Available online at www.sciencedirect.com

SCIENCE DIRECT®

Theoretical Computer Science 345 (2005) 370–385

Theoretical Computer Science

www.elsevier.com/locate/tcs

# Universal test for quantum one-way permutations☆

Akinori Kawachi[a], Hirotada Kobayashi[b], Takeshi Koshiba[c,*], Raymond H. Putra[d,e]

[a] *Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan*

[b] *Quantum Computation and Information Project, Exploratory Research for Advanced Technology, Japan Science and Technology Agency, 5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan*

[c] *Secure Computing Laboratory, Fujitsu Laboratories Ltd., 4-1-1 Kamikodanaka, Nakahara-ku, Kawasaki 211-8588, Japan*

[d] *Quantum Computation and Information Project, Exploratory Research for Advanced Technology, Japan Science and Technology Agency, Matsuo Bldg. 2F, 406 Iseyacho, Kawaramachi Marutamachi, Kamigyo-ku, Kyoto 602-0873, Japan*

[e] *Graduate School of Informatics, Kyoto University, Yoshida-Honmachi, Sakyo-ku, Kyoto 606-8501, Japan*

## Abstract

The next bit test was introduced by Blum and Micali and proved by Yao to be a universal test for cryptographic pseudorandom generators. On the other hand, no universal test for the cryptographic one-wayness of functions (or permutations) is known, although the existence of cryptographic pseudorandom generators is equivalent to that of cryptographic one-way functions. In the quantum computation model, Kashefi, Nishimura and Vedral gave a sufficient condition of (cryptographic) quantum one-way permutations and conjectured that the condition would be necessary. In this paper, we affirmatively settle their conjecture and complete a necessary and sufficient condition for quantum one-way permutations. The necessary and sufficient condition can be regarded as a universal test

☆A preliminary version [12] of this paper appeared in the Proceedings of the 29th International Symposium on Mathematical Foundations of Computer Science (MFCS).

* Corresponding author. Tel.: +81 44 754 2681; fax: +81 44 754 2666.

*E-mail addresses:* kawachi@is.titech.ac.jp (A. Kawachi), hirotada@qci.jst.go.jp (H. Kobayashi), koshiba@acm.org (T. Koshiba), raymond@kuis.kyoto-u.ac.jp (R.H. Putra).

0304-3975/$ - see front matter © 2005 Published by Elsevier B.V.
doi:10.1016/j.tcs.2005.07.036

for quantum one-way permutations, since the condition is described as a collection of stepwise tests similar to the next bit test for pseudorandom generators.

*Keywords:* Quantum computation; Computational cryptography; One-way permutation; One-way function; Universal test

## 1. Introduction

One-way functions are functions $f$ such that, for each $x$, $f(x)$ is efficiently computable but $f^{-1}(y)$ is computationally tractable only for a negligible fraction of all $y$'s. While the modern cryptography depends heavily on one-way functions, the existence of one-way functions is one of the most important open problems in theoretical computer science. On the other hand, Shor [14] showed that famous candidates of one-way functions such as the RSA function or the discrete logarithm function are no longer one-way in the quantum computation model. Nonetheless, some cryptographic applications based on quantum one-way functions have been considered (see, e.g., [1,5]).

As a cryptographic primitive other than one-way functions, pseudorandom generators have been studied well. Blum and Micali [3] proposed how to construct pseudorandom generators from one-way permutations and introduced the next bit test for pseudorandom generators. (They actually constructed a pseudorandom generator assuming the hardness of the discrete logarithm problem.) Since Yao [15] proved that the next bit test is a universal test for pseudorandom generators, the Blum–Micali construction paradigm of pseudorandom generators from one-way permutations was proved to work properly. In the case of pseudorandom generators based on one-way permutations, the next bit unpredictability can be proved by using hard-core predicates for one-way permutations. After that, Goldreich and Levin [8] showed that there exists a hard-core predicate for any one-way function (and also permutation) and Håstad et al. [10] showed that the existence of pseudorandom generators is equivalent to that of one-way functions.

Yao's result on the universality of the next bit test assumes that all bits appearing among the pseudorandom bits are computationally unbiased. Schrift and Shamir [13] extended Yao's result to the biased case and proposed universal tests for non-uniform distributions. On the other hand, no universal test for the one-wayness of a function (or a permutation) is known, although pseudorandom generators and one-way functions (or permutations) are closely related.

In the quantum computation model, Kashefi et al. [11] gave a necessary and sufficient condition for the existence of *worst-case* quantum one-way permutations. They also considered the *cryptographic* (i.e., *average-case*) quantum one-way permutations and gave a sufficient condition of (cryptographic) quantum one-way permutations, and posed a conjecture that the condition would be necessary. Their conditions are based on the efficient implementability of reflection operators about some class of quantum states. Note that the reflection operators are successfully used in the Grover algorithm [9] and the quantum amplitude amplification technique [4]. To obtain a sufficient condition of cryptographic quantum one-way permutations, a notion of "pseudo identity" operators was introduced

[11]. Since the worst-case hardness of reflection operators is concerned with the worst-case hardness of the inversion of the permutation *f*, we need some technical tool with which the inversion process of $f$ becomes tolerant of some computational errors in order to obtain a sufficient condition of cryptographic quantum one-way permutations. Actually, pseudo identity operators permit *exponentially* small errors during the inversion process [11].

In this paper, we complete a necessary and sufficient condition of cryptographic quantum one-way permutations conjectured in [11]. We incorporate their basic ideas with a probabilistic argument in order to obtain a technical tool to permit *polynomially* small errors during the inversion process. Roughly speaking, pseudo identity operators are close to the identity operator in a sense. The similarity is defined by an intermediate notion between the statistical distance and the computational distance. In [11], it is "by upper-bounding the similarity" that the sufficient condition of cryptographic quantum one-way permutations was obtained. By using a probabilistic argument, we can estimate the expectation of the similarity and then handle polynomially small errors during the inversion of the permutation *f*.

