On the Efficiency of Generic, Quantum Cryptographic Constructions

Keita Xagawa

Technology Innovation Institute, Abu Dhabi, United Arab Emirates

Abstract. One of the central questions in cryptology is how efficient generic constructions of cryptographic primitives can be. Gennaro, Gertner, Katz, and Trevisan [SIAM J. of Compt., 2005] studied the lower bounds of the number of invocations of a (trapdoor) one-way permutation in order to construct cryptographic schemes, e.g., pseudorandom number generators, digital signatures, and public-key and symmetric-key encryption.

Recently, quantum machines have been explored to construct cryptographic primitives other than quantum key distribution. This paper studies the efficiency of quantum black-box constructions of cryptographic primitives when the communications are classical. Following Gennaro et al., we give the lower bounds of the number of invocations of an underlying quantumly-computable quantum-one-way permutation when the quantum construction of pseudorandom number generator and symmetric-key encryption is weakly black-box. Our results show that the quantum black-box constructions of pseudorandom number generator and symmetric-key encryption do not improve the number of invocations of an underlying quantumly-computable quantum-one-way permutation.

Keywords: Quantum reduction · black-box construction · efficiency

1 Introduction

It is widely believed that showing the existence of (trapdoor) one-way permutations/functions is incredibly hard. If it is shown, then the long-standing open problem $P = NP$ is solved negatively, and we notice that we live in Minicrypt/Cryptomania of Impagliazzo’s five worlds [Imp95]. Cryptographers assume the existence of (trapdoor) one-way permutations/functions and construct various useful cryptographic schemes upon them.

Since cryptographic tools and protocols are used in the real world, the efficiency of the constructions is also an important target of studies. For example, Kim, Simon, and Tetali [KST99], Gennaro and Trevisan [GT00], and Gennaro, Gertner, and Katz [GGK03] (and their journal version [GGKT05]) studied the efficiency of cryptographic constructions based on general assumptions.

Example: pseudorandom generator from one-way permutation. As an example, let us consider the basic construction of pseudorandom generator (PRG) from one-way permutation (OWP) (See e.g., [KL20]): By using the Goldreich-Levin hardcore function [GL89], we can construct PRG: $\{0,1\}^\ell \to \{0,1\}^{\ell+k}$ from OWP: $\{0,1\}^n \to \{0,1\}^n$, where $\ell = 2n$. If we let the range of the hardcore function $\{0,1\}^{O(\ell n)}$, this basic construction requires $O(k/\lg(n))$-invocations of the underlying OWP in the black-box way to extend $k$-bits. Gennaro and Trevisan [GT00] showed that this is optimal up to constant factor; they
showed that if there exists a PRG of extension length \( k \) that invokes the underlying OWP \( o(k/\lg(n)) \)-times in a black-box way, then there exists unconditionally-secure PRG, which immediately implies the existence of unconditionally-secure OWF, \( \text{DistNP} \not\subseteq \text{AvgP} \), and \( P \neq NP \). \(^1\) \(^2\)

**Quantum adversary, quantum construction, and quantum reduction:** Cryptographic researches exploit the properties of quantum machines and channels to advance the classical counterparts. See, e.g., certified deletion [BI20, HMNY21] and multi-party quantum computation [BCKM21a, BCKM21b, GLSV21].

Here, we consider the moderate setting where the machines are quantum but the channels are classical, which is called the quantum-computation classical-communication (QC-CC) model. This model has the benefit that we can reuse strings (e.g., secret key, public key, ciphertext, and signature) since we can copy classical strings easily. While the channels are classical, the quantum power of computation would improve the constructions and reductions; for example, if the construction is quantum, we can factor an integer and solve the discrete logarithm problem in polynomial time, which is already exploited by Okamoto, Tanaka, and Uchiyama for construction [OTU00] and by Gentry for reduction [Gen10]. Moreover, Ananth, Gulati, Qian, and Yuen [AGQY22] constructed quantumly-computable secret-key encryption with classical keys/ciphertexts from pseudorandom state generator (PRS) [JLS18] which produces quantum states.

Let us turn back our example on PRG from OWP, where we consider post-quantum-secure OWP (qOWP). In the case of the generic construction of PRG, we already know that the above PRG construction using the quantum version of the Goldreich-Levin hardcore function [AC02, KY10] yields a similar upperbound for quantum-secure PRG from classical access to qOWP, while it improves the tightness. Our question is:

Can quantum access to qOWP improve the efficiency of the construction?

### 1.1 Our Contribution

In this paper, we give the lower bounds of the number of quantum invocations of underlying quantum-one-way permutation (qOWP) when the quantum construction of pseudorandom number generator (PRG) and symmetric-key encryption (SKE) is quantum-black-box. Our quantum lower bounds are asymptotically equivalent to those classical lower bounds in [GGKT05].

#### 1.1.1 OWP-to-PRG:

Roughly speaking, we show that if there exists a quantumly-computable PRG of extension length \( k \) that invokes the underlying qOWP secure against \( S \)-size quantum adversaries \( o(k/\lg(S)) \)-times in a quantum-black-box way, then there exists unconditionally-secure quantumly-computable PRG. This implies the existence of quantumly-computable qOWF (QC-qOWF in short), the proof of (QCMA, BQP-Samp) \( \not\subseteq \text{AvgBQP} \) in the average-case complexity, and the proof of BQP \( \neq \text{QCMA} \), which are quantum analogs of OWF, DistNP \( \not\subseteq \text{AvgP} \), and \( P \neq NP \).

Gennaro and Trevisan [GT00] first showed that a random permutation is one-way. They then observed that, if the number of queries is at most \( q \), then a random permutation can be simulated by random \( q \) strings, known as lazy sampling. Using this simulation, they constructed a new PRG that takes a random seed \( s \) and the random \( q \) strings and

\(^1\) Later, Holenstein and Sinha [HS12] improved the results as any black-box construction with fully-black-box reduction of PRG requires \( \Omega(n/\lg(n)) \) queries to (regular) OWF.

\(^2\) Reingold, Trevisan, and Vadhan [RTV06] also gave an unconditional black-box construction of PRG from OWF with at most one invocation of OWF. We note that the construction strongly depends on whether OWF exists or not.
outputs the output of PRG on the seed $s$ where the random permutation is simulated by the random $q$ strings. Thus, this implies unconditionally secure PRG if the extension length $k$ is longer than the length of the random $q$ strings.

Let us consider the quantum version: In order to adopt their idea to the quantum setting, we need two techniques; one is the quantum one-wayness of the random permutation; the other is the way to simulate quantumly-queried random permutation with classical strings.

