One-Wayness in Quantum Cryptography

Tomoyuki Morimae
Yukawa Institute for Theoretical Physics, Kyoto University, Japan

Takashi Yamakawa
NTT Social Informatics Laboratories, Tokyo, Japan
NTT Research Center for Theoretical Quantum Information, Atsugi, Japan
Yukawa Institute for Theoretical Physics, Kyoto University, Japan

Abstract

The existence of one-way functions is one of the most fundamental assumptions in classical cryptography. In the quantum world, on the other hand, there are evidences that some cryptographic primitives can exist even if one-way functions do not exist [Kretschmer, TQC 2021; Morimae and Yamakawa, CRYPTO 2022; Ananth, Qian, and Yuen, CRYPTO 2022]. We therefore have the following important open problem in quantum cryptography: What is the most fundamental assumption in quantum cryptography? In this direction, [Brakerski, Canetti, and Qian, ITCS 2023] recently defined a notion called EFI pairs, which are pairs of efficiently generatable states that are statistically distinguishable but computationally indistinguishable, and showed its equivalence with some cryptographic primitives including commitments, oblivious transfer, and general multi-party computations. However, their work focuses on decision-type primitives and does not cover search-type primitives like quantum money and digital signatures. In this paper, we study properties of one-way state generators (OWSGs), which are a quantum analogue of one-way functions proposed by Morimae and Yamakawa. We first revisit the definition of OWSGs and generalize it by allowing mixed output states. Then we show the following results.

1. We define a weaker version of OWSGs, which we call weak OWSGs, and show that they are equivalent to OWSGs. It is a quantum analogue of the amplification theorem for classical weak one-way functions.
2. (Bounded-time-secure) quantum digital signatures with quantum public keys are equivalent to OWSGs.
3. Private-key quantum money schemes (with pure money states) imply OWSGs.
4. Quantum pseudo one-time pad schemes imply both OWSGs and EFI pairs. For EFI pairs, single-copy security suffices.
5. We introduce an incomparable variant of OWSGs, which we call secretly-verifiable and statistically-invertible OWSGs, and show that they are equivalent to EFI pairs.

2012 ACM Subject Classification Theory of computation → Cryptographic primitives

Keywords and phrases Quantum Cryptography

Digital Object Identifier 10.4230/LIPIcs.TQC.2024.4

Related Version *Full Version*: `https://arxiv.org/abs/2210.03394`

Funding *Tomoyuki Morimae*: JST CREST JPMJCR23I3, JST Moonshot JPMJMS2061-5-1-1, JST FOREST, MEXT QLEAP, the Grant-in Aid for Transformative Research Areas (A) 21H05183, and the Grant-in-Aid for Scientific Research (A) No.22H00522.

1 Introduction

One-way functions (OWFs) are functions that are easy to compute but hard to invert. The existence of OWFs is one of the most fundamental assumptions in classical cryptography. OWFs are equivalent to many cryptographic primitives, such as commitments, digital signatures, pseudorandom generators (PRGs), symmetric-key encryption (SKE), and zero-knowledge, etc. Moreover, almost all other cryptographic primitives, such as collision-resistant

19th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2024).
Editors: Frédéric Magniez and Alex Bredariol Grilo; Article No. 4; pp. 4:1–4:21
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

hashes, public-key encryption (PKE), oblivious transfer (OT), multi-party computations (MPCs), etc., imply OWFs. In the quantum world, on the other hand, it seems that OWFs are not necessarily the most fundamental element. In fact, recently, several quantum cryptographic primitives, such as commitments, (one-time secure) digital signatures, quantum pseudo one-time pad (QPOTP)[1], and MPCs are constructed from pseudorandom states generators (PRSGs) [18, 3]. A PRSG [13], which is a quantum analogue of a PRG, is a QPT algorithm that outputs a quantum state whose polynomially-many copies are computationally indistinguishable from the same number of copies of Haar random states. Kretschmer [14] showed that PRSGs exist even if $\mathbf{BQP} = \mathbf{QMA}$ (relative to a quantum oracle), which means that PRSGs (and all the above primitives that can be constructed from PRSGs) could exist even if all quantum-secure (classical) cryptographic primitives including OWFs are broken.[2] Kretschmer, Qian, Sinha, and Tal [15] also showed that 1-PRSGs (which are variants of PRSGs secure against adversaries that get only a single copy of the state) exist even if $\mathbf{NP} = \mathbf{P}$. We therefore have the following important open problem in quantum cryptography:

Question 1: *What is the most fundamental assumption in quantum cryptography?*

In classical cryptography, a pair of PPT algorithms whose output probability distributions are statistically distinguishable but computationally indistinguishable is known to be fundamental. Goldreich [8] showed the equivalence of such a pair to PRGs, which also means the equivalence of such a pair to all cryptographic primitives in Minicrypt [11]. It is natural to consider its quantum analogue: a pair of QPT algorithms whose output quantum states are statistically distinguishable but computationally indistinguishable. In fact, such a pair was implicitly studied in quantum commitments [20]. In the canonical form of quantum commitments [22], computationally hiding and statistically binding quantum commitments are equivalent to such pairs. The importance of such a pair as an independent quantum cryptograpic primitive was pointed out in [20, 4]. In particular, the authors of [4] explicitly defined it as *EFI pairs*,[3] and showed that EFI pairs are implied by several quantum cryptographic primitives such as (semi-honest) quantum OT, (semi-honest) quantum MPCs, and (honest-verifier) quantum computational zero-knowledge proofs. It is therefore natural to ask the following question.

Question 2: *Which other quantum cryptographic primitives imply EFI pairs?*

PRSGs and EFI pairs are "decision type" primitives, which correspond to PRGs in classical cryptography. An example of the other type of primitives, namely, "search type" one in classical cryptography, is OWFs. Recently, a quantum analogue of OWFs, so called one-way states generators (OWSGs), are introduced [18]. A OWSG is a QPT algorithm that, on input a classical bit string (key) k, outputs a quantum state $|\phi_k\rangle$. As the security, we require that it is hard to find k' such that $|\langle\phi_k|\phi_{k'}\rangle|^2$ is non-negligible given polynomially many copies of $|\phi_k\rangle$. The authors showed that OWSGs are implied by PRSGs, and that OWSGs imply (one-time secure) quantum digital signatures with quantum public keys. In classical cryptography, OWFs are connected to many cryptographic primitives. We are therefore interested in the following question.

[1] QPOTP schemes are a one-time-secure SKE with quantum ciphertexts where the key length is shorter than the massage length. (For the definition, see Definition 29.)

[2] If $\mathbf{QMA} = \mathbf{BQP}$, then $\mathbf{NP} \subseteq \mathbf{BQP}$. Because all quantum-secure classical cryptographic primitives are in $\mathbf{NP}$, it means that they are broken by QPT algorithms.

[3] It stands for efficiently samplable, statistically far but computationally indistinguishable pairs of distributions.

Question 3: *Which quantum cryptographic primitives are related to OWSGs?*

In classical cryptography, PRGs (i.e., a decision-type primitive) and OWFs (i.e., a search-type primitive) are equivalent. In quantum cryptography, on the other hand, we do not know whether OWSGs and EFI pairs (or PRSGs) are equivalent or not. We therefore have the following open problem.

Question 4: *Are OWSGs and EFI pairs (or PRSGs) equivalent?*

1.1 Our Results

The study of quantum cryptography with complexity assumptions has became active only very recently, and therefore we do not yet have enough knowledge to answer **Question 1**. However, as an important initial step towards the ultimate goal, we give some answers to other questions above. Our results are summarized as follows. (See also Fig. 1.)

1. We first revisit the definition of OWSGs. In the original definition in [18], output states of OWSGs are assumed to be pure states. Moreover, the verification is done as follows: a bit string k' from the adversary is accepted if and only if the state $|\phi_k\rangle\langle\phi_k|$ is measured in the basis $\{|\phi_{k'}\rangle\langle\phi_{k'}|, I - |\phi_{k'}\rangle\langle\phi_{k'}|\}$, and the first result is obtained. (Note that in classical OWFs, the verification is implicit because it is trivial: just computing $f(x')$ for x' given by the adversary, and check whether it is equal to $f(x)$ or not. However, in the quantum case, we have to explicitly define the verification.) In this paper, to capture more general settings, we generalize the definition of OWSGs by allowing outputs to be mixed states. A non-trivial issue that arises from this modification is that there is no canonical way to verify input-output pairs of OWSGs. To deal with this issue, we include such a verification algorithm as a part of syntax of OWSGs.
2. We show an "amplification theorem" for OWSGs. That is, we define weak OWSGs (wOWSGs), which only requires the adversary's advantage to be $1 - 1/\mathrm{poly}(\lambda)$ instead of $\mathsf{negl}(\lambda)$, and show that a parallel repetition of wOWSGs gives OWSGs. This is an analogue of the equivalence of weak one-way functions and (strong) one-way functions in classical cryptography [23].
3. We show that one-time-secure quantum digital signatures (QDSs) with quantum public keys are equivalent to OWSGs.[4] Moreover, we can generically upgrade one-time-secure QDSs into bounded-time-secure one.[5]
4. We show that private-key quantum money schemes (with pure money states or with verification algorithms that satisfy some symmetry) imply OWSGs.
5. We show that QPOTP schemes imply OWSGs. This in particular means that IND-CPA secure quantum SKE or quantum PKE implies OWSGs.
6. We show that single-copy-secure QPOTP schemes imply EFI pairs. Single-copy-security means that the adversary receives only a single copy of the quantum ciphertext. This in particular means that IND-CPA secure quantum SKE or quantum PKE implies EFI pairs.
7. We introduce an incomparable variant of OWSGs, which we call secretly-verifiable and statistically-invertible OWSGs (SV-SI-OWSGs), and show that SV-SI-OWSGs are equivalent to EFI pairs.

[4] A construction of QDSs from OWSGs was already shown in [18], but in this paper, we generalize the definition of OWSGs, and we give the proof in the new definition.

[5] We thank Or Sattath for asking if we can get (stateless) bounded-time QDSs.

We remark that we consider the generalized definition of OWSGs with mixed state outputs by default. However, all the relationships between OWSGs and other primitives naturally extend to the pure state version if we consider the corresponding pure state variants of the primitives.

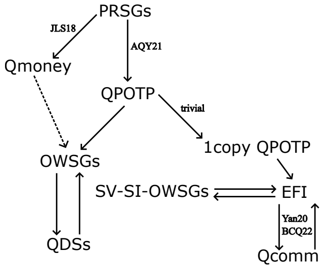

Figure 1 Summary of results. The dotted line means some restrictions: OWSGs are implied by quantum money schemes with *pure* money states or with *symmetric* verification algorithms.

2 Preliminaries

2.1 Basic Notations

We use the standard notations of quantum computing and cryptography. We use λ as the security parameter. $[n]$ means the set $\{1,2,...,n\}$. For any set S, $x \leftarrow S$ means that an element x is sampled uniformly at random from the set S. negl is a negligible function, and poly is a polynomial. PPT stands for (classical) probabilistic polynomial-time and QPT stands for quantum polynomial-time. If we say that an adversary is QPT, it implicitly means non-uniform QPT. A QPT unitary is a unitary operator that can be implemented in a QPT quantum circuit.

