YITP-21-155

Quantum commitments and signatures without one-way functions

Tomoyuki Morimae[1, *] and Takashi Yamakawa[1, 2, †]
[1] *Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan*
[2] *NTT Corporation, Tokyo, Japan*

All known constructions of classical or quantum commitments require at least one-way functions. Are one-way functions really necessary for commitments? In this paper, we show that non-interactive quantum commitments (for classical messages) with computational hiding and statistical binding exist if pseudorandom quantum states exist. Pseudorandom quantum states are sets of quantum states that are efficiently generated but computationally indistinguishable from Haar random states [Z. Ji, Y.-K. Liu, and F. Song, CRYPTO 2018]. It is known that pseudorandom quantum states exist even if BQP = QMA (relative to a quantum oracle) [W. Kretschmer, TQC 2021], which means that pseudorandom quantum states can exist even if no quantum-secure classical cryptographic primitive exists. Our result therefore shows that quantum commitments can exist even if no quantum-secure classical cryptographic primitive exists. In particular, quantum commitments can exist even if no quantum-secure one-way function exists. We also show that one-time secure signatures with quantum public keys exist if pseudorandom quantum states exist. In the classical setting, the existence of signatures is equivalent to the existence of one-way functions. Our result, on the other hand, suggests that quantum signatures can exist even if no quantum-secure classical cryptographic primitive (including quantum-secure one-way functions) exists.

I. INTRODUCTION

A. Background

Commitments are one of the most central primitives in cryptography [1]. Assume that Alice (sender) wants to commit a message m to Bob (receiver). Alice encrypts it, and sends it to Bob. Later, Alice sends a key so that Bob can open the message m. Before Alice sending the key, Bob should not be able to learn the message m, which is called *hiding*. Furthermore, Alice should not be able to change the message later once she commits it, which is called *binding*. (Imagine that Alice's message is put in a safe box, and sent to Bob. Bob cannot open it until he receives the key, and Alice cannot change the message in the safe box once it is sent to Bob.) In cryptography, there are two types of definitions for security. One is statistical security and the other is computational security. Statistical security means that it is secure against any computationally-unbounded adversary, while computational security means that it is secure against adversaries restricted to polynomial-time classical/quantum computations. It is easy to see that both hiding and binding cannot be statistical at the same time in the classical setting [2], and therefore one of them has to be based on a computational assumption. In other words, in a computationally hiding commitment scheme, malicious Bob can learn the message m before the opening if his computational power is unbounded, and in a computationally binding commitment scheme, malicious Alice can change her committed message later if her computational power is unbounded. For the computational assumption, the existence of one-way functions is known to be equivalent to the existence of classical commitments [3, 4]. Intuitively, a one-way function is a function such that computing $f(x)$ is easy, but inverting it is hard [5]. The existence of one-way functions is considered the weakest assumption in classical cryptography, because virtually all complexity-based cryptographic primitives are known to imply the existence of one-way functions [6–8].

The history of quantum information has demonstrated that utilizing quantum physics in information processing achieves many advantages. In particular, it has been shown in quantum cryptography that quantum physics can weaken cryptographic assumptions. For example, if quantum states are transmitted, statistically-secure key distribution is possible [9], although it is impossible classically. Furthermore, oblivious transfer [10] is possible with only (quantum-secure) one-way functions when quantum states are transmitted [11–17]. Classically, it is known to be impossible to construct oblivious transfer from only one-way functions [18, 19].

As we have mentioned, it is classically impossible to realize commitments with statistical hiding and statistical binding. Does quantum physics overcome the barrier? Unfortunately, it is already known that both binding and hiding cannot be statistical at the same time even in the quantum world [20, 21]. In fact, all known constructions of quantum commitments require at least (quantum-secure) one-way functions [22–28].

In this paper, we ask the following fundamental question:

Are one-way functions really necessary for commitments?

[*] tomoyuki.morimae@yukawa.kyoto-u.ac.jp
[†] takashi.yamakawa.ga@hco.ntt.co.jp

It could be the case that in the quantum world commitments can be constructed from an assumption weaker than the existence of one-way functions. This possibility is mentioned in previous works [11, 12], but no construction is provided.

Digital signatures [29] are another important primitive in cryptography. In a signature scheme, a secret key sk and a public key pk are generated. The secret key sk is used to generate a signature σ for a message m, and the public key pk is used for the verification of (m,σ). Any adversary who has pk and can query the signing oracle many times cannot forge a signature σ' for a message m' which is not queried. In other words, (m',σ') is not accepted by the verification algorithm.

