Quantum trapdoor functions from classical one-way functions

Andrea Coladangelo *

Paul G. Allen School of Computer Science and Engineering, University of Washington

Abstract

We introduce the notion of a *quantum trapdoor function*. This is an efficiently computable unitary that takes as input a "public" quantum state and a classical string x, and outputs a quantum state. This map is such that (i) it is hard to invert, in the sense that it is hard to recover x given the output state (and many copies of the public state), and (ii) there is a classical trapdoor that allows efficient inversion. We show that a quantum trapdoor function can be constructed from any quantum-secure one-way function. A direct consequence of this result is that, *assuming just the existence of quantum-secure one-way functions*, there exist: (i) a public-key encryption scheme with a *quantum* public key, and (ii) a *two-message* key-exchange protocol, assuming an appropriate notion of a quantum authenticated channel.

Contents

*Email: coladan@cs.washington.edu

1 Introduction

One-way functions and *trapdoor* functions are two of the most well-studied cryptographic primitives. The former are functions that are easy to compute but hard to invert on average. The latter satisfy the same property with the additional feature that there exists some special information, a "trapdoor", that enables efficient inversion, but without which inversion remains hard.

In classical cryptography, there is a marked dividing line between one-way functions and trapdoor functions. One-way functions are equivalent to so-called "minicrypt" primitives, e.g. pseudorandom generators, pseudorandom functions, commitments and *private-key* encryption. On the other hand, (injective) trapdoor functions imply *public-key* cryptosystems [Yao82, GM82]. This dividing line can be made formal: one can provably show that injective trapdoor functions cannot be constructed from black-box use of one-way functions [IR89, BMG09].

In this work, we consider the question of whether the dividing line between one-way and trapdoor functions also stands in a quantum world, i.e. a world where parties have access to quantum computation and communication. Concretely, we ask:

Can we achieve some version of trapdoor functions and public-key encryption from one-way functions, in a quantum world?

1.1 Our results

We provide a partial positive answer to the question above. Our first contribution is to introduce the notion of a *quantum trapdoor function* (QTF). This is similar to a classical trapdoor function, but differs in two crucial ways:

- The generation procedure outputs a classical trapdoor tr and a *quantum* evaluation key $|eval\rangle$.
- Evaluation takes as input a classical string x, and the evaluation key $|eval\rangle$, and outputs a *quantum* state $|\psi_x\rangle$.

For security, we require that (without the trapdoor) it should be hard to recover x from $|\psi_x\rangle$, *even given access to polynomially many copies of* $|eval\rangle$. On the other hand, given the trapdoor tr, inversion is easy. We additionally restrict our attention to the case where (the same) $|eval\rangle$ can be efficiently generated given the trapdoor tr. The reason for this is that we think of $|eval\rangle$ as being a "publicly" available resource: anyone can request copies of $|eval\rangle$ from the party who has the trapdoor.

Our main result is the following.

Theorem 1 (informal)**.** *Quantum trapdoor functions exist, assuming the existence of quantum-secure one-way functions.*

Our construction is remarkably simple. It uses as a building block a construction of pseudorandom states from one-way functions proposed by Ji, Liu, and Song [JLS18], and later proven secure by Brakerski and Shmueli [BS19]. To achieve the trapdoor property we leverage the particular structure of this PRS construction. To prove security, we invoke the PRS property in order to reduce an adversary that inverts our quantum trapdoor function to one that succeeds at a certain information-theoretic "state-discrimination" task involving Haar random states.

In classical cryptography, the most common application of trapdoor functions is to construct public-key encryption. Any injective trapdoor function implies a public-key encryption scheme, where the secret key is the trapdoor, and the public key is the (description of the) tradpoor function f itself. In particular, encryption of a message $m \in \{0,1\}$ takes the form $(f(x), hc(x) \oplus m)$, where x is sampled uniformly at random, and $hc(x)$ is a hardcore bit of x, e.g. the one obtained via Goldreich-Levin [GL89]. A quantum trapdoor function yields a public-key encryption scheme in an analogous way, except that the "public key" is now the evaluation key $|eval\rangle$, and hence is a quantum state. Thus, the following is a direct consequence of Theorem 1.

Corollary 1 (informal)**.** *Assuming the existence of quantum-secure one-way functions, there exists a public-key encryption scheme with a* quantum *public key.*

While a quantum state as public key is most likely impractical, and in some sense against the spirit of public-key encryption (where the point is that a party's public-key should be readily available to any party that wishes to send them an encrypted message), we still find the conclusion significant from a conceptual standpoint: the quantum public key is still "public" in the sense that the scheme is secure even if an adversary obtains an arbitrary (polynomial) number of copies of the public key.

Our result suggests that there is some subtlety in defining what it means for quantum information to be "public": while in the classical setting having access to a single copy of a string is trivially equivalent to knowing a circuit that generates the string, in the quantum setting, having *access to many copies of a state* is crucially different (in the computational setting) from *knowing a circuit that generates the state*.

Corollary 1 implies the following simple *two-message* key-exchange protocol: Alice samples a secret key and a public key, and sends the public key to Bob; then, Bob sends back an encryption of a uniformly sampled key, which Alice is able to decrypt. This protocol is secure in a model where the quantum channel used by Alice and Bob is *authenticated* in the following sense: Alice and Bob can trust the origin of the quantum message that they receive, and that it has not been tampered with, but the adversary obtains a copy of the same quantum message. One can think of this model as capturing a scenario where Alice is broadcasting many copies of the same state (which she can efficiently prepare) to a network of parties which includes Bob and potentially also an adversary. We have the following.

Corollary 2 (informal)**.** *Assuming the existence of quantum-secure one-way functions, and of a quantum authenticated channel as described above, there exists a two-message key-exchange protocol.*

To place this result into context, in the analogous classical setting with authenticated channels, there is a well-known two-message key-exchange protocol based on the hardness of Decision Diffie-Hellman (DDH) [DH76], but one can provably show that key-exchange, with any number of rounds, *cannot be realized from black-box use of one-way functions* [IR89]. On the other hand, if one allows for more rounds of communication in the quantum setting, key exchange can of course be realized unconditionally via the BB84 protocol (where *classical* authenticated channels suffice) [BB84]. We refer to Section 5.2 for a more detailed discussion about Corollary 2, and the need for authenticated channels.

1.2 Related work

Our results fit into a broader line of work that aims to understand how the landscape of cryptographic primitives changes in the presence of quantum information. The most well-known result in this direction is that key-exchange (or key-distribution) can be realized unconditionally using quantum communication, via the BB84 protocol [BB84]. However, this is somewhat of a standalone result, and does not directly imply that any of the other primitives in "cryptomania", e.g. trapdoor functions, public-key encryption, oblivious transfer and multiparty-computation, can be realized unconditionally or even from weaker assumptions than what is known classically. In a more recent development, two concurrent works [BCKM21, GLSV21] show that oblivious transfer, and hence multiparty computation, can be realized from one-way functions. One can think of the constructions from these two works as making a more sophisticated use of the original ideas from BB84 in order to instantiate a template for oblivious transfer proposed in [CK88].

Our work is the first to draw a connection between trapdoor functions and one-way functions in the quantum setting, and it does so by leveraging a simple novel idea based on the use of pseudorandom states (PRS). While in our work we only make use of the structure of a particular construction of PRSs from one-way functions, PRSs have recently received increasing attention more generally. They have been a central object of study in a related line of work that explores the possibility of basing cryptography on the computational hardness of *genuinely quantum* problems (i.e. problems with quantum inputs and/or quantum outputs) [AQY22, BCQ22, MY22]. The existence of PRSs is an example of a computational assumption, involving a quantum problem, that is potentially weaker than the existence of one-way functions. While PRSs can be constructed from one-way functions, the converse is not known to be true: there is in fact evidence to the contrary, namely an oracle with respect to which PRSs exist, but one-way functions do not [Kre21, KQST22].

1.3 Open questions

The main open questions left open by our work are:

- Can we build a quantum trapdoor function with a *classical* evaluation key from quantum-secure one-way functions? This would imply a public-key encryption scheme with a *classical* public key (and quantum ciphertexts) from one-way functions. Note that the current definition of quantum trapdoor function asks for a classical trapdoor. Does relaxing this requirement to allow for a *quantum* secret key help achieve a scheme with a classical public key? If not, can we prove that this is not possible if one makes black-box use of the one-way function? The current classical black-box separation of public-key encryption and one-way functions does not seem to directly apply as it relies on the ciphertext being classical.
- In the converse direction, does the existence of a *quantum* trapdoor function (any of the variants), imply the existence of *classical* one-way function? While in the classical setting trapdoor functions are a special case of one-way functions, it is unclear what the answer to the above question is. It seems plausible that there exists an oracle relative to which quantum trapdoor functions exist, but classical one-way functions do not. An intermediate step in this direction would be to exhibit an oracle relative to which quantum trapdoor functions exists, but classical trapdoor functions do not.

2 Technical Overview

In this overview, we informally describe the construction of a quantum trapdoor function from one-way functions, and discuss its security. As mentioned, this construction uses as a building block a construction of PRSs from one-way functions due to Ji, Liu, and Song [JLS18], and later proven secure by Brakerski and Shmueli [BS19].

2.1 Pseudorandom States from one-way functions

First, recall what a PRS is. A PRS can be thought of as a *quantum analogue of a pseudorandom generator (PRG)*. A PRS takes as input a classical seed $s \in \{0,1\}^n$, where n is a security parameter, and outputs a state $|PRS(s)\rangle$. We ask that the PRS satisfies the following property: it is computationally hard to distinguish between polynomially many copies of $|PRS(s)\rangle$, for a uniformly random s, and polynomially many copies of a state sampled from the Haar distribution. More precisely, for any quantum polynomial time A, and any $m = poly(n)$,

$$\left|\Pr[A(|PRS(s)\rangle^{\otimes m}) = 1 : s \leftarrow \{0,1\}^n] - \Pr[A(|\psi\rangle^{\otimes m}) = 1 : |\psi\rangle \leftarrow \text{Haar}]\right| = \mathsf{negl}(n)\,.$$

The following is a construction of a PRS from any (quantum-secure) one-way function. The construction is simple (although the proof that it is secure is quite involved). Let $\mathsf{PRF} : \mathcal{K} \times \mathcal{X} \leftarrow \{0,1\}$ be a pseudorandom function (PRF) with a one-bit output, where there is an implicit security parameter that we are omitting. Then the PRS seed is a PRF key k, and

$$|PRS(k)\rangle = \frac{1}{|\mathcal{X}|}\sum_{y\in\mathcal{X}}(-1)^{\mathsf{PRF}(k,y)}\,|y\rangle\ .$$

Invoking the security of the PRF, we deduce that m copies of $|PRS(k)\rangle$ are computationally indistinguishable from m copies of a state that is a uniform superposition with a uniformly random ± 1 phase. Showing that the latter is *statistically* indistinguishable from m copies of a Haar random state is quite involved, and is the main technical contribution of [BS19]. A simpler proof of this was later given in [AGQY23].