For an algorithm A, $y \leftarrow A(x)$ means that the algorithm A outputs y on input x. In particular, if x and y are quantum states and A is a quantum algorithm, $y \leftarrow A(x)$ means the following: a unitary U is applied on $x \otimes |0...0\rangle\langle 0...0|$, and some qubits are traced out. Then, the state of remaining qubits is y. This, importantly, means that the state y is *uniquely decided* by the state x. If A is a QPT algorithm, the unitary U is QPT and the number of ancilla qubits $|0...0\rangle$ is $\mathrm{poly}(\lambda)$. If x is a classical bit string, y is a quantum state, and A is a quantum algorithm, $y \leftarrow A(x)$ sometimes means the following: a unitary U_x that depends on x is applied on $|0...0\rangle$, and some qubits are traced out. The state of the remaining qubits is y. This picture is the same as the most general one where x is given as input, but we sometime choose this picture if it is more convenient.

$\|X\|_1 := \mathrm{Tr}\sqrt{X^\dagger X}$ is the trace norm. $\mathrm{Tr}_{\mathbf{A}}(\rho_{\mathbf{A},\mathbf{B}})$ means that the subsystem (register) $\mathbf{A}$ of the state $\rho_{\mathbf{A},\mathbf{B}}$ on two subsystems (registers) $\mathbf{A}$ and $\mathbf{B}$ is traced out. For simplicity, we sometimes write $\mathrm{Tr}_{\mathbf{A},\mathbf{B}}(|\psi\rangle_{\mathbf{A},\mathbf{B}})$ to mean $\mathrm{Tr}_{\mathbf{A},\mathbf{B}}(|\psi\rangle\langle\psi|_{\mathbf{A},\mathbf{B}})$. I is the two-dimensional identity operator. For simplicity, we sometimes write $I^{\otimes n}$ as I if the dimension is clear from the context. For the notational simplicity, we sometimes write $|0...0\rangle$ just as $|0\rangle$, when the number of zeros is clear from the context. For two pure states $|\psi\rangle$ and $|\phi\rangle$, we sometimes write $\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\|_1$ as $\||\psi\rangle - |\phi\rangle\|_1$ to simplify the notation. $F(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ is the fidelity between ρ and σ. We often use the well-known relation between the trace distance and the fidelity: $1 - \sqrt{F(\rho,\sigma)} \le \frac{1}{2}\|\rho - \sigma\|_1 \le \sqrt{1 - F(\rho,\sigma)}$.

2.2 EFI Pairs

The concept of EFI pairs was implicitly studied in [20], and explicitly defined in [4].

▶ **Definition 1** (EFI pairs [4]). *An EFI pair is an algorithm* $\mathsf{StateGen}(b, 1^\lambda) \to \rho_b$ *that, on input* $b \in \{0,1\}$ *and the security parameter* λ*, outputs a quantum state* ρ_b *such that all of the following three conditions are satisfied.*

- *It is a uniform QPT algorithm.*
- ρ_0 *and* ρ_1 *are computationally indistinguishable. In other words, for any QPT adversary* $\mathcal{A}$*,* $|\Pr[1 \leftarrow \mathcal{A}(1^\lambda, \rho_0)] - \Pr[1 \leftarrow \mathcal{A}(1^\lambda, \rho_1)]| \le \mathsf{negl}(\lambda)$.
- ρ_0 *and* ρ_1 *are statistically distinguishable, i.e.,* $\frac{1}{2}\|\rho_0 - \rho_1\|_1 \ge \frac{1}{\mathrm{poly}(\lambda)}$.

▶ Remark 2. Note that in the above definition, the statistical distinguishability is defined with only $\ge 1/\mathrm{poly}(\lambda)$ advantage. However, if EFI pairs with the above definition exist, EFI pairs with $\ge 1 - \mathsf{negl}(\lambda)$ statistical distinguishability exist as well. In fact, we have only to define a new $\mathsf{StateGen}'$ that runs $\mathsf{StateGen}$ n times with sufficiently large $n = \mathrm{poly}(\lambda)$, and outputs $\rho_b^{\otimes n}$. The $\ge 1 - \mathsf{negl}(\lambda)$ statistical distinguishability for $\mathsf{StateGen}'$ is shown from the inequality [4], $\frac{1}{2}\|\rho^{\otimes n} - \sigma^{\otimes n}\|_1 \ge 1 - \exp(-n\|\rho - \sigma\|_1/4)$. The computational indistinguishability for $\mathsf{StateGen}'$ is shown by the standard hybrid argument.

2.3 Quantum Commitments

We define canonical quantum bit commitments [20] as follows.

▶ **Definition 3** (Canonical quantum bit commitments [20]). *A canonical quantum bit commitment scheme is a family* $\{Q_0(\lambda), Q_1(\lambda)\}_{\lambda\in\mathbb{N}}$ *of QPT unitaries on two registers* $\mathbf{C}$ *(called the* commitment *register) and* $\mathbf{R}$ *(called the* reveal *register). For simplicity, we often omit* λ *and simply write* $\{Q_0, Q_1\}$ *to mean* $\{Q_0(\lambda), Q_1(\lambda)\}_{\lambda\in\mathbb{N}}$.

▶ Remark 4. Canonical quantum bit commitments are used as follows. In the commit phase, to commit to a bit $b \in \{0,1\}$, the sender generates a state $Q_b|0\rangle_{\mathbf{C},\mathbf{R}}$ and sends $\mathbf{C}$ to the receiver while keeping $\mathbf{R}$. In the reveal phase, the sender sends b and $\mathbf{R}$ to the receiver. The receiver projects the state on $(\mathbf{C},\mathbf{R})$ onto $Q_b|0\rangle_{\mathbf{C},\mathbf{R}}$, and accepts if it succeeds and otherwise rejects. (In other words, the receiver applies the unitary $Q_b^\dagger$ on the registers $\mathbf{C}$ and $\mathbf{R}$, and measure all qubits in the computational basis. If all result are zero, accept. Otherwise, reject.)

▶ **Definition 5** (Hiding). *We say that a canonical quantum bit commitment scheme* $\{Q_0, Q_1\}$ *is computationally (rep. statistically)* hiding *if* $\mathrm{Tr}_{\mathbf{R}}(Q_0 |0\rangle_{\mathbf{C},\mathbf{R}})$ *is computationally (resp. statistically) indistinguishable from* $\mathrm{Tr}_{\mathbf{R}}(Q_1 |0\rangle_{\mathbf{C},\mathbf{R}})$*. We say that it is perfectly hiding if they are identical states.*

▶ **Definition 6** (Binding). *We say that a canonical quantum bit commitment scheme* $\{Q_0, Q_1\}$ *is computationally (rep. statistically)* binding *if for any QPT (resp. unbounded-time) unitary* U *over* $\mathbf{R}$ *and an additional register* $\mathbf{Z}$ *and any polynomial-size state* $|\tau\rangle_{\mathbf{Z}}$*, it holds that*

$$\left\|(\langle 0| Q_1^\dagger)_{\mathbf{C},\mathbf{R}}(I_{\mathbf{C}} \otimes U_{\mathbf{R},\mathbf{Z}})((Q_0 |0\rangle)_{\mathbf{C},\mathbf{R}} |\tau\rangle_{\mathbf{Z}})\right\| = \mathsf{negl}(\lambda). \tag{1}$$

We say that it is perfectly hiding if the LHS is 0 *for all unbounded-time unitary* U*.* [6]

[6] The above definition is asymmetric for 0 and 1, but it is easy to show that Equation (1) implies

$$\left\|(\langle 0| Q_0^\dagger)_{\mathbf{C},\mathbf{R}}(I_{\mathbf{C}} \otimes U_{\mathbf{R},\mathbf{Z}})((Q_1 |0\rangle)_{\mathbf{C},\mathbf{R}} |\tau\rangle_{\mathbf{Z}})\right\| = \mathsf{negl}(\lambda)$$

for any U and $|\tau\rangle$.

▶ Remark 7. One may think that honest-binding defined above is too weak because it only considers honestly generated commitments. However, somewhat surprisingly, [20] proved that it is equivalent to another binding notion called the *sum-binding* [5].[7] The sum-binding property requires that the sum of probabilities that any (quantum polynomial-time, in the case of computational binding) *malicious* sender can open a commitment to 0 and 1 is at most $1 + \mathsf{negl}(\lambda)$. In addition, it has been shown that the honest-binding property is sufficient for cryptographic applications including zero-knowledge proofs/arguments (of knowledge), oblivious transfers, and multi-party computation [22, 6, 18, 21]. In this paper, we refer to honest-binding if we simply write binding.

In this paper, we use the following result.

▶ **Theorem 8** (Converting flavors [20, 10]). *Let $\{Q_0, Q_1\}$ be a canonical quantum bit commitment scheme. Then there exists a canonical quantum bit commitment scheme $\{Q'_0, Q'_1\}$, and the following hold for $\mathtt{X}, \mathtt{Y} \in \{$computationally,statistically,perfectly$\}$:*

- *If $\{Q_0, Q_1\}$ is $\mathtt{X}$ hiding, then $\{Q'_0, Q'_1\}$ is $\mathtt{X}$ binding.*
- *If $\{Q_0, Q_1\}$ is $\mathtt{Y}$ binding, then $\{Q'_0, Q'_1\}$ is $\mathtt{Y}$ hiding.*

3 OWSGs

In this section, we first define OWSGs (Section 3.1). We then define weak OWSGs and show that weak OWSGs are equivalent to OWSGs (Section 3.2).

3.1 Definition of OWSGs

In this subsection, we define OWSGs. Note that the definition below is a generalization of the one given in [18] in the following three points. First, in [18], the generated states are pure, but here they can be mixed. Second, in [18], the secret key k is uniformly sampled at random, but now it is sampled by a QPT algorithm. Third, in [18], the verification algorithm is the specific algorithm that accepts the alleged key k' with probability $|\langle\phi_k|\phi_{k'}\rangle|^2$, while here we consider a general verification algorithm. We think the definition below is more general (and therefore more fundamental) than that in [18]. Hence hereafter we choose the definition below as the definition of OWSGs.

▶ **Definition 9** (One-way states generators (OWSGs)). *A one-way states generator (OWSG) is a set of algorithms* $(\mathsf{KeyGen}, \mathsf{StateGen}, \mathsf{Ver})$ *such that*

- $\mathsf{KeyGen}(1^\lambda) \to k$: *It is a QPT algorithm that, on input the security parameter λ, outputs a classical key $k \in \{0,1\}^\kappa$.*
- $\mathsf{StateGen}(k) \to \phi_k$: *It is a QPT algorithm that, on input k, outputs an m-qubit quantum state ϕ_k.*
- $\mathsf{Ver}(k', \phi_k) \to \top/\bot$: *It is a QPT algorithm that, on input ϕ_k and a bit string k', outputs $\top$ or $\bot$.*

We require the following correctness and security.

Correctness: $\Pr\big[\top \leftarrow \mathsf{Ver}(k, \phi_k) : k \leftarrow \mathsf{KeyGen}(1^\lambda), \phi_k \leftarrow \mathsf{StateGen}(k)\big] \geq 1 - \mathsf{negl}(\lambda)$.

Security: *For any QPT adversary $\mathcal{A}$ and any polynomial t*[8]*,*

$$\Pr\big[\top \leftarrow \mathsf{Ver}(k', \phi_k) : k \leftarrow \mathsf{KeyGen}(1^\lambda), \phi_k \leftarrow \mathsf{StateGen}(k), k' \leftarrow \mathcal{A}(1^\lambda, \phi_k^{\otimes t})\big] \leq \mathsf{negl}(\lambda).$$

[7] The term “sum-binding” is taken from [19].

[8] $\mathsf{StateGen}$ is actually run t times to generate t copies of ϕ_k, but for simplicity, we just write $\phi_k \leftarrow \mathsf{StateGen}(k)$ only once. This simplification will often be used in this paper.