For the latter, we need to show that the random permutation is one-way against quantum adversaries: Formally, due to a technical reason, we want to show that all but negligible $\delta$ fractions of random permutations over $\{0, 1\}^t$ cannot be invertible with probability at least $2^{-t/\epsilon}$ by any quantum adversary of size at most $2^{t/c}$ for some constant $c$, where the advantage of a quantum adversary $A$ against a permutation $f$ is defined as $\Pr_{x,A}[f(A(f(x))) = f(x)]$. (See Section 3.) There is research on quantum random permutation/function’s one-wayness (and more with advice), e.g., [Amb02, NABT15, HXY19, CLQ20, CGLQ20, Liu23]. While Ambainis [Amb02] and Nayebi et al. [NABT15] considered one-wayness of random permutations, their theorems and that of [NABT15] are given in the relation between $2^t$, the length of the advice $\alpha$, and the advantage $\epsilon$, e.g., $\epsilon = \tilde{O}(\alpha S + S^3)/2^t$ in [CGLQ20]. To give the bound in our wanted form, we give an explicit proof by combining lemmas in [GGKT05, NABT15, HXY19].

For the former, we need to emulate the random permutation quantumly queried $q$-times with compact classical strings. We here use the quantum random-function/random-permutation switching lemma [Zha12a, Zha15, Yue14] and Zhandry’s lemma that a random function can be simulated with $2q$-wise independent functions [Zha12b], which can be described by random $2q + 1$ strings.

Using those two ideas, we solve the above two problems and obtain the lower bound as we want.

1.1.2 OWP-to-SKE:

Roughly speaking, we show that if there exists a quantumly-computable SKE of message length $m$ and key length $k$ whose encryption and decryption algorithms invoke the underlying qOWP secure against $S$-size quantum adversaries $o((m - k)/\lg(S))$-times in a quantum-black-box way, then there exists unconditionally-secure quantumly-computable SKE. This implies the proof of $(\text{QCMA}, \text{BQP-Samp}) \not\subseteq \text{AvgBQP}$ and the proof of $\text{BQP} \neq \text{QCMA}$. If the underlying SKE computes a function, then it further implies the existence of QC-qOWF.

Gennaro et al. [GGKT05] showed the relation between one-way trapdoor permutation and public-key encryption and obtained the results for OWP and SKE as a corollary. For simplicity, we review the SKE version here. Gennaro et al. [GGKT05] first observed that the queried points of encryption and decryption may be different. Thus, the simulations in new encryption and decryption algorithms should share the information between the underlying encryption and decryption. This is done by encrypting the list of pairs of queries and answers using the one-time pad. The new encryption algorithm takes a message $M$ of length $m$ and a new secret key $K'$, which is parsed as secret key $K$, random $2q$ strings for the answers, and a secret key for the one-time pad; it outputs a ciphertext $C$ of $M$ by the underlying encryption algorithm with secret key $K$ and message $M$ and a ciphertext $C'$ of the list produced by the simulation of the random permutation. The new decryption algorithm takes a pair of ciphertexts $C$ and $C'$ and the new secret key $K'$; it decrypts the list from $C''$ and outputs a message $M'$ by using the underlying decryption algorithm with secret key $K$ and a ciphertext $C$ by simulating the random permutation with the list. The length of a new secret key is $k + O(q)\lg(S)$. If $m > k + O(q)\lg(S)$, then the new SKE
scheme is non-trivial, that is, not the one-time-pad, and unconditionally secure.

Let us consider the quantum setting: We again adopt the simulation of the random permutation by $2q$-wise independent hash function. We note that this simulation is the same in both encryption and decryption algorithms, and we have no need to send the list. The construction of a new SKE scheme becomes simple. As in the classical case, if $m > k + O(q) \lg(S)$, then there exists an unconditionally secure SKE with negligible decryption failure. Such an SKE scheme implies $(\text{QCMA}, \text{BQP-Samp}) \not\subseteq \text{AvgBQP}$ and $\text{BQP} \neq \text{QCMA}$. Roughly speaking, the secret key and message are the classical witness of QCMA, and the witness is verified by the decryption algorithm. As previously mentioned, if the SKE computes a function, then the SKE implies QC-qOWF.

1.1.3 Limitations

Gennaro et al. [GGKT05] showed the lower bounds of the numbers of the queries to construct a family of universal one-way hash functions (UOWHF) and weakly one-time-secure signature scheme from one-way permutation and the queries to construct a public-key encryption from trapdoor permutation. To upgrade those results into the quantum setting, there are several hurdles.

For OWP-to-UOWHF and OWP-to-Signature, we fail to adapt the lower bounds in the classical setting into the quantum setting because the proofs exploit input/output pairs of the ideal one-way permutation. Very roughly speaking, the proof construct unconditionally secure UOWHF or OWF whose input contains the random strings $y_i$'s returned by the ‘one-way permutation’ and the output contains the queries $x_i$'s made by UOWHF or the verification algorithm of the signature scheme and $y_i$'s. Constructing a proper UOWHF/OWF in the quantum setting is an interesting open problem.

For TDP-to-PKE, we fail at the first stone, the simulation of a TDP with a short classical description. As far as we know, this is a long-standing important open problem in this area.

1.2 Related works

Hosoyamada and Yamakawa studied the gap between collision-resistant hash function and one-way (trapdoor) permutations [HY20]. Austrin et al. studied the impossibility of quantum construction of key exchange from one-way permutations [ACC+22]. Chung, Lin, and Mahmoody showed that there is no quantum black-box construction of a quantum-computation and classical-communication (QCCC) non-interactive commitment scheme from OWP [CLM23].

1.3 Open Problems

As we discussed in above, the limit of the black-box OWP-to-UOWHF, OWP-to-Signature, and TDP-to-PKE constructions are left as an open problem.

Holenstein and Sinha [HS12] improved the parameter setting of the limit of the black-box OWP-to-PRG construction of Gennaro and Trevisan [GT00]. It is interesting whether we can obtain a similar quantum lower-bound to that in Holenstein and Sinha [HS12].

An extension to a quantum-computation and quantum-communication (QCQC)-model is also interesting. Let $\lambda$ be the security parameter. For example, [AQY22] showed that if we have appropriate PRS which outputs $d = O(\lg(\lambda))$ qubits, then we have pseudorandom functional state generator (PRFS) by calling PRS at most $O(2^d\lambda)$-times. It is very interesting whether it matches the lower bound or not.

We also leave showing a general non-trivial unconditionally-secure SKE scheme implies QC-qOWF as an interesting open problem. We also have a question on the complete
problems of (Q(C)MA, BQP-Samp) and (Q(C)MA, BQP-Comp), and the relation between them.

**Organization:** Section 2 reviews basic notions and notations. Section 3 gives a generic quantum hardness of one-way permutations. Section 4 and Section 5 give the lower bounds for PRGs and SKEs, respectively.

Appendix A reviews definitions of the average-case complexity class. Appendix B discusses the relation between unconditionally-secure non-trivial quantum SKE and the hard distributional problem in (QCMA, BQP-Samp).