Note that the state $|PRS(k)\rangle$ can be generated efficiently by (i) preparing a uniform superposition over the elements of $\mathcal{X}$, (ii) initializing a second register in the state $|-\rangle$, and (iii) computing PRF in superposition, treating the second register as the output register.

2.2 Quantum trapdoor functions

As informally described earlier, a quantum trapdoor function (QTF) consists of the following quantum polynomial time algorithms:

(i) A generation procedure that outputs a classical trapdoor tr and a *quantum* evaluation key $|eval\rangle$. Additionally we ask that there be an efficient algorithm to generate (the same) $|eval\rangle$ given tr.

(ii) An evaluation procedure that takes as input a string x, and $|eval\rangle$, and outputs a *quantum* state $|\psi_x\rangle$.

(iii) An inversion procedure that takes as input the trapdoor tr and a state $|\psi_x\rangle$ and returns x.

For security, we require that, without knowing tr, it is hard to recover x given $|\psi_x\rangle$ and an arbitrary (polynomial) number of copies of $|eval\rangle$.

Construction The simple idea behind our construction of a QTF is the following. Consider the PRS construction described in Subsection 2.1. We will take the trapdoor of our QTF to be a PRF key k (uniformly sampled), and the evaluation key to be $|eval\rangle = |PRS(k)\rangle$. For concreteness, for security parameter n, take the domain $\mathcal{X}$ of PRF to be $\{0,1\}^n$, so that $|\mathrm{PRS}(k)\rangle$ is an n-qubit state. Then, the evaluation of the QTF on input x, and evaluation key $|PRS(k)\rangle$, is

$$|\psi_x\rangle = Z^x |PRS(k)\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y+\mathsf{PRF}(k,y)} |y\rangle \ .$$

Here Z^x denotes the n-qubit operator that applies Pauli Z to the i-th qubit or not based on the value of the i-th bit x_i.

To invert, i.e. to recover x given $|\psi_x\rangle$ and the trapdoor k, simply "undo" the PRF phase, namely apply the unitary $G_{\mathsf{PRF}}(k) : |y\rangle \mapsto (-1)^{\mathsf{PRF}(k,y)} |y\rangle$. The crucial observation is that $G_{\mathsf{PRF}}(k)$ commutes with Z^x. Thus, the PRF phase can be undone "out of order", and

$$G_{\mathsf{PRF}}(k) |\psi_x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle = H^{\otimes n} |x\rangle \ .$$

Finally, applying $H^{\otimes n}$ returns x.

Security Recall that we wish to establish that, without the trapdoor, it is hard to recover x given $|\psi_x\rangle$ and m copies of the evaluation key $|eval\rangle$, for any $m = poly$. In the case of our construction, this means that it should be hard to recover x from the state

$$\left(|Z^x\rangle |PRS(k)\rangle \right) \otimes |PRS(k)\rangle^{\otimes m} \ .$$

We can think of this of a "state discrimination" task: given a (uniformly random) mixed state from the ensemble

$$\left\{ \mathbb{E}_k \left(Z^x |PRS(k)\rangle \langle PRS(k)| Z^x \right) \otimes \left(|PRS(k)\rangle \langle PRS(k)| \right)^{\otimes m} \right\}_{x\in\{0,1\}^n} , \tag{1}$$

the task is to guess x. We wish to argue that the probability of guessing x is negligible.

Now, suppose that there is an adversary A that breaks security of our QTF construction, and thus succeeds at the above discrimination task with non-negligible probability. Then, by invoking the security of the PRS, it must be the case the same adversary A also succeeds with non-negligible probability when we replace $|PRS(k)\rangle$ with a Haar random state (otherwise we can construct an adversary that has non-negligible advantage at distinguishing copies of the PRS state from copies of a Haar random state). Thus, A must also succeed with non-negligible probability at the following discrimination task: given a uniformly random mixed state from the ensemble

$$\left\{ \mathbb{E}_{|\psi\rangle\leftarrow \mathrm{Haar}(2^n)} \left(Z^x |\psi\rangle \langle\psi| Z^x \right) \otimes \left(|\psi\rangle \langle\psi| \right)^{\otimes m} \right\}_{x\in\{0,1\}^n} , \tag{2}$$

the task is to guess x (where $|\psi\rangle \leftarrow \mathrm{Haar}(2^n)$ denotes sampling from the Haar distribution on n-qubit states).

We get a contradiction by showing that the optimal success probability at the state discrimination task in (2) is exponentially small when $m = poly(n)$ (see Lemma 5 for the precise scaling). At first, this might seem slightly surprising because the "classical analogue" of this discrimination task is *easy*, and can be solved perfectly. The classical analogue is distinguishing between *distributions over strings* given a single sample.

Thinking of the operator Z^x as "xoring x" (in the Hadamard basis), and realizing that copies of a string are "for free" classically, a natural classical analogue of the state discrimination task in (2) is: given a single sample drawn from one of the distributions in the following ensemble (where x is picked uniformly at random)

$$\{(\psi \oplus x, \psi) : \psi \leftarrow \{0,1\}^n\}_{x \in \{0,1\}^n}, \tag{3}$$

guess x. Clearly one can recover x by taking the xor of ϕ and $\phi \oplus x$. In contrast, this intuition fails for the state discrimination task in (2): even though one has access to polynomially many copies of $|\psi\rangle$, it is unclear how one can "compare" the first copy (to which Z^x was applied) to the others in order to recover x. The proof that recovering x can be done at most with exponentially small probability is somewhat involved, and we refer to Section 4.3 for the details.

3 Preliminaries

For $n \in \mathbb{N}$, we denote $[n] = \{1, \ldots, n\}$. For a finite set X, we write $x \leftarrow X$ to mean that x is sampled uniformly at random from S.

We think of a quantum algorithm as a uniform family of quantum circuits. If the circuits in the family are polynomial-sized then we say that the algorithm is quantum polynomial time, which we abbreviate as QPT. We use the notation *poly* to denote an (unspecified) polynomially-bounded function.

3.1 Quantum information

We introduce some facts that we will use later on. For $n \in \mathbb{N}$, denote by $\{|j\rangle : j \in [2^n]\}$ the standard basis of the space of n qubits. Let Z be the Pauli Z operator. For $s \in \{0,1\}^n$, let $Z^s := \bigotimes_{i=1}^n Z^{s_i}$.

Lemma 1 (Pauli Z twirl)**.** *Let $n, m \in \mathbb{N}$. For any $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes m}$,*

$$\mathbb{E}_{s \leftarrow \{0,1\}^n} (Z^s \otimes I) |\psi\rangle \langle\psi| (Z^s \otimes I) = \sum_{j \in [2^n]} (|j\rangle \langle j| \otimes I) |\psi\rangle \langle\psi| (|j\rangle \langle j| \otimes I).$$

Proof. This follows from a straightforward calculation. □

We will also make use of what is referred to as the "Pretty Good Measurement". In a state discrimination task, one receives a single copy of a (mixed) state ρ_x from an ensemble $\{\rho_x\}_{x \in \mathcal{X}}$, where $\mathcal{X}$ is some index set. The goal is to correctly guess x, where usually x is sampled uniformly at random from $\mathcal{X}$. Let $\sigma := \sum_x \rho_x$. Then, the "Pretty Good Measurement" (PGM) is the POVM $\{M_x\}_{x \in \mathcal{X}} \cup \{M_\perp\}$ where $M_x = \sigma^{-\frac{1}{2}} \rho_x \sigma^{-\frac{1}{2}}$ and $M_\perp = \mathbb{1}_{\mathrm{Ker}(\sigma)}$ is the projection onto the kernel of σ.[1]. While in general the PGM may not be the POVM that gives the optimal success probability at the state discrimination task, the following lemma says that the PGM is "pretty good".

Lemma 2 (PGM is optimal up to quadratic loss)**.** *If p is the optimal success probability at a state discrimination task, then the success probability of the PGM for the same task is at least p^2.*

3.2 Pseudorandom functions

We recall the notion of *quantum-secure* pseudorandom functions.

Definition 1 (Quantum-secure pseudorandom function)**.** *Let $\mathsf{PRF} = \{\mathsf{PRF}_n\}_{n \in \mathbb{N}}$, $\mathsf{PRF}_n : \mathcal{K}_n \times \mathcal{X}_n \to \mathcal{Y}_n$ be an efficiently computable function, where $\mathcal{K}_n$ is referred to as the key space, $\mathcal{X}_n$ as the domain, and $\mathcal{Y}_n$ as the co-domain. We say that PRF is a quantum-secure pseudorandom function if for every (non-uniform) QPT oracle algorithm A, there exists a negligible function negl such that, for all $n \in \mathbb{N}$,*

$$\left| \Pr_{k \leftarrow \mathcal{K}_n} [A^{\mathsf{PRF}(k,\cdot)}(1^n) = 1] - \Pr_{O \leftarrow \mathcal{Y}^{\mathcal{X}}} [A^O(1^n) = 1] \right| \leq \mathsf{negl}(n).$$

Quantum-secure pseudorandom functions exist, assuming the existence of quantum-secure one-way functions [Zha12].

[1] Equivalently, to get a POVM without an additional "$\perp$" outcome, the POVM element $M_\perp$ can be summed to one of the other POVM elements without affecting any of the outcome probabilities

3.3 Quantum randomness and pseudorandomness

3.3.1 The Haar Measure on Quantum States

The Haar measure on a d-dimensional quantum state is the uniform (continuous) probability distribution over d-dimensional quantum states i.e. the uniform distribution over unit vectors in $\mathbb{C}^d$. It can be thought of as the quantum analogue of a classical uniform distribution over strings.

For $d, m \in \mathbb{N}$, we denote the density matrix obtained by sampling a state according to the Haar measure on d-dimensional states, and outputting m copies of it, as

$$\mathbb{E}_{|\psi\rangle \leftarrow \mathrm{Haar}(d)} \left[(|\psi\rangle \langle\psi|)^{\otimes m} \right] . \tag{4}$$

For a Hilbert space $\mathcal{H}$, we sometimes also denote the Haar measure on states in $\mathcal{H}$ as $\mathrm{Haar}(\mathcal{H})$.