▶ Remark 10. If ϕ_k is pure, StateGen runs as follows. Apply a QPT unitary U on $|k\rangle|0...0\rangle$ to generate $|\phi_k\rangle \otimes |\eta_k\rangle$, and output $|\phi_k\rangle$. In this case, the existence of the "junk state" $|\eta_k\rangle$ is essential, because otherwise it is not secure against a QPT adversary who does the application of $U^\dagger$ and the computational-basis measurement.

▶ Remark 11. Note that statistically-secure OWSGs do not exist. In other words, there exists an unbounded algorithm $\mathcal{A}$ that can break the security of OWSGs as follows:

1. Given $\phi_k^{\otimes t}$ with a certain polynomial t as input, run the shadow tomography algorithm [1] to find k' such that $\Pr[\mathsf{Ver}(k', \phi_k) \to \top] \geq 1 - \frac{1}{\mathrm{poly}(\lambda)}$. If there exists such k', such k' can be found with only a certain polynomial t. If there is no such k', choose k' uniformly at ramdom.
2. Output k'.

3.2 Hardness Amplification for OWSGs

In this subsection, we define a weaker variant called weak one-way states generators (wOWSGs), and show that they are equivalent to OWSGs.

wOWSGs are defined as follows.

▶ **Definition 12** (Weak one-way states generators (wOWSGs)). *A weak one-way states generator (wOWSG) is a tuple of algorithms* (KeyGen, StateGen, Ver) *defined similarly to OWSGs except that the security is replaced with the following weak security.*

Weak Security: *There exists a polynomial p such that for any QPT adversary $\mathcal{A}$ and any polynomial t,*

$$\Pr\left[\top \leftarrow \mathsf{Ver}(k', \phi_k) : k \leftarrow \mathsf{KeyGen}(1^\lambda), \phi_k \leftarrow \mathsf{StateGen}(k), k' \leftarrow \mathcal{A}(1^\lambda, \phi_k^{\otimes t})\right] \leq 1 - \frac{1}{p}.$$

We prove that the existence of wOWSGs imply the existence of OWSGs. This is an analogue of Yao's amplification theorem for OWFs in the classical setting [23, 9].

▶ **Theorem 13.** *OWSGs exist if and only if wOWSGs exist.*

For its proof, see the full version.

4 QDSs

In this section, we first define QDSs (Section 4.1), and show that one-time-secure QDSs can be extended to q-time-secure ones (Section 4.2). We then show that one-time-secure QDSs are equivalent to OWSGs (Section 4.3).

4.1 Definition of QDSs

Quantum digital signatures are defined as follows.

▶ **Definition 14** (Quantum digital signatures (QDSs) [18]). *A quantum digital signature (QDS) scheme is a set of algorithms* (SKGen, PKGen, Sign, Ver) *such that*

- $\mathsf{SKGen}(1^\lambda) \to \mathsf{sk}$: *It is a QPT algorithm that, on input the security parameter λ, outputs a classical secret key* sk.
- $\mathsf{PKGen}(\mathsf{sk}) \to \mathsf{pk}$: *It is a QPT algorithm that, on input* sk*, outputs a quantum public key* pk.
- $\mathsf{Sign}(\mathsf{sk}, m) \to \sigma$: *It is a QPT algorithm that, on input* sk *and a message m, outputs a classical signature σ.*
- $\mathsf{Ver}(\mathsf{pk}, m, \sigma) \to \top/\bot$: *It is a QPT algorithm that, on input* pk*, m, and σ, outputs $\top/\bot$.*

We require the correctness and the security as follows.

Correctness: *For any m,*

$$\Pr\left[\top \leftarrow \mathsf{Ver}(\mathsf{pk}, m, \sigma) : \begin{array}{c} \mathsf{sk} \leftarrow \mathsf{SKGen}(1^\lambda), \\ \mathsf{pk} \leftarrow \mathsf{PKGen}(\mathsf{sk}), \\ \sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m) \end{array}\right] \geq 1 - \mathsf{negl}(\lambda).$$

q-time security: *Let us consider the following security game,* Exp*, between a challenger $\mathcal{C}$ and a QPT adversary $\mathcal{A}$:*

1. *$\mathcal{C}$ runs* $\mathsf{sk} \leftarrow \mathsf{SKGen}(1^\lambda)$*.*
2. *$\mathcal{C}$ runs* $\mathsf{pk} \leftarrow \mathsf{PKGen}(\mathsf{sk})$ *t times, and sends* $\mathsf{pk}^{\otimes t}$ *to $\mathcal{A}$.*
3. *For $i = 1$ to q, do:*
   - **a.** *$\mathcal{A}$ sends a message $m^{(i)}$ to $\mathcal{C}$.*
   - **b.** *$\mathcal{C}$ runs* $\sigma^{(i)} \leftarrow \mathsf{Sign}(\mathsf{sk}, m^{(i)})$*, and sends $\sigma^{(i)}$ to $\mathcal{A}$.*
4. *$\mathcal{A}$ sends σ' and m' to $\mathcal{C}$.*
5. *$\mathcal{C}$ runs* $\mathsf{pk} \leftarrow \mathsf{PKGen}(\mathsf{sk})$ *and* $v \leftarrow \mathsf{Ver}(\mathsf{pk}, m', \sigma')$*. If $m' \notin \{m^{(1)}, \dots, m^{(q)}\}$ and $v = \top$, the output of the game is 1. Otherwise, the output of the game is 0.*

For any QPT adversary $\mathcal{A}$ and any polynomial t, $\Pr[\mathsf{Exp} = 1] \leq \mathsf{negl}(\lambda)$.

▶ Remark 15. By using the shadow tomography, we can show that statistically-secure QDSs do not exist.

4.2 Extension to q-time Security

▶ **Theorem 16.** *If one-time-secure QDSs exist, then q-time-secure QDSs exist for any polynomial q.*

The idea is similar to the one-time to q-time conversion for attribute-based encryption in [12]. We first consider a scheme where we generate q^2 key pairs of one-time-secure scheme and uniformly chooses one of q^2 signing keys to generate a signature whenever we run the signing algorithm. This scheme is not q-bounded-secure because the probability that the same signing key is used more than once is non-negligible. However, by a simple combinatorial argument, we can upper bound the probability of such a "bad" event by some constant smaller than 1. Thus, by repeating this construction λ times, we can amplify the security to get q-bounded-secure scheme.

For a formal proof, see the full version.

4.3 Equivalence of OWSGs and QDSs

▶ **Theorem 17.** *OWSGs exist if and only if one-time-secure QDSs exist.*

▶ Remark 18. By using the equivalence between OWSGs and wOWSGs (Theorem 13), the result that one-time-secure QDSs imply OWSGs can be improved to a stronger result (with a similar proof) that one-time-secure QDSs with weak security imply OWSGs. Here, the weak security of QDSs means that there exists a polynomial p such that for any QPT adversary $\mathcal{A}$ and any polynomial t, $\Pr[\mathsf{Exp} = 1] \leq 1 - \frac{1}{p}$.

It is proven in [18] that OWSGs implies one-time-secure QDSs. However, since we generalize the definition of OWSGs, we need to reprove it. Fortunately, almost the same construction as that in [18] works with the generalized definition of OWSGs. Roughly, the construction is as follows when the message space is one-bit: a secret key is $\mathsf{sk} = (k_0, k_1)$, a public key is $\mathsf{pk} = (\phi_{k_0}, \phi_{k_1})$, and a signature for a bit $b \in \{0, 1\}$ is k_b. The verification algorithm of QDSs simply runs that of the OWSG.

For the other direction, we construct OWSGs from QDSs by regarding sk and pk of QDSs as k and ϕ_k of OWSGs.

For a formal proof, see the full version.

5 Quantum Money

In this section, we first define private-key quantum money schemes (Section 5.1). We then construct OWSGs from quantum money schemes with pure money states (Section 5.2). We also show that OWSGs can be constructed from quantum money schemes where the verification algorithms satisfy a certain symmetric property (Section 5.3).

5.1 Definition of Private-key Quantum Money

Private-key quantum money schemes are defined as follows.

▶ **Definition 19** (Private-key quantum money [13, 2]). *A private-key quantum money scheme is a set of algorithms* $(\mathsf{KeyGen},\mathsf{Mint},\mathsf{Ver})$ *such that*

- $\mathsf{KeyGen}(1^\lambda)\to k$: *It is a QPT algorithm that, on input the security parameter* λ*, outputs a classical secret key* k*.*
- $\mathsf{Mint}(k)\to \$_k$: *It is a QPT algorithm that, on input* k*, outputs an* m*-qubit quantum state* $\$_k$*.*
- $\mathsf{Ver}(k,\rho)\to \top/\bot$: *It is a QPT algorithm that, on input* k *and a quantum state* ρ*, outputs* $\top/\bot$*.*

We require the following correctness and security.

Correctness:

$$\Pr\left[\top\leftarrow\mathsf{Ver}(k,\$_k):k\leftarrow\mathsf{KeyGen}(1^\lambda),\$_k\leftarrow\mathsf{Mint}(k)\right]\geq 1-\mathsf{negl}(\lambda).$$

Security: *For any QPT adversary* $\mathcal{A}$ *and any polynomial* t*,*

$$\Pr\left[\mathsf{Count}(k,\xi)\geq t+1:k\leftarrow\mathsf{KeyGen}(1^\lambda),\$_k\leftarrow\mathsf{Mint}(k),\xi\leftarrow\mathcal{A}(1^\lambda,\$_k^{\otimes t})\right]\leq\mathsf{negl}(\lambda),$$

where ξ *is a quantum state on* ℓ *registers,* $R_1,...,R_\ell$*, each of which is of* m *qubits, and* Count *is the following QPT algorithm: on input* ξ*, it runs* $\top/\bot\leftarrow\mathsf{Ver}(k,\xi_j)$ *for each* $j\in[1,2,...,\ell]$*, where* $\xi_j:=Tr_{R_1,...,R_{j-1},R_{j+1},...,R_\ell}(\xi)$*, and outputs the total number of* $\top$*.*

▶ Remark 20. Private-key quantum money schemes are constructed from PRSGs [13].

▶ Remark 21. As is shown in [1], private-key quantum money schemes are broken by an unbounded adversary, and therefore statistically-secure private-key quantum money schemes do not exist. (The idea is as follows: the unbounded adversary first finds all $\{k_i\}_i$ such that $\mathsf{Ver}(k_i,\$_k)$ is large with the shadow tomography, and then searches a state ρ by the brute-force such that $\mathsf{Ver}(k_i,\rho)$ is close to $\mathsf{Ver}(k_i,\$_k)$ FOR ALL i. Finally, the adversary outputs many copies of ρ.)

5.2 OWSGs from Quantum Money with Pure Money States

▶ **Theorem 22.** *If private-key quantum money schemes with pure quantum money states exist, then OWSGs exist.*

▶ Remark 23. For example, the private-key quantum money scheme of [13] has pure quantum money states.

▶ Remark 24. By using the equivalence between OWSGs and wOWSGs (Theorem 13), this result can be improved to a stronger result (with a similar proof) that private-key quantum money schemes with pure quantum money states and with weak security imply OWSGs. Here, the weak security means that there exists a polynomial p such that for any QPT adversary $\mathcal{A}$ and any polynomial t,

$$\Pr\left[\mathsf{Count}(k,\xi)\geq t+1:k\leftarrow\mathsf{KeyGen}(1^\lambda),\$_k\leftarrow\mathsf{Mint}(k),\xi\leftarrow\mathcal{A}(1^\lambda,\$_k^{\otimes t})\right]\leq 1-\frac{1}{p}.$$

Proof of Theorem 22. Let $(\mathsf{QM.KeyGen}, \mathsf{QM.Mint}, \mathsf{QM.Ver})$ be a private-key quantum money scheme with pure money states. From it, we construct a OWSG as follows.