Obviously, statistically-secure signatures are impossible, because an unbounded adversary who can access pk and the verification algorithm can find a valid signature by a brute-force search. In the classical world, it is known that the existence of digital signatures is equivalent to the existence of one-way functions [5]. In the quantum setting, on the other hand, there is no known construction of digital signatures that imply one-way functions. Gottesman and Chuang introduced digital signatures with quantum public keys [30], but they considered information-theoretical security, and therefore the number of public keys should not be large. Our second fundamental question in this paper is the following:

Are digital signatures possible without one-way functions?

B. Our results

In this paper, we answer the above two questions affirmatively. The first result of this paper is the following:

Theorem 1. *If pseudorandom quantum states exist, then non-interactive quantum commitments (for classical messages) with computational hiding and statistical binding exist.*

Pseudorandom quantum states [31–33] are sets of quantum states that can be efficiently generated but computationally indistinguishable from Haar random states. (The formal definition is given in Definition 1.) In Ref. [34], it is shown that pseudorandom quantum states exist even if BQP = QMA relative to a quantum oracle. If BQP = QMA, no quantum-secure classical cryptographic primitive exists, because BQP = QMA means NP $\subseteq$ BQP. In particular, no quantum-secure one-way function exists. Our Theorem 1 therefore shows that quantum commitments can exist even if no quantum-secure classical cryptographic primitive exists. In particular, quantum commitments can exist even if no quantum-secure one-way function exists.

As we will see later, what we actually need is a weaker version of pseudorandom states where only the computational indistinguishability of a single copy of pseudorandom state from the Haar random state is required. (The indistinguishability has to be satisfied only for $t=1$ in Definition 1.) Because a single copy of the Haar random state is equivalent to the maximally-mixed state, what we require is the computational indistinguishability from the maximally-mixed state. It could be the case that realization of such a weaker version of pseudorandom states is easier than that of the standard pseudorandom states.

Non-interactive commitments are a special type of commitments. In general, the sender and the receiver exchange many rounds of messages during the commitment phase, but in non-interactive commitments, only a single message from the sender to the receiver is enough for the commitment. It is known that non-interactive quantum commitments (for classical messages) are possible with (quantum-secure) one-way functions [22], while it is subject to a black-box barrier in classical case [35].

As the definition of binding, we use sum-binding [36], which roughly means that $p_0+p_1\le 1$, where p_0 and p_1 are probabilities that the malicious sender makes the receiver open 0 and 1, respectively. (The formal definition of statistical sum-binding is given in Definition 4.)

Our main result, Theorem 1, that quantum commitments can be possible without one-way functions has important consequences in cryptography. It is known that quantum commitments imply the existence of quantum-secure zero-knowledge proofs (of knowledge) for all NP languages and quantum-secure oblivious transfer [37]. Thus, those primitives can also exist even if BQP = QMA (and in particular quantum-secure one-way functions do not exist) while classical constructions of them imply the existence of one-way functions. We remark that Ref. [37] only proves a game-based security for their oblivious transfer, which is weaker than the standard simulation-based security. Therefore, their oblivious transfer does not suffice for constructing general multi-party computation. Since we just plug our commitments into their construction, our result on oblivious transfer also has a similar limitation. However, we believe that we can construct oblivious transfer with the simulation-based security from quantum commitments by applying the technique of Ref. [37] to the construction of Refs. [11, 38]. If this is true, multi-party computation can also exist even if BQP = QMA. We leave a formal proof of it as an interesting future work.

We also remark that there is no known construction of pseudorandom quantum states from weaker assumptions than the existence of one-way functions without oracles. Thus, our result should be understood as a theoretical evidence that quantum commitments can exist even if BQP = QMA rather than a new concrete construction. It is an interesting open problem to construct pseudorandom quantum states from weaker assumptions than the existence of one-way functions without oracles. Such a construction immediately yields commitments (and more) by our result.

Our second result in this paper is the following:

Theorem 2. *If pseudorandom quantum states exist, then one-time secure signatures with quantum public keys* *exist.*

One-time security means that the adversary can query the signing oracle at most once. In the classical setting, it is known how to construct many-time secure signatures from one-time secure signatures [5], but we do not know how to generalize our one-time signature scheme to a many-time one, because in our case public keys are quantum. It is an important open problem to construct many-time secure signatures from pseudorandom states.

