satisfies $f(k, x) = f(k, x \oplus k_1)$ for all $x \in \{0,1\}^n$. That is, the function $f(k_0, \cdot)$ has a period k_1. However, if $k \neq k_0$, with a high probability, the function $f(k, \cdot)$ does not have any period. Then they apply Grover search over $k \in \{0,1\}^m$. They construct the classifier $\mathcal{B}$ that identifies the sates as good if $k = k_0$ by using Simon's algorithm to $f(k, \cdot)$. The complexity of Grover search is $O(2^{m/2})$ and Simon's algorithm runs in time $O(n)$ in the classifier $\mathcal{B}$. Thus this attack runs in time $O(2^{m/2})$. For more details, see [LM17].

3 Previous Attacks

In this section, we review the quantum attacks against Type-1 generalized Feistel ciphers by Dong et al. [DLW19]. They showed a $(2d-1)$-round distinguishing attack and a $(d^2 - d + 2)$-round key recovery attack.

We first review the distinguishing attack. Let $\alpha_0, \alpha_1 \in \{0,1\}^n$ be two arbitrary distinct n-bit constants, and $x_1^0, x_2^0, \ldots, x_{d-2}^0 \in \{0,1\}^n$ be arbitrary n-bit constants. Given the oracle $\mathcal{O}$, they define a function $f^{\mathcal{O}}$ as

$$\begin{aligned} f^{\mathcal{O}} : \{0,1\} \times \{0,1\}^n &\to \{0,1\}^n \\ (b, x) &\mapsto \alpha_b \oplus y_1, \\ \text{where } (y_0, y_1, \ldots, y_{d-1}) &= \mathcal{O}(\alpha_b, x_1^0, x_2^0, \ldots, x_{d-2}^0, x). \end{aligned} \tag{2}$$

Let the intermediate state value after the first i rounds be $(x_0^i, x_1^i, \ldots, x_{d-1}^i)$. If $\mathcal{O}$ is Φ_{2d-1}, then the function $f^{\mathcal{O}}$ is described as

$$\begin{aligned} f(b, x) &= \alpha_b \oplus x_1^{2d-1} \\ &= \alpha_b \oplus x_0^d \\ &= \alpha_b \oplus R_d(x_0^{d-1}) \oplus \alpha_b \\ &= R_d(R_{d-1}(R_{d-2}(\cdots R_2(R_1(\alpha_b) \oplus x_1^0) \oplus x_2^0 \cdots) \oplus x_{d-2}^0) \oplus x), \end{aligned} \tag{3}$$

where in the second equality, we use the fact that $x_0^i = x_{d-1}^{i+1} = x_{d-2}^{i+2} = \cdots = x_1^{i+d-1}$ (See Fig. 3). Let $h(\cdot) = R_{d-1}(R_{d-2}(\cdots R_2(R_1(\cdot) \oplus x_1^0) \oplus x_2^0 \cdots) \oplus x_{d-2}^0)$. We see that $h(\cdot)$ is a function that is independent of the input (b, x), since