We refer to $\mathrm{span}\{|\phi\rangle^{\otimes m} : |\phi\rangle \in \mathbb{C}^d\}$ as the *symmetric subspace* of $(\mathbb{C}^d)^{\otimes m}$. We will later make use of the following characterization of the density matrix in (4). Let $\Pi^{d,m}_{\mathrm{sym}}$ denote the orthogonal projector onto the *symmetric subspace* of $(\mathbb{C}^d)^{\otimes m}$. We have the following.

Lemma 3 ([Har13])**.** *Let $d, m \in \mathbb{N}$. Then,*

$$\mathbb{E}_{|\psi\rangle \leftarrow \mathrm{Haar}(d)} \left[(|\psi\rangle \langle\psi|)^{\otimes m} \right] = \binom{d+m-1}{m}^{-1} \Pi^{d,m}_{\mathrm{sym}} .$$

We will also use the fact that the symmetric subspace has the following convenient basis. For $d, m \in \mathbb{N}$, define $\mathcal{I}_{d,m} = \{(t_1, .., t_d) : t_1, \cdots, t_d \in \mathbb{N}, t_1 + \cdots + t_d = m\}$. For a vector $\vec{j} = (j_1, \ldots, j_m) \in [d]^m$, denote by $T(\vec{j})$ its *type*, i.e. $T(\vec{j})$ is defined to be the vector in $\mathcal{I}_{d,m}$ whose i-th entry is the number of times i appears in the string $(j_1, \ldots, j_m)$. For $\vec{t} \in \mathcal{I}_{d,m}$, define

$$s(\vec{t}) := \binom{m}{\vec{t}}^{-\frac{1}{2}} \sum_{\vec{j}:T(\vec{j})=\vec{t}} |j_1, \ldots, j_m\rangle ,$$

where $\binom{m}{\vec{t}} = \frac{m!}{t_1! \ldots t_d!}$. The $s(\vec{t})$ vectors form an orthonormal basis of the symmetric subspace.

Lemma 4 ([Har13])**.** *Let $d, m \in \mathbb{N}$. Then,*

$$\mathrm{span}\{|\phi\rangle^{\otimes m} : |\phi\rangle \in \mathbb{C}^d\} = \mathrm{span}\{|s(\vec{t})\rangle : \vec{t} \in \mathcal{I}_{d,m}\} .$$

3.3.2 Pseudorandom states

The notion of pseudorandom quantum states was introduced in [JLS18]. The following is a formal definition.

Definition 2 (Pseudorandom Quantum State (PRS))**.** *A Pseudorandom Quantum State (PRS) is a pair of QPT algorithms* $(\mathsf{GenKey}, \mathsf{GenState})$ *such that the following holds. There is a family of Hilbert spaces $\{\mathcal{H}_n\}_{n\in\mathbb{N}}$, and a family $\{\mathcal{K}_n\}_{n\in\mathbb{N}}$ of subsets of $\{0,1\}^*$ such that:*

- $\mathsf{GenKey}(1^n) \to k$*: Takes as input a security parameter n, and outputs a key $k \in \mathcal{K}_n$.*
- $\mathsf{GenState}(k) \to |\mathrm{PRS}(k)\rangle$*: Takes as input a key $k \in \mathcal{K}_n$, for some n, and outputs a state in $\mathcal{H}_n$. We additionally require that the state on input k be unique, and we denote this as $|\mathrm{PRS}(k)\rangle$.*

Moreover, the following holds. For any (non-uniform) QPT quantum algorithm A, and any $m = poly$, there exists a negligible function negl *such that, for all $n \in \mathbb{N}$,*

$$\left| \Pr_{k \leftarrow \mathsf{GenKey}(1^n)} [A(|\mathrm{PRS}(k)\rangle^{\otimes m(n)}) = 1] - \Pr_{|\psi\rangle \leftarrow \mathrm{Haar}(\mathcal{H}_n)} [A(|\psi\rangle^{\otimes m(n)}) = 1] \right| \leq \mathsf{negl}(n) .$$

A PRS can be constructed from any quantum-secure one-way function [JLS18]. Here we describe a particularly simple construction of PRSs that was proposed, and conjectured to be secure, in [JLS18], and later proven secure in [BS19].

Construction 1 (PRS with binary phase [JLS18, BS19])**.** *Let* $\mathsf{PRF} = \{\mathsf{PRF}_n\}_{n\in\mathbb{N}}$ *be a pseudorandom function family, where* $\mathsf{PRF}_n : \mathcal{K}_n \times \{0,1\}^n \to \{0,1\}$*. Define* $(\mathsf{GenKey}, \mathsf{GenState})$ *as follows.*

- $\mathsf{GenKey}(1^n) \to k$*: Sample a PRF key* $k \leftarrow \mathcal{K}_n$*. Output* k*.*
- $\mathsf{GenState}(k) \to |\mathrm{PRS}(k)\rangle$*: On input* $k \in \mathcal{K}_n$*, output* $|\mathrm{PRS}(k)\rangle = \sum_{y\in\{0,1\}^n} (-1)^{\mathsf{PRF}(k,y)} |y\rangle$*.*

Note that GenState *can be implemented efficiently by initializing an ancilla qubit in the state* $|-\rangle$*, and applying the unitary that computes* $\mathsf{PRF}(k,\cdot)$ *into that qubit.*

Theorem 2 ([BS19])**.** *Construction 1 is a PRS.*

4 Quantum trapdoor functions

4.1 Definition

Definition 3 (Quantum trapdoor function)**.** *A quantum trapdoor function (QTF) is a tuple of QPT algorithms* $(\mathsf{Sample}, \mathsf{Eval}, \mathsf{Invert})$*, where:*

- $\mathsf{GenTR}(1^n) \to tr$*: Takes as input a security parameter, and outputs a classical trapdoor* tr*.*
- $\mathsf{GenEV}(tr) \to |eval\rangle$*: Takes as input a trapdoor* tr*, and outputs a state* $|eval\rangle$*. We require that there is a unique* $|eval\rangle$ *for each* tr*.*
- $\mathsf{Eval}(|eval\rangle, x) \to |\phi\rangle$*: Takes as input an evaluation key* $|eval\rangle$ *and a classical string* x*, and outputs a quantum state* $|\phi\rangle$*.*
- $\mathsf{Invert}(tr, |\phi\rangle) \to x$*: Takes as input a trapdoor* tr *and a quantum state* $|\phi\rangle$ *and outputs a classical string* x*.*

These algorithms should satisfy the following:

(a) (Hard to invert) For any QPT algorithm A*, for any* $m = poly$*, there exists a negligible function* negl *such that, for all* $n \in \mathbb{N}$*,*

$$\Pr\left[A\left(\mathsf{Eval}(|eval\rangle, x), |eval\rangle^{\otimes m(n)}\right) = x \;:\; tr \leftarrow \mathsf{GenTR}(1^n), |eval\rangle \leftarrow \mathsf{GenEV}(tr), x \leftarrow \{0,1\}^n\right] \leq \mathsf{negl}(n)\,.$$

(b) (Trapdoor) For all $n \in \mathbb{N}$*,*

$$\Pr\left[\mathsf{Invert}\big(tr, \mathsf{Eval}(|eval\rangle, x)\big) = x : tr \leftarrow \mathsf{GenTR}(1^n), |eval\rangle \leftarrow \mathsf{GenEV}(tr), x \leftarrow \{0,1\}^n\right] = 1\,.$$

Note that requirement (b) is implicitly imposing that, for any fixed evaluation key, the induced map $x \to |\psi_x\rangle$ is "*injective*", in the sense that for any honestly generated $|\psi_x\rangle$, there is a *unique* "inverse" x.

4.2 Construction

Theorem 3. *A quantum trapdoor function exists, assuming the existence of any quantum-secure one-way function.*

We describe a construction of a quantum trapdoor function from a quantum-secure PRF. Let $\mathsf{PRF} = \{\mathsf{PRF}_n\}_{n\in\mathbb{N}}$ be a quantum-secure PRF, where $\mathsf{PRF}_n : \mathcal{K}_n \times \{0,1\}^n \to \{0,1\}$. Let $(\mathsf{PRS.GenKey}, \mathsf{PRS.GenState})$ be the PRS from construction 1, based on PRF.

For $k \in \mathcal{K}_n$, let $G_{\mathsf{PRF}}(k)$ be the unitary that, for $y \in \{0,1\}^n$ acts as $|y\rangle \mapsto (-1)^{\mathsf{PRF}_n(k,y)} |y\rangle$. From now on, we will drop the subscript n in $\mathsf{PRF}_n(k,y)$ for convenience.

Note that $G_{\mathsf{PRF}}(k)$ can be implemented efficiently by initializing an ancilla qubit in the state $|-\rangle$ and applying the unitary that computes $\mathsf{PRF}(k,\cdot)$ into that qubit.

Construction 2. *Define* $(\mathsf{GenTR}, \mathsf{GenEV}, \mathsf{Eval}, \mathsf{Invert})$ *as follows:*

- $\mathsf{GenTR}(1^n) \to tr$: *Sample a key* $k \leftarrow \mathsf{PRS.GenKey}(1^n)$. *Set* $tr = k$.
- $\mathsf{GenEV}(tr) \to |eval\rangle$: *Set*
$$|eval\rangle = \mathsf{PRS.GenState}(k) = |PRS(k)\rangle \ .$$
- $\mathsf{Eval}(|eval\rangle, x) \to |\phi\rangle$: *Output* $|\phi\rangle = Z^x |eval\rangle$.
- $\mathsf{Invert}(tr, |\phi\rangle) \to x$: *Compute* $H^{\otimes n} G_{\mathsf{PRF}}(tr) |\phi\rangle$, *and measure in the standard basis. Output the outcome* x.

We show the following.

Theorem 4. *Assuming* PRF *is a quantum-secure PRF, Construction 2 is a quantum trapdoor function.*

Since a quantum-secure PRF can be built from any quantum-secure one-way function [Zha12], Theorem 4 implies Theorem 3. The rest of Section 4 is dedicated to proving Theorem 4.