Due to the oracle separation by Ref. [34], Theorem 2 means that (at least one-time secure) signatures can exist even if no quantum-secure classical cryptographic primitive exists. In particular, (one-time secure) signatures can exist even if no quantum-secure one-way function exists.

Our construction is similar to the "quantum public key version" of the classical Lamport signature [40] by Gottesman and Chuang [30]. They consider information-theoretical security, and therefore the number of public keys should not be large. On the other hand, our construction from pseudorandom states allows unbounded polynomial number of public keys. Quantum cryptography with quantum public keys are also studied in Refs. [41, 42].

As we will see later, our construction of signatures is actually based on what we call one-wayness of quantum algorithms (Definition 5). Intuitively, we say that a quantum algorithm that outputs a quantum state $|\phi_k\rangle$ on input $k \in \{0,1\}^n$ has one-wayness if it is hard to find, given many copies of $|\phi_k\rangle$, $\sigma \in \{0,1\}^n$ such that $|\phi_\sigma\rangle$ is close to $|\phi_k\rangle$. In other words, what we actually show is the following:

Theorem 3. *If a quantum algorithm that has one-wayness exists, then one-time secure signatures with quantum public keys exist.*

We show that pseudorandom states generators have one-wayness (Lemma 3), and therefore, Theorem 2 is obtained as a corollary of Theorem 3. The concept of one-wayness itself seems to be of independent interest.

Unlike our commitment scheme, our signature scheme requires the security of pseudorandom states for unbounded polynomial number of copies ($t = poly(n)$ in Definition 1), because the number of copies decides the number of quantum public keys. In other words, pseudorandom states secure for a single copy enable commitments but those for unbounded polynomially-many copies enable signatures. There could be therefore a kind of "hierarchy" in pseudorandom states for different numbers of copies, which seems to be an interesting future research subject.

C. Concurrent work

A concurrent work also constructs commitments from pseudorandom quantum states [43]. We give comparisons between our and their results.

1. Their definition of binding is seemingly stronger than sum-binding, which we consider. However, we agree on that these definitions seem actually equivalent for commitments in a purified form like the proposed scheme in this paper [44].

2. For achieving the security level of $O(2^{-n})$ for binding, they rely on $2\log n + \omega(\log\log n)$-qubit pseudorandom quantum states that are secure against adversaries that get arbitrarily many copies of the states or $7n$-qubit pseudorandom quantum states that are secure against adversaries that get a single copy of the state where n is the key-length. On the other hand, we rely on $3n$-qubit pseudorandom quantum states that are secure against adversaries that get a single copy of the state. Thus, the required parameters are incomparable.

3. Our scheme is non-interactive whereas theirs is interactive though we believe that their scheme can also be made non-interactive by a similar technique to ours.

4. They consider a more general definition of pseudorandom quantum states than us that allows the state generation algorithm to sometimes fail. We do not take this into account since we can rely on pseudorandom quantum states of Ref. [34] whose state generation never fails for our primary goal to show that commitments can exist even if one-way functions do not exist.

Besides commitments, the result on digital signatures is unique to this paper. On the other hand, Ref. [43] contains results that are not covered in this paper such as pseudorandom function-like states and symmetric key encryption.

II. PRELIMINARIES

In this section, we provide preliminaries.

A. Basic notations

We use standard notations in quantum information. For example, I is the two-dimensional identity operator. For notational simplicity, we sometimes write a d-dimensional identity operator just I when it is clear from the context. X, Y, Z are Pauli operators. X_j means the Pauli X operator that acts on jth qubit. $\mathrm{Tr}_A(\rho_{AB})$ is the partial trace of ρ_{AB} over subsystem A. For n-bit strings $x, z \in \{0,1\}^n$, $X^x \equiv \bigotimes_{j=1}^n X_j^{x_j}$ and $Z^z \equiv \bigotimes_{j=1}^n Z_j^{z_j}$. A function f is negligible if for all constant $c > 0$, $f(\lambda) < \lambda^{-c}$ for large enough λ. QPT and PPT stand for quantum polynomial time and (classical) probabilistic polynomial time, respectively. $k \leftarrow \{0,1\}^n$ means that k is sampled from $\{0,1\}^n$ uniformly at random. For an algorithm $\mathcal{A}$, $\mathcal{A}(\xi) \to \eta$ means that the algorithm outputs η on input ξ.

