Quantum Attacks on Type-1 Generalized Feistel Schemes

Hong-Wei Sun[1], Bin-Bin Cai[1], Su-Juan Qin[1], Qiao-Yan Wen[1], and Fei Gao*[1]

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
gaof@bupt.edu.cn

Abstract. Generalized Feistel schemes (GFSs) are extremely important and extensively researched cryptographic schemes. In this paper, we investigate the security of Type-1 GFS in quantum circumstances. On the one hand, in the qCCA setting, we give a new quantum polynomial-time distinguisher on (d^2-1)-round Type-1 GFS with branches $d \geq 3$, which extends the previous results by $d-2$ rounds. This leads to a more efficient analysis of type-1 GFS, that is, the complexity of some previous key-recovery attacks is reduced by a factor of $2^{\frac{(d-2)k}{2}}$, where k is the key length of the internal round function. On the other hand, for CAST-256, which is a certain block cipher based on Type-1 GFS, we give a 17-round quantum distinguisher in the qCPA setting. As a result, we construct an $r(r > 17)$ round quantum key-recovery attack with complexity $O(2^{\frac{37(r-17)}{2}})$.

Keywords: Generalized Feistel scheme · CAST-256 · Simon algorithm · Quantum cryptanalysis · Quantum algorithm.

1 Introduction

Quantum attacks against symmetric crypto primitives. Quantum computing is more computationally powerful than classical computing in solving specific problems, such as solving factorization [1], equations [2–4], dimensionality reduction [5–7], anomaly detection [8, 9], classification [10–12], and so on [13–15]. Recent works show that the quantum algorithm has a dramatic speedup on the cryptanalysis of symmetric crypto primitives. This started with the 3-round Feistel distinguisher proposed by Kuwakado and Morii [16]. After that, more generic constructions, such as Even-Mansour cipher [17, 18], FX construction [19], message authentication codes (MACs) [20–23], etc [24–26], were broken using different quantum algorithms, including Simon algorithm [27], Grover algorithm [28], Grover-meets-Simon algorithm [19], Bernstein-Vazirani (BV) algorithm [29], etc.

Feistel ciphers. The Feistel cipher, also known as the Luby-Rackoff cipher, is a classical construction to build a random permutation out of random functions or random permutations. This construction has been extensively studied and

adopted in several block cipher standards, such as DES, Triple-DES, Gost [30], and CAST-128 [31]. At CRYPTO 1989, Zheng et al. [32] introduced three general frameworks Type-1, Type-2, and Type-3 generalized Feistel schemes (GFSs) for Feistel-type constructions with more branches and different operations. Many important primitives were designed based on the three GFSs, such as CAST-256 [33] (Type-1), CLEFIA (Type-2), RC6 (Type 2), and MARS [34] (Type-3).

Previous attacks. In addition to Kuwakado and Morii's work [16], Ito et al. [35] introduced the first 4-round quantum distinguisher on Feistel cipher in the quantum chosen-ciphertext setting. At CRYPTO 2022, Canalc et al. [36] found new periodic functions for 4-round Feistel-FK and 5-round Feistel-FK with internal permutation. For GFSs, Dong et al. [37] showed quantum distinguisher attacks against $(2d-1)$-round Type-1 and $(d+1)$-round Type-2 GFSs with branches $d \geq 3$. Later on, Ni et al. [38] proposed some improved polynomial-time quantum distinguishers on Type-1 GFSs in quantum chosen-plaintext attack (qCPA) and quantum chosen-ciphertext attack (qCCA) settings. That is, $(3d-3)$-round and (d^2-d+1)-round Type-1 GFSs were broken in qCPA and qCCA settings, respectively. In PQCrypto 2020, Hodžić et al. [39] proposed quantum distinguisher attacks on d-round Type-3 GFSs. Zhang et al. [40] improved the Type-3 distinguisher to cover $d+1$ round. These results rely crucially on the fact that many popular designs in symmetric cryptography have a strong algebraic structure such that the adversary can build a periodic function based on the target cryptographic scheme, and then use Simon algorithm to recover the period. This kind of Simon-based attack provides an exponential speedup in the number of queries compared to classical attacks.

In addition, based on the above quantum distinguishers, the adversary can give generic quantum key-recovery attacks by applying the combination of Simon algorithm and Grover algorithm (Grover-meets-Simon algorithm [19]). In these attacks, the attacker first makes a guess u for part of the key, say k_1 (the Grover part). Only for the correct guess, the attacker gets a periodic function, which is then detected with the Simon algorithm. With this technique, Dong et al. [41] introduced some key-recovery attacks by appending several rounds to the quantum distinguisher of Feistel construction. Unlike the exponential speedup of the Simon-based distinguisher, these key-recovery attacks only provide a polynomial speedup compared with the quantum brute force search.

Our contributions. In this work, we deepen our understanding of how to apply quantum algorithms to evaluate the security of Type-1 GFSs. We answer the following two open questions by Ni et al. [38].

1. Can we distinguish more than (d^2-d+1)-round Type-1 GFSs in the qCCA setting?
   We give a new quantum polynomial-time distinguisher on (d^2-1)-round Type-1 GFSs with branches $d \geq 3$, which extends the previous results by $d-2$ rounds. Based on the Grover-meets-Simon algorithm, we can get more effi-

cient key-recovery attacks, whose time complexities gain a factor of $2^{\frac{(d-2)k}{2}}$, where k is the key length of the internal round function. The distinguishers and key-recovery attacks are summarized in Tables 1 and 2.

2. Can we distinguish more than 14 rounds of CAST-256 when considering its special structure, which applies both Type-1 GFSs and its inverse as the round functions?
   For CAST-256, which is a certain block cipher based on Type-1 GFS, we give a 17-round quantum distinguisher in the qCPA setting. Based on the proposed distinguisher, we construct an $r(r > 17)$-round quantum key-recovery attack with complexity $O(2^{\frac{37(r-17)}{2}})$. Based on this, we could attack up to 23-round CAST-256 (256-bit key version) in time 2^{111}, which is better than the best previous attack (20 rounds [38]). Tables 3 and 4 summarize our main results and comparison with previous classical and quantum works. In particular, for 128-bit key version, our results reach 20 rounds, which gains three more rounds than before.

Table 1: Rounds of quantum distinguishers on Type-1 GFSs.

Source	Setting	Distinguisher	$d=3$	$d=4$	$d=5$	$d=6$	$\cdots$
[37]	qCPA	$(2d-1)$	5	7	9	11	$\cdots$
[38]	qCCA	(d^2-d+1)	7	13	21	31	$\cdots$
Sect. 3	qCCA	(d^2-1)	8	15	24	35	$\cdots$

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

Setting	Distinguisher	Key-recovery rounds	Complexity (log)
qCPA	$(2d-1)$ [37]	$r \geq d^2-d+2$	$(\frac{1}{2}d^2-\frac{2}{3}d+2)\cdot\frac{k}{2}+\frac{(r-d^2+d-2)k}{2}$
qCCA	(d^2-d+1) [38]	$r > d^2-d+1$	$\frac{(r-(d^2-d+1))k}{2}$
qCCA	(d^2-1) (ours)	$r > d^2-1$	$\frac{(r-(d^2-1))k}{2}$

* Note that for Type-1 GFSs, the trivial bound is $\frac{rk}{2}$, where k is the key size of the internal round function.

Organization. The paper is organized as follows. In Sect. 2, we introduce some basic notations, the quantum algorithms (Grover algorithm, Simon algorithm, and Grover-meets-Simon algorithm) used in this paper, and some previous attacks. In Sect. 3, we propose a new distinguisher for the Type-1 GFS. Based on this, we introduce new quantum key-recovery attacks. In Sect. 4, for CAST-256, we give a 17-round quantum distinguisher in the qCPA setting. Finally, we conclude in Sect. 5.

Table 3: Quantum attacks on CAST-256.

Rsource	Setting	Distinguisher	Attacked rounds					
			$r = 18$	$r = 19$	$r = 20$	$r = 21$	$r = 22$	$r = 23$
[37]	qCPA	7	-	-	-	-	-	-
[38]	qCPA	14	2^{74}	$2^{92.5}$	2^{111}	-	-	-
Setc. 4	qCPA	17	$2^{18.5}$	2^{37}	$2^{55.5}$	2^{74}	$2^{92.5}$	2^{111}

* Note that for CAST-256, the trivial bound is 2^{128} by Grover algorithm.

