Quantum Distinguisher Between the 3-Round Feistel Cipher and the Random Permutation

Hidenori Kuwakado
Graduate School of Engineering
Kobe University
1-1 Rokkodai-cho Nada-ku Kobe 657-8501, Japan

Masakatu Morii
Graduate School of Engineering
Kobe University
1-1 Rokkodai-cho Nada-ku Kobe 657-8501, Japan

***Abstract*—No polynomial classical algorithms can distinguish between the 3-round Feistel cipher with internal permutations and a random permutation. It means that the 3-round Feistel cipher with internal permutations is secure against any chosen plaintext attack on the classical computer. This paper shows that there exists a polynomial quantum algorithm for distinguishing them. Hence, the 3-round Feistel cipher with internal permutations may be insecure against a chosen plaintext attack on a quantum computer. This distinguishing problem is an instance that can be efficiently solved by exploiting the quantum parallelism. The proposed algorithm is the first application of Simon's algorithm to cryptographic analysis.**

I. Introduction

Quantum algorithms are superior to classical algorithms in solving distinguishing problems such as the Deutsch-Jozza problem [2], the Bernstein-Vazirani problem [1], and the Simon problem [5]. The significance lies in the fact that they can be solved dramatically faster on a quantum computer. However, these distinguishing problems are somewhat artificial.

The concept of (in)distinguishability is important to prove the security of classical cryptographic schemes. The typical security proof is to prove that a cryptographic scheme is indistinguishable from an ideal scheme. The Feistel cipher, which is a structure of common-key block ciphers (e.g., DES, Twofish, Camellia, and DEAL), has been extensively studied in terms of the indistinguishability — Is the Feistel cipher distinguishable from a random permutation? Patarin [4] has summarized the results on this topic. Treger and Patarin [6] have analyzed the indistinguishability of the Feistel cipher with internal permutations recently. These results show that the exponential-number queries are required to distinguish between the Feistel cipher with 3 (or more) rounds and a random permutation. It means that the Feistel cipher with 3 (or more) rounds is secure against any chosen plaintext attack.

Previous analysis on the Feistel cipher is based on the classical algorithm. In this paper, we address the (in)distinguishability of the 3-round Feistel cipher with internal permutations from a random permutation using a quantum algorithm. Their distinguishability means that the 3-round Feistel cipher with internal permutations may be insecure against a chosen plaintext attack based on the quantum algorithm.

Precisely speaking, we discuss the (in)distinguishability of the unitary operator for computing the Feistel cipher from the unitary operator for computing the random permutation. Since the Feistel cipher is a classical cipher, one may think that the comparison of unitary operators is meaningless. However, if quantum computers are inexpensively realized in feature, then even classical ciphers will be implemented on quantum computers. In such a situation, an adversary will have access to the unitary operator instead of the classical oracle. Hence, it is significant to study the (in)distinguishability in the context of quantum algorithms.

We previously reported that there exist quantum algorithms that are more efficient than any classical algorithm for distinguishing between the 2(or 3)-round Feistel cipher and a random permutation [3]. However, the complexity of the previous algorithm for the 3-round Feistel cipher is exponential.

This paper shows that there exists a polynomial quantum algorithm for distinguishing between the 3-round Feistel cipher with internal permutations and a random permutation. It means that the 3-round Feistel cipher with internal permutations is potentially insecure against a chosen plaintext attack on the quantum computer. Notice that no polynomial classical algorithms can distinguish between the 3-round Feistel cipher with internal permutations and a random permutation.

This paper is organized as follows: Section II describes definitions and notations. Section III describes the proposed algorithm for distinguishing between the 3-round Feistel cipher with internal permutations and a random permutation. The success probability and the complexity of the algorithm are shown. Section IV concludes this paper.