B. Pseudorandom quantum states

Let us review pseudorandom quantum states [31–33]. Intuitively, pseudorandom quantum states $\{|\phi_k\rangle\}_k$ are sets of quantum states such that each state $|\phi_k\rangle$ is efficiently generated on input k, but $|\phi_k\rangle^{\otimes t}$ is computationally indistinguishable from t copies of a Haar random state. More precisely, the definition of a pseudorandom states generator is given as follows.

Definition 1 (PRS generator)**.** *A pseudorandom state (PRS) generator is a QPT algorithm* $\mathsf{StateGen}$ *that, on input* $k \in \{0,1\}^n$*, outputs an* m*-qubit quantum state* $|\phi_k\rangle$*. As the security, we require the following: for any polynomial* t *and any non-uniform QPT adversary* $\mathcal{A}$*, there exists a negligible function* negl *such that for all* n*,*

$$\left|\Pr_{k\leftarrow\{0,1\}^n}\left[\mathcal{A}(|\phi_k\rangle^{\otimes t(n)}) \to 1\right] - \Pr_{|\psi\rangle\leftarrow\mu_m}\left[\mathcal{A}(|\psi\rangle^{\otimes t(n)}) \to 1\right]\right|$$
$$\leq \mathsf{negl}(n),$$

where μ_m *is the Haar measure on* m*-qubit states.*

Note that in this paper, we assume $m \geq cn$ for a constant $c > 1$. Although it is possible to construct PRS without this restriction [33], this is satisfied in the construction of Ref. [34, 39].

It is important to remark that what we actually need for our construction of commitments is a weaker version of PRS: we need the security only for $t = 1$. In that case, the security is the computational indistinguishability of a single copy of $|\phi_k\rangle$ from the m-qubit maximally-mixed state $\frac{I^{\otimes m}}{2^m}$, because a single copy of the Haar random state is equivalent to the maximally-mixed state. It could be the case that such a weaker version of PRS is easier to realize than the general $t(n) = poly(n)$ PRS [45]. This justifies our assumption that $m \geq cn$ for $c > 1$ since there is a trivial construction of the single copy version of pseudorandom quantum states with $m = n$ without any assumption.

III. TECHNICAL OVERVIEWS

In this section, we provide technical overviews of our results.

A. Commitments

The basic idea of our construction of commitments is, in some sense, a quantum generalization of classical Naor's commitment scheme [3].

Let us recall Naor's construction. The receiver first samples uniformly random $\eta \leftarrow \{0,1\}^{3n}$, and sends it to the sender. The sender chooses a uniformly random seed $s \leftarrow \{0,1\}^n$, and sends $G(s) \oplus \eta^b$ to the receiver, where $G : \{0,1\}^n \to \{0,1\}^{3n}$ is a length-tripling pseudorandom generator, and $b \in \{0,1\}$ is the bit to commit. Hiding is clear: because the receiver does not know s, the receiver cannot distinguish $G(s)$ and $G(s) \oplus \eta$. The decommitment is (b, s). The receiver can check whether the commitment is $G(s)$ or $G(s) \oplus \eta$ from s. Binding comes from the fact that if both 0 and 1 can be opened, there exist s_0, s_1 such that $G(s_0) = G(s_1) = \eta$. There are 2^{2n} such seeds, and therefore for a random η, it is impossible except for 2^{-n} probability.

Our idea is to replace $G(s)$ with a PRS $|\phi_k\rangle$, and to replace the addition of η^b with the quantum one-time pad, which randomly applies Pauli X and Z. By the security of PRS, the committed state is computationally indistinguishable from Haar random states, which shows computational hiding. For statistical binding, we show that the fidelity between $\sum_k |\phi_k\rangle\langle\phi_k|$ and the one-time-padded version of it is small. (Intuitively, $\sum_k |\phi_k\rangle\langle\phi_k|$ has a support in at most 2^n-dimensional space, but random Pauli on it makes it the maximally-mixed m-qubit state.) A detailed explanation of our construction and its security proof are given in Sec. IV.

B. Digital Signatures

Our construction of digital signatures is a quantum public key version of the classical Lamport signature [40]. The Lamport signature scheme is constructed from a one-way function. For simplicity, let us explain the Lamport signature scheme for a single-bit message. Let f be a one-way function. The secret key is $sk \equiv (sk_0, sk_1)$, where sk_0, sk_1 are uniform randomly chosen n-bit strings. The public key is $pk \equiv (pk_0, pk_1)$, where $pk_0 \equiv f(sk_0)$ and $pk_1 \equiv f(sk_1)$. The signature σ for a message $m \in \{0,1\}$ is sk_m, and the verification is to check whether $pk_m = f(\sigma)$. Intuitively, the (one-time) security of this signature scheme comes from that of the one-way function f.

