Quantum Information and Computation, Vol. 2, No. 5 (2002) 379–398
© Rinton Press

ON QUANTUM ONE-WAY PERMUTATIONS

ELHAM KASHEFI
Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Parks Road
Oxford OX1 3PU, England
Optics Section, The Blackett Laboratory, Imperial College
London SW7 2BZ, England

HARUMICHI NISHIMURA
Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Parks Road
Oxford OX1 3PU, England
CREST, Japan Science and Technology

VLATKO VEDRAL
Optics Section, The Blackett Laboratory, Imperial College
London SW7 2BZ, England

Received October 1, 2001
Revised July 25, 2002

We discuss the question of the existence of quantum one-way permutations. First, we consider the question: if a state is difficult to prepare, is the reflection operator about that state difficult to construct? By revisiting Grover's algorithm, we present the relationship between this question and the existence of quantum one-way permutations. Next, we prove the equivalence between inverting a permutation and that of constructing polynomial size quantum networks for reflection operators about a class of quantum states. We will consider both the worst case and the average case complexity scenarios for this problem. Moreover, we compare our method to Grover's algorithm and discuss possible applications of our results.

Keywords: one-way permutation, one-way function, Grover's algorithm, computational complexity
Communicated by: R Cleve & J Watrous

1. Introduction

Quantum computation is a rapidly growing field which explores the relationship between quantum physics and computation [1]. We have two strong indications that quantum systems are potentially more efficient than their classical counter-parts at performing computational tasks. One is Shor's algorithm [2], which solves the factoring problem and the discrete logarithm problem in quantum polynomial time. The other is Grover's algorithm [3], which works quadratically faster than any classical algorithm for the search problem in the oracle setting. On the other hand, in spite of these results, Bennett, Bernstein, Brassard, and Vazirani [4] have shown that with probability 1 there exists a quantum one-way permutation relative to a random permutation oracle.

The existence of one-way functions is one of the most important open problems in classical computation. It is also well-known that one-way functions have applications in cryptography [5]. Loosely speaking, a one-way function is one that is easy to compute but hard to invert. We will give the precise definition of one-way function in the following sections. The existence of one-way functions is linked to the complexity class **UP**, the class of languages accepted by a special, called *unambiguous*, polynomial time bounded nondeterministic Turing machines and the following relationship is well-known, $\mathbf{P} \subseteq \mathbf{UP} \subseteq \mathbf{NP}$. Furthermore the existence of one-way functions is equivalent to the separation between the complexity classes **P** and **UP** [6], and hence **P** and **NP** which indicates the difficulty of the problem of the existence of one-way functions.

In this paper we consider the quantum one-way permutations which is a restricted class of one-way functions. First, we consider the relationship between the complexity of preparing a state and the reflection about that state. We define a *unitary operator* on n qubits to be *easy* if there exists a polynomial size network implementing that operator. The n-qubit *state* $|\phi\rangle$ is defined to be *easy* if there exists an easy operator U on $\mathrm{poly}(n)$ qubits such that $U|0\rangle = |\phi\rangle$ up to a total phase. It is straightforward to see that if a state $|\phi\rangle$ is easy, the reflection about $|\phi\rangle$ is also easy. We consider the other direction, and by exposing another view of Grover's algorithm, we can find a counter-example to its validity if a quantum one-way permutation exists.

Next, we consider a necessary and sufficient condition for inverting efficiently a polynomial time computable permutation. In the classical case, Hemaspaandra and Rothe [7] presented a necessary and sufficient condition for the existence of one-way permutations. We show that in the quantum setting, the problem of inverting a permutation in polynomial time is equivalent to the problem of constructing polynomial size quantum networks for the reflection about a class of quantum states that we will define in this paper. In the proof of this equivalence, we present a quantum algorithm for inverting a permutation efficiently under the condition that reflections about their quantum states are efficiently implementable. The reason for considering those special quantum states is that, similar to Grover's algorithm, our algorithm also consists of the iteration of the tagging and reflection operators [3]; we show that the exponential speed-up over Grover's algorithm is possible if and only if all the efficient reflections about those quantum states are possible.

This paper is organized as follows. In Section 2, we revisit Grover's algorithm from the viewpoint of the notion of easy states and easy operators. In Section 3, we consider the worst case complexity scenario and we prove the equivalence between inverting a permutation and constructing quantum networks implementing the reflection about a class of quantum states. Then in Section 4 we explore an analogue of our result from Section 3, but now in the setting of the average case complexity. Finally in Section 5 we discuss other related results and possible applications of our results.

2. General View

In this paper, we will consider permutation functions in the following setting.

Definition 1 *A function $f : \{0,1\}^* \to \{0,1\}^*$ is called a permutation if it satisfies the following conditions*

(i) f is one-to-one and length preserving.

(ii) For some strictly increasing function $a : \mathbf{N} \to \mathbf{N}$, $\mathrm{Dom}(f) = \bigcup_{n \in \mathbf{N}} \{0,1\}^{a(n)}$.

These conditions imply that the restriction of f to $\{0,1\}^n \subseteq \mathrm{Dom}(f)$ is a permutation on $\{0,1\}^n$. The definition of one-way function in the worst case complexity is as follows.

Definition 2 *A function f is a worst case quantum one-way function, if the following conditions are satisfied:*

(i) f is one-to-one, and for all $x \in \{0,1\}^*, |x|^{\frac{1}{k}} \leq |f(x)| \leq |x|^k$ for some $k > 0$. That is, $f(x)$ is at most polynomially longer or shorter than x.

(ii) f can be computed by a (uniform) polynomial size (classical) network.

(iii) f^{-1} cannot be computed by any polynomial size quantum network.

Note that condition (i) is naturally satisfied for one-way permutations we consider in this paper. Next, we introduce a notion of complexity of preparing quantum states and constructing unitary operators.

Definition 3 *A unitary operator U on n qubits is easy, if there exists a network implementing U with polynomial size in n. An n-qubit state $|\phi\rangle$ is defined to be easy, if there exists an easy operator U on* $\mathrm{poly}(n)$ *qubits such that $U|0\rangle = |\phi\rangle$.*

As mentioned in the introduction, it is well-known that if a state is easy, then the reflection about that state is easy (Problem 6.2(1) in [1]). Does the converse hold? We call its converse, i.e., the statement "if the reflection about a state is easy, the state itself is easy", the *Reflection Assumption.* In the following, we revisit Grover's algorithm for inverting a permutation function from the viewpoint of complexity of preparing a quantum state and the reflection about that state, and discuss the relationship between the existence of quantum one-way permutations and the Reflection Assumption.

For any permutation f on n-bit strings, let U_f denote the unitary operator mapping the basis state $|x\rangle|y\rangle$ to $|x\rangle|f(x) \oplus y\rangle$, where $|x\rangle$ and $|y\rangle$ each consist of n qubits. We consider the following problem called hereafter **INVERT**: for any given $x \in \{0,1\}^n$, find $f^{-1}(x)$. In the setting where f is given as an oracle, Grover's algorithm [3] can solve **INVERT** with $\Theta(\sqrt{2^n})$ queries, while any classical algorithm needs $\Theta(2^n)$ queries to solve it. In his algorithm, Grover uses the tagging operator O defined as

$$O|x\rangle|y\rangle = \begin{cases} -|x\rangle|y\rangle & \text{if } f(y) = x \\ |x\rangle|y\rangle & \text{if } f(y) \neq x \end{cases} \tag{1}$$

and the reflection $2|\psi\rangle\langle\psi| - I$ about the uniform state,

$$|\psi\rangle = \sum_{y \in \{0,1\}^n} |y\rangle, \tag{2}$$

which is also called the inversion about the average amplitude. Grover's algorithm for **INVERT** (Algorithm **A** below) is as follows.