II. Definition

Let $\mathcal{P}_m$ be a set of all permutations on $\{0,1\}^m$. A permutation is called a *random permutation* (RP) if it is chosen from $\mathcal{P}_m$ randomly. Figure 1 illustrates a *3-round Feistel cipher with internal permutations* (FP). In Fig. 1, internal permutations P_1, P_2, P_3 are independent random permutations on $\{0,1\}^n$. The 3-round Feistel cipher with internal permutations is a permutation on $\{0,1\}^{2n}$. Formally, for a given $x = a \parallel c$ where $a, c \in \{0,1\}^n$ and $\parallel$ is the concatenation operator on

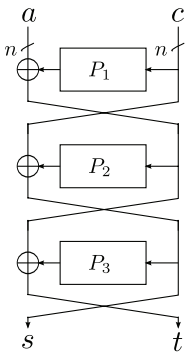

Fig. 1. The 3-round Feistel cipher with internal permutations, $\mathrm{FP}(a \parallel c) = s \parallel t$.

strings, the FP is defined as

$$\begin{aligned}\mathrm{FP}(x) &= \mathrm{FP}(a \parallel c) \\ &= c \oplus P_2(a \oplus P_1(c)) \\ &\quad \parallel (a \oplus P_1(c)) \oplus P_3(c \oplus P_2(a \oplus P_1(c))) \\ &= s \parallel t. \end{aligned} \quad (1)$$

Consider the following distinguishing problem.

> Let V be either the 3-round Feistel cipher with internal permutations (FP) or a random permutation (RP) on $\{0,1\}^{2n}$. Determine whether V is the FP or the RP by making queries to V. Notice that the query to the inverse mapping V^{-1} is not allowed.

Treger and Patarin [6] have shown that any classical algorithm requires $\Theta(2^{\frac{n}{2}})$ queries to determine it. Namely, FP is secure against any chosen plaintext attack that makes queries less than $\Theta(2^{\frac{n}{2}})$.

This paper addresses solving this problem with a quantum algorithm. The above problem is translated as follows:

> Let V be either the 3-round Feistel cipher with internal permutations (FP) or a random permutation (RP) on $\{0,1\}^{2n}$. Let U_V be a unitary operator for computing V, which is defined by
>
> $$\mathsf{U}_V|x\rangle|y\rangle = |x\rangle|y \oplus V(x)\rangle,$$
>
> where $x, y \in \{0,1\}^{2n}$. Determine whether V is the FP or the RP by making queries to U_V. The unitary operator for the inverse mapping V^{-1} is not given.

We previously showed that there was an exponential quantum algorithm for solving the problem with $\mathrm{O}\left(2^{\frac{n}{3}}\right)$ queries [3]. The next section will give a polynomial algorithm for solving the problem.

III. Proposed Algorithm

A. Idea

This section shows that the addressed problem can be solved in a similar manner as Simon's problem. We first define a function W as the first n bits of V. If V is the 3-round Feistel cipher with internal permutations (FP), then W is written as

$$\begin{aligned} W(x) &= W(a \parallel c) \\ &= c \oplus P_2(a \oplus P_1(c)) \end{aligned} \quad (2)$$

by using notation of Eq. (1). Let α, β be distinct fixed strings in $\{0,1\}^n$. Consider the following function f from $\{0,1\}^{n+1}$ to $\{0,1\}^n$.

$$f(b \parallel a) = \begin{cases} W(a \parallel \alpha) \oplus \beta & \text{if } b = 0 \\ W(a \parallel \beta) \oplus \alpha & \text{if } b = 1, \end{cases}$$

where $b \in \{0,1\}$ and $a \in \{0,1\}^n$. The behavior of f depends on W (i.e., V). To determine whether V is the FP or the RP, we focus on the behavior of f. When V is the FP, f has a remarkable property as follows:

$$\begin{aligned} &f(b \parallel a) = f(b' \parallel a') \\ &\quad \text{if and only if } \ b' = b \oplus 1 \ \wedge \ a' = a \oplus z, \end{aligned}$$

where $z = P_1(\alpha) \oplus P_1(\beta)$. In other words, for a given $b \parallel a \in \{0,1\}^{n+1}$, a value t satisfying

$$f(b \parallel a) = f(t)$$

is only $(b \parallel a) \oplus (1 \parallel z)$. The proof is given in Appendix. On the other hand, when V is the RP, there is no such a relation.

The above remarkable property is essentially equivalent to the condition on Simon's problem. Furthermore, the unitary operator U_f for computing f can be constructed with one invocation of the unitary operator U_V for computing V.

$$\mathsf{U}_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle,$$

where $x \in \{0,1\}^{n+1}$ and $y \in \{0,1\}^n$. Hence, the addressed problem is closely related to Simon's problem.

B. Algorithm and Analysis

The quantum algorithm for solving the addressed problem is described below. This algorithm is very similar to Simon's algorithm. The proposed algorithm is the first instance in which Simon's algorithm is used for cryptographic analysis.