We consider the quantum public key version of it: pk is a quantum state. More precisely, we take $pk_b = |\phi_{sk_b}\rangle$ for $b \in \{0,1\}$. Intuitively, this signature scheme is one-time secure because sk_b cannot be obtained from $|\phi_{sk_b}\rangle^{\otimes t}$: If sk_b is obtained, $|\phi_{sk_b}\rangle^{\otimes t}$ can be distinguished from Haar random states, which contradict the security of PRS. We formalize this intuition as one-wayness (Definition 5), and show that PRS generators have one-wayness. For details, see Sec. V.

IV. COMMITMENTS

In this section, we provide our construction of commitments, and show its security.

A. Definition

Let us first give a formal definition of non-interactive quantum commitments.

Definition 2 (Non-interactive quantum commitments (Syntax))**.** *A non-interactive quantum commitment scheme is the following protocol.*

- **Commit phase:** *Let $b \in \{0,1\}$ be the bit to commit. The sender generates a quantum state $|\psi_b\rangle_{RC}$ on registers R and C, and sends the register C to the receiver. The states $\{|\psi_b\rangle\}_{b\in\{0,1\}}$ can be generated in quantum polynomial-time from the all zero state.*

- **Reveal phase:** *The sender sends b and the register R to the receiver. The receiver does the measurement $\{|\psi_b\rangle\langle\psi_b|, I-|\psi_b\rangle\langle\psi_b|\}$ on the registers R and C. If the result is $|\psi_b\rangle\langle\psi_b|$, the receiver outputs b. Otherwise, the receiver outputs $\perp$. Because $\{|\psi_b\rangle\}_{b\in\{0,1\}}$ can be generated in quantum polynomial-time from the all zero state, the measurement $\{|\psi_b\rangle\langle\psi_b|, I-|\psi_b\rangle\langle\psi_b|\}$ can be implemented efficiently.*

The computational hiding is defined as follows:

Definition 3 (Computational hiding)**.** *Let us consider the following security game, $\mathsf{Exp}(b)$, with the parameter $b \in \{0,1\}$ between a challenger $\mathcal{C}$ and a QPT adversary $\mathcal{A}$.*

1. *$\mathcal{C}$ generates $|\psi_b\rangle_{RC}$ and sends the register C to $\mathcal{A}$.*
2. *$\mathcal{A}$ outputs $b' \in \{0,1\}$, which is the output of the experiment.*

We say that a non-interactive quantum commitment scheme is computationally hiding if for any QPT adversary $\mathcal{A}$ there exists a negligible function negl *such that,*

$$|\Pr[\mathsf{Exp}(0)=1] - \Pr[\mathsf{Exp}(1)=1]| \le \mathsf{negl}(\lambda).$$

As the definition of binding, we consider sum-binding that is defined as follows [36]:

Definition 4 (Statistical sum-binding)**.** *Let us consider the following security game between a challenger $\mathcal{C}$ and an unbounded adversary $\mathcal{A}$:*

1. *$\mathcal{A}$ generates a quantum state $|\Psi\rangle_{ERC}$ on the three registers E, R, and C.*
2. *$\mathcal{A}$ sends the register C to $\mathcal{C}$, which is the commitment.*
3. *If $\mathcal{A}$ wants to make $\mathcal{C}$ open $b \in \{0,1\}$, $\mathcal{A}$ applies a unitary $U_{ER}^{(b)}$ on the registers E and R, and sends the register R to $\mathcal{C}$.*

Let p_b be the probability that $\mathcal{A}$ makes $\mathcal{C}$ open $b \in \{0,1\}$:

$$p_b \equiv \langle\psi_b|_{RC}\, Tr_E(U_{ER}^{(b)}|\Psi\rangle\langle\Psi|_{ERC}U_{ER}^{(b)\dagger})|\psi_b\rangle_{RC}.$$

We say that the commitment scheme is statistical sum-binding if for any unbounded $\mathcal{A}$ there exists a negligible function negl *such that*

$$p_0 + p_1 \le 1 + \mathsf{negl}(\lambda).$$

B. Construction

Let us explain our construction of signatures [46]. The commit phase is the following.

