On the Efficiency of Generic, Quantum Cryptographic Constructions

Keita Xagawa

Technology Innovation Institute
P.O.Box 9639, Masdar City, Abu Dhabi, United Arab Emirates
keita.xagawa@tii.ae

Abstract. One of the central questions in cryptology is how efficient generic constructions of cryptographic primitives can be. Gennaro, Gertner, Katz, and Trevisan [GGKT05] studied the lower bounds of the number of invocations of a (trapdoor) oneway 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-oneway permutation (QC-qOWP) when the *quantum* construction of pseudorandom number generator (PRG) and symmetric-key encryption (SKE) is weakly black-box. Our results show that the quantum black-box constructions of PRG and SKE do not improve the number of invocations of an underlying QC-qOWP.
keywords: Quantum reduction, black-box construction, efficiency.

1 Introduction

It is widely believed that showing the existence of (trapdoor) oneway permutations/functions is incredibly hard. If it is shown, then the long-standing open problem $\mathsf{P} = \mathsf{NP}$ is solved negatively and we notice that we live in Minicrypt/Cryptomania of Impagliazzo's five worlds [Imp95]. Cryptographers *assume* the existence of (trapdoor) oneway 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 oneway permutation. As an example, let us consider the basic construction of pseudorandom generator (PRG) from oneway permutation (OWP) (See e.g. [KL20]): By using the Goldreich-Levin hardcore function [GL89], we can construct $\mathsf{PRG}\colon \{0,1\}^{\ell} \to \{0,1\}^{\ell+k}$ from $\mathsf{OWP}\colon \{0,1\}^{n} \to \{0,1\}^{n}$, where $\ell = 2n$. If we let the range of the hardcore function $\{0,1\}^{O(\lg(n))}$, 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, $\mathsf{DistNP} \not\subseteq \mathsf{AvgP}$, and $\mathsf{P} \neq \mathsf{NP}$. [1] [2]

Quantum adversary, quantum construction, and quantum reduction: Crytpgraphic researches exploit the properties of *quantum* machines and channels to advance the classical counterparts; see e.g., certified deletion [BI20, HMNY21] and MPQC [BCKM21a, BCKM21b, GLSV21].

We here 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-quantumly-secure OWP (qOWP). In the case of the generic construction of PRG, we already know that the above PRG construc-

[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 [RTV04] 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.

tion 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-oneway 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].

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 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 $(\mathsf{QCMA}, \mathsf{BQP\text{-}Samp}) \not\subseteq \mathsf{AvgBQP}$ in the average-case complexity, and the proof of $\mathsf{BQP} \neq \mathsf{QCMA}$, quantum analogs of OWF, $\mathsf{DistNP} \not\subseteq \mathsf{AvgP}$, and $\mathsf{P} \neq \mathsf{NP}$. (The seed of new PRG is the classical witness of QCMA and it is verified by the quantum computation of new PRG.)

Gennaro and Trevisan [GT00] first showed that a random permutation is oneway. 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 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 onewayness of the random permutation; the other is the way to simulate *quantumly-queried* random permutation with classical strings:

– For the former, we show that the random permutation is quantum-oneway. We follow a simple proof following that in [GGKT05, NABT15,

HXY19], while there are researches of quantum random oracle's onewayness (and more with advice), see e.g., [NABT15, HXY19, CGLQ20, Liu23].
– For the latter, we need to emulate the random permutation quantumly queried q-times with compact *classical* strings. We here use the RF-RP switching lemma [Zha12a, Zha15] 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.

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 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 $(\mathsf{QCMA}, \mathsf{BQP\text{-}Samp}) \not\subseteq \mathsf{AvgBQP}$ and the proof of $\mathsf{BQP} \neq \mathsf{QCMA}$. If the underlying SKE computes a *function*, then further implies the existence of QC-qOWF.

Gennaro et al. [GGKT05] showed the relation between OWTDP and PKE and obtained the results for OWP and SKE as a corollary. For simplicity, we here review the SKE version. 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 by 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 $(\mathsf{QCMA}, \mathsf{BQP\text{-}Samp}) \not\subseteq \mathsf{AvgBQP}$ and $\mathsf{BQP} \neq \mathsf{QCMA}$. 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.

1.2 Related works

Hosoyamada and Yamakawa studied the gap between collision-resistant hash function and oneway (trapdoor) permutations [HY20]. Austrin et al. studied the impossibility of quantum construction of key exchange from oneway 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

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 λ 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 $(\mathsf{Q(C)MA}, \mathsf{BQP\text{-}Samp})$ and $(\mathsf{Q(C)MA}, \mathsf{BQP\text{-}Comp})$, and the relation between them.