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

Algorithm	Source	Attack	Rounds	Data	Time
CAST-128	[42]	boomerang	16	$2^{49.3}$	-
	[37]	qCPA	12	-	$2^{55.5}$
	[38]	qCPA	17	-	$2^{55.5}$
	Sect. 4	qCPA	20	-	$2^{55.5}$
CAST-192	[43]	linear	24	$2^{124.1}$	$2^{156.52}$
	[37]	qCPA	15	-	$2^{92.5}$
	[38]	qCPA	19	-	$2^{92.5}$
	Sect. 4	qCPA	22	-	$2^{92.5}$
CAST-256	[44]	multidim.ZC	28	$2^{98.8}$	$2^{246.9}$
	[37]	qCPA	16	-	2^{111}
	[38]	qCPA	20	-	2^{111}
	Sect. 4	qCPA	23	-	2^{111}

2 Preliminaries

Let F_2 denote the prime field with two elements 0 and 1, i.e. $\{0,1\}$. And the n-dimensional vector space of F_2 is denoted by F_2^n, i.e. $\{0,1\}^n$. We let " $\oplus$ " denote the XOR (addition in F_2^n), and " $\cdot$ " denote the scalar product of bit-strings seen as n-bit vectors. Let $Perm(n)$ be a random permutation on $\{0,1\}^n$, and let $Func(n)$ be the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$.

2.1 Type-1 generalized Feistel schemes

Type-1 generalized Feistel schemes (GFSs) are widely used frameworks in symmetric-key primitive designs such as CAST-256. In type-1 GFSs, we divide the dn-bit state into $d \geq 3$ branches, and each branch constitutes an n-bit sub-block. Let E_r denote the encryption algorithm of the r-round Type-1 GFS (corresponds to decryption algorithm E_r^{-1}). Given r keyed round functions $R_1, R_2, \cdots, R_r \in Func(n)$, and $(x_1^0, x_2^0, \cdots, x_d^0) \in (\{0,1\}^n)^d$, one computes the output $(x_1^r, x_2^r, \cdots, x_d^r)$ by computing

$$x_1^i \leftarrow R_i(x_1^{i-1}) \oplus x_2^{i-1}, x_2^i \leftarrow x_3^{i-1}, x_3^i \leftarrow x_4^{i-1}, \cdots, x_d^i \leftarrow x_1^{i-1}$$

for $i = 1, 2, \cdots, r$, which is depicted in Fig. 1. By shifting the branches in the reverse direction, the decryption is automatically determined. We consider that a k-bit key, k_i, is required as input for the round function R_i, making the total key length of E_r is rk-bit.

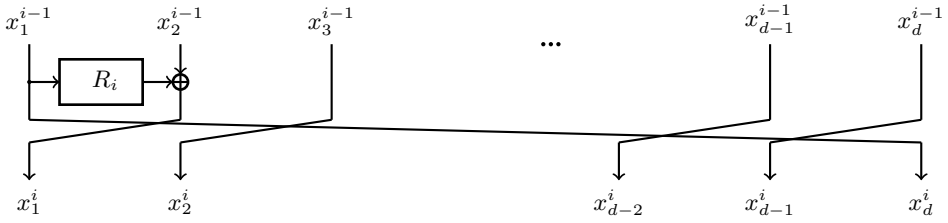

Fig. 1: The i-th round of Type-1 GFS.

2.2 Pseudo-Random Permutation

Next, we take into account the adversary A performing a quantum chosen-plaintext attack (qCPA) or a quantum chosen-ciphertext attack (qCCA), in which the adversary requests plaintexts or ciphertexts and receives corresponding ciphertexts or plaintexts, respectively. Let PRP-qCPA and PRP-qCCA denote the pseudo-random permutation (PRP) security under qCPA and qCCA respectively. The standard definitions are as follows.

Definition 1 [35, 45]. (PRP-qCPA) Let $E_k : K \times X \to X$ be a family of permutations indexed by the elements in K, $g : X \to X$. Let A be a quantum adversary[1]. The PRP-qCPA advantage of A is defined as

$$Adv_E^{PRP-qCPA}(A) = |Pr_{k\in K}[A^{E_k(\cdot)} \Rightarrow 1] - Pr_{g\in Perm(X)}[A^{g(\cdot)} \Rightarrow 1]|.$$

Here, let $A^{E_k(\cdot)} \Rightarrow 1$ denote an adversary performing quantum queries to oracle E_k and outputs 1.

Definition 2 [35, 45]. (PRP-qCCA) Let $E_k : K \times X \to X$ be a family of permutations indexed by the elements in K, $g : X \to X$. Let A be a quantum adversary. The PRP-qCCA advantage of A is defined as

$$Adv_E^{PRP-qCCA}(A) = |Pr_{k\in K}[A^{E_k^{-1}(\cdot)} \Rightarrow 1] - Pr_{g\in Perm(X)}[A^{g^{-1}(\cdot)} \Rightarrow 1]|.$$

In particular, these two definitions guarantee that we can distinguish E_k from $Perm(X)$ if $Adv_E^{PRP-qCPA/qCCA}(A)$ is a big value.

[1] It is supposed that the adversary can make arbitrary quantum superposition of queries of the form $|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$.

2.3 Quantum Algorithm

In the following, we review Grover, Simon, and Grover-meets-Simon algorithms used in this paper. We refer to [19, 46] for a broader presentation.

1) Grover algorithm. Grover algorithm [28] allows a quadratic speedup on classical exhaustive search. Precisely, it solves the following problem.

Grover problem. Consider a function $f : \{0,1\}^n \to \{0,1\}$ is given as a black box[1], with a promise that there is x such that $f(x) = 1$. Then, find $x \in \{0,1\}^n$ such that $f(x) = 1$.

In the classical setting, one preimage is expected to be found in time (and oracle access to f) $O(2^n/e)$ if there are e preimages of 1 ($|\{x : f(x) = 1\}| = e$). However, in the quantum setting, Grover algorithm finds one preimage in time (and oracle access to O_f) $O(\sqrt{2^n/e})$. The Grover algorithm consists of the following three quantum steps.

1. Grover algorithm works first by producing a uniform superposition $|\psi\rangle = \frac{1}{\sqrt{2^n}}\Sigma_x|x\rangle$.
2. Next, it repeatedly applies the unitary operator $(2|\psi\rangle\langle\psi| - I)O_f$ on the state $|\psi\rangle$.
3. Then a final measurement will return x such that $f(x) = 1$, with an overwhelming probability.

Generally, the checking procedure can be done only with some errors. That is, the test function always returns 1 for elements in the target set, but for elements not in the target set that it also returns 1 with a negligible probability. The following theorem tackles this case.

Theorem 1 [47, 23]. Let n be a positive integers, $X(|X| = e)$ be a subset in $\{0,1\}^n$, $p_0 := \frac{e}{2^n}$ and $f : \{0,1\}^n \to \{0,1\}$ be a test function such that

$$\begin{cases} Pr[f(x) = 1] = 1 & \text{if } x \in X, \\ Pr[f(x) = 1] \leq p_1 & \text{if } x \notin X. \end{cases}$$

Assume the quantum implementation of $f(x)$ costs $O(n)$ qubits. Then Grover algorithm with $t = \lceil \frac{\pi}{4arcsin\sqrt{p_0}} \rceil$ quantum queries to $f(x)$ and $O(n)$ qubits will output an $x \in X$ with probability at least $\frac{p_0}{p_0+p_1}[1-(\frac{p_1}{p_0}+\sqrt{p_0+p_1}+2\sqrt{1+\frac{p_1}{p_0}}^3 p_0)^2]$.

In particular, if $e \leq 2$ and $p_1 \leq \frac{1}{2^{2n}}$, the error decreases exponentially with n.

[1] We can input x to the "black box" and ask it to compute $f(x)$, but we don't have access to its internal computation process.

2) Simon algorithm. Simon algorithm [27] gives the first example of an exponential quantum time speedup relative to an oracle. That is, it allows to efficiently compute the period of a Boolean function.

Simon problem. Given a Boolean function $f : \{0,1\}^n \to \{0,1\}^d$ and promise that there exists $s \in \{0,1\}^n$ such that for any $(x, y) \in \{0,1\}^n$, $[f(x) = f(y)] \Leftrightarrow [x \oplus y \in \{0, s\}]$, the goal is to find s.