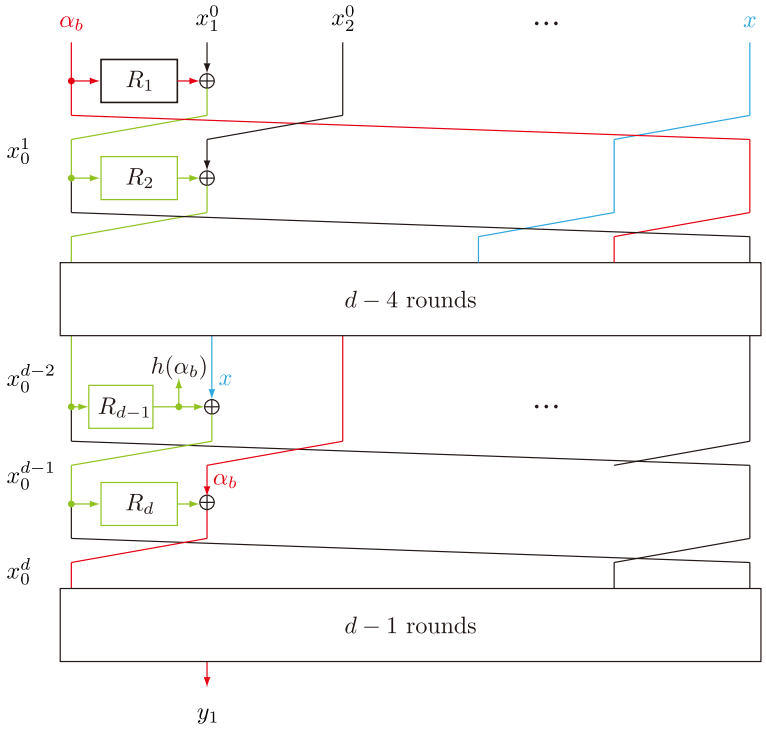

Fig. 3. $(2d-1)$-round distinguishing attack

$x_1^0, x_2^0, \ldots, x_{d-2}^0$ are constants. By using $h(\cdot)$, we can describe (3) as $f^{\mathcal{O}} = R_d(h(\alpha_b) \oplus x)$, and $f^{\mathcal{O}}$ satisfies

$$\begin{aligned} f(b,x) &= R_d(h(\alpha_b) \oplus x) \\ &= R_d(h(\alpha_{b\oplus 1}) \oplus h(\alpha_0) \oplus h(\alpha_1) \oplus x) \\ &= f(b \oplus 1, x \oplus h(\alpha_0) \oplus h(\alpha_1)). \end{aligned}$$

This implies that the function $f^{\mathcal{O}}$ has the period $(1, h(\alpha_0) \oplus h(\alpha_1))$.

If $f^{\mathcal{O}}$ is Π, then with a high probability, $f^{\mathcal{O}}$ does not have any period. Therefore, $\Pr_{\Pi}[\Pi \in \mathsf{irr}_f^{\delta}]$ is a small value and we can distinguish the two cases.

We next review the key recovery attack. We recover the key of the (d^2-d+2)-round Type-1 generalized Feistel cipher by appending (d^2-3d+3) rounds after the $(2d-1)$-round distinguisher (See Fig. 4). The subkey length that we need to recover is $(\frac{d^2}{2} - \frac{3d}{2} + 2)k$ bits. Thus, the time complexity of the exhaustive search for (d^2-d+2) rounds by Grover search is $O(2^{(\frac{d^2}{2} - \frac{3d}{2}+2)\cdot\frac{k}{2}})$. The distinguisher runs in time $O(n)$ and the time complexity of this attack is $O(2^{(\frac{d^2}{2} - \frac{3d}{2}+2)\cdot\frac{k}{2}})$.

We see that this attack is better than the direct application of Grover search to the entire $(d^2-d+2)k$-bit subkey. If we recover the key of $r > d^2-d+2$

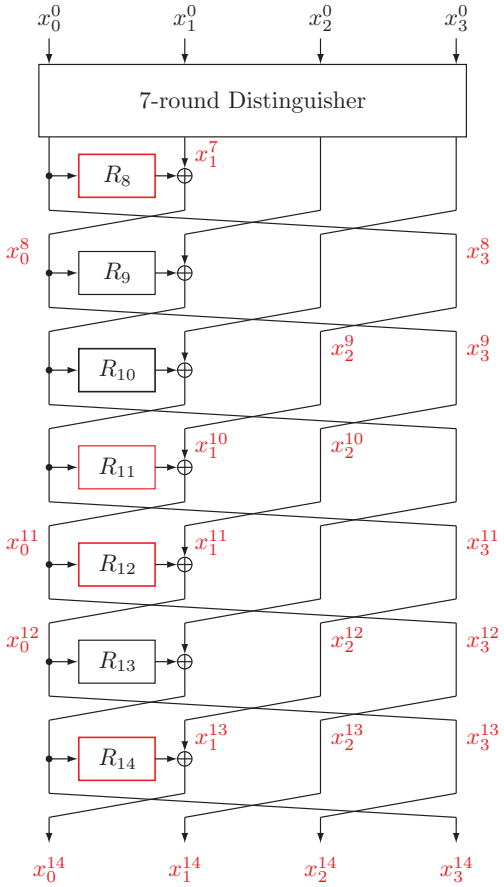

Fig. 4. $(d^2 - d + 2)$-round key recovery attack for $d = 4$

rounds, the time complexity is $O(2^{(\frac{d^2}{2} - \frac{3d}{2} + 2) \cdot \frac{k}{2} + \frac{(r - d^2 + d - 2)k}{2}})$, since the subkey length that we need to recover becomes $(\frac{d^2}{2} - \frac{3d}{2} + 2)k + (r - d^2 + d - 2)k$ bits in total.