- $\mathsf{KeyGen}(1^\lambda) \to k$: Run $k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)$. Output k.
- $\mathsf{StateGen}(k) \to \phi_k$: Run $|\$_k\rangle \leftarrow \mathsf{QM.Mint}(k)$. Output $\phi_k := |\$_k\rangle\langle\$_k|$.
- $\mathsf{Ver}(k', \phi_k) \to \top/\bot$: Parse $\phi_k = |\$_k\rangle\langle\$_k|$. Measure $|\$_k\rangle$ with the basis $\{|\$_{k'}\rangle\langle\$_{k'}|, I - |\$_{k'}\rangle\langle\$_{k'}|\}$, and output $\top$ if the first result is obtained. Output $\bot$ if the second result is obtained. (This measurement is done in the following way: generate $U(|k'\rangle|0...0\rangle) = |\$_{k'}\rangle|\eta_{k'}\rangle$, and discard the first register. Then apply $U^\dagger$ on $|\$_k\rangle|\eta_{k'}\rangle$, and measure all qubits in the computationl basis. If the result is $k'0...0$, accept. Otherwise, reject.)

The correctness is clear. Let us show the security. Assume that it is not secure. Then, there exists a QPT adversary $\mathcal{A}$, a polynomial t, and a polynomial p such that

$$\sum_{k,k'} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] \Pr\big[k' \leftarrow \mathcal{A}(|\$_k\rangle^{\otimes t})\big] |\langle\$_k|\$_{k'}\rangle|^2 \geq \frac{1}{p}.$$

Define the set $S := \Big\{(k, k') \;\Big|\; |\langle\$_k|\$_{k'}\rangle|^2 \geq \frac{1}{2p}\Big\}$. Then, we have

$$\sum_{(k,k')\in S} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] \Pr\big[k' \leftarrow \mathcal{A}(|\$_k\rangle^{\otimes t})\big] > \frac{1}{2p}.$$

This is shown as follows.

$$\begin{aligned}
\frac{1}{p} &\leq \sum_{k,k'} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] \Pr\big[k' \leftarrow \mathcal{A}(|\$_k\rangle^{\otimes t})\big] |\langle\$_k|\$_{k'}\rangle|^2 \\
&= \sum_{(k,k')\in S} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] \Pr\big[k' \leftarrow \mathcal{A}(|\$_k\rangle^{\otimes t})\big] |\langle\$_k|\$_{k'}\rangle|^2 \\
&\quad + \sum_{(k,k')\notin S} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] \Pr\big[k' \leftarrow \mathcal{A}(|\$_k\rangle^{\otimes t})\big] |\langle\$_k|\$_{k'}\rangle|^2 \\
&< \sum_{(k,k')\in S} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] \Pr\big[k' \leftarrow \mathcal{A}(|\$_k\rangle^{\otimes t})\big] + \frac{1}{2p}.
\end{aligned}$$

Let us also define $T := \Big\{k \;\Big|\; \Pr[\top \leftarrow \mathsf{QM.Ver}(k, |\$_k\rangle)] \geq 1 - \frac{1}{8p}\Big\}$. Then, $\sum_{k\in T} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] > 1 - \mathsf{negl}(\lambda)$. This is shown as follows.

$$\begin{aligned}
1 - \mathsf{negl}(\lambda) &\leq \sum_{k} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] \Pr[\top \leftarrow \mathsf{QM.Ver}(k, |\$_k\rangle)] \\
&= \sum_{k\in T} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] \Pr[\top \leftarrow \mathsf{QM.Ver}(k, |\$_k\rangle)] \\
&\quad + \sum_{k\notin T} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] \Pr[\top \leftarrow \mathsf{QM.Ver}(k, |\$_k\rangle)] \\
&< \sum_{k\in T} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big] \\
&\quad + \Big(1 - \frac{1}{8p}\Big)\Big(1 - \sum_{k\in T} \Pr\big[k \leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big]\Big).
\end{aligned}$$

Here, the first inequality is from the correctness of the quantum money scheme.

Let us fix (k,k') such that $(k,k')\in S$ and $k\in T$. The probability of having such (k,k') is, from the union bound,

$$\begin{aligned}\sum_{(k,k')\in S\wedge k\in T}\Pr\big[k\leftarrow \mathsf{QM.KeyGen}(1^\lambda)\big]\Pr\big[k'\leftarrow\mathcal{A}(|\$_k\rangle^{\otimes t})\big] &> \frac{1}{2p}+1-\mathsf{negl}(\lambda)-1\\ &= \frac{1}{2p}-\mathsf{negl}(\lambda).\end{aligned}$$

From the $\mathcal{A}$, we construct a QPT adversary $\mathcal{B}$ that breaks the security of the private-key quantum money scheme as follows: On input $|\$_k\rangle^{\otimes t}$, it runs $k'\leftarrow\mathcal{A}(|\$_k\rangle^{\otimes t})$. It then runs $|\$_{k'}\rangle\leftarrow\mathsf{QM.Mint}(k')$ ℓ times, where ℓ is a polynomial specified later, and outputs $\xi:=|\$_{k'}\rangle^{\otimes\ell}$. Let us show that thus defined $\mathcal{B}$ breaks the security of the private-key quantum money scheme. Let v_j be the bit that is 1 if the output of $\mathsf{QM.Ver}(k,\xi_j)$ is $\top$, and is 0 otherwise. Then, for any (k,k') such that $(k,k')\in S$ and $k\in T$,

$$\begin{aligned}\Pr[v_j=1] &= \Pr[\top\leftarrow\mathsf{QM.Ver}(k,\xi_j)]=\Pr[\top\leftarrow\mathsf{QM.Ver}(k,|\$_{k'}\rangle)]\\ &\geq \Pr[\top\leftarrow\mathsf{QM.Ver}(k,|\$_k\rangle)]-\sqrt{1-\frac{1}{2p}}\geq 1-\frac{1}{8p}-\sqrt{1-\frac{1}{2p}}\geq\frac{1}{8p}\end{aligned}$$

for each $j\in[1,2,...,\ell]$. Here, in the first inequality, we have used the fact that $\Pr[1\leftarrow\mathcal{D}(|\$_k\rangle)]-\Pr[1\leftarrow\mathcal{D}(|\$_{k'}\rangle)]\leq\sqrt{1-\frac{1}{2p}}$ for any algorithm $\mathcal{D}$. This is because $|\langle\$_k|\$_{k'}\rangle|^2\geq\frac{1}{2p}$ for any $(k,k')\in S$.[9] Moreover, in the second inequality, we have used the fact that $\Pr[\top\leftarrow\mathsf{QM.Ver}(k,|\$_k\rangle)]\geq 1-\frac{1}{8p}$ for any $k\in T$. Finally, in the last inequality, we have used the Bernoulli's inequality.[10]

Let us take $\ell\geq\max(16p(t+1),16^2p^3)$. Then, for any (k,k') such that $(k,k')\in S$ and $k\in T$,

$$\begin{aligned}\Pr\big[\mathsf{Count}(k,|\$_{k'}\rangle^{\otimes\ell})\geq t+1\big] &= \Pr\left[\sum_{j=1}^{\ell}v_j\geq t+1\right]\geq\Pr\left[\sum_{j=1}^{\ell}v_j\geq\frac{\ell}{16p}\right]\\ &= \Pr\left[\sum_{j=1}^{\ell}v_j\geq\frac{\ell}{8p}-\frac{\ell}{16p}\right]\geq\Pr\left[\sum_{j=1}^{\ell}v_j\geq\mathbb{E}(\sum_{j=1}^{\ell}v_j)-\frac{\ell}{16p}\right]\\ &\geq 1-2\exp\left[-\frac{2\ell}{16^2p^2}\right]\geq 1-2e^{-2p}.\end{aligned}$$

Here, in the third inequality, we have used Hoeffding's inequality. The probability that $\mathcal{B}$ breaks the security of the quantum money scheme is therefore

$$\begin{aligned}&\sum_{k,k'}\Pr\big[k\leftarrow\mathsf{QM.KeyGen}(1^\lambda)\big]\Pr\big[k'\leftarrow\mathcal{A}(|\$_k\rangle^{\otimes t})\big]\Pr\big[\mathsf{Count}(k,|\$_{k'}\rangle^{\otimes\ell})\geq t+1\big]\\ \geq&\sum_{(k,k')\in S\wedge k\in T}\Pr\big[k\leftarrow\mathsf{QM.KeyGen}(1^\lambda)\big]\Pr\big[k'\leftarrow\mathcal{A}(|\$_k\rangle^{\otimes t})\big]\Pr\big[\mathsf{Count}(k,|\$_{k'}\rangle^{\otimes\ell})\geq t+1\big]\\ \geq&\ (1-2e^{-2p})\sum_{(k,k')\in S\wedge k\in T}\Pr\big[k\leftarrow\mathsf{QM.KeyGen}(1^\lambda)\big]\Pr\big[k'\leftarrow\mathcal{A}(|\$_k\rangle^{\otimes t})\big]\\ \geq&\ (1-2e^{-2p})\Big(\frac{1}{2p}-\mathsf{negl}(\lambda)\Big),\end{aligned}$$

which is non-negligible. The $\mathcal{B}$ therefore breaks the security of the private-key quantum money scheme. ◀

[9] Due to the relation between the fidelity and the trace distance, we have $\frac{1}{2}\||\$_k\rangle\langle\$_k|-|\$_{k'}\rangle\langle\$_{k'}|\|_1\leq\sqrt{1-|\langle\$_k|\$_{k'}\rangle|^2}$, which means that $\langle\$_k|\Pi|\$_k\rangle-\langle\$_{k'}|\Pi|\$_{k'}\rangle\leq\sqrt{1-|\langle\$_k|\$_{k'}\rangle|^2}$ for any POVM element Π.

[10] $(1+x)^r\leq 1+rx$ for any real r and x such that $0\leq r\leq 1$ and $x\geq -1$.

5.3 OWSGs from Quantum Money with Symmetric Verifiability

We consider the following restriction for quantum money.

▶ **Definition 25** (Symmetric-verifiability). *We say that a private-key quantum money scheme satisfies the symmetric-verifiability if* $\Pr[\top \leftarrow \mathsf{Ver}(k, \$_{k'})] = \Pr[\top \leftarrow \mathsf{Ver}(k', \$_k)]$ *for all* $k \neq k'$.

▶ Remark 26. For example, if all money states are pure, and $\mathsf{Ver}(\alpha, \rho)$ is the following algorithm, the symmetric-verifiability is satisfied: Measure ρ with the basis $\{|\$_\alpha\rangle\langle\$_\alpha|, I - |\$_\alpha\rangle\langle\$_\alpha|\}$. If the first result is obtained, output $\top$. Otherwise, output $\bot$.

▶ **Theorem 27.** *If private-key quantum money schemes with symmetric-verifiability exist, then OWSGs exist.*

▶ Remark 28. By using the equivalence between OWSGs and wOWSGs (Theorem 13), this result can be improved to a stronger result (with a similar proof) that private-key quantum money schemes with symmetric-verifiability and with weak security imply OWSGs. Here, the weak security means that there exists a polynomial p such that for any QPT adversary $\mathcal{A}$ and any polynomial t,

$$\Pr\left[\mathsf{Count}(k, \xi) \geq t+1 : k \leftarrow \mathsf{KeyGen}(1^\lambda), \$_k \leftarrow \mathsf{Mint}(k), \xi \leftarrow \mathcal{A}(1^\lambda, \$_k^{\otimes t})\right] \leq 1 - \frac{1}{p}.$$

The proof of Theorem 27 is similar to that of Theorem 22. For a proof, see the full version.