## 2 Preliminaries

For a positive integer $N$, $[N]$ denotes the set $\{1, 2, \ldots, N\}$. We use $\log(\cdot) := \log_2(\cdot)$. For two finite sets $D$ and $R$, $\text{Func}(D,R)$ denotes a set of all functions whose domain is $D$ and whose range is $R$. For a finite set $F$, $U(F)$ denotes the uniform distribution over $F$. For a distribution $D$, $d \leftrightarrow D$ indicates we take a random sample $d$ according to $D$. For a finite set $F$, we often write $d \leftrightarrow F$ instead of $d \leftrightarrow U(F)$.

PPT (and QPT resp.) stands for probabilistic (quantum resp.) polynomial-time. For gates of quantum machines, we employ Toffoli ($CCX$), Hadamard ($H$), and $R_\pi/4$ gates as the basis of the universal computation due to Kitaev.

We say that a PPT oracle machine $P^{(\cdot)}$ is a black-box construction from OWP if for any OWP $\pi$, (1) $P^\pi$ satisfies the functionalities and (2) $P^\pi$ is secure against ever efficient adversary $A^\pi$. We consider its quantum version: We say that a QPT oracle machine $P^{(\cdot)}$ is a quantum black-box construction from qOWP if for any qOWP $\pi$, (1) $P^{(\pi)}$ satisfies the functionalities and (2) $P^{(\pi)}$ is secure against ever quantum efficient adversary $A^{(\pi)}$.

We review $k$-wise independent functions and their properties.

**Definition 1.** A family $F$ of functions $D \rightarrow R$ is said to be $k$-wise independent if for any $a, a_1, \ldots, a_{k-1} \in D$ and $b, b_1, \ldots, b_{k-1} \in R$ satisfying $b \neq b_t$ for all $t < k$, the following holds:

$$\Pr_{f \leftarrow F} [f(a) = b \mid f(a_1) = b_1 \land \cdots \land f(a_{k-1}) = b_{k-1}] = 1/|R|.$$  

**Lemma 1** ([Zha12b]). For any finite sets $D$ and $R$ of classical strings and $q$-quantum query algorithm $A$, we have

$$\Pr_{H \leftarrow \text{Func}(D,R)} [A^H] = 1 = \Pr_{H \leftarrow H_{2q}(D,R)} [A^H] = 1,$$

where $H_{2q}(D,R)$ is a family of $2q$-wise independent hash functions from $D$ to $R$.

## 2.1 One-way Permutation/Function

We define the quantum one-wayness of permutation and function in the concrete security style:

**Definition 2.** We say that a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ is $(S, \epsilon)$-quantumly-one-way or quantumly-one-way function (qOWF) if for every quantum circuit $A$ of size at most $S$, we have

$$\Pr_{x \leftarrow \{0,1\}^n} [f(A(f(x))) = f(x)] \leq \epsilon.$$  

When $f$ is given as a quantum oracle, we will denote $A^f$. We say if a function is $(S,1/S)$-qOWF, then we will call it $S$-qOWF.

If $f$ is a permutation, then we use the term quantumly-one-way permutation (qOWP).
We will denote the set of all permutations over \( \{0,1\}^n \) by \( \Pi_n \). For \( t \leq n \), we define \( \Pi_{t,n} \) the subset of \( \Pi_n \) such that the set of all permutations which keep \( n-t \) last bits unchanged; that is, \( \Pi_{t,n} := \{ \pi \in \Pi_n : \exists \hat{\pi} \in \Pi_t \text{ such that } \forall (a,b) \in \{0,1\}^t \times \{0,1\}^{n-t}, \pi(a,b) = (\hat{\pi}(a),b) \} \). We also denote the set of all functions over \( \{0,1\}^n \) by \( \Phi_n \) and define the set of all functions which keep the \( n-t \) last bits unchanged by \( \Phi_{n,t} \); that is, \( \Phi_{t,n} := \{ \phi \in \Phi_n : \exists \hat{\phi} \in \Phi_t \text{ such that } \forall (a,b) \in \{0,1\}^t \times \{0,1\}^{n-t}, \phi(a,b) = (\hat{\phi}(a),b) \} \).

The following theorem is a quantum version of the random-function and random-permutation (RF-RP) switching lemma shown by Zhandry [Zha15].

**Theorem 1** (The quantum RF-RP switching lemma ([Zha12a, Thm. 7.3] and [Zha15, Thm. 7])). Let \( A \) be an oracle-aided quantum algorithm that makes at most \( q \) quantum queries. Then we have

\[
\left| \Pr_{\pi \sim \Pi_n} [A^{\pi}(\cdot) = 1] - \Pr_{\phi \sim \Phi_n} [A^{\phi}(\cdot) = 1] \right| \leq (8\pi^2/3) \cdot (q^3/2^n).
\]

### 2.2 Pseudorandom Number Generator

A pseudorandom number generator is a QPT algorithm \( \text{PRG} \) which takes a seed \( s \in \{0,1\}^f \) as input and outputs a pseudorandom string \( y \in \{0,1\}^{f+k} \).

**Definition 3.** We say a function \( \text{PRG} : \{0,1\}^f \rightarrow \{0,1\}^{f+k} \) is an \( (S, \epsilon) \)-secure pseudorandom number generator (PRG) if for any quantum circuit \( A \) of size at most \( S \), we have

\[
\left| \Pr_{s \sim \{0,1\}^f} [A(\text{PRG}(s)) = 1] - \Pr_{z \sim \{0,1\}^{f+k}} [A(z) = 1] \right| \leq \epsilon.
\]

We call \( f \) as the seed length and \( k \) as the stretch length.

### 2.3 Symmetric-Key Encryption

The symmetric-key encryption (SKE) scheme for \( m \)-bit messages using \( k \)-bit keys is a pair of QPT algorithms \( \text{SKE} = (\text{Enc}, \text{Dec}) \);

- \( \text{Enc} \) takes a key \( K \in \{0,1\}^k \) and a message \( M \in \{0,1\}^m \) as input and outputs a ciphertext \( C \in \{0,1\}^m \).
- \( \text{Dec} \) takes a key \( K \in \{0,1\}^k \) and a ciphertext \( C \in \{0,1\}^m \) as input and outputs a message \( M \in \{0,1\}^m \) or the rejection symbol \( \bot \).

We require statistical correctness as follows: SKE is statistically correct if for any \( M \in \{0,1\}^m \), \( \Pr_{K \leftarrow \{0,1\}^k, C \leftarrow \text{Enc}(K, M)} [\text{Dec}(K, C) = M] \) is overwhelming.

We consider the basic security notion of SKE:

**Definition 4.** We say that \( \text{SKE} \) is \( (S, \epsilon) \)-secure if for any quantum circuit \( A \) of size at most \( S \) and for any messages \( M_0, M_1 \in \{0,1\}^m \) we have

\[
\left| \Pr_{K \leftarrow \{0,1\}^k, C \leftarrow \text{Enc}(K, M_0)} [A(C) = 1] - \Pr_{K \leftarrow \{0,1\}^k, C \leftarrow \text{Enc}(K, M_1)} [A(C) = 1] \right| \leq \epsilon.
\]

**Remark 1.** We remark that the above definitions can be extended into an interactive symmetric-key encryption. In the interactive case, we will consider a transcript between an encryption algorithm and a decryption algorithm as a ciphertext and denote \( C \leftarrow (\text{Enc}(K, M), \text{Dec}(K)) \). As Gennaro et al. [GGKT05], our result applies to the interactive case.
3 Hardness of Random Permutations

In what follows, we only consider purified quantum circuits with Toffoli (CCX), Hadamard (H), $R_{\pi/4}$, and $f$ gates, where $f$ will be a function. The following lemma gives the upperbound of the number of quantum circuits.