1. Let $b \in \{0,1\}$ be the bit to commit. The sender generates
$$|\psi_b\rangle \equiv \frac{1}{\sqrt{2^{2m+n}}}\sum_{x,z\in\{0,1\}^m}\sum_{k\in\{0,1\}^n}|x,z,k\rangle_R \otimes P_{x,z}^b|\phi_k\rangle_C,$$
and sends the register C to the receiver, where $P_{x,z} \equiv \bigotimes_{j=1}^m X_j^{x_j}Z_j^{z_j}$.

The reveal phase is the following.

1. The sender sends the register R and the bit b to the receiver.
2. The receiver measures the state with $\{|\psi_b\rangle\langle\psi_b|, I-|\psi_b\rangle\langle\psi_b|\}$. If the result is $|\psi_b\rangle\langle\psi_b|$, the receiver outputs b. Otherwise, the receiver outputs $\perp$. (Note that such a measurement can be done efficiently: first apply $V_b^\dagger$ such that $|\psi_b\rangle = V_b|0...0\rangle$, and then measure all qubits in the computational basis to see whether all results are zero or not.)

Note that if we slightly modify the above construction, the communication in the reveal phase can be classical. In fact, we can show it for general settings. In general quantum commitments (Definition 2), the sender who wants to commit $b \in \{0,1\}$ generates a certain state $|\psi_b\rangle_{RC}$ on the registers R and C, and sends the register C to the receiver, which is the commit phase. In the reveal phase, b and the register R is sent to the receiver. The receiver runs the verification algorithm on the registers R and C. Let us modify it as follows. In the commit phase, the sender chooses uniform random $x,z \leftarrow \{0,1\}^{|R|}$ and applies $\bigotimes_{j=1}^{|R|}X_j^{x_j}Z_j^{z_j}$ on the register R of $|\psi_b\rangle_{RC}$, where $|R|$ is the number of qubits in the register R. The sender then sends both the registers R and C to the receiver. It ends the commit phase. In the reveal phase, the sender sends the bit b to open and (x,z) to the receiver. The receiver applies $\bigotimes_{j=1}^{|R|}X_j^{x_j}Z_j^{z_j}$ on the register R and runs the original verification algorithm. Hiding is clear because the register R is traced out for the receiver before the reveal phase. Binding is also easy to understand: Assume a malicious sender of the modified scheme can break binding. Then, we can construct a malicious sender that breaks binding of the original scheme, because the malicious sender of the original scheme can simulate the malicious sender of the modified scheme.

We also note that our construction of commitments can be extended to more general cases where ancilla qubits are used in PRS. Let us consider a more general PRS generator, $\mathsf{StateGen}(k) \to |\phi_k\rangle \otimes |\eta_k\rangle$, where $|\eta_k\rangle$ is an ancilla. In that case, hiding and binding holds if we replace $|\psi_b\rangle$ with

$$\frac{1}{\sqrt{2^{2m+n}}} \sum_{x,z\in\{0,1\}^m} \sum_{k\in\{0,1\}^n} (|x,z,k\rangle \otimes |\eta_k\rangle)_R \otimes P^b_{x,z}|\phi_k\rangle_C.$$

C. Computational hiding

We show computational hiding of our construction.

Theorem 4 (Computational hiding). *Our construction satisfies computational hiding.*

Proof of Theorem 4. Let us consider the following security game, $\mathsf{Hyb}_0(b)$, which is the same as the original experiment.

1. The challenger $\mathcal{C}$ generates

$$|\psi_b\rangle = \frac{1}{\sqrt{2^{2m+n}}} \sum_{x,z\in\{0,1\}^m} \sum_{k\in\{0,1\}^n} |x,z,k\rangle_R \otimes P^b_{x,z}|\phi_k\rangle_C,$$

   and sends the register C to the adversary $\mathcal{A}$, where $P_{x,z} = \bigotimes_{j=1}^m X_j^{x_j} Z_j^{z_j}$.

2. $\mathcal{A}$ outputs $b' \in \{0,1\}$, which is the output of this hybrid.

Let us define $\mathsf{Hyb}_1(b)$ as follows:

1. If $b = 0$, $\mathcal{C}$ chooses a Haar random m-qubit state $|\psi\rangle \leftarrow \mu_m$, and sends it to $\mathcal{A}$. If $b = 1$, $\mathcal{C}$ generates $|\psi_1\rangle_{RC}$ and sends the register C to $\mathcal{A}$.
2. $\mathcal{A}$ outputs $b' \in \{0,1\}$, which is the output of this hybrid.

