Statistical Zero Knowledge and quantum one-way functions

Citation for published version:
Kashefi, E & Kerenidis, I 2007, 'Statistical Zero Knowledge and quantum one-way functions' Theoretical Computer Science, vol. 378, no. 1, pp. 101-116. DOI: 10.1016/j.tcs.2007.03.013

Digital Object Identifier (DOI):
10.1016/j.tcs.2007.03.013

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Theoretical Computer Science

Statistical Zero Knowledge and quantum one-way functions

Elham Kashefi
Christ Church, University of Oxford &
IQC, University of Waterloo
elham.kashefi@comlab.ox.ac.uk

Iordanis Kerenidis
University of Paris (LRI), CNRS &
Dept. of Mathematics, M.I.T.
jkeren@lri.fr

February 1, 2008

Abstract

One-way functions are a fundamental notion in cryptography, since they are the necessary condition for the existence of secure encryption schemes. Most examples of such functions, including Factoring, Discrete Logarithm or the RSA function, can be, however, inverted with the help of a quantum computer. Hence, it is very important to study the possibility of *quantum one-way functions*, i.e. functions which are easily computable by a classical algorithm but are hard to invert even by a quantum adversary. In this paper, we provide a set of problems that are good candidates for quantum one-way functions. These problems include Graph Non-Isomorphism, Approximate Closest Lattice Vector and Group Non-Membership. More generally, we show that any hard instance of Circuit Quantum Sampling gives rise to a quantum one-way function. By the work of Aharonov and Ta-Shma [2], this implies that any language in Statistical Zero Knowledge which is hard-on-average for quantum computers, leads to a quantum one-way function. Moreover, extending the result of Impagliazzo and Luby [10] to the quantum setting, we prove that quantum distributionally one-way functions are equivalent to quantum one-way functions.

1 Introduction

One-way functions are at the core of modern cryptography. The fundamental task of cryptography is that of secure encryption of information against malicious parties. The existence of such secure encryption schemes implies that there is an efficient way of generating instances of problems together with some auxiliary information, such that it is easy to solve these instances with the help of the auxiliary information but hard to solve on average without it.

This concept is exactly captured by the definition of one-way functions, which are the necessary condition for the existence of cryptography. Moreover, one-way functions have many theoretical applications, for example in their connections to cryptographic primitives like bit commitment and oblivious transfer, Zero Knowledge Proof Systems and pseudorandom generators.

However, proving that one-way functions exist would imply that P $\neq$ NP and hence, we only have "candidate" one-way functions. Such candidate problems include Factoring, Discrete Logarithm, Graph Isomorphism, Quadratic Residuosity, Approximate Shortest Vector and Closest Vector and the RSA function. These problems seem to belong to a class called NP-*Intermediate*, i.e. they are NP problems for which we do not know any efficient algorithm, but they don't seem to be NP-hard. Moreover, many of the candidate problems belong to the class of Statistical Zero Knowledge (SZK). In fact, Ostrovsky [14] showed that if SZK contains any *hard-on-average* problem, then one-way functions exist.

The emergence of quantum computation and communication has provided the field of cryptography with many new strengths and challenges. The possibility of unconditionally secure key distribution shows that the laws of quantum mechanics can allow for the secure transmission of information over quantum channels. Moreover, Shor's celebrated algorithm for Factoring and Discrete Logarithm implies that many classical one-way functions and hence cryptosystems, including RSA, will not be secure against quantum adversaries. It is a very important question to ask whether we can construct cryptosystems which are secure even against quantum attacks. To this end, we need to find good candidates for quantum one-way functions, i.e. functions which are easily computable by a classical algorithm but hard to invert even by a quantum adversary.

Several other applications of quantum one-way functions have also been studied in a series of papers. For example, the connections between quantum one-way functions and quantum computationally secure bit commitment schemes were explored in [5, 1, 3]. On the other hand, Gottesman *et.al.* [7] proposed a digital signature scheme based on a quantum one-way function with classical inputs but quantum outputs and proved the informational security of their protocol. Moreover, Kashefi *et.al.* [11] and Kawachi *et.al.* [12] presented a necessary and sufficient condition for testing the one-wayness of a given permutation in the quantum setting based on the efficiency of constructing a family of reflection operators. Recently, Watrous [16] proved that several classical interactive proof systems are statistically zero-knowledge against quantum attacks and showed that Computational Zero Knowledge against quantum attacks for NP is implied by the existence of quantum one-way permutations.

Despite the importance of the applications of quantum one-way functions, there had been few results so far that provided good candidate problems [4]. Here, we prove the quantum analogue of Ostrovsky's result and show that if there exists a problem in Statistical Zero Knowledge which is hard-on-average for a quantum computer, then quantum one-way functions exist and hence provide a set of problems that are good candidates for quantum one-way functions.

The key insight in our result is the connection of quantum one-way functions to the problem of *Circuit Quantum Sampling*. Informally speaking, *quantum sampling* is the ability to prepare efficiently a superposition that corresponds to a samplable classical probability distributions, i.e. a superposition whose amplitudes are the square roots of the probabilities of a classical distribution from which one can efficiently sample. The hardness of this task depends on the structure of the underlying set. For example, it is well known that being able to quantumly sample from the set of homomorphisms of a given input graph is sufficient to solve the notorious Graph Isomorphism problem. Aharanov and Ta-shma [2] have introduced this framework of circuit quantum sampling and have shown that many problems in quantum computation, including Graph Isomorphism, Discrete Logarithm, Quadratic Residuosity and Approximate Closest Lattice Vector (CVP), are all instances of it.

We relate the problem of quantum sampling to quantum one-way functions by giving a simple proof that any hard instance of the quantum sampling problem implies the existence of a quantum one-way function. We first prove our results for the case of one-to-one one-way functions, the existence of which seems to be a stronger assumption than that of general one-way functions. Then, we generalize our results for many-to-one one-way functions. We show that a hard instance of the CQS problem implies a quantum distributionally one-way function and then prove that a quantum distributionally one-way function implies a quantum one-way function. The notion of classical distributionally one-way function was introduced by Impagliazzo and Luby in [10], where they also prove its equivalence to classical one-way function.

Aharonov and Ta-Shma showed that any Statistical Zero Knowledge language (SZK) can be reduced to a family of instances of the CQS problem. Using our result that a hard instance of CQS implies the existence of a quantum one-way function, we conclude that if there exists a language in Statistical Zero Knowledge which is hard-on-average, then quantum one-way functions exist.

2 Preliminaries

In this section we provide a brief overview of classical one-way functions and quantum computation. For an excellent exposition on quantum computation we refer the reader to [13] and for one-way functions to [6].

2.1 Classical one-way functions

Definition 1 *A function* $f : \{0,1\}^* \rightarrow \{0,1\}^*$ *is a* weak one-way function, *if the following conditions are satisfied:*

(i) easy to compute: *f can be computed by a polynomial size classical circuit.*

(ii) slightly-hard to invert: *There exists a polynomial $p(\cdot)$ such that for any probabilistic polynomial time algorithm I and for all sufficiently large $n \in \mathbf{N}$ we have*

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \text{Prob}[I(f(x), 1^n) \in f^{-1}(f(x))] \leq 1 - \frac{1}{p(n)} \,.$$

A classical weak one-way function f is defined in terms of a uniform family of functions f_n, one for each input length n. The inverter I of the function takes as input the value $f(x)$ and the size n in unary. For simplicity, in the following definitions we omit the parameter n. One can also assume, without loss of generality that the function f, is *length regular i.e.* for every $x, y \in \{0,1\}^*$, if $|x| = |y|$ then $|f(x)| = |f(y)|$ and *length preserving i.e.* for every $x \in \{0,1\}^*$, $|f(x)| = |x|$ (for proof see [6]).

Intuitively, the above definition of a weak one-way function says that the function is easy to compute but the probability that any algorithm fails to invert it, is not negligible as Condition (ii) can be equivalently written in the following form:

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \text{Prob}[I(f(x), 1^n) \notin f^{-1}(f(x))] \geq \frac{1}{p(n)}\,.$$

Of course, such a definition seems to be very weak. One can define another type of one-way function, called *strong one-way function*, where we require that any algorithm inverts the function with negligible probability, where Condition (ii) will be replaced as follows:

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \text{Prob}[I(f(x), 1^n) \in f^{-1}(f(x))] \leq \frac{1}{p(n)}\,.$$

However, the two definitions are known to be equivalent both in the classical and quantum setting [6, 8, 11], meaning that if a weak one-way function exists then a strong one-way function also exists. Hence, it suffices to work with the weaker but equivalent notion of weak one-wayness given in Definition 1.