6 QPOTP

In this section, we first define (IND-based) QPOTP schemes (Section 6.1). We then show that QPOTP schemes imply OWSGs (Section 6.2), and that single-copy-secure QPOTP schemes imply EFI pairs (Section 6.3).

6.1 Definition of QPOTP

Quantum pseudo one-time pad schemes are defined as follows.

▶ **Definition 29** ((IND-based) quantum pseudo one-time pad (QPOTP)). *An (IND-based) quantum pseudo one-time pad (QPOTP) scheme with the key length* κ *and the plaintext length* ℓ ($\ell > \kappa$) *is a set of algorithms* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *such that*

- $\mathsf{KeyGen}(1^\lambda) \to \mathsf{sk}$: *It is a QPT algorithm that, on input the security parameter* λ, *outputs a classical secret key* $\mathsf{sk} \in \{0,1\}^\kappa$.
- $\mathsf{Enc}(\mathsf{sk}, x) \to \mathsf{ct}$: *It is a QPT algorithm that, on input* sk *and a classical plaintext message* $x \in \{0,1\}^\ell$, *outputs an* ℓn*-qubit quantum ciphertext* ct.
- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) \to x'$: *It is a QPT algorithm that, on input* sk *and* ct, *outputs* $x' \in \{0,1\}^\ell$.

We require the following correctness and security.

Correctness: *For any* $x \in \{0,1\}^\ell$, $\Pr\left[x \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) : \mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\lambda), \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, x)\right] \geq 1 - \mathsf{negl}(\lambda)$.

Security: *For any* $x_0, x_1 \in \{0,1\}^\ell$, *any QPT adversary* $\mathcal{A}$, *and any polynomial* t,

$$\begin{aligned}&|\Pr\left[1 \leftarrow \mathcal{A}(\mathsf{ct}_0^{\otimes t}) : \mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\lambda), \mathsf{ct}_0 \leftarrow \mathsf{Enc}(\mathsf{sk}, x_0)\right] \\ &- \Pr\left[1 \leftarrow \mathcal{A}(\mathsf{ct}_1^{\otimes t}) : \mathsf{sk} \leftarrow \mathsf{KeyGen}(1^\lambda), \mathsf{ct}_1 \leftarrow \mathsf{Enc}(\mathsf{sk}, x_1)\right]| \leq \mathsf{negl}(\lambda).\end{aligned}$$

▶ **Definition 30.** *We say that a QPOTP scheme is single-copy-secure if the security holds only for $t = 1$.*

▶ Remark 31. Note that the above definition of QPOTP is different from that of [3] in the following two points. First, we consider a general secret key generation QPT algorithm, while they consider uniform sampling of the secret key. Second, we consider the IND-based version of the security, while the security definition of [3] is as follows: For any $x \in \{0,1\}^\ell$, any QPT adversary $\mathcal{A}$, and any polynomial t,

$$\begin{aligned}&|\Pr[1 \leftarrow \mathcal{A}(\mathsf{ct}^{\otimes t}) : \mathsf{sk} \leftarrow \{0,1\}^\kappa, \mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{sk}, x)]\\ &- \Pr[1 \leftarrow \mathcal{A}((|\psi_1\rangle \otimes ... \otimes |\psi_\ell\rangle)^{\otimes t}) : |\psi_1\rangle, ..., |\psi_\ell\rangle \leftarrow \mu_n]| \le \mathsf{negl}(\lambda),\end{aligned}$$

where $|\psi\rangle \leftarrow \mu_n$ means the Haar random sampling of n-qubit states. It is clear that the security definition of [3] implies our IND-based security, and therefore if QPOTP schemes of [3] exist, those of Definition 29 exist. Since our results are constructions of OWSGs and EFI pairs from QPOTP, the above modification only makes our results stronger.

▶ Remark 32. QPOTP is constructed from PRSGs [3].

6.2 OWSGs from QPOTP

▶ **Theorem 33.** *If QPOTP schemes with $\kappa < \ell$ exist, then OWSGs exist.*

Proof of Theorem 33. Let $(\mathsf{OTP.KeyGen}, \mathsf{OTP.Enc}, \mathsf{OTP.Dec})$ be a QPOTP scheme with $\kappa < \ell$. From it, we construct a wOWSG as follows.[11] (From Theorem 13, it is enough for the existence of OWSGs.)

- $\mathsf{KeyGen}(1^\lambda) \to k$: Run $\mathsf{sk} \leftarrow \mathsf{OTP.KeyGen}(1^\lambda)$. Choose $x \leftarrow \{0,1\}^\ell$. Output $k := (\mathsf{sk}, x)$.
- $\mathsf{StateGen}(k) \to \phi_k$: Parse $k = (\mathsf{sk}, x)$. Run $\mathsf{ct}_{\mathsf{sk},x} \leftarrow \mathsf{OTP.Enc}(\mathsf{sk}, x)$. Output $\phi_k := \mathsf{ct}_{\mathsf{sk},x} \otimes |x\rangle\langle x|$.
- $\mathsf{Ver}(k', \phi_k) \to \top/\bot$: Parse $k' = (\mathsf{sk}', x')$. Parse $\phi_k = \mathsf{ct}_{\mathsf{sk},x} \otimes |x\rangle\langle x|$. Run $x'' \leftarrow \mathsf{OTP.Dec}(\mathsf{sk}', \mathsf{ct}_{\mathsf{sk},x})$. If $x'' = x' = x$, output $\top$. Otherwise, output $\bot$.

The correctness is clear. Let us show the security. Assume that it is not secure. It means that for any polynomial p there exist a QPT adversary $\mathcal{A}$ and a polynomial t such that

$$\Pr\left[x' = x'' = x : \begin{array}{l}\mathsf{sk} \leftarrow \mathsf{OTP.KeyGen}(1^\lambda),\\ x \leftarrow \{0,1\}^\ell,\\ \mathsf{ct}_{\mathsf{sk},x} \leftarrow \mathsf{OTP.Enc}(\mathsf{sk}, x),\\ (\mathsf{sk}', x') \leftarrow \mathcal{A}(\mathsf{ct}_{\mathsf{sk},x}^{\otimes t} \otimes |x\rangle\langle x|^{\otimes t})\\ x'' \leftarrow \mathsf{OTP.Dec}(\mathsf{sk}', \mathsf{ct}_{\mathsf{sk},x})\end{array}\right] \ge 1 - \frac{1}{p}. \tag{2}$$

From this $\mathcal{A}$, we construct a QPT adversary $\mathcal{B}$ that breaks the security of the QPOTP scheme as follows. Let $b \in \{0,1\}$ be the parameter of the following security game.

1. $\mathcal{B}$ chooses $x_0, x_1 \leftarrow \{0,1\}^\ell$, and sends them to the challenger $\mathcal{C}$.
2. $\mathcal{C}$ runs $\mathsf{sk} \leftarrow \mathsf{OTP.KeyGen}(1^\lambda)$.
3. $\mathcal{C}$ runs $\mathsf{ct}_{\mathsf{sk},x_b} \leftarrow \mathsf{OTP.Enc}(\mathsf{sk}, x_b)$ $t+1$ times.
4. $\mathcal{C}$ sends $\mathsf{ct}_{\mathsf{sk},x_b}^{\otimes t+1}$ to $\mathcal{B}$.
5. $\mathcal{B}$ runs $(\mathsf{sk}', x') \leftarrow \mathcal{A}(\mathsf{ct}_{\mathsf{sk},x_b}^{\otimes t} \otimes |x_0\rangle\langle x_0|^{\otimes t})$.
6. $\mathcal{B}$ runs $x'' \leftarrow \mathsf{OTP.Dec}(\mathsf{sk}', \mathsf{ct}_{k,x_b})$. If $x' = x'' = x_0$, $\mathcal{B}$ outputs $b' = 0$. Otherwise, it outputs $b' = 1$.

[11] A similar proof idea was given in Lemma 4.6 of [7]. However, the direct application of the proof will not work, because ciphertexts (and therefore output states of OWSGs) are quantum and the verification of "preimages" is done by the additional verification algorithm.

It is clear that $\Pr[b' = 0|b = 0]$ is equivalent to the left-hand-side of Eq. (2). On the other hand,

$$\begin{aligned}
\Pr\left[b' = 0|b = 1\right] &= \frac{1}{2^{2\ell}} \sum_{x_0, x_1, \mathsf{sk}, \mathsf{sk}'} \Pr\left[\mathsf{sk} \leftarrow \mathsf{OTP.KeyGen}(1^\lambda)\right] \Pr\left[\mathsf{sk}' \leftarrow \mathcal{A}(\mathsf{ct}_{\mathsf{sk}, x_1}^{\otimes t} \otimes |x_0\rangle\langle x_0|^{\otimes t})\right] \\
&\quad \times \Pr\left[x_0 \leftarrow \mathsf{OTP.Dec}(\mathsf{sk}', \mathsf{ct}_{\mathsf{sk}, x_1})\right] \\
&\leq \frac{1}{2^{2\ell}} \sum_{x_0, x_1, \mathsf{sk}, \mathsf{sk}'} \Pr\left[\mathsf{sk} \leftarrow \mathsf{OTP.KeyGen}(1^\lambda)\right] \Pr\left[x_0 \leftarrow \mathsf{OTP.Dec}(\mathsf{sk}', \mathsf{ct}_{\mathsf{sk}, x_1})\right] \\
&= \frac{1}{2^{2\ell}} \sum_{x_1, \mathsf{sk}, \mathsf{sk}'} \Pr\left[\mathsf{sk} \leftarrow \mathsf{OTP.KeyGen}(1^\lambda)\right] \sum_{x_0} \Pr\left[x_0 \leftarrow \mathsf{OTP.Dec}(\mathsf{sk}', \mathsf{ct}_{\mathsf{sk}, x_1})\right] \\
&= \frac{1}{2^{2\ell}} \sum_{x_1, \mathsf{sk}, \mathsf{sk}'} \Pr\left[\mathsf{sk} \leftarrow \mathsf{OTP.KeyGen}(1^\lambda)\right] = \frac{2^\kappa}{2^\ell} \leq \frac{1}{2}.
\end{aligned}$$

Therefore $|\Pr[b' = 0|b = 0] - \Pr[b' = 0|b = 1]|$ is non-negligible, which means that the $\mathcal{B}$ breaks the security of the QPOTP. ◀

6.3 EFI Pairs from Single-Copy-Secure QPOTP

▶ **Theorem 34.** *If single-copy-secure QPOTP schemes with $\kappa < \ell$ exist then EFI pairs exist.*

We prove this theorem based on a result shown by Lai and Chung [16], which gives a quantum analogue of Shannon's impossibility. Roughly speaking, they show that if a SKE scheme for n-qubit messages and κ-bit secret keys is information theoretically one-time-secure, then we must have $\kappa \geq 2n$. By a reduction to their result via a hybrid encryption of QPOTP and quantum one-time pads, we can show that any QPOTP scheme with $\kappa < \ell$ is *not* one-time-secure against unbounded-time adversaries. On the other hand, we assume that it is one-time-secure against QPT adversaries. This computationally-secure and information-theoretically-insecure encryption scheme can be directly used to construct EFI pairs. For a formal proof, see the full version.