Moreover, the necessary and sufficient condition of quantum one-way permutations can be regarded as a universal test for the quantum one-wayness of permutations. To discuss universal tests for the one-wayness of permutations, we briefly review the universality of the next bit test for pseudorandom generators. Let $g(x)$ be a length-regular deterministic function such that $g(x)$ is of length $\ell(n)$ for any $x$ of length *n*. The universality of the next bit test says that we have only to check a collection of stepwise polynomial-time tests $T_1, \ldots, T_{\ell(n)}$ instead of considering all the polynomial-time tests that try to distinguish the truly random bits from output bits from *g*, where each $T_i$ is the test whether, given the $(i-1)$-bit prefix of $g(x)$ (and the value of $\ell(|x|)$), the *i*th bit of $g(x)$ is predictable or not with probability non-negligibly higher than $\frac{1}{2}$. Our necessary and sufficient condition of quantum one-way permutations says that the quantum one-wayness of a given permutation *f* can be checked by a collection of stepwise tests $T'_1, \ldots, T'_n$ instead of considering all the tests of polynomial-size quantum circuit, where each $T'_i$ is the test whether, given some quantum state $q_{i-1}$ that can be defined by using the $(i-1)$-bit prefix of $f(x)$, some other quantity $t_i$ is computable with polynomial-size quantum circuit or not and the next state $q_i$ can be determined from $q_{i-1}$ and $t_i$. In this sense, our universal test for quantum one-way permutations is analogous to the universal test (i.e., the next bit test) for pseudorandom generators.

## 2. Preliminaries

Since our study is an extension of the results by Kashefi et al. [11], we use the same notions, definitions and notations. In this section, we describe them and review the results in [11].

### 2.1. Notations and basic operators

We say that a unitary operator $U$ (on $n$ qubits) is *easy* if there exists a quantum circuit implementing $U$ of size polynomial in *n*. Similarly, a set $\mathcal{F}$ of unitary operators is *easy* if

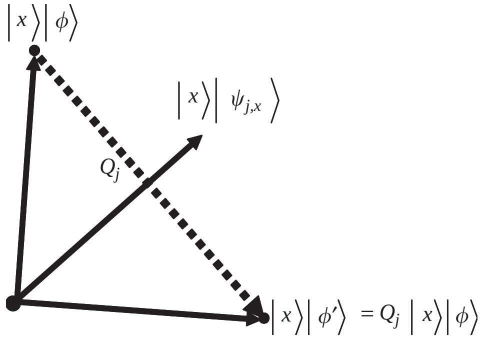
$|x\rangle|\phi\rangle$
$|x\rangle|\psi_{j,x}\rangle$
$Q_j$
$|x\rangle|\phi'\rangle = Q_j|x\rangle|\phi\rangle$

Fig. 1. Reflection operator.

every $U \in \mathcal{F}$ is easy. Throughout this paper, we assume that $f : \{0,1\}^* \to \{0,1\}^*$ is a length-preserving permutation unless otherwise stated. Namely, for any $x \in \{0,1\}^n$, $f(x)$ is an $n$-bit string and the set $\{f(x) : x \in \{0,1\}^n\}$ is of cardinality $2^n$ for every $n$. First, we mention some useful operators for describing the previous and our results. The *tagging* operators $O_j$ are defined as follows:

$$O_j|x\rangle|y\rangle = \begin{cases} -|x\rangle|y\rangle & \text{if } f(y)_{(2j+1,2j+2)} = x_{(2j+1,2j+2)}, \\ |x\rangle|y\rangle & \text{if } f(y)_{(2j+1,2j+2)} \neq x_{(2j+1,2j+2)}, \end{cases}$$

where $y_{(i,j)}$ denotes the substring from the $i$th bit to the $j$th bit of the bit string $y$ if $i \leqslant j$ and the null string otherwise. Note that these unitary operators $O_j$ are easy if $f$ is efficiently computable. Next, we consider the *reflection* operators $Q_j(f)$ as follows:

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

where

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

Fig.1 illustrates the intuitive image of the reflection operator. We sometimes use the notation $Q_j$ instead of $Q_j(f)$.

Actually, these reflection operators are somewhat special for our purpose. In general, reflection operators are commonly and successfully used in the Grover algorithm [9] and the quantum amplitude amplification technique [4].

### 2.2. Review of previous results

Informally speaking, a function $f$ is said to be worst-case quantum one-way if $f$ can be computed by an efficient quantum machine and $f^{-1}$ cannot be computed by any efficient quantum machine. One of the results in [11] is the following characterization of worst-case quantum one-way permutations.

**Theorem 1** (*Kashefi et al. [11]*). *Let $f : \{0,1\}^n \to \{0,1\}^n$ be a permutation. Then f is worst-case quantum one-way if and only if the set $\mathcal{F}_n = \{Q_j(f)\}_{j=0,1,\ldots,n/2-1}$ of unitary operators is not easy*.