Organization: Section 2 reviews basic notions and notations. Section 3 gives a generic quantum hardness of oneway 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 $\lg(\cdot) := \log_2(\cdot)$. For two finite sets D and R, $\mathsf{Func}(D, R)$ denotes a set of all functions whose domain is D and whose range is R. For a distribution $\mathcal{D}$, $d \hookleftarrow \mathcal{D}$ indicates we take a random sample d according to $\mathcal{D}$. For a finite set S, $U(F)$ denotes the uniform distribution over F. If $F = \{0,1\}^k$, we use U_k instead of $U(\{0,1\}^k)$.

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

We review k-wise independent functions and its property.

Definition 2.1. *A family F of functions $D \to R$ 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:*

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

Lemma 2.1 ([Zha12b]). *For any finite sets D and R of classical strings and q-quantum query algorithm A, we have*

$$\Pr_{H \hookleftarrow \mathsf{Func}(D,R)}[A^{|H\rangle} = 1] = \Pr_{H \hookleftarrow \mathcal{H}_{2q}(D,R)}[A^{|H\rangle} = 1],$$

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

2.1 Oneway Permutation/Function

We define the quantum onewayness of permutation and function in the concrete security style:

Definition 2.2. *We say that a function $f\colon \{0,1\}^n \to \{0,1\}^n$ is (S,ϵ)-quantumly-oneway or quantumly-oneway function (qOWF) if for every quantum circuit A of size at most S, we have*

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

When f is given as a quantum oracle, we will denote $A^{|f\rangle}$. 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-oneway permutation (qOWP).

We will denote the set of all permutations over $\{0,1\}^n$ by Π_n. For $t \leq n$, we define $\Pi_{t,n}$ the subset of Π_n such that the set of all permutations which keep $n-t$ last bits unchanged; that is, $\Pi_{t,n} := \{\pi \in \Pi_n : \exists \hat{\pi} \in \Pi_t$ 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 $\{0,1\}^t$ by Φ_n and define the set of all functions which keep the $n-t$ last bits unchanged by $\Phi_{n,t}$; that is, $\Phi_{t,n} := \{\phi \in \Phi_n : \exists \hat{\phi} \in \Phi_t$ 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 RF-RP switching lemma shown by Zhandry [Zha15].

Theorem 2.1 (The RF-RP quantum 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*

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

2.2 Pseudorandom Number Generator

A pseudorandom number generator is an quantum polynomial-time algorithm PRG which takes a seed $s \in \{0,1\}^\ell$ as input and outputs a pseudorandom string $y \in \{0,1\}^{\ell+k}$.

Definition 2.3. *We say a function $\mathsf{PRG}\colon \{0,1\}^\ell \to \{0,1\}^{\ell+k}$ is an (S,ϵ)-secure pseudorandom number generator (PRG) if for any quantum circuit A of size at most S, we have*

$$\left|\Pr_{s\hookleftarrow\{0,1\}^\ell}[A(\mathsf{PRG}(s)) = 1] - \Pr_{z\hookleftarrow\{0,1\}^{\ell+k}}[A(z) = 1]\right| \leq \epsilon.$$

We call ℓ 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 quantum polynomial-time algorithms $\mathsf{SKE} = (\mathsf{Enc}, \mathsf{Dec})$;

- Enc takes a key $K \in \{0,1\}^k$ and a message $M \in \{0,1\}^m$ as input and outputs a ciphertext $C \in \{0,1\}^{m'}$.
- 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 $\perp$.

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

We consider the basic security notion of SKE:

Definition 2.4. *We say that* SKE *is (S,ϵ)-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*

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

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

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 source of input-output wires. The numbers of the possible sources are at most $(2n)!/n!$ because we consider f-gate with $f\colon \{0,1\}^n \to \{0,1\}^n$. In addition, the numbers of the possible output wires are at most $(2n)!/n!$. Thus, the upperbound of the number of quantum circuits is at most $(4(2n)!/n!)^S \cdot (2n)!/n! \leq (4(2n)!/n!)^{S+1}$. □

Remark 3.1. If we allow $(S-n)$-qubits ancilla, then we have the upper-bound $(4S!/n!)^{S+1}$.

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 3.1. *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 3.1. *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 3.2. Nayebi et al. [NABT15] showed the onewayness of quantum random permutations with classical advice. Moreover, there are studies of more properties of quantum random functions/permutations with advice (See e.g., [HXY19, CGLQ20, Liu23]).

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

Lemma 3.2 ([DTT10, Fact 8.1], Randomized Compression Lemma). *Suppose there is a randomized encoding procedure $E\colon X \times R \to Y$ and a decoding procedure $D\colon Y \times R \to X$. For any constant $c \in [0,1]$, if $\Pr_{r\hookleftarrow R}[D(E(x,r),r)=x] \geq c$, then $|Y| \geq c|X|$.*

The next one is taken from Hhan et al. [HXY19], while we adapt it slightly.