Furthermore, Impagliazzo and Luby [10] defined a seemingly weaker notion of one-wayness for many-to-one functions, called *distributionally one-way function*, and proved that, in fact, the existence of a distributionally one-way function implies the existence of a one-way function.

Definition 2 *A function $f : \{0,1\}^* \to \{0,1\}^*$ is a* distributionally one-way function*, if the following conditions are satisfied:*

(i) easy to compute: *f can be computed by a polynomial size classical circuit.*

(ii) hard to sample: *There exists a polynomial $p(\cdot)$ such that for any probabilistic polynomial time algorithm S and for all sufficiently large $n \in \mathbf{N}$, the distribution defined by $(x, f(x))$ and the distribution defined by $(S(f(x)), f(x))$ are statistically distinguishable by (i.e. have total variation distance) at least $\frac{1}{p(n)}$ when $x \in \{0,1\}^n$ is chosen uniformly.*

2.2 Quantum Computation

Let H denote a 2-dimensional complex vector space, equipped with the standard inner product. We pick an orthonormal basis for this space, label the two basis vectors $|0\rangle$ and $|1\rangle$, and for simplicity identify them with the vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, respectively. A *qubit* is a unit length vector in this space, and so can be expressed as a linear combination of the basis states:

$$\alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}.$$

Here α_0, α_1 are complex *amplitudes*, and $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

An *m-qubit system* is a unit vector in the m-fold tensor space $H \otimes \cdots \otimes H$. The 2^m basis states of this space are the m-fold tensor products of the states $|0\rangle$ and $|1\rangle$. For example, the basis states of a 2-qubit system are the 4-dimensional unit vectors $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, and $|1\rangle \otimes |1\rangle$. We abbreviate, *e.g.* , $|1\rangle \otimes |0\rangle$ to $|0\rangle|1\rangle$, or $|1, 0\rangle$, or $|10\rangle$, or even $|2\rangle$ (since 2 is 10 in binary). With these basis states, an m-qubit state $|\phi\rangle$ is a 2^m-dimensional complex unit vector

$$|\phi\rangle = \sum_{i \in \{0,1\}^m} \alpha_i |i\rangle.$$

We use $\langle\phi| = |\phi\rangle^*$ to denote the conjugate transpose of the vector $|\phi\rangle$, and $(\phi\ ,\ \psi) = \langle\phi| \cdot |\psi\rangle$ for the inner product between states $|\phi\rangle$ and $|\psi\rangle$. These two states are *orthogonal* if $(\phi\ ,\ \psi) = 0$. The *norm* of $|\phi\rangle$ is $\|\phi\| = \sqrt{|(\phi\ ,\ \phi)|}$.

A quantum state can evolve by a unitary operation or by a measurement. A *unitary* transformation is a linear mapping that preserves the ℓ_2 norm. If we apply a unitary U to a state $|\phi\rangle$, it evolves to $U|\phi\rangle$.

The most general measurement allowed by quantum mechanics is specified by a family of positive semidefinite operators $E_i = M_i^* M_i$, $1 \leq i \leq k$, subject to the condition that $\sum_i E_i = I$. A projective measurement is defined in the special case where the operators are projections. Let $|\phi\rangle$ be an m-qubit state and $B = \{|b_1\rangle, \ldots, |b_{2^m}\rangle\}$ an orthonormal basis of the m-qubit space. A projective measurement of the state $|\phi\rangle$ in the B basis means that we apply the projection operators $P_i = |b_i\rangle\langle b_i|$ to $|\phi\rangle$. The resulting quantum state is $|b_i\rangle$ with probability $p_i = |(\phi\ ,\ b_i)|^2$.

2.3 Quantum Sampling

Let $\{C_i\}$ be a uniform classical circuit family and for every input size n define D_{C_n} to be the distribution over outputs of the circuit $C_n : \{0,1\}^n \rightarrow \{0,1\}^m$ when the input distribution is uniform. Denote by $|C_n\rangle = \sum_{z \in \{0,1\}^m} \sqrt{D_{C_n}(z)}|z\rangle$, the *quantum sample of outputs* of C_n.

Definition 3 *Given a uniform family of classical circuit $\{C_i\}$ and a real number $0 \leq \epsilon < \frac{1}{2}$, define QS_C to be an efficient quantum circuit which for any sufficiently large input size n, prepares a state that is ϵ-close to the quantum sample $|C_n\rangle$, i.e. $|(QS_C(|0\rangle, 1^n)\ ,\ |C_n\rangle)|^2 \geq 1 - \epsilon$.*

The problem of finding such a quantum circuit QS_C for any given uniform family of classical circuits $\{C_i\}$ was introduced by Aharanov and Ta-shma in [2], as the *Circuit Quantum Sampling Problem* (CQS). In fact, they defined CQS as $\|QS_C(|0\rangle, 1^n) - |C_n\rangle\| \leq \epsilon$, however both definitions suffice for the proof that Statistical Zero Knowledge reduces to a family of instances of the CQS problem. We say that the quantum sampling problem for $\{C_i\}$ is *hard* if there exists no efficient QS for any constant $\epsilon \in [0, 1/2]$.

3 Definitions of quantum one-way functions

A *quantum one-way function* is defined similarly to the classical case, where now the inverter I is a polynomial size uniform quantum circuit family. For simplicity, we follow again the convention of omitting the parameter of the input size n.

Definition 4 *A one-to-one function $f : \{0,1\}^* \rightarrow \{0,1\}^*$ is a* weak quantum one-way function*, if the following conditions are satisfied:*

(i) easy to compute: *f can be computed by a polynomial size classical circuit.*

(ii) slightly-hard to invert: *There exists a polynomial $p(\cdot)$ such that for any quantum polynomial time algorithm I and all sufficiently large $n \in \mathbf{N}$ we have*

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \text{Prob}[I(f(x)) \in f^{-1}(f(x))] \leq 1 - \frac{1}{p(n)}\,.$$

In the quantum case, the probability of success of the inverter I is defined as the square of the inner product between the outcome of I and the outcome of the perfect inverter P, where

$$P : |f(x)\rangle|\beta\rangle \mapsto |f(x)\rangle|x \oplus \beta\rangle\,.$$

In other words, for the case of one-to-one functions

$$\text{Prob}[I(f(x)) \in f^{-1}(f(x))] = \text{Prob}[I(f(x)) = x] = |(I(|f(x)\rangle|\beta\rangle)\ ,\ |f(x)\rangle|x \oplus \beta\rangle)|^2.$$

As said before, one can also define another type of quantum one-way function (strong quantum one-way function), where we require that any quantum algorithm inverts the function with negligible probability (instead of just failing with non-negligible probability). However, similar to the classical case, if there exists a weak quantum one-way function (Definition 4), then there exists a strong quantum one-way function as well [6, 8, 11]. In this article, one-way function means a weak one-way function if not stated otherwise.

We now provide an alternative definition for a one-to-one quantum one-way function, which is more suitable for constructing the relation between quantum one-way functions and the CQS problems and prove the equivalence of the two definitions.

Definition 5 *A one-to-one function $f : \{0,1\}^* \rightarrow \{0,1\}^*$ is a* weak quantum one-way function *if:*

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

(ii) There exists a polynomial $p(\cdot)$ such that there exists no quantum polynomial time algorithm I' with the property that for all sufficiently large $n \in \mathbf{N}$ we obtain

$$I' : |f(x)\rangle|\beta\rangle \mapsto a_{f(x)}|f(x)\rangle|x \oplus \beta\rangle + b_{f(x)}|f(x)\rangle|G_{f(x)}\rangle\,, \qquad (1)$$

where $G_{f(x)}$ is a garbage state, $\frac{1}{2^n}\sum_{x\in\{0,1\}^n} a^2_{f(x)} \geq 1 - \frac{1}{p(n)}$ and $a_{f(x)}$ are positive real numbers.

It is clear that definition 4 implies definition 5 and we also prove the converse.