4 $(3d - 3)$-Round Distinguishing Attack

In this section, we present our distinguishing attacks against $(3d - 3)$-round Type-1 generalized Feistel ciphers. We improve the number of rounds that we can distinguish from $(2d - 1)$ rounds to $(3d - 3)$ rounds by shifting the position of α_b in the plaintext.

As before, we first fix two arbitrary distinct constants $\alpha_0, \alpha_1 \in \{0,1\}^n$ and fix arbitrary constants $x_0^0, x_1^0, \ldots, x_{d-3}^0 \in \{0,1\}^n$. Given the oracle $\mathcal{O}$, we define

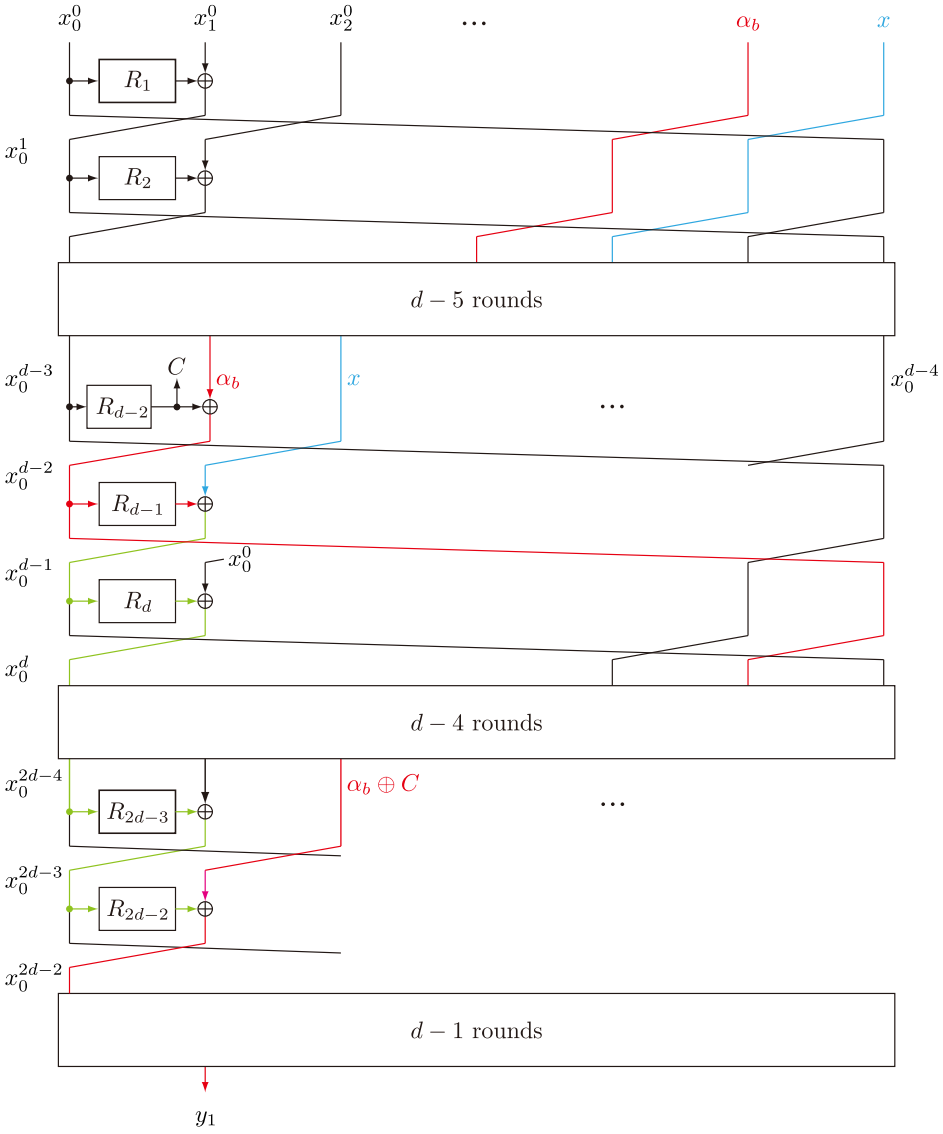

Fig. 5. $(3d-3)$-round distinguishing attack

a function $f^{\mathcal{O}}$ as

$$f^{\mathcal{O}} : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$$
$$(b, x) \mapsto \alpha_b \oplus y_1,$$
$$\text{where } (y_0, y_1, \ldots, y_{d-1}) = \mathcal{O}(x_0^0, x_1^0, \ldots, x_{d-3}^0, \alpha_b, x).$$

Observe that the difference from (2) is the position of α_b.