As a part of the proof of Theorem 1, Kashefi et al. [11] give a quantum algorithm, which we call Algorithm INV in what follows, that computes $f^{-1}(x)$ by using unitary operators $O_j$ and $Q_j$. The initial input state to INV is assumed to be

$$\frac{1}{\sqrt{2^n}}|x\rangle \sum_{y\in\{0,1\}^n} |y\rangle \quad (= |x\rangle|\psi_{0,x}\rangle).$$

Then INV performs the following steps:

```
foreach $j = 0$ to $n/2 - 1$
        (step W.j.1) Apply $O_j$ to the first and the second registers;
        (step W.j.2) Apply $Q_j$ to the first and the second registers.
```

After each step, we have the following:

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

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

The above properties are with respect to “worst-case” (i.e., non-cryptographic) quantum one-way permutations, but they also play essential roles in the case of “average-case” (i.e., cryptographic) quantum one-way permutations. Before reviewing a known sufficient condition of cryptographic quantum one-way permutations, we define two types of cryptographic “one-wayness” in the quantum computational setting.

**Definition 2.** A permutation *f* is *weakly quantum one-way* if the following conditions are satisfied:

(1) *f* can be computed by a polynomial-size quantum circuit (and whenever inputs are classical the corresponding outputs must be classical) with certainty; [1]

(2) there exists a polynomial $p(\cdot)$ such that for every polynomial-size quantum circuit *A* and all sufficiently large *n*’s,

$$\Pr[\, A(f(U_n)) \neq U_n \,] > 1/p(n),$$

where $U_n$ is the uniform distribution over $\{0,1\}^n$.

[1] There are several ways to define what is the efficient computation of *f*. We may replace “a polynomial-size quantum circuit” in the definition by “a polynomial-size classical circuit”. This choice does not harm our results in this paper. We note that this footnote is also applicable to our definition of strongly quantum one-way permutations.

**Definition 3.** A permutation *f* is *strongly quantum one-way* if the following conditions are satisfied:

(1) *f* can be computed by a polynomial-size quantum circuit (and whenever inputs are classical the corresponding outputs must be classical) with certainty;

(2) for every polynomial-size quantum circuit *A* and every polynomial $p(\cdot)$ and all sufficiently large *n*'s,

$$\Pr[\, A(f(U_n)) = U_n \,] < 1/p(n).$$

As in the classical one-way permutations, we can show that the existence of weakly quantum one-way permutations is equivalent to that of strongly quantum one-way permutations. [2] Thus, we consider the weakly quantum one-way permutations in this paper. While Theorem 1 is a necessary and sufficient condition of *worst-case* quantum one-way permutations, Kashefi et al. [11] also gave a sufficient condition of *cryptographic* quantum one-way permutations by using the following notion.

**Definition 4.** Let $d(n) \geqslant n$ 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 $|X_n|/2^n \leqslant b(n)$ and for every $z \in \{0,1\}^n \setminus X_n$

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

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.

The closeness between a pseudo identity operator and the identity operator is measured by a pair of parameters $a(n)$ and $b(n)$. The first parameter $a(n)$ is a measure of a statistical property and the second one $b(n)$ is the ratio of "ill-behaved" elements. Note that we do not care where each $z \in X_n$ is mapped by the pseudo identity operator $J_n$. While we will give a necessary and sufficient condition of quantum one-way permutations by using the notion of pseudo identity, we introduce a new notion, which may be helpful to understand intuitions of our and previous conditions, in the following.

**Definition 5.** Let $d'(n) \geqslant n$ be a polynomial in *n* and $P_n$ be a $d'(n)$-qubit unitary operator. $P_n$ is called $(a(n), b(n))$-*pseudo reflection* (with respect to $|\psi(z)\rangle$) if there exists a set $X_n \subseteq \{0,1\}^n$ such that $|X_n|/2^n \leqslant b(n)$ and for every $z \in \{0,1\}^n \setminus X_n$ and every *n*-dimensional vector *w*

$$\left| 1 - \left( \langle z|_1 \otimes \langle w|_2 \left( \sum_{y \in \{0,1\}^n} |y\rangle\langle y|_1 \otimes (2|\psi(y)\rangle\langle\psi(y)| - I)_2 \right) \otimes \langle 0|_3 \right) P_n (|z\rangle_1 |w\rangle_2 |0\rangle_3) \right| \leqslant a(n).$$

[2] Theorem 2.3.2 in [6] states the equivalence between the existence of weakly one-way functions and that of strongly one-way functions and holds even in the quantum case. In case of classical one-way permutations, Theorem 2.6.2 in [6] mentions a tighter connection. You may also see [7] for the tight connection.

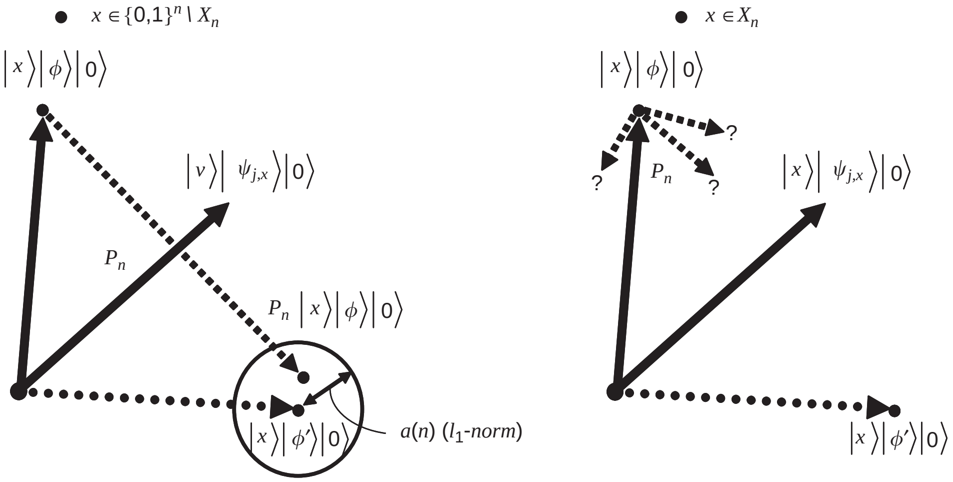
● $x \in \{0,1\}^n \setminus X_n$
$|x\rangle|\phi\rangle|0\rangle$
$|v\rangle|\psi_{j,x}\rangle|0\rangle$
$P_n$
$P_n|x\rangle|\phi\rangle|0\rangle$
$|x\rangle|\phi'\rangle|0\rangle$
$a(n)$ ($l_1$-norm)
● $x \in X_n$
$|x\rangle|\phi\rangle|0\rangle$
?
?
?
$P_n$
$|x\rangle|\psi_{j,x}\rangle|0\rangle$
$|x\rangle|\phi'\rangle|0\rangle$

Fig. 2. Pseudo reflection operator.