Theorem 1 *If a one-to-one function f is weak quantum one-way according to definition 5, then it is also weak quantum one-way according to definition 4.*

Proof. Let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be a quantum one-way function according to definition 5. Assume for contradiction that this function is not one-way according to definition 4. Then, for all polynomials $p(\cdot)$ there exists a quantum polynomial time algorithm I with the property that for all sufficiently large $n \in \mathbf{N}$

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \text{Prob}[I(f(x)) \in f^{-1}(f(x))] \geq 1 - \frac{1}{p(n)}\,,$$

or equivalently

$$I : |f(x)\rangle|\beta\rangle \mapsto c_{f(x)}|f(x)\rangle|x \oplus \beta\rangle + d_{f(x)}|\psi_{f(x)}\rangle\,, \tag{2}$$

where $|\psi_{f(x)}\rangle$ is a garbage state and $\frac{1}{2^n}\sum_{x\in\{0,1\}^n}|c_{f(x)}|^2 \geq 1 - \frac{1}{p(n)}$. Without loss of generality we can assume that $c_{f(x)}$ are real numbers since it is well known that any quantum circuit with complex amplitudes can be replaced by another circuit with one more qubit and real amplitudes. We use this inverter to construct the following unitary that achieves the positive amplitudes. For clarity, here and in subsequent places in the paper we only show the unitary construction for the case where the ancilla registers are set to $|0\rangle$, unless the general ancilla state is required for the construction. It is clear of course how to unitarily extend the $|0\rangle$ ancilla to the other basis states.

$$\begin{array}{lll}
|f(x)\rangle|0\rangle|0\rangle|0\rangle & \rightarrow_{(\mathrm{CNOT})_{1,3}} & |f(x)\rangle|0\rangle|f(x)\rangle|0\rangle \\
 & \rightarrow_{I_{1,2}} & (c_{f(x)}|f(x)\rangle|x\rangle + d_{f(x)}|\psi_{f(x)}\rangle)|f(x)\rangle|0\rangle \\
 & \rightarrow_{I_{3,4}} & c^2_{f(x)}|f(x)\rangle|x\rangle|f(x)\rangle|x\rangle + c_{f(x)}d_{f(x)}|f(x)\rangle|x\rangle|\psi_{f(x)}\rangle + \\
 & & d_{f(x)}c_{f(x)}|\psi_{f(x)}\rangle|f(x)\rangle|x\rangle + d^2_{f(x)}|\psi_{f(x)}\rangle|\psi_{f(x)}\rangle \\
 & \rightarrow_{(\mathrm{CNOT})_{1,3}(\mathrm{CNOT})_{2,4}} & c^2_{f(x)}|f(x)\rangle|x\rangle|0\rangle|0\rangle + b_{f(x)}|\psi'_{f(x)}\rangle\,,
\end{array}$$

where $|\psi'_{f(x)}\rangle$ is the new garbage state, orthogonal to the ideal state $|f(x)\rangle|x\rangle|0\rangle|0\rangle$ and by the fact that the average of the squares is larger than the square of the average we have

$$\tfrac{1}{2^n}\textstyle\sum_{x\in\{0,1\}^n} c^4_{f(x)} \geq (\tfrac{1}{2^n}\sum_{x\in\{0,1\}^n} c^2_{f(x)})^2 \geq (1 - \tfrac{1}{p(n)})^2 \geq 1 - \tfrac{1}{p'(n)}\,.$$

Hence we have a new inverter

$$I' : |f(x)\rangle|\beta\rangle \mapsto a_{f(x)}|f(x)\rangle|x \oplus \beta\rangle + b_{f(x)}|\psi'_{f(x)}\rangle\,, \tag{3}$$

with $\frac{1}{2^n}\sum_{x\in\{0,1\}^n} a^2_{f(x)} \geq 1 - \frac{1}{p(n)}$ and $a_{f(x)} = c^2_{f(x)}$ being positive real numbers. Finally, we can obtain the required form of the garbage state:

$$\begin{array}{lll}
|f(x)\rangle|0\rangle|0\rangle & \rightarrow_{(\mathrm{CNOT})_{1,2}} & |f(x)\rangle|f(x)\rangle|0\rangle \\
 & \rightarrow_{I'_{2,3}} & a_{f(x)}|f(x)\rangle|f(x)\rangle|x\rangle + b_{f(x)}|f(x)\rangle|\psi'_{f(x)}\rangle \\
 & \rightarrow_{(\mathrm{CNOT})_{1,2}} & a_{f(x)}|f(x)\rangle|0\rangle|x\rangle + b_{f(x)}|f(x)\rangle|G_{f(x)}\rangle\,.
\end{array}$$

We reached a contradiction and therefore the function f is one-way according to definition 4. Note that for simplicity of presentation we dropped the $|0\rangle$ registers that are constant for all x. □

The important aspect of Theorem 1 is the positivity of the amplitude $a_{f(x)}$ in the definition of the inverter algorithm I'. We will use this fact in order to relate one-way functions and circuit quantum sampling.

In the standard definition, a many-to-one function is called one-way if there exists no inverter that outputs with high probability an arbitrary preimage of $f(x)$. For many-to-one functions, Impagliazzo and Luby [10] defined a seemingly weaker notion, the *distributionally one-way function*. In this case, an inverter is required to output a *random* preimage of $f(x)$ and not just an arbitrary one. However, they prove that, in fact, the existence of a distributionally one-way function implies the existence of a one-way function. We also define quantum distributionally one-wayness for many-to-one functions and will prove its equivalence to the quantum one-way functions.

Definition 6 *A many-to-one function $f : \{0,1\}^* \to \{0,1\}^*$ is a* quantum distributionally one-way function, *if the following conditions are satisfied:*

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

(ii) hard to invert: *There exists a polynomial $p(\cdot)$ such that for any quantum polynomial time algorithm S and all sufficiently large $n \in \mathbf{N}$ we have*

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} |(S(|f(x)\rangle|0\rangle) \ , \ |f(x)\rangle|H_{f(x)}\rangle)|^2 \leq 1 - \frac{1}{p(n)},$$

where $|H_{f(x)}\rangle = \frac{1}{\sqrt{|f^{-1}(f(x))|}} \sum_{x \in f^{-1}(f(x))} |x\rangle$.

Note that one could potentially consider different definitions for quantum distributionally one-way functions, for example the quantum inverter could return a superposition with equal amplitudes but different phases. We believe that our quantum definition captures the essence of the classical one and moreover, we only use the above notion as an intermediate step in our proofs. Similar to the case of one-to-one functions we also give an equivalent definition

Definition 7 *A many-to-one function $f : \{0,1\}^* \to \{0,1\}^*$ is a* quantum distributionally one-way function *if:*

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

(ii) There exists a polynomial p such that there exists no quantum polynomial time algorithm S' with the property that for all sufficiently large $n \in \mathbf{N}$ we obtain

$$S' : |f(x)\rangle|0\rangle \mapsto a_{f(x)}|f(x)\rangle|H_{f(x)}\rangle + b_{f(x)}|f(x)\rangle|G_{f(x)}\rangle \, , \tag{4}$$

where $|G_{f(x)}\rangle$ is a garbage state, $\frac{1}{2^n}\sum_{x \in \{0,1\}^n} a^2_{f(x)} \geq 1 - \frac{1}{p(n)}$, $a_{f(x)}$ are positive real numbers and $|H_{f(x)}\rangle = \frac{1}{\sqrt{|f^{-1}(f(x))|}} \sum_{x \in f^{-1}(f(x))} |x\rangle$.

We can easily extend the above algorithm S' into a unitary operation by mapping every other basis state $|f(x)\rangle|\beta\rangle$ to $|f(x)\rangle|T^{\beta}_{f(x)}\rangle$, where the set $\{|H_{f(x)}\rangle, T^1_{f(x)}, \ldots, T^{2^n-1}_{f(x)}\}$ is any orthonormal basis. Following the same steps as in the proof of Theorem 1 we have

Theorem 2 *If a many-to-one function f is quantum one-way according to definition 7, then it is also quantum one-way according to definition 6.*

4 Circuit quantum sampling and one-way functions

In this section, we show that hard instances of the Circuit Quantum Sampling problem are good candidates for quantum one-way functions.

4.1 One-to-one one-way functions

We first focus our attention to the case of one-to-one one-way functions. The existence of one-to-one one-way functions is a seemingly stronger assumption than that of the existence of general one-way functions, since a one-way function doesn't immediately imply a one-to-one one-way function. However, this case illustrates the main ideas of our construction. In the following sections, we generalize our results for the case of many-to-one functions.

Theorem 3 *Assume for a classical circuit family $\{C_n\}$, which computes a one-to-one function, the corresponding CQS problem is hard , i.e. there exists no efficient quantum circuit implementing QS_C. Then the function $f : \{0,1\}^* \to \{0,1\}^*$ which is defined for every input size n as $f_n : x \mapsto C_n(x)$ is a quantum one-way function.*

Proof. For clarity, we are going to omit the parameter of the input size n from the inverter. Since, the circuit is efficient, one can implement the unitary map

$$U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle \,, \tag{5}$$

The theorem follows by proving the contrapositive. Assume that f is not a quantum one-way function. Then according to definition 5, for every polynomial p there exists a quantum circuit I' which succeeds in approximately inverting f, i.e. for all sufficiently large $n \in \mathbf{N}$ we have

$$I' : |f(x)\rangle|\beta\rangle \mapsto a_{f(x)}|f(x)\rangle|x \oplus \beta\rangle + b_{f(x)}|f(x)\rangle|G_{f(x)}\rangle \,, \tag{6}$$

where $|G_{f(x)}\rangle$ is a garbage state, $\frac{1}{2^n}\sum_x a^2_{f(x)} > 1 - \frac{1}{p(n)}$ and the $a_{f(x)}$'s are positive. Now, from equations 5 and 6 we have

$$\begin{array}{lll} |x\rangle|0\rangle & \rightarrow_{U_f} & |x\rangle|f(x)\rangle \\ & \rightarrow_{\text{SWAP}} & |f(x)\rangle|x\rangle \\ & \rightarrow_{I'} & a_{f(x)}|f(x)\rangle|0\rangle + b_{f(x)}|f(x)\rangle|G'_{f(x)}\rangle \,. \end{array}$$

Starting with a uniform superposition of $x \in \{0,1\}^n$ we have

$$\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle \quad \rightarrow \quad \frac{1}{2^{n/2}} \sum_x (\; a_{f(x)}|f(x)\rangle|0\rangle + b_{f(x)}|f(x)\rangle|G'_{f(x)}\rangle \;) \equiv |Q_n\rangle \,.$$

We claim that the above circuit that on input $(|0\rangle, 1^n)$ outputs $|Q_n\rangle$ is a quantum sampler for C. Let $|C_n\rangle = \frac{1}{2^{n/2}}\sum_x |f(x)\rangle|0\rangle$ be the quantum sample of the circuit C, then

$$|\langle Q_n|C_n\rangle|^2 = |\frac{1}{2^n}\sum_x a_{f(x)}|^2 \geq |\frac{1}{2^n}\sum_x a^2_{f(x)}|^2 > (1 - 1/p(n))^2 > 1 - \epsilon \,,$$

where $\epsilon = \frac{2}{p(n)} - \frac{1}{p^2(n)}$. This is a contradiction to C being a hard instance of the CQS problem and hence f is a quantum one-way function. □

4.2 Many-to-one one-way functions

The previous section dealt with the case of one-to-one one-way functions. Here, we generalize our results to the case of many-to-one functions. We show that the existence of a hard instance of CQS problem, where the circuit family $\{C_n\}$ is many-to-one, implies the existence of a quantum distributionally one-way function. In the next section we prove that a quantum distributionally one-way function implies a quantum one-way function.

Theorem 4 *Assume for a classical circuit family $\{C_n\}$, which computes a many-to-one function, the corresponding CQS problem is hard , i.e. there exists no efficient quantum circuit implementing QS_C. Then the function $f : \{0,1\}^* \to \{0,1\}^*$ which is defined for every input size n as $f_n : x \mapsto C_n(x)$ is a quantum distributionally one-way function.*

Proof. Since the classical circuit is efficient one can implement the unitary map

$$U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle\,.$$

Assume that f is not a quantum distributional one-way, then according to definition 7 for every polynomial p there exists a quantum polynomial time algorithm S' which succeeds in approximately implementing a sampler for f, i.e. for all sufficiently large $n \in \mathbf{N}$ we have

$$S' : |f(x)\rangle|0\rangle \mapsto a_{f(x)}|f(x)\rangle|H_{f(x)}\rangle + b_{f(x)}|f(x)\rangle|G_{f(x)}\rangle\,, \tag{7}$$

where $\frac{1}{2^n}\sum_{x\in\{0,1\}^n} a^2_{f(x)} > 1-\frac{1}{p(n)}$ and the $a_{f(x)}$'s are positive. Note that one can unitarily extend the S' to apply over any state of the form $|f(x)\rangle|\beta\rangle$ with $\beta \neq 0$. Using the above unitaries, we can construct a quantum sampler QS_C that for every input n constructs a quantum sample for C_n:

$$\begin{aligned}
\sum_{x\in\{0,1\}^n}\frac{1}{2^{n/2}}|x\rangle|0\rangle \quad &\equiv \quad \sum_{f(x)}\frac{\sqrt{|f^{-1}(f(x))|}}{2^{n/2}}|H_{f(x)}\rangle|0\rangle \\
&\rightarrow_{U_f} \quad \sum_{f(x)}\frac{\sqrt{|f^{-1}(f(x))|}}{2^{n/2}}|H_{f(x)}\rangle|f(x)\rangle \\
&\rightarrow_{\text{SWAP}} \quad \sum_{f(x)}\frac{\sqrt{|f^{-1}(f(x))|}}{2^{n/2}}|f(x)\rangle|H_{f(x)}\rangle \\
&\rightarrow_{S'^\dagger} \quad \sum_{f(x)}\frac{\sqrt{|f^{-1}(f(x))|}}{2^{n/2}}(\ a_{f(x)}|f(x)\rangle|0\rangle + b_{f(x)}|f(x)\rangle|G'_{f(x)}\rangle) \equiv |Q_n\rangle\,.
\end{aligned}$$

The quantum sample for the circuit C_n is $|C_n\rangle = \sum_{f(x)}\frac{\sqrt{|f^{-1}(f(x))|}}{2^{n/2}}|f(x)\rangle|0\rangle$. Similarly to the proof of Theorem 3:

$$\begin{aligned}
|\langle Q_n|C_n\rangle|^2 &= |\textstyle\sum_{f(x)}\frac{|f^{-1}(f(x))|}{2^n}a_{f(x)}|^2 \\
&= |\textstyle\frac{1}{2^n}\sum_{x\in\{0,1\}^n} a_{f(x)}|^2 \\
&\geq |\textstyle\frac{1}{2^n}\sum_{x\in\{0,1\}^n} a^2_{f(x)}|^2 \\
&> (1-1/p(n))^2 > 1-\epsilon\,,
\end{aligned}$$

where $\epsilon = \frac{2}{p(n)} - \frac{1}{p^2(n)}$. This is a contradiction and hence, f is a quantum distributionally one-way function. □

4.3 From quantum distributionally one-way functions to quantum one-way functions

In the classical setting, Impagliazzo and Luby [10] proved that the existence of a distributionally one-way function implies the existence of a one-way function. In this section, we describe the main ideas of their construction and show how to prove the equivalent result in the quantum setting.

Theorem 5 *If there exists a quantum distributionally one-way function then there exists a quantum one-way function.*

4.3.1 The Impagliazzo and Luby construction

Let $f : \{0,1\}^* \to \{0,1\}^*$ be a candidate distributionally one-way function. Then, there exists a function g such that an inverter I for g implies the existence of a sampler S for f. Let us fix the size of input to n, this can be done as we are working with a uniform circuit family. More precisely, Impagliazzo and Luby showed that if there exists an inverter I for g that succeeds with probability $1 - \delta^2/n$, then there exists a sampler S for f, such that the distributions $(S(f(x)), f(x))$ and $(x, f(x))$ are $O(\delta)$-close in total variation distance (δ is the inverse of a large polynomial). Without loss of generality, the inverter for g outputs $\perp$ when it's given as input something which is not in the image of g.

Now, let us try to describe the main ideas of their construction. First, assume that for a given $f(x)$ we know the size of the preimage $|f^{-1}(f(x))|$ and let $k = \lfloor \log |f^{-1}(f(x))| \rfloor + O(\log n)$. We define the function g as

$$g(x, h_k) = (f(x), h_k, h_k(x))\,.$$

In other words, g takes as inputs an x and a random string h_k which can be thought of as a random universal hash function $h_k : \{0,1\}^n \to \{0,1\}^k$. The output of g is the value $f(x)$, the random universal hash function and the output of the hash function on x.

There are two observations to be made about the hash function. First, since the range of the hash function is slightly larger than the number of x's in the preimage of $f(x)$, with high probability the mapping $x \mapsto h_k(x)$ for $\{x \in f^{-1}(f(x))\}$ is a one-to-one mapping. This implies, that if we could pick uniformly an element from the set $\{h_k(x) | x \in f^{-1}(f(x))\}$ then the inverter of g on input $(f(x), h_k, h_k(x))$ would return a uniform $x \in f^{-1}(f(x))$.

Second, it's indeed possible to pick a uniform element of the set $\{h_k(x) | x \in f^{-1}(f(x))\}$. Since the range of the hash function is not too much larger than the size of the preimage of $f(x)$, if we pick a random element $r_k \in \{0,1\}^k$, then with non negligible probability it holds that $r_k = h_k(x)$ for some $x \ \in f^{-1}(f(x))$. By repeating the process a polynomial number of times, we can achieve high success probability.

The above two properties enable one to prove that, when one knows the size of the preimage of $f(x)$, the following procedure is a sampler for $f(x)$:

Partial Sampler PS(f(x),k)

```
Repeat a polynomial number of times
    Pick a random hash function $h_k$ and $r_k \in \{0,1\}^k$.
    If $I(f(x), h_k, r_k) \neq \perp$ then output it and exit.
Output $\perp$ .
```

The remaining issue is that the sampler doesn't know the size of the preimage of $f(x)$. Suppose we pick the range of the hash function to be much larger than the actual size of the preimage of $f(x)$. Then the above sampler outputs $\perp$ with very high probability. However, conditioned on it producing an output x, then this x is still almost uniformly distributed in $\{f^{-1}(f(x))\}$. This is true since the hash function randomly hashes $|f^{-1}(f(x))|$ values of x to a much larger range, and therefore, the mapping is with very high probability one-to-one.

Hence, we can construct a sampler for f by starting with the largest possible value for the range of the hash function and keep decreasing it until there is an outcome:

Sampler S(f(x))

```
  For $j = n + O(\log n)$ to $O(\log n)$:
      If $PS(f(x), j) \neq \perp$ output it and exit.
  Output $\perp$.
```

Impaglazzo and Luby show that the overall errors of the sampler S are at most $O(\delta)$, i.e. inverse polynomially small. Their analysis is based on the following claims proved in [10]:

1. The errors from the fact that the hash function h_k is not truly one-to-one are negligible for all values $j \geq k$.

2. Since the inverter for g is not perfect, the sampler doesn't work for every $f(x)$ but for $f(x)$'s that correspond to at least a $(1-\delta)$ fraction of the x's (we call such $f(x)$ 'good'). This is sufficient, since the total error from the rest of the inputs is at most $O(\delta)$. Moreover, for these 'good' $f(x)$'s the inverter I of g succeeds with probability $(1 - O(\delta))$.

3. In the case of a 'good' $f(x)$, if the sampler produces an output for a $j \geq k$, then this x is guaranteed to be almost uniform (i.e. the distributions $(S(f(x)), f(x))$ and $(x, f(x))$ have $O(\delta)$ total variation distance).

4. In the case of a 'good' $f(x)$, the probability that the sampler actually produces an output for $j \geq k$ is, in fact, very close to 1 (i.e. $1 - O(\delta)$).

We will also need the following precise lemma from [10]

Lemma 1 *[10] Let p_j be the probability that the Partial Sampler $PS(f(x), j)$ produces a legal output. Then, for all $j \geq k = \lfloor \log |f^{-1}(f(x))| \rfloor + \log n$*

$$(1 - o(1)) \left(1 - \left(\frac{1}{n}\right)^{2^{k-j}}\right) \leq p_j \leq 1 - \left(\frac{1}{n}\right)^{2^{k-j}} .$$

4.3.2 The construction of the Quantum Sampler

Here, we reproduce the Impagliazzo and Luby construction in the quantum setting. Most of the analysis remains the same and hence we do not repeat all the details, however we highlight the places where the analysis differs.

As before, let $f : \{0,1\}^* \to \{0,1\}^*$ be the candidate quantum distributionally one-way function, fix the input size to be n, and define $g(x, h_k) = (f(x), h_k, h_k(x))$. Assuming that we have a quantum inverter I for g, our goal is to construct a quantum sampler for f, namely the following unitary

$$\text{QSampler: } |f(x)\rangle|0\rangle \mapsto a_{f(x)}|f(x)\rangle|H_{f(x)}\rangle + b_{f(x)}|G_{f(x)}\rangle,$$

where $\frac{1}{2^n}\sum_{x\in\{0,1\}^n} a^2_{f(x)} \geq 1-o(1)$ and $|H_{f(x)}\rangle = \frac{1}{\sqrt{|f^{-1}(f(x))|}}\sum_{x\in f^{-1}(f(x))}|x\rangle$.

Similar to the classical case, we restrict ourselves to 'good' $f(x)$'s. First, we assume that for a given $f(x)$ we know the size of the preimage $|f^{-1}(f(x))|$ and $k = \lfloor \log|f^{-1}(f(x))|\rfloor + O(\log n)$. The following unitary operations are the quantum equivalents of picking a random universal hash function h_k and a random string $r_k \in \{0,1\}^k$ and are efficiently constructible:

$$Q \ : \ |k\rangle|0\rangle \to |k\rangle\frac{1}{\sqrt{|H|}}\sum_{h_k}|h_k\rangle \quad , \quad B \ : \ |k\rangle|0\rangle \to |k\rangle\frac{1}{2^{k/2}}\sum_{r_k\in\{0,1\}^k}|r_k\rangle,$$

where H is the number of possible universal hash functions $h_k : \{0,1\}^n \to \{0,1\}^k$[1]. From what follows we drop the above normalization factors.

Let us, now, define a perfect inverter I for g. The inverter, given an input $(f(x), h_k, h_k(x))$, such that there exists a unique $x \in f^{-1}(f(x))$ mapped to $h_k(x)$, always returns x and given an input $(f(x), h_k, s_k)$, such that there is no $x \in f^{-1}(f(x))$ mapped to s_k, returns an "error" symbol.

$$I \ : \ \left\{ \begin{array}{lcl} |f(x)\rangle|h_k\rangle|h_k(x)\rangle|0\rangle|0\rangle & \to & |f(x)\rangle|h_k\rangle|h_k(x)\rangle|x\rangle|0\rangle \\ |f(x)\rangle|h_k\rangle|s_k\rangle|0\rangle|0\rangle & \to & |f(x)\rangle|h_k\rangle|s_k\rangle|0\rangle|1\rangle \end{array} \right\}.$$

The last register-input to I acts as the "error flag". Note first, that by the analysis of [10] the errors from the fact that h_k may not be one-to-one are small. Also, the inverter of g is not guaranteed to be perfect but only work with probability $1-O(\delta)$, but these errors are also small (i.e. inverse polynomially small). For clarity of exposition, in our description of the quantum sampler we are going to use the perfect inverter of g and assume that h_k is a one-to-one mapping.

Last, recall that h_k is an efficient hash function and hence, having $|h_k\rangle$ and $|x\rangle$ one can efficiently compute $|h_k(x)\rangle$ and construct the following unitary:

$$T : |h_k\rangle|h_k(x)\rangle|x\rangle \quad \to \quad |h_k\rangle|0\rangle|x\rangle\,.$$

We are now ready to define a partial quantum sampler for $f(x)$, when we know the size of its preimage. Denote by $p_{k,f(x)}$ the probability that the perfect inverter would return a legal output for given values of $f(x)$ and k. In the following, we drop the second subscript and have $p_k = p_{k,f(x)}$.

Partial Quantum Sampler PQS(f(x),k)

$$|f(x)\rangle|k\rangle|0\rangle|0\rangle|0\rangle|0\rangle$$

$$\overset{Q_3\otimes B_4}{\to} \quad |f(x)\rangle|k\rangle\sum_{h_k,r_k}|h_k\rangle|r_k\rangle|0\rangle|0\rangle \tag{i}$$

$$\overset{I_{1,3,4,5,6}}{\to} \quad \sqrt{p_k}|f(x)\rangle|k\rangle\sum_{h_k,h_k(x)}|h_k\rangle|h_k(x)\rangle|x\rangle|0\rangle + \sqrt{1-p_k}|f(x)\rangle|k\rangle\sum_{h_k,s_k}|h_k\rangle|s_k\rangle|0\rangle|1\rangle \tag{ii}$$

$$\overset{T_{3,4,5}}{\to} \quad \sqrt{p_k}|f(x)\rangle|k\rangle\sum_{h_k}|h_k\rangle|0\rangle\sum_{x\in f^{-1}(f(x))}|x\rangle|0\rangle + \sqrt{1-p_k}|f(x)\rangle|k\rangle\sum_{h_k,s_k}|h_k\rangle|s_k\rangle|0\rangle|1\rangle \tag{iii}$$

$$\overset{Q_3^\dagger}{\to} \quad \sqrt{p_k}|f(x)\rangle|k\rangle|0\rangle|0\rangle|H_{f(x)}\rangle|0\rangle + \sqrt{1-p_k}|f(x)\rangle|k\rangle|G_{f(x),k}\rangle|1\rangle\,, \tag{iv}$$

[1] In fact, similar to the classical case one has to use a polynomial number of independent universal hash functions instead of one.

where $|H_{f(x)}\rangle = \frac{1}{\sqrt{|f^{-1}(f(x))|}} \sum_{x \in f^{-1}(f(x))} |x\rangle$. In the first step, we construct a uniform superposition of all possible hash functions h_k and random strings $r_k \in \{0,1\}^k$. In the second step, we perform the Inverter of g. Assuming that the inverter is perfect and the mapping $x \mapsto h_k(x)$ is truly one-to-one, then the state is exactly the one in (ii). The first term corresponds to the strings $r_k \in \{0,1\}^k$ such that $r_k = h_k(x)$ for a unique $x \in f^{-1}(f(x))$ and this happens with probability p_k. The second term corresponds to the rest of the strings. In the third step, we uncompute $h_k(x)$ and in the last step we uncompute the superposition of h_k. The final state in the perfect case consists of two terms. The first one is $|f(x)\rangle|k\rangle|H_{f(x)}\rangle$, where the third register contains a uniform superposition of the preimages of $f(x)$ and the second term denotes that the Sampler has failed ("error flag" register is 1). The norm of the first term is p_k, which is the probability that the inverter outputs a legal output for the given values $k, f(x)$.

Our partial quantum sampler imitates exactly the Impagliazzo and Luby one and hence their analysis implies exactly that conditioned on our sampler not failing, the actual state produced at the end is very close to the state $|f(x)\rangle|k\rangle|H_{f(x)}\rangle$. Moreover, since we picked $k = \lfloor \log |f^{-1}(f(x))| \rfloor + O(\log n)$ the norm (p_k) of the term $|f(x)\rangle|k\rangle|H_{f(x)}\rangle$ is not negligible.

Though the classical and quantum partial samplers seem identical, there is, in fact, a difference. In the above procedure, for superposition inputs, different values of $|k\rangle$ and $|f(x)\rangle$ get entangled and so the naive way of implementing the classical sampler $S(f(x))$ as a quantum circuit will fail. This can be overcome by applying the classical procedure in a "clean" way *i.e.* garbage-free where the garbage in this case is the $|k\rangle$ register. However, since the classical procedure consists of a "While Loop" (a loop with an exit command) the procedure of un-computing the garbage is more demanding than the usual case where one deals with a "For Loop". To do so, instead of implementing the while loop of the classical algorithm we prepare a weighted superposition of all k's as an ancilla register which then leads to our garbage-free quantum sampler.

First we construct a partial ancilla preparation circuit for the case where the value of k is known. Basically, we apply our partial quantum sampler twice in order to "clean" the register that contains $|H_{f(x)}\rangle$, while copying the "error flag" in between.

Partial Ancilla Preparation, PAP(f(x),k)

$$\begin{aligned}
& |f(x)\rangle|k\rangle|0\rangle|0\rangle|0\rangle \\
\overset{PQS(f(x),k)}{\longrightarrow} \quad & \sqrt{p_k}|f(x)\rangle|k\rangle|H_{f(x)}\rangle|0\rangle|0\rangle + \sqrt{1-p_k}|f(x)\rangle|k\rangle|G_{f(x),k}\rangle|1\rangle|0\rangle \\
\overset{(\text{ctrl}-\text{NOT})_{4,5}}{\longrightarrow} \quad & \sqrt{p_k}|f(x)\rangle|k\rangle|H_{f(x)}\rangle|0\rangle|0\rangle + \sqrt{1-p_k}|f(x)\rangle|k\rangle|G_{f(x),k}\rangle|1\rangle|1\rangle \\
\overset{PQS(f(x),k)^\dagger}{\longrightarrow} \quad & \sqrt{p_k}\Big(\sqrt{p_k}|f(x)\rangle|k\rangle|0\rangle|0\rangle + \sqrt{1-p_k}|f(x)\rangle|k\rangle|G'\rangle\Big)|0\rangle + \\
& \sqrt{1-p_k}\Big(\sqrt{1-p_k}|f(x)\rangle|k\rangle|0\rangle|0\rangle + \sqrt{p_k}|f(x)\rangle|k\rangle|G''\rangle\Big)|1\rangle \\
= \quad & |f(x)\rangle|k\rangle|0\rangle|0\rangle\Big(p_k|0\rangle + (1-p_k)|1\rangle\Big) + \\
& \sqrt{p_k(1-p_k)}(|f(x)\rangle|k\rangle|G'\rangle|0\rangle + |f(x)\rangle|k\rangle|G''\rangle|1\rangle)\,.
\end{aligned}$$

We rewrite the transformation $PAP(f(x),k)$ by adding a flag register that is 1 when the third register is not $|0\rangle$ and also for clarity we do not write the third the fourth registers

$$PAP(f(x),k) : |f(x)\rangle|k\rangle|0\rangle|0\rangle \mapsto |f(x)\rangle|k\rangle\Big(p_k|0\rangle + (1-p_k)|1\rangle\Big)|0\rangle + |G_{f(x),k}\rangle|1\rangle\,.$$

We now describe a circuit for the ancilla preparation when we start our algorithm for a large value of k and decrease it at each step by one. For clarity, the quantum registers contain the values n to 1 instead of $n + O(\log n)$ to $O(\log n)$ which are the real values for which the Sampler is run. Furthermore, all the operations are controlled by the "error flag" being the last register.

Ancilla Preparation AP(f(x))

$$\begin{array}{cl}
 & |f(x)\rangle|n\rangle|0\rangle|n-1\rangle|0\rangle\cdots|1\rangle|0\rangle|0\rangle \\
\overset{PAP_{1,2,3}}{\rightarrow} & |f(x)\rangle|n\rangle\Big(p_n|0\rangle + (1-p_n)|1\rangle\Big)|n-1\rangle|0\rangle\cdots|1\rangle|0\rangle|0\rangle + |G\rangle|1\rangle \\
\overset{\text{ctr}_3-PAP_{1,4,5}}{\rightarrow} & |f(x)\rangle|n\rangle p_n|0\rangle|n-1\rangle|0\rangle\cdots|1\rangle|0\rangle|0\rangle + \\
 & |f(x)\rangle|n\rangle(1-p_n)|1\rangle|n-1\rangle\Big(p_{n-1}|0\rangle + (1-p_{n-1})|1\rangle\Big)\cdots|1\rangle|0\rangle|0\rangle + \\
 & |G'\rangle|1\rangle \\
\overset{\text{ctr}_5-PAP_{1,6,7}}{\rightarrow} & |f(x)\rangle|n\rangle p_n|0\rangle|n-1\rangle|0\rangle\cdots|1\rangle|0\rangle|0\rangle \\
+ & |f(x)\rangle|n\rangle(1-p_n)|1\rangle|n-1\rangle p_{n-1}|0\rangle\cdots|1\rangle|0\rangle|0\rangle \\
+ & |f(x)\rangle|n\rangle(1-p_n)|1\rangle|n-1\rangle(1-p_{n-1})|1\rangle|n-2\rangle\Big(p_{n-2}|0\rangle + (1-p_{n-2})|1\rangle\Big)\cdots|1\rangle|0\rangle|0\rangle \\
+ & |G''\rangle|1\rangle \\
\rightarrow & \\
\vdots & \\
\rightarrow & |f(x)\rangle|n\rangle\cdots|1\rangle\sum_j q_j|j\rangle|0\rangle + |G_f\rangle|1\rangle\,,
\end{array}$$

where $q_j = \prod_{i=1}^{j-1}(1-p_i)p_j$ is the probability that the sampler PQS succeeds at the j-th round and has failed on all previous rounds. Since the registers that contain the values n to 1 are not entangled with $f(x)$ we can ignore them and have

$$AP : |f(x)\rangle|0\rangle|0\rangle \mapsto |f(x)\rangle\sum_j q_j|j\rangle|0\rangle + |G_f\rangle|1\rangle\,.$$

Now we present the garbage-free quantum sampler for the general case where we don't know the size of the pre-image for a given $f(x)$. For clarity, we don't explicitly write down all the necessary $|0\rangle$ registers in every step and also all the unitaries are performed when the "error flag" is 0.

Quantum Sampler, QS(f(x))

$$\begin{aligned}
& |f(x)\rangle|0\rangle|0\rangle \\
\overset{AP}{\rightarrow} \quad & |f(x)\rangle \sum_j q_j |j\rangle|0\rangle + |G^1_{f(x)}\rangle|1\rangle \\
\overset{PQS}{\rightarrow} \quad & |f(x)\rangle \sum_j q_j |j\rangle \Big(\sqrt{p_j}|H_{f(x)}\rangle|0\rangle + \sqrt{1-p_j}|G^2_{f(x),j}\rangle|1\rangle \Big)|0\rangle + |G^1_{f(x)}\rangle|1\rangle \\
= \quad & |f(x)\rangle \sum_j q_j \sqrt{p_j}|j\rangle|H_{f(x)}\rangle|0\rangle + |G^3_{f(x)}\rangle|1\rangle \\
\overset{AP^\dagger}{\rightarrow} \quad & \sum_j q_j^2 \sqrt{p_j}|f(x)\rangle|H_{f(x)}\rangle|0\rangle + |G^4_{f(x)}\rangle|1\rangle\,,
\end{aligned}$$

where the last step follows from the unitarity of $AP^\dagger$, *i.e.* from

$$\begin{aligned}
|f(x)\rangle \sum_j q_j |j\rangle|0\rangle + |G^1_{f(x)}\rangle|1\rangle \quad & \overset{AP^\dagger}{\rightarrow} \quad |f(x)\rangle|0\rangle|0\rangle \\
|f(x)\rangle \sum_j q_j \sqrt{p_j}|j\rangle|0\rangle \quad & \overset{AP^\dagger}{\rightarrow} \quad \alpha|f(x)\rangle|0\rangle|0\rangle + \beta|G\rangle|1\rangle\,.
\end{aligned}$$

We conclude that $\alpha = \Big(\langle f(x)| \sum_j q_j \langle j|\langle 0| + \langle G^1_{f(x)}|\langle 1|\Big)\Big(|f(x)\rangle \sum_j q_j \sqrt{p_j}|j\rangle|0\rangle\Big) = \sum_j q_j^2 \sqrt{p_j}$.

It remains to compute the success probability of the Garbage-free Quantum Sampler, i.e to calculate the square of the sum $\sum_j q_j^2\sqrt{p_j}$. Proving that it is $1-o(1)$, then we obtain a contradiction to f being a quantum distributionally one-way function and hence we conclude that g is a quantum one-way function. Note that the success probability of the Impagliazzo and Luby sampler is $\sum_j q_j$ and Lemma 1 proves that for $j \geq k = \lfloor \log |f^{-1}(f(x))| \rfloor + O(\log n)$ one obtains $\sum_{j\geq k} q_j = 1 - o(1)$. Here, we have a slightly more complicated expression that can still be shown to be large.

Lemma 2 *The procedure QS is a quantum sampler for f with probability $1-o(1)$, i.e.* $\sum_j q_j^2 \sqrt{p_j} \geq 1 - o(1)$.

Proof. We are going to bound this sum by showing that there exists a particular m for which the term $q_m^2\sqrt{p_m}$ is $1 - o(1)$. In order to do so, we slightly change the procedure we described above and instead of starting from $j = n + \log n$ and decreasing j at each step by 1, we pick a random offset $r \in [\log\log n]$, start with $j = n + \log n + r$ and decrease j at each step by $\log\log n$. Also, let $k = \lfloor \log |f^{-1}(f(x))| \rfloor + \log n$. The values of p_j for different j's can be estimated using Lemma 1

$$(1 - o(1)) \left(1 - \left(\frac{1}{n}\right)^{2^{k-j}}\right) \leq p_j \leq 1 - \left(\frac{1}{n}\right)^{2^{k-j}}\,.$$

First, we bound the probability that the algorithm fails in all the rounds for $j = n + \log n + r$ to $j \geq k + (1+\epsilon)\log\log n$, where for example $\epsilon = \frac{1}{\log\log\log n}$. Note that at each round j is decreased by $\log\log n$. Since p_j is a decreasing function of j the minimum probability of failure is obtained for $r = 0$ and is

$$\begin{aligned}\prod_{j=k+(1+\epsilon)\log\log n}^{n+\log n}(1-p_j) &\geq \prod_{j=k+(1+\epsilon)\log\log n}^{n+\log n}\left(\frac{1}{n}\right)^{2^{k-j}} = \prod_{\ell\geq 1}\left(\frac{1}{n}\right)^{2^{-(\ell+\epsilon)\log\log n}}\\ &= \prod_{\ell\geq 1}\left(\frac{1}{n}\right)^{(\log n)^{-(\ell+\epsilon)}} = \left(\frac{1}{n}\right)^{\sum_{\ell\geq 1}(\log n)^{-(\ell+\epsilon)}}\\ &\approx \left(\frac{1}{n}\right)^{\frac{1}{(\log n)^{1+\epsilon}-1}} = 1-o(1)\,.\end{aligned}$$

Moreover, for any $j \in [k+\epsilon\log\log n, k+(1-\epsilon)\log\log n]$, we have that

$$p_j \geq 1-\left(\frac{1}{n}\right)^{2^{-(1-\epsilon)\log\log n}} = 1-\left(\frac{1}{n}\right)^{(\log n)^{-(1-\epsilon)}} = 1-\left(\frac{1}{2}\right)^{(\log n)^{\epsilon}} = 1-o(1)\,.$$

Since we pick a random initial offset $r \in [1, \log\log n]$, then with probability $(1-2\epsilon)$ over r the algorithm is run for an $m \in [k+\epsilon\log\log n, k+(1-\epsilon)\log\log n]$. In this case, we have already shown that $p_m = 1-o(1)$ and, moreover, for all previous rounds we have $j \geq k+(1+\epsilon)\log\log n$ and hence the probability of failure is $\prod_{j>m}(1-p_j) = 1-o(1)$. To sum up, with probability $(1-2\epsilon) = 1-o(1)$ our algorithm is run for an m such that

$$\sum_j q_j^2\sqrt{p_j} \geq q_m^2\sqrt{p_m} = \prod_{j>m}(1-p_j)^2 p_m^{5/2} = 1-o(1)\,,$$

and therefore the overall success probability of the algorithm is $1-o(1)$. □

This concludes the proof of Theorem 5 and together with Theorem 4 we have

Theorem 6 *Assume for a classical circuit C, which computes a many-to-one function, the corresponding CQS problem is hard , i.e. there exists no poly($|C|$) size quantum circuit implementing QS_C. Then there exists a quantum one-way function.*

5 Statistical Zero Knowledge and quantum one-way functions

The CQS problem has an interesting connection to the classical complexity class of Statistical Zero Knowledge (SZK) languages:

Theorem 7 *[2] Any language $\mathcal{L} \in \mathrm{SZK}$ can be reduced to a set of instances of the CQS problem.*

The proof is based on a reduction of the following SZK-complete problem to a quantum sampling problem.