This problem can be solved classically by searching collisions with $O(2^{n/2})$ queries. As the quantum superposition of queries of form $\Sigma_{x,y}\lambda_{x,y}|x\rangle|y\rangle \mapsto \Sigma_{x,y}\lambda_{x,y}|x\rangle|f(x) \oplus y\rangle$ is introduced in Simon algorithm, its query complexity is only $O(n)$. After repeating the following subroutine (Algorithm 1) cn times, we can obtain s by solving a system of linear equations. The algorithm can be applied to the problem of which condition "$f(x) = f(y)$ if and only if $x \oplus y \in \{0, s\}$" is replaced with the weaker condition "$f(x \oplus s) = f(x)$ for any x", under the assumption that f satisfies some good properties. Concretely, Kaplan et al. [20] have proved the following theorem.

Algorithm 1 Quantum subroutine of Simon algorithm.

Input: n, $O_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$
Output: y orthogonal to s

1: Applying a Hadamard transform $H^{\otimes n}$ to the initial state $|\psi_0\rangle = |0\rangle|0\rangle$ (a $(n + d)$-qubit state) to obtain the quantum superposition

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\Sigma_{x\in F_2^n}|x\rangle|0\rangle.$$

2: A quantum query to the function f maps to the state

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}}\Sigma_{x\in F_2^n}|x\rangle|f(x)\rangle.$$

3: Measuring the second register gives a value $f(z)$ and the first register is collapsed to

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle).$$

4: Applying again the Hadamard transform $H^{\otimes n}$ to the first register yields

$$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\Sigma_{y\in F_2^n}(-1)^{y\cdot z}(1 + (-1)^{y\cdot s})|y\rangle.$$

5: Measuring the state yields a value of y, which meets that $y \cdot s = 0$.

Theorem 2 [20]. Let $\varepsilon(f,s) := \max_{t\in\{0,1\}^n\setminus\{0,s\}} Pr_x[f(x)=f(x\oplus t)]$. If $\varepsilon(f,s)\leq p_0<1$, then Simon algorithm returns s with cn queries and $O(n+d)$ qubits, with probability at least $1-(2(\frac{1+p_0}{2})^c)^n$.

3) Grover-meets-Simon algorithm. In Ref. [19], Leander and May proposed to combine Simon's algorithm with Grover's algorithm (i.e., Grover-meets-Simon algorithm) to attack the construction with whitening keys. This algorithm solves the following problem.

Grover-meets-Simon problem. Let $f:\{0,1\}^m\times\{0,1\}^n\to\{0,1\}^d$ be a function such that there exist some $u\in\{0,1\}^m$ such that $f(u,\cdot)$ hide a non-trivial period s_u. Find any tuple $(u,s_u)\in U_s$, where $U_s := \{(u,s_u) : u\in\{0,1\}^m, s_u \text{ is the period of } f(u,\cdot)\}$.

In this algorithm, the attacker first makes a guess u (the Grover part). Only for the correct guess, the attacker gets a periodic function, which is then detected with the Simon algorithm. Thus, they have Grover as an outer loop with a running time of roughly $2^{m/2}$, and Simon as an inner loop with polynomial complexity. The following theorem shows the effect of the parameter

$$\varepsilon(f) := \max_{(u,t)\in\{0,1\}^m\times\{0,1\}^n\setminus\{0,U_s\}} Pr_x[f(u,x)=f(u,x\oplus t)]$$

on the success probability of the Grover-meets-Simon algorithm.

Theorem 3 [47, 23]. Let c be a positive integer, $p_0 := \frac{e}{2^m}$ and $p_1 := [2\cdot(\frac{1+\varepsilon(f)}{2})^c]^n$. Then Grover-meets-Simon algorithm with $\lceil\frac{\pi}{4arcsin\sqrt{p_0}}\rceil\cdot cn$ quantum queries to f and $O(m+cn^2+cdn)$ qubits outputs a tuple $(u,s_u)\in U_s$ with probability at least $\frac{(1-p_1)p_0}{p_0+p_1}[1-(\frac{p_1}{p_0}+\sqrt{p_0+p_1}+2\sqrt{1+\frac{p_1}{p_0}}^3 p_0)^2]$.

In particular, if $\varepsilon(f)\leq 1/2$ and $e\leq 2$, the error decreases exponentially with n. In case $d=m=n$, the Grover-meets-Simon algorithm solves this problem with $O(2^{n/2}n)$ quantum queries and $O(n^2)$ qubits.

2.4 Previous Attacks

In the following, we review the quantum attacks against Type-1 GFSs by Ni et al. [38]. They proposed a (d^2-d+1)-round distinguisher attack in the qCCA setting.

In order to distinguish Type-1 GFSs from a random permutation in a quantum setting, Ni et al. define the following function, with two arbitrary constants α_0, α_1 such that $\alpha_0\neq\alpha_1$, and

$$f^{O^{-1}}:\{0,1\}\times\{0,1\}^n\to\{0,1\}^n$$
$$b,x\mapsto\alpha_b\oplus y_1,$$

where $(y_1, y_2, \cdots, y_d) = O^{-1}(x, x_2^0, x_3^0, \cdots, x_{d-1}^0, \alpha_b)$, and $x_2^0, x_3^0, \cdots, x_{d-1}^0$ are arbitrary n-bit constants. Let the intermediate state value after the first i rounds be $(x_1^i, x_2^i, \cdots, x_d^i)$. For d^2-d+1-round decryption oracle O^{-1}, the function $f^{O^{-1}}$ is described as

$$\begin{aligned} f^{O^{-1}}(b, x) &= \alpha_b \oplus y_1 \\ &= \alpha_b \oplus x_1^{d^2-d+1} \\ &= \alpha_b \oplus x_2^{d^2-2d+2}, \end{aligned}$$

where $x_2^i = x_3^{i+1} = x_4^{i+2} = \cdots = x_1^{i+d-1}$. In the first round, $x_2^1 = x \oplus R_1(\alpha_b)$ (see Fig. 1). In the d-th round, $x_2^d = R_d(R_1(\alpha_b) \oplus x) \oplus x_2^0$. The function $R(\cdot) = R_d(\cdot) \oplus x_2^0$ is independent of the input (b, x), since x_2^0 is a constant. Then, $x_2^d = R(R_1(\alpha_b) \oplus x)$, where $R \in Func(n)$. Therefore, for some constants $x_3^0, x_4^0, \cdots, x_{d-1}^0, \alpha_b$, the value of $x_2^{d^2-2d+2}$ can be described as $x_2^{d^2-2d+2} = R'(R_1(\alpha_b) \oplus x) \oplus \alpha_b$, where $R' \in Func(n)$. In particular, this $f^{O^{-1}}$ satisfies $f^{O^{-1}}(b, x) = f^{O^{-1}}(b \oplus 1, x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1))$. Moreover,

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

Therefore, the function satisfies Simon's promise with $s = 1 \| R_1(\alpha_0) \oplus R_1(\alpha_1)$, and we can recover $R_1(\alpha_0) \oplus R_1(\alpha_1)$ using Simon algorithm. This gives a distinguisher, because Simon algorithm applied to a random permutation returns zero with high probability.

Next, we review the key-recovery attack.

Key-recovery attacks. With the (d^2-d+1)-round distinguisher in the qCCA setting, Ni et al. [38] can recover the key of the r-round Type-1 GFS for $r > d^2-d+1$ in time $O(2^{\frac{(r-(d^2-d+1))k}{2}})$, where the subkey size that they need to recover is $(r-d^2+d-1)k$ bits. Thus, their attack achieves a polynomial speedup compared with the quantum brute force search (Grover search [28]).

Truncate outputs of quantum oracles. Note that in their attack, Ni et al. implicitly assume that the attacker can query in superposition an oracle that returns solely the part $y_1 = x_2^{d^2-d+1}$ of the encryption. However, it is not trivial. Fortunately, Hosoyamada and Sasaki introduced a technique to simulate the truncation of outputs of quantum oracles without destroying quantum entanglements. To apply their attack, we need to simulate $x_2^{d^2-d+1}$. In a similar way as Ref. [48], let $O : |x\rangle|y\rangle|z\rangle \cdots |w\rangle \mapsto |x\rangle|y \oplus O_1(x)\rangle|z \oplus O_2(x)\rangle \cdots |w \oplus O_d(x)\rangle$ is the complete encryption oracle, where $O_j (1 \le j \le d)$ denotes the component of complete encryption. Our goal is to simulate oracle $O_2 : |x\rangle|z\rangle \to |x\rangle|z \oplus O_2(x)\rangle$. Now, we define $O_2' := (I \otimes H^{\otimes n} \otimes I \otimes H^{\otimes(d-2)n}) \cdot O \cdot (I \otimes H^{\otimes n} \otimes I \otimes H^{\otimes(d-2)n})$.