The trapdoor property is straightforward to verify. Let tr be in the support of $\mathsf{GenTR}(1^n)$, and let $|eval\rangle = \mathsf{GenEV}(tr)$. Then, $tr = k$ and $|eval\rangle = |PRS(k)\rangle$, for some k in the support of $\mathsf{PRS.GenKey}(1^n)$. Then, for any x, we have

$$\mathsf{Invert}(tr, \mathsf{Eval}(|eval\rangle, x)) = H^{\otimes n} G_{\mathsf{PRF}}(k) Z^x |PRS(k)\rangle \ .$$

Notice that, by construction 1, $|PRS(k)\rangle = G_{\mathsf{PRF}}(k) H^{\otimes n} |0\rangle^{\otimes n}$. Then,

$$\mathsf{Invert}(tr, \mathsf{Eval}(|eval\rangle, x)) = H^{\otimes n} G_{\mathsf{PRF}}(k) Z^x G_{\mathsf{PRF}}(k) H^{\otimes n} |0\rangle^{\otimes n} \ .$$

Crucially, notice that Z^x commutes with $G_{\mathsf{PRF}}(k)$, since they are both diagonal in the standard basis, and moreover notice that $G_{\mathsf{PRF}}(k)$ is self-inverse. Thus, we have

$$\mathsf{Invert}(tr, \mathsf{Eval}(|eval\rangle, x)) = H^{\otimes n} Z^x H^{\otimes n} |0\rangle^{\otimes n} = |x\rangle \ .$$

The crucial part of this calculation is that Z^x commutes with $G_{\mathsf{PRF}}(k)$, and thus that the PRF phase can be "undone" even *after* the Z^x phase is applied.

4.3 Security

In this subsection, we show that Construction 2 also satisfies property (a) from Definition 3, i.e. it is hard to invert without knowing the trapdoor. This will conclude the proof of Theorem 4, and thus of Theorem 3.

Suppose for a contradiction that there exists a QPT algorithm A, a function $m = poly$, and a non-negligible function $\mathsf{non\text{-}negl}$ such that, for all $n \in \mathbb{N}$,

$$\Pr\left[A\left(\mathsf{Eval}(|eval\rangle, x), |eval\rangle^{\otimes m(n)}\right) = x \ : \ tr \leftarrow \mathsf{GenTR}(1^n), |eval\rangle \leftarrow \mathsf{GenEV}(tr), x \leftarrow \{0,1\}^n\right] \geq \mathsf{non\text{-}negl}(n) \ . \tag{5}$$

Using A, we will construct a distinguisher D that breaks the security of the underlying PRS. Let m be as in Equation (5). D is defined as follows, where we omit the security parameter for ease of notation:

- On input $|\psi\rangle^{\otimes m+1}$ (where $|\psi\rangle$ is either sampled according to the PRS or the Haar random distribution), sample $x \leftarrow \{0,1\}^n$.
- Give $(Z^x \otimes I^{\otimes m}) |\psi\rangle^{\otimes m+1}$ as input to A.
- Let x' be A's output. If $x' = x$, guess that the input came from the PRS distribution. Otherwise, guess that it came from the Haar distribution.

Denote by $\Pr[x' = x | \, |\psi\rangle \leftarrow \text{PRS}]$ the probability that A's guess x' is equal to x, when $|\psi\rangle$ is sampled from the PRS distribution, and by $\Pr[x' = x | \, |\psi\rangle \leftarrow \text{Haar}]$ the analogous probability when $|\psi\rangle$ is sampled from

the Haar distribution. Notice that in the case that $|\psi\rangle$ is sampled from the PRS distribution, the input that D provides to A is distributed exactly as in Equation (5). Thus, the probability that D guesses correctly is

$$\Pr[x' = x \,|\, |\psi\rangle \leftarrow \mathrm{PRS}] \cdot \frac{1}{2} + \Pr[x' \neq x \,|\, |\psi\rangle \leftarrow \mathrm{PRS}] \cdot \frac{1}{2} = \mathsf{non\text{-}negl}(n) \cdot \frac{1}{2} + \Pr[x' \neq x \,|\, |\psi\rangle \leftarrow \mathrm{Haar}] \cdot \frac{1}{2}\,. \quad (6)$$

In particular, notice that D's distinguishing advantage is non-negligible if $\Pr[x' = x \,|\, |\psi\rangle \leftarrow \mathrm{Haar}]$ is negligible. We will show that the latter is the case, which thus implies that the distinguisher D breaks the security of the PRS.

The problem of guessing x, in the case where $|\psi\rangle \leftarrow$ Haar, can be viewed as a "state discrimination" problem. Then, the fact that $\Pr[x' = x \,|\, |\psi\rangle \leftarrow \mathrm{Haar}]$ is negligible is implied by the following more general lemma, which says that the (information-theoretically) optimal probability of guessing x is exponentially small (when $m = poly(n)$).

Lemma 5. *Let $n, m \in \mathbb{N}$ be such that $2^n > 2(m+1)$. Consider the ensemble of states:*

$$\{\rho_x\}_{x\in\{0,1\}^n} = \left\{\mathbb{E}_{|\psi\rangle\leftarrow\mathrm{Haar}(2^n)}[(Z^x \otimes I^{\otimes m})(|\psi\rangle\langle\psi|)^{\otimes m+1}(Z^x \otimes I^{\otimes m})]\right\}_{x\in\{0,1\}^n}$$

Then, there is a constant $C > 0$, such that, for any POVM $\{M_x\}_{x\in\{0,1\}^n}$,

$$\mathbb{E}_{x\leftarrow\{0,1\}^n}\mathrm{Tr}[M_x\rho_x] < C \cdot \left(\frac{m}{2^n} + \frac{m^7}{2^{3n}}\right)^{\frac{1}{2}}\,.$$

Since in our case $m = poly(n)$, the bound in Lemma 5 is exponentially small in n, and hence $\Pr[x' = x \,|\, |\psi\rangle \leftarrow \mathrm{Haar}]$ is exponentially small in n. This implies that the distinguisher D described above breaks the security of the PRS, giving us a contradiction.

Thus, to conclude our proof of security, i.e. that Construction 2 satisfies property (a) from Definition 3, we are left with proving Lemma 5.

Proof of Lemma 5. We consider the "Pretty Good Measurement" (PGM) for this discrimination task. We show that the PGM achieves a guessing probability that is $C' \cdot \left(\frac{m}{2^n} + \frac{m^6}{2^{2n}}\right)$ for some constant $C' > 0$. By Lemma 2, this implies the desired bound of Lemma 5.

Let $\sigma = \sum_{x\in\{0,1\}^n}\rho_x$, and let σ^{-1} be its pseudoinverse. The PGM for this discrimination task is $\{M_x\}_{x\in\{0,1\}^n} \cup \{M_\perp\}$ where $M_x = \sigma^{-\frac{1}{2}}\rho_x\sigma^{-\frac{1}{2}}$ and $M_\perp = \mathbb{1}_{\mathrm{Ker}(\sigma)}$ is the projection onto the kernel of σ. For ease of notation, let $d = 2^n$. For $N \in \mathbb{N}$, denote by $\Pi^{d,N}_{\mathrm{sym}}$ the projector onto the symmetric subspace of $(\mathbb{C}^d)^{\otimes N}$.

Now, notice that

$$\sigma = \sum_x (Z^x \otimes I)\mathbb{E}_{|\psi\rangle\leftarrow\mathrm{Haar}(d)}[|\psi\rangle\langle\psi|^{\otimes m+1}](Z^x \otimes I) \quad (7)$$

$$= \binom{d+m}{m+1}^{-1} \cdot \sum_{x\in\{0,1\}^n} (Z^x \otimes I)\Pi^{d,m+1}_{\mathrm{sym}}(Z^x \otimes I) \quad (8)$$

$$= \binom{d+m}{m+1}^{-1} \cdot d \sum_{j\in[d]} (|j\rangle\langle j| \otimes I)\Pi^{d,m+1}_{\mathrm{sym}}(|j\rangle\langle j| \otimes I)\,, \quad (9)$$

where the second equality is by Lemma 3, and the third equality is by Lemma 1.

Now, define $\tilde{\sigma} = \sum_j (|j\rangle\langle j| \otimes I)\Pi^{d,m+1}_{\mathrm{sym}}(|j\rangle\langle j| \otimes I)$, and let $\tilde{\sigma}^{-1}$ be its pseudoinverse. Then, we have

$$\sigma^{-1} = \binom{d+m}{m+1} \cdot \frac{1}{d} \cdot \tilde{\sigma}^{-1}\,.$$

In order to compute $\tilde{\sigma}^{-1}$, we take a closer look at $\tilde{\sigma}$ and write it in terms of an eigenbasis. To do so, we first consider the convenient orthonormal basis for the symmetric subspace described in Subsection 3.3.1,

which we recall here. For $N \in \mathbb{N}$, define $\mathcal{I}_{d,N} = \{(t_1, .., t_d) : t_1, \cdots, t_d \in \mathbb{N}, t_1 + \cdots + t_d = N\}$. For a vector $\vec{j} = (j_1, \ldots, j_N) \in [d]^N$, denote by $T(\vec{j})$ its *type*, i.e. $T(\vec{j})$ is defined to be the vector in $\mathcal{I}_{d,N}$ whose i-th entry is the number of times i appears in the string $(j_1, \ldots, j_N)$. For $\vec{t} \in \mathcal{I}_{d,N}$, define

$$s(\vec{t}) := \binom{N}{\vec{t}}^{-\frac{1}{2}} \sum_{\vec{j}:T(\vec{j})=\vec{t}} |j_1, \ldots, j_N\rangle \ ,$$

where $\binom{N}{\vec{t}} = \frac{N!}{t_1!\ldots t_d!}$. The content of Lemma 4 is that $\{|s(\vec{t})\rangle : \vec{t} \in \mathcal{I}_{d,N}\}$ is an orthonormal basis for the symmetric subspace of $(\mathbb{C}^d)^{\otimes N}$. This implies that $\Pi_{\mathrm{sym}}^{d,N} = \sum_{\vec{t}\in\mathcal{I}_{d,N}} |s(\vec{t})\rangle \langle s(\vec{t})|$.