**Lemma 2.** Let $n \geq 3$. The number of quantum circuits of size $S$ having input/output length $n$, $(S-n)$-qubits ancilla, and oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$ is at most $(4S)^n(S+1)$.\hfill $\square$

**Proof.** Let us count the number of possible quantum circuits. A quantum circuit of size $S$ is specified as follows: For $i = 1, \ldots, S$, the $i$-th step is specified by the type of gates (CCX, H, $R_{\pi/4}$, and $f$) and the list of input-output qubits. The numbers of the possible list of qubits are at most $S \cdot (S-1) \cdots (S-n+1) = S!/(S-n)!$ because we consider $f$-gate with $f : \{0,1\}^n \to \{0,1\}^n$. In addition, the numbers of the possible output wires are at most $S!/(S-n)!$. Thus, the upperbound of the number of quantum circuits is at most $(4S)!/(S-n)!^S \cdot S!/(S-n)!^t \geq (4S)!/(S-n)!^{S+1} \leq (4S)^n(S+1)$.\hfill $\square$

### 3.1 Hardness of Random Permutations

Gennaro et al. [GGKT05] proved that a random $\pi \in \Pi_t$ is $2^{t/5}$-hard with probability at least $1 - 2^{-2^{t/2}}$ for sufficiently large $t$. We prove its quantum analog as follows:

**Theorem 2.** For sufficiently large $t$, a random $\pi \in \Pi_t$ is $2^{t/6}$-qOWP with probability at least $1 - 2^{-2^{t/6}}$.

**Corollary 1.** For sufficiently large $t \leq n$, a random $\pi \in \Pi_{t,n}$ is $2^{t/6}$-qOWP with probability at least $1 - 2^{-2^{t/6}}$.

**Remark 2.** Nayebi et al. [NABT15] showed the one-wayness of quantum random permutations with classical advice. Moreover, there are studies of more properties of quantum random functions/permutations with advice, e.g., [HXY19, CGLQ20, Liu23].

### 3.1.1 Preliminaries:

Before giving the proof, we review useful lemmas. The first one is the randomized compression lemma.

**Lemma 3** ([DTT10, Fact 8.1, Randomized Compression Lemma]. Suppose there is a randomized encoding procedure $E : X \times R \to Y$ and a decoding procedure $D : Y \times R \to X$. For any constant $c \in [0, 1]$, if $\Pr_{x \leftarrow X}[D(E(x, r), r) = x] \geq c$, then $|Y| \geq c|x|$.

The next one is taken from Hhan et al. [HXY19], while we adapt it slightly to consider permutations instead of keyed functions to permutations.

**Lemma 4** ([HXY19], Reduction to biased adversary, adapted). Let $\Pi$ be the set of all permutations over $[N]$ and let $X$ be its subset. Suppose that we have a quantum adversary $B$ of size $S$ whose number of queries is at most $Q$ such that, for all $\pi \in X$, $B$ inverts $\pi$ with advantage at least $\epsilon$, that is,

$$\Pr_{x \leftarrow [N]}[B^{(x)}(\pi(x)) = x] \geq \epsilon. \quad (1)$$

Then, we have a biased quantum adversary $A$ of size $\tilde{S}$ whose number of queries is at most $\tilde{Q}$ such that, for all $\pi \in X$, we have

$$\Pr_{x \leftarrow [N]}[\Pr_A[A^{(x)}(\pi(x)) = x] \geq 2/3] \geq \tilde{\epsilon}, \quad (2)$$

where $\tilde{S} = S \cdot O(1/\sqrt{\epsilon})$, $\tilde{Q} = Q \cdot O(1/\sqrt{\epsilon})$, and $\tilde{\epsilon} = \epsilon/2$. 
In order to verify how we can compute $\tilde{S}$, $\tilde{Q}$, and $\tilde{\epsilon}$, we include the proof of this lemma.

**Proof.** Fix $\pi \in X$. By applying the average argument to Equation 1, we have

$$\Pr_{x \leftarrow [N]} \left[ \Pr_{B} [B^{\pi}(x)] = x \right] \geq \epsilon/2 \geq \epsilon/2.$$

Let us consider $\tilde{B}, \tilde{B}^{-1}$, the unitaries corresponding to $B$ without final measurement. Using the amplitude amplification technique (see e.g., [BHMT00]), with $O(1/\sqrt{\epsilon/2})$ repetition of $\tilde{B}$ and $\tilde{B}^{-1}$, the success probability is amplified to $2/3$. The amplified circuit is called as $\tilde{A}$.

From the above arguments, we can set $\tilde{S} = S \cdot O(1/\sqrt{\epsilon/2})$, $\tilde{Q} = Q \cdot O(1/\sqrt{\epsilon/2})$, and $\tilde{\epsilon} = \epsilon/2$.

We finally review the main theorem of Nayebi et al. [NABT15], which states that if there exists a biased quantum adversary for $\pi \in X$, then we can construct randomized encoding procedures.

**Lemma 5** ([NABT15, Lemma 5], adapted). Let $\Pi$ be the set of all permutations over $[N]$ and let $X$ be its subset. Let $A$ be a quantum adversary of size at most $S$ that queries to $\pi$ at most $\tilde{Q}$ times. Suppose that, for all $\pi \in X$, we have $\Pr_{x \leftarrow [N]} \left[ \Pr_{\pi} [A^{\pi}(x)] = x \right] \geq 2/3 \geq \tilde{\epsilon}$. Then, there exists a randomized encoding procedure $E: X \times R \rightarrow Y$ and a decoding procedure $D: Y \times R \rightarrow X$ such that, for all $\pi \in X$, we have $\Pr_{r \leftarrow R} [D(E(\pi, r)) = \pi] \geq 0.8$ and $\text{Pr}(|Y|) \leq \Omega(\epsilon N/\tilde{Q}^2) + O(\log(N))$.