Then easy calculations show that

$$\begin{aligned}
O_2'|x\rangle|0\rangle|z\rangle|0\rangle &= (I\otimes H^{\otimes n}\otimes I\otimes H^{\otimes(d-2)n})\cdot O \\
&\quad \cdot(I\otimes H^{\otimes n}\otimes I\otimes H^{\otimes(d-2)n})|x\rangle|0\rangle|z\rangle|0\rangle \\
&= (I\otimes H^{\otimes n}\otimes I\otimes H^{\otimes(d-2)n})\cdot O|x\rangle|+\rangle|z\rangle|+\rangle \\
&= (I\otimes H^{\otimes n}\otimes I\otimes H^{\otimes(d-2)n})|x\rangle[\frac{1}{\sqrt{2^n}}\Sigma_y|y\oplus O_1(x)\rangle] \\
&\quad |z\oplus O_2(x)\rangle\cdots[\frac{1}{\sqrt{2^n}}\sum_w |w\oplus O_n(x)\rangle] \\
&= (I\otimes H^{\otimes n}\otimes I\otimes H^{\otimes(d-2)n})|x\rangle|+\rangle|z\oplus O_2(x)\rangle\cdots|+\rangle \\
&= |x\rangle|0\rangle|z\oplus O_2(x)\rangle|0\rangle
\end{aligned}$$

where the fourth equality follows from the fact that $\frac{1}{\sqrt{2^n}}\Sigma_y|y\oplus O_1(x)\rangle = \frac{1}{\sqrt{2^n}}\Sigma_{y'}|y'\rangle = |+\rangle$. Hence, we can simulate O_2 given the complete encryption oracle O, using ancilla qubits.

3 Quantum Attack on the Type-1 GFS

In this section, we give new Simon-based distinguishing attacks against (d^2-1)-round Type-1 GFSs, in the qCCA setting. In particular, we construct new periodic functions corresponding to targeted schemes, and improve the number of rounds that we can distinguish from (d^2-d+1) rounds to (d^2-1) rounds.

3.1 (d^2-1)-Round Distinguisher Attack in qCCA Setting

In order to distinguish the (d^2-1)-round Type-1 GFS from a random permutation, we consider the case is $O^{-1}=E_{d^2-1}^{-1}$, and define the following function, with two distinct constants α_0, α_1 and $d-2$ constants $x_3^0, x_4^0, \cdots, x_d^0$,

$$\begin{aligned}
f^{O^{-1}} : \{0,1\}^n &\to \{0,1\}^n \\
x &\mapsto y_1^{\alpha_0}\oplus y_1^{\alpha_1}\oplus\alpha_0\oplus\alpha_1,
\end{aligned}$$

where $(y_1^{\alpha_b}, y_2^{\alpha_b}, \cdots, y_d^{\alpha_b}) = O^{-1}(x, \alpha_b, x_3^0, x_4^0, \cdots, x_d^0)$ (See Fig. 2).

For the (d^2-1)-round Type-1 GFS, the intermediate parameters after the first i rounds are $(x_1^i, x_2^i, \cdots, x_d^i)$. Then, we have

$$\begin{aligned}
f^{O^{-1}}(x) &= y_1^{\alpha_0}\oplus y_1^{\alpha_1}\oplus\alpha_0\oplus\alpha_1 \\
&= x_1^{d^2-1}(\alpha_0)\oplus x_1^{d^2-1}(\alpha_1)\oplus\alpha_0\oplus\alpha_1 \\
&= x_2^{d^2-d}(\alpha_0)\oplus x_2^{d^2-d}(\alpha_1)\oplus\alpha_0\oplus\alpha_1, \qquad (1)
\end{aligned}$$

[1] Note that, we can get y_1 by truncating outputs of quantum oracle O^{-1} (See Sect. 2.4).

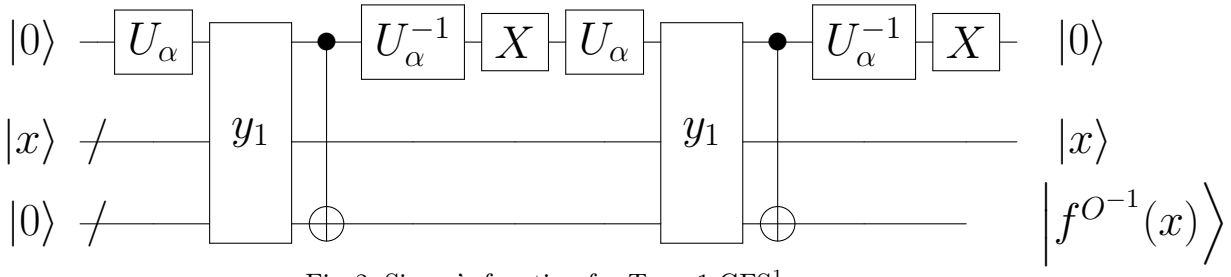

Fig. 2: Simon's function for Type-1 GFS[1].

where $x_2^i = x_3^{i+1} = x_4^{i+2} = \cdots = x_1^{i+d-1}$ (See Fig. 3).

By running Simon algorithm on $f^{O^{-1}}$, one can distinguish the (d^2-1)-round Type-1 GFS from a random permutation with overwhelming probability. Specially, we have the following theorem.

Theorem 4. Let R_i $(1 \le i \le d^2-1)$ be random functions, we can construct a quantum CCA distinguisher against (d^2-1)-round Type-1 GFSs in $O(n)$ quantum queries by using Simon algorithm.

Proof. In the first round, $R_1(x_d^0)$ is xored into x. In the d-th round, the value $R_1(x_d^0) \oplus x$ is used as the input of R_d and the output of R_d is xored into α_b. Then, the value of x_2^d is described as

$$x_2^d = \alpha_b \oplus R_d(x \oplus R_1(x_d^0)).$$

The function $R(\cdot) = R_d(\cdot \oplus R_1(x_d^0))$ is independent of the input x since x_d^0 is a constant. Then, we have

$$x_2^d = \alpha_b \oplus R(x)$$

with some functions $R \in Func(n)$. After additional d rounds, we have

$$\begin{aligned} x_2^{2d} &= x_1^{2d-1} \oplus R_{2d}(x_d^{2d-1}) \\ &= x_2^d \oplus R_{2d}(x_2^{d+1}) \\ &= x_2^d \oplus R_{2d}(x \oplus R_1(x_d^0) \oplus R_{d+1}(x_d^0 \oplus R_2(x_{d-1}^0))), \end{aligned}$$

where $x_2^i = x_3^{i+1} = x_4^{i+2} = \cdots = x_1^{i+d-1}$ (See Fig. 3). The function $R'(\cdot) = R_{2d}(\cdot \oplus R_1(x_d^0) \oplus R_{d+1}(x_d^0 \oplus R_2(x_{d-1}^0)))$ is independent of the input x since x_d^0 and x_{d-1}^0 are constants. Therefore, for some functions $R', R'' \in Func(n)$, the value of x_2^{2d} is described as

$$x_2^{2d} = \alpha_b \oplus R(x) \oplus R'(x) = \alpha_b \oplus R''(x).$$

For $d-2$ constants $x_3^0, x_4^0, \cdots, x_d^0$, the value of $x_2^{2d+d(d-4)} = x_2^{d^2-2d}$ is described as