Lemma 1.

$$|\Pr[\mathsf{Hyb}_0(b) = 1] - \Pr[\mathsf{Hyb}_1(b) = 1]| \le \mathsf{negl}(\lambda)$$

for each $b \in \{0,1\}$.

Proof of Lemma 1. It is clear that

$$\Pr[\mathsf{Hyb}_0(1) = 1] = \Pr[\mathsf{Hyb}_1(1) = 1].$$

Let us show

$$|\Pr[\mathsf{Hyb}_0(0) = 1] - \Pr[\mathsf{Hyb}_1(0) = 1]| \le \mathsf{negl}(\lambda).$$

To show it, assume that

$$|\Pr[\mathsf{Hyb}_0(0) = 1] - \Pr[\mathsf{Hyb}_1(0) = 1]|$$

is non-negligible. Then, we can construct an adversary $\mathcal{A}'$ that breaks the security of PRS as follows. Let $b'' \in \{0,1\}$ be the parameter of the security game of PRS.

1. The challenger $\mathcal{C}'$ of the security game of PRS sends $\mathcal{A}'$ the state $|\phi_k\rangle$ with uniform random k if $b'' = 0$ and a Haar random state $|\psi\rangle \leftarrow \mu_m$ if $b'' = 1$.
2. $\mathcal{A}'$ sends the received state to $\mathcal{A}$.
3. $\mathcal{A}'$ outputs the output of $\mathcal{A}$.

If $b'' = 0$, it simulates $\mathsf{Hyb}_0(0)$. If $b'' = 1$, it simulates $\mathsf{Hyb}_1(0)$. Therefore, $\mathcal{A}'$ breaks the security of the PRS. □

Let us define $\mathsf{Hyb}_2(b)$ as follows:

1. The challenger $\mathcal{C}$ chooses a Haar random m-qubit state $|\psi\rangle \leftarrow \mu_m$, and sends it to the adversary.
2. The adversary outputs $b' \in \{0,1\}$, which is the output of this hybrid.

Lemma 2.

$$|\Pr[\mathsf{Hyb}_1(b) = 1] - \Pr[\mathsf{Hyb}_2(b) = 1]| \le \mathsf{negl}(\lambda)$$

for each $b \in \{0,1\}$.

Proof of Lemma 2.

$$\Pr[\mathsf{Hyb}_1(0) = 1] = \Pr[\mathsf{Hyb}_2(0) = 1]$$

is clear. Let us show

$$|\Pr[\mathsf{Hyb}_1(1) = 1] - \Pr[\mathsf{Hyb}_2(1) = 1]| \le \mathsf{negl}(\lambda).$$

To show it, assume that

$$|\Pr[\mathsf{Hyb}_1(1) = 1] - \Pr[\mathsf{Hyb}_2(1) = 1]|$$

is non-negligible. Then, we can construct an adversary $\mathcal{A}'$ that breaks the security of PRS as follows. Let $b'' \in \{0,1\}$ be the parameter of the security game of PRS.

1. The challenger $\mathcal{C}'$ of the security game of PRS sends $\mathcal{A}'$ the state $|\phi_k\rangle$ with uniform random k if $b'' = 0$ and a Haar random state $|\psi\rangle \leftarrow \mu_m$ if $b'' = 1$.
2. $\mathcal{A}'$ applies $X^x Z^z$ with uniform random $x, z \leftarrow \{0,1\}^m$, and sends the state to $\mathcal{A}$.
3. $\mathcal{A}'$ outputs the output of $\mathcal{A}$.

If $b'' = 0$, it simulates $\mathsf{Hyb}_1(1)$. If $b'' = 1$, it simulates $\mathsf{Hyb}_2(1)$. Therefore, $\mathcal{A}'$ breaks the security of the PRS. □

It is obvious that

$$\Pr[\mathsf{Hyb}_2(0) = 1] = \Pr[\mathsf{Hyb}_2(1) = 1].$$

Therefore, from Lemma 1 and Lemma 2, we conclude

$$|\Pr[\mathsf{Hyb}_0(0) = 1] - \Pr[\mathsf{Hyb}_0(1) = 1]| \le \mathsf{negl}(\lambda),$$

which shows Theorem 4. □

D. Statistical binding

Let us show that our construction satisfies statistical sum-binding.