The above definition of pseudo reflection operators is somewhat complicated. Fig. 2 illustrates a geometrical intuition of the pseudo reflection operator, which may be helpful to understand the underlying idea of Definition 5. Let $J_n$ be a $d(n)$-qubit $(a(n), b(n))$-pseudo identity operator. Then $(I_n \otimes J_n)^\dagger (Q_j \otimes I_{d(n)-n})(I_n \otimes J_n)$ is a $(d(n)+n)$-qubit $(a'(n), b'(n))$-pseudo reflection operator with respect to $|\psi_{j,x}\rangle$, where $a'(n) \leqslant 2a(n)$ and $b'(n) \leqslant 2b(n)$. These estimations of $a'(n)$ and $b'(n)$ are too rough to obtain a necessary and sufficient condition. Rigorous estimation of these parameters is a main technical issue in this paper.

Now, we are ready to mention results with respect to “average-case” quantum one-way permutations shown in [11].

**Theorem 6** (*Kashefi et al. [11]*). *Let f be a permutation that can be computed by a polynomial-size quantum circuit. If f is not* (*weakly*) *quantum one-way, then for all polynomials p's and infinitely many n's, there exist a polynomial $r_p(n)$ and an $r_p(n)$-qubit $(\frac{1}{2}^{p(n)}, 1/p(n))$-pseudo identity operator $J_n$ such that the family of pseudo reflection operators*

$$\mathcal{F}_{p,n}(f) = \{(I_n \otimes J_n)^\dagger (Q_j(f) \otimes I_{r_p(n)-n})(I_n \otimes J_n)\}_{j=0,1,\ldots,n/2-1}$$

*is easy*.

Note that the second parameter $1/p(n)$ of the pseudo identity operator stated in Theorem 6 comes from the error bound of inverting algorithms for weakly one-way quantum permutations. Kashefi et al. [11] conjectured that the converse of Theorem 6 should still hold and proved a weaker version (with respect to the error bound of pseudo identity operators) of the converse as follows.

**Theorem 7** (*Kashefi et al. [11]*). *Let $f$ be a permutation that can be computed by a polynomial-size quantum circuit. If for all polynomials $p$'s and infinitely many $n$'s there exist a polynomial $r_p(n)$ and an $r_p(n)$-qubit $(\frac{1}{2}^{p(n)}, p(n)/2^n)$-pseudo identity operator family*[3] $\{J_{j,n}\}_{j=0,1,\ldots,n/2-1}$ *such that the family of pseudo reflection operators*

$$\mathcal{F}_{p,n}(f) = \{(I_n \otimes J_{j,n})^\dagger (Q_j(f) \otimes I_{r_p(n)-n})(I_n \otimes J_{j,n})\}_{j=0,1,\ldots,n/2-1}$$

*is easy*, *then f is not* (*weakly*) *quantum one-way*.

Note that pseudo identity operators stated in Theorem 7 permit "exponentially" small errors while pseudo identity operators that will appear in our statement permit "polynomially" small errors. We mention why it is difficult to show the converse of Theorem 6 (or, equivalently, the resulting statement by replacing "$p(n)/2^n$" of Theorem 7 with "$1/p(n)$"). To prove it by contradiction, all we can assume is the existence of a pseudo identity operator. This means that we cannot know how the pseudo identity operator is close to the identity operator. To overcome this difficulty, we introduce a probabilistic technique and estimate the expected behavior of the pseudo identity operator. Eventually, we give a necessary and sufficient condition of the existence of cryptographic quantum one-way permutations in terms of reflection operators. This affirmatively settles their conjecture. We stress that results with respect to cryptographic functions are obtained by generalizing ones with respect to non-cryptographic functions, since there are few connections between cryptographic and non-cryptographic functions in the classical computation model.

### 2.3. Universal tests

In this subsection, we explain what universal tests mean. Pseudorandom bits $w$'s, which are drawn according to some probability distribution, can be defined as ones that pass "all" polynomial-time computable statistical tests. Since $w$ passes "all" polynomial-time computable statistical tests if $w$ passes the *next bit test*, the next bit test is said to be *universal* for (unbiased) pseudorandom generators. On the other hand, "passing through the next bit test" means that the next bit is computationally unpredictable from the previous bits read so far and the *unpredictability* is defined for "all" polynomial-time algorithms. In this sense, "passing through the next bit test" is just a necessary and sufficient condition for pseudorandom generators. Furthermore, it is worthwhile to mention that the next bit test is a family of sub-tests which are uniformly defined. Namely, the next bit test means a family that consists of the 2nd bit test, the 3rd bit test, and so on. After all, the advantage of the next bit test for pseudorandom generators is not only its universality but also the fact that it is defined in terms of more primitive uniform components.

[3] In the corresponding statement in [11], "single" pseudo identity operator rather than pseudo identity operator "family" is used. On the other hand, their actual proof in [11] is for "family", which is as strong a statement as Theorem 7.