Now, for $j \in [d]$, $r \in \{0, \ldots, m\}$, let $T_{j,r}^m = \{\vec{t} \in \mathcal{I}_{d,m} : t_j = r\}$. Moreover, for $\vec{t} = (t_1, \ldots, t_d) \in \mathcal{I}_{d,m+1}$ with $t_j \geq 1$, define $\vec{t}_{-j} \in \mathcal{I}_{d,m}$ to be such that its i-th entry is

$$t_i' := \begin{cases} t_i & \text{if } i \neq j \\ t_i - 1 & \text{if } i = j \end{cases}$$

In other words, $\vec{t}_{-j}$ is identical to $\vec{t}$ except that the j-th entry is reduced by 1 (and hence $\vec{t}_{-j} \in \mathcal{I}_{d,m}$). Then, notice that, for any $\vec{t} \in \mathcal{I}_{d,m+1}$,

$$\begin{aligned} |s(\vec{t})\rangle &= \binom{m+1}{\vec{t}}^{-\frac{1}{2}} \sum_{k\in[d]:t_k\geq 1} |k\rangle \otimes \sum_{\vec{j}\in[d]^m:T(\vec{j})=\vec{t}_{-k}} |j_1, \ldots, j_m\rangle \\ &= \binom{m+1}{\vec{t}}^{-\frac{1}{2}} \sum_{k:t_k\geq 1} |k\rangle \otimes \binom{m}{\vec{t}_{-k}}^{\frac{1}{2}} |s(\vec{t}_{-k})\rangle \\ &= \sum_{k:t_k\geq 1} \sqrt{\frac{t_k}{m+1}} |k\rangle \otimes |s(\vec{t}_{-k})\rangle \ . \end{aligned} \tag{10}$$

Then, we have

$$\begin{aligned} \tilde{\sigma} &= \sum_{j\in[d]} (|j\rangle\langle j| \otimes I)\Pi_{\mathrm{sym}}^{d,m+1}(|j\rangle\langle j| \otimes I) \\ &= \sum_{j\in[d]} (|j\rangle\langle j| \otimes I)\left(\sum_{\vec{t}\in\mathcal{I}_{d,m+1}} |s(\vec{t})\rangle\langle s(\vec{t})|\right)(|j\rangle\langle j| \otimes I) \\ &= \sum_{j\in[d]} (|j\rangle\langle j| \otimes I)\left(\sum_{\vec{t}\in\mathcal{I}_{d,m+1}} \sum_{k:t_k\geq 1} \sum_{k':t_{k'}\geq 1} \sqrt{\frac{t_k}{m+1}} \cdot \sqrt{\frac{t_{k'}}{m+1}} |k\rangle\langle k'| \otimes |s(\vec{t}_{-k})\rangle\langle s(\vec{t}_{-k'})|\right)(|j\rangle\langle j| \otimes I) \\ &= \sum_{\vec{t}\in\mathcal{I}_{d,m+1}} \sum_{j:t_j\geq 1} \frac{t_j}{m+1} |j\rangle\langle j| \otimes |s(\vec{t}_{-j})\rangle\langle s(\vec{t}_{-j})| \\ &= \sum_{j\in[d]} |j\rangle\langle j| \otimes \sum_{\vec{t}\in\mathcal{I}_{d,m+1}:t_j\geq 1} \frac{t_j}{m+1} |s(\vec{t}_{-j})\rangle\langle s(\vec{t}_{-j})| \\ &= \sum_{j\in[d]} |j\rangle\langle j| \otimes \sum_{r=0}^{m} \frac{r+1}{m+1} \sum_{\vec{t}\in T_{j,r}^m} |s(\vec{t})\rangle\langle s(\vec{t})| \\ &= \frac{1}{m+1} \sum_{j\in[d]} |j\rangle\langle j| \otimes \sum_{\vec{t}\in T_{j,0}^m} |s(\vec{t})\rangle\langle s(\vec{t})| + \frac{1}{m+1} \sum_{j\in[d]} |j\rangle\langle j| \otimes \sum_{r=1}^{m} (r+1) \cdot \sum_{\vec{t}\in T_{j,r}^m} |s(\vec{t})\rangle\langle s(\vec{t})| \ , \end{aligned} \tag{11}$$

where the third equality uses Equation (10).

Equation (11) implies that $\{|j\rangle \otimes |s(\vec{t})\rangle : j \in [d], \vec{t} \in \mathcal{I}_{d,m}\}$ is exactly the set of eigenvectors of $\tilde{\sigma}$ with non-zero eigenvalue. Hence, the pseudoinverse $\tilde{\sigma}$ is obtained by taking the inverse of the (non-zero) elements

on the diagonal. Thus, we have

$$\tilde{\sigma}^{-1} = (m+1)\cdot \sum_{j\in[d]} |j\rangle\langle j| \otimes \sum_{\vec{t}\in T^m_{j,0}} |s(\vec{t})\rangle\langle s(\vec{t})| + \frac{m+1}{r+1}\sum_{j\in[d]} |j\rangle\langle j| \otimes \sum_{r=1}^{m}\cdot \sum_{\vec{t}\in T^m_{j,r}} |s(\vec{t})\rangle\langle s(\vec{t})| \ .$$

Then,

$$\tilde{\sigma}^{-\frac{1}{2}} = \sqrt{m+1}\cdot \sum_{j\in[d]} |j\rangle\langle j| \otimes \sum_{\vec{t}\in T^m_{j,0}} |s(\vec{t})\rangle\langle s(\vec{t})| + \sqrt{\frac{m+1}{r+1}}\sum_{j\in[d]} |j\rangle\langle j| \otimes \sum_{r=1}^{m}\cdot \sum_{\vec{t}\in T^m_{j,r}} |s(\vec{t})\rangle\langle s(\vec{t})| \ .$$

Notice that, for any $j\in[d]$, we can write $\Pi^{d,m}_{\mathrm{sym}} = \sum_{\vec{t}\in\mathcal{I}_{d,m}} |s(\vec{t})\rangle\langle s(\vec{t})| = \sum_{r=0}^{m}\sum_{\vec{t}\in T^m_{j,r}} |s(\vec{t})\rangle\langle s(\vec{t})|$. Then, we have

$$\tilde{\sigma}^{-\frac{1}{2}} = \sqrt{m+1}\cdot \mathbb{1}\otimes\Pi^{d,m}_{\mathrm{sym}} - \sqrt{m+1}\cdot\sum_{r=1}^{m}\left(1-\frac{1}{\sqrt{r+1}}\right)\cdot\sum_{j\in[d]} |j\rangle\langle j| \otimes \sum_{\vec{t}\in T^m_{j,r}} |s(\vec{t})\rangle\langle s(\vec{t})| \ . \tag{12}$$

For convenience, for $r\in\{0,\dots,m\}$, define $Q_r = \sum_{j\in[d]} |j\rangle\langle j| \otimes \sum_{\vec{t}\in T^m_{j,r}} |s(\vec{t})\rangle\langle s(\vec{t})|$. The probability of guessing x when using the PGM is

$$\begin{aligned}
&\mathbb{E}_{x\leftarrow\{0,1\}^n}\mathrm{Tr}\left[\rho_x\sigma^{-\frac{1}{2}}\rho_x\sigma^{-\frac{1}{2}}\right]\\
&= \binom{d+m}{m+1}\cdot\frac{1}{d}\cdot\mathbb{E}_{x\leftarrow\{0,1\}^n}\mathrm{Tr}\left[\rho_x\tilde{\sigma}^{-\frac{1}{2}}\rho_x\tilde{\sigma}^{-\frac{1}{2}}\right]\\
&= \binom{d+m}{m+1}\cdot\frac{m+1}{d}\cdot\mathbb{E}_{x\leftarrow\{0,1\}^n}\mathrm{Tr}\left[\rho_x\left(\mathbb{1}\otimes\Pi^{d,m}_{\mathrm{sym}}\right)\rho_x\left(\mathbb{1}\otimes\Pi^{d,m}_{\mathrm{sym}}\right)\right]\\
&+ \binom{d+m}{m+1}\cdot\frac{m+1}{d}\cdot\sum_{r,r'=1}^{m}\left(1-\frac{1}{\sqrt{r+1}}\right)\left(1-\frac{1}{\sqrt{r'+1}}\right)\mathbb{E}_{x\leftarrow\{0,1\}^n}\mathrm{Tr}\left[\rho_x Q_r\rho_x Q_{r'}\right]\\
&- 2\binom{d+m}{m+1}\cdot\frac{m+1}{d}\cdot\sum_{r=1}^{m}\left(1-\frac{1}{\sqrt{r+1}}\right)\mathbb{E}_{x}\mathrm{Tr}\left[\rho_x\left(\mathbb{1}\otimes\Pi^{d,m}_{\mathrm{sym}}\right)\rho_x Q_r\right].
\end{aligned}\tag{13}$$

where the last equality follows by using Equation (12) to replace the two appearances of $\tilde{\sigma}^{-\frac{1}{2}}$. Now, note that, by Lemma 3, $\rho_x = \binom{d+m}{m+1}^{-1}(Z^x\otimes\mathbb{1})\Pi^{d,m+1}_{\mathrm{sym}}(Z^x\otimes\mathbb{1})$. Further, note that $Z^x\otimes\mathbb{1}$ commutes with both $\mathbb{1}\otimes\Pi^{d,m}_{\mathrm{sym}}$ and Q_r. Substituting the last expression for ρ_x into Equation (13), and noticing that the Z^x's cancel each other out thanks to the commutation, we obtain:

$$\begin{aligned}
&\mathbb{E}_{x\leftarrow\{0,1\}^n}\mathrm{Tr}\left[\rho_x\sigma^{-\frac{1}{2}}\rho_x\sigma^{-\frac{1}{2}}\right]\\
&= \binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\mathbb{E}_{x\leftarrow\{0,1\}^n}\mathrm{Tr}\left[\Pi^{d,m+1}_{\mathrm{sym}}\left(\mathbb{1}\otimes\Pi^{d,m}_{\mathrm{sym}}\right)\Pi^{d,m+1}_{\mathrm{sym}}\left(\mathbb{1}\otimes\Pi^{d,m}_{\mathrm{sym}}\right)\right]\\
&+ \binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\sum_{r,r'=1}^{m}\left(1-\frac{1}{\sqrt{r+1}}\right)\left(1-\frac{1}{\sqrt{r'+1}}\right)\mathbb{E}_{x\leftarrow\{0,1\}^n}\mathrm{Tr}\left[\Pi^{d,m+1}_{\mathrm{sym}}Q_r\Pi^{d,m+1}_{\mathrm{sym}}Q_{r'}\right]\\
&- 2\binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\sum_{r=1}^{m}\left(1-\frac{1}{\sqrt{r+1}}\right)\mathbb{E}_{x}\mathrm{Tr}\left[\Pi^{d,m+1}_{\mathrm{sym}}\left(\mathbb{1}\otimes\Pi^{d,m}_{\mathrm{sym}}\right)\Pi^{d,m+1}_{\mathrm{sym}}Q_r\right].
\end{aligned}$$