Theorem 5 (Statistical sum-binding)**.** *Our construction satisfies statistical sum-binding.*

Proof of Theorem 5. Let

$$F(\rho,\sigma) := \Big(\mathrm{Tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\Big)^2$$

be the fidelity between two states ρ and σ. Then we have

$$\begin{aligned} p_b &= \langle\psi_b|_{RC}\mathrm{Tr}_E(U_{ER}^{(b)}|\Psi\rangle\langle\Psi|_{ERC}U_{ER}^{(b)\dagger})|\psi_b\rangle_{RC} \\ &= F\Big(|\psi_b\rangle_{RC}, \mathrm{Tr}_E(U_{ER}^{(b)}|\Psi\rangle\langle\Psi|_{ERC}U_{ER}^{(b)\dagger})\Big) \\ &\le F\Big(\mathrm{Tr}_R(|\psi_b\rangle\langle\psi_b|_{RC}), \mathrm{Tr}_{RE}(U_{ER}^{(b)}|\Psi\rangle\langle\Psi|_{ERC}U_{ER}^{(b)\dagger})\Big) \\ &= F\Big(\mathrm{Tr}_R(|\psi_b\rangle\langle\psi_b|_{RC}), \mathrm{Tr}_{RE}(|\Psi\rangle\langle\Psi|_{ERC})\Big). \end{aligned}$$

Here, we have used the facts that if $\sigma = |\sigma\rangle\langle\sigma|$, $F(\rho,\sigma) = \langle\sigma|\rho|\sigma\rangle$, and that for any bipartite states ρ_{AB}, σ_{AB}, $F(\rho_{AB},\sigma_{AB}) \le F(\rho_A,\sigma_A)$, where $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ and $\sigma_A = \mathrm{Tr}_B(\sigma_{AB})$ [47].

Therefore,

$$\begin{aligned} p_0 + p_1 &\le 1 + \sqrt{F\Big(\mathrm{Tr}_R(|\psi_0\rangle\langle\psi_0|_{RC}), \mathrm{Tr}_R(|\psi_1\rangle\langle\psi_1|_{RC})\Big)} \\ &= 1 + \sqrt{F\Big(\frac{1}{2^n}\sum_k |\phi_k\rangle\langle\phi_k|, \frac{1}{2^{2m}}\frac{1}{2^n}\sum_{x,z}\sum_k X^xZ^z|\phi_k\rangle\langle\phi_k|X^xZ^z\Big)} \\ &= 1 + \sqrt{F\Big(\frac{1}{2^n}\sum_k |\phi_k\rangle\langle\phi_k|, \frac{I^{\otimes m}}{2^m}\Big)} \\ &= 1 + \Big\|\sum_{i=1}^{\xi}\sqrt{\lambda_i}\frac{1}{\sqrt{2^m}}|\lambda_i\rangle\langle\lambda_i|\Big\|_1 \\ &= 1 + \sum_{i=1}^{\xi}\sqrt{\lambda_i}\frac{1}{\sqrt{2^m}} \\ &\le 1 + \sqrt{\sum_{i=1}^{\xi}\lambda_i}\sqrt{\sum_{i=1}^{\xi}\frac{1}{2^m}} \\ &\le 1 + \sqrt{\frac{2^n}{2^m}} \\ &\le 1 + \frac{1}{\sqrt{2^{(c-1)n}}}. \end{aligned}$$

In the first inequality, we have used the fact that for any states ρ, σ, ξ,

$$F(\rho,\xi) + F(\sigma,\xi) \le 1 + \sqrt{F(\rho,\sigma)}$$

is satisfied [48]. In the fourth equality, $\sum_{i=1}^{\xi}\lambda_i|\lambda_i\rangle\langle\lambda_i|$ is the diagonalization of $\frac{1}{2^n}\sum_k|\phi_k\rangle\langle\phi_k|$. In the sixth inequality, we have used Cauchy–Schwarz inequality. In the seventh inequality, we have used $\xi \le 2^n$. In the last inequality, we have used $m \ge cn$ for a constant $c > 1$. □

V. DIGITAL SIGNATURES

In this section, we provide our construction of digital signatures and show its security. For that goal, we first define the concept of one-wayness (Definition 5), and show that PRS generators satisfy one-wayness (Lemma 3).

A. One-wayness

For the construction of our signature scheme, we use one-wayness, which is defined as follows:

Definition 5 (One-wayness)**.** *Let G is a QPT algorithm that, on input $k \in \{0,1\}^n$, outputs a quantum state $|\phi_k\rangle$. Let us consider the following security game,* