A Characterization of Quantum One-Way Permutations

Akinori Kawachi[1, 2, *] Hirotada Kobayashi[3, †] Takeshi Koshiba[1, 4, ‡] Raymond H. Putra[1, 2, §]

[1] *ERATO Quantum Computation and Information Project, JST.*
Matsuo-Bldg 2F, 406 Iseya-cho, Kawaramachi-Marutamachi, Kamigyo-ku, Kyoto 602-0873, Japan.
[2] *Graduate School of Informatics, Kyoto University.*
Yoshida-Honmachi, Sakyo-ku, Kyoto 606-8501, Japan.
[3] *ERATO Quantum Computation and Information Project, JST.*
Hongo White Building, 5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan.
[4] *Secure Computing Lab., Fujitsu Laboratories Ltd.*
4-1-1 Kamikodanaka, Nakahara-ku, Kawasaki 211-8588, Japan.

Abstract. We affirmatively settle the conjecture given by Kashefi, Nishimura and Vedral and complete a characterization of average-case quantum one-way permutations in terms of reflection operator and pseudo identity. We incorporate their basic idea with the universal hashing technique and modify the reduction between inverting quantum one-way permutation and the other problem appeared in the characterization of worst-case quantum one-way permutations given by them.

Keywords: quantum one-way permutation, reflection operator, universal hash function

1 Introduction

The class of one-way permutations is a restricted class of one-way functions and the existence of one-way permutations has been still open. Towards the settlement of the open problem, some characterizations have been introduced. In the classical case, Hemaspaandra and Rothe [4] gave a necessary and sufficient condition for the existence of (worst-case) one-way permutation. In the quantum case, Kashefi, Nishimura and Vedral [5] gave a necessary and sufficient condition for the existence of (worst-case) quantum one-way permutation. They also considered the average-case quantum one-way permutations and gave a partial result on characterizing the average-case quantum one-way permutations and some conjecture on the full characterization. Their characterization is based on the efficient implementability of reflections about some class of quantum states. In this paper, we affirmatively settle the conjecture and complete a characterization of average-case quantum one-way permutations. We incorporate the basic idea in [5] with the universal hashing technique [2, 6] and modify the reduction between inverting quantum one-way permutation and the other problem appeared in the characterization.

2 Preliminaries

We say that a unitary operator (on n qubits) is *easy* if there exists a quantum circuit implementing U with polynomial size in n and a set $\mathcal{F}$ of unitary operators is *easy* if every $U \in \mathcal{F}$ is easy. Throughout this paper, we assume that $f : \{0,1\}^* \to \{0,1\}^*$ is a quantum one-way permutation. First, we mention some useful operators in describing the previous and our results. The tagging operators $O[k]$ are defined as follows:

$$O[k]|x\rangle|y\rangle = \begin{cases} -|x\rangle|y\rangle & \text{if } f(y)_{(k,k+1)} = x_{(k,k+1)} \\ |x\rangle|y\rangle & \text{if } f(y)_{(k,k+1)} \neq x_{(k,k+1)} \end{cases}$$

where $y_{(i,j)}$ denotes the substring from the i-th bit to the j-th bit of the bit string y. Note that the unitary operators $O[k]$ are easy. Next, we consider the reflection operators Q_j as follows:

$$Q_j = \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes (2|\psi_{j,x}\rangle\langle\psi_{j,x}| - I),$$

$$\text{where} \qquad |\psi_{j,x}\rangle = \frac{1}{\sqrt{2^{n-2j}}} \sum_{y:\, f(y)_{(1,2j)}=x_{(1,2j)}} |y\rangle.$$

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a permutation. Kashefi, Nishimura and Vedral [5] showed that f is (worst-case) quantum one-way if and only if the set $\mathcal{F}_n = \{Q_j(f)\}_{j=0,1,\ldots,\frac{n}{2}-1}$ of unitary operators is not easy. As a part of the proof of the characterization of the worst-case one-way permutations, they give a quantum algorithm (we call Algorithm INV in what follows) computing f^{-1} by using unitary operators $O[k]$ and Q_j. The initial input state to INV is assumed to be $\frac{1}{\sqrt{2^n}}|x\rangle \sum_{y\in\{0,1\}^n} |y\rangle$, where INV trys to compute $f^{-1}(x)$. Then INV performs the following steps:

```
foreach $j = 0$ to $\frac{n}{2} - 1$
    (step $j$.1) Apply $O[2j+1]$ to the 1st and the 2nd registers;
    (step $j$.2) Apply $Q_j$ to the 1st and the 2nd registers.
```

After each step, we have the following:

$$\begin{pmatrix}\text{the state} \\ \text{after step } j.1\end{pmatrix} = \frac{2^j}{\sqrt{2^n}}|x\rangle \left(\sqrt{2^{n-2j}}|\psi_{j,x}\rangle - 2\sum_{y:\, f(y)_{(1,2j+2)}=x_{(1,2j+2)}} |y\rangle\right);$$

$$\begin{pmatrix}\text{the state} \\ \text{after step } j.2\end{pmatrix} = \frac{2^{j+1}}{\sqrt{2^n}}|x\rangle \sum_{y:\, f(y)_{(1,2j+2)}=x_{(1,2j+2)}} |y\rangle.$$

To characterize average-case quantum one-way permutations, the following notion is quite useful.