Clearly both $\Pi^{d,m+1}_{\mathrm{sym}}\left(\mathbb{1}\otimes\Pi^{d,m}_{\mathrm{sym}}\right)\Pi^{d,m+1}_{\mathrm{sym}}$ and Q_r are positive semidefinite. Using the fact that $\mathrm{Tr}[AB]\geq 0$ if

A and B are positive semidefinite, we have that $\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}\left(\mathbb{1}\otimes\Pi_{\mathrm{sym}}^{d,m}\right)\Pi_{\mathrm{sym}}^{d,m+1}Q_r\right]\geq 0$. Thus, we have

$$
\begin{aligned}
&\mathbb{E}_{x\leftarrow\{0,1\}^n}\mathrm{Tr}\left[\rho_x\sigma^{-\frac{1}{2}}\rho_x\sigma^{-\frac{1}{2}}\right]\\
&\leq\binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}\left(\mathbb{1}\otimes\Pi_{\mathrm{sym}}^{d,m}\right)\Pi_{\mathrm{sym}}^{d,m+1}\left(\mathbb{1}\otimes\Pi_{\mathrm{sym}}^{d,m}\right)\right]\\
&+\binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\sum_{r,r'=1}^{m}\left(1-\frac{1}{\sqrt{r+1}}\right)\left(1-\frac{1}{\sqrt{r'+1}}\right)\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}Q_r\Pi_{\mathrm{sym}}^{d,m+1}Q_{r'}\right]\\
&\leq\binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}\left(\mathbb{1}\otimes\Pi_{\mathrm{sym}}^{d,m}\right)\Pi_{\mathrm{sym}}^{d,m+1}\left(\mathbb{1}\otimes\Pi_{\mathrm{sym}}^{d,m}\right)\right] \qquad (14)\\
&+\binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\sum_{r,r'=1}^{m}\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}Q_r\Pi_{\mathrm{sym}}^{d,m+1}Q_{r'}\right], \qquad (15)
\end{aligned}
$$

where the last line follows from the fact that, for any r,r', $\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}Q_r\Pi_{\mathrm{sym}}^{d,m+1}Q_{r'}\right]\geq 0$ since both $\Pi_{\mathrm{sym}}^{d,m+1}Q_r\Pi_{\mathrm{sym}}^{d,m+1}$ and $Q_{r'}$ are positive semidefinite. Next, we bound each of the terms (14) and (15) separately. First, notice that

$$
\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}\left(\mathbb{1}\otimes\Pi_{\mathrm{sym}}^{d,m}\right)\Pi_{\mathrm{sym}}^{d,m+1}\left(\mathbb{1}\otimes\Pi_{\mathrm{sym}}^{d,m}\right)\right]=\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}\right].
$$

Thus,

$$
\begin{aligned}
(14)&=\binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}\right]\\
&=\binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\binom{d+m}{m+1}\\
&=\frac{m+1}{d}, \qquad (16)
\end{aligned}
$$

where the second equality is again due to Lemma 3.

Define, for any $j\in[d]$ and $r\in[m]$, $Q_{j,r}:=\sum_{\vec{t}\in T_{j,r}^m}|s(\vec{t})\rangle\langle s(\vec{t})|$. Then, $Q_r=\sum_{j\in[d]}|j\rangle\langle j|\otimes Q_{j,r}$. We have,

$$
\begin{aligned}
(15)&\leq\binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\sum_{r,r'=1}^{m}\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}Q_r\Pi_{\mathrm{sym}}^{d,m+1}Q_{r'}\right]\\
&=\binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\sum_{r,r'=1}^{m}\sum_{j,j'\in[d]}\mathrm{Tr}\left[\Pi_{\mathrm{sym}}^{d,m+1}\left(|j\rangle\langle j|\otimes Q_{j,r}\right)\Pi_{\mathrm{sym}}^{d,m+1}\left(|j'\rangle\langle j'|\otimes Q_{j',r'}\right)\right]\\
&=\binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\sum_{r,r'=1}^{m}\sum_{j,j'\in[d]}\mathrm{Tr}\left[|j'\rangle\langle j'|\,\Pi_{\mathrm{sym}}^{d,m+1}\,|j\rangle\langle j|\left(\mathbb{1}\otimes Q_{j,r}\right)|j\rangle\langle j|\,\Pi_{\mathrm{sym}}^{d,m+1}\,|j'\rangle\langle j'|\left(\mathbb{1}\otimes Q_{j',r'}\right)\right], \qquad (17)
\end{aligned}
$$

where in the last line we are writing $|j\rangle\langle j|$ and $|j'\rangle\langle j'|$ as short for $|j\rangle\langle j|\otimes\mathbb{1}$ and $|j'\rangle\langle j'|\otimes\mathbb{1}$ respectively.

For $n\in\mathbb{N}$, $j,j'\in[d]$ and $l,l'\in\{0,\ldots,n\}$, define $T_{(j,l),(j',l')}^n:=\{\vec{t}\in\mathcal{I}_{d,n}:t_j=l\text{ and }t_{j'}=l'\}$. Then, for any $j,j'\in[d]$, we can write

$$
\Pi_{\mathrm{sym}}^{d,m+1}=\sum_{l,l'=0}^{m+1}\sum_{\vec{t}\in T_{(j,l),(j',l')}^{m+1}}|s(\vec{t})\rangle\langle s(\vec{t})|\,. \qquad (18)
$$

Recall that, for $j\in[d]$ and $\vec{t}=(t_1,\ldots,t_d)\in\mathcal{I}_{d,m+1}$ such that $t_j\geq 1$, we defined $\vec{t}_{-j}\in\mathcal{I}_{d,m}$ to be identical

to $\vec{t}$ except that the j-th entry is reduced by 1. Then, combining Equations (18) and (10) implies

$$|j'\rangle\langle j'|\,\Pi_{\mathrm{sym}}^{d,m+1}\,|j\rangle\langle j| = |j'\rangle\langle j| \otimes \sum_{l,l'\geq 1}^{m+1} \sqrt{\frac{l}{m+1}}\cdot\sqrt{\frac{l'}{m+1}} \sum_{\vec{t}\in T^{m+1}_{(j',l'),(j,l)}} |s(\vec{t}_{-j'})\rangle\langle s(\vec{t}_{-j})| \tag{19}$$

For ease of notation, for $j,j'\in[d]$ and $l,l'\in\{1,\dots,m+1\}$, let $P_{(j',l'),(j,l)} := \sum_{\vec{t}\in T^{m+1}_{(j',l'),(j,l)}} |s(\vec{t}_{-j'})\rangle\langle s(\vec{t}_{-j})|$. Then, plugging (19) into (17) (twice) and simplifying, we obtain

$$\begin{aligned}(15) &\leq \binom{d+m}{m+1}^{-1}\cdot\frac{1}{d(m+1)}\cdot\sum_{r,r'=1}^{m}\sum_{j,j'\in[d]}\sum_{\substack{l,l'\geq 1\\ l'',l'''\geq 1}}^{m+1}\sqrt{l\cdot l'\cdot l''\cdot l'''}\mathrm{Tr}\Big[\,|j'\rangle\langle j'|\otimes\big(P_{(j',l'),(j,l)}Q_{j,r}P_{(j,l''),(j',l''')}Q_{j',r'}\big)\,\Big]\\ &= \binom{d+m}{m+1}^{-1}\cdot\frac{1}{d(m+1)}\cdot\sum_{r,r'=1}^{m}\sum_{j,j'\in[d]}\sum_{\substack{l,l'\geq 1\\ l'',l'''\geq 1}}^{m+1}\sqrt{l\cdot l'\cdot l''\cdot l'''}\mathrm{Tr}\Big[P_{(j',l'),(j,l)}Q_{j,r}P_{(j,l''),(j',l''')}Q_{j',r'}\Big] \end{aligned}\tag{20}$$

We can further simplify the expression using $l,l',l'',l'''\leq m+1$ to obtain

$$(15) \leq \binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\sum_{r,r'=1}^{m}\sum_{j,j'\in[d]}\sum_{\substack{l,l'\geq 1\\ l'',l'''\geq 1}}^{m+1}\Big|\mathrm{Tr}\Big[P_{(j',l'),(j,l)}Q_{j,r}P_{(j,l''),(j',l''')}Q_{j',r'}\Big]\Big| \tag{21}$$

Observe that

$$Q_{j,r}P_{(j,l''),(j',l''')}Q_{j',r'} = \delta_{r=l''-1}\cdot\delta_{r'=l'''-1}\cdot\sum_{\vec{t}\in T^{m+1}_{(j,l''),(j',l''')}} |s(\vec{t}_{-j})\rangle\langle s(\vec{t}_{-j'})| \tag{22}$$

Then, with a similar observation, and additionally using the ciclicity of trace, we have

$$\begin{aligned}\mathrm{Tr}\Big[P_{(j',l'),(j,l)}Q_{j,r}P_{(j,l''),(j',l''')}Q_{j',r'}\Big] &= \delta_{r=l-1=l''-1}\cdot\delta_{r'=l'''-1=l'-1}\cdot\mathrm{Tr}\Big[\,\textstyle\sum_{\vec{t}\in T^{m+1}_{(j,l''),(j',l''')}}|s(\vec{t}_{-j'})\rangle\langle s(\vec{t}_{-j'})|\,\Big]\\ &= \delta_{r=l-1=l''-1}\cdot\delta_{r'=l'''-1=l'-1}\cdot\mathrm{Tr}\Big[\,\textstyle\sum_{\vec{t}\in T^{m}_{(j,l''),(j',l'''-1)}}|s(\vec{t})\rangle\langle s(\vec{t})|\,\Big]\\ &= \delta_{r=l-1=l''-1}\cdot\delta_{r'=l'''-1=l'-1}\cdot\big|T^{m}_{(j,l''),(j',l'''-1)}\big|\,,\end{aligned}\tag{23}$$

where $|T^{m}_{(j,l''),(j',l'''-1)}|$ is the cardinality of the set $T^{m}_{(j,l''),(j',l'''-1)}$.