$$x_2^{d^2-2d} = \alpha_b \oplus R'''(x)$$

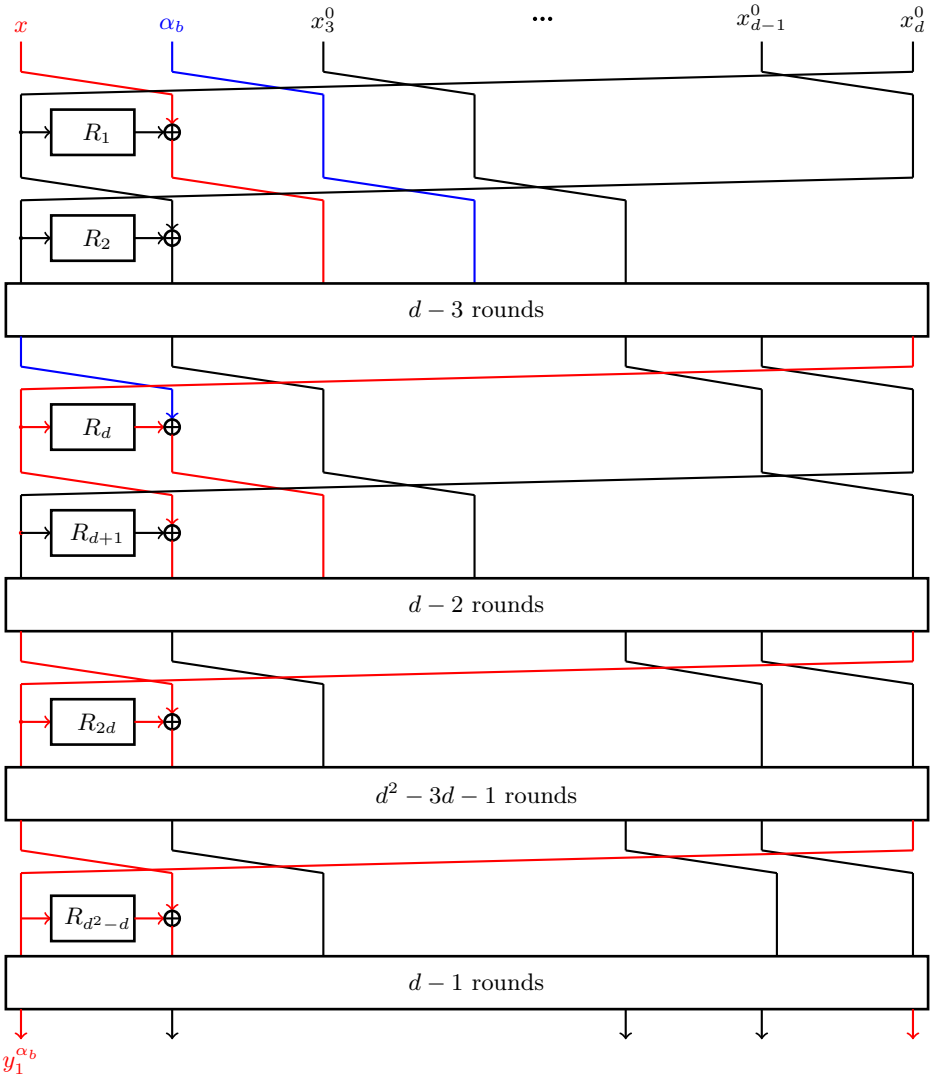

Fig. 3: (d^2-1)-round distinguishing attack.

for some functions $R''' \in Func(n)$. In the (d^2-d)-th round, the value $x_d^{d^2-d-1}$ is used as the input to the round function R_{d^2-d} and the output is xored into $x_2^{d^2-2d}$. Then, we have

$$\begin{aligned}
x_2^{d^2-d} &= x_1^{d^2-d-1} \oplus R_{d^2-d}(x_d^{d^2-d-1}) \\
&= x_2^{d^2-2d} \oplus R_{d^2-d}[x \oplus R_1(x_d^0) \oplus R_{d+1}(x_d^0 \oplus R_2(x_{d-1}^0)) \\
&\quad \oplus R_{2d+1}(x_d^0 \oplus R_2(x_{d-1}^0) \oplus R_{d+2}(x_{d-1}^0 \oplus R_3(x_{d-2}^0))) \oplus \cdots \\
&\quad \oplus R_{d^2-2d+1}(x_d^0 \oplus R_2(x_{d-1}^0) \oplus R_{d+2}(x_{d-1}^0 \oplus R_3(x_{d-2}^0)) \oplus \cdots \\
&\quad \oplus R_{d^2-3d+2}(x_{d-1}^0 \oplus R_3(x_{d-2}^0) \oplus R_{d+3}(x_{d-2}^0 \oplus R_4(x_{d-3}^0)) \oplus \cdots \\
&\quad \oplus R_{d^2+3d-2}(x_{d-2}^0 \oplus R_4(x_{d-3}^0) \oplus R_{d+4}(x_{d-3}^0 \oplus R_5(x_{d-4}^0)) \oplus \cdots \oplus R_{d^2-5d+4}(x_3^0 \oplus R_{d-1}(\alpha_b)))))].
\end{aligned}$$

The function $h(\alpha_b) = R_{d^2-2d+1}[x_d^0 \oplus R_2(x_{d-1}^0) \oplus \cdots \oplus R_{d^2-3d+2}(x_{d-1}^0 \oplus R_3(x_{d-2}^0) \oplus \cdots \oplus R_{d^2+3d-2}(x_{d-2}^0 \oplus R_4(x_{d-3}^0) \oplus \cdots \oplus R_{d^2-5d+4}(x_3^0 \oplus R_{d-1}(\alpha_b))))]$ is independent of the input b, since $x_3^0, x_4^0, \cdots, x_d^0$ are constants. Therefore, $x_2^{d^2-d}$ can be described as

$$x_2^{d^2-d} = \alpha_b \oplus R'''(x) \oplus R_{d^2-d}(x \oplus C \oplus h(\alpha_b)), \tag{2}$$

where $C = R_1(x_d^0) \oplus R_{d+1}(x_d^0 \oplus R_2(x_{d-1}^0)) \oplus R_{2d+1}(x_d^0 \oplus R_2(x_{d-1}^0) \oplus R_{d+2}(x_{d-1}^0 \oplus R_3(x_{d-2}^0))) \cdots$. In particular, from Eqs. (1) and (2), this $f^{O^{-1}}$ satisfies $f^{O^{-1}}(x \oplus h(\alpha_0) \oplus h(\alpha_1)) = f^{O^{-1}}(x)$. Moreover,

$$\begin{aligned}
f^{O^{-1}}(x \oplus h(\alpha_0) \oplus h(\alpha_1)) &= y_1^{\alpha_0} \oplus y_1^{\alpha_1} \oplus \alpha_0 \oplus \alpha_1 \\
&= x_2^{d^2-d}(\alpha_0) \oplus x_2^{d^2-d}(\alpha_1) \oplus \alpha_0 \oplus \alpha_1 \\
&= \alpha_0 \oplus R'''(x \oplus h(\alpha_0) \oplus h(\alpha_1)) \oplus R_{d^2-d}(x \oplus h(\alpha_0) \oplus h(\alpha_1) \oplus C \oplus h(\alpha_0)) \\
&\quad \oplus \alpha_1 \oplus R'''(x \oplus h(\alpha_0) \oplus h(\alpha_1)) \oplus R_{d^2-d}(x \oplus h(\alpha_0) \oplus h(\alpha_1) \oplus C \oplus h(\alpha_1)) \\
&\quad \oplus \alpha_0 \oplus \alpha_1 \\
&= R_{d^2-d}(x \oplus C \oplus h(\alpha_1)) \oplus R_{d^2-d}(x \oplus C \oplus h(\alpha_0)) \\
&= f^{O^{-1}}.
\end{aligned}$$

Therefore, the function satisfies Simon's promise with $s = h(\alpha_0) \oplus h(\alpha_1)$, and we can recover $h(\alpha_0) \oplus h(\alpha_1)$ using Simon algorithm. This gives a distinguisher because the Simon algorithm applied to a random permutation returns zero with high probability. Concretely, in the first query we ask x, and then we ask $x \oplus s$. If A is asking about (d^2-1)-round Type-1 GFS, then the outputs are the same. If A is asking about random permutation, then the outputs are different. Therefore, $Adv^{PRP-qCCA}_{Type-1GFS}(A) = 1 - (2(\frac{3}{4})^c)^n - \frac{1}{2^{n/2}}$. In particular, choosing $c \geq 3/(1-p_0)$ ensures that the probability is exponentially close to 1.

Example case of Type-1 GFS with $d = 3$. For Type-1 GFSs with $d = 3$, we give an 8-round quantum distinguisher as shown in Fig. 4. Concretely, from the above analysis, we define the following function, with two distinct constants α_0, α_1 and constant x_3^0.