7 SV-SI-OWSGs

In this section, we define SV-SI-OWSGs (Section 7.1), and show that SV-SI-OWSGs are equivalent to EFI pairs (Section 7.2). In Section 7.1, before defining SV-SI-OWSGs, we first define SV-OWSGs for a didactic purpose. We will point out that SV-OWSGs seem to need a more constraint so that they become equivalent to EFI. We then define SV-SI-OWSGs.

7.1 Definition of SV-SI-OWSGs

We first define secretly-verifiable OWSGs (SV-OWSGs) as follows.

▶ **Definition 35** (Secretly-verifiable OWSGs (SV-OWSGs)). *A secretly-verifiable OWSG (SV-OWSG) is a set of algorithms* $(\mathsf{KeyGen}, \mathsf{StateGen}, \mathsf{Ver})$ *as follows.*

- $\mathsf{KeyGen}(1^\lambda) \to k$: *It is a QPT algorithm that, on input the security parameter λ, outputs a key $k \in \{0,1\}^\kappa$.*
- $\mathsf{StateGen}(k) \to \phi_k$: *It is a QPT algorithm that, on input k, outputs an m-qubit state ϕ_k.*
- $\mathsf{Ver}(k', k) \to \top/\bot$: *It is a QPT algorithm that, on input k and k', outputs $\top/\bot$.*

We require the following two properties.

Correctness:

$$\Pr\left[\top \leftarrow \mathsf{Ver}(k,k) : k \leftarrow \mathsf{KeyGen}(1^\lambda)\right] \geq 1 - \mathsf{negl}(\lambda).$$

Security: *For any QPT adversary $\mathcal{A}$ and any polynomial t,*

$$\Pr\left[\top \leftarrow \mathsf{Ver}(k',k) : k \leftarrow \mathsf{KeyGen}(1^\lambda), \phi_k \leftarrow \mathsf{StateGen}(k), k' \leftarrow \mathcal{A}(\phi_k^{\otimes t})\right] \leq \mathsf{negl}(\lambda).$$

The following lemma shows that, without loss of generality, Ver can be replaced with the algorithm of just checking whether $k = k'$ or not.

▶ **Lemma 36.** *Let* $(\mathsf{KeyGen}, \mathsf{StateGen}, \mathsf{Ver})$ *be a SV-OWSG. Then, the following SV-OWSG* $(\mathsf{KeyGen}', \mathsf{StateGen}', \mathsf{Ver}')$ *exists.*

- KeyGen' *and* $\mathsf{StateGen}'$ *are the same as* KeyGen *and* $\mathsf{StateGen}$, *respectively.*
- $\mathsf{Ver}'(k', k) \to \top/\bot$ *: On input k and k', output $\top$ if $k = k'$. Otherwise, output $\bot$.*

For a proof, see the full version.

Note that statistically-secure SV-OWSGs are easy to realize. For example, consider the following construction:

- $\mathsf{KeyGen}(1^\lambda)$: Sample $k \leftarrow \{0,1\}^\lambda$.
- $\mathsf{StateGen}(k)$: Output $\frac{I^{\otimes m}}{2^m}$.
- $\mathsf{Ver}(k', k)$: Output $\top$ if $k' = k$. Otherwise, output $\bot$.

We therefore need a constraint to have a meaningful primitive. We define secretly-verifiable and statistically-invertible OWSGs (SV-SI-OWSGs) as follows. Introducing the statistical invertibility allows us to avoid trivial constructions with the statistical security.

▶ **Definition 37** (Secretly-verifiable and statistically-invertible OWSGs (SV-SI-OWSGs))**.** *A secretly-verifiable and statistically-invertible OWSG (SV-SI-OWSG) is a set of algorithms* $(\mathsf{KeyGen}, \mathsf{StateGen})$ *as follows.*

- $\mathsf{KeyGen}(1^\lambda) \to k$ *: It is a QPT algorithm that, on input the security parameter λ, outputs a key $k \in \{0,1\}^\kappa$.*
- $\mathsf{StateGen}(k) \to \phi_k$ *: It is a QPT algorithm that, on input k, outputs an m-qubit state ϕ_k.*

We require the following two properties.

Statistical invertibility: *There exists a polynomial p such that, for any k and k' $(k \neq k')$,* $\frac{1}{2}\|\phi_k - \phi_{k'}\|_1 \geq \frac{1}{p}$.

Computational non-invertibility: *For any QPT adversary $\mathcal{A}$ and any polynomial t,*

$$\Pr\left[k \leftarrow \mathcal{A}(\phi_k^{\otimes t}) : k \leftarrow \mathsf{KeyGen}(1^\lambda), \phi_k \leftarrow \mathsf{StateGen}(k)\right] \leq \mathsf{negl}(\lambda).$$

The following lemma shows that the statistical invertibility with advantage $\frac{1}{\mathrm{poly}(\lambda)}$ can be amplified to $1 - 2^{-q}$ for any polynomial q.

▶ **Lemma 38.** *If a SV-SI-OWSG exists then a SV-SI-OWSG with statistical invertibility larger than $1 - 2^{-q}$ with any polynomial q exists.*

Proof. Let $(\mathsf{KeyGen}, \mathsf{StateGen})$ be a SV-SI-OWSG with statistical invertibility larger than $\frac{1}{p}$, where p is a polynomial. From it, we construct a new SV-SI-OWSG $(\mathsf{KeyGen}', \mathsf{StateGen}')$ as follows:

- $\mathsf{KeyGen}'(1^\lambda) \to k$: Run $k \leftarrow \mathsf{KeyGen}(1^\lambda)$, and output k.
- $\mathsf{StateGen}'(k) \to \phi_k'$: Run $\phi_k \leftarrow \mathsf{StateGen}(k)$ $2pq$ times, and output $\phi_k' := \phi_k^{\otimes 2pq}$.

First, for any k and k' ($k \neq k'$),

$$\begin{aligned}\frac{1}{2}\|\phi'_k - \phi'_{k'}\|_1 &= \frac{1}{2}\|\phi_k^{\otimes 2pq} - \phi_{k'}^{\otimes 2pq}\|_1 \geq 1 - \exp(-2qp\|\phi_k - \phi_{k'}\|_1/4)\\ &\geq 1 - \exp(-q) \geq 1 - 2^{-q},\end{aligned}$$

which shows the statistical invertibility of $(\mathsf{KeyGen}', \mathsf{StateGen}')$ with the advantage larger than $1 - 2^{-q}$. Second, from the computational non-invertibility of $(\mathsf{KeyGen}, \mathsf{StateGen})$,

$$\begin{aligned}&\Pr\big[k \leftarrow \mathcal{A}(\phi_k'^{\otimes t}) : k \leftarrow \mathsf{KeyGen}'(1^\lambda), \phi'_k \leftarrow \mathsf{StateGen}'(k)\big]\\ =\ &\Pr\Big[k \leftarrow \mathcal{A}(\phi_k^{\otimes 2pqt}) : k \leftarrow \mathsf{KeyGen}(1^\lambda), \phi_k \leftarrow \mathsf{StateGen}(k)\Big] \leq \mathsf{negl}(\lambda)\end{aligned}$$

for any QPT adversary $\mathcal{A}$ and any polynomial t, which shows the computational non-invertibility of $(\mathsf{KeyGen}', \mathsf{StateGen}')$. ◀

The following lemma shows that the statistical invertibility is equivalent to the existence of a (unbounded) adversary that can find the correct k given many copies of ϕ_k except for a negligible error.

▶ **Lemma 39.** *The statistical invertibility is satisfied if and only if the following is satisfied: There exists a (not necessarily QPT) POVM measurement $\{\Pi_k\}_{k\in\{0,1\}^\kappa}$ and a polynomial t such that $Tr(\Pi_k\phi_k^{\otimes t}) \geq 1 - \mathsf{negl}(\lambda)$ and $Tr(\Pi_{k'}\phi_k^{\otimes t}) \leq \mathsf{negl}(\lambda)$ for all k and k' ($k \neq k'$).*

Proof. First, we show the if part. Assume that there exists a POVM measurement $\{\Pi_k\}_{k\in\{0,1\}^\kappa}$ and a polynomial t such that $\mathrm{Tr}(\Pi_k\phi_k^{\otimes t}) \geq 1 - \mathsf{negl}(\lambda)$ and $\mathrm{Tr}(\Pi_{k'}\phi_k^{\otimes t}) \leq \mathsf{negl}(\lambda)$ for all k and k' ($k \neq k'$). Then,

$$\begin{aligned}\frac{t}{2}\|\phi_k - \phi_{k'}\|_1 &\geq \frac{1}{2}\|\phi_k^{\otimes t} - \phi_{k'}^{\otimes t}\|_1 \geq \mathrm{Tr}\big(\Pi_k\phi_k^{\otimes t}\big) - \mathrm{Tr}\big(\Pi_k\phi_{k'}^{\otimes t}\big) \geq 1 - \mathsf{negl}(\lambda) - \mathsf{negl}(\lambda)\\ &= 1 - \mathsf{negl}(\lambda),\end{aligned}$$

which means $\frac{1}{2}\|\phi_k - \phi_{k'}\|_1 \geq \frac{1}{t} - \mathsf{negl}(\lambda) \geq \frac{1}{2t}$.

Next, we show the only if part. Assume that the statistical invertibility is satisfied. Then, there exists a polynomial p such that $\frac{1}{2}\|\phi_k - \phi_{k'}\|_1 \geq \frac{1}{p}$ for all k and k' ($k \neq k'$). Let $t := 12p\kappa$. Then,

$$\frac{1}{2}\|\phi_k^{\otimes t} - \phi_{k'}^{\otimes t}\|_1 \geq 1 - e^{-t\frac{\|\phi_k - \phi_{k'}\|_1}{4}} \geq 1 - e^{-6\kappa} \geq 1 - 2^{-6\kappa},$$

which means $F(\phi_k^{\otimes t}, \phi_{k'}^{\otimes t}) \leq 2^{-6\kappa+1}$. From Theorem 40 below,

$$\max_k(1 - \mathrm{Tr}(\mu_k\phi_k^{\otimes t})) \leq \sum_{k\neq k'}\sqrt{F(\phi_k^{\otimes t}, \phi_{k'}^{\otimes t})} \leq 2^{-3\kappa+1}(2^{2\kappa} - 2^\kappa) \leq 2^{-\kappa+1},$$

which means $\mathrm{Tr}(\mu_k\phi_k^{\otimes t}) \geq 1 - 2^{-\kappa+1}$ and $\mathrm{Tr}(\mu_{k'}\phi_k^{\otimes t}) \leq 2^{-\kappa+1}$ for any k and k' ($k' \neq k$). ◀

▶ **Theorem 40** ([17])**.** *Let $\{\rho_i\}_i$ be a set of states. Define the POVM measurement $\{\mu_i\}_i$ with $\mu_i := \Sigma^{-1/2}\rho_i\Sigma^{-1/2}$, where $\Sigma := \sum_i \rho_i$, and the inverse is taken on the support of Σ. Then, $\max_i(1 - Tr(\mu_i\rho_i)) \leq \sum_{i\neq j}\sqrt{F(\rho_i, \rho_j)}$.*

7.2 Equivalence of SV-SI-OWSGs and EFI Pairs

▶ **Theorem 41.** *SV-SI-OWSGs exist if and only if EFI pairs exist.*

This Theorem is shown by combining the following two theorems.