1) Initialize a set $\mathcal{V}$ as the empty set.
2) Prepare a state $|\phi_1\rangle$

$$|\phi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^{n+1}} |x\rangle|f(x)\rangle$$

by using the unitary operator U_f.
3) Measure the second register $|f(x)\rangle$. The measurement is denoted by y. The resulting state is written as

$$|\phi_2\rangle = \frac{1}{\sqrt{\lambda}} \sum_{x \in \mathcal{X}_y} |x\rangle, \quad (3)$$

where $\mathcal{X}_y$ is a set of x's satisfying $y = f(x)$ and λ is the number of elements in $\mathcal{X}_y$. Since the second register will be fixed from now on, we will no longer write it down explicitly.

4) Apply the Hadamard transformation H_{n+1} to $|\phi_2\rangle$.

$$\begin{aligned} |\phi_3\rangle &= H_{n+1}|\phi_2\rangle \\ &= \frac{1}{\sqrt{\lambda 2^{n+1}}} \sum_{v\in\{0,1\}^{n+1}} (-1)^{x\cdot v}|v\rangle, \end{aligned} \quad (4)$$

where '$\cdot$' indicates the inner product of two $(n+1)$-bit binary vectors.

5) Measure the register $|v\rangle$. The measurement v is appended to the set $\mathcal{V}$.

6) If $\mathcal{V}$ does not contain n lineally independent v's, then go back to step 2. Otherwise, find an n-bit string $z = (z_0, z_1, \ldots, z_{n-1})$ by solving the following equations.

$$\begin{pmatrix} v_1^{(0)} & v_2^{(0)} & \ldots & v_n^{(0)} \\ v_1^{(1)} & v_2^{(1)} & \ldots & v_n^{(1)} \\ & \cdots & & \\ v_1^{(n-1)} & v_2^{(n-1)} & \ldots & v_n^{(n-1)} \end{pmatrix} \begin{pmatrix} z_0 \\ z_1 \\ \vdots \\ z_{n-1} \end{pmatrix} = \begin{pmatrix} v_0^{(0)} \\ v_0^{(1)} \\ \vdots \\ v_0^{(n-1)} \end{pmatrix} \pmod 2, \quad (5)$$

where $v_j^{(i)} \in \{0,1\}$ and $(v_0^{(i)}, v_1^{(i)}, \ldots, v_n^{(i)})$ is an element in $\mathcal{V}$.

7) Choose an $(n+1)$-bit string u at random. Let

$$u' = u \oplus (1 \parallel z).$$

Compute $f(u)$ and $f(u')$ classically. If they are equal, then V is guessed to be the FP. Otherwise V is guessed to be the RP.

We justify the output of the above algorithm. Suppose that V is the FP. Then, Eq. (3) is written by

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle + |x \oplus (1 \parallel z)\rangle\right)$$

because of the property of f described in Sect. III-A. Equation (4) is given by

$$\begin{aligned} |\phi_3\rangle &= \frac{1}{\sqrt{2^{n+2}}} \sum_{v\in\{0,1\}^{n+1}} \left((-1)^{x\cdot v} + (-1)^{(x\oplus(1\|z))\cdot v}\right)|v\rangle \\ &= \frac{1}{\sqrt{2^{n+2}}} \sum_{v\in\{0,1\}^{n+1}} (-1)^{x\cdot v}\left(1 + (-1)^{(1\|z)\cdot v}\right)|v\rangle \end{aligned}$$

The above equation implies that the measurement v in step 5 satisfies

$$(1 \parallel z)\cdot v = 0 \pmod 2,$$

which is one of equations in Eq. (5). Since $f(u)$ is always equal to $f(u')$ in step 7, the output of this algorithm is correct.

On the other hand, suppose that V is the RP. The string z obtained by solving Eq. (5) is random if exists. Hence, the probability that $f(u) = f(u\oplus(1 \parallel z))$ is $(2^n-1)/(2^{2n}-1) \approx 2^{-n}$.

The number of iterations from step 2 to step 5 is expected to be $\mathrm{O}(n)$. This estimation on iteration is obtained in a manner similar to Simon's analysis.

Theorem 1: There is a quantum algorithm for distinguishing the 3-round Feistel cipher with internal permutations from a random permutation on $\{0,1\}^{2n}$. The complexity of the algorithm is $\mathrm{O}(n)$ and the error probability is approximately equal to 2^{-n}.