Definition 1 Let $d(n) \geq n$ be a polynomial in n and J_n be a $d(n)$-qubit unitary operator. J_n is called $(a(n), b(n))$-pseudo identity if there exists a set $X_n \subseteq \{0,1\}^n$ such that $|X_n|/2^n \leq b(n)$ and for any $z \in \{0,1\}^n \setminus X_n$

$$|1 - (\langle z|_1\langle 0|_2)J_n(|z\rangle_1|0\rangle_2)| \leq a(n),$$

where $|z\rangle_1$ is the n-qubit basis state for each z and $|0\rangle_2$ corresponds to the ancillae of $d(n) - n$ qubits.

[*] kawachi@kuis.kyoto-u.ac.jp

[†] hirotada@qci.jst.go.jp

[‡] koshiba@qci.jst.go.jp

[§] raymond@kuis.kyoto-u.ac.jp

Kashefi, Nishimura and Vedral [5] also gave a partial characterization of average-case quantum one-way permutations using the notion of pseudo identity and stated a conjecture with respect to a complete characterization of average-case quantum one-way permutations. In this paper, we affirmatively settle their conjecture and complete a characterization of average-case quantum one-way permutations in terms of reflection operator and pseudo identity.

3 Universal Hashing Operator

Before showing our results, we prepare a technical tool, which may be useful by itself. In general, random permutations can be a useful tool to analysis of randomized algorithm. In the case of quantum computation, the efficient and faithful implementation of random permutations seems to be hard to realize. Instead, we introduce the universal hashing technique [2, 6] to quantum computing and settle the conjecture by using the efficient implementability of the universal hash functions and the similar property to random permutations.

Let $r_1, r_2 \in \mathrm{GF}(2^n)$ and h_{r_1,r_2} be a function from $\mathrm{GF}(2^n)$ to $\mathrm{GF}(2^n)$ such that $h_{r_1,r_2}(x) = r_1 x + r_2$. Let $\mathcal{R} = \{h_{r_1,r_2} : r_1, r_2 \in \mathrm{GF}(2^n) \text{ with } r_1 \neq 0\}$. Since it is easy to identify $\mathrm{GF}(2^n)$ with $\{0,1\}^n$ by considering the standard conversion, we regard $\mathcal{R}$ as the family of functions from $\{0,1\}^n$ to $\{0,1\}^n$. Note that any function in $\mathcal{R}$ is a permutation but it is generally called a "hash" function because of the historical and conventional reason. Then, $\mathcal{R}$ is *strongly 2-univeral*, namely, for any $x_1 \neq x_2 \in \{0,1\}^n$ and $y_1 \neq y_2 \in \{0,1\}^n$ and h chosen uniformly at random from $\mathcal{R}$, $\Pr[h(x_1) = y_1 \text{ and } h(x_2) = y_2] = 1/(2^n)^2$. We call it *hashing* operator and denote it by R. We note that, instead of using the hashing operator R, we can choose polynomially many pairs of (r_1, r_2) beforehand and consider (r_1, r_2) being fixed during quantum computation. Namely, we can consider that the whole computation is performed by choosing a quantum circuit randomly and then feeding a given input to the quantum circuit. For the simplicity, while we take this manner, we still describe the hashing computation just like the unitary operator. (Also note that the whole process can be done by unitary operators.)

4 Characterization

Theorem 2 *There exists a weakly quantum one-way permutation if and only if there exists a polynomial-time computable function f satisfying that there exists a polynomial p such that for infinitely many n and any $(1/2^{p(n)}, 1/p(n))$-pseudo identity operators $J_{p(n)}$, the following family is not easy: $\mathcal{F}_{n,p}(f) = \{(I_n \otimes (R^\dagger J_{p(n)} R)^\dagger)(Q_j(f) \otimes I_{r_p(n)-n})(I_n \otimes (R^\dagger J_{p(n)} R))\}_{j=0,1,\ldots,\frac{n}{2}-1}$.*

Since the *if*-part can be proved by using a similar argument to the one in [5], we omit the proof. Thus, we give a proof sketch of the *only-if*-part. Suppose that for some fixed polynomial, infinitely many n, and some $(1/2^{p(n)}, 1/p(n))$-pseudo identity operators $J_{p(n)}$, the family $\mathcal{F}_{p,n}$ of unitary operators is easy. We construct a polynomial-size algorithm av-INV to invert f by using unitary operations in $\mathcal{F}_{p,n}$. Algorithm av-INV is almost similar to Algorithm INV except the following change: the operator Q_j is now replaced with $\tilde{Q}_j$.