Plugging (23) into (21), and simplifying, gives

$$\begin{aligned}(15) &\leq \binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\sum_{r,r'=1}^{m}\sum_{j,j'\in[d]}|T^{m}_{(j,r+1),(j',r')}|\\ &= \binom{d+m}{m+1}^{-1}\cdot\frac{m+1}{d}\cdot\sum_{r,r'=1}^{m}\left(\sum_{j\in[d]}|T^{m}_{(j,r+1),(j,r')}| + \sum_{j\neq j'\in[d]}|T^{m}_{(j,r+1),(j',r')}|\right).\end{aligned}\tag{24}$$

Now, let's consider the first summand in the last expression of (24). Notice that $T^{m}_{(j,r+1),(j,r')} = \emptyset$ whenever $r+1\neq r'$. When $r+1=r'$, we have $T^{m}_{(j,r+1),(j,r')} = T^{m}_{j,r'}$. Notice that the size of the latter is just equal to the dimension of the symmetric subspace of $(\mathbb{C}^{d-1})^{\otimes m-r'}$ (since j must appear exactly r' times). Thus,

$$|T^{m}_{(j,r+1),(j,r')}| = \delta_{r+1=r'}\cdot|T^{m}_{j,r'}| = \delta_{r+1=r'}\cdot\binom{d+m-r'-2}{m-r'}.$$

Hence, we have

$$
\begin{aligned}
&\binom{d+m}{m+1}^{-1} \cdot \frac{m+1}{d} \cdot \sum_{r,r'=1}^{m} \sum_{j\in[d]} |T^m_{(j,r+1),(j,r')}| \\
&= \binom{d+m}{m+1}^{-1} \cdot \frac{m+1}{d} \cdot \sum_{r'=2}^{m} \sum_{j\in[d]} \binom{d+m-r'-2}{m-r'} \\
&= \sum_{r'=2}^{m} \binom{d+m}{m+1}^{-1} \cdot (m+1) \binom{d+m-r'-2}{m-r'} \\
&= \sum_{r'=2}^{m} \frac{(m+1)!(d-1)!}{(d+m)!} \cdot (m+1) \cdot \frac{(d+m-r'-2)!}{(m-r')!(d-2)!} \\
&= \sum_{r'=2}^{m} \frac{(m+1)\cdots(m-r'+1)\cdot(d-1)}{(d+m)\cdots(d+m-r'-1)} \cdot (m+1) \\
&\le \sum_{r'=2}^{m} \frac{d-1}{d+m-r'-1} \cdot (m+1) \cdot \left(\frac{m+1}{d}\right)^{r'+1} \\
&\le (m+1) \cdot \sum_{r'=2}^{m} \left(\frac{m+1}{d}\right)^{r'+1} \\
&= (m+1) \cdot \left(\frac{m+1}{d}\right)^{3} \cdot \sum_{r=0}^{m-2} \left(\frac{m+1}{d}\right)^{r} \\
&= \frac{(m+1)^4}{d^3} \cdot \frac{1-\left(\frac{m+1}{d}\right)^{m-1}}{1-\frac{m+1}{d}} \\
&\le \frac{(m+1)^4}{d^3} \cdot \frac{1}{1-\frac{m+1}{d}} \qquad \text{(as long as } d > m+1\text{)} \\
&= \frac{(m+1)^4}{d^2(d-m-1)} \le 2\frac{(m+1)^4}{d^3} \qquad \text{(as long as } d > 2(m+1)\text{)}\,. \qquad (25)
\end{aligned}
$$

Next, consider the second summand in the last expression of (24) (corresponding to $j \neq j'$). Notice that $T^m_{(j,r+1),(j',r')} = \emptyset$ whenever $r + r' \geq m$. When $r + r' \leq m - 1$, the size of $T^m_{(j,r+1),(j',r')}$ is equal to the dimension of the symmetric subspace of $(\mathbb{C}^{d-2})^{\otimes m-r-r'-1}$ (since j must appear exactly $r+1$ times, and j'

must appear exactly r' times). Thus, we have

$$\begin{aligned}
&\binom{d+m}{m+1}^{-1} \cdot \frac{m+1}{d} \cdot \sum_{r,r'=1}^{m} \sum_{j \neq j' \in [d]} |T^m_{(j,r+1),(j',r')}| \\
&= \binom{d+m}{m+1}^{-1} \cdot \frac{m+1}{d} \cdot \sum_{r,r'=1}^{m} \sum_{j \in [d]} \binom{d+m-r-r'-4}{m-r'-r'-1} \\
&= \sum_{r,r'=1}^{m} \binom{d+m}{m+1}^{-1} \cdot d \cdot (m+1) \cdot \binom{d+m-r-r'-4}{m-r'-r'-1} \\
&= \sum_{r,r'=1}^{m} \frac{(m+1)!(d-1)!}{(d+m)!} \cdot d \cdot (m+1) \cdot \frac{(d+m-r-r'-4)!}{(m-r-r'-1)!(d-3)!} \\
&= \sum_{r,r'=1}^{m} \frac{d(d-1)(d-2) \cdot (m+1)^2 m \cdots (m-r-r')}{(d+m) \cdots (d+m-r-r'-3)} \\
&\leq \frac{d(d-1)(d-2)}{d+m} \cdot \sum_{r,r'=1}^{m} \left(\frac{m+1}{d+m-1} \right)^{r+r'+3} \\
&\leq d^2 \cdot m^2 \cdot \left(\frac{m+1}{d+m-1} \right)^5 \leq C'' \cdot \frac{m^7}{d^3}\,, \qquad (26)
\end{aligned}$$

for some constant $C'' > 0$ independent of m and d. Plugging the bounds (25) and (26) into (24), we obtain, provided $d > 2(m+1)$:

$$(15) \leq 2\frac{(m+1)^4}{d^3} + C'' \cdot \frac{m^7}{d^3} \qquad (27)$$

Finally, using the bounds we obtained for terms (14) and (15), we have, provided $d > 2(m+1)$:

$$\mathbb{E}_{x \leftarrow \{0,1\}^n} \mathrm{Tr}\left[\rho_x \sigma^{-\frac{1}{2}} \rho_x \sigma^{-\frac{1}{2}}\right] \leq \frac{m+1}{d} + 2\frac{(m+1)^4}{d^3} + C'' \cdot \frac{m^7}{d^3} = C' \cdot \left(\frac{m}{d} + \frac{m^7}{d^3} \right)\,, \qquad (28)$$

for some constant $C' > 0$ independent of m and d. Since, by Lemma 2, the PGM achieves a success probability that is at most the square of the optimal, this gives the desired bound of Lemma 5 (with $C = \sqrt{C'}$). □

5 Applications

We describe two applications of quantum trapdoor functions.

5.1 Public-key encryption with quantum public key

A public-key encryption scheme with a *quantum* public key has almost the same syntax as a classical public-key encryption scheme, except that the public key is a quantum state $|pk\rangle$, and we additionally require that $|pk\rangle$ be efficiently generatable given the classical secret key. In the (CPA) security game, the adversary has access to an arbitrary polynomial number of copies of $|pk\rangle$. For completeness, we provide a formal definition.

Definition 4 (Public-key encryption with quantum public key)**.** *A public-key encryption scheme with quantum public key is a tuple of QPT algorithms* $(\mathsf{GenSK}, \mathsf{GenPK}, \mathsf{Enc}, \mathsf{Dec})$ *as follows.*

- $\mathsf{GenSK}(1^n) \to sk$*: Takes as input a security parameter, and outputs a classical secret key* sk*.*
- $\mathsf{GenPK}(sk) \to |pk\rangle$*: Takes as input the secret key* sk*, and outputs the quantum public key* $|pk\rangle$*. We additionally require that* $|pk\rangle$ *be unique given* sk*.*
- $\mathsf{Enc}(|pk\rangle, m) \to |c\rangle$*: Takes as input a copy of the public key* $|pk\rangle$ *and a message* $m \in \{0,1\}^*$*, and outputs a quantum ciphertext* $|c\rangle$*.*

- $\mathsf{Dec}(sk, |c\rangle) \to m$: *Takes as input the secret key sk and a ciphertext $|c\rangle$, and outputs a string m.*

These algorithms should satisfy "correctness", i.e. for all $m \in \{0,1\}^*$, for all n,

$$\Pr[\mathsf{Dec}(sk, |c\rangle) = m : sk \leftarrow \mathsf{Gen}(1^n), |pk\rangle \leftarrow \mathsf{GenPK}(sk), |c\rangle \leftarrow \mathsf{Enc}(|pk\rangle, m)] = 1\,.$$

The definition of CPA security is analogous to the classical one, except that we explicitly give the adversary access to an arbitrary polynomial number of copies of the quantum public key.

Definition 5 (CPA security with quantum public key)**.** *A public-key encryption scheme with quantum public key satisfies CPA security if the following holds. For all QPT algorithms A_0, A_1, for all $t = poly$, there exists a negligible function* negl *such that, for all n,*

$$\Pr[b = b' : sk \leftarrow \mathsf{GenSK}(1^n), |pk\rangle \leftarrow \mathsf{GenPK}(sk), (m_0, m_1, |aux\rangle) \leftarrow A_0(|pk\rangle^{\otimes t(n)}),$$
$$b \leftarrow \{0,1\}, |c\rangle \leftarrow \mathsf{Enc}(|pk\rangle, m_b), b' \leftarrow A_1(|aux\rangle, |c\rangle)] \leq \frac{1}{2} + \mathsf{negl}(n)\,.$$

We show that quantum trapdoor functions imply a public-key encryption scheme with quantum public key. The construction is analogous to the construction of a (classical) public-key encryption scheme from injective trapdoor functions[2]. We start by describing a construction that supports encryptions of single-bit messages.

Let $(\mathsf{QTF.GenTR}, \mathsf{QTF.GenEV}, \mathsf{QTF.Eval}, \mathsf{QTF.Invert})$ be a quantum trapdoor function, as in Definition 3.

Construction 3 (Public-key encryption with quantum public key, supporting single-bit messages)**.** *Define* $(\mathsf{GenSK}, \mathsf{GenPK}, \mathsf{Enc}, \mathsf{Dec})$ *as follows:*

- $\mathsf{GenSK}(1^n) \to sk$: *Sample a trapdoor $tr \leftarrow \mathsf{QTF.GenTR}(1^n)$. Set $sk = tr$.*
- $\mathsf{GenPK}(sk) \to |pk\rangle$: *Let $|eval\rangle = \mathsf{QTF.GenEV}(sk)$. Set $|pk\rangle = |eval\rangle$.*
- $\mathsf{Enc}\big(|pk\rangle, m \in \{0,1\}\big) \to |c\rangle$: *Sample $r, x \leftarrow \{0,1\}^n$. Compute $|\psi_x\rangle \leftarrow \mathsf{QTF.Eval}(|pk\rangle, x)$. Set*
$$|c\rangle = (|\psi_x\rangle,\ r,\ r \cdot x \oplus m)\,.$$
- $\mathsf{Dec}(sk, |c\rangle) \to m'$: *Parse $|c\rangle$ as $|c\rangle = (|\phi\rangle, r, b)$. Compute $x' \leftarrow \mathsf{QTF.Invert}(sk, |\phi\rangle)$. Set $m' = r \cdot x' \oplus b$.*

Correctness of this scheme clearly follows from the trapdoor property of the underlying QTF. We show the following.