Lemma 3.3 ([HXY19], Reduction to biased adversary). *Let Π be the set of all permutations over $[N]$ and let X be its subset. Suppose that we have an adversary B of size S whose number of queries is at most Q such that, for all $\pi \in X$, B inverts π with advantage at least ϵ, that is,*

$$\Pr_{x\hookleftarrow[N],B}[B^{|\pi\rangle}(\pi(x))=x] \geq \epsilon. \tag{1}$$

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

$$\Pr_{x\hookleftarrow[N]}\left[\Pr_{A}[A^{|\pi\rangle}(\pi(x))=x] \geq 2/3\right] \geq \tilde{\epsilon}, \tag{2}$$

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 Eq. (1), we have

$$\Pr_x\left[\Pr[B^{|\pi\rangle}(\pi(x)) = x] \geq \epsilon/2\right] \geq \epsilon/2.$$

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 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 adversary for $\pi \in X$, then we can construct randomized encoding procedures.

Lemma 3.4 ([NABT15, Lemma 5], adapted). *Let Π be the set of all permutations over $[N]$ and let X be its subset. Let A be an adversary of size at most $\tilde{S}$ that queries to π at most $\tilde{Q}$ times. Suppose that, for all $\pi \in X$, we have $\Pr_{x\leftarrow[N]}\left[\Pr[A^{|\pi\rangle}(\pi(x)) = x] \geq 2/3\right] \geq \tilde{\epsilon}$. Then, there exists a randomized encoding procedure $E\colon X \times R \to Y$ and a decoding procedure $D\colon Y \times R \to X$ such that, for all $\pi \in X$, we have $\Pr_{r\leftarrow R}[D(E(\pi, r), r) = \pi] \geq 0.8$ and $\lg(|Y|) \leq \lg(N!) - \Omega(\tilde{\epsilon}N/\tilde{Q}^2) + O(\lg(N))$.*

Proof of Main Theorem: We first show the following claim:

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

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

Proof. Using Lemma 3.3, we can construct an 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 $\pi \in X$,

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

According to Lemma 3.4, there exists a randomized encoding procedure E and its decoder D such that for all $\pi \in X$, we have

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

Using Lemma 3.2, the former implies that $|Y| \geq 0.8|X|$. Therefore, we have the following inequality:

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

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

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

□

Now, we can prove the theorem 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 with $2t$-qubit register is at most $(4(2t)!/t!)^{S+1}$. Due to the Stirling inequality, we have $(2t)! \leq e\sqrt{2t}(2t/e)^{2t}$ and $t! \geq \sqrt{2\pi \cdot t}(t/e)^t$. Therefore,

$$\begin{aligned}\left(\frac{4(2t)!}{t!}\right)^{S+1} &\leq \left(\frac{4e\sqrt{2t}(2t/e)^{2t}}{\sqrt{2\pi t}(t/e)^t}\right)^{S+1} = \left(\frac{4e}{\sqrt{\pi}} \cdot \left(\frac{4t}{e}\right)^t\right)^{S+1} \\ &= (2^{O(t\lg(t))})^{S+1} = 2^{\tilde{O}(S)} = 2^{\tilde{O}(N^{1/c})},\end{aligned}$$

where we use the definition $S = 2^{\Theta(t)}$, which results in $O(t\lg(t)) \cdot S = \tilde{O}(S)$.

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 $\delta \leq 2^{-\tilde{\Omega}(\epsilon^2 N/S^2)} \leq 2^{-\tilde{\Omega}(N/S^4)} = 2^{-\tilde{\Omega}(N^{1-4/c})}$.

Taking the union bound, the probability over a random choice of π that there exists a quantum circuit of size S which will invert π 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, $2^{\tilde{O}(N^{1/c})} \cdot 2^{-\tilde{\Omega}(N^{1-4/c})}$. By setting $c = 6$, the probability is at most $2^{\tilde{O}(N^{1/6})} \cdot 2^{-\tilde{\Omega}(N^{1/3})} \leq 2^{-N^{1/6}}$ 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. □

Remark 3.3. If we use S-qubit register, we will get $2^{\tilde{O}(S^2)}$ as the upper-bound of the number of the quantum circuits. In that case, we set $S = 2^{t/7}$ and we still have $2^{\tilde{O}(N^{1/7})} \cdot 2^{-\tilde{\Omega}(N^{3/7})} \leq 2^{-N^{2/7}}$ for sufficiently large N.

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 4.1. *A construction of a PRG scheme based on qOWP is an oracle procedure* $\mathsf{PRG}^{|\cdot\rangle}\colon \{0,1\}^{\ell} \to \{0,1\}^{\ell+k}$. *We refer* k *as the stretch length of* PRG.