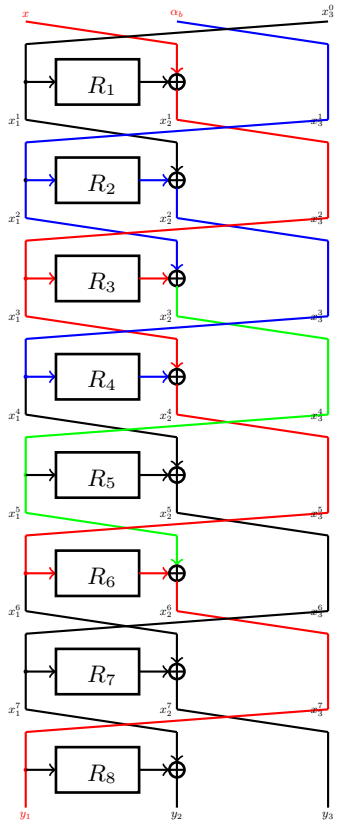

Fig. 4: 8-round distinguisher on Type-1 GFS with $d = 3$.

$$
\begin{aligned}
f^{O^{-1}} : \{0,1\}^n &\to \{0,1\}^n \\
x &\mapsto y_1^{\alpha_0} \oplus y_1^{\alpha_1} \oplus \alpha_0 \oplus \alpha_1 \\
f^{O^{-1}}(x) &= \alpha_0 \oplus R_3(x \oplus R_1(x_3^0)) \oplus R_6[x \oplus R_1(x_3^0) \oplus R_4(x_3^0 \oplus R_2(\alpha_0))] \\
&\quad \oplus \alpha_1 \oplus R_3(x \oplus R_1(x_3^0)) \oplus R_6[x \oplus R_1(x_3^0) \oplus R_4(x_3^0 \oplus R_2(\alpha_1))] \oplus \alpha_0 \oplus \alpha_1 \\
&= R_6[x \oplus R_1(x_3^0) \oplus R_4(x_3^0 \oplus R_2(\alpha_0))] \oplus R_6[x \oplus R_1(x_3^0) \oplus R_4(x_3^0 \oplus R_2(\alpha_1))],
\end{aligned}
$$

where $(y_1^{\alpha_b}, y_2^{\alpha_b}, y_3^{\alpha_b}) = O^{-1}(x, \alpha_b, x_3^0)$ (See Fig. 4). In particular, we have

$$
\begin{aligned}
f^{O^{-1}}(x \oplus s) &= R_6[x \oplus s \oplus R_1(x_3^0) \oplus R_4(x_3^0 \oplus R_2(\alpha_0))] \oplus R_6[x \oplus s \oplus R_1(x_3^0) \oplus R_4(x_3^0 \oplus R_2(\alpha_1))] \\
&= R_6[x \oplus R_1(x_3^0) \oplus R_4(x_3^0 \oplus R_2(\alpha_1))] \oplus R_6[x \oplus R_1(x_3^0) \oplus R_4(x_3^0 \oplus R_2(\alpha_0))] \\
&= f^{O^{-1}}(x),
\end{aligned}
$$

where $s = R_4(x_3^0 \oplus R_2(\alpha_0)) \oplus R_4(x_3^0 \oplus R_2(\alpha_1))$, and x_3^0 is a constant. Therefore, $f^{O^{-1}}(x)$ satisfies the promise of Simon algorithm with s, we can easily apply Simon algorithm to recover s, and distinguish it from the random permutation.

3.2 Key Recovery Attacks on the Type-1 GFS

In what follows, based on the (d^2-1)-round distinguisher, we could get better key-recovery attacks using Grover-meets-Simon algorithm, whose time complexities gain a factor of $2^{\frac{(d-2)k}{2}}$, where k is the key length of the internal round function. Concretely, we give key-recovery attacks on r-round Type-1 GFSs by adding $r-d^2+1$ rounds before the (d^2-1)-round distinguisher, in the qCCA setting.

The attack procedures can be summarized as follows.

1. Construct the quantum circuit, which requires the intermediate state value $(x, \alpha_b, x_3^{r-d^2+1}, x_4^{r-d^2+1}, \cdots, x_d^{r-d^2+1})$ after the first $r-d^2+1$ rounds and the first $r-d^2+1$ rounds' subkeys as input, and decrypt the first $r-d^2+1$ rounds to get the plaintext. Then use the oracle $f^{O^{-1}}$ encrypt the plaintext $(x_1^0, x_2^0, \cdots, x_d^0)$ to get the ciphertext $(x_1^r, x_2^r, \cdots, x_d^r)$.
2. Guess the subkeys of the first $r-d^2+1$ rounds. For each guessed subkey, use the d^2-1 rounds distinguisher to check its correctness. Concretely, only for the correct guess, the attacker gets a periodic function, which is then detected with the Simon algorithm.

For the r $(r > d^2-1)$ rounds, we need to guess the $(r-d^2+1)k$-bit key using Grover algorithm. Therefore, the key of the r-round Type-1 GFS can be recovered with $O(2^{\frac{(r-(d^2-1))k}{2}})$ quantum queries using $O(n^2)$ qubits by Theorem 3.

4 Quantum Attack on Round-Reduced CAST-256 Block Cipher in qCPA Setting

The CAST-256 block cipher [33] is designed as a candidate for Advanced Encryption Standard (AES). Even though CAST-256 was not among the finalists in the AES Process, its analysis may help understand the design rationale of other ciphers from the CAST family.

CAST-256 operates on 128-bit text blocks (four branches with 32-bit) under keys of 128, 192, or 256 bits. CAST-256 is based on the GFS structure and iterates 48 rounds for all key sizes, including 24 rounds Type-1 GFS and 24 rounds inverse Type-1 GFS. Each round function absorbs a 37-bit subkey. Note that in our attack, we don't need to know any additional encryption information for our attack because it is extremely broad.

In what follows, we present a 17-round quantum distinguishing attack in the qCPA setting and give an $r(r > 17)$-round quantum key-recovery attack. We first focus on the distinguishing attack.

Distinguishing Attack. Based on the special structure of CAST-256, we give a new 17-round (from 23-th round to 39-th round) quantum distinguisher (See Fig.5), which is composed of 2-round Type-1 GFS and 15-round inverse Type-1 GFS. More precisely, for the 17-round CAST-256 encryption oracle O, we define the following function, with two arbitrary constants α_0 and α_1 such that $\alpha_0 \neq \alpha_1$ and two constants x_1^{22} and x_2^{22}.

$$\begin{aligned} f^O : \{0,1\}^n &\to \{0,1\}^n \\ x &\mapsto y_1^{\alpha_0} \oplus y_1^{\alpha_1} \oplus \alpha_0 \oplus \alpha_1, \end{aligned}$$

where $(y_1^{\alpha_b}, y_2^{\alpha_b}, y_3^{\alpha_b}, y_4^{\alpha_b}) = O(x_1^{22}, x_2^{22}, x, \alpha_b)$ (See Fig. 5).

For the 17-round CAST-256, we have

$$\begin{aligned} f^O(x) &= y_1^{\alpha_0} \oplus y_1^{\alpha_1} \oplus \alpha_0 \oplus \alpha_1 \\ &= x_1^{39}(\alpha_0) \oplus x_1^{39}(\alpha_1) \oplus \alpha_0 \oplus \alpha_1 \\ &= x_2^{36}(\alpha_0) \oplus x_2^{36}(\alpha_1) \oplus \alpha_0 \oplus \alpha_1, \end{aligned} \tag{3}$$

where $x_1^{39} = x_4^{38} = x_3^{37} = x_2^{36}$ (See Fig. 5).

Specially, we have the following theorem.

Theorem 5. Let R_i $(1 \leq i \leq d^2 - 1)$ be random functions, we can construct a quantum CPA distinguisher against CAST-256 in $O(n)$ quantum queries by using Simon algorithm.