Theorem 5. *Construction 3 satisfies CPA security.*

Proof. Suppose for a contradiction that there is a QPT adversary A, a $t = poly$, and a non-negligible function $\mathsf{non\text{-}negl}$ such that, for all n,

$$\Pr[A(|c\rangle \otimes |pk\rangle^{\otimes t}) = m : sk \leftarrow \mathsf{Gen}(1^n), |pk\rangle \leftarrow \mathsf{GenPK}(sk), m \leftarrow \{0,1\},\ |c\rangle \leftarrow \mathsf{Enc}(|pk\rangle, m)]$$
$$\geq \frac{1}{2} + \mathsf{non\text{-}negl}(n)\,.$$

In the case of Construction 3, this implies that

$$\Pr\Big[A(|\psi_x\rangle,\ r,\ r \cdot x \oplus m, |eval\rangle^{\otimes t}) = m : tr \leftarrow \mathsf{QTF.GenTR}(1^n), |eval\rangle \leftarrow \mathsf{QTF.GenEV}(tr), m \leftarrow \{0,1\},$$
$$r, x \leftarrow \{0,1\}^n, |\psi_x\rangle \leftarrow \mathsf{QTF.Eval}(|eval\rangle, x)\Big] \geq \frac{1}{2} + \mathsf{non\text{-}negl}(n)\,. \tag{29}$$

[2]Recall in particular that, for a quantum trapdoor function, the quantum map $x \to |\psi_x\rangle$ induced by a fixed evaluation key is "injective", in the sense that for each honestly generated $|\psi_x\rangle$ there is a unique inverse x.

It is clear that guessing m is equivalent to guessing $r \cdot x$. Thus, the existence of A satisfying (29) implies the existence of an algorithm A' such that

$$\Pr\Big[A'(|\psi_x\rangle, r, |eval\rangle^{\otimes t}) = r \cdot x : tr \leftarrow \mathsf{QTF.GenTR}(1^n), |eval\rangle \leftarrow \mathsf{QTF.GenEV}(tr), \\ r, x \leftarrow \{0,1\}^n, |\psi_x\rangle \leftarrow \mathsf{QTF.Eval}(|eval\rangle, x)\Big] \geq \frac{1}{2} + \mathsf{non\text{-}negl}(n). \quad (30)$$

Invoking the quantum version of Goldreich-Levin [AC02], which crucially works even in the presence of quantum auxiliary information (since the reduction of [AC02] only makes a single call to A), we obtain an adversary A'' that breaks security of the quantum trapdoor function, i.e. given as input $(|\psi_x\rangle, |eval\rangle^{\otimes t})$, A'' outputs x with non-negligible probability. □

The scheme of Construction 3 supports encryptions of single-bit messages. In the classical setting, it is well-known that, for public-key schemes, CPA security for single-messages is equivalent to CPA security for multiple messages. Thus, a scheme that supports encryptions of single-bit messages can be bootstrapped to a scheme that supports encryptions of messages of arbitrary length by simply encrypting each bit of the message under the same public key. In the case of *quantum* public key, we need to be a bit more careful. This trivial bootstrapping does not work because the encryption algorithm crucially only receives as input a *single* copy of $|pk\rangle$ (this is of course not an issue classically, since the public key can be copied).

This issue can be circumvented by a slight modification of the classical bootstrapping technique that is referred to as "hybrid encryption":

(i) We first obtain a scheme that supports encryptions of n-bit messages by having the public key consist of n copies of the public key for a single-bit scheme, i.e. $|pk\rangle^{\otimes n}$. Note that this alone does not resolve the issue because the size of the public-key still grows with the size of the message.

(ii) We modify encryption as follows. To encrypt a message m (of arbitrary length), use $|pk\rangle^{\otimes n}$ to encrypt a freshly sampled secret key $\tilde{sk}$ of a *private-key* encryption scheme corresponding to security parameter n (we are assuming this secret key is n-bits long), which supports encryption of messages of arbitrary length. Use $\tilde{sk}$ to encrypt m (this step is entirely classical). The ciphertext consists of both encryptions.

Theorem 6. *Assuming the existence of quantum-secure one-way functions, there exists a public-key encryption scheme with a quantum public key (as in Definition 4).*

Proof. The proof that CPA security is preserved through steps (i) and (ii) follows essentially unchanged from the respective proofs in the classical setting. The reductions in these proofs only make straightline use of the adversaries. Moreover, these reductions are allowed to make use of an arbitrary polynomial number of copies of the public key, since the adversary in the definition of CPA security (Definition 5) is allowed the same. □

5.2 Two-message key-exchange

In this subsection, we informally discuss the implications of the result from the previous subsection on the possibility of realizing *two-message* key-exchange *from one-way functions*.

Any public-key encryption scheme implies a simple two-message key-exchange protocol: (i) Alice samples sk and pk, and sends pk to Bob; (ii) Bob samples a uniformly random string x and sends back an encryption of x, which Alice is able to decrypt. Alice and Bob set x to be the shared key.

One can construct an analogous two-message key-exchange protocol from a public-key encryption scheme with a *quantum* public key (like the one described in Subsection 5.1). The only difference is that Alice and Bob's messages are now quantum states. Then, given the results from the previous section, does this mean that quantum communication allows for a two-message key-exchange protocol from one-way functions?

The answer is a bit subtle, and depends on how one models the attacker's access to the quantum communication. In the case of the BB84 quantum key-exchange protocol, only the *classical* communication channels (used by Alice and Bob to perform the steps of "information reconciliation" and "privacy amplification") are assumed to be authenticated. The quantum channel is *not* assumed to be authenticated, and the attacker is free to tamper arbitrarily with the qubits that are being exchanged (and the protocol itself takes care of

the fact that tampering can be detected by Alice and Bob by subsequently exchanging classical messages). Note that the BB84 protocol requires strictly more than two messages.

If one insists on considering *two-message* key-exchange protocols, then it is easy to see that some form of authenticated quantum channel is *necessary*. If Alice and Bob's messages are not authenticated at all, then the attacker can simply perform a "man-in-the-middle" attack: it can impersonate Bob when interacting with Alice, and viceversa, resulting in the attacker sharing one key with Alice and another with Bob (and the two of them not detecting this).

Then, the question becomes: what is the right notion of *authenticated quantum channel*? In the classical setting, an authenticated channel has the following properties:

(a) Messages sent through it are guaranteed to not be tampered with, and the origin is trusted.

(b) However, messages sent through the channel are "in the clear", i.e. they can be read by an attacker.

When trying to generalize this definition to the quantum setting, we run into an obstacle: "reading" a quantum message is not something that is well-defined. In particular, the only way that (a) can be satisfied is if the attacker acts as the *identity* on the quantum states that are sent through the channel. Then, trivially the attacker does not gain any information about these quantum states.

One non-trivial quantum analogue of the classical authenticated channel described above is the following:

(a') Same as (a), but for quantum messages.

(b') The attacker gets an arbitrary (polynomial) number of copies of any quantum message sent through the channel.

This model is not "realistic" in the sense that copying a quantum message is not possible in general. However, it does reasonably capture a scenario in which the sender is generating many copies of the message, in our case the quantum public key $|pk\rangle$ (which can be generated efficiently given sk), and distributing them to parties in a network. Then, the receiver gets one copy of the message, while the attacker may be able to collect many other copies.

Our two-message key-exchange protocol from public-key encryption with a quantum public key is secure as long as Alice's message is sent through a quantum authenticated channel satisfying (a') and (b') (Bob's message need not be sent through an authenticated channel). The security of this key-exchange protocol reduces exactly to the security of the underlying public-key encryption scheme.

References

[AC02] Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 323–334. Springer, 2002.

[AGQY23] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In *Theory of Cryptography: 20th International Conference, TCC 2022, Chicago, IL, USA, November 7–10, 2022, Proceedings, Part I*, pages 237–265. Springer, 2023.

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part I*, pages 208–236. Springer, 2022.

[BB84] Charles H Bennett and Gilles Brassard. Quantum cryptography. In *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India*, pages 175–179, 1984.

[BCKM21] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In *Annual International Cryptology Conference*, pages 467–496. Springer, 2021.

[BCQ22] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. *arXiv preprint arXiv:2209.04101*, 2022.

[BMG09] Boaz Barak and Mohammad Mahmoody-Ghidary. Merkle puzzles are optimal-an o (n2)-query attack on any key exchange from a random oracle. In *CRYPTO*, volume 5677, pages 374–390. Springer, 2009.

[BS19] Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase. In *Theory of Cryptography: 17th International Conference, TCC 2019, Nuremberg, Germany, December 1–5, 2019, Proceedings, Part I*, pages 229–250. Springer, 2019.

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions. In *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*, pages 42–52. IEEE Computer Society, 1988.

[DH76] Whitfield Diffie and Martin E Hellman. New directions in cryptography. *IEEE Transactions On Information Theory*, 22(6), 1976.

[GL89] Oded Goldreich and Leonid A Levin. A hard-core predicate for all one-way functions. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 25–32, 1989.

[GLSV21] Alex B Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In *Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part II*, pages 531–561. Springer, 2021.

[GM82] Shafi Goldwasser and Silvio Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pages 365–377, 1982.

[Har13] Aram W Harrow. The church of the symmetric subspace. *arXiv preprint arXiv:1308.6595*, 2013.

[IR89] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 44–61, 1989.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pages 126–152. Springer, 2018.

[KQST22] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. *arXiv preprint arXiv:2212.00879*, 2022.

[Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography*, 2021.

[MY22] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In *Advances in Cryptology–CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part I*, pages 269–295. Springer, 2022.

[Yao82] Andrew C Yao. Theory and application of trapdoor functions. In *23rd Annual Symposium on Foundations of Computer Science (SFCS 1982)*, pages 80–91. IEEE, 1982.

[Zha12] Mark Zhandry. How to construct quantum random functions. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 679–687. IEEE, 2012.