We say that $\mathsf{PRG}^{|\cdot\rangle}$ *is an* (S_p, S_g, ϵ)*-qOWP-to-PRG weak black-box construction if for every* $\pi \in \Pi_n$ *that is* S_p*-hard,* $\mathsf{PRG}^{|\pi\rangle}$ *is* (S_g, ϵ)*-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 $x_i = (a_i, b_i) \in \{0,1\}^t \times \{0,1\}^{4t}$, 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 2.1). In addition, the random function and the random permutation is indistinguishable up to $2^{t/2}$ queries (Theorem 2.1). Hence, we can construct an *unconditionally-secure PRG* from secure PRG upon qOWF and this implies unconditionally-secure QC-qOWF.

Theorem 4.1. *Let* $\mathsf{PRG}^{|\cdot\rangle}$ *be an* (S_p, S_g, ϵ)*-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* $|\pi\rangle$*, where* $\pi \in \Pi_n$*. Let* $t = 6 \lg S_p < n$*. 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* $\epsilon_0 = (8\pi^2/3)(q^3/S_p^6)$ *is the maximum advantage of* q*-query distinguisher against the random permutation in* Π_t *and the random function in* Φ_t.

Proof (Proof of Theorem 4.1). From the hypothesis, if $\pi\colon \{0,1\}^n \to \{0,1\}^n$ is $(S_p, 1/S_p)$-hard, then for any distinguisher T of size at most S_g, we have

$$\left| \Pr_{z\leftarrow\{0,1\}^{\ell+k}}[T(z)=1] - \Pr_{s\leftarrow\{0,1\}^{\ell}}[T(\mathsf{PRG}^{|\pi\rangle}(s))=1] \right| \le \epsilon.$$

We here drop the quantum oracle access of T, since this only makes T weaker. Let $t = 6\lg(S_p) < n$. According to Corollary 3.1, a random permutation $\pi \in \Pi_{t,n}$ is S_p-hard with probability greater than $1-2^{-2^{t/6}} = 1-2^{-S_p}$. Using the average argument, we have

$$\left| \Pr_{z\leftarrow\{0,1\}^{\ell+k}}[T(z)=1] - \Pr_{\pi\leftarrow\Pi_{t,n},s\leftarrow\{0,1\}^{\ell}}[T(\mathsf{PRG}^{|\pi\rangle}(s))=1] \right| \le \epsilon + 2^{-S_p}.$$

We next replace $\pi \in \Pi_{t,n}$ with $\phi \in \Phi_{t,n}$. Due to Theorem 2.1, we have

$$\left| \Pr_{\pi\leftarrow\Pi_{t,n},s\leftarrow\{0,1\}^{\ell}}[T(\mathsf{PRG}^{|\pi\rangle}(s))=1] - \Pr_{\phi\leftarrow\Phi_{t,n},s\leftarrow\{0,1\}^{\ell}}[T(\mathsf{PRG}^{|\phi\rangle}(s))=1] \right| \le \epsilon_0,$$

where $\epsilon_0 := (8\pi^2/3)(q^3/2^t) = (8\pi^2/3)(q^3/S_p^6)$. Using the triangle inequality, we obtain

$$\left| \Pr_{z\leftarrow\{0,1\}^{\ell+k}}[T(z)=1] - \Pr_{\phi\leftarrow\Phi_{t,n},s\leftarrow\{0,1\}^{\ell}}[T(\mathsf{PRG}^{|\phi\rangle}(s))=1] \right| \le \epsilon + 2^{-S_p} + \epsilon_0.$$

Here, we note that $\mathsf{PRG}^{|\phi\rangle}(s)$ may fail because the construction might exploit the fact that π is the permutation. However, the failure probability of $\mathsf{PRG}^{|\phi\rangle}(s)$ is at most ϵ_0 due to Theorem 2.1.

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

Now, we define

$$\mathsf{PRG}'(s') := \mathsf{PRG}'(s, f_0, \dots, f_{2q}) = \mathsf{PRG}^{|F\rangle}(s).$$

According to Zhandry's lemma (Lemma 2.1), the $2q$-wise independent hash functions and the random functions are indistinguishable up to q-queries and we have

$$\Pr_{\phi\leftarrow\Phi_{t,n},s\leftarrow\{0,1\}^{\ell}}[T(\mathsf{PRG}^{|\phi\rangle}(s))=1] = \Pr_{s'\leftarrow\{0,1\}^{\ell'}}[T(\mathsf{PRG}'(s'))=1].$$

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

Remark 4.1. We note that $\mathsf{PRG}'\colon \{0,1\}^{\ell'} \to \{0,1\}^{\ell'+k}$ is efficiently computable because it just runs PRG with simulation of F based on $2q$-wise independent hash function $f(z) = \sum_i f_i z^i$. Thus, PRG' yields an unconditionally-secure QC-qOWF; if it is not qOWF, then it is not secure 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 5.1. *Construction of an SKE scheme based on qOWP is a pair of oracle procedures* $\mathsf{SKE}^{|\cdot\rangle} = (\mathsf{Enc}^{|\cdot\rangle}, \mathsf{Dec}^{|\cdot\rangle})$ *such that, for all* $\pi \in \Pi_n$*, the resulting* $\mathsf{SKE}^{|\pi\rangle}$ *satisfies the functional definition of an SKE scheme.*

We say that $\mathsf{SKE}^{|\cdot\rangle}$ *is an* (S_p, S_e, ϵ)*-qOWP-to-SKE weak black-box construction if for every* $\pi \in \Pi_n$ *that is* S_p*-hard,* $\mathsf{SKE}^{|\pi\rangle}$ *is* (S_e, ϵ)*-hard.*

We only consider a non-interactive SKE scheme.

