Quantum Attacks Against Type-1 Generalized Feistel Ciphers and Applications to CAST-256

Boyu Ni[1,2], Gembu Ito[3], Xiaoyang Dong[4(✉)], and Tetsu Iwata[3(✉)]

[1] Key Laboratory of Cryptologic Technology and Information Security, Shandong University, Ministry of Education, Qingdao, People's Republic of China
[2] School of Cyber Science and Technology, Shandong University, Qingdao, People's Republic of China
[3] Nagoya University, Nagoya 464-8603, Japan
g_itou@echo.nuee.nagoya-u.ac.jp, tetsu.iwata@nagoya-u.jp
[4] Institute for Advanced Study, Tsinghua University, Beijing 100084, People's Republic of China
xiaoyangdong@tsinghua.edu.cn

Abstract. Generalized Feistel Schemes (GFSs) are important components of symmetric ciphers, which have been extensively studied in the classical setting. However, detailed security evaluations of GFS in the quantum setting still remain to be explored.

In this paper, we give improved polynomial-time quantum distinguishers on Type-1 GFS in quantum chosen-plaintext attack (qCPA) setting and quantum chosen-ciphertext attack (qCCA) setting. In qCPA setting, we give a new quantum polynomial-time distinguisher on $(3d-3)$-round Type-1 GFS with branches $d \geq 3$, which gains $(d-2)$ more rounds than the previous distinguishers. This leads us to obtain a better key-recovery attack with reduced time complexities by a factor of $2^{\frac{(d-2)n}{2}}$, where n is the bit length of the branch. We also show a quantum distinguishing attack against (d^2-d+1)-round version in qCCA setting, and this gives a key-recovery attack with much lower time complexity.

In addition, based on a 14-round quantum distinguisher, we give quantum key-recovery attacks on round-reduced CAST-256 block cipher. For the 256-bit key version, we could attack up to 20-round CAST-256 in time 2^{111}, which is faster than the quantum brute-force attack by a factor of 2^{17}. For the 128-bit key version, we could attack 17 rounds in time $2^{55.5}$, while the best previous classical or quantum attacks are no more than 16 rounds.

Keywords: Generalized Feistel scheme · Quantum attack · Simon's algorithm · CAST-256

1 Introduction

Feistel block ciphers are featured by the efficient Feistel network, whose encryption and decryption processes are based on similar operations. This design

F. Hao et al. (Eds.): INDOCRYPT 2019, LNCS 11898, pp. 433–455, 2019.
https://doi.org/10.1007/978-3-030-35423-7_22

has been extensively studied [8,15,20,27] and adopted in many standard block ciphers, including DES, Triple-DES, Camellia [3], and GOST [12]. Feistel network was also generalized to form Generalized Feistel Networks (GFNs) or Generalized Feistel Schemes (GFSs). GFSs adopt more than two branches and different operations between the branches. At CRYPTO 1989, Zheng et al. [46] summarized several types of GFSs, called Type-1, Type-2, and Type-3 GFSs. In addition, some other GFSs were invented by Anderson and Biham [2], Lucks [32] and Schneier and Kelsey [38]. Many important primitives employ GFSs, such as block ciphers CAST-256 [1] (Type-1), CLEFIA [39] (Type-2), Simpira [14] (Type-2), as well as hash functions MD5 and SHA-1 (Type-1). GFSs inherit the advantages of Feistel network. Besides, it allows a small round function to construct a cipher with a larger block size, which is beneficial to lightweight implementations.

Classically, Luby and Rackoff [31] proved that the 3-round Feistel scheme is a secure pseudo-random permutation. At CRYPTO 1989, Zheng et al. [46] showed that the $(2d-1)$-round Type-1 GFS is secure against chosen-plaintext attacks. Moriai and Vaudenay pointed out that (d^2-d)-round Type-1 GFS is not secure against chosen-ciphertext attacks [33]. See also the analysis by Hoang and Rogaway [17]. Generic attacks on these constructions are also widely studied, such as birthday attack [23], meet-in-the-middle attack [16], differential attacks [34,41], and Patarin et al.'s attacks [35,36,42].

It was a common belief that quantum attacks on symmetric primitives are of minor concern, as they mainly consist of employing Grover's algorithm [13] to generically speed up search (sub-)problems. However, Kuwakado and Morii [28] found the first polynomial-time quantum distinguisher on 3-round Feistel block ciphers by using Simon's algorithm [40]. This result proves that there is a case that quantum attacks can exponentially improve classical attacks. Later, various quantum attacks against symmetric primitives were invented, such as key-recovery attacks against Even-Mansour constructions [29], forgery or key-recovery attacks against block cipher based MACs [5,24], key-recovery attacks against the FX construction [30], and so on.

At FOCS 2012, Zhandry et al. [45] classified the quantum cryptanalysis into two models, i.e., the standard security (Q1 model) and quantum security (Q2 model). In Q1 model, adversaries could only collect data classically and process them with local quantum computers. In contrast to this, in Q2 model, the adversaries could query the oracle with quantum superpositions of inputs, and obtain the corresponding superposition of outputs. Adversaries from Q2 model are more powerful, while Q2 model is not realistic for the foreseeable future. However, Q2 model is still theoretically interesting. Moreover, as stated by Ito et al. [22], *"the threat of this attack model becomes significant if an adversary has access to its white-box implementation. Because arbitrary classical circuit can be converted into quantum one, the adversary can construct a quantum circuit from the classical source code given by the white-box implementation"*. In this paper, we assume that the adversaries are in the Q2 model.

There have already been papers investigating Feistel schemes or GFSs against Q2 adversaries. Besides Kuwakado and Morii [28]'s work, Ito et al. [22] extended

the quantum distinguisher to 4-round Feistel scheme under quantum chosen-ciphertext attack setting. Based on the Grover-meets-Simon algorithm by Leander and May [30], Hosoyamada et al. [19] and Dong et al. [11] introduced some quantum key-recovery attacks on Feistel schemes. Dong et al. [10] gave some quantum distinguishers and key-recovery attacks on some GFSs. Dong et al. [9] and Bonnetain et al. [6] studied 2K-/4K-Feistel schemes against quantum slide attacks. Notably, Hosoyamada and Iwata [18] proved a quantum security bound of the 4-Round Luby-Rackoff construction recently.