We now move to universal tests for quantum one-way permutations. To test the quantum one-wayness for given a permutation *f*, we have to consider all the polynomial-time quantum algorithms. Theorem 1 provides a universal test for worst-case quantum one-way permutations. Namely, *f* has an efficient implementation of all reflection operators $Q_j$'s with respect to *f* if and only if *f* is not one-way. The efficient implementability of all $Q_j$'s also means the next quantum state computability, which we have mentioned in Section 1. Thus, we call the universal test *next quantum state computability test*. Note that the next quantum state computability test for worst-case quantum one-way permutations is also defined in terms of more primitive uniform components as the next bit test for pseudorandom generators is.

In this paper, we give a universal test for "cryptographic" quantum one-way permutations by generalizing the next quantum state computability test for worst-case quantum one-way permutations. Since, in our universal test, we do not have to compute exactly the next quantum state, we may call our test *next quantum state approximability test*. Note that the next quantum state approximability test for average-case quantum one-way permutations is also defined in terms of more primitive uniform components.

## 3. Necessary and sufficient condition of quantum one-way permutations

We have a necessary and sufficient condition of cryptographic quantum one-way permutations as follows.

**Theorem 8.** *The following statements are equivalent*:

(1) *there exists a weakly quantum one-way permutation,*

(2) *there exists a polynomial-time computable function f satisfying that there exists a polynomial p such that for all sufficiently large n's, all polynomials $r_p(n)$'s and all $r_p(n)$-qubit $(\frac{1}{2}^{p(n)}, 1/p(n))$-pseudo identity operator families $\{J_{j,n}\}_{j=0,1,\ldots,n/2-1}$, the family of pseudo reflection operators*

$$\mathcal{F}_{p,n}(f) = \{(I_n \otimes J_{j,n})^\dagger (Q_j(f) \otimes I_{r_p(n)-n})(I_n \otimes J_{j,n})\}_{j=0,1,\ldots,n/2-1}$$

$\{J_{j,n}\}_{j=0,1,\ldots,n/2-1}$, *the family of pseudo reflection operators is not easy*.

To grasp the intuition of Theorem 8, Fig. 3 may be helpful. Theorem 8 can be proved as the combination of Theorem 6 and the following theorem.

**Theorem 9.** *Let f be a permutation that can be computed by a polynomial-size quantum circuit. If for all polynomials p's and infinitely many n's there exist a polynomial $r_p(n)$ and an $r_p(n)$-qubit $(\frac{1}{2}^{p(n)}, 1/p(n))$-pseudo identity operator family $\{J_{j,n}\}_{j=0,1,\ldots,n/2-1}$ such that the family of pseudo reflection operators*

$$\mathcal{F}_{p,n}(f) = \{\tilde{Q}_j(f)\} = \{(I_n \otimes J_{j,n})^\dagger (Q_j(f) \otimes I_{r_p(n)-n})(I_n \otimes J_{j,n})\}_{j=0,1,\ldots,n/2-1}$$

*is easy*, *then f is not* (*weakly*) *quantum one-way*.

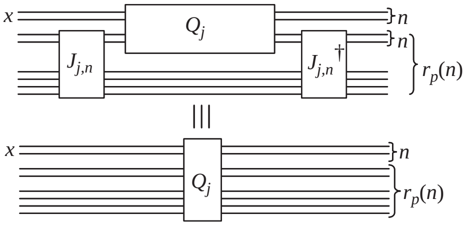

Fig. 3. Basic operations for the inversion.

We devote the rest of this section to the proof of Theorem 9.

**Proof.** Suppose that for every polynomials $p(n)$, infinitely many $n$'s, and some $(\frac{1}{2}^{p(n)}, 1/p(n))$-pseudo identity operator family $\{J_{j,n}\}_{j=0,1,\ldots,n/2-1}$, the family $\mathcal{F}_{p,n}$ of unitary operators is easy. Moreover, let *f* be a weakly quantum one-way permutation. By a probabilistic argument, we show that a contradiction follows from this assumption. For more detail, we construct an efficient inverter for *f* using $\mathcal{F}_{p,n}$ and then, if we choose a polynomial $p(n)$ appropriately, this efficient inverter can compute $x$ from $f(x)$ for a large fraction of inputs, which violates the assumption that *f* is a weakly quantum one-way permutation.

We first construct a polynomial-size algorithm av-INV to invert *f* by using unitary operations in $\mathcal{F}_{p,n}$. Algorithm av-INV is similar to Algorithm INV except the following change: the operator $Q_j$ is now replaced with $\tilde{Q}_j$. The initial input state to av-INV is also assumed to be

$$\frac{1}{\sqrt{2^n}}|x\rangle_1 \sum_{y\in\{0,1\}^n} |y\rangle_2|0\rangle_3,$$

where $|z\rangle_1$ (resp., $|z\rangle_2$ and $|z\rangle_3$) denotes the first $n$-qubit (resp., the second $n$-qubit and the last $(r_p(n)-n)$-qubit) register.
Algorithm av-INV performs the following steps:

```
foreach $j = 0$ to $n/2 - 1$
    (step j.1) Apply $O_j$ to the first and the second registers;
    (step j.2) Apply $\tilde{Q}_j$ to all the registers.
```

For analysis of Algorithm av-INV, we use the following functionally equivalent description:

```
foreach $j = 0$ to $n/2 - 1$
    (step A.j.1) Apply $O_j$ to the first and the second registers;
    (step A.j.2) Apply $J_{j,n}$ to the second and third registers;
    (step A.j.3) Apply $Q_j$ to the first and the second registers;
    (step A.j.4) Apply $J_{j,n}^\dagger$ to the second and third registers.
```

Then, we can prove the following two claims.