Proof. In the 3-th round, the value $x_2^{22} \oplus R_{23}(x_1^{22})$ is used as the input of R_{25} and the output of R_{25} is xored into $x \oplus R_{24}(x_2^{22} \oplus R_{23}(x_1^{22}))$. This implies that

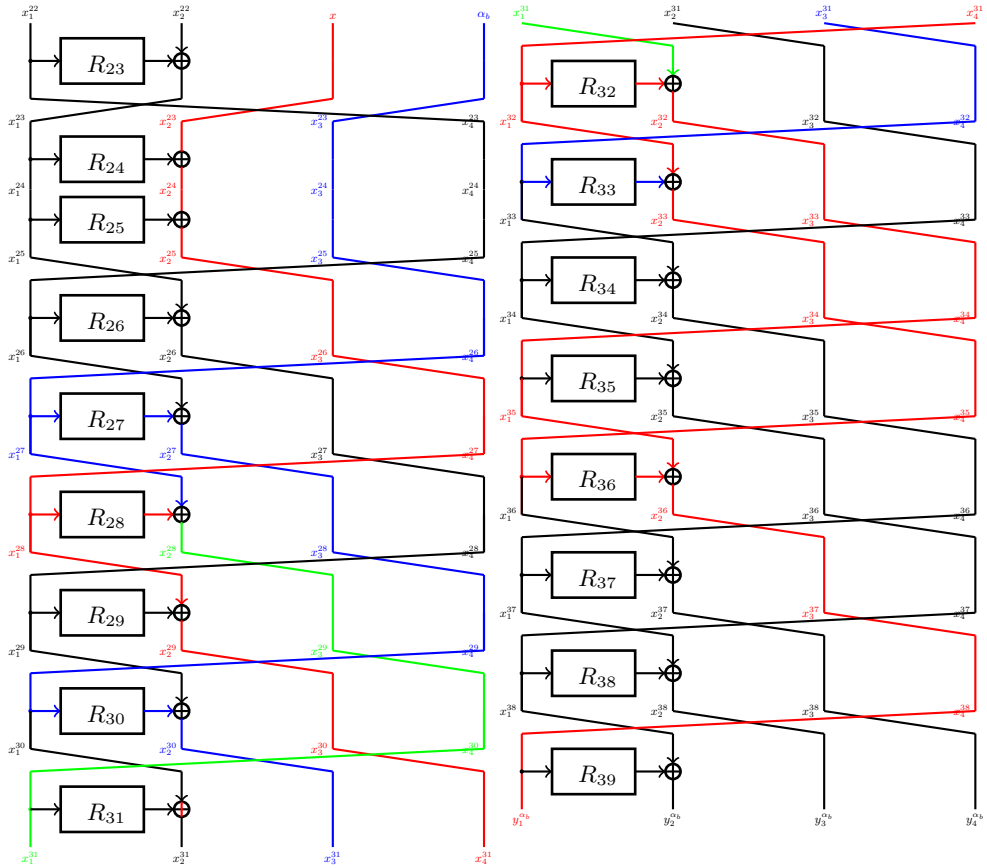

Fig. 5: 17-round distinguisher on CAST-256.

x_2^{25} is

$$x_2^{25} = x \oplus R_{24}(x_2^{22} \oplus R_{23}(x_1^{22})) \oplus R_{25}(x_2^{22} \oplus R_{23}(x_1^{22})).$$

See Fig.5 (red line). The function can be described as

$$x_2^{25} = x \oplus C_1,$$

where $C_1 = R_{24}(x_2^{22} \oplus R_{23}(x_1^{22})) \oplus R_{25}(x_2^{22} \oplus R_{23}(x_1^{22}))$ is a constant. After an additional 1 round, the value x_1^{22} is used as the input of R_{26} and the output of R_{26} is xored into $x_2^{22} \oplus R_{23}(x_1^{22})$. Then, we have

$$x_2^{26} = x_2^{22} \oplus R_{23}(x_1^{22}) \oplus R_{26}(x_1^{22}),$$

where x_1^{22}, x_2^{22} are constants. This implies that $x_2^{26} = C_2$ is a constant. Similarly, we have

$$x_2^{27} = x_1^{22} \oplus R_{27}(\alpha_b).$$

In the 10-th round, we have

$$\begin{aligned} x_2^{32} &= x_1^{31} \oplus R_{32}(x_4^{31}) \\ &= \alpha_b \oplus R_{28}(x_2^{25}) \oplus R_{32}(x_2^{25} \oplus R_{29}(x_2^{26})) \\ &= \alpha_b \oplus R_{28}(x \oplus C_1) \oplus R_{32}(x \oplus C_1 \oplus R_{29}(C_2)). \end{aligned}$$

The function $R(x) = R_{28}(x \oplus C_1) \oplus R_{32}(x \oplus C_1 \oplus R_{29}(C_2))$ is independent of the input x. Therefore, x_2^{32} is equal to

$$x_2^{32} = \alpha_b \oplus R(x).$$

In the 14-th round, we have

$$\begin{aligned} x_2^{36} &= x_1^{35} \oplus R_{36}(x_4^{35}) \\ &= x_2^{32} \oplus R_{36}(x_2^{25} \oplus R_{29}(x_2^{26}) \oplus R_{33}(x_2^{26} \oplus R_{30}(x_2^{27}))) \\ &= \alpha_b \oplus R(x) \oplus R_{36}(x \oplus C_1 \oplus R_{29}(C_2) \oplus R_{33}(C_2 \oplus R_{30}(x_1^{22} \oplus R_{27}(\alpha_b)))) \\ &= \alpha_b \oplus R(x) \oplus R_{36}(x \oplus C \oplus h(\alpha_b)), \end{aligned} \tag{4}$$

where $C = C_1 \oplus R_{29}(C_2)$, $h(\alpha_b) = R_{33}(C_2 \oplus R_{30}(x_1^{22} \oplus R_{27}(\alpha_b)))$ is independent of the input b, since x_1^{22}, x_2^{22} are constants.

In particular, from Eqs. (3) and (4), $f^O(x)$ satisfies $f^O(x) = f^O(x \oplus h(\alpha_0) \oplus h(\alpha_1))$. Moreover,

$$\begin{aligned} f^O(x \oplus h(\alpha_0) \oplus h(\alpha_1)) &= y_1^{\alpha_0} \oplus y_1^{\alpha_1} \oplus \alpha_0 \oplus \alpha_1 \\ &= x_2^{36}(\alpha_0) \oplus x_2^{36}(\alpha_1) \oplus \alpha_0 \oplus \alpha_1 \\ &= \alpha_0 \oplus R(x \oplus h(\alpha_0) \oplus h(\alpha_1)) \oplus R_{36}(x \oplus h(\alpha_0) \oplus h(\alpha_1) \oplus C \oplus h(\alpha_0)) \\ &\quad \oplus \alpha_1 \oplus R(x \oplus h(\alpha_0) \oplus h(\alpha_1)) \oplus R_{36}(x \oplus h(\alpha_0) \oplus h(\alpha_1) \oplus C \oplus h(\alpha_1)) \oplus \alpha_0 \oplus \alpha_1 \\ &= R_{36}(x \oplus C \oplus h(\alpha_1)) \oplus R_{36}(x \oplus C \oplus h(\alpha_0)) \\ &= f^O(x). \end{aligned}$$

Then, if $R_i(23 \leq i \leq 39)$ is a pseudo-random permutation family, $\varepsilon(f, s) \leq 1/2$ with overwhelming probability [20], and running Simon algorithm on the function f^O returns $h(\alpha_0) \oplus h(\alpha_1)$ with probability at least $1-(2(\frac{3}{4})^c)^n$. Therefore, $Adv^{PRP-qCPA}_{CAST-256}(A) = 1-(2(\frac{3}{4})^c)^n - \frac{1}{2^{n/2}}$. In particular, choosing $c \geq 6$ ensures that the probability is exponentially close to 1.

We now turn to the key-recovery attack.

Key Recovery Attack. With the 17-round distinguisher in the qCPA setting, we can recover the key of the $r(r > 17)$-round CAST-256 in time $O(2^{\frac{37(r-17)}{2}})$, where the key length of the internal round function is 37 bit. Compared with the previous 14-round distinguisher in Ni et al.'s attack [38], we can get more efficient key-recovery attacks, whose time complexities gain a factor $2^{\frac{37\times 3}{2}} = 2^{55.5}$.

Based on this, we can attack 23-round CAST-256 with 256-bit key in time 2^{111}, which is better than quantum brute force search by a factor of 2^{17}. In particular, for the 128-bit key version, we can attack 20 rounds in time $2^{55.5}$, while the best previous classical [42] or quantum attacks [37, 38] are no more than 17 rounds.

5 Conclusion

In this paper, we give some improved polynomial-time quantum distinguishers on Type-1 GFS (CAST256-like) in qCPA or qCCA settings. First, we present new qCCA quantum distinguishers on (d^2-1)-round Type-1 GFS with branches $d \geq 3$, which extends the previous results by $d-2$ rounds. Then, we could get more efficient key-recovery attacks, whose time complexities gain a factor of $2^{\frac{(d-2)k}{2}}$. Second, based on the special structure of CAST-256, we propose a 17-round quantum distinguisher in the qCPA setting. This leads to a more efficient analysis of CAST-256, that is, the complexity of some previous key-recovery attacks is reduced by a factor of $2^{55.5}$. As an interesting research direction, we leave our method for further investigation in the context of the tight bound of the number of rounds that we can distinguish, other block ciphers, combination with other attacks, and so on.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant Nos. 62272056, 61972048, 61976024).