From the definition of pseudo identity operators, there exists a set $X_n \subseteq \{0,1\}$ with $|X_n| \leq 2^n/p(n)$ such that for any $y \in Y_n = \{0,1\}^n \setminus X_n$, $J_{p(n)}|y\rangle_2|0\rangle_3 = \alpha_y|y\rangle_2|0\rangle_3 + |\psi_y\rangle_{23}$, where $|\psi_y\rangle_{23} \perp |y\rangle_2|0\rangle_3$ and $|1 - \alpha_y| \leq \frac{1}{2^{p(n)}}$.

In Algorithm av-INV, we apply $J_{p(n)}$ before and after step j.2 for each j. Note that the application of R before and after $J_{p(n)}$ does not affect the expected performance of $J_{p(n)}$. The application of $J_{p(n)}$ makes an error in computation of f^{-1}. We call the vector $J_{p(n)}|\psi\rangle - |\psi\rangle$ the *error* associated to $|\psi\rangle$. To measure the effect of this error, we use the following lemmas. Due to the space limitation, we omit proofs. (Lemma 4 was stated in [5].)

Lemma 3 *Assume that $T \subseteq S \subseteq \{0,1\}^n$. Then length $l(S,T)$ of the error associated to the state*

$$|\psi(S,T)\rangle = \frac{1}{\sqrt{|S|}}\left(\sum_{y \in S \setminus T} |y\rangle|0\rangle - \sum_{y \in T} |y\rangle|0\rangle\right)$$

satisfies that $l(S,T) \leq 2\sqrt{|S \cap X_n|/|S|} + \gamma(n)$, where $\gamma(n)$ is a negligible function in n.

Lemma 4 *Let $J_{p(n)}|\psi(S,T)\rangle = \alpha|\psi(S,T)\rangle + |\psi(S,T)^\perp\rangle$, where $|\psi(S,T)\rangle \perp |\psi(S,T)^\perp\rangle$. Then, $\||\psi(S,T)^\perp\rangle| \leq l(S,T)$.*

For analysis of Algorithm av-INV, we use Lemma 3 and Lemma 4. For each j, we let $S_j = \{y : f(y)_{(1,2j)} = x_{(1,2j)}\}$ and $S_j = \{y : f(y)_{(1,2j+2)} = x_{(1,2j+2)}\}$. Then, we have the following.

Lemma 5 *For each j, $\mathbf{E}[l(S_j, T_j)] \leq 2/\sqrt{p(n)}$, where the expectation is over the random selection of parameters of hashing operators.*

Using Lemma 5, we can show that the length of the accumulated error is at most $2 \cdot (n/2) \cdot (2/\sqrt{p(n)})$ after the termination of Algorithm av-INV. Thus, the length is bounded by $1/q(n)$ for some polynomial q. Therefore, there exists a polynomial-size quantum circuit A and infinitely many n such that $\frac{1}{2^n}\sum_{x \in \{0,1\}^n} \Pr[A(x) = f^{-1}(x)] > 1 - 1/(q(n))^2$. This implies that f is not weakly quantum one-way. □

References

[1] M. Adcock and R. Cleve, "A quantum Goldreich-Levin theorem with cryptographic applications", In *Proc. 19th STACS*, Lecture Notes in Computer Science 2285, Springer, pp.323–334, 2002.

[2] J. L. Carter and M. N. Wegman, "Universal classes of hash functions", J. Computer and System Sciences 18(2), pp.143–154, 1979.

[3] P. Dumais, D. Mayers and L. Salvail, "Perfectly concealing quantum bit commitment from any one-way permutations", In *Proc. EUROCRYPT 2000*, Lecture Notes in Computer Science 1807, Springer, pp.300–315, 2000.

[4] L. Hemaspaandra and J. Rothe, "Characterizing the existence of one-way permutations", Theoretical Computer Science 244(1–2), pp.257–261, 2000.

[5] E. Kashefi, H. Nishimura and V. Vedral, "On quantum one-way permutations", Quantum Information and Computation 2(5), pp. 379–398, 2002.

[6] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality", J. Computer and System Sciences 22(3), pp.265–279, 1981.