▶ **Theorem 42.** *If EFI pairs exist then SV-SI-OWSGs exist.*

▶ **Theorem 43.** *If SV-SI-OWSGs exist then EFI pairs exist.*

Proof of Theorem 42. We show that if EFI pairs exist then SV-SI-OWSGs exist. Let $\mathsf{EFI.StateGen}(1^\lambda,b)\to\rho_b$ be an EFI pair. As is explained in Remark 2, we can assume without loss of generality that $\frac{1}{2}\|\rho_0-\rho_1\|_1\ge 1-\mathsf{negl}(\lambda)$, which means $F(\rho_0,\rho_1)\le\mathsf{negl}(\lambda)$. From the EFI pair, we construct a SV-SI-OWSG as follows.

- $\mathsf{KeyGen}(1^\lambda)\to k$: Choose $k\leftarrow\{0,1\}^\kappa$, and output k.
- $\mathsf{StateGen}(k)\to\phi_k$: Run $\mathsf{EFI.StateGen}(1^\lambda,k_i)\to\rho_{k_i}$ for each $i\in[\kappa]$. Output $\phi_k:=\bigotimes_{i=1}^{\kappa}\rho_{k_i}$.

The statistical invertibility is easily shown as follows. If $k\neq k'$, there exists a $j\in[\kappa]$ such that $k_j\neq k'_j$. Then,

$$F(\phi_k,\phi_{k'}) \quad=\quad \prod_{i=1}^{\kappa}F(\rho_{k_i},\rho_{k'_i})\le F(\rho_{k_j},\rho_{k'_j})\le\mathsf{negl}(\lambda),$$

which means $\frac{1}{2}\|\phi_k-\phi_{k'}\|_1\ge 1-\mathsf{negl}(\lambda)$. This shows the statistical invertibility.

Let us next show the computational non-invertibility. From the standard hybrid argument, and the computational indistinguishability of ρ_0 and ρ_1, we have

$$\left|\frac{1}{2^\kappa}\sum_{k\in\{0,1\}^\kappa}\Pr\left[k\leftarrow\mathcal{A}(\phi_k^{\otimes t})\right]-\frac{1}{2^\kappa}\sum_{k\in\{0,1\}^\kappa}\Pr\left[k\leftarrow\mathcal{A}(\phi_{0^\kappa}^{\otimes t})\right]\right|\le\mathsf{negl}(\lambda) \tag{3}$$

for any QPT adversary $\mathcal{A}$ and any polynomial t. (It will be shown later.) Hence

$$\begin{aligned}&\Pr\left[k\leftarrow\mathcal{A}(\phi_k^{\otimes t}):k\leftarrow\mathsf{KeyGen}(1^\lambda),\phi_k\leftarrow\mathsf{StateGen}(k)\right]\\=&\frac{1}{2^\kappa}\sum_{k\in\{0,1\}^\kappa}\Pr\left[k\leftarrow\mathcal{A}(\phi_k^{\otimes t})\right]\le\frac{1}{2^\kappa}\sum_{k\in\{0,1\}^\kappa}\Pr\left[k\leftarrow\mathcal{A}(\phi_{0^\kappa}^{\otimes t})\right]+\mathsf{negl}(\lambda)=\frac{1}{2^\kappa}+\mathsf{negl}(\lambda),\end{aligned}$$

which shows the computational non-invertibility.

Let us show Eq. (3). For each $z\in\{0,1\}^{\kappa t}$, define $\Phi_z:=\bigotimes_{i=1}^{\kappa t}\rho_{z_i}$. Let $z,z'\in\{0,1\}^{\kappa t}$ be two bit strings such that, for a single $j\in[\kappa t]$, $z_j=0$, $z'_j=1$, and $z_i=z'_i$ for all $i\neq j$. (In other words, z and z' are the same except for the jth bit.) Then, we can show that

$$\left|\frac{1}{2^\kappa}\sum_{k\in\{0,1\}^\kappa}\Pr[k\leftarrow\mathcal{A}(\Phi_z)]-\frac{1}{2^\kappa}\sum_{k\in\{0,1\}^\kappa}\Pr[k\leftarrow\mathcal{A}(\Phi_{z'})]\right|\le\mathsf{negl}(\lambda) \tag{4}$$

for any QPT adversary $\mathcal{A}$. In fact, assume that

$$\left|\frac{1}{2^\kappa}\sum_k\Pr[k\leftarrow\mathcal{A}(\Phi_z)]-\frac{1}{2^\kappa}\sum_k\Pr[k\leftarrow\mathcal{A}(\Phi_{z'})]\right|\ge\frac{1}{\mathrm{poly}(\lambda)}$$

for a QPT adversary $\mathcal{A}$. Then, from this $\mathcal{A}$, we can construct a QPT adversary $\mathcal{B}$ that breaks the security of the EFI pair as follows: On input ρ_b, choose $k\leftarrow\{0,1\}^\kappa$, and run $k'\leftarrow\mathcal{A}((\bigotimes_{i=1}^{j-1}\rho_{z_i})\otimes\rho_b\otimes(\bigotimes_{i=j+1}^{\kappa t}\rho_{z_i}))$. If $k'=k$, output $b'=1$. If $k'\neq k$, output $b'=0$. Because

$$\Pr[b'=1|b=0]=\frac{1}{2^\kappa}\sum_k\Pr[k\leftarrow\mathcal{A}(\Phi_z)],\quad\Pr[b'=1|b=1]=\frac{1}{2^\kappa}\sum_k\Pr[k\leftarrow\mathcal{A}(\Phi_{z'})],$$

we have $|\Pr[b'=1|b=0]-\Pr[b'=1|b=1]|\ge\frac{1}{\mathrm{poly}(\lambda)}$, which means that the $\mathcal{B}$ breaks the security of the EFI pair. From the standard hybrid argument and Eq. (4), we have Eq. (3). ◀

Proof of Theorem 43. We show that if SV-SI-OWSGs exist then EFI pairs exist. Let $(\mathsf{OWSG.KeyGen}, \mathsf{OWSG.StateGen})$ be a SV-SI-OWSG. Without loss of generality, we can assume that $\mathsf{OWSG.KeyGen}$ is the following algorithm: first apply a QPT unitary U on $|0...0\rangle$ to generate $U|0...0\rangle = \sum_k \sqrt{\Pr[k \leftarrow \mathsf{OWSG.KeyGen}(1^\lambda)]}|k\rangle|\mu_k\rangle$, and trace out the second register, where $\{|\mu_k\rangle\}_k$ are some normalized states. Moreover, without loss of generality, we can also assume that $\mathsf{OWSG.StateGen}$ is the following algorithm: first apply a QPT unitary V_k that depends on k on $|0...0\rangle$ to generate $V_k|0...0\rangle = |\psi_k\rangle_{\mathbf{A},\mathbf{B}}$, and trace out the register $\mathbf{A}$.

From the SV-SI-OWSG, we want to construct an EFI pair. For that goal, we construct a statistically-hiding and computationally-binding canonical quantum bit commitment scheme from SV-SI-OWSG. Due to Theorem 8 (the equivalence between different flavors of commitments), we then have a statistically-binding and computationally-hiding canonical quantum bit commitment scheme, which is equivalent to an EFI pair. From the SV-SI-OWSG, we construct a statistically-hiding and computationally-binding canonical quantum bit commitment scheme $\{Q_0, Q_1\}$ as follows.

$$\begin{aligned} Q_0|0\rangle_{\mathbf{C},\mathbf{R}} &:= \sum_k \sqrt{\Pr[k]}(|k\rangle|\mu_k\rangle)_{\mathbf{C}_1}|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0\rangle_{\mathbf{R}_3}, \\ Q_1|0\rangle_{\mathbf{C},\mathbf{R}} &:= \sum_k \sqrt{\Pr[k]}(|k\rangle|\mu_k\rangle)_{\mathbf{C}_1}|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|k\rangle_{\mathbf{R}_3}, \end{aligned}$$

where $\Pr[k] := \Pr\big[k \leftarrow \mathsf{OWSG.KeyGen}(1^\lambda)\big]$, $\mathbf{C}_2$ is the combination of all "$\mathbf{A}$ registers" of $|\psi_k\rangle$, $\mathbf{R}_2$ is the combination of all "$\mathbf{B}$ registers" of $|\psi_k\rangle$, $\mathbf{C} := (\mathbf{C}_1, \mathbf{C}_2)$ and $\mathbf{R} := (\mathbf{R}_2, \mathbf{R}_3)$. Moreover, t is a polynomial specified later. It is clear that such $\{Q_0, Q_1\}$ is implemented in QPT in a natural way.

Let us first show the computational binding of $\{Q_0, Q_1\}$. Assume that it is not computationally binding. Then, there exists a QPT unitary U, an ancilla state $|\tau\rangle$, and a polynomial p such that $\|(\langle 0|Q_1^\dagger)_{\mathbf{C},\mathbf{R}}U_{\mathbf{R},\mathbf{Z}}(Q_0|0\rangle_{\mathbf{C},\mathbf{R}} \otimes |\tau\rangle_{\mathbf{Z}})\| \ge \frac{1}{p}$. Then,

$$\begin{aligned} \frac{1}{p^2} &\le \|(\langle 0|Q_1^\dagger)_{\mathbf{C},\mathbf{R}}U_{\mathbf{R},\mathbf{Z}}(Q_0|0\rangle_{\mathbf{C},\mathbf{R}} \otimes |\tau\rangle_{\mathbf{Z}})\|^2 \\ &= \Big\|\Big(\sum_{k'} \sqrt{\Pr[k']}\langle k', \mu_{k'}|_{\mathbf{C}_1}\langle\psi_{k'}|^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}\langle k'|_{\mathbf{R}_3}\Big) \\ &\quad \times\Big(\sum_k \sqrt{\Pr[k]}|k, \mu_k\rangle_{\mathbf{C}_1}U_{\mathbf{R},\mathbf{Z}}|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0\rangle_{\mathbf{R}_3}|\tau\rangle_{\mathbf{Z}}\Big)\Big\|^2 \\ &= \Big\|\sum_k \Pr[k]\langle\psi_k|^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}\langle k|_{\mathbf{R}_3}U_{\mathbf{R},\mathbf{Z}}|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0\rangle_{\mathbf{R}_3}|\tau\rangle_{\mathbf{Z}}\Big\|^2 \\ &\le \Big(\sum_k \Pr[k]\Big\|\langle\psi_k|^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}\langle k|_{\mathbf{R}_3}U_{\mathbf{R},\mathbf{Z}}|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0\rangle_{\mathbf{R}_3}|\tau\rangle_{\mathbf{Z}}\Big\|\Big)^2 \\ &\le \sum_k \Pr[k]\Big\|\langle\psi_k|^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}\langle k|_{\mathbf{R}_3}U_{\mathbf{R},\mathbf{Z}}|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0\rangle_{\mathbf{R}_3}|\tau\rangle_{\mathbf{Z}}\Big\|^2 \\ &\le \sum_k \Pr[k]\Big\|\langle k|_{\mathbf{R}_3}U_{\mathbf{R},\mathbf{Z}}|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0\rangle_{\mathbf{R}_3}|\tau\rangle_{\mathbf{Z}}\Big\|^2. \end{aligned} \tag{5}$$

In the third inequality, we have used Jensen's inequality.[12] From this U, we construct a QPT adversary $\mathcal{B}$ that breaks the computational non-invertibility of the SV-SI-OWSG as follows: On input the $\mathbf{R}_2$ register of $|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}$, apply $U_{\mathbf{R},\mathbf{Z}}$ on $|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0\rangle_{\mathbf{R}_3}|\tau\rangle_{\mathbf{Z}}$, and

[12] For a real convex function f, $f(\sum_i p_i x_i) \le \sum_i p_i f(x_i)$.

measure the $\mathbf{R}_3$ register in the computational basis. Output the result. Then, the probability that $\mathcal{B}$ correctly outputs k is equal to Eq. (5). Therefore, $\mathcal{B}$ breaks the computational non-invertibility of the SV-SI-OWSG.