References

1. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science. pp. 124-134. IEEE Computer Society (1994).
2. Liu H L, Wu Y S, Wan L C, et al. Variational quantum algorithm for the Poisson equation. Physical Review A, 104(2): 022418 (2021).
3. Wan L C, Yu C H, Pan S J, et al. Asymptotic quantum algorithm for the Toeplitz systems. Physical Review A, 97(6): 062322 (2018).
4. Wan L C, Yu C H, Pan S J, et al. Block-encoding-based quantum algorithm for linear systems with displacement structures. Physical Review A, 104(6): 062414 (2021).
5. I. Cong and L. Duan, Quantum discriminant analysis for dimensionality reduction and classification, New Journal of Physics, 18: 073011 (2016).
6. Pan S J, Wan L C, Liu H L, et al. Improved quantum algorithm for A-optimal projection. Physical Review A, 102(5): 052402 (2020).
7. Pan S J, Wan L C, Liu H L, et al. Quantum algorithm for Neighborhood Preserving Embedding. Chinese Physics B, 31(6): 060304 (2022).
8. M C. Guo, H L. Liu, Y M. Li, W M. Li, F. Gao, S J. Qin, Q Y. Wen, Quantum algorithms for anomaly detection using amplitude estimation, Physica A: Statistical Mechanics and its Applications 604: 127936 (2022).
9. Wang, H., Xue, Y., Qu, Y. et al. Multidimensional Bose quantum error correction based on neural network decoder. npj Quantum Inf 8, 134 (2022).
10. P. Rebentrost, M. Mohseni, and S. Lloyd, Quantum support vector machine for big data classification, Physical Review Letters, 113: 130503 (2014).
11. M. Schuld, I. Sinayskiy, and F. Petruccione. Quantum computing for pattern classification. in Pacific Rim International Conference on Artificial Intelligence (Springer, 2014), pp. 208-220.
12. Huang R, Tan X, Xu Q. Variational quantum tensor networks classifiers. Neurocomputing, 452: 89-98 (2021).
13. Li Y M, Liu H L, Pan S J, et al. Quantum k-medoids algorithm using parallel amplitude estimation. Physical Review A, 2023, 107(2): 022421.
14. Wang, H., Xue, Y., Qu, Y. et al. Multidimensional Bose quantum error correction based on neural network decoder. npj Quantum Inf 8, 134 (2022).
15. Yu C H, Gao F, Wang Q L, et al. Quantum algorithm for association rules mining. Physical Review A, 94(4): 042311 (2016).
16. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In: 2010 IEEE International Symposium on Information Theory Proceedings (ISIT), June 2010, pp. 2682-2685 (2010).
17. Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: ISITA. pp. 312-316. IEEE (2012).
18. Sun, HW., Wei, CY., Cai, BB. et al. Improved BV-based quantum attack on block ciphers. Quantum Inf Process 22, 9 (2023). https://doi.org/10.1007/s11128-022-03752-x
19. G. Leander, A. May. Grover Meets Simon - Quantumly Attacking the FX-construction, Advances in Cryptology - ASIACRYPT, pp. 161-178 (2017).
20. Kaplan M., Leurent G., Leverrier A., et al.: Breaking symmetric cryptosystems using quantum period finding. In: CRYPTO 2016, Part II, pp. 207-237 (2016).
21. Sun H W, Cai B B, Qin S J, et al. Quantum Attacks on Beyond-Birthday-Bound MACs. Cryptology ePrint Archive, Paper 2023/025, 2023. https://eprint.iacr.org/2023/025.

22. X. Bonnetain, G. Leurent,M. N.-Plasencia, A. Schrottenloher. Quantum linearization attacks. Advances in Cryptology - ASIACRYPT 2021, LNCS vol, 13090, pp. 422-452, (2021).
23. Guo, T., Wang, P., Hu, L., Ye, D.: Attacks on beyond-birthday-bound macs in the quantum setting. In: PQCrypto. Lecture Notes in Computer Science, vol. 12841, pp. 421-441. Springer (2021).
24. Li, Z., Cai, B., Sun, H. et al. Novel quantum circuit implementation of Advanced Encryption Standard with low costs. Sci. China Phys. Mech. Astron. 65, 290311 (2022).
25. Cai B B, Wu Y S, Dong J, Qin S J, Gao F and Wen Q Y. Quantum Attacks on 1K-AES and PRINCE. The Computer Journal, bxab216, doi: https://doi.org/10.1093/comjnl/bxab216.
26. Cai B B, Gao F and Leander G. Quantum attacks on two-round even-mansour. Front. Phys. 10:1028014. doi: 10.3389/fphy.2022.1028014.
27. Simon, D.R.: On the power of quantum computation. SIAM J. Comput. 26(5), 1474-1483 (1997).
28. Grover, L.K.: A Fast Quantum Mechanical Algorithm for Database Search. In: Miller, G.L. (ed.) Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996. pp. 212-219. ACM (1996).
29. Bernstein, E., Vazirani, U.V.: Quantum complexity theory. SIAM J. Comput. 26(5), 1411-1473 (1997).
30. National Soviet Bureau of Standards: Information Processing System-Cryptographic Protection-Cryptographic Algorithm GOST 28147-89 (1989).
31. International Organization for Standardization (ISO).: International Standard-ISO/IEC 18033-3, Information technology-Security techniques-Encryption algorithms-Part 3: Block ciphers (2010).
32. Zheng Y L, Matsumoto T, Imai H. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. In: Brassard G, eds. Advances in Cryptology - CRYPTO 1989. Lecture Notes in Computer Science, Vol 435. New York: Springer-Verlag, 461-480 (1989).
33. Carlisle Adams and Jeff Gilchrist. The CAST-256 Encryption Algorithm. RFC 2612, June (1999).
34. 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).
35. Ito G., Hosoyamada A., Matsumoto R., Sasaki Y., Iwata T.: Quantum chosen-ciphertext attacks against feistel ciphers. In: Matsui M (eds.) Topics in Cryptology-CT-RSA 2019-The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11405. Springer, pp. 391-411 (2019).
36. Canale, F., Leander, G., Stennes, L. (2022). Simon's Algorithm and Symmetric Crypto: Generalizations and Automatized Applications. In: Dodis, Y., Shrimpton, T. (eds) Advances in Cryptology - CRYPTO 2022. CRYPTO 2022. Lecture Notes in Computer Science, vol 13509. Springer, Cham.
37. Dong, X., Li, Z., Wang, X.: Quantum cryptanalysis on some generalized Feistel schemes. Sci. China Inf. Sci. 62(2), 022501 (2019).
38. Ni, B., Ito, G., Dong, X., Iwata, T.: Quantum attacks against type-1 generalized feistel ciphers and applications to CAST-256. In: Hao, F., Ruj, S., Gupta, S.S.

(eds.) Progress in Cryptology - INDOCRYPT 2019 - 20th International Conference on Cryptology in India, Hyderabad, India, December 15-18, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11898, pp. 433-455. Springer (2019).
39. S. Hodžić, L. Ramkilde, and A. Kidmose, "On quantum distinguishers for Type-3 generalized Feistel network based on separability," in Proceedings of International Conference on Post-Quantum Cryptography (PQCrypto 2020), Paris, France, pp.461-480, (2020).
40. Zhang Z, Wu W, Sui H, et al. Quantum Attacks on Type-3 Generalized Feistel Scheme and Unbalanced Feistel Scheme with Expanding Functions. Chinese Journal of Electronics, 32(2): 209-216 (2023).
41. Dong, X., Wang, X. Quantum key-recovery attack on Feistel structures. Sci. China Inf. Sci. 61, 102501 (2018).
42. 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).
43. 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).
44. 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).
45. Mao S, Guo T, Wang P, et al. Quantum Attacks on Lai-Massey Structure. Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event, September 28-30, 2022, Proceedings. Cham: Springer International Publishing, 205-229 (2022).
46. Nielsen, M.A., Chuang, I.: Quantum computation and quantum information. AAPT (2002).
47. Bonnetain, X.: Tight bounds for simon's algorithm. In: LATINCRYPT 2021. vol. 12912, pp. 3-23. Springer (2021).
48. 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.), Security and Cryptography for Networks-11th International Conference, SCN 2018. Lecture Notes in Computer Science, vol. 11035. Springer, Cham, pp. 386-403 (2018).