**3.1.2 Proof of Theorem 2:**

We first show the following claim:

**Claim.** Let $X$ be a subset of $\Pi$. Let $\delta$ be a fraction of $X$ in $\Pi$, that is, $\delta := |X|/N!$. If there exists a quantum adversary $B$ of size $S$ such that, for all $\pi \in X$, $B$ inverts $\pi$ with a probability at least $\epsilon$ by making at most $Q$ queries, then we have

$$\delta \leq 2^{-\Omega(\epsilon^2 N/\tilde{Q}^2)}.$$

**Proof of Claim.** Using Lemma 4, we can construct a quantum adversary $A$ of size $\tilde{S} = S \cdot O(1/\sqrt{\epsilon/2})$ that queries to a permutation at most $\tilde{Q} = Q \cdot O(1/\sqrt{\epsilon/2})$ such that, for any $\pi \in X$,

$$\Pr_{x \leftarrow [N]} \left[ \Pr_{\tilde{A}} [A^{\tilde{\pi}}(x)] = x \right] \geq 2/3 \geq \tilde{\epsilon} = \epsilon/2.$$

According to Lemma 5, there exists a randomized encoding procedure $E$ and its decoder $D$ such that for all $\pi \in X$, we have

$$\Pr_{r \leftarrow R} [D(E(\pi, r)) = \pi] \geq 0.8 \text{ and } \log(|Y|) \leq \log(N!) - \Omega(\epsilon N/\tilde{Q}^2) + O(\log(N)).$$

Using Lemma 3, the former implies that $|Y| \geq 0.8 |X|$. Therefore, we have the following inequality:

$$0.8 |X| \leq |Y| \leq N! \cdot 2^{-\Omega(\epsilon N/\tilde{Q}^2)} \cdot \text{poly}(N).$$

Recall that the relations $|X| = \delta N!$, $\tilde{\epsilon} = \epsilon/2$, and $\tilde{Q} = Q \cdot O(1/\sqrt{\epsilon/2})$. Putting them into the above and dividing by $N!$, we obtain

$$\delta \leq 2^{-\Omega(\epsilon^2 N/\tilde{Q}^2)} \cdot \text{poly}(N) \leq 2^{-\Omega(\epsilon^2 N/\tilde{Q}^2)}.$$

$\square$
Now, we can prove Theorem 2 as follows: Let $N = 2^t$. Let $c > 1$ be a constant, which we will set later. Let $A$ be an oracle quantum circuit of size $S = 2^{t/c} = N^{1/c}$. This yields $Q = 2^{t/c}$.

First, we recall that the number of circuits of size at most $S$ is at most $(4S)^{t(S+1)} = 2^{\tilde{O}(S)} = 2^{\tilde{O}(N^{1/c})}$.

Second, according to our claim, if $B$ of size $S$ inverts for all $\pi \in X$ with a probability at least $\epsilon = 1/S$, then the fraction of $X$ should be $\delta \leq 2^{-\tilde{O}(\epsilon^2 S/S^2)} \leq 2^{-\tilde{O}(N/S^4)} = 2^{-\tilde{O}(N^{1-4/c})}$.

Taking the union bound, the probability over a random choice of $\pi$ that there exists a quantum circuit of size $S$ which will invert $\pi$ with a probability at least $1/S$ is at most the product of the number of circuits of size $S$ and the maximum fraction of invertible $X$ for $S$, that is, $2^{\tilde{O}(N^{1/c})} \cdot 2^{-\tilde{O}(N^{1-4/c})}$. By setting $c = 6$, the probability is at most $2^{\tilde{O}(N^{1/6})} \cdot 2^{-\tilde{O}(N^{1/6})} \leq 2^{-N^{1/6}}$ for sufficiently large $N$. Hence, a random $\pi \in \Pi_t$ is $S = 2^{t/6}$-hard with a probability greater than $1 - 2^{-2^{t/6}}$ as we wanted. \hfill \qed

4 The Bound on Pseudo-Random Number Generator

We show the lower bound for the number of invocations of qOWP to construct PRG. We first review the definition of the black-box construction of PRG from qOWP.

**Definition 5.** A construction of a PRG scheme based on qOWP is an oracle procedure $\text{PRG}^{(\cdot)} : \{0, 1\}^t \rightarrow \{0, 1\}^{t+k}$. We refer $k$ as the stretch length of PRG.

We say that $\text{PRG}^{(\cdot)}$ is an $(S_p, S_q, \epsilon)$-qOWP-to-PRG weak black-box construction if for every $\pi \in \Pi_n$ that is $S_p$-hard, $\text{PRG}^{(\pi)}$ is $(S_q, \epsilon)$-secure PRG.

**Intuition:** First, we review the proof in the classical setting by Gennaro and Trevisan. We note that the answers of the random permutation $\pi \in \Pi_{t,n}$ on $q$ queries can be simulated with $q$ random $t$-bit strings $y_1, \ldots, y_q$ unless the strings $y_1, \ldots, y_q$ collide: On the $i$-th query $x_i = (a_i, b_i) \in \{0, 1\}^t \times \{0, 1\}^t$, we answer with $(y_i, b_i)$. Based on PRG with extension length $k$ using OWF $q$-times, Gennaro and Trevisan constructed a new secure PRG with longer seed $s, y_1, \ldots, y_q$ which emulates a random permutation by using $y_1, \ldots, y_q$. Thus, if the extension length $k$ is larger than $qt$, then we have unconditionally-secure PRG, which implies the unconditionally-secure OWF.

In the quantum setting, the black-box construction will access to the random permutation with the superposition queries. Thus, the classical pre-sampling strings $y_1, \ldots, y_q$ are not enough to answer those $q$ superposition queries. Instead, we simulate the random permutation by $2q$-wise independent hash function. Zhandry showed that such hash function perfectly simulates the random function (Lemma 1). In addition, the random function and the random permutation is indistinguishable up to $2^{t/2}$ queries (Theorem 1). Hence, we can construct an unconditionally-secure PRG from secure PRG upon qOWF and this implies unconditionally-secure QC-qOWF.

**Theorem 3.** Let $\text{PRG}^{(\cdot)}$ be an $(S_p, S_q, \epsilon)$-qOWP-to-PRG weak black-box quantum construction for message of length $m$ using a key of length $k$ in which PRG makes $q$ quantum queries to an oracle $\pi$, where $\pi \in \Pi_n$. Let $t = 6 \log S_p < n$. If $(2q + 1)t < k$, then there exists an $(S_p, \epsilon + 2^{-S_p} + \epsilon_0)$-secure PRG scheme without any access to oracles, where $\epsilon_0 = (8\pi^2/3)(q^2/S_p^6)$ is the maximum advantage of $q$-query distinguisher against the random permutation in $\Pi_t$ and the random function in $\Phi_t$.