If $\mathcal{O}$ is Φ_{3d-3}, let $(x_0^i, x_1^i, \ldots, x_{d-1}^i)$ be the intermediate state value after the first i rounds. Now $f^{\mathcal{O}}$ is described as

$$\begin{aligned} f^{\mathcal{O}}(b,x) &= \alpha_b \oplus y_1 \\ &= \alpha_b \oplus x_1^{3d-3} \\ &= \alpha_b \oplus x_0^{2d-2}, \end{aligned} \tag{4}$$

since $x_0^i = x_{d-1}^{i+1} = x_{d-2}^{i+2} = \cdots = x_1^{i+d-1}$ (See Fig. 5).

Our main observation is the following lemma.

Lemma 1. *If $\mathcal{O}$ is Φ_{3d-3}, then for any $b \in \{0,1\}$ and $x \in \{0,1\}^n$, the function $f^{\mathcal{O}}$ satisfies*

$$f^{\mathcal{O}}(b,x) = f^{\mathcal{O}}(b \oplus 1, x \oplus R_{d-1}(C \oplus \alpha_0) \oplus R_{d-1}(C \oplus \alpha_1)),$$

where $C = R_{d-2}(R_{d-3}(\cdots R_1(x_0^0) \oplus x_1^0 \cdots) \oplus x_{d-3}^0)$. That is, $f^{\mathcal{O}}$ has the period $s = (1, R_{d-1}(C \oplus \alpha_0) \oplus R_{d-1}(C \oplus \alpha_1))$.

Proof. We first consider the intermediate state value after the first $(d-2)$ rounds in which α_b reaches the leftmost position (See the red lines in Fig. 5). The value is described as

$$\begin{aligned} (x_0^{d-2}, x_1^{d-2}, \ldots, x_{d-1}^{d-2}) &= \Phi_{d-2}(x_0^0, x_1^0, \ldots, x_{d-3}^0, \alpha_b, x) \\ &= (R_{d-2}(x_0^{d-3}) \oplus \alpha_b, x, x_0^0, x_0^1, \ldots, x_0^{d-3}). \end{aligned}$$

For $1 \le i \le d-3$, x_0^i is described as

$$x_0^i = R_i(R_{i-1}(\cdots R_1(x_0^0) \oplus x_1^0 \cdots) \oplus x_{i-1}^0) \oplus x_i^0,$$

and x_0^i is a constant that is independent of the input (b,x), since $x_0^0, x_1^0, \ldots, x_{d-3}^0$ are constants. Let $C = R_{d-2}(x_0^{d-3})$, which is independent of (b,x) and hence can be treated as a constant. The output after one more round, which is the output after the first $(d-1)$ rounds, is described as

$$(x_0^{d-1}, x_1^{d-1}, \ldots, x_{d-1}^{d-1}) = (R_{d-1}(C \oplus \alpha_b) \oplus x, x_0^0, x_0^1, \ldots, x_0^{d-3}, C \oplus \alpha_b).$$

Now we consider the value of x_0^{2d-2}. This is the intermediate state value after the first $(2d-2)$ rounds in which $\alpha_b \oplus C$ reaches the leftmost position again, and is described as

$$x_0^{2d-2} = R'(R_{d-1}(C \oplus \alpha_b) \oplus x) \oplus \alpha_b \oplus C, \tag{5}$$

where $R'(\cdot) = R_{2d-2}(R_{2d-3}(\cdots R_{d+1}(R_d(\cdot) \oplus x_0^0) \oplus x_0^1 \cdots) \oplus x_0^{d-3})$ (See the green lines in Fig. 5). $R'(\cdot)$ is a function that is independent of the input (b,x), since $x_0^0, x_0^1, \ldots, x_0^{d-3}$ are constants. From (4) and (5), the function $f^{\mathcal{O}}$ is described as