IV. Concluding Remarks

Any classical algorithm requires $\Theta(2^{\frac{n}{2}})$ queries for distinguishing between the 3-round Feistel cipher with internal permutations and a random permutation. This result means that the 3-round Feistel cipher with internal permutations is secure against any chosen plaintext attack on a classical computer. This paper has shown that there exists a quantum algorithm for distinguishing them with $\mathrm{O}(n)$ queries. It means that the 3-round Feistel cipher with internal permutations may be insecure against a chosen plaintext attack on a quantum computer. This quantum algorithm is the first instance in which Simon's algorithm is applied to cryptographic analysis.

Acknowledgments

The authors would like to thank anonymous reviewers for their valuable comments. Especially, one of anonymous reviewers has substantially improved the algorithm that was described at the initial submission. The algorithm described in this paper follows the improvement done by the anonymous reviewer.

References

[1] E. Bernstein and U. Vazirani, "Quantum complexity theory," SIAM Journal of Computing, vol. 26, no. 5, pp. 1411–1473, 1997.

[2] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," Proceedings of Royal Society of London A, vol. 439, pp. 553–558, 1992.

[3] H. Kuwakado and M. Morii, "Quantum analysis of 2,3-round Feistel schemes," Proceedings of the 9th Asian Conference on Quantum Information Science, pp. 39–40, 2009.

[4] J. Patarin, "Generic attacks on Feistel schemes," Cryptology ePrint Archive, Report 2008/036, 2008. http://eprint.iacr.org/.

[5] D. R. Simon, "On the power of quantum computing," SIAM Journal of Computing, vol. 26, no. 5, pp. 1474–1483, October 1997.

[6] J. Treger and J. Patarin, "Generic attacks on Feistel networks with internal permutations," Progress in Cryptology – AFRICACRYPT 2009, Lecture Notes in Computer Science, vol. 5580, pp. 41–59, 2009.

Appendix

Supposing that V is the FP, we prove the following lemma.

Lemma 1: For any distinct strings $b \parallel a, b' \parallel a'$ in $\{0,1\}^{n+1}$,

$$\begin{aligned} &f(b \parallel a) = f(b' \parallel a') \\ &\quad\Leftrightarrow\quad b' = b \oplus 1 \ \wedge\ a' = a \oplus z, \end{aligned}$$

where $z = P_1(\alpha) \oplus P_1(\beta)$.

($\Rightarrow$) Suppose that $b = b' = 0$. Then, using Eq. (2), we have

$$\begin{aligned} f(0 \parallel a) &= W(a \parallel \alpha) \oplus \beta \\ &= \alpha \oplus P_2(a \oplus P_1(\alpha)) \oplus \beta, \\ f(0 \parallel a') &= W(a' \parallel \alpha) \oplus \beta \\ &= \alpha \oplus P_2(a' \oplus P_1(\alpha)) \oplus \beta. \end{aligned}$$

Since $f(0 \parallel a) = f(0 \parallel a')$ and P_2 is permutation we obtain $a = a'$. It follows that $b' \parallel a' = b \parallel a$, which is a trivial case.

Next, suppose that $b = 0, b' = 1$. Then, we have

$$\begin{aligned} f(1 \parallel a') &= W(a' \parallel \beta) \oplus \alpha \\ &= \beta \oplus P_2(a' \oplus P_1(\beta)) \oplus \alpha. \end{aligned}$$

Since $f(0 \parallel a) = f(1 \parallel a')$ and P_2 is permutation, we obtain

$$\begin{aligned} a' &= P_1(\beta) \oplus a \oplus P_1(\alpha) \\ &= a \oplus z. \end{aligned}$$

We can prove other cases in a simiar manner.

($\Leftarrow$) This is proved with direct calculation. Suppose that $b = 0$. Then, we have

$$\begin{aligned} f(0 \parallel a) &= \alpha \oplus P_2(a \oplus P_1(\alpha)) \oplus \beta, \\ f(1 \parallel a') &= f(1 \parallel (a \oplus z)) \\ &= \beta \oplus P_2((a \oplus z) \oplus P_1(\beta)) \oplus \alpha \\ &= \beta \oplus P_2(a \oplus P_1(\alpha)) \oplus \alpha. \end{aligned}$$

Hence, $f(0 \parallel a) = f(1 \parallel a')$. We can prove the case of $b = 1$ in a simiar manner.