**Claim 10.** *Suppose that f is a weakly quantum one-way permutation, i.e., there exists a polynomial $r(n) \geqslant 1$ such that for every polynomial-size quantum circuit A and all sufficiently large n's,* $\Pr[\, A(f(U_n)) \neq U_n\,] > 1/r(n)$. *Then, for every polynomial $q(n) > r^{1/2}(n)$, there are at least $2^n(1/r(n) - 1/q^2(n))/(1 - 1/q^2(n))$ x's such that A cannot compute x from $f(x)$ better than with probability $1 - 1/q^2(n)$.*

**Claim 11.** *Let $q(n) = p^{1/4}(n)/\sqrt{2n}$. There are at most $2^n/q(n)$ x's such that Algorithm* av-INV *cannot compute x from $f(x)$ with probability at least $1 - 1/q^2(n)$.*

The proof of Claim 11 is delayed and that of Claim 10 follows immediately from the definition of a weakly quantum one-way permutation by a counting argument.

Recall that we assume that *f* is a weakly quantum one-way permutation at the beginning of this proof. Now, we can set $p(n) = 4n^2(r(n)+1)^4$, that is, $q(n) = r(n) + 1 \geqslant 2$. It follows that $(1/r(n) - 1/q^2(n))/(1 - 1/q^2(n)) > 1/q(n)$, which is a contradiction since av-INV is an inverter violating the assumption of a weakly quantum one-way permutation *f*. This implies that *f* is not weakly quantum one-way. □

In what follows, we present a proof of Claim 11 to complete the proof of Theorem 9.

**Proof of Claim 11.** Let $J_n$ be a $(\frac{1}{2}^{p(n)}, 1/p(n))$-pseudo identity operator. From the definition of pseudo identity operators, there exists a set $X_n \subseteq \{0,1\}^n$ with $|X_n| \leqslant 2^n/p(n)$ such that for every $y \in Y_n = \{0,1\}^n \setminus X_n$,

$$J_n|y\rangle_2|0\rangle_3 = \alpha_y|y\rangle_2|0\rangle_3 + |\psi_y\rangle_{23}, \tag{1}$$

where $|\psi_y\rangle_{23} \perp |y\rangle_2|0\rangle_3$ and $|1 - \alpha_y| \leqslant 1/2^{p(n)}$.

In Algorithm av-INV, we apply $J_{j,n}$ before and after step A.j.3 for each *j*. Each application of a pseudo identity operator $J_n \in \{J_{j,n}\}$ makes an error in computation of $f^{-1}$. We call the vector $J_n|\psi\rangle - |\psi\rangle$ the *error* associated to $|\psi\rangle$. To measure the effect of this error, we use the following lemmas. (Lemma 13 itself was stated in [11].) We note, in the sequel, the norm over vectors is Euclidean. □

**Lemma 12.** *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*

$$l(S,T) \leqslant 2\sqrt{\frac{|S \cap X_n|}{|S|}} + \gamma(n),$$

*where $\gamma(n)$ is a negligible function in n.*

**Proof.** First, we show a property of the length of the error associated to the state $|y\rangle|0\rangle$. The property is that the length is at most $2/2^{p(n)/2}$ if $y \in Y_n$. From Eq. (1), if $y \in Y_n$, $1 - |\alpha_y| \leqslant |1 - \alpha_y| \leqslant 1/2^{p(n)}$ and hence

$$||\psi_y\rangle|^2 = 1 - |\alpha_y|^2 = (1 - |\alpha_y|)(1 + |\alpha_y|) \leqslant 2/2^{p(n)}.$$

Thus, we obtain the following:

$$\begin{aligned} |J_n|y\rangle|0\rangle - |y\rangle|0\rangle| &= |(\alpha_y - 1)|y\rangle|0\rangle + |\psi_y\rangle| \\ &= \sqrt{|\alpha_y - 1|^2 + ||\psi_y\rangle|^2} \\ &\leqslant \sqrt{1/2^{2p(n)} + 2/2^{p(n)}} \\ &\leqslant 2/2^{p(n)/2}. \end{aligned}$$

Using this property, we have a tight bound of $l(S, T)$:

$$\begin{aligned} l(S,T) &= |J_n|\psi(S,T)\rangle - |\psi(S,T)\rangle| \\ &= \frac{1}{\sqrt{|S|}}\left|(J_n - I)\left(\sum_{y\in Y_n\cap(S\setminus T)}|y\rangle|0\rangle - \sum_{y\in Y_n\cap T}|y\rangle|0\rangle + \sum_{y\in X_n\cap(S\setminus T)}|y\rangle|0\rangle - \sum_{y\in X_n\cap T}|y\rangle|0\rangle\right)\right| \\ &\leqslant \frac{1}{\sqrt{|S|}}\left|(J_n - I)\left(\sum_{y\in Y_n\cap(S\setminus T)}|y\rangle|0\rangle - \sum_{y\in Y_n\cap T}|y\rangle|0\rangle\right)\right| \\ &\quad + \frac{1}{\sqrt{|S|}}\left|(J_n - I)\left(\sum_{y\in X_n\cap(S\setminus T)}|y\rangle|0\rangle - \sum_{y\in X_n\cap T}|y\rangle|0\rangle\right)\right| \\ &\leqslant \frac{1}{\sqrt{|S|}}\left(\sum_{y\in Y_n\cap(S\setminus T)}|J_n|y\rangle|0\rangle - |y\rangle|0\rangle| + \sum_{y\in Y_n\cap T}|J_n|y\rangle|0\rangle - |y\rangle|0\rangle|\right) \\ &\quad + \frac{1}{\sqrt{|S|}}\left(\left|J_n\left(\sum_{y\in X_n\cap(S\setminus T)}|y\rangle|0\rangle - \sum_{y\in X_n\cap T}|y\rangle|0\rangle\right)\right| + \left|\sum_{y\in X_n\cap(S\setminus T)}|y\rangle|0\rangle - \sum_{y\in X_n\cap T}|y\rangle|0\rangle\right|\right). \end{aligned}$$

The first term in the above is bounded by

$$\frac{2}{2^{p(n)/2}}\,\frac{|S\cap Y_n|}{\sqrt{|S|}} < \frac{2^{n+1}}{2^{p(n)/2}} < \frac{1}{2^n}$$

and negligible. Since any unitarity transformations preserve the Euclidean norm, the second term is rewritten as

$$\frac{2}{\sqrt{|S|}}\left|\sum_{y\in X_n\cap(S\setminus T)}|y\rangle|0\rangle - \sum_{y\in X_n\cap T}|y\rangle|0\rangle\right|$$

and equal to

$$\frac{2}{\sqrt{|S|}}\sqrt{(|X_n \cap (S \setminus T)| + |X_n \cap T|)} = 2\sqrt{\frac{|S \cap X_n|}{|S|}}.$$

These imply that the statement of Lemma 12 holds. □

**Lemma 13.** *Let $J_n|\psi(S,T)\rangle = \alpha|\psi(S,T)\rangle + |\psi(S,T)^{\perp}\rangle$, where $|\psi(S,T)\rangle \perp |\psi(S,T)^{\perp}\rangle$. Then, $||\psi(S,T)^{\perp}\rangle| \leqslant l(S,T)$.*

By using Lemmas 12 and 13, we consider the effect of the additional applications of pseudo identity operators to INV in order to analyze Algorithm av-INV.

For each *j*, we let $S_{x,j} = \{y : f(y)_{(1,2j)} = x_{(1,2j)}\}$ and $T_{x,j} = \{y : f(y)_{(1,2j+2)} = x_{(1,2j+2)}\}$. We assume that the state before step A.j.2 is

$$|x\rangle_1|\psi(S_{x,j}, T_{x,j})\rangle_{23} = |x\rangle_1 \frac{2^j}{\sqrt{2^n}}\left(\sum_{y\in S_{x,j}\setminus T_{x,j}} |y\rangle_2 - \sum_{y\in T_{x,j}} |y\rangle_2\right)|0\rangle_3.$$

Note that the above state is the same as the one before step W.j.2 in Algorithm INV.

In step A.j.2, $J_{j,n}$ is applied to the state. From Lemma 12 and a probabilistic argument, we have the following.

**Lemma 14.** *For each j,*

$$\mathbf{E}[\, l(S_{x,j}, T_{x,j})\,] \leqslant \frac{2}{\sqrt{p(n)}} + \gamma(n),$$

*where the expectation is over $x \in \{0,1\}^n$ and $\gamma(n)$ is a negligible function in n.*

**Proof.** Since *f* is a permutation, by the definition of $S_{x,j}$, $|S_{x,j}| = 2^{n-2j}$. Also, $y \in S_{x,j}$ for some *x* if and only if $f(y)_{(1,2j)} = x_{(1,2j)}$. Then,

$$\Pr[\, y \in S_{x,j}\,] = \frac{2^{n-2j}}{2^n} = \frac{1}{2^{2j}},$$

where the probability is taken over $x \in \{0,1\}^n$ uniformly. Thus we have, for every $(1/2^{p(n)}, 1/p(n))$-pseudo identity,

$$\mathbf{E}[\,|X_n \cap S_{x,j}|\,] = \frac{|X_n|}{2^{2j}}, \quad |S_{x,j}| = 2^{n-2j} \quad \text{and} \quad \frac{|X_n|}{2^n} = \frac{1}{p(n)}.$$

It follows that

$$\mathbf{E}\left[\frac{|X_n \cap S_{x,j}|}{|S_{x,j}|}\right] = \frac{1}{p(n)},$$

where the expectation is over $x \in \{0,1\}^n$. By Lemma 12,

$$\begin{aligned}\mathbf{E}\left[\, l(S_{x,j}, T_{x,j})\,\right] &\leqslant 2\mathbf{E}\left[\sqrt{\frac{|X_n \cap S_{x,j}|}{|S_{x,j}|}}\right] + \gamma(n)\\ &\leqslant 2\sqrt{\mathbf{E}\left[\frac{|X_n \cap S_{x,j}|}{|S_{x,j}|}\right]} + \gamma(n)\\ &= \frac{2}{\sqrt{p(n)}} + \gamma(n)\end{aligned}$$

for some negligible function $\gamma$ as required. □

From Lemmas 13 and 14, we obtain a vector $v = v_1 + v_2$ where $v_1/|v_1|$ is the unit vector corresponding to the state before step W.j.2 in Algorithm INV and $v_2$ is a vector of expected length at most $2/\sqrt{p(n)}$ orthogonal to $v_1$. (For simplicity, we neglect a negligible term $\gamma(n)$.) The vector $v_2$ corresponds to an error that happens when $J_{j,n}$ is applied before step A.j.3.

Next, we consider the state after step A.j.3. We assume that the state after step A.j.3 is

$$|x\rangle_1|\psi(S_{x,j+1},\emptyset)\rangle_{23} = |x\rangle_1 \frac{2^j}{\sqrt{2^n}}\left(\sum_{y\in S_{x,j+1}} |y\rangle_2\right)|0\rangle_3.$$

Note that the above state is the same as the one after step W.j.2 in Algorithm INV. In order to analyze the effect of the application of $J^{\dagger}_{j,n}$ after step A.j.3, we need another lemma similar to Lemma 14. (The proof is omitted since its proof is also similar.)

**Lemma 15.** *For each j,*

$$\mathbf{E}[\, l(S_{x,j+1},\emptyset)\,] \leqslant \frac{2}{\sqrt{p(n)}} + \gamma(n),$$

*where the expectation is over $x \in \{0,1\}^n$ and $\gamma(n)$ is a negligible function in n.*

By a similar argument to the above, we obtain a vector $v = v_1 + v_2$ where $v_1/|v_1|$ is the unit vector corresponding to the state after step W.j.2 in Algorithm INV and $v_2$ is a vector of expected length at most $2/\sqrt{p(n)}$ orthogonal to $v_1$. (For simplicity, we neglect a negligible term $\gamma(n)$.) The vector $v_2$ corresponds to an error that happens when $J^{\dagger}_{j,n}$ is applied after step A.j.3.

From the above analysis, we can see that after the completion of Algorithm av-INV on input $x$ the final state becomes $v(x) = v_1(x) + v_2(x)$ where $v_1(x)$ is parallel to

$$|x\rangle_1 |f^{-1}(x)\rangle_2 |0\rangle_3,$$

and $v_2(x)$ is a vector orthogonal to $v_1$. By Lemmas 14, 15 and the linearity of expectation, we have

$$\mathbf{E}[\,|v_2(x)|\,] \leqslant 2 \cdot \frac{n}{2} \cdot \frac{2}{\sqrt{p(n)}} = \frac{2n}{\sqrt{p(n)}} \leqslant \frac{1}{q^2(n)},$$

for $q(n) = p^{1/4}(n)/\sqrt{2n}$, where the expectation is over $x \in \{0,1\}^n$. It follows that the number of $x$ such that $|v_2(x)| > 1/q(n)$ is at most $2^n/q(n)$, i.e., av-INV can invert $f(x)$ for at least $2^n(1 - 1/q(n))$ $x$'s with probability at least $1 - 1/q^2(n)$. □

## 4. Conclusion

By giving a proof of the conjecture posed by Kashefi et al. [11], we have completed a necessary and sufficient condition of cryptographic quantum one-way permutations in terms of pseudo identity and reflection operator in this paper.

The necessary and sufficient condition of quantum one-way permutations can be regarded as a universal test for the quantum one-wayness of permutations. As far as the authors know, this is, classical or quantum, the first result on the universality for one-way permutations, although the next bit test is a universal test for pseudorandom generators in the classical computation model. We believe that our universal test for quantum one-way permutations may help to find good candidates for them, which are currently not known.

## 5. Uncited reference

[2].

## Acknowledgment

We are grateful for valuable comments from Harumichi Nishimura and anonymous referees.

## References

[1] M. Adcock, R. Cleve, A quantum Goldreich–Levin theorem with cryptographic applications, in: Proc. 19th Annu. Symp. on Theoretical Aspects of Computer Science, Lecture Notes in Computer Science, Vol. 2285, Springer, Berlin, 2002, pp. 323–334.

[2] C.H. Bennett, E. Bernstein, G. Brassard, U.V. Vazirani, Strengths and weaknesses of quantum computing, SIAM J. Comput. 26 (5) (1997) 1510–1523.

[3] M. Blum, S. Micali, How to generate cryptographically strong sequences of pseudo-random bits, SIAM J. Comput. 13 (4) (1984) 850–864.

[4] G. Brassard, P. Høyer, M. Mosca, A. Tapp, Quantum amplitude amplification and estimation, in: S.J. Lomonaco, Jr., H.E. Brandt (Eds.), Quantum computation and quantum information, AMS Contemporary Mathematics, Vol. 305, American Mathematical Society, Providence, RI, 2002.

[5] P. Dumais, D. Mayers, L. Salvail, Perfectly concealing quantum bit commitment from any one-way permutations, in: Advances in Cryptology—EUROCRYPT 2000, Lecture Notes in Computer Science, Vol. 1807, Springer, Berlin, 2000, pp. 300–315.

[6] O. Goldreich, Foundations of Cryptography: Basic Tools, Cambridge University Press, Cambridge, 2001.

[7] O. Goldreich, R. Impagliazzo, L.A. Levin, R. Venkatesan, D. Zuckerman, Security preserving amplification of hardness, in: Proc. 31st IEEE Symp. on Foundations of Computer Science, 1990, pp. 318–326.

[8] O. Goldreich, L.A. Levin, A hard-core predicate for all one-way functions, in: Proc. 21st ACM Symp. on Theory of Computing, 1989, pp. 25–32.

[9] L.K. Grover, A fast quantum mechanical algorithm for database search, in: Proc. 28th ACM Symp. on Theory of Computing, 1996, pp. 212–219.

[10] J. Håstad, R. Impagliazzo, L.A. Levin, M. Luby, A pseudorandom generator from any one-way function, SIAM J. Comput. 28 (4) (1999) 1364–1396.

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

[12] A. Kawachi, H. Kobayashi, T. Koshiba, R.H. Putra, Universal test for quantum one-way permutations, in: Proc. 29th Internat. Symp. on Mathematical Foundations of Computer Science, Lecture Notes in Computer Science, Vol. 3153, Springer, Berlin, 2004, pp. 839–850.

[13] A.W. Schrift, A. Shamir, Universal tests for nonuniform distributions, J. Cryptology 6 (3) (1993) 119–133.

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

[15] A.C. Yao, Theory and applications of trapdoor functions, in: Proc. 23rd IEEE Symp. on Foundations of Computer Science, 1982, pp. 80–91.