Let us next show the statistical hiding of $\{Q_0, Q_1\}$. In the following, we construct a (not necessarily QPT) unitary $W_{\mathbf{R},\mathbf{Z}}$ such that

$$\|W_{\mathbf{R},\mathbf{Z}}Q_0|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}} - Q_1|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}}\|_1 \quad \leq \quad \mathsf{negl}(\lambda). \tag{6}$$

Then, we have

$$\begin{aligned}
& \|\mathrm{Tr}_{\mathbf{R}}(Q_0|0\rangle_{\mathbf{C},\mathbf{R}}) - \mathrm{Tr}_{\mathbf{R}}(Q_1|0\rangle_{\mathbf{C},\mathbf{R}})\|_1 = \|\mathrm{Tr}_{\mathbf{R},\mathbf{Z}}(Q_0|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}}) - \mathrm{Tr}_{\mathbf{R},\mathbf{Z}}(Q_1|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}})\|_1 \\
= \; & \|\mathrm{Tr}_{\mathbf{R},\mathbf{Z}}(W_{\mathbf{R},\mathbf{Z}}Q_0|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}}) - \mathrm{Tr}_{\mathbf{R},\mathbf{Z}}(Q_1|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}})\|_1 \\
\leq \; & \|W_{\mathbf{R},\mathbf{Z}}Q_0|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}} - Q_1|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}}\|_1 \leq \mathsf{negl}(\lambda),
\end{aligned}$$

which shows the statistical hiding of $\{Q_0, Q_1\}$.

Now we explain how to construct $W_{\mathbf{R},\mathbf{Z}}$. From Lemma 39, there exists a (not necessarily QPT) POVM measurement $\{\Pi_k\}_k$ and a polynomial t such that $\mathrm{Tr}(\Pi_k\phi_k^{\otimes t}) \geq 1 - \mathsf{negl}(\lambda)$ and $\mathrm{Tr}(\Pi_{k'}\phi_k^{\otimes t}) \leq \mathsf{negl}(\lambda)$ for all k and k' ($k \neq k'$). Let $U_{\mathbf{R}_2,\mathbf{Z}}$ be a unitary operator that implements the POVM measurement $\{\Pi_k\}_k$ in the following way

$$U_{\mathbf{R}_2,\mathbf{Z}}|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0...0\rangle_{\mathbf{Z}} \quad = \quad \sqrt{1-\epsilon_k}|k\rangle|junk_k\rangle + \sum_{k':k'\neq k}\sqrt{\epsilon_{k'}}|k'\rangle|junk_{k'}\rangle,$$

where $\mathbf{Z}$ is the ancilla register, $\{\epsilon_i\}_i$ are real numbers such that $1 - \epsilon_k \geq 1 - \mathsf{negl}(\lambda)$ and $\epsilon_{k'} \leq \mathsf{negl}(\lambda)$ for all $k' \neq k$, and $\{|junk_i\rangle\}_i$ are "junk" states that are normalized. Measuring the first register of the state realizes the POVM. Let $V_{\mathbf{R},\mathbf{Z}}$ be the following unitary:[13]

1. Apply $U_{\mathbf{R}_2,\mathbf{Z}}$ on $|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0...0\rangle_{\mathbf{Z}}|0\rangle_{\mathbf{R}_3}$:
$$U_{\mathbf{R}_2,\mathbf{Z}}|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0...0\rangle_{\mathbf{Z}}|0\rangle_{\mathbf{R}_3} \quad = \quad \left[\sqrt{1-\epsilon_k}|k\rangle|junk_k\rangle + \sum_{k':k'\neq k}\sqrt{\epsilon_{k'}}|k'\rangle|junk_{k'}\rangle\right]|0\rangle_{\mathbf{R}_3}.$$
2. Copy the content of the first register to the register $\mathbf{R}_3$:
$$\sqrt{1-\epsilon_k}|k\rangle|junk_k\rangle|k\rangle_{\mathbf{R}_3} + \sum_{k':k'\neq k}\sqrt{\epsilon_{k'}}|k'\rangle|junk_{k'}\rangle|k'\rangle_{\mathbf{R}_3}.$$

Define $W_{\mathbf{R},\mathbf{Z}} \coloneqq U^{\dagger}_{\mathbf{R}_2,\mathbf{Z}}V_{\mathbf{R},\mathbf{Z}}$.

Let us show that thus constructed $W_{\mathbf{R},\mathbf{Z}}$ satisfies Eq. (6).

$$\begin{aligned}
& \Big((\langle 0|Q_1^{\dagger})_{\mathbf{C},\mathbf{R}}\langle 0|_{\mathbf{Z}}\Big)\Big(W_{\mathbf{R},\mathbf{Z}}Q_0|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}}\Big) \\
& = \Big((\langle 0|Q_1^{\dagger})_{\mathbf{C},\mathbf{R}}\langle 0|_{\mathbf{Z}}\Big)\Big(U^{\dagger}_{\mathbf{R}_2,\mathbf{Z}}V_{\mathbf{R},\mathbf{Z}}Q_0|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}}\Big) \\
& = \Big((\langle 0|Q_1^{\dagger})_{\mathbf{C},\mathbf{R}}\langle 0|_{\mathbf{Z}}U^{\dagger}_{\mathbf{R}_2,\mathbf{Z}}\Big)\Big(V_{\mathbf{R},\mathbf{Z}}Q_0|0\rangle_{\mathbf{C},\mathbf{R}}|0\rangle_{\mathbf{Z}}\Big) \\
& = \Big(\sum_k \sqrt{\Pr[k]}(\langle k|\langle\mu_k|)_{\mathbf{C}_1}\Big[\sqrt{1-\epsilon_k}\langle k|\langle junk_k|\langle k|_{\mathbf{R}_3} + \sum_{k'\neq k}\sqrt{\epsilon_{k'}}\langle k'|\langle junk_{k'}|\langle k|_{\mathbf{R}_3}\Big]\Big) \\
& \times \Big(\sum_k \sqrt{\Pr[k]}(|k\rangle|\mu_k\rangle)_{\mathbf{C}_1}\Big[\sqrt{1-\epsilon_k}|k\rangle|junk_k\rangle|k\rangle_{\mathbf{R}_3} + \sum_{k'\neq k}\sqrt{\epsilon_{k'}}|k'\rangle|junk_{k'}\rangle|k'\rangle_{\mathbf{R}_3}\Big]\Big) \\
& = \sum_k \Pr[k](1-\epsilon_k) \geq 1 - \mathsf{negl}(\lambda).
\end{aligned}$$

◀

[13] For simplicity, we define $V_{\mathbf{R},\mathbf{Z}}$ by explaining how it acts on $|\psi_k\rangle^{\otimes t}_{\mathbf{C}_2,\mathbf{R}_2}|0...0\rangle_{\mathbf{Z}}|0\rangle_{\mathbf{R}_3}$, but it is clear from the explanation how $V_{\mathbf{R},\mathbf{Z}}$ is defined.

References

1 Scott Aaronson. Shadow tomography of quantum states. *SIAM J. Comput.*, 49(5):STOC18–368, 2019.

2 Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In Howard J. Karloff and Toniann Pitassi, editors, *44th ACM STOC*, pages 41–60. ACM Press, May 2012. doi:10.1145/2213977.2213983.

3 Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. Cryptology ePrint Archive, Paper 2021/1663, 2021. URL: https://eprint.iacr.org/2021/1663.

4 Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. Cryptology ePrint Archive, Paper 2022/1181, 2022. URL: https://eprint.iacr.org/2022/1181.

5 Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 300–315. Springer, Heidelberg, May 2000. doi:10.1007/3-540-45539-6_21.

6 Junbin Fang, Dominique Unruh, Jun Yan, and Dehua Zhou. How to base security on the perfect/statistical binding property of quantum bit commitment? Cryptology ePrint Archive, Report 2020/621, 2020. URL: https://ia.cr/2020/621.

7 Rosario Gennaro, Yael Gertner, Jonathan Katz, and Luca Trevisan. Bounds on the efficiency of generic cryptographic constructions, 2005. doi:10.1137/S0097539704443276.

8 Oded Goldreich. A note on computational indistinguishability. Information Processing Letters 34.6 (1990), pp.277–281., 1990. doi:10.1016/0020-0190(90)90010-U.

9 Oded Goldreich. *The Foundations of Cryptography - Volume 1: Basic Techniques*. Cambridge University Press, 2001. doi:10.1017/CBO9780511546891.

10 Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. From the hardness of detecting superpositions to cryptography: Quantum public key encryption and commitments. *arXiv*, 2022. arXiv:2210.05978.

11 Russell Impagliazzo. A personal view of average-case complexity. In *Proceedings of the Tenth Annual Structure in Complexity Theory Conference, Minneapolis, Minnesota, USA, June 19-22, 1995*, pages 134–147. IEEE Computer Society, 1995. doi:10.1109/SCT.1995.514853.

12 Gene Itkis, Emily Shen, Mayank Varia, David Wilson, and Arkady Yerukhimovich. Bounded-collusion attribute-based encryption from minimal assumptions. In Serge Fehr, editor, *PKC 2017, Part II*, volume 10175 of *LNCS*, pages 67–87. Springer, Heidelberg, March 2017. doi:10.1007/978-3-662-54388-7_3.

13 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. doi:10.1007/978-3-319-96878-0_5.

14 W. Kretschmer. Quantum pseudorandomness and classical complexity. *TQC 2021*, 2021. doi:10.4230/LIPICS.TQC.2021.2.

15 William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 1589–1602, New York, NY, USA, 2023. Association for Computing Machinery. doi:10.1145/3564246.3585225.

16 Ching-Yi Lai and Kai-Min Chung. Quantum encryption and generalized quantum shannon impossibility. *Designs, Codes and Cryptography volume 87, pages 1961–1972 (2019)*, 2019. doi:10.1007/s10623-018-00597-3.

17 Ashley Montanaro. Pretty simple bounds on quantum state discrimination. *arXiv*, 2019. doi:10.48550/arXiv.1908.08312.

18 Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. Cryptology ePrint Archive, Paper 2021/1691, 2021. URL: https://eprint.iacr.org/2021/1691.

19 Dominique Unruh. Computationally binding quantum commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 497–527. Springer, Heidelberg, May 2016. `doi:10.1007/978-3-662-49896-5_18`.

20 Jun Yan. General properties of quantum bit commitments. Cryptology ePrint Archive, Paper 2020/1488, 2020. URL: `https://eprint.iacr.org/2020/1488`.

21 Jun Yan. Quantum computationally predicate-binding commitments with application in quantum zero-knowledge arguments for NP. In *ASIACRYPT 2021, Part I*, LNCS, pages 575–605. Springer, Heidelberg, December 2021. `doi:10.1007/978-3-030-92062-3_20`.

22 Jun Yan, Jian Weng, Dongdai Lin, and Yujuan Quan. Quantum bit commmitment with application in quantum zero-knowledge proof (extended abstract). In Khaled M. Elbassioni and Kazuhisa Makino, editors, *ISAAC 2015*, volume 9472 of *Lecture Notes in Computer Science*, pages 555–565. Springer, 2015. `doi:10.1007/978-3-662-48971-0_47`.

23 Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *23rd FOCS*, pages 80–91. IEEE Computer Society Press, November 1982. `doi:10.1109/SFCS.1982.45`.