**Proof of Theorem 3.** From the hypothesis, if $\pi : \{0, 1\}^n \rightarrow \{0, 1\}^n$ is $(S_p, 1/S_p)$-hard, then for any distinguisher $T$ of size at most $S_q$, we have

$$\Pr_{z \sim \{0, 1\}^t} [T(z) = 1] - \Pr_{s \sim \{0, 1\}^t} [T(\text{PRG}^{(\pi)}(s)) = 1] \leq \epsilon.$$
We here drop the quantum oracle access of $T$, since this only makes $T$ weaker. Let $t = 6 \log(S_p) < n$. According to Corollary 1, a random permutation $\pi \in \Pi_{t,n}$ is $S_p$-hard with probability greater than $1 - 2^{-2^{t/n}} = 1 - 2^{-S_p}$. Using the average argument, we have

\[
\left| \mathbb{P}_{z \leftarrow \{0,1\}^{\ell+k}}[T(z) = 1] - \mathbb{P}_{\pi \leftarrow \Pi_{t,n}, s \leftarrow \{0,1\}^t}[T(\text{PRG}[\pi](s)) = 1] \right| \leq \epsilon + 2^{-S_p}.
\]

We next replace $\pi \in \Pi_{t,n}$ with $\phi \in \Phi_{t,n}$. Due to Theorem 1, we have

\[
\left| \mathbb{P}_{\pi \leftarrow \Pi_{t,n}, s \leftarrow \{0,1\}^{t}}[T(\text{PRG}[\pi](s)) = 1] - \mathbb{P}_{\phi \leftarrow \Phi_{t,n}, s \leftarrow \{0,1\}^{t}}[T(\text{PRG}[\phi](s)) = 1] \right| \leq \epsilon_0,
\]

where $\epsilon_0 := (8\pi^2/3)(q^3/2^t) = (8\pi^2/3)(q^3/S_p^2)$. Using the triangle inequality, we obtain

\[
\left| \mathbb{P}_{z \leftarrow \{0,1\}^{\ell+k}}[T(z) = 1] - \mathbb{P}_{\phi \leftarrow \Phi_{t,n}, s \leftarrow \{0,1\}^{t}}[T(\text{PRG}[\phi](s)) = 1] \right| \leq \epsilon + 2^{-S_p} + \epsilon_0.
\]

Here, we note that $\text{PRG}[\phi](s)$ may fail because the construction might exploit the fact that $\pi$ is the permutation. However, the failure probability of $\text{PRG}[\phi](s)$ is at most $\epsilon_0$ due to Theorem 1.

Recall that $\text{PRG}$ queries to $|\pi\rangle$ (and $|\phi\rangle$) at most $q$ times. We construct $\text{PRG}'$: $\{0,1\}^\ell \rightarrow \{0,1\}^{\ell+k}$, where $\ell' := \ell + (2q + 1)t < \ell + k$, as follows: Parse $s' \in \{0,1\}^{\ell+(2q+1)t}$ as $(s, f_0, \ldots, f_{2q}) \in \{0,1\}^{\ell} \times \{0,1\}^{2q+1}$ and define $f: \{0,1\}^\ell \rightarrow \{0,1\}^\ell$ by $f(z) := \sum_i f_i z^i \in \text{GF}(2^\ell)$, which is $2q$-wise independent hash functions [WC81]. Using this $f$ instead of a random function $\phi$, we define $F(a, b) = (f(a), b)$.

Now, we define

\[
\text{PRG}'(s') := \text{PRG}'(s, f_0, \ldots, f_{2q}) = \text{PRG}[F](s).
\]

According to Zheng's lemma (Lemma 1), the $2q$-wise independent hash functions and the random functions are indistinguishable up to $q$-queries and we have

\[
\mathbb{P}_{\phi \leftarrow \Phi_{t,n}, s \leftarrow \{0,1\}^{t}}[T(\text{PRG}[\phi](s)) = 1] = \mathbb{P}_{s' \leftarrow \{0,1\}^{\ell}}[T(\text{PRG}'(s')) = 1].
\]

Combining the (in)equalities, we obtain our theorem.

\[\Box\]

Remark. We note that $\text{PRG}'$: $\{0,1\}^\ell \rightarrow \{0,1\}^{\ell+k}$ is efficiently computable because it just runs $\text{PRG}$ with simulation of $F$ based on $2q$-wise independent hash function $f(z) = \sum_i f_i z^i$. Thus, $\text{PRG}'$ yields an unconditionally-secure QC-qOWF; if it is not qOWF, then it is not secure $\text{PRG}$.

5 The Bound on Symmetric-Key Encryption

We show the lower bound for the number of invocations of qOWP to construct SKE. We start with a review of the definition of the black-box construction of SKE from qOWP.

Definition 6. Construction of an SKE scheme based on qOWP is a pair of oracle procedures $\text{SKE}^{(\pi)} = (\text{Enc}^{(\pi)}, \text{Dec}^{(\pi)})$ such that, for all $\pi \in \Pi_n$, the resulting $\text{SKE}^{(\pi)}$ satisfies the functional definition of an SKE scheme.

We say that $\text{SKE}^{(\pi)}$ is an $(S_p, S_r, \epsilon)$-qOWP-to-SKE weak black-box construction if for every $\pi \in \Pi_n$ that is $S_p$-hard, $\text{SKE}^{(\pi)}$ is $(S_r, \epsilon)$-hard.
Intuition: We start to review the proof in the classical setting by Gennaro, Gertner, and Katz [GGK03]: Let $k$ be the key length and $m$ be the message length. We again note that the answers of the random permutation $\pi \in \Pi_{t,n}$ on $q$ queries can be simulated with $q$ random $t$-bit strings $y_1, \ldots, y_q$ unless the strings $y_1, \ldots, y_q$ collide: On the $i$-the query $x_i = (a_i, b_i) \in \{0,1\}^t \times \{0,1\}^t$, we answer with $(y_i, b_i)$. However, SKE involves two algorithms $Enc$ and $Dec$ which may ask different queries. In order to maintain the queried points, they make a new encryption algorithm $Enc'$ sends a ciphertext made by $Enc$ plus the encrypted list of queried points by the one-time pad. If the key length $k$ is shorter than $m - O(qt)$, then we have unconditionally-secure SKE, which implies the unconditionally-secure OWF [IL89, GGKT05].

In the quantum setting, we again simulate the random permutation by $4q$-wise independent hash function, since $Enc$ and $Dec$ make $q$ queries. Since this simulation allows us to share the same function in both algorithms, we do not need to send the encrypted list and the simulation becomes simple.

Using the same idea, we can show that if the key length $k$ is shorter than $m - (4q + 1)t$, then we have unconditionally-secure non-trivial SKE. While we tend to conclude this unconditionally-secure SKE implies the unconditional existence of qOWF, we cannot say so since the new encryption algorithm and decryption algorithm are probabilistic, which we discuss later.

Theorem 4. Let $SKE^{(1)}$ be an $(S_p, S_e, \epsilon)$-qOWP-to-SKE weak black-box construction for message of length $m$ using a key of length $k$ in which $Enc^{(1)}$ and $Dec^{(1)}$ makes $q$ queries to an oracle $\pi \in \Pi_n$. Let $t = 6\lg(S_p)$. If $m > k + (4q + 1)t$, then there exists an $(S_e, \epsilon)$-secure SKE scheme whose message length is $m' = m$ and key length is $k' = k + (4q + 1)t$ without any access to oracles, where $\epsilon = \epsilon_0 + 2 - S_p + 1 + (16n^2/3)(q^3/S_p^6)$.

Proof. We set $n = 6t$ and consider $\Pi_{t,n} \subseteq \Pi_n$.

The hypothesis of the theorem on $SKE^{(1)} = (Enc^{(1)}, Dec^{(1)})$ implies that if $\pi$ is $S_p$-hard, then for any circuit $B$ of size $S_e$ and for any messages $M_0, M_1 \in \{0,1\}^m$ we have

$$\left| \Pr_{s \leftarrow \{0,1\}^k, v \leftarrow Enc^{(1)}(s, M_0)}[B(v) = 1] - \Pr_{s \leftarrow \{0,1\}^k, v \leftarrow Enc^{(1)}(s, M_1)}[B(v) = 1] \right| < \epsilon.$$  

We here drop the quantum oracle access of $B$, since this only makes $B$ weaker.

According to Theorem 2, $\pi \in \Pi_{t,n}$ is $S_p$-hard for all but except $2 - S_p$ fraction. By using the averaging argument, for any circuit $B$ of size at most $S_e$ and for any two messages $M_0, M_1 \in \{0,1\}^m$ we have

$$\left| \Pr_{s \leftarrow \{0,1\}^k, \pi \leftarrow \Pi_{t,n}}[B(v) = 1] - \Pr_{s \leftarrow \{0,1\}^k, \pi \leftarrow \Pi_{t,n}}[B(v) = 1] \right| < \epsilon + 2 - S_p + 1.$$  

Using Zhandry’s lemma (Theorem 1), we can replace $\pi \leftarrow \Pi_{t,n}$ with $\phi \leftarrow \Phi_{t,n}$ as follows:

$$\left| \Pr_{s \leftarrow \{0,1\}^k, \phi \leftarrow \Phi_{t,n}}[B(v) = 1] - \Pr_{s \leftarrow \{0,1\}^k, \phi \leftarrow \Phi_{t,n}}[B(v) = 1] \right| < \epsilon + 2 - S_p + 1 + 2\epsilon_0 = \epsilon_0,$$

where $\epsilon_0 = (8\pi^2/3)(q^3/S_p^6)$.

Let us construct a new SKE scheme $SKE'$ for $m$-bit messages using a random key of length $k' = k + (4q + 1)t$, which is $(S_e, \epsilon)$-secure and has no oracle access. Again, we simulate the random function $\phi$ by $4q$-wise independent hash function. The simulation is very simple: We prepare $F(a, b) := f(a, b)$, where $f: \{0,1\}^t \rightarrow \{0,1\}^t : f(a) = \sum_{i=0}^{4q} f_i a^i \in GF(2^t)$. Now, $SKE'$ is defined as follows:

- $Enc'$ parses the shared key $s' \in \{0,1\}^{k'}$ as the original shared key $s$ and $4q$-wise independent hash function $f$ and encrypts a message into $C$ by $C \leftarrow Enc'(F)(s, M)$. 

Keita Xagawa 11
• Dec′ parses the shared key s′ as s and f and decrypts a ciphertext C by $M′ \leftarrow \text{Dec}^{f')}(s, C)$.

The $(S_e, \bar{e})$-security of SKE′ directly follows from Equation 3.

**Remark 4.** We note that our SKE′ may have negligible decryption errors because we replace a permutation with a 4q-wise independent hash function. This is similar to the case that $y_i$’s collide in the classical setting.

**Remark 5.** We only consider a non-interactive SKE scheme for simplicity. We can extend the results into the interactive setting by replacing $v \leftarrow \text{Enc}^{()}(s, M_b)$ with $v \leftarrow (\text{Enc}^{()}(s, M_b), \text{Dec}^{()}(s))$ in the equations in the proof.

**References**


A Complexity Class and Instance Generator

For the basic complexity classes (P, NP, BQP, QMA, and QCMA), see the standard textbooks.
We say a language is in QCMA if there exists QPT machine $V$, called as a verifier, such that there exists a polynomial $r(\cdot)$ and $1$ for any $x \in L$, there is a classical string $w \in \{0, 1\}^*$ of length polynomial in $|x|$ such that $\Pr[V(x, w) = 1] \geq 1 - 2^{-r(|x|)}$; and $2)$ for any $x \notin L$, for all classical strings $w \in \{0, 1\}^*$ of length polynomial in $|x|$, $\Pr[V(x, w) = 1] < 2^{-r(|x|)}$.

We follow the terminology in Bogdanov and Trevisan [BT06]. A pair $(L, \mu)$ is said to be a distributional problem if $L \subseteq \{0, 1\}^*$ and $\mu = \{\mu_n\}_{n \in \mathbb{Z} \geq 0}$ is an ensemble of probability distributions. Following the definition of P-sampleable distribution, we define its quantum version as follows:

**Definition 7.** A distribution $\mu$ is said to be BQP-sampleable if there exists a QPT machine $S$ such that $\Pr[S(1^n) = x] = \mu_n(x)$.

We define the quantum analogs of the average-case complexity $(\text{NP, P-Samp})$.

**Definition 8.** $(\text{QMA, BQP-Samp})$ denotes the set of distributional problems $(L, \mu)$ with $L \subseteq \text{QMA}$ and BQP-sampleable $\mu$. $(\text{QCMA, BQP-Samp})$ denotes the set of distributional problems $(L, \mu)$ with $L \subseteq \text{QCMA}$ and BQP-sampleable $\mu$.

We here call a sampling machine an instance generator if it samples a pair of an instance $x$ in a language $L$ and its corresponding witness $w$. We say that a problem $(L, \mu) \in (\text{QCMA, BQP-Samp})$ is $(S, \epsilon)$-hard if $1$ there exists a QPT instance generator $E$ such that $E$’s first output distributes as $\mu$ and $2)$ for any quantum machine $A$ of size at most $S = S(n)$, $\Pr_{(x, w) \leftarrow E(1^n)}[V(x, A(x)) = 1] \leq \epsilon$, where $V$ is a verifier of $(L, \mu)$.

We also define the quantum analog of the average-case complexity AvgBQP:

**Definition 9.** We say that a distributional problem $(L, \mu)$ is in AvgBQP if there exists a quantum algorithm $A$ such that

1. for every $n, \delta, x$, $\Pr_{x \leftarrow \mu_n}[A(x, 1^n, \delta) \notin \{L(x), \bot\}] \leq 1/4$ holds, where $L(x) \in \{0, 1\}$ is an indicator function;
2. for every $n, \delta$, $\Pr_{x \leftarrow \mu_n}[\Pr_{A \leftarrow L}[A(x, 1^n, \delta) = \bot] \geq 1/4] \leq \delta$ holds; and
3. $A$ runs in a polynomial time of $n/\delta$.

**Relations:** If there exists qOWF, then we have FBQP $\neq$ FQCMA (and BQP $\neq$ QCMA). Kretschmer [Kre21] showed that there exists an oracle relative to which BQP = QMA but secure PRS exists. Aaronson, Ingram, and Kretschmer [AIK22] showed that there exists an oracle relative to which P $=$ NP but BQP $\neq$ QCMA. They also showed that there exists an oracle relative to which P $\neq$ NP but BQP = QCMA = QMA. Kretschmer, Qian, Sinha, and Tal [KQST23] further showed that there exists an oracle relative to which P $=$ NP but single-copy-secure PRS exists [JLS18].

**B SKE implies hard instance generator for QCMA**

Unfortunately, unconditionally-secure non-trivial QC-SKE does not imply qOWF. The existing proofs in [IL89, GGKT05] require an encryption algorithm to be a PPT machine, where we can treat a random tape explicitly. Instead, we consider the class of average-case complexity, $(\text{QMA, BQP-Samp})$, which consists of pairs of a language in QCMA and a probability distribution of instances sampleable by a QPT machine, and AvgBQP. Our unconditionally-secure non-trivial QC-SKE, QC-qSKE in short, implies $(\text{QMA, BQP-Samp}) \not\subseteq \text{AvgBQP}$, quantum analogue of $(\text{NP, P-Samp}) \not\subseteq \text{AvgP}$.

The proof is essentially the same as that of [GGKT05]:
Theorem 5. Let $(\text{Enc}, \text{Dec})$ be an $(S, \delta)$-secure perfectly-correct quantum SKE scheme whose message length is $m$ and key length is $k < m$. Let $S_\ell$ be the size of the circuit of $	ext{Enc}$ and let $S_d$ be the size of the circuit of $	ext{Dec}$. For any $\ell$, there exists a pair of a QPT instance generator and a QPT verifier $(E, D)$ that is $(S - 2\ell S_\ell - 2\ell S_d - \text{poly}(m, k, \ell), \delta + 2^{-\ell(m-k)})$-hard.

We can easily extend the correctness to quantum SKE to statistical one.

Proof. Let $\text{SKE}_\ell = (\text{Enc}_\ell, \text{Dec}_\ell)$ be an intermediate quantum SKE scheme whose message length and key length are $\ell m$ and $\ell k$, respectively defined as follows: $\text{Enc}_\ell$ takes $(s_k_1, \ldots, s_k_\ell) \in \{0,1\}^{\ell k}$ and $(M_1, \ldots, M_\ell) \in \{0,1\}^{\ell m}$ as input and outputs $(C_1, \ldots, C_\ell)$ where $C_i \leftarrow \text{Enc}(s_k_i, M_i)$; $\text{Dec}_\ell$ takes $(s_k_1, \ldots, s_k_\ell) \in \{0,1\}^{\ell k}$ and $(C_1, \ldots, C_\ell)$ as input and outputs $(\text{Dec}(s_k_1, C_1), \ldots, \text{Dec}(s_k_\ell, C_\ell)) \in \{0,1\}^{\ell m}$. By the standard hybrid argument, it is easy to see that $\text{SKE}_\ell$ is $(S - \ell S_\ell, \ell \delta)$-secure quantum SKE scheme.

We now define a QPT instance generator $E$ and a QPT verifier $D$ as follows: $E$ on input $s_k \in \{0,1\}^{\ell k}$ and $M \in \{0,1\}^{\ell m}$ outputs $\text{Enc}_\ell(s_k, M)||M$. $D$ on input $(c, M)$ and $s_k'$ checks if $M = \text{Dec}_\ell(s_k', c)$ or not.

We want to show that the distribution $E(U_{sk}, U_{\ell m})$ generates average-case hard instances. Let us assume the contrary; suppose that there exists an algorithm $B$ of size at most $S'$ breaking $(S', \delta')$-hardness of $E$. Let $adv_B$ denote the advantage of $B$, that is,

$$adv_B := \Pr_{s_k \sim \{0,1\}^{\ell k}, M \sim \{0,1\}^{\ell m}, c \sim \text{Enc}_\ell(s_k, M)}[D(c||M, B(c||M)) = 1] > \delta'.$$

We then construct an algorithm $A$ of size at most $S' - S_d - \text{poly}(m, k, \ell)$ with whose advantage against $\text{SKE}_\ell$ is at least $\ell \delta$, where the advantage is

$$\left| \Pr_{s_k \sim \{0,1\}^{\ell k}, M_0, M_1 \sim \{0,1\}^{\ell m}, c \sim \text{Enc}_\ell(s_k, M_0)}[A(M_0, M_1, c) = 1] - \Pr_{s_k \sim \{0,1\}^{\ell k}, M_0, M_1 \sim \{0,1\}^{\ell m}, c \sim \text{Enc}_\ell(s_k, M_1)}[A(M_0, M_1, c) = 1] \right|.$$

$A$ is defined as follows: Given $M_0$, $M_1$, and $c$, the algorithm $A$ runs $B$ on input $c$ and $M_0$ and receives $s_k'||M'$. It then checks whether both $\text{Dec}_\ell(s_k'||M') = C$ and $M' = M_0$ hold or not. If so, $B$ succeeds to find such $s_k'$ and $M'$, and $A$ outputs 1. Otherwise, $A$ outputs 0.

By the definition of $A$, when $c$ is produced by $M_0$, $A$ outputs 1 if $B$ succeeds. Thus, we have

$$\Pr_{s_k \sim \{0,1\}^{\ell k}, M_0, M_1 \sim \{0,1\}^{\ell m}, c \sim \text{Enc}_\ell(s_k, M_0)}[A(M_0, M_1, c) = 1] = adv_B > \delta'.$$

We also have

$$\Pr_{s_k \sim \{0,1\}^{\ell k}, M_0, M_1 \sim \{0,1\}^{\ell m}, c \sim \text{Enc}_\ell(s_k, M_1)}[A(M_0, M_1, c) = 1] \leq \Pr_{s_k \sim \{0,1\}^{\ell k}, M_0, M_1 \sim \{0,1\}^{\ell m}, c \sim \text{Enc}_\ell(s_k, M_1)}[\exists s_k' \text{ s.t. } \text{Dec}_\ell(s_k', c) = M_0]$$

$$\leq \sum_{s_k' \in \{0,1\}^{\ell k}} \Pr_{s_k \sim \{0,1\}^{\ell k}, M_0, M_1 \sim \{0,1\}^{\ell m}, c \sim \text{Enc}_\ell(s_k, M_1)}[\text{Dec}_\ell(s_k', c) = M_0]$$

$$\leq \sum_{s_k' \in \{0,1\}^{\ell k}} 2^{-\ell m} = 2^{-\ell(k-m)},$$

where we use the fact that the distribution of $M_0$ is independent of $\text{Dec}(s_k', C)$.

Thus, the advantage of $A$ is at least $\delta' - 2^{-\ell(k-m)}$. By setting $S' = S - \ell S_e$ and $\delta' = \ell \delta + 2^{-\ell(k-m)}$, we have $S_A = S' - \ell S_d - \text{poly}(m, k, \ell) = S - \ell S_e - \ell S_d - \text{poly}(m, k, \ell)$ and $\delta_A = \delta' - 2^{-\ell(k-m)} = \ell \delta$ as we wanted. $\square$

We note that if $\text{Enc}$ computes a function, then the above construction implies QC-qOWF as in [GGKT05].