ALGORITHM **A**

Step 1 (Preparation).
Prepare the uniform superposition

$$|\psi\rangle = \sum_{y \in \{0,1\}^n} |y\rangle. \tag{3}$$

Step 2 (Iteration).
Iterate Step 2.1 and Step 2.2.
Step 2.1 Carry out the tagging operator

$$O = I - 2|f^{-1}(x)\rangle\langle f^{-1}(x)|. \tag{4}$$

Step 2.2 Carry out the reflection about the state $|\psi\rangle$.

Step 1 and Step 2.2 are easy. The operator O in Step 2.1 is a tagging operator and can be implemented by using the transformation

$$U_f : |y\rangle|z\rangle \mapsto |y\rangle|f(y) \oplus z\rangle\,. \tag{5}$$

In fact, for any $y \in \{0,1\}^n$ we have

$$\{(I - 2|f^{-1}(x)\rangle\langle f^{-1}(x)|) \otimes I\}|y\rangle|0\rangle = U_f(I \otimes (I - 2|x\rangle\langle x|))U_f|y\rangle|0\rangle\,. \tag{6}$$

Thus, given U_f as an oracle, we can compute $f^{-1}(x)$ with high probability in $O(\sqrt{2^n})$ queries. This algorithm is shown to be optimal [14]. Note that the operator $2|f^{-1}(x)\rangle\langle f^{-1}(x)| - I$ is performing the reflection about the state $|f^{-1}(x)\rangle$. Thus, Algorithm **A** shows that even if the reflection about the state $|f^{-1}(x)\rangle$ is *assumed to be* easy, the state itself is not necessarily easy (where here “easy” means that the number of queries to prepare the state is at most polynomial in n).

Now, let us consider the case when f is a quantum one-way permutation. Different from the query model, we will consider the circuit size complexity of preparing the state $|f^{-1}(x)\rangle$ and constructing the reflection operator about it. By condition (ii) of Definition 2 and Eq. (6), the operator U_f is easy and hence $2|f^{-1}(x)\rangle\langle f^{-1}(x)| - I$ is also easy. On the other hand, by condition (iii), the state $|f^{-1}(x)\rangle$ is not easy. Therefore, we can infer the following interesting fact: *if there exists a quantum one-way permutation, then there exists a counter-example to the Reflection Assumption.*

So far we have considered only the exact setting. However, using the diamond metric and its properties [15], similar results also hold in the bounded error setting. In the latter setting we define the notions of easy superoperator, easy state, and quantum one-way function as follows. A completely trace-preserving positive superoperator (CPSO) U is defined to be *approximately easy* if there exists a family of polynomial size quantum networks $\{N_\epsilon\}$ such that

$$||U - U_\epsilon||_\diamond \leq \epsilon\,, \tag{7}$$

where U_ϵ is the superoperator implemented by N_ϵ exactly. A mixed state ρ is defined to be *approximately easy* if there exists an approximately easy CPSO U such that

$$U(|0\rangle\langle 0|) = \rho\,. \tag{8}$$

To give the definition of quantum one-way function in the bounded-error setting, it is enough to replace conditions (ii) and (iii) of Definition 2 with the following conditions:

(ii′) The superoperator $U_f \cdot U_f^\dagger$ corresponding to the unitary operator

$$U_f : |x\rangle|z\rangle \mapsto |x\rangle|z \oplus f(x)\rangle \tag{9}$$

is approximately easy.

(iii′) f^{-1} cannot be computed with probability 2/3 with any polynomial size quantum network.

It is straightforward to check that, in the bounded error setting, if there exists a quantum one-way permutation then there exists a counter-example for the Reflection Assumption.

3. Worst case complexity

In this section we consider "one-wayness" in the worst case complexity, i.e. the complexity required for the *hardest* input. Definitions 1 and 2 give the precise description of quantum one-way permutation in the worst case scenario.

As mentioned before, Grover's algorithm for **INVERT** uses the tagging operator O (defined in Eq. (1)) which can be simulated by two applications of U_f and n controlled-not gates. Moreover, if f is polynomial time computable, then it is also possible to efficiently construct the unitary operator $O[k]$ defined by

$$O[k]|x\rangle|y\rangle = \begin{cases} -|x\rangle|y\rangle & \text{if } f(y)_{(k,k+1)} = x_{(k,k+1)} \\ |x\rangle|y\rangle & \text{if } f(y)_{(k,k+1)} \neq x_{(k,k+1)} \end{cases} \tag{10}$$

where $y_{(i,j)}$ denotes the bit string from i-th bit to j-th bit of the bit string y. The operators $O[k]$'s will enable us to mark all the states $|y\rangle$ such that 2 qubits of $|f(y)\rangle$ are equal to the corresponding qubits of $|x\rangle$. Geometrically, $O[k]$ can be considered to be the reflection about the hyper-plane spanned by the vectors $\{|y\rangle : f(y)_{(k,k+1)} \neq x_{(k,k+1)}\}$. We will show that if we can efficiently implement $O[k]$'s and the set of unitary operators

$$Q_j = \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes (2|\psi_{j,x}\rangle\langle\psi_{j,x}| - I)\,, \tag{11}$$

where

$$|\psi_{j,x}\rangle = \frac{1}{\sqrt{2^{n-2j}}} \sum_{y:f(y)_{(1,2j)}=x_{(1,2j)}} |y\rangle\,, \tag{12}$$

then we can efficiently invert f by a polynomial size network. Conversely, we will also prove that if f is difficult to invert, then Q_j's are also difficult to construct.

Now we state and prove this result formally. We say that a set F of unitary operators is *easy* if every $U \in F$ is easy.

Theorem 1 *A function $f : \{0,1\}^n \to \{0,1\}^n$ is a worst case quantum one-way permutation if and only if the set $F_n = \{Q_j\}_{j=0,1,\ldots,\frac{n}{2}-1}$ of unitary operators is not easy.*

Proof: Without loss of generality, we can assume that n is even.

($\Rightarrow$) Suppose that F_n is easy. Then we show that f^{-1} is computable by a polynomial size quantum network. A quantum algorithm (Algorithm **B** below) computing f^{-1} is as follows. Assume that x is given as the input in the first register of the quantum network to be constructed.

ALGORITHM **B**

Step 1 (Preparation).
Prepare the second register in the uniform superposition

$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} |y\rangle. \tag{13}$$

Step 2 (Iteration).
For $j = 0$ to $\frac{n}{2} - 1$, implement the following steps 2.j.1–2.j.2.
Step 2.j.1 Carry out $O[2j+1]$ on the first and the second registers.
Step 2.j.2 Carry out Q_j on the first and the second registers.

Step 2.j.1 can be implemented through the following three steps: (1) Carry out $U_f : |y\rangle|z\rangle \mapsto |y\rangle|f(y) \oplus z\rangle$ on the second and third registers. (2) Compare the $2j+1$-th and the $2j+2$-th qubits of the first register with the corresponding qubits of the third register, and apply a phase shift of -1 if they are same; otherwise do nothing. (3) Carry out U_f on the second and third registers.

Now we show that Algorithm **B** computes f^{-1}. After Step 1, the state of the system is

$$\frac{1}{\sqrt{2^n}}|x\rangle \sum_{y\in\{0,1\}^n} |y\rangle. \tag{14}$$

We show that after Step 2.j.2 the state of the system is

$$\frac{2^{j+1}}{\sqrt{2^n}}|x\rangle \sum_{y:f(y)_{(1,2j+2)}=x_{(1,2j+2)}} |y\rangle\,, \tag{15}$$

which means that Algorithm **B** computes f^{-1} after $\frac{n}{2}$ iterations. In the case $j = 0$, the state evolves as follows (note that for any x we have $|\psi_{0,x}\rangle = |\psi_0\rangle$):

$$\begin{aligned} &\frac{1}{\sqrt{2^n}}|x\rangle \sum_{y\in\{0,1\}^n} |y\rangle \\ \xrightarrow{2.0.1}\ &\frac{1}{\sqrt{2^n}}|x\rangle \left(\sum_{y:f(y)_{(1,2)}\neq x_{(1,2)}} |y\rangle - \sum_{y:f(y)_{(1,2)}=x_{(1,2)}} |y\rangle \right) \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{\sqrt{2^n}}|x\rangle\left(\sqrt{2^n}|\psi_0\rangle - 2\sum_{y:f(y)_{(1,2)}=x_{(1,2)}}|y\rangle\right)\\
&\xrightarrow{2.0.2} \frac{1}{\sqrt{2^n}}|x\rangle(2|\psi_0\rangle\langle\psi_0| - I)\left(\sqrt{2^n}|\psi_0\rangle - 2\sum_{y:f(y)_{(1,2)}=x_{(1,2)}}|y\rangle\right)\\
&= \frac{1}{\sqrt{2^n}}|x\rangle\left(2\sqrt{2^n}|\psi_0\rangle - \sqrt{2^n}|\psi_0\rangle - 4|\psi_0\rangle\sum_{y:f(y)_{(1,2)}=x_{(1,2)}}\langle\psi_0|y\rangle\right)\\
&+2\sum_{y:f(y)_{(1,2)}=x_{(1,2)}}|y\rangle\\
&= \frac{2}{\sqrt{2^n}}|x\rangle\sum_{y:f(y)_{(1,2)}=x_{(1,2)}}|y\rangle.
\end{aligned}\tag{16}$$

On the other hand, suppose that the case $j = k-1$ holds. Then, following Steps $2.k.1$–$2.k.2$, the state evolves as follows:

$$\begin{aligned}
&\frac{2^k}{\sqrt{2^n}}|x\rangle\sum_{y:f(y)_{(1,2k)}=x_{(1,2k)}}|y\rangle\\
&\xrightarrow{2.k.1} \frac{2^k}{\sqrt{2^n}}|x\rangle\left(\sum_{y:f(y)_{(1,2k)}=x_{(1,2k)}}|y\rangle - 2\sum_{y:f(y)_{(1,2k+2)}=x_{(1,2k+2)}}|y\rangle\right)\\
&= \frac{2^k}{\sqrt{2^n}}|x\rangle\left(\sqrt{2^{n-2k}}|\psi_{k,x}\rangle - 2\sum_{y:f(y)_{(1,2k+2)}=x_{(1,2k+2)}}|y\rangle\right)\\
&\xrightarrow{2.k.2} \frac{2^k}{\sqrt{2^n}}|x\rangle(2|\psi_{k,x}\rangle\langle\psi_{k,x}| - I)\left(\sqrt{2^{n-2k}}|\psi_{k,x}\rangle - 2\sum_{y:f(y)_{(1,2k+2)}=x_{(1,2k+2)}}|y\rangle\right)\\
&= \frac{2^k}{\sqrt{2^n}}|x\rangle\left(2\sqrt{2^{n-2k}}|\psi_{k,x}\rangle - \sqrt{2^{n-2k}}|\psi_{k,x}\rangle - 4|\psi_{k,x}\rangle\sum_{y:f(y)_{(1,2k+2)}=x_{(1,2k+2)}}\langle\psi_{k,x}|y\rangle\right)\\
&+\frac{2^k}{\sqrt{2^n}}|x\rangle\left(2\sum_{y:f(y)_{(1,2k+2)}=x_{(1,2k+2)}}|y\rangle\right)\\
&= \frac{2^{k+1}}{\sqrt{2^n}}|x\rangle\sum_{y:f(y)_{(1,2k+2)}=x_{(1,2k+2)}}|y\rangle\,.
\end{aligned}\tag{17}$$

Thus, the case $j = k$ holds. From the assumption that $\{Q_j\}$ is easy, it is simple to see that Algorithm **B** can be implemented by a polynomial size quantum network.

($\Leftarrow$) Suppose that f is not a worst-case one-way permutation. Then we show that $\{Q_j\}_{j=0,1,\ldots,\frac{n}{2}-1}$ can be implemented by a polynomial size quantum network. According to the assumption, f and f^{-1} are quantum polynomial time computable. The following operator

$$M_f : |x\rangle \mapsto |f(x)\rangle \tag{18}$$

can be implemented by a polynomial size quantum network [8, 9]. To see why note that: for any $x \in \{0,1\}^n$ we have

$$[M_f \otimes I]|x\rangle|0\rangle = [(U_{f^{-1}})^{-1} S U_f]|x\rangle|0\rangle\,, \tag{19}$$

where the swap gate S is defined as $S : |a\rangle \otimes |b\rangle \mapsto |b\rangle \otimes |a\rangle$.

In the following we show that the unitary operator $Q'_j = (I \otimes M_f)Q_j(I \otimes M_f)^\dagger$ can be implemented by a polynomial size quantum network, which means that Q_j can also be implemented by a polynomial size quantum network. The operator Q'_j can be rewritten as follows:

$$\begin{aligned}
Q'_j &= (I \otimes M_f)\left\{ \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes \left(2\left(\frac{1}{2^{n-2j}}\sum_{y,y'}{}^{*}|y\rangle\langle y'|\right) - I\right)\right\}(I \otimes M_f)^\dagger \\
&= \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes \left(2\frac{1}{2^{n-2j}}\sum_{y,y'}{}^{*}|f(y)\rangle\langle f(y')| - I\right) \\
&= \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes \left(2|x_{(1,2j)}\rangle\langle x_{(1,2j)}|\frac{1}{2^{n-2j}}\sum_{y,y'}{}^{*}|f(y)_{(2j+1,n)}\rangle\langle f(y')_{(2j+1,n)}| - I\right) \\
&= \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes (2|x_{(1,2j)}\rangle\langle x_{(1,2j)}| \otimes |\psi_j\rangle\langle\psi_j| - I) \\
&= \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes \left(|x_{(1,2j)}\rangle\langle x_{(1,2j)}| \otimes (2|\psi_j\rangle\langle\psi_j| - I) - \sum_{y:y\neq x_{(1,2j)}} |y\rangle\langle y| \otimes I\right).
\end{aligned} \tag{20}$$

Here, $\sum^*_{y,y'}$ denotes $\sum_{y,y':f(y)_{(1,2j)}=f(y')_{(1,2j)}=x_{(1,2j)}}$ and $|\psi_j\rangle$ denotes

$$|\psi_j\rangle = \frac{1}{\sqrt{2^{n-2j}}} \sum_{i\in\{0,1\}^{n-2j}} |i\rangle\,. \tag{21}$$

Thus, we can implement Q'_j by comparing the first $2j$ qubits of the first register with the corresponding qubits of the second register and applying $2|\psi_j\rangle\langle\psi_j| - I$ if they are the same and applying $-I$ otherwise. The operator $2|\psi_j\rangle\langle\psi_j| - I$ is easy, since $2|\psi_j\rangle\langle\psi_j| - I = H^{\otimes n-2j}(2|0\rangle\langle 0| - I)H^{\otimes n-2j}$, where H is the Hadamard gate and the superscript $n-2j$ indicates that the Hadamard gate is applied to the last $n-2j$ qubits. Therefore, Q'_j is easy and this completes the proof. □

Note that all unitary operators U_k are easy if and only if the operation

$$\sum_k |k\rangle\langle k| \otimes U_k\,, \tag{22}$$

which implements U_k conditionally, is easy. The operator Q_j implements the reflection about the state $|\psi_{j,x}\rangle$ conditionally, therefore Theorem 1 gives a necessary and sufficient condition for quantum one-way permutations in terms of the reflection about a quantum state.

Using quantum amplitude amplification method [12] we can generalize the definition of operators $O[k]$ and Q_j in Algorithm **B** as follows. In each step of Algorithm **B** we are concerned with only 2 qubits of input, i.e. the tagging operator $O[k]$ works only with the kth and $(k+1)$th qubits of its input register. However, one can consider the more general operators $O[k,l]$ as follows:

$$O[k,l]|x\rangle|y\rangle = \begin{cases} -|x\rangle|y\rangle & \text{if } f(y)_{(k,k+l-1)} = x_{(k,k+l-1)} \\ |x\rangle|y\rangle & \text{if } f(y)_{(k,k+l-1)} \neq x_{(k,k+l-1)}, \end{cases} \tag{23}$$

where l is any integer satisfying $2 \leq l \leq O(\log(n))$. The corresponding reflection operators $Q_{j,l}$ are

$$Q_{j,l} = \sum_{x\in\{0,1\}^n} |x\rangle\langle x| \otimes (2|\psi_{j,l,x}\rangle\langle\psi_{j,l,x}| - I)\,, \tag{24}$$

where

$$|\psi_{j,l,x}\rangle = \frac{1}{\sqrt{2^{n-lj}}} \sum_{y:f(y)_{(1,lj)}=x_{(1,lj)}} |y\rangle\,. \tag{25}$$

Now the generalized Algorithm **B′** has the same structure as Algorithm **B**, but in Algorithm **B′** steps 2.j.1 and 2.j.2 will be iterated $T_l = O(\sqrt{2^l})$ times, where the integer T_l is known in advance. Note that T_l is a polynomial in n. Intuitively, Step 2 of Algorithm **B** is an analogue of Grover's algorithm for the search problem where the number of the required items is $\frac{1}{4}$ of the total number of items. On the other hand, Step 2 of Algorithm **B′** is also an analogue of Grover's algorithm for the search problem where the number of required items is $\frac{1}{2^l}$ of the total number of items. After applying steps 2.j.1 and 2.j.2 (for $j = k$) of Algorithm **B′**, we obtain the state

$$|x\rangle \left(\sum_{y\in S_{k+1}} A_l|y\rangle + \sum_{y\in S_{k+1}\setminus S_k} B_l|y\rangle \right), \tag{26}$$

where $S_k = \{y : f(y)_{(1,lk)} = x_{(1,lk)}\}$ and positive numbers A_l and B_l are known in advance. Thus, using the quantum amplitude amplification process [12], we obtain the desired state:

$$\frac{1}{\sqrt{2^{n-l(k+1)}}}|x\rangle \sum_{y:f(y)_{(1,l(k+1))}=x_{(1,l(k+1))}} |y\rangle \tag{27}$$

and hence we can proceed to the next step.

In the rest of this section we give the relationship between the existence of one-way functions and well-known complexity classes **UP** and **EQP**. To this end we recall some definitions given in [6]. Assume that C is a complexity class; then we define the complexity class C_g as follows:

$$C_g = \{f \in C | graph(f) \in \mathbf{P}\}\,, \tag{28}$$

where

$$graph(f) = \{(x,y) | x \in \mathrm{Dom}(f)\,\&\, y = f(x)\}\,. \tag{29}$$

Denote by **QPSV**, the class of all single valued functions which can be computed exactly by polynomial time quantum Turing machines; **NPSV**, the class of all single valued nondeterministic polynomial time computable function; and **UPSV**, the class of all functions f

in **NPSV** such that for every x in domain of f there exists a unique accepting computational path. The following lemma introduces two relationships between the quantum and classical complexity classes.

Lemma 1 *The following relations hold:*

(i) $\mathbf{UP} \subseteq \mathbf{EQP}$

$\Rightarrow$ *(ii)* $\mathbf{UPSV} \subseteq \mathbf{QPSV}$

$\Rightarrow$ *(iii)* $\mathbf{UPSV}_g \subseteq \mathbf{QPSV}$.

Proof: The proof of (ii) $\Rightarrow$ (iii) is trivial. We give a sketch of the proof of (i) $\Rightarrow$ (ii) [6]. Assume that f is in **UPSV** and define R_f to be the following language:

$$R_f = \{(x, y) | x \in \mathrm{Dom}(f) \,\&\, y \leq f(x)\}\,. \tag{30}$$

Since $f \in$ **UPSV**, given input (x, y) one can compute $f(x)$ unambiguously and then check from the output whether $y \leq f(x)$. This shows that R_f belongs to **UP** and by assumption also belongs to **EQP**. Therefore using binary search one can show that $f \in$ **QPSV**. □

Now using a similar method to [6] we can prove the following theorem.

Theorem 2 *There exists a worst case quantum one-way function if and only if* $\mathbf{UP} \not\subseteq \mathbf{EQP}$.

Proof: ($\Rightarrow$) Assume that f is a worst case quantum one-way function. Then by definition we have $f^{-1} \in \mathbf{UPSV}_g$. However $f \notin$ **QPSV** therefore from Lemma 1 we derive $\mathbf{UP} \not\subseteq \mathbf{EQP}$.

($\Leftarrow$) Assume L to be a language in $\mathbf{UP} \setminus \mathbf{EQP}$ and M to be an unambiguous Turing machine accepting L. Then, the total function f defined below is a worst case one-way function:

$$f(x) = \begin{cases} y0 & \text{if } x = \mathrm{Comp}_M(y) \\ x1 & \text{otherwise,} \end{cases} \tag{31}$$

where $\mathrm{Comp}_M(y)$ denote the unique accepting computation of M on input y. □

4. Average case complexity

In order to apply our result to a realistic cryptographic scenario we need to consider also the average case complexity domain. This is because a realistic cryptographic protocol should be secure on "most" cases, which implies that it is hard to break on the average. We define two types of one-wayness in the average case setting. In what follows, for a property Q defined on $\mathbf{N}$, we say that $Q(n)$ holds for all sufficiently large n if the set $\{n \in \mathbf{N} | Q(n)$ does not hold$\}$ is finite.

Definition 4 *A permutation f is weakly quantum one-way, if the following conditions are satisfied:*

(i) f can be computed by a polynomial size network.

(ii) There exists a polynomial p such that for any polynomial size quantum network A and all sufficiently large $n \in \mathbf{N}$,

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \mathrm{Prob}[A(f(x)) \neq x] > \frac{1}{p(n)}\,, \tag{32}$$

where Prob: $\{0,1\}^n \to [0,1]$ *is a probability distribution induced by the measurement in the standard basis on the output register of the network A given the input x, and where $A(x)$ is a random variable distributed with the function* Prob.

In other words, a weakly quantum one-way permutation is easy to compute but the probability that any quantum algorithm fails to invert it is not negligible.

Definition 5 *A permutation f is strongly quantum one-way, if the following conditions are satisfied*

(i) f can be computed by a polynomial size network.

(ii) For any quantum polynomial size network A, any polynomial p, all sufficiently large n,

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \mathrm{Prob}[A(f(x)) = x] < \frac{1}{p(n)}, \tag{33}$$

where $A(x)$ is a random variable given as the output of the quantum algorithm A given the input x.

Again, in simple terms, a strongly quantum one-way permutation is easy to compute but the probability that any quantum algorithm succeeds in inverting it is negligible.

From the above definitions, it is easy to check the following relations.

Proposition 1 *In general we have*

(i) Every strongly quantum one-way permutation is also a weakly quantum one-way permutation.

(ii) Every weakly quantum one-way permutation is also a worst case quantum one-way permutation.

In the applications to cryptography, the existence of strongly quantum one-way permutations is the main concern. However, the following proposition shows that it is sufficient to characterize the existence of weakly quantum one-way permutations. We omit the proof as it is the same as the proof of Theorem 2.8 in [13].

Proposition 2 *Weakly quantum one-way permutations exist if and only if strongly quantum one-way permutations exist.*

For the rest of this section we discuss the relationships between weakly quantum one-way permutations and reflection operators, as we did in the worst case setting. We give a weaker analogue of Theorem 1 in the average case and finish the section with an open conjecture regarding the characterization of weakly quantum one-way permutations. In order to carry out our discussion in the average case setting we need to introduce an approximation of the identity operator as follows:

Definition 6 *Let d: $\mathbf{N} \to \mathbf{N}$ be a function satisfying $d(n) \geq n$. A $d(n)$ qubit unitary operator J_n is called $(a(n), b(n))$-pseudo identity, if there exists a set X_n with $|X_n|/2^n \leq b(n)$ such that for $i \in \{0,1\}^n \setminus X_n$,*

$$|1 - (\langle i|_1 \langle 0|_2) J_n (|i\rangle_1 |0\rangle_2)| \leq a(n)\,, \tag{34}$$

where $|\cdot\rangle_1$ and $|\cdot\rangle_2$ denote the first n qubit state and the last $d(n) - n$ qubit state.

In what follows, I_j denotes the j-qubit identity operator, and $|\psi\rangle_{i_1 \cdots i_l}$ means that the system consists of the registers $i_1, \ldots, i_l$ and its state is $|\psi\rangle$. For a vector v, we denote the length of v by $|v|$. Now we can give the first result on the link between average case one-wayness and the reflections about quantum states.

Theorem 3 *Let f: $\{0,1\}^* \to \{0,1\}^*$ be a permutation that can be computed by a classical polynomial size network. If f is not weakly quantum one-way, then for any polynomial p and infinitely many n, there exist a polynomial r_p and $r_p(n)$-qubit $(1/2^{p(n)}, 1/p(n))$-pseudo identity operators $J_{p(n)}$ such that the family*

$$F_{p,n} = \{(I_n \otimes J_{p(n)})^\dagger (Q_j \otimes I_{r_p(n)-n})(I_n \otimes J_{p(n)})\}_{j=0,1,\ldots,\frac{n}{2}-1} \tag{35}$$

is easy, where Q_j is the same reflection operator defined in Section 3.

Proof: Assume that f is not weakly quantum one-way. Then, for any polynomial p, there exist a polynomial size quantum network A and infinitely many n such that

$$\frac{1}{2^n} \sum_{y \in \{0,1\}^n} \mathrm{Prob}[A(y) = f^{-1}(y)] > 1 - \frac{1}{p(n)}\,. \tag{36}$$

Let $X'_n = \{y \in \{0,1\}^n | \ \mathrm{Prob}[A(y) = f^{-1}(y)] \leq \frac{1}{2}\}$ and $Y'_n = \{0,1\}^n \setminus X'_n$. From Eq. (36) we have

$$\frac{1}{2^n} \left(|Y'_n| \cdot 1 + |X'_n| \cdot \frac{1}{2} \right) > 1 - \frac{1}{p(n)}\,, \tag{37}$$

and hence we obtain $|X'_n| < \frac{2}{p(n)} 2^n$. Define $q(n) = \frac{1}{4} p(n)$, then $|Y'_n| \geq (1 - \frac{1}{2q(n)}) 2^n$.

Now assume $y \in Y'_n$. The final state of the network A for input y is:

$$\alpha_y |y\rangle_1 |f^{-1}(y)\rangle_2 |\psi^a_y\rangle_3 + |y\rangle_1 |w(y)\rangle_2 |\phi^a_y\rangle_3\,, \tag{38}$$

where $\alpha_y \in \mathbf{R}$, $|1 - \alpha_y| \leq \frac{1}{2}$, $|f^{-1}(y)\rangle_2 \perp |w(y)\rangle_2$, and $||\psi^a_y\rangle_3| = ||w(y)\rangle_2| = 1$ (note that $|\phi^a_y\rangle_3$ is not a unit vector). By repeating the network A at most $O(q(n))$ times, we can easily construct a polynomial size quantum network B whose final state has the same form as Eq. (38), where now $|1-\alpha_y| \leq \frac{1}{2^{q(n)+1}}$. Denote by C the quantum network constructed from B by the approximate clean garbage method [4] as follows: (1) Apply B, (2) copy the contents of the second register (which is the output register of B) to an extra register, (3) apply the inverse of B and change the contents of the second and the extra registers. Then, we can see that the final state of C on y is written in the following form:

$$\beta_y|y\rangle_1|f^{-1}(y)\rangle_2|0\rangle_3 + |\phi^b_y\rangle_{123}, \tag{39}$$

where $\beta_y \in \mathbf{R}$, $|1-\beta_y| \leq \frac{1}{2^{q(n)}}$ and $|y\rangle_1|f^{-1}(y)\rangle_2|0\rangle_3 \perp |\phi^b_y\rangle_{123}$.

To establish the analogue result of Theorem 1 we define the following two approximation operators. First, the approximation of the operator M_f from Theorem 1 for the average case is defined as follows:

$$\tilde{M}_f = (U_C)^{-1}(S\otimes I)(U_f\otimes I)\,, \tag{40}$$

where S denotes the swap operator on the first and the second registers and U_C is a unitary operator corresponding to the network C. The operator $\tilde{M}_f$ can be written in more detail as follows:

$$\begin{aligned}\tilde{M}_f \quad &= \quad \sum_{x\in Y_n}(\beta_{f(x)}|f(x)\rangle_1|0\rangle_{23} + |\phi^c_x\rangle_{123})\langle x|_1\langle 0|_{23} \\ &\quad + \sum_{x\in X_n}|\psi^c_x\rangle_{123}\langle x|_1\langle 0|_{23} + \sum_{x}\sum_{z:z\neq 0}|\psi^c_{x,z}\rangle_{123}\langle x|_1\langle z|_{23},\end{aligned} \tag{41}$$

where $|1-\beta_{f(x)}| \leq \frac{1}{2^{q(n)}}$ for any $x \in Y_n = \{x \in Y'_n | f(x) \in Y'_n\}$, $|f(x)\rangle_1|0\rangle_{23} \perp |\phi^c_x\rangle_{123}$, $X_n = \{0,1\}^n \setminus Y_n$, and $||\psi^c_x\rangle_{123}| = ||\psi^c_{x,z}\rangle_{123}| = 1$. The above form can be obtained by replacing the following forms of the operators $(U_C)^{-1}$ and $(S\otimes I)(U_f\otimes I)$ in the Eq. (40):

$$\begin{aligned}(U_C)^{-1} \quad &= \quad \sum_{y\in Y'_n}|y,0,0\rangle_{123}(\beta_y\langle y,f^{-1}(y),0|_{123} + \langle\phi^b_y|_{123}) \\ &\quad + \quad \sum_{y\in X'_n}|y,0,0\rangle_{123}\langle y,0,0|_{123}U_C^{-1} \\ &\quad + \quad \sum_{y}\sum_{(z,z')\neq(0,0)}|y,z,z'\rangle_{123}\langle y,z,z'|_{123}U_C^{-1}\end{aligned} \tag{42}$$

and

$$\begin{aligned}(S\otimes I)(U_f\otimes I) \quad &= \quad \sum_{x\in Y'_n}|f(x),x,0\rangle_{123}\langle x,0,0|_{123} \\ &\quad + \quad \sum_{x\in X'_n}|f(x),x,0\rangle_{123}\langle x,0,0|_{123} \\ &\quad + \quad \sum_{x}\sum_{(z,z')\neq(0,0)}|f(x)\oplus z,x,z'\rangle_{123}\langle x,z,z'|_{123}\,.\end{aligned} \tag{43}$$

Next, the approximation of the reflection operators Q_j's from Theorem 1 is defined as follows:

$$\begin{aligned}\tilde{Q}_j \quad &= \quad (I\otimes\tilde{M}_f)^\dagger(Q'_j\otimes I)(I\otimes\tilde{M}_f) \\ &= \quad (I\otimes M_f^{-1}\tilde{M}_f)^\dagger(Q_j\otimes I)(I\otimes M_f^{-1}\tilde{M}_f),\end{aligned} \tag{44}$$

where Q'_j is the same unitary operator defined in the proof of Theorem 1. The family $\{\tilde{Q}_j\}_j$ satisfies the required conditions of Theorem 3. First, $\tilde{Q}_j$ is easy, since Q'_j, M_f and $\tilde{M}_f$ can be implemented by polynomial size quantum networks. Next, we check that $M_f^{-1}\tilde{M}_f$ is $(1/2^{q(n)}, 1/q(n))$-pseudo identity. Indeed, from $|Y'_n| \geq (1 - 1/2q(n))2^n$ and $|X'_n| \leq (1/2q(n))2^n$, we have that

$$\begin{aligned} |Y_n| &= |Y'_n| - |\{x \in Y'_n | f(x) \in X'_n\}| \\ &\geq (1 - \frac{1}{2q(n)})2^n - |X'_n| \\ &\geq (1 - \frac{1}{q(n)})2^n \end{aligned} \tag{45}$$

and hence $|X_n| \leq (\frac{1}{q(n)})2^n$. Thus, it is sufficient to check that for $x \in Y_n$ we have

$$|1 - (\langle x|_1 \langle 0|_{23}) M_f^{-1} \tilde{M}_f (|x\rangle_1 |0\rangle_{23})| \leq \frac{1}{2^{q(n)}}. \tag{46}$$

This relation can be checked as follows. For $x \in Y_n$ we have

$$\tilde{M}_f |x\rangle_1 |0\rangle_{23} = \beta_{f(x)} |f(x)\rangle_1 |0\rangle_{23} + |\phi_x^c\rangle_{123} \tag{47}$$

and

$$\langle x|_1 \langle 0|_{23} M_f^{-1} = \langle f(x)|_1 \langle 0|_{23}. \tag{48}$$

Thus, for $x \in Y_n$ we have

$$(\langle x|_1 \langle 0|_{23}) M_f^{-1} \tilde{M}_f (|x\rangle_1 |0\rangle_{23}) = \beta_{f(x)} \tag{49}$$

and hence from $|1 - \beta_{f(x)}| \leq \frac{1}{2^{q(n)}}$ we obtain Eq. (46), which completes the proof. □

It is an open problem whether the converse of the above theorem holds. However, by restricting the second parameters of pseudo identity operators, we can prove the following restricted version of the converse of Theorem 3.

Theorem 4 *Let f:$\{0,1\}^* \to \{0,1\}^*$ be a permutation that can be computed by a classical polynomial size network. If for any polynomial p and infinitely many n there exist a polynomial r_p and an $r_p(n)$-qubit $(1/2^{p(n)}, p(n)/2^n)$-pseudo identity operator $J_{p(n)}$ such that the family*

$$F_{n,p} = \{\tilde{Q}_j\}_j = \{(I_n \otimes J_{p(n)})^\dagger (Q_j \otimes I_{r_p(n)-n})(I_n \otimes J_{p(n)})\}_{j=0,1,\ldots,\frac{n}{2}-1} \tag{50}$$

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

Proof: Assume that for a fixed polynomial p, infinitely many n, and some $(1/2^{p(n)}, p(n)/2^n)$-pseudo identity operator $J_{p(n)}$ the family $F_{n,p}$ is easy. To show that f is not a weakly quantum one-way permutation we give a polynomial size algorithm for inverting f. Algorithm $\widetilde{\mathbf{B}}$ has the same steps as Algorithm **B** except the following two changes:

(i) The number of iterations of Step 2 is now $\frac{n}{2} - \lceil 2\log p(n) \rceil$.

(ii) The operator Q_j is now replaced by $\tilde{Q}_j$.

A quantum network implementation for Algorithm $\widetilde{\mathbf{B}}$ consists of three registers. The first and the second registers consist of n qubits similar to the network for Algorithm **B**. The third register consists of $r_p(n) - n$ qubits. From the definition of pseudo identity operators, there exists a set X_n with $|X_n| \leq p(n)$ such that if $y \in Y_n = \{0,1\}^n \setminus X_n$,

$$J_{p(n)}|y\rangle_2|0\rangle_3 = \alpha_y|y\rangle_2|0\rangle_3 + |\psi_y\rangle_{23}, \tag{51}$$

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

In Algorithm $\widetilde{\mathbf{B}}$, we apply $J_{p(n)}$ before and after Step 2.j.2 for each j. The application of $J_{p(n)}$ creates 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 (the proof is given later).

Lemma 2 *Assume that $T \subseteq S \subseteq \{0,1\}^n$. Then length $l(S,T)$ of the error associated to the state*

$$|\psi(S,T)\rangle = \frac{1}{\sqrt{|S|}}\left(\sum_{y\in S\setminus T}|y\rangle|0\rangle - \sum_{y\in T}|y\rangle|0\rangle\right), \tag{52}$$

satisfies the following relation

$$l(S,T) \leq \frac{\frac{2}{2^{\frac{p(n)}{2}}}\cdot|S\cap Y_n| + 2|S\cap X_n|}{\sqrt{|S|}}. \tag{53}$$

Moreover, one can easily check the following lemma.

Lemma 3 *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 $||\psi(S,T)^\perp\rangle| \leq l(S,T)$.*

First, suppose that for some $j = k$ all steps before step 2.k.2 of Algorithm $\widetilde{\mathbf{B}}$ have been implemented as Algorithm **B**. By a similar argument to the proof of Theorem 1 we get the state

$$|x\rangle_1|\psi(S,T)\rangle_{23} = |x\rangle_1\frac{2^k}{\sqrt{2^n}}\left(\sum_{y\in S\setminus T}|y\rangle_2 - \sum_{y\in T}|y\rangle_2\right)|0\rangle_3, \tag{54}$$

where $S = \{y : f(y)_{(1,2k)} = x_{(1,2k)}\}$ and $T = \{y : f(y)_{(1,2k+2)} = x_{(1,2k+2)}\}$. In Algorithm $\widetilde{\mathbf{B}}$, $J_{p(n)}$ is applied for the state $|\psi(S,T)\rangle_{23}$. For $k \leq n/2 - \lceil 2\log p(n)\rceil$, from Lemma 2 we have

$$\begin{aligned} l(S,T) &\leq \frac{\frac{2}{2^{\frac{p(n)}{2}}}\cdot|S\cap Y_n| + 2|S\cap X_n|}{\sqrt{|S|}} \\ &\leq \frac{\frac{2}{2^{\frac{p(n)}{2}}}\cdot|S| + 2|X_n|}{\sqrt{|S|}} \end{aligned}$$

$$\begin{aligned} &\le \frac{\frac{2}{2^{\frac{p(n)}{2}}} \times 2^{n-2k} + 2p(n)}{\sqrt{2^{n-2k}}} \le \frac{2^{n+1-\frac{p(n)}{2}} + 2p(n)}{\sqrt{2^{n-2k}}} \\ &\le \frac{4p(n)}{2^{\frac{n}{2}-k}} \le \frac{4p(n)}{2^{\lceil 2\log p(n)\rceil}} \\ &\le \frac{4}{p(n)}. \end{aligned} \tag{55}$$

Therefore, for $k \le n/2 - \lceil 2\log p(n) \rceil$, from Lemma 3 we get a vector $v = v_1 + v_2$ where $\frac{v_1}{|v_1|}$ is the unit vector corresponding to the state before Step 2.k.2 (up to a total phase) and v_2 is a vector of length at most $\frac{4}{p(n)}$ orthogonal to v_1. The vector v_2 corresponds to an error which happens when $J_{p(n)}$ is applied before Step 2.k.2.

Next, assume that for some $j = k$ all steps before Step 2.k.2 and Step 2.k.2 itself have been implemented in the same way as for Algorithm **B**. We obtain the state

$$|x\rangle_1 |\psi(S,T)\rangle_{23} = |x\rangle_1 \frac{2^{k+1}}{\sqrt{2^n}} \sum_{y \in S} |y\rangle_2 |0\rangle_3, \tag{56}$$

where $S = \{y : f(y)_{(1,2k+2)} = x_{(1,2k+2)}\}$ and $T = \emptyset$. By a similar argument to the above, we get a vector $v = v_1 + v_2$, where $\frac{v_1}{|v_1|}$ is the unit vector corresponding to the state after Step 2.k.2 and v_2 is a vector of length at most $\frac{4}{p(n)}$ orthogonal to v_1. The vector v_2 corresponds to an error which occurs when $J_{p(n)}$ is applied after Step 2.k.2.

Now, from the above analysis, we can see that after the completion of Algorithm $\widetilde{\mathbf{B}}$ on input x the final state is $v = v_1 + v_2$, where v_1 is parallel to

$$|x\rangle_1 \frac{1}{\sqrt{2^{2\lceil 2\log p(n)\rceil}}} \sum_{y : f(y)_{(1,n-2\lceil 2\log p(n)\rceil)} = x_{(1,n-2\lceil 2\log p(n)\rceil)}} |y\rangle_2 |0\rangle_3 \tag{57}$$

and v_2 is a vector of length at most $2(n/2 - \lceil 2\log p(n) \rceil)(4/p(n))$ orthogonal to v_1. Thus, $|v_2| \le 1/q(n)$ for some polynomial q. We know in advance that for any x the probability of obtaining $f^{-1}(x)$ upon measuring the second register in the state v_1 is $1/2^{2\lceil 2\log p(n)\rceil}$. Now, using the algorithm in [12] (the quantum amplitude amplification when the success probability is known), we can change the state v into $w = w_1 + w_2$, where w_1 is parallel to $|x\rangle_1 |f^{-1}(x)\rangle_2 |0\rangle_3$, $w_1 \perp w_2$, and $|w_2|^2 = |v_2|^2 \le \frac{1}{q^2(n)}$. Therefore, there exist a polynomial size quantum network B and infinitely many n such that

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \mathrm{Prob}[B(x) = f^{-1}(x)] > 1 - \frac{1}{q^2(n)}. \tag{58}$$

We can give any large polynomial $q^2(n)$ by taking any large polynomial p. Thus, f is not weakly quantum one-way. □

Finally, we give the proof of Lemma 2.

Proof of Lemma 2: First, we show that the length of the error associated to the state $|y\rangle|0\rangle$ is at most $\frac{2}{2^{\frac{p(n)}{2}}}$ if $y \in Y_n$, and is at most 2 if $y \in X_n$. For $y \in Y_n$, from Eq. (51) we have

$1 - |\alpha_y| \leq |1 - \alpha_y| \leq \frac{1}{2^{p(n)}}$, and hence

$$|| \psi_y \rangle_{23}|^2 = 1 - |\alpha_y|^2 = (1 + |\alpha_y|)(1 - |\alpha_y|) \leq \frac{2}{2^{p(n)}}. \tag{59}$$

Thus, for the length of the error associated to $|y\rangle|0\rangle$ we obtain the following relation

$$\begin{aligned} |J_{p(n)}|y\rangle_2|0\rangle_3 - |y\rangle_2|0\rangle_3| &= |(\alpha_y - 1)|y\rangle_2|0\rangle_3 + |\psi_y\rangle_{23}| \\ &= \sqrt{|\alpha_y - 1|^2 + ||\psi_y\rangle_{23}|^2} \\ &\leq \sqrt{(\frac{1}{2^{p(n)}})^2 + \frac{2}{2^{p(n)}}} \\ &\leq \sqrt{\frac{4}{2^{p(n)}}} = \frac{2}{2^{\frac{p(n)}{2}}}\,. \end{aligned} \tag{60}$$

On the other hand, if $y \in X_n$, we have

$$|J_{p(n)}|y\rangle|0\rangle - |y\rangle|0\rangle| \leq |J_{p(n)}|y\rangle|0\rangle| + ||y\rangle|0\rangle| \leq 2. \tag{61}$$

Finally, for the length $l(S,T)$ of the error associated to the state $|\psi(S,T)\rangle$ we have

$$\begin{aligned} l(S,T) &= |J_{p(n)}|\psi(S,T)\rangle - |\psi(S,T)\rangle| \\ &\leq \frac{1}{\sqrt{|S|}} \left(\sum_{y \in S \setminus T} |(J_{p(n)} - I)|y\rangle|0\rangle| + \sum_{y \in T} |(J_{p(n)} - I)|y\rangle|0\rangle| \right) \\ &= \frac{1}{\sqrt{|S|}} \sum_{y \in S} |(J_{p(n)} - I)|y\rangle|0\rangle| \\ &= \frac{1}{\sqrt{|S|}} \left(\sum_{y \in S \cap Y_n} |(J_{p(n)} - I)|y\rangle|0\rangle| + \sum_{y \in S \cap X_n} |(J_{p(n)} - I)|y\rangle|0\rangle| \right) \\ &\leq \frac{1}{\sqrt{|S|}} \left(\frac{2}{2^{\frac{p(n)}{2}}} |S \cap Y_n| + 2|S \cap X_n| \right)\,.\ \Box \end{aligned} \tag{62}$$

From Proposition 2, Theorem 3 and Theorem 4, we obtain the following relationship between the existence of quantum one-way permutations and the reflection operators about a particular class of quantum states.

Theorem 5 *The following relations hold.*

(i) There exists a polynomial time computable function f such that: there exists a polynomial p such that for all sufficiently large n and all $(1/2^{p(n)}, 1/p(n))$-pseudo identity operators $J_{p(n)}$,

$$F_{n,p}(f) = \{(I_n \otimes J_{p(n)})^\dagger (Q_j(f) \otimes I_{r_p(n)-n})(I_n \otimes J_{p(n)})\}_{j=0,1,\ldots,\frac{n}{2}-1}. \tag{63}$$

is not easy.

$\Rightarrow$ *(ii) There exists a weakly quantum one-way permutation.*

$\Leftrightarrow$ *(iii) There exists a strongly quantum one-way permutation.*

$\Rightarrow$ *(iv) There exists a polynomial time computable function f such that: there exists a polynomial p such that for all sufficiently large n and all $(1/2^{p(n)}, p(n)/2^n)$-pseudo identity operators $J_{p(n)}$,*

$$F_{n,p}(f) = \{(I_n \otimes J_{p(n)})^\dagger (Q_j(f) \otimes I_{r_p(n)-n})(I_n \otimes J_{p(n)})\}_{j=0,1,\ldots,\frac{n}{2}-1}. \qquad (64)$$

is not easy.

On the other hand, for the bounded-error setting in the worst case complexity, we can prove the following necessary and sufficient condition by a similar argument to the proofs of Theorems 3 and 4 (the proof is therefore omitted).

Theorem 6 *The following statements are equivalent.*

(i) Worst case quantum one-way permutations exist in the bounded error setting.

(ii) There exists a polynomially computable function f satisfying the condition: there exists a polynomial p such that for infinitely many *n and all $(1/2^{p(n)}, p(n)/2^n)$-pseudo identity operators $J_{p(n)}$,*

$$F_{n,p}(f) = \{\tilde{Q}_j\}_j = \{(I_n \otimes J_{p(n)})^\dagger (Q_j(f) \otimes I_{r_p(n)-n})(I_n \otimes J_{p(n)})\}_{j=0,1,\ldots,\frac{n}{2}-1}. \qquad (65)$$

is not easy.

Comparing Theorem 6 with Theorem 5, we can see that condition (iv) of Theorem 5 is given essentially to characterize the existence of worst case quantum one-way permutation in the bounded-error setting (the only different part is the condition "all sufficient large" and "infinitely many"). We conjecture that condition (i) of Theorem 5 gives a necessary and sufficient condition for the existence of weakly (and strongly) quantum one-way permutations.

5. Discussions

We have reduced the problem of the existence of a quantum one-way permutation to the problem of constructing a polynomial size network for performing the specific task of the reflection about a given state. Ambainis [14] proved that inverting a permutation on the n-bit strings in the standard query model requires $\Omega(\sqrt{2^n})$ queries. In the standard query model [16], a quantum computation with T queries is a sequence of unitary operators

$$U_0 \to O \to U_1 \to O \cdots \to U_{T-1} \to O \to U_T, \qquad (66)$$

where U_j's are arbitrary unitary operators independent of a database to be searched or a permutation to be computed, and O is the standard query operator. However, our algorithm is consistent with Ambainis' result, since we consider the case that U_j's depend on a permutation to be computed and this does not fit his model.

Another related issue is the work of Chen and Diao [17] where they attempted to present an efficient quantum algorithm for the search problem, which is similar to our algorithm for the problem **INVERT**. They mentioned that the tagging operation and the reflection about a given state which varies dynamically can be constructed by polynomial size networks, but they did not show the construction for their operations. (This construction is, of course, impossible given Grover's black box, since it would violate the optimality proof of Grover's algorithm [10, 11, 14].) For the problem **INVERT** we have given a polynomial size network for the tagging operation and we have shown that the difficulty of the construction of the reflection operation is equivalent to the existence of worst case quantum one-way permutations. Furthermore it is an interesting open problem whether there exists a reduction from other types of one-way functions to constructing a polynomial size network for performing the reflection about a given state.

On the other hand, we have seen that Grover's algorithm gives us an example of states that are difficult to prepare but the reflections about these states are easy, i.e., it provides a counter-example to Reflection Assumption assuming the existence of one-way permutations. This investigation of Reflection Assumption seems to be useful for cryptographic applications since recently, quantum bit commitment protocols based on quantum one-way permutations have been proposed [18, 19]. Moreover, it is interesting to find such a concrete counter-example without the existence of quantum one-way permutations. Presenting such examples of states may provide us with more ideas for constructing novel quantum algorithms.

Acknowledgements

We would like to acknowledge the anonymous referees for useful suggestions. This work was supported by EPSRC, the European grant EQUIP and the QUIPROCONE grant.

References

1. M.A. Nielsen and I.L. Chuang (2000), *Quantum Computation and Quantum Information*, Cambridge University Press.
2. P.W. Shor (1994), *Algorithms for quantum computation: Discrete logarithms and factoring*, in Proceedings of 35th IEEE Symposium on Foundations of Computer Science, pp. 124-134; P.W. Shor (1997), *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput., 26, pp.1484-1509.
3. L.K. Grover (1996), *A fast quantum mechanical algorithm for database search*, in Proceedings of 28th ACM Symposium on the Theory of Computing, pp. 212-219.
4. C.H. Bennett, E. Bernstein, G. Brassard, and U.Vazirani (1997), *Strengths and weaknesses of quantum computing*, SIAM J. Comput., 26, pp.1510-1523.
5. C.H. Papadimitriou (1994), *Computational Complexity*, Addision-Wesley.
6. J. Grollmann and A.L. Selman (1988), *Complexity measures for public-key cryptosystems*, SIAM J. Comput., 17, pp. 309-335.
7. L. Hemaspaandra and J. Rothe (2000), *Characterizing the existence of one-way permutation*, Theoret. Comput. Sci., 244, pp. 257-261.
8. C.H. Bennett (1973), *Logical reversibility of computations*, IBM J. Res. Develop., 17, pp. 525-532.
9. E. Kashefi, A. Kent, V. Vedral, and K. Banaszek (2002), Comparison of quantum oracles, Phys. Rev. A, 65, 050304-050307.
10. M. Boyer, G. Brassard, P. Høyer, and A. Tapp (1998), *Tight bounds on quantum searching*, Fortsch. Phys., 46, pp. 493-505.
11. C. Zalka (1999), *Grover's quantum searching algorithm is optimal*, Phys. Rev. A, 60, pp. 2746-2751.

12. G. Brassard, P. Høyer, M. Mosca, and A. Tapp (2000), *Quantum amplitude amplification and estimation*, to appear in AMS Contemporary Mathematics Series Millennium Volume entitled "Quantum Computation & Information", quant-ph/0005055.
13. O. Goldreich (1995), *Foundations of Cryptography – Fragment of a Book*, http://www. wisdom.weizmann.ac.il / oded/frag.html .
14. A. Ambainis. (2000), *Quantum lower bounds by quantum arguments*, in Proceedings of 32th ACM Symposium on the Theory of Computing, pp. 636-643.
15. D. Aharonov, A. Kitaev and N. Nisan (1998), *Quantum circuits with mixed states*, in Proceedings of 30th ACM Symposium on the Theory of Computing, pp. 20-30.
16. R. Beal, H. Buhrman, R. Cleve, M. Mosca and R. de Wolf. (1998), *Quantum lower bounds by polynomials*, in Proceedings of 39th IEEE Symposium on Foundations of Computer Science, pp. 352-361.
17. G. Chen and Z. Diao (2000), *An exponentially fast quantum search algorithm*, quant-ph/0011109.
18. P. Dumais, D. Mayers and L. Salvail (2000), *Perfectly concealing quantum bit commitment from any one-way permutation*, Advances in Cryptology – EUROCRYPT 2000, B. Preneel (Ed.), Lecture Note in Computer Science 1807, Springer-Verlag, pp. 300-315.
19. M. Adcock and R. Cleve. (2002), *A quantum Goldreich-Levin theorem with cryptographic applications*, in Proceedings of 19th Annual Symposium on Theoretical Aspect of Computer Sciences, Lecture Note in Computer Sceinece 2285, Springer-Verlag, pp. 323-334.