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 $x_i = (a_i, b_i) \in \{0,1\}^t \times \{0,1\}^{4t}$, 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 5.1. *Let* $\mathsf{SKE}^{|\cdot\rangle}$ *be an* (S_p, S_e, ϵ)*-qOWP-to-SKE weak black-box construction for message of length* m *using a key of length* k *in which* $\mathsf{Enc}^{|\cdot\rangle}$ *and* $\mathsf{Dec}^{|\cdot\rangle}$ *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* $(S_e, \tilde{\epsilon})$*-secure SKE scheme without any access to oracles, where* $\tilde{\epsilon} = \epsilon + 2^{-S_p+1} + (16\pi^2/3)(q^3/S_p^6)$*.*

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

The hypothesis of the theorem on $\mathsf{SKE}^{|\cdot\rangle} = (\mathsf{Enc}^{|\cdot\rangle}, \mathsf{Dec}^{|\cdot\rangle})$ implies that if π 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

$$\left| \Pr_{s,v \hookleftarrow \mathsf{Enc}^{|\pi\rangle}(s,M_0)}[B(v) = 1] - \Pr_{s,v \hookleftarrow \mathsf{Enc}^{|\pi\rangle}(s,M_1)}[B(v) = 1] \right| < \epsilon.$$

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

According to Theorem 3.1, $\pi \in \Pi_{t,n}$ 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

$$\left| \begin{array}{l} \Pr_{s,\pi \hookleftarrow \Pi_{t,n}, v \hookleftarrow \mathsf{Enc}^{|\pi\rangle}(s,M_0)}[B(v) = 1] \\ \quad - \Pr_{s,\pi \hookleftarrow \Pi_{t,n}, v \hookleftarrow \mathsf{Enc}^{|\pi\rangle}(s,M_1)}[B(v) = 1] \end{array} \right| < \epsilon + 2^{-S_p+1}.$$

Using Zhandry's lemma (Theorem 2.1), we can replace $\pi \hookleftarrow \Pi_{t,n}$ with $\phi \hookleftarrow \Phi_{t,n}$ as follows:

$$\left| \begin{array}{l} \Pr_{s,\phi \hookleftarrow \Phi_{t,n}, v \hookleftarrow \mathsf{Enc}^{|\phi\rangle}(s,M_0)}[B(v) = 1] \\ \quad - \Pr_{s,\phi \hookleftarrow \Phi_{t,n}, v \hookleftarrow \mathsf{Enc}^{|\phi\rangle}(s,M_1)}[B(v) = 1] \end{array} \right| < \epsilon + 2^{-S_p+1} + 2\epsilon_0 = \tilde{\epsilon}, \quad (3)$$

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 $k' = k + (4q+1) \cdot t$, which is $(S_e, \tilde{\epsilon})$-secure and has no oracle access. Again, we simulate the random function ϕ by $4q$-wise independent hash function. The simulation is very simple: We prepare $F(a,b) := (f(a), b)$, where $f\colon \{0,1\}^t \to \{0,1\}^t : f(a) = \sum_{i=0}^{4q} f_i a^i \in \mathrm{GF}(2^t)$. 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 $C \leftarrow \mathsf{Enc}^{|F\rangle}(s, M)$.
– Dec' parses the shared key s' as s and f and decrypts a ciphertext C by $M' \leftarrow \mathsf{Dec}^{|F\rangle}(s, C)$.

The $(S_e, \tilde{\epsilon})$-security of SKE' directly follows from Eq. (3). □

Remark 5.1. 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.

References

AC02. Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In Helmut Alt and Afonso Ferreira, editors, *STACS 2002*, volume 2285 of *LNCS*, pages 323–334. Springer, Heidelberg, February 2002. 3

ACC+22. Per Austrin, Hao Chung, Kai-Min Chung, Shiuan Fu, Yao-Ting Lin, and Mohammad Mahmoody. On the impossibility of key agreements from quantum random oracles. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 165–194. Springer, Heidelberg, August 2022. 5

AGQY22. Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 237–265. Springer, Heidelberg, November 2022. 2

AIK22. Scott Aaronson, DeVon Ingram, and William Kretschmer. The acrobatics of BQP. In Shachar Lovett, editor, *CCC 2022*, volume 234 of *LIPIcs*, pages 20:1–20:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. 20

AQY22. Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 208–236. Springer, Heidelberg, August 2022. 5

BCKM21a. James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. On the round complexity of secure quantum computation. In Malkin and Peikert [MP21], pages 406–435. 2

BCKM21b. James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In Malkin and Peikert [MP21], pages 467–496. 2

BHMT00. Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation and Information*, volume 305 of *Contemporary Mathematics*, pages 53–74. AMS, 2000. See also arXiv:quant-ph/0005055. 10

BI20. Anne Broadbent and Rabib Islam. Quantum encryption with certified deletion. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part III*, volume 12552 of *LNCS*, pages 92–122. Springer, Heidelberg, November 2020. 2

BT06. Andrej Bogdanov and Luca Trevisan. Average-case complexity. *Foundations and Trends® in Theoretical Computer Science*, 2(1):1–106, 2006. 19

CGLQ20. Kai-Min Chung, Siyao Guo, Qipeng Liu, and Luowen Qian. Tight quantum time-space tradeoffs for function inversion. In *61st FOCS*, pages 673–684. IEEE Computer Society Press, November 2020. 4, 9

CLM23. Kai-Min Chung, Yao-Ting Lin, and Mohammad Mahmoody. Black-box separations for non-interactive classical commitments in a quantum world. In Hazay and Stam [HS23], pages 144–172. 5

DTT10. Anindya De, Luca Trevisan, and Madhur Tulsiani. Time space tradeoffs for attacks against one-way functions and PRGs. In Rabin [Rab10], pages 649–665. 9

FOC12. *53rd FOCS*. IEEE Computer Society Press, October 2012. 17, 19

Gen10. Craig Gentry. Toward basing fully homomorphic encryption on worst-case hardness. In Rabin [Rab10], pages 116–137. 2

GGK03. Rosario Gennaro, Yael Gertner, and Jonathan Katz. Lower bounds on the efficiency of encryption and digital signature schemes. In *35th ACM STOC*, pages 417–425. ACM Press, June 2003. 1, 14

GGKT05. Rosario Gennaro, Yael Gertner, Jonathan Katz, and Luca Trevisan. Bounds on the efficiency of generic cryptographic constructions. *SIAM Journal on Computing*, 35(1):217–246, 2005. 1, 3, 4, 9, 14, 20, 22

GL89. Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *21st ACM STOC*, pages 25–32. ACM Press, May 1989. 2

GLSV21. Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in MiniQCrypt. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 531–561. Springer, Heidelberg, October 2021. 2

GT00. Rosario Gennaro and Luca Trevisan. Lower bounds on the efficiency of generic cryptographic constructions. In *41st FOCS*, pages 305–313. IEEE Computer Society Press, November 2000. 1, 2, 3, 5

HMNY21. Taiga Hiroka, Tomoyuki Morimae, Ryo Nishimaki, and Takashi Yamakawa. Quantum encryption with certified deletion, revisited: Public key, attribute-based, and classical communication. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 606–636. Springer, Heidelberg, December 2021. 2

HS12. Thomas Holenstein and Makrand Sinha. Constructing a pseudorandom generator requires an almost linear number of calls. In FOCS 2012 [FOC12], pages 698–707. 2, 5

HS23. Carmit Hazay and Martijn Stam, editors. *EUROCRYPT 2023, Part I*, volume 14004 of *LNCS*. Springer, Heidelberg, April 2023. 17, 18

HXY19. Minki Hhan, Keita Xagawa, and Takashi Yamakawa. Quantum random oracle model with auxiliary input. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part I*, volume 11921 of *LNCS*, pages 584–614. Springer, Heidelberg, December 2019. 4, 9

HY20. Akinori Hosoyamada and Takashi Yamakawa. Finding collisions in a quantum world: Quantum black-box separation of collision-resistance and one-wayness. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part I*, volume 12491 of *LNCS*, pages 3–32. Springer, Heidelberg, December 2020. 5

IL89. Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *30th FOCS*, pages 230–235. IEEE Computer Society Press, October / November 1989. 14, 20

Imp95. Russell Impagliazzo. Hard-core distributions for somewhat hard problems. In *36th FOCS*, pages 538–545. IEEE Computer Society Press, October 1995. 1

JLS18. Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 126–152. Springer, Heidelberg, August 2018. 2, 20

KL20. Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman & Hall/CRC, third edition, 2020. 2

KQST23. William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In Barna Saha and Rocco A. Servedio, editors, *STOC 2023*, pages 1589–1602. ACM, 2023. 20

Kre21. William Kretschmer. Quantum Pseudorandomness and Classical Complexity. In Min-Hsiu Hsieh, editor, *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*, volume 197 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:20, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. 20

KST99. Jeong Han Kim, Daniel R. Simon, and Prasad Tetali. Limits on the efficiency of one-way permutation-based hash functions. In *40th FOCS*, pages 535–542. IEEE Computer Society Press, October 1999. 1

KY10. Akinori Kawachi and Tomoyuki Yamakami. Quantum hardcore functions by complexity-theoretical quantum list decoding. *SIAM Journal on Computing*, 39(7):2941–2969, 2010. The preliminary version is in *ICALP 2006*. 3

Liu23. Qipeng Liu. Non-uniformity and quantum advice in the quantum random oracle model. In Hazay and Stam [HS23], pages 117–143. 4, 9

MP21. Tal Malkin and Chris Peikert, editors. *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, Virtual Event, August 2021. Springer, Heidelberg. 16

NABT15. Aran Nayebi, Scott Aaronson, Aleksandrs Belovs, and Luca Trevisan. Quantum lower bound for inverting a permutation with advice. *Quantum Information & Computation*, 15(11&12):901–913, 2015. 4, 9, 10

OTU00. Tatsuaki Okamoto, Keisuke Tanaka, and Shigenori Uchiyama. Quantum public-key cryptosystems. In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880 of *LNCS*, pages 147–165. Springer, Heidelberg, August 2000. 2

Rab10. Tal Rabin, editor. *CRYPTO 2010*, volume 6223 of *LNCS*. Springer, Heidelberg, August 2010. 17

RTV04. Omer Reingold, Luca Trevisan, and Salil P. Vadhan. Notions of reducibility between cryptographic primitives. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 1–20. Springer, Heidelberg, February 2004. 2

WC81. Mark N. Wegman and Larry Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265–279, 1981. 13

Zha12a. Mark Zhandry. How to construct quantum random functions. In FOCS 2012 [FOC12], pages 679–687. 4, 7

Zha12b. Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Heidelberg, August 2012. 4, 6

Zha15. Marc Zhandry. A note on the quantum collision and set equality problems. *Quantum Information & Computation*, 15(7&8):557–567, 2015. 4, 7

A Complexity Class and Instance Generator

For the basic complexity classes (P, NP, BQP, and QMA), 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 sting $w \in \{0,1\}^*$ 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 stings $w \in \{0,1\}^*$ 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,μ) is said to be a *distributional problem* if $L \subseteq \{0,1\}^*$ and $\mu = \{\mu_n\}_{n\in\mathbb{Z}^{\geq 0}}$ is an ensamble of probability distributions. Following the definition of P-sampleable distribution, we define its quantum version as follows:

Definition A.1. *A distribution μ 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 (NP, P-Samp).

Definition A.2. (QMA, BQP-Samp) *denotes the set of distributional problems (L,μ) with $L \in$ QMA and* BPQ*-sampleable μ.* (QCMA, BQP-Samp) *denotes the set of distributional problems (L,μ) with $L \in$ QCMA and* BPQ*-sampleable μ.*

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 $(L,\mu) \in$ (QCMA, BQP-Samp) is (S,ϵ)-hard if 1) there exists a QPT instance generator E such that E's first output distributes as μ and 2) for any quantum machine A of size at most $S = S(n)$, $\Pr_{(x,w)\hookleftarrow E(1^n)}[V(x,A(x))=1] \leq \epsilon$, where V is a verifier of (L,μ).

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

Definition A.3. *We say that a distributional problem (L, μ) is in* AvgBQP *if there exists a quantum algorithm A such that 1) for every n, δ, x, $\Pr_A[A(x, 1^n, \delta) \notin \{L(x), \bot\}] \leq 1/4$ holds, where $L(x) \in \{0,1\}$ is an indicator function; 2) for every n, δ, $\Pr_{x\sim\mu_n}[\Pr_A[A(x, 1^n, \delta) = \bot] \geq 1/4] \leq \delta$ holds; 3) and A runs in a polynomial time of n/δ.*

Relations: If there exists qOWF, then we have $\mathsf{FBQP} \neq \mathsf{FQCMA}$ (and $\mathsf{BQP} \neq \mathsf{QCMA}$). Kretschmer [Kre21] showed that there exists an oracle relative to which $\mathsf{BQP} = \mathsf{QMA}$ but secure PRS exists. Aaronson, Ingram, and Kretschmer [AIK22] showed that there exists an oracle relative to which $\mathsf{P} = \mathsf{NP}$ but $\mathsf{BQP} \neq \mathsf{QCMA}$. They also showed that there exists an oracle relative to which $\mathsf{P} \neq \mathsf{NP}$ but $\mathsf{BQP} = \mathsf{QCMA} = \mathsf{QMA}$. Kretschmer, Qian, Sinha, and Tal [KQST23] further showed that there exists an oracle relative to which $\mathsf{P} = \mathsf{NP}$ 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, $(\mathsf{QCMA}, \mathsf{BQP\text{-}samp})$, 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 $(\mathsf{QCMA}, \mathsf{BQP\text{-}samp}) \not\subseteq \mathsf{AvgBQP}$, quantum analogue of $(\mathsf{NP}, \mathsf{P\text{-}samp}) \not\subseteq \mathsf{AvgP}$.

The proof is essentially the same as that of [GGKT05]:

Theorem B.1. *Let $(\mathsf{Enc}, \mathsf{Dec})$ be an (S, δ)-secure perfectly-correct quantum SKE scheme whose message length is m and key length is $k < m$. Let S_e be the size of the circuit of Enc and let S_d be the size of the circuit of Dec. For any ℓ, there exists a pair of a QPT instance generator and a QPT verifier (E, D) that is $(S - 2\ell S_e - 2\ell S_d - \mathsf{poly}(m, k, \ell), \ell\delta + 2^{-\ell(m-k)})$-hard.*

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

Proof. Let $\mathsf{SKE}_\ell = (\mathsf{Enc}_\ell, \mathsf{Dec}_\ell)$ be an intermediate quantum SKE scheme whose message length and key length are ℓm and ℓk, respectively defined as follows: Enc_ℓ takes $(sk_1, \dots, sk_\ell) \in \{0,1\}^{\ell k}$ and $(M_1, \dots, M_\ell) \in \{0,1\}^{\ell m}$ as input and outputs $(C_1, \dots, C_\ell)$ where $C_i \hookleftarrow \mathsf{Enc}(sk_i, M_i)$; Dec_ℓ takes $(sk_1, \dots, sk_\ell) \in \{0,1\}^{\ell k}$ and $(C_1, \dots, C_\ell)$ as input and outputs

$(\mathsf{Dec}(sk_1, C_1), \ldots, \mathsf{Dec}(sk_\ell, C_\ell)) \in \{0,1\}^{\ell m}$. By the standard hybrid argument, it is easy to see that SKE_ℓ is $(S - \ell S_e, \ell\delta)$-secure quantum SKE scheme.

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

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

$$adv_B \coloneqq \Pr_{sk \leftarrow\!\!\$ \{0,1\}^{\ell k}, M \leftarrow\!\!\$ \{0,1\}^{\ell m}, c \leftarrow \mathsf{Enc}_\ell(sk, M)}[D(c\|M, B(c\|M)) = 1] > \delta'.$$

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

$$\left| \begin{array}{l} \Pr_{sk \leftarrow\!\!\$ \{0,1\}^{\ell k}, M_0, M_1 \leftarrow\!\!\$ \{0,1\}^{\ell m}, c \leftarrow \mathsf{Enc}_\ell(sk, M_0)}[A(M_0, M_1, c) = 1] \\ \quad - \Pr_{sk \leftarrow\!\!\$ \{0,1\}^{\ell k}, M_0, M_1 \leftarrow\!\!\$ \{0,1\}^{\ell m}, c \leftarrow \mathsf{Enc}_\ell(sk, M_1)}[A(M_0, M_1, c) = 1] \end{array} \right|.$$

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 $sk'\|M'$. It then checks whether both $\mathsf{Dec}_\ell(sk', M') = C$ and $M' = M_0$ hold or not. If so, B succeeds to find such sk' 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

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

We also have

$$\begin{aligned} &\Pr_{sk \leftarrow\!\!\$ \{0,1\}^{\ell k}, M_0, M_1 \leftarrow\!\!\$ \{0,1\}^{\ell m}, c \leftarrow \mathsf{Enc}_\ell(sk, M_1)}[A(M_0, M_1, c) = 1] \\ &\leq \Pr_{sk \leftarrow\!\!\$ \{0,1\}^{\ell k}, M_0, M_1 \leftarrow\!\!\$ \{0,1\}^{\ell m}, c \leftarrow \mathsf{Enc}_\ell(sk, M_1)}[\exists sk' \text{ s.t. } \mathsf{Dec}_\ell(sk', c) = M_0] \\ &\leq \sum_{sk' \in \{0,1\}^{\ell k}} \Pr_{sk \leftarrow\!\!\$ \{0,1\}^{\ell k}, M_0, M_1 \leftarrow\!\!\$ \{0,1\}^{\ell m}, c \leftarrow \mathsf{Enc}_\ell(sk, M_1)}[\mathsf{Dec}_\ell(sk', c) = M_0] \\ &\leq \sum_{sk' \in \{0,1\}^{\ell k}} 2^{-\ell m} = 2^{-\ell(k-m)}, \end{aligned}$$

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

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 $S_A = S' - \ell S_d - \mathsf{poly}(m,k,\ell) = S - \ell S_e - \ell S_d - \mathsf{poly}(m,k,\ell)$ and $\delta_A = \delta' - 2^{-\ell(k-m)} = \ell\delta$ as we wanted. □

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