$$f^{\mathcal{O}}(b,x) = \alpha_b \oplus R'(R_{d-1}(C \oplus \alpha_b) \oplus x) \oplus \alpha_b \oplus C$$

$$= R'(R_{d-1}(C \oplus \alpha_b) \oplus x) \oplus C.$$

The function $f^{\mathcal{O}}$ has the claimed period since it satisfies

$$\begin{aligned}
&f^{\mathcal{O}}(b \oplus 1, x \oplus R_{d-1}(C \oplus \alpha_0) \oplus R_{d-1}(C \oplus \alpha_1)) \\
&= R'(R_{d-1}(C \oplus \alpha_{b\oplus 1}) \oplus R_{d-1}(C \oplus \alpha_0) \oplus R_{d-1}(C \oplus \alpha_1) \oplus x) \oplus C \\
&= R'(R_{d-1}(C \oplus \alpha_b) \oplus x) \oplus C \\
&= f^{\mathcal{O}}(b, x),
\end{aligned}$$

and hence the lemma follows. □

Therefore, we can distinguish the $(3d-3)$-round Type-1 generalized Feistel cipher by using the function $f^{\mathcal{O}}$. The success probability of the distinguishing attack with measuring $(4n+4)$ times is at least $1-(2/e)^{n+1} - \Pr[\Pi \in \mathsf{irr}_f^{1/2}]$, where we use $\delta = 1/2$ and $\eta = 4n+4$. $\Pr[\Pi \in \mathsf{irr}_f^{1/2}]$ is a small value, since with a high probability, the function $f^{\mathcal{O}}$ does not have any period when $\mathcal{O}$ is Π.

5 $(d^2 - d + 1)$-Round Distinguishing Attack

If we can use the decryption oracle in the quantum setting, we can construct a distinguishing attack against the (d^2-d+1)-round Type-1 generalized Feistel cipher. We write the i-th round function in decryption as R_i. Note that this is different from the notation in Sect. 4.

We fix two distinct constants α_0, α_1 and $(d-1)$ constants $x_1^0, x_2^0, \ldots, x_{d-2}^0$, which are all n bits. Given the decryption oracle $\mathcal{O}^{-1}$, we define $f^{\mathcal{O}^{-1}}$ as

$$\begin{aligned}
f^{\mathcal{O}^{-1}} : \{0,1\} \times \{0,1\}^n &\to \{0,1\}^n \\
(b, x) &\mapsto \alpha_b \oplus y_0, \\
\text{where } (y_0, y_1, \ldots, y_{d-1}) &= \mathcal{O}^{-1}(x, x_1^0, x_2^0, \ldots, x_{d-2}^0, \alpha_b).
\end{aligned}$$

Consider the case $\mathcal{O}^{-1} = \Phi_{d^2-d+1}^{-1}$, and let the intermediate state value after the first i rounds be $(x_0^i, x_1^i, \ldots, x_{d-1}^i)$. $\mathcal{O}^{-1}$ is described as

$$\begin{aligned}
f^{\mathcal{O}^{-1}}(b, x) &= \alpha_b \oplus y_0 \\
&= \alpha_b \oplus x_0^{d^2-d+1} \\
&= \alpha_b \oplus x_1^{d^2-2d+2}, \qquad (6)
\end{aligned}$$

since $x_1^i = x_2^{i+1} = x_3^{i+2} = \cdots = x_0^{i+d-1}$ (See Fig. 6).

The following lemma holds.

Lemma 2. *If $\mathcal{O}^{-1}$ is $\Phi_{d^2-d+1}^{-1}$, then for any $b \in \{0,1\}$ and $x \in \{0,1\}^n$, the function $f^{\mathcal{O}^{-1}}$ satisfies*

$$f^{\mathcal{O}^{-1}}(b, x) = f^{\mathcal{O}^{-1}}(b \oplus 1, x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1)).$$

That is, $f^{\mathcal{O}^{-1}}$ has the period $s = (1, R_1(\alpha_0) \oplus R_1(\alpha_1))$.

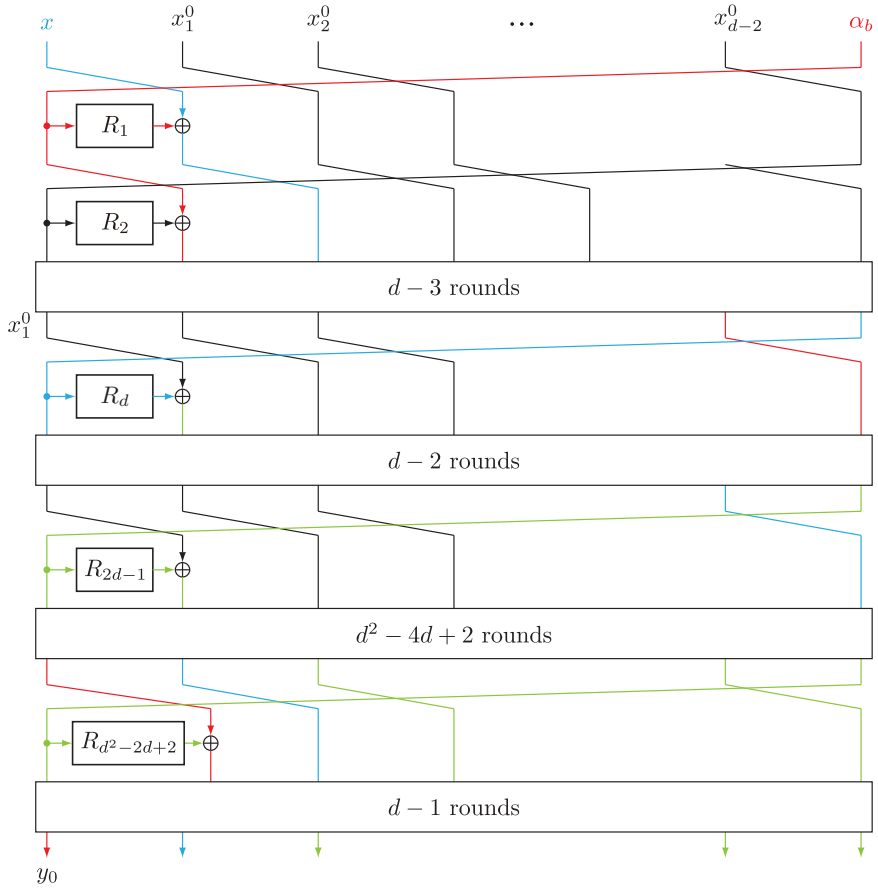

Fig. 6. (d^2-d+1)-round distinguishing attack

Proof. In the first round, $R_1(\alpha_b)$ is xored to x. In the d-th round, the value $R_1(\alpha_b) \oplus x$ is used as the input of R_d, and the output of R_d is xored to x_1^0. This implies that x_1^d is

$$x_1^d = R_d(R_1(\alpha_b) \oplus x) \oplus x_1^0. \tag{7}$$

See the green lines in Fig. 6. The function $R(\cdot) = R_d(\cdot) \oplus x_1^0$ is independent of the input (b, x), since x_1^0 is a constant. Therefore, (7) can be described as

$$x_1^d = R(R_1(\alpha_b) \oplus x)$$

with some function $R \in \mathrm{Func}(n)$. After additional $(d-1)$ rounds, this value is used as the input of R_{2d-1}, and the output of R_{2d-1} is xored to the sub-block which was x_2^0 at the input. The sub-block which was x_2^0 at the input is a constant because it is not xored by the value that includes b nor x. Therefore, for some

function $R' \in \mathrm{Func}(n)$, the value of x_1^{2d-1} is described as

$$x_1^{2d-1} = R'(R_1(\alpha_b) \oplus x).$$

After that, for each $(d-1)$ rounds, this value is used as the input to the round function and the output is xored to the sub-block which was x_i^0 at the input, for $i = 3, 4, \ldots, d-2$. Since the sub-block is a constant that is independent of the input (b, x), the value of $x_1^{2d-1+(d-1)\times(d-4)} = x_1^{d^2-3d+3}$ is described as

$$x_1^{d^2-3d+3} = R''(R_1(\alpha_b) \oplus x)$$

for some function $R'' \in \mathrm{Func}(n)$.

In the (d^2-2d+2)-th round, $R_{d^2-2d+2}(R''(R_1(\alpha_b) \oplus x))$ is xored to the sub-block which was α_b at the input. Since only the value that does not include b nor x is xored to the sub-block which was α_b, with some function $R''' \in \mathrm{Func}(n)$, the value of $x_1^{d^2-2d+2}$ is described as

$$x_1^{d^2-2d+2} = R'''(R_1(\alpha_b) \oplus x) \oplus \alpha_b. \tag{8}$$

From (6) and (8), the function $f^{\mathcal{O}^{-1}}$ can be written as

$$\begin{aligned} f^{\mathcal{O}^{-1}}(b, x) &= \alpha_b \oplus R'''(R_1(\alpha_b) \oplus x) \oplus \alpha_b \\ &= R'''(R_1(\alpha_b) \oplus x). \end{aligned}$$

The function $f^{\mathcal{O}}$ satisfies

$$\begin{aligned} f^{\mathcal{O}^{-1}}(b \oplus 1, x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1)) &= R'''(R_1(\alpha_{b\oplus 1}) \oplus x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1)) \\ &= R'''(R_1(\alpha_b) \oplus x) \\ &= f^{\mathcal{O}^{-1}}(b, x), \end{aligned}$$

and hence we have the lemma. □

The success probability of the distinguishing attack using the function $f^{\mathcal{O}^{-1}}$ with measuring $(4n+4)$ times is at least $1 - (2/e)^{n+1} - \Pr[\Pi \in \mathsf{irr}_f^{1/2}]$, where we use $\delta = 1/2$ and $\eta = 4n+4$. We see that $\Pr[\Pi \in \mathsf{irr}_f^{1/2}]$ is a small value, and hence the attack succeeds with a high probability.

6 Key Recovery Attacks

Similarly to the previous key recovery attacks by Dong et al. that combine Grover search and the distinguisher, we can construct key recovery attacks against Type-1 generalized Feistel cipher based on our distinguishers.

With the $(3d-3)$-round distinguisher, we can recover the key of the d^2-round Type-1 generalized Feistel cipher in time $O(2^{(\frac{d^2}{2}-\frac{3d}{2}+2)\cdot\frac{k}{2}})$ by replacing the $(2d-1)$-round distinguisher in Dong et al.'s attack with our $(3d-3)$-round

distinguisher. In general, the key recovery attack against the r-round version, where $r \geq d^2$, runs in time $O(2^{(\frac{d^2}{2}-\frac{3d}{2}+2)\cdot\frac{k}{2}+\frac{(r-d^2)k}{2}})$.

With the (d^2-d+1)-round distinguisher, by using the decryption oracle, we can recover the key of the r-round Type-1 generalized Feistel cipher for $r \geq d^2-d+1$ in time $O(2^{\frac{(r-(d^2-d+1))k}{2}})$, because the subkey length that we need to recover is $(r-d^2+d-1)k$ bits.

If $d=3$, the time complexity of these two key recovery attacks is the same because $(\frac{d^2}{2}-\frac{3d}{2}+2)\cdot\frac{k}{2}+\frac{(r-d^2)k}{2}-\frac{(r-(d^2-d+1))k}{2}=\frac{k(d-2)(d-3)}{4}$. If $d>3$, the key recovery attack with the (d^2-d+1)-round distinguisher is better than the one with the $(3d-3)$-round distinguisher.

7 Concluding Remarks

In this paper, we presented the $(3d-3)$-round distinguisher against Type-1 generalized Feistel cipher with quantum chosen-plaintext attacks that can distinguish more rounds than the previous distinguisher. We also gave the (d^2-d+1)-round distinguisher by using the quantum decryption oracle. Based on these distinguishers, we presented quantum key recovery attacks. Our quantum key recovery attacks against the r-round Type-1 generalized Feistel cipher recover keys in time $O(2^{(\frac{d^2}{2}-\frac{3d}{2}+2)\cdot\frac{k}{2}+\frac{(r-d^2)k}{2}})$ with the $(3d-3)$-round distinguisher and $O(2^{\frac{(r-(d^2-d+1))k}{2}})$ with the (d^2-d+1)-round distinguisher.

As an open question, the tight bound of the number of rounds that we can distinguish is not known. There is a possibility that we can distinguish more than $(3d-3)$ rounds, and we may distinguish more than (d^2-d+1) rounds in the quantum chosen-ciphertext setting.

References

[AG99] Carlisle Adams and Jeff Gilchrist. The CAST-256 Encryption Algorithm. RFC 2612, June 1999.

[BCD+99] Carolynn Burwick, Don Coppersmith, Edward D'Avignon, Rosario Gennaro, Shai Halevi, Charanjit Jutla, Stephen M. Matyas Jr., Luke O'Connor, Mohammad Peyravian, David Safford, and Nevenko Zunic. MARS - a candidate cipher for AES. NIST AES proposal, September 1999.

[BHMT02] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. *Contemporary Mathematics*, 305:53–74, 2002.

[Bon17] Xavier Bonnetain. Quantum Key-Recovery on Full AEZ. In Carlisle Adams and Jan Camenisch, editors, *SAC 2017*, volume 10719 of *LNCS*, pages 394–406. Springer, 2017.

[DLW19] Xiaoyang Dong, Zheng Li, and Xiaoyun Wang. Quantum Cryptanalysis on Some Generalized Feistel Schemes. *SCIENCE CHINA Information Sciences*, 62(2):022501, 2019.

[DW18] Xiaoyang Dong and Xiaoyun Wang. Quantum key-recovery attack on Feistel structures. *SCIENCE CHINA Information Sciences*, 61(10):102501:1–102501:7, 2018.

[Gro96] Lov K. Grover. A Fast Quantum Mechanical Algorithm for Database Search. In Gary L. Miller, editor, *STOC 1996*, pages 212–219. ACM, 1996.

[HR10] Viet Tung Hoang and Phillip Rogaway. On Generalized Feistel Networks. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 613–630. Springer, 2010.

[HS18] Akinori Hosoyamada and Yu Sasaki. Quantum Demiric-Selçuk Meet-in-the-Middle Attacks: Applications to 6-Round Generic Feistel Constructions. In Dario Catalano and Roberto De Prisco, editors, *SCN 2018*, volume 11035 of *LNCS*, pages 386–403. Springer, 2018.

[IHM+19] Gembu Ito, Akinori Hosoyamada, Ryutaroh Matsumoto, Yu Sasaki, and Tetsu Iwata. Quantum Chosen-Ciphertext Attacks Against Feistel Ciphers. In Mitsuru Matsui, editor, *CT-RSA 2019*, volume 11405 of *LNCS*, pages 391–411. Springer, 2019.

[KLLN16] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking Symmetric Cryptosystems Using Quantum Period Finding. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part II*, volume 9815 of *LNCS*, pages 207–237. Springer, 2016.

[KM10] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In *ISIT 2010*, pages 2682–2685. IEEE, 2010.

[KM12] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type Even-Mansour cipher. In *ISITA 2012*, pages 312–316. IEEE, 2012.

[KR96] Joe Kilian and Phillip Rogaway. How to Protect DES Against Exhaustive Key Search. In Neal Koblitz, editor, *CRYPTO 1996*, volume 1109 of *LNCS*, pages 252–267. Springer, 1996.

[KR01] Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search (an analysis of DESX). *J. Cryptology*, 14(1):17–35, 2001.

[LM17] Gregor Leander and Alexander May. Grover meets Simon - Quantumly attacking the FX-construction. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 161–178. Springer, 2017.

[LR88] Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[MV00] Shiho Moriai and Serge Vaudenay. On the Pseudorandomness of Top-Level Schemes of Block Ciphers. In Tatsuaki Okamoto, editor, *ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 289–302. Springer, 2000.

[RRSY98] Ronald L. Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin. The RC6$^{\text{TM}}$ Block Cipher. NIST AES proposal, August 1998.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

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

[SS17] Thomas Santoli and Christian Schaffner. Using Simon's algorithm to attack symmetric-key cryptographic primitives. *Quantum Information & Computation*, 17(1&2):65–78, 2017.

[SSA+07] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-Bit Blockcipher CLEFIA (Extended Abstract). In Alex Biryukov, editor, *FSE 2007*, volume 4593 of *LNCS*, pages 181–195. Springer, 2007.

[YWO+07] Hirotaka Yoshida, Dai Watanabe, Katsuyuki Okeya, Jun Kitahara, Hongjun Wu, Özgül Küçük, and Bart Preneel. MAME: A Compression Function with Reduced Hardware Requirements. In Pascal Paillier and Ingrid Verbauwhede, editors, *CHES 2007*, pages 148–165, 2007.

[ZMI89] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In Gilles Brassard, editor, *CRYPTO '89*, volume 435 of *LNCS*, pages 461–480. Springer, 1989.