Definition 8 *[15] Consider two constants $0 \leq \beta < \alpha \leq 1$ such that $\alpha^2 > \beta$. Statistical Difference ($SD_{\alpha,\beta}$) is the promise problem of deciding for any two given classical circuits C_0 and C_1 whether their output distributions are close to or far from each other, i.e. whether:*

$$||D_{C_0} - D_{C_1}|| \;\geq\; \alpha \quad \textit{or} \quad ||D_{C_0} - D_{C_1}|| \;\leq\; \beta\,.$$

It is not hard to see that the above problem can be reduced to the problem of quantum sampling the circuits C_0 and C_1. Indeed, if one could efficiently construct the quantum samples $|C_0\rangle$ and $|C_1\rangle$, then, by performing a SWAP-test, one could decide whether the two circuit distributions are close to or far from each other. Equivalently, the above problem can be reduced to the problem of quantum sampling the circuit $C \triangleq C_0 \otimes C_1$, since a SWAP-test would again decide whether the two circuit distributions are close or far. Based on this result, we obtain the quantum analog of Ostrovsky's result [14]:

Theorem 8 *Assume there exists a language $\mathcal{L} \in \mathrm{SZK} \setminus \mathrm{AvgBQP}$, then quantum one-way functions exist.*

Proof. Assume $\mathcal{L} \in \mathrm{SZK} \setminus \mathrm{AvgBQP}$. For every input size n, let $\{C^x\}_{x\in\{0,1\}^n}$ be the set of classical circuits which decide L via reduction to the complete language in Definition 8. Denote by $m = poly(n)$ the size of the input to the circuits from this set. Since the language $\mathcal{L}$ is not in AvgBQP, for any sufficiently large input size n, there exists a samplable distribution $\mathcal{D}_n$ such that for $x \sim \mathcal{D}_n$, the language $\mathcal{L}$ can not be decided with high probability with a polynomial time quantum algorithm. Equivalently there is no polynomial quantum algorithm that produces a quantum sample of C^x for an average $x \sim \mathcal{D}_n$. We can assume this distribution to be uniform [9] and hence we have a uniform family of sets of circuits $\{\{C^x\}_{x\in\{0,1\}^n}\}_{n\in\mathbf{N}}$, such that for any polynomial time quantum algorithm Q, any constant $\epsilon \in [0, 1/2)$, and all sufficiently large $n \in \mathbf{N}$

$$Q : |x\rangle|0\rangle \mapsto c_x|x\rangle|C^x\rangle + d_x|G_x\rangle\,,$$

with

$$\frac{1}{2^n}\sum_x |(Q(|x\rangle|0\rangle)\ ,\ |x\rangle|C^x\rangle)|^2 = \frac{1}{2^n}\sum_x |c_x|^2 < 1-\epsilon\,.$$

We define the function $f_C : \{0,1\}^* \to \{0,1\}^*$ such that $f_C : (x, y) \mapsto (x, C^x(y))$ and prove that it is a quantum one-way function. We assume that f is one-to-one otherwise from Theorem 5, we can obtain the same result. Suppose that the function f_C is not one-way, then there exists an inverter such that

$$I : |f(x,y)\rangle|0\rangle|0\rangle \mapsto a_{f(x,y)}|f(x,y)\rangle|x\rangle|y\rangle + b_{f(x,y)}|G_{f(x,y)}\rangle\,,$$

or equivalently

$$I : |x\rangle|C^x(y)\rangle|0\rangle \mapsto a_{f(x,y)}|x\rangle|C^x(y)\rangle|y\rangle + b_{f(x,y)}|G_{f(x,y)}\rangle\,,$$

where $\frac{1}{2^{n+m}}\sum_{x,y} a^2_{f(x,y)} \geq 1 - \frac{1}{p(n)}$ (the average is taken over x and y) and the $a_{f(x,y)}$'s are positive. We start from a uniform superposition of all y and use the inverter to create a circuit that is a good-on-average quantum sampler (similar to the proof of Theorem 3):

$$\begin{array}{lll} |x\rangle\frac{1}{2^{m/2}}\sum_y |y\rangle|0\rangle & \to_{U_f} & |x\rangle\frac{1}{2^{m/2}}\sum_y |y\rangle|C^x(y)\rangle \\ & \to_{\mathrm{SWAP}} & |x\rangle\frac{1}{2^{m/2}}\sum_y |C^x(y)\rangle|y\rangle \\ & \to_I & |x\rangle\frac{1}{2^{m/2}}\sum_y (a_{f(x,y)}|C^x(y)\rangle|0\rangle + b_{f(x,y)}|G'_{f(x,y)}\rangle) \equiv |x\rangle|T_m\rangle\,, \end{array}$$

and hence for an average x

$$\begin{aligned} \frac{1}{2^n}\sum_x |\langle x|\langle T_m||x\rangle|C^x\rangle|^2 &= \frac{1}{2^n}\sum_x |\frac{1}{2^m}\sum_y a_{f(x,y)}|^2 \ \geq\ |\frac{1}{2^{n+m}}\sum_{x,y} a_{f(x,y)}|^2 \\ &\geq |\frac{1}{2^{n+m}}\sum_{x,y} a^2_{f(x,y)}|^2 \ \geq\ (1-\frac{1}{p(n)})^2 \ \geq\ 1-\epsilon\,. \end{aligned}$$

This is a contradiction and hence the function f_C is a quantum one-way. □

6 Conclusions

In this paper we prove that the existence of any problem in SZK which is hard-on-average for a quantum computer, implies the existence of quantum one-way functions. Our proofs go through the problem of quantum sampling. Aharonov and Ta-Shma cast many important problems as quantum sampling problems and described a possible way for attacking them. It is, hence, very interesting to investigate the real hardness of quantum sampling. We already know that if SZK $\not\subseteq$ AvgBQP then there exist hard instances of quantum sampling. Under what other assumptions can one prove the existence of hard instances of the CQS problem and consequently quantum one-way functions?

Furthermore, we saw that our candidate one-way problems include some of the most notorious problems in quantum computing, like Graph Non-Isomorphism and approximate Closest Lattice Vector problem. Could we construct one-way functions from other problems, such as the hidden subgroup problem in the dihedral or other non-abelian groups?

Last, Watrous [16] proved that computational zero knowledge for NP is implied by the existence of quantum one-way permutations. What other implications does the existence of quantum one-way functions have?

Acknowledgements

We wish to thank Oded Regev, Ben Reichardt and Alain Tapp for useful discussions and Andrej Bogdanov for sharing with us his notes on [10]. EK was partially supported by the ARDA, MITACS, ORDCF, and CFI projects during her stay at University of Waterloo where this work was begun. IK gratefully acknowledges professor Peter w. Shor who has supported his research from a scholarly allowance provided from his appointment as the holder of the Henry Adams Morss and Henry Adams Morss, Jr. Professorship and from NSF CCF-0431787.

References

[1] M. Adcock and R. Cleve. A quantum Goldreich-Levin theorem with cryptographic applications. In *Proceedings of STACS03 – Symposium on Theoretical Aspect of Computer Sciences*, 2002.

[2] D. Aharonov and A. Ta-shma. Adiabatic quantum state generation and statistical zero knowledge. In *Proceedings of STOC02 – Symposium on the Theory of Computing*, 2001.

[3] C. Crépeau, F. Légaré, and L. Salvail. How to convert the flavor of a quantum bit commitment. In *Proceedings of EUROCRYPT01 – Advances in Cryptology*, 2001.

[4] I. Damgard, S. Fehr, and L. Salvail. Zero-Knowledge Proofs and String Commitments Withstanding Quantum Attacks. In *Proceedings of EUROCRYPT04 – Advances in Cryptology*, 2004.

[5] P. Dumais, D. Mayers, and L. Salvail. Perfectly concealing quantum bit commitment from any one-way permutation. In *Proceedings of EUROCRYPT00 – Advances in Cryptology*, 2000.

[6] O. Goldreich. *Foundations of Cryptography - Volume 1.* Cambridge University Press, 2001.

[7] D. Gottesman and I. Chuang. Quantum digital signatures. *arXiv.org e-Print quant-ph/0105032*, 2001.

[8] J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal of Computing*, 17:309, 1988.

[9] R. Impagliazzo and L. A. Levin. No better ways to generate hard np instances than picking uniformly at random. In *Proceedings of FOCS90 – Symposium on Foundations of Computer Science*, 1990.

[10] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *Proceedings of FOCS89 – Symposium on Foundations of Computer Science*, 1989.

[11] E. Kashefi, H. Nishimura, and V. Vedral. On quantum one-way permutations. *Quantum Information and Computation*, 2:379, 2002.

[12] A. Kawachi, H. Kobayashi, T. Koshiba, and R. H. Putra. Universal test for quantum one-way permutations. *Theoretical Computer Science*, 2-3:345, 2005.

[13] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[14] R. Ostrovsky One-way functions, hard on average problems and Statistical Zero Knowledge proofs. *IEEE Conference on Structure in Complexity Theory*, 1991

[15] A. Sahai and S. P. Vadhan. A complete promise problem for Statistical Zero Knowledge. In *Proceedings of FOCS97 – Symposium on Foundations of Computer Science*, 1997.

[16] J. Watrous. Zero knowledge against quantum attacks. In *Proceedings of STOC06 – Symposium on Theory of Computing*, 2006.