Our Contributions. We continue the work of Dong, Li, and Wang [10] to evaluate the security of Type-1 GFSs against quantum attacks. We focus on Type-1 GFSs, as the structure is employed in the above mentioned practical designs[1]. We give some improved attacks on Type-1 GFSs in Q2 model with both quantum chosen-plaintext attack (qCPA) setting and quantum chosen-ciphertext attack (qCCA) setting. Then, some applications to CAST-256 block ciphers are given. We have three contributions:

- First, in qCPA setting, we give new quantum polynomial-time distinguishers on $(3d-3)$-round Type-1 GFS with branches $d \geq 3$, which gain $(d-2)$ more rounds than the previous distinguishers. The improvement is obtained by shifting 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 observation is simple, but effective to improve the number of rounds that we can attack. Based on Leander and May's algorithm [30], we could get better key-recovery attacks, whose time complexities gain a factor of $2^{\frac{(d-2)n}{2}}$, where n is the bit length of the branch.
- Second, assuming that we are in the qCCA 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 GFS in the decryption direction is slow, which is pointed out in [33]. The distinguishers in both qCPA and qCCA settings and the key-recovery attacks are summarized in Tables 1 and 2.
- Third, we also evaluate CAST-256 block cipher against quantum attacks. We find 14-round polynomial-time quantum distinguishers in qCPA setting. Note that the best previous one is 7 rounds [10]. Based on this, we could derive quantum key-recovery attack on 20-round CAST-256. Compared to this, the best previous quantum key-recovery attack is on 16 rounds. The results are summarized in Table 3. We also compare our quantum attacks with classical attacks in Table 4. When the key size of CAST-256 is 128, our result also reaches 17 rounds, which gains one more round than before.

[1] Dong, Li, and Wang also analyzed Type-2 GFSs [10], and we do not know if quantum attacks on Type-2 GFSs can be improved.

Table 1. Rounds of quantum distinguishers on Type-1 GFS

Source	Setting	Distinguisher	$d=3$	$d=4$	$d=5$	$d=6$	$d=7$	...
[10]	qCPA	$2d-1$	5	7	9	11	13	...
Sect. 4	qCPA	$3d-3$	6	9	12	15	18	...
Sect. 5	qCCA	d^2-d+1	7	13	21	31	43	...

Table 2. Key-recovery attacks on Type-1 GFS ($d \geq 3$) in quantum settings

Setting	Distinguisher	Key-recovery rounds	Complexity (log)
qCPA	$2d-1$ [10]	$r \geq d^2-d+2$	$(\frac{1}{2}d^2-\frac{3}{2}d+2)\cdot\frac{k}{2}+\frac{(r-d^2+d-2)k}{2}$
qCPA	$3d-3$ [Ours]	$r \geq d^2$	$(\frac{1}{2}d^2-\frac{3}{2}d+2)\cdot\frac{k}{2}+\frac{(r-d^2)k}{2}$
qCCA	d^2-d+1 [Ours]	$r \geq d^2-d+1$	$\frac{(r-(d^2-d+1))k}{2}$

Table 3. Quantum attacks on CAST-256†

Source	Setting	Distinguisher	Attacked rounds					
			$r=15$	$r=16$	$r=17$	$r=18$	$r=19$	$r=20$
[10]	qCPA	7	$2^{92.5}$	2^{111}	–	–	–	–
Sect. 7	qCPA	14	$2^{18.5}$	2^{37}	$2^{55.5}$	2^{74}	$2^{92.5}$	2^{111}

†: Note that for CAST-256 with 256-bit key, the trivial bound is 2^{128} by Grover's algorithm.

Table 4. Comparison between classical and quantum attacks on CAST-256

Source	Key	Attack	Rounds	Data	Time
[43]	128	boomerang	16	$2^{49.3}$	–
[10]	128	qCPA	12	–	$2^{55.5}$
Sect. 7	128	qCPA	17	–	$2^{55.5}$
[44]	192	linear	24	$2^{124.1}$	$2^{156.52}$
Sect. 7	192	qCPA	18	–	2^{74}
[4]	256	multidim.ZC	28	$2^{98.8}$	$2^{246.9}$
[10]	256	qCPA	16	–	2^{111}
Sect. 7	256	qCPA	20	–	2^{111}

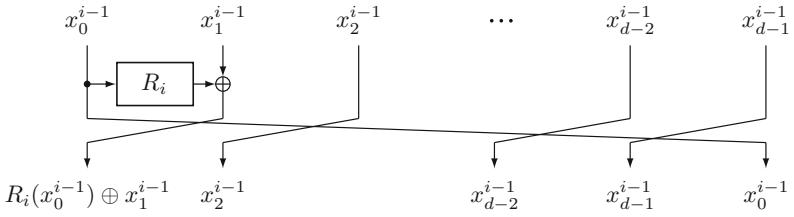

Fig. 1. The i-th round of Type-1 GFS

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 functions 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 Schemes

In this section, we describe Type-1 generalized Feistel schemes (GFSs) [46]. In Type-1 GFS, 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 GFS, 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

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

The decryption is naturally defined by reversing the direction of the shift of the branches. Figure 1 shows the i-th round of Type-1 GFS.

2.3 Simon's Algorithm

Here we review Simon's algorithm [40] that is the basis of our distinguishers. Simon's algorithm solves the following problem efficiently.

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.

In the classical setting, $O(2^{n/2})$ queries are needed to find s, while Simon's algorithm finds s with $O(n)$ quantum queries.

In what follows, we recall how Simon's algorithm works. 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 Eq. (1) can be rearranged as

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

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 the first n qubits of $\mathcal{S}_f|0^n\rangle|0^n\rangle$ 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 Quantum 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. [24] and Santoli and Schaffner [37], and the formalization by Ito et al. [22]. 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 [22] 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 follows:

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 $\mathcal{O} = \Pi$, 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 $\mathcal{O} = \Pi$ 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 $\Pi = \pi$. 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 $0 \leq \delta < 1$ 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 in [22].

Theorem 1 ([22]). *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 Hosoyamada and Sasaki's Method to Truncate Outputs of Quantum Oracles

At ISIT 2010, Kuwakado and Morii [28] introduced a quantum distinguishing attack on 3-round Feistel scheme by using Simon's algorithm. As shown in Fig. 2, let α_0 and α_1 be arbitrary constants, and define f as:

$$\begin{aligned} f : \{0,1\} \times \{0,1\}^n &\to \{0,1\}^n \\ (b, x) &\mapsto \alpha_b \oplus x_1^3 , \\ \text{where} \quad (x_0^3, x_1^3) &= E(\alpha_b, x) . \end{aligned}$$

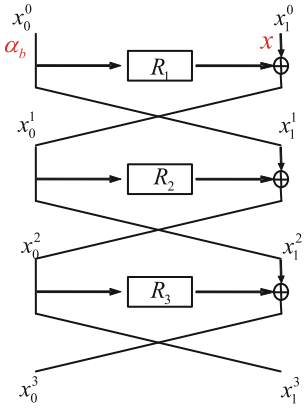

Fig. 2. 3-round Feistel cipher

E is the 3-round Feistel scheme and f can be written as $f(b,x) = R_2(R_1(\alpha_b) \oplus x))$. It is easy to see that f is a periodic function that satisfies $f(b,x) = f(b \oplus 1, x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1))$ for any (b,x). Then by using Simon's algorithm, one obtains the period $s = 1 \| R_1(\alpha_0) \oplus R_1(\alpha_1)$ in polynomial time.

In the above distinguisher, one has to truncate the $2n$-bit output of E to obtain the right half n bits, namely x_1^3. However, Kaplan et al. [24] and Hosoyamada et al. [19] pointed out that in quantum setting, it is non-trivial to truncate the entangled $2n$ qubits to n qubits, since the usual truncation destroys entanglements.

At SCN 2018, Hosoyamada and Sasaki [19] introduced a method to simulate truncation of outputs of quantum oracles without destroying quantum entanglements. Here, we review their method. Let $\mathcal{O} : |x\rangle|y\rangle|z\rangle|w\rangle \mapsto |x\rangle|y\rangle|z \oplus \mathcal{O}_L(x,y)\rangle|w \oplus \mathcal{O}_R(x,y)\rangle$ be the encryption oracle E_K, where $\mathcal{O}_L$, $\mathcal{O}_R$ denote the left and right n bits of the complete encryption, respectively. The goal is to simulate the oracle $\mathcal{O}_R : |x\rangle|y\rangle|w\rangle \mapsto |x\rangle|y\rangle|w \oplus \mathcal{O}_R(x,y)\rangle$. Hosoyamada and Sasaki first try to simulate a tweaked $\mathcal{O}_R$, i.e., $\mathcal{O}'_R : |x\rangle|y\rangle|w\rangle|0^n\rangle \mapsto |x\rangle|y\rangle|w \oplus \mathcal{O}_R(x,y)\rangle|0^n\rangle$ with ancilla qubits. Let $|+\rangle := H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_z |z\rangle$, where $H^{\otimes n}$ is an n-qubit Hadamard gate. Thus,

$$\begin{aligned} \mathcal{O}|x\rangle|y\rangle|+\rangle|w\rangle &= \mathcal{O}(|x\rangle|y\rangle[\frac{1}{\sqrt{2^n}} \sum_z |z\rangle]|w\rangle) \\ &= |x\rangle|y\rangle[\frac{1}{\sqrt{2^n}} \sum_z |z \oplus \mathcal{O}_L(x,y)\rangle]|w \oplus \mathcal{O}_R(x,y)\rangle\,. \end{aligned} \tag{2}$$

Let $z' = z \oplus \mathcal{O}_L(x,y)$. Then Eq. (2) becomes

$$\begin{aligned} |x\rangle|y\rangle[\frac{1}{\sqrt{2^n}} \sum_z |z'\rangle]|w \oplus \mathcal{O}_R(x,y)\rangle &= |x\rangle|y\rangle[\frac{1}{\sqrt{2^n}} \sum_{z'} |z'\rangle]|w \oplus \mathcal{O}_R(x,y)\rangle \\ &= |x\rangle|y\rangle|+\rangle|w \oplus \mathcal{O}_R(x,y)\rangle\,. \end{aligned}$$

So $\mathcal{O}|x\rangle|y\rangle|+\rangle|w\rangle = |x\rangle|y\rangle|+\rangle|w \oplus \mathcal{O}_R(x,y)\rangle$. Hosoyamada and Sasaki define $\mathcal{O}'_R := (I \otimes H^{\otimes n}) \circ \texttt{Swap} \circ \mathcal{O} \circ \texttt{Swap} \circ (I \otimes H^{\otimes n})$, where $\texttt{Swap}$ is an operator that swaps the last $2n$ bits: $|x\rangle|y\rangle|z\rangle|w\rangle \mapsto |x\rangle|y\rangle|w\rangle|z\rangle$. So we have

$$\begin{aligned}
\mathcal{O}'_R|x\rangle|y\rangle|w\rangle|0^n\rangle &= (I \otimes H^{\otimes n}) \circ \texttt{Swap} \circ \mathcal{O} \circ \texttt{Swap} \circ (I \otimes H^{\otimes n})|x\rangle|y\rangle|w\rangle|0^n\rangle \\
&= (I \otimes H^{\otimes n}) \circ \texttt{Swap} \circ \mathcal{O}|x\rangle|y\rangle|+\rangle|w\rangle \\
&= (I \otimes H^{\otimes n}) \circ \texttt{Swap}|x\rangle|y\rangle|+\rangle|w \oplus \mathcal{O}_R(x,y)\rangle \\
&= (I \otimes H^{\otimes n})|x\rangle|y\rangle|w \oplus \mathcal{O}_R(x,y)\rangle|+\rangle \\
&= |x\rangle|y\rangle|w \oplus \mathcal{O}_R(x,y)\rangle|0^n\rangle\,.
\end{aligned}$$

Hence, $\mathcal{O}_R$ could be simulated given the complete encryption oracle $\mathcal{O}$ using ancilla qubits. Intuitively, Hosoyamada and Sasaki first randomize the left part by using the Hadamard transformation, and then force it to become $|0^n\rangle$ by applying the Hadamard transformation again.

2.6 Combining Grover Search and Distinguishers

Leander and May combined Grover search and Simon's algorithm to show a key recovery attack against the FX construction [30]. Hosoyamada and Sasaki [19], and Dong and Wang [11] showed key recovery attacks against Feistel schemes by using this combining technique.

Grover Search. Grover search provides a quadratic speed up on unsorted-database search [13]. 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. [7] as in the following theorem.

Theorem 2 ([7]). *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,*

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

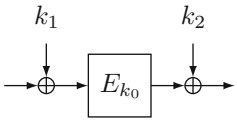

Fig. 3. The FX construction

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 the FX Construction. The FX construction by Killian and Rogaway is a way to extend the key length of a block cipher [25,26]. Let E be an n-bit block cipher that takes an m-bit key k_0 as input. The FX construction under two additional n-bit keys k_1, k_2 is described as

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

Figure 3 shows the 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 states as good if $k = k_0$ by using Simon's algorithm to $f(k, \cdot)$. The time 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 [30].

3 Previous Attacks

In this section, we review the quantum attacks against Type-1 GFSs by Dong et al. [10]. 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

$$\begin{aligned} f^{\mathcal{O}} : \{0,1\} \times \{0,1\}^n &\to \{0,1\}^n \\ (b, x) &\mapsto \alpha_b \oplus y_1 \,, \\ \text{where } (y_0, y_1, \ldots, y_{d-1}) &= \mathcal{O}(\alpha_b, x_1^0, x_2^0, \ldots, x_{d-2}^0, x) \,. \end{aligned} \tag{3}$$

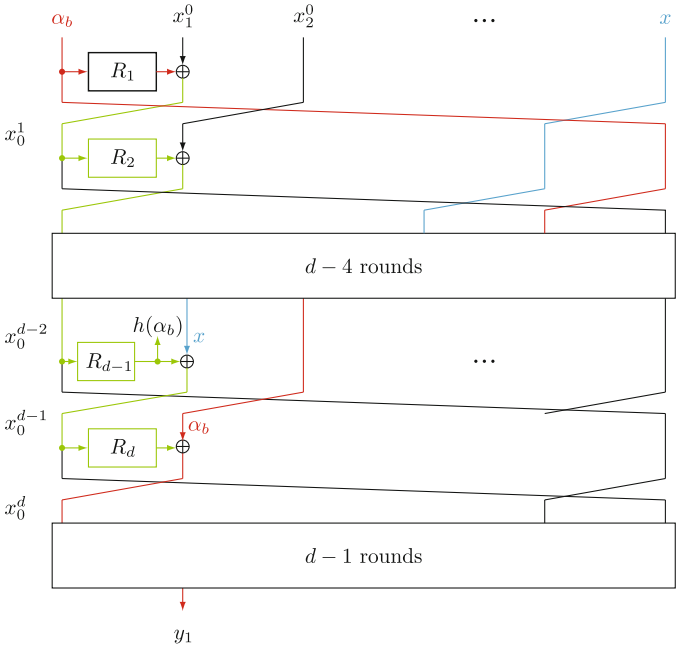

Fig. 4. $(2d-1)$-round distinguishing attack

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

$$\begin{aligned} f(b,x) &= \alpha_b \oplus x_1^{2d-1} \\ &= \alpha_b \oplus x_0^d \\ &= \alpha_b \oplus R_d(x_0^{d-1}) \oplus \alpha_b \\ &= R_d(R_{d-1}(R_{d-2}(\cdots R_2(R_1(\alpha_b) \oplus x_1^0) \oplus x_2^0 \cdots) \oplus x_{d-2}^0) \oplus x)\,, \end{aligned} \tag{4}$$

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. 4). 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 $x_1^0, x_2^0, \ldots, x_{d-2}^0$ are constants. By using $h(\cdot)$, we can describe Eq. (4) 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 $\mathcal{O}$ 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.

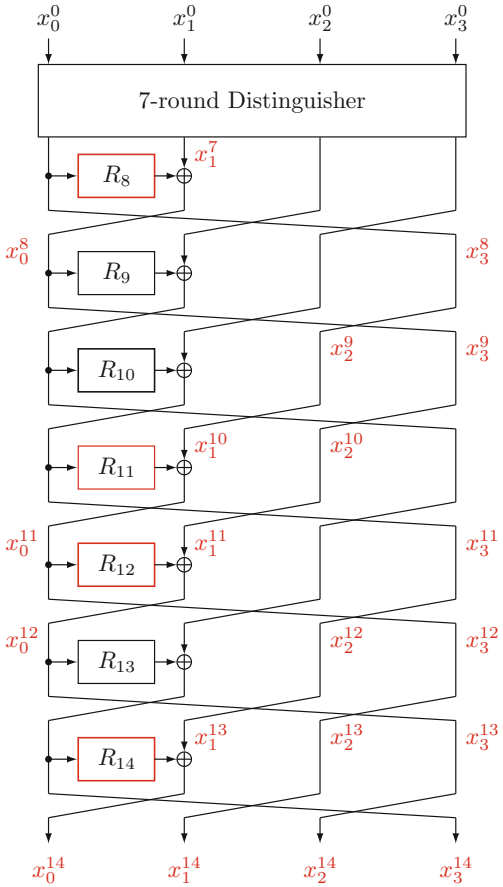

Fig. 5. $(d^2 - d + 2)$-round key recovery attack for $d = 4$

We next review the key recovery attack. We recover the key of the $(d^2 - d + 2)$-round Type-1 GFS by appending $(d^2 - 3d + 3)$ rounds after the $(2d - 1)$-round distinguisher (See Fig. 5). For each x_1^i, where $d \geq 3$, we have $x_1^i = R_{i+1}(x_d^{i+1}, k_{i+1}) \oplus x_0^{i+1}$. This implies that when we need the value of x_1^i, we have to recover k_{i+1}. From the property of Feistel cipher, we have $x_j^i = x_{j-1}^{i+1} = \cdots = x_1^{i+j-1}$ for $3 \leq j \leq d$, and $x_0^i = x_1^{i+d-1}$. For d branches, it holds that $x_1^{2d-1} = R_{2d}(x_{d-1}^{2d}, k_{2d}) \oplus x_0^{2d}$, and thus we need to recover one sub-key k_{2d}, and since $x_0^{2d} = x_1^{3d-1}$ and $x_{d-1}^{2d} = x_1^{3d-2}$ hold, we need two sub-keys k_{3d-1} and k_{3d}. By parity of this reasoning, the subkey length that we need to recover becomes $[1+2+3+\cdots+(d-2)]k+k = (\frac{d^2}{2} - \frac{3d}{2} + 2)k$ 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 $O(2^{(\frac{d^2}{2} - \frac{3d}{2} + 2) \cdot \frac{k}{2}})$.

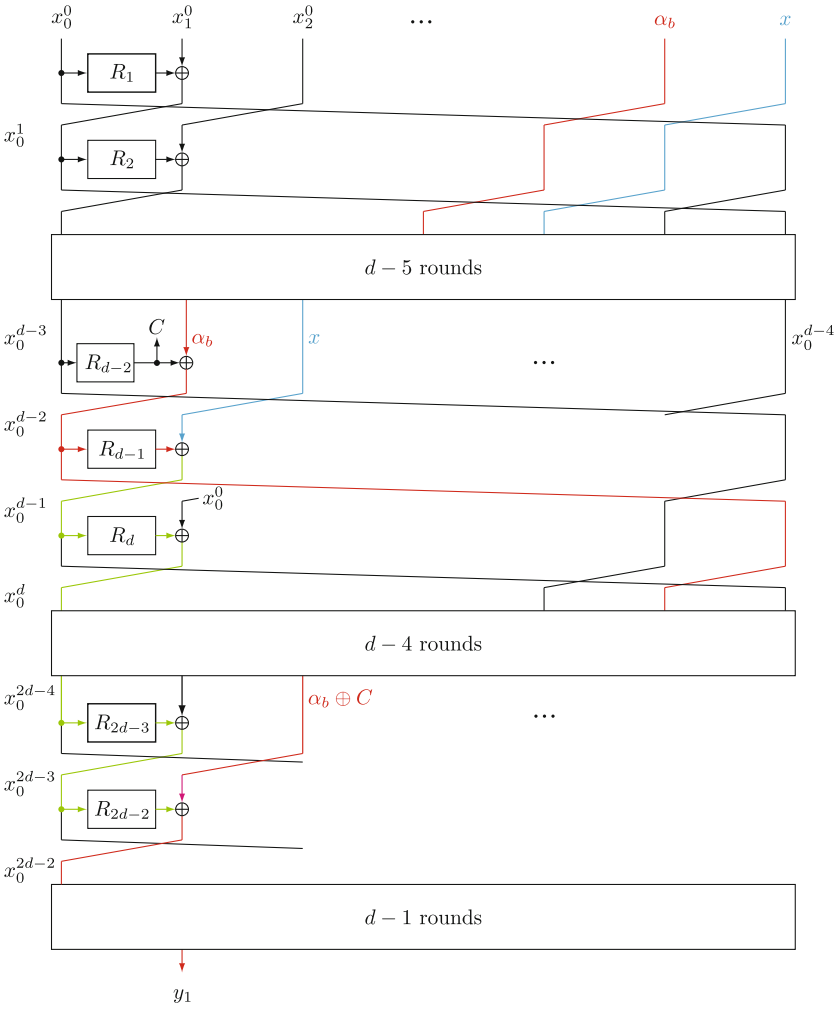

Fig. 6. $(3d-3)$-round distinguishing attack

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 subkey of r rounds for $r > d^2-d+2$, 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 qCPA Setting

In this section, we present our distinguishing attacks against $(3d-3)$-round Type-1 GFSs. 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 a function $f^{\mathcal{O}}$ as

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

Observe that the difference from Eq. (3) 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:

$$\begin{aligned} f^{\mathcal{O}}(b, x) &= \alpha_b \oplus y_1 \\ &= \alpha_b \oplus x_1^{3d-3} \\ &= \alpha_b \oplus x_0^{2d-2} \,, \end{aligned} \tag{5}$$

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

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 Fig. 6). 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

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

We see that 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

$$x_0^{2d-2} = R'(R_{d-1}(C \oplus \alpha_b) \oplus x) \oplus \alpha_b \oplus C \,, \tag{6}$$

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 Fig. 6). $R'(\cdot)$ 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 Eqs. (5) and (6), the function $f^{\mathcal{O}}$ is described as

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

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 GFS 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 $\eta = 4n+4$. Note that $\Pr[\Pi \in \mathsf{irr}_f^{1/2}]$ is a small value, since with a high probability, the function $f^{\mathcal{O}}$ does not have any period when $\mathcal{O}$ is Π, since Π is a random permutation.[2]

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

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 GFS. 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 $(d-2)$ 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

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

[2] This is intuitively obvious. However, precise computation of the probability is not known. See [21, Appendix C] (full version of [22]) for experimental computation of a related setting of Feistel cipher for small values of n.

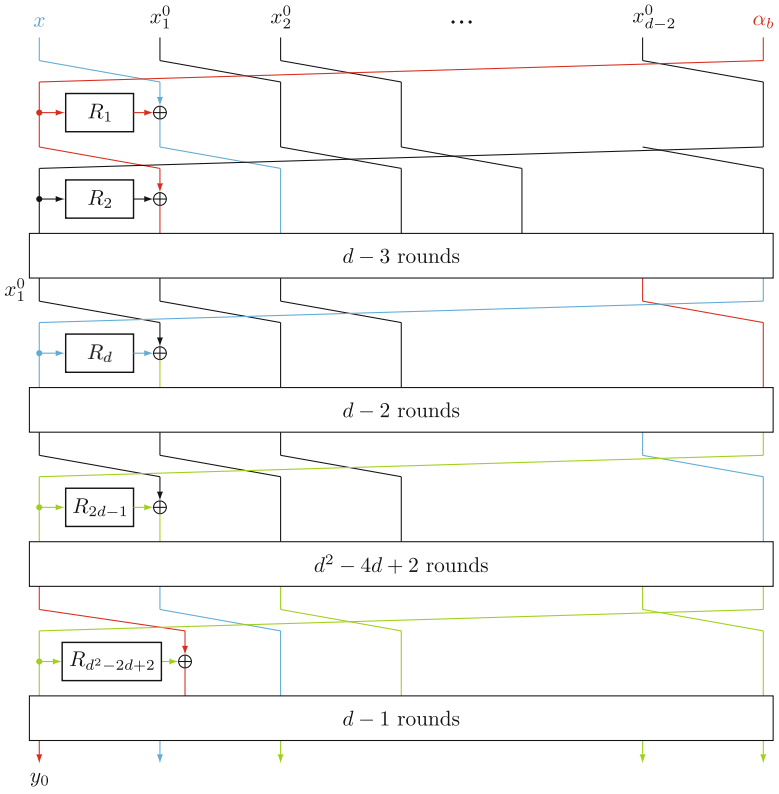

Fig. 7. $(d^2 - d + 1)$-round distinguishing attack

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

$$\begin{aligned} f^{\mathcal{O}^{-1}}(b, x) &= \alpha_b \oplus y_0 \\ &= \alpha_b \oplus x_0^{d^2-d+1} \\ &= \alpha_b \oplus x_1^{d^2-2d+2}, \end{aligned} \tag{7}$$

since $x_1^i = x_2^{i+1} = x_3^{i+2} = \cdots = x_0^{i+d-1}$ (See Fig. 7).

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 $s = (1, R_1(\alpha_0) \oplus R_1(\alpha_1))$.

Proof. In the first round, $R_1(\alpha_b)$ is xored into 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 into x_1^0. This implies that x_1^d is

$$x_1^d = R_d(R_1(\alpha_b) \oplus x) \oplus x_1^0 . \tag{8}$$

See Fig. 7. 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, Eq. (8) 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 into 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 (Specifically, it depends only on x_1^0). 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 into the sub-block which was x_i^0 at the input, for $i = 3, 4, \ldots, d-2$. We see that the sub-block itself depends on $x_1^0, \ldots, x_{i-1}^0$, but it is a constant that is independent of the input (b, x) since a value related to (b, x) is not xored into the sub-block. Therefore, 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 into the sub-block which was α_b at the input. Since only the value that does not include b nor x is xored into 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

$$x_1^{d^2-2d+2} = R'''(R_1(\alpha_b) \oplus x) \oplus \alpha_b . \tag{9}$$

From Eqs. (7) and (9), 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 on Type-1 GFSs

Similarly to the previous key recovery attacks by Dong et al. [10] that combine Grover search and the distinguisher, we can construct key recovery attacks against Type-1 GFSs based on our distinguishers.

With the $(3d-3)$-round distinguisher in qCPA setting, 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 in qCCA setting, by using the decryption oracle, we can recover the key of the r-round Type-1 GFS for $r > d^2-d+1$ 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 Quantum Attacks on Round-Reduced CAST-256 Block Cipher in qCPA Setting

CAST-256 block cipher [1] is a first-round AES candidate. It has 48 rounds, including 24 rounds Type-1 GFS and 24 rounds inverse Type-1 GFS. The block size is 128 bits, which are divided into four 32-bit branches and the key size can be 128, 192 or 256 bits. Each round function absorbs 37-bit subkey. Our attack is quite general and does not need any other details of the cipher.

In this section, we introduce a new 14-round quantum distinguisher in qCPA on CAST-256 shown in Fig. 8. The distinguisher, started from the 24th round, is composed of 1-round Type-1 GFS and 13-round inverse Type-1 GFS. It is derived based on the result presented in Sect. 5. When $d=4$, $(d^2-d+1)=13$ round distinguisher is obtained (from round R_{25} to R_{37} of CAST-256). Thanks to the special structure of CAST-256, we could add one more round R_{24} to the 13-round distinguisher for free. Hence, the 14-round distinguisher is derived.

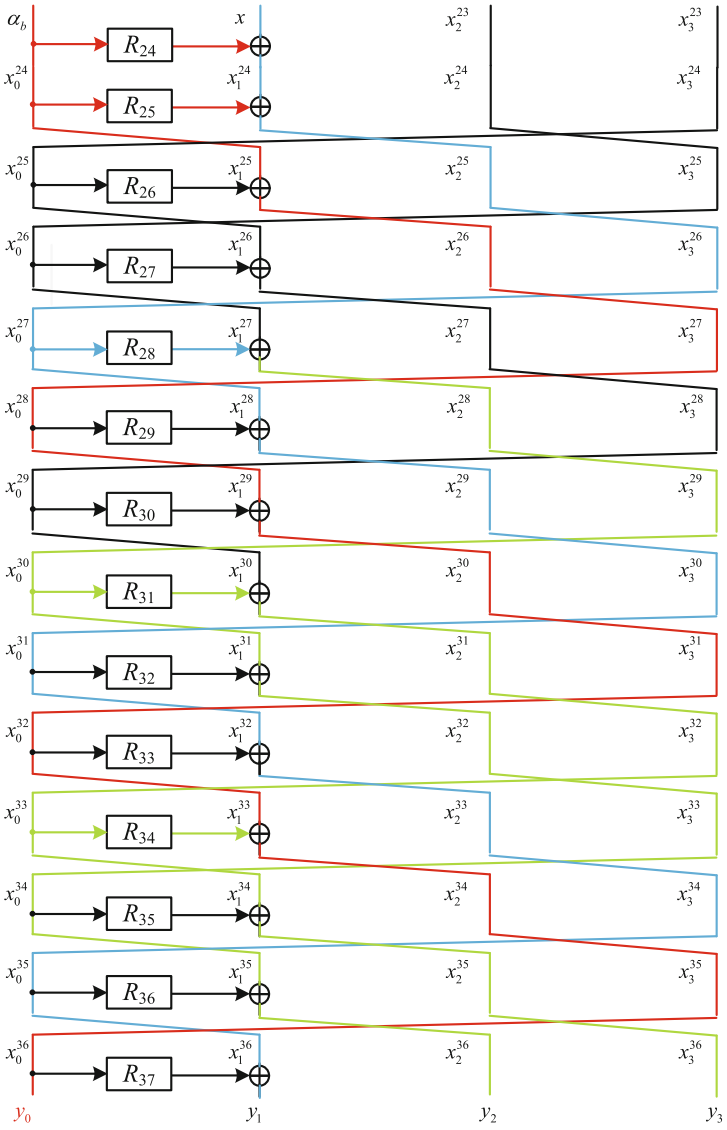

Fig. 8. 14-round distinguishing attack on CAST-256

We also fix two distinct constants α_0, α_1 and 2 constants x_2^{23}, x_3^{23}, which are all n bits. Given the 14-round CAST-256 encryption oracle $\mathcal{O}$, we define $f^{\mathcal{O}}$ as

$$f^{\mathcal{O}} : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$$
$$(b, x) \mapsto \alpha_b \oplus y_0 \,,$$
$$\text{where } (y_0, y_1, y_2, y_3) = \mathcal{O}(\alpha_b, x, x_2^{23}, x_3^{23}) \,.$$

According to Lemma 2, $f^{\mathcal{O}}$ has the period $s = (1, R_{24}(\alpha_0) \oplus R_{25}(\alpha_0) \oplus R_{24}(\alpha_1) \oplus R_{25}(\alpha_1))$. As is shown in Sect. 6, we could add or append several rounds to attack $r > 14$ rounds CAST-256 in time $\mathcal{O}(2^{\frac{37(r-14)}{2}})$, because the subkey length that we need to recover is $37(r-14)$ bits. Thus we could attack 20-round CAST-256 with 256-bit key in time 2^{111}, which is faster than Grover's algorithm by a factor of $2^{128-111} = 2^{17}$.

8 Conclusions

In this paper, we give some improved polynomial-time quantum distinguishers on Type-1 GFS in qCPA and qCCA settings. First, we give new qCPA quantum distinguishers on $(3d-3)$-round Type-1 GFS with branches $d \geq 3$, which gain $(d-2)$ more rounds than the previous distinguishers. Hence, we could get better key-recovery attacks, whose time complexities gain a factor of $2^{\frac{(d-2)n}{2}}$. We also obtain (d^2-d+1)-round qCCA quantum distinguishers on Type-1 GFS, which gain many more rounds than the previous distinguishers. In addition, we also discuss the quantum attack on CAST-256 block cipher.

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 in qCPA setting, and we may distinguish more than (d^2-d+1) rounds in qCCA setting. Moreover, we may distinguish more than 14 rounds of CAST-256 when considering its special structure, which applies both Type-1 GFS and its inverse as the round functions. We anticipate the analysis with respect to the provable security approach in [18] can settle the problem, while this is beyond the scope of this paper. We also note that we do not know the impact of combining qCPA and qCCA as applied against 4-round Feistel block ciphers in [22].

Another open question is that, we could apply (d^2-d+1)-round qCCA quantum distinguishers to other block ciphers. Note that when the branch number is large, the distinguisher becomes very long.

Acknowledgments. The authors thank the anonymous reviewers for helpful comments. Boyu Ni and Xiaoyang Dong are supported by the National Key Research and Development Program of China (No. 2017YFA0303903), the National Natural Science Foundation of China (No. 61902207), the National Cryptography Development Fund (No. MMJJ20180101, MMJJ20170121).

References

1. Adams, C., Gilchrist, J.: The CAST-256 encryption algorithm. RFC 2612, June 1999
2. Anderson, R.J., Biham, E.: Two practical and provably secure block ciphers: BEAR and LION. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 113–120. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-60865-6_48

3. Aoki, K., et al.: *Camellia*: a 128-bit block cipher suitable for multiple platforms—design and analysis. In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 39–56. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44983-3_4
4. Bogdanov, A., Leander, G., Nyberg, K., Wang, M.: Integral and multidimensional linear distinguishers with correlation zero. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 244–261. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_16
5. Bonnetain, X.: Quantum key-recovery on full AEZ. In: Adams, C., Camenisch, J. (eds.) SAC 2017. LNCS, vol. 10719, pp. 394–406. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-72565-9_20
6. Bonnetain, X., Naya-Plasencia, M., Schrottenloher, A.: On quantum slide attacks. Cryptology ePrint Archive, Report 2018/1067 (2018). https://eprint.iacr.org/2018/1067
7. Brassard, G., Hoyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. Contemp. Math. **305**, 53–74 (2002)
8. Dinur, I., Dunkelman, O., Keller, N., Shamir, A.: New attacks on Feistel structures with improved memory complexities. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 433–454. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_21
9. Dong, X., Dong, B., Wang, X.: Quantum attacks on some Feistel block ciphers. Cryptology ePrint Archive, Report 2018/504 (2018). https://eprint.iacr.org/2018/504
10. Dong, X., Li, Z., Wang, X.: Quantum cryptanalysis on some generalized Feistel schemes. Sci. China Inf. Sci. **62**(2), 022501 (2019)
11. Dong, X., Wang, X.: Quantum key-recovery attack on Feistel structures. Sci. China Inf. Sci. **61**(10), 102501:1–102501:7 (2018)
12. National Soviet Bureau of Standards: Information processing system - cryptographic protection - cryptographic algorithm GOST 28147–89
13. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22–24, 1996, pp. 212–219 (1996)
14. Gueron, S., Mouha, N.: Simpira v2: a family of efficient permutations using the AES round function. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 95–125. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_4
15. Guo, J., Jean, J., Nikolić, I., Sasaki, Y.: Meet-in-the-middle attacks on generic Feistel constructions. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 458–477. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_24
16. Guo, J., Jean, J., Nikolic, I., Sasaki, Y.: Meet-in-the-middle attacks on classes of contracting and expanding Feistel constructions. IACR Trans. Symmetric Cryptol. **2016**(2), 307–337 (2016)
17. Hoang, V.T., Rogaway, P.: On generalized Feistel networks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 613–630. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_33
18. Hosoyamada, A., Iwata, T.: 4-round Luby-Rackoff construction is a qPRP. In: Galbraith, S., Moriai, S. (eds.) ASIACRYPT 2019. LNCS, Springer, Cham (2019). To appear

19. Hosoyamada, A., Sasaki, Y.: Quantum Demiric-Selçuk meet-in-the-middle attacks: applications to 6-round generic Feistel constructions. In: Catalano, D., De Prisco, R. (eds.) SCN 2018. LNCS, vol. 11035, pp. 386–403. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98113-0_21
20. Isobe, T., Shibutani, K.: Generic key recovery attack on Feistel scheme. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8269, pp. 464–485. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-42033-7_24
21. Ito, G., Hosoyamada, A., Matsumoto, R., Sasaki, Y., Iwata, T.: Quantum chosen-ciphertext attacks against Feistel ciphers. Cryptology ePrint Archive, Report 2018/1193 (2018). https://eprint.iacr.org/2018/1193
22. Ito, G., Hosoyamada, A., Matsumoto, R., Sasaki, Y., Iwata, T.: Quantum chosen-ciphertext attacks against Feistel ciphers. In: Matsui, M. (ed.) CT-RSA 2019. LNCS, vol. 11405, pp. 391–411. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12612-4_20
23. Jutla, C.S.: Generalized birthday attacks on unbalanced Feistel networks. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 186–199. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0055728
24. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9815, pp. 207–237. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_8
25. Kilian, J., Rogaway, P.: How to protect DES against exhaustive key search. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 252–267. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68697-5_20
26. Kilian, J., Rogaway, P.: How to protect DES against exhaustive key search (an analysis of DESX). J. Cryptol. **14**(1), 17–35 (2001)
27. Knudsen, L.R.: The security of Feistel ciphers with six rounds or less. J. Cryptol. **15**(3), 207–222 (2002)
28. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: IEEE International Symposium on Information Theory, ISIT 2010, June 13–18, 2010, Austin, Texas, USA, Proceedings, pp. 2682–2685 (2010)
29. Kuwakado, H., Morii, M.: Security on the quantum-type Even-Mansour cipher. In: Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28–31, 2012, pp. 312–316 (2012)
30. Leander, G., May, A.: Grover meets Simon – quantumly attacking the FX-construction. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10625, pp. 161–178. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70697-9_6
31. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput. **17**(2), 373–386 (1988)
32. Lucks, S.: Faster Luby-Rackoff ciphers. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 189–203. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-60865-6_53
33. Moriai, S., Vaudenay, S.: On the pseudorandomness of top-level schemes of block ciphers. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 289–302. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-44448-3_22

34. Nachef, V., Volte, E., Patarin, J.: Differential attacks on generalized Feistel schemes. In: Abdalla, M., Nita-Rotaru, C., Dahab, R. (eds.) CANS 2013. LNCS, vol. 8257, pp. 1–19. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-02937-5_1
35. Patarin, J., Nachef, V., Berbain, C.: Generic attacks on unbalanced Feistel schemes with contracting functions. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 396–411. Springer, Heidelberg (2006). https://doi.org/10.1007/11935230_26
36. Patarin, J., Nachef, V., Berbain, C.: Generic attacks on unbalanced Feistel schemes with expanding functions. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 325–341. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76900-2_20
37. Santoli, T., Schaffner, C.: Using Simon's algorithm to attack symmetric-key cryptographic primitives. Quantum Inf. Comput. **17**(1&2), 65–78 (2017)
38. Schneier, B., Kelsey, J.: Unbalanced Feistel networks and block cipher design. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 121–144. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-60865-6_49
39. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74619-5_12
40. Simon, D.R.: On the power of quantum computation. SIAM J. Comput. **26**(5), 1474–1483 (1997)
41. Tjuawinata, I., Huang, T., Wu, H.: Improved differential cryptanalysis on generalized Feistel schemes. In: Patra, A., Smart, N.P. (eds.) INDOCRYPT 2017. LNCS, vol. 10698, pp. 302–324. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-71667-1_16
42. Volte, E., Nachef, V., Patarin, J.: Improved generic attacks on unbalanced Feistel schemes with expanding functions. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 94–111. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17373-8_6
43. Wagner, D.: The boomerang attack. In: Knudsen, L. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48519-8_12
44. Wang, M., Wang, X., Hu, C.: New linear cryptanalytic results of reduced-round of CAST-128 and CAST-256. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 429–441. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04159-4_28
45. Zhandry, M.: How to construct quantum random functions. In: 53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20–23, 2012, pp. 679–687 (2012)
46. Zheng, Y., Matsumoto, T., Imai, H.: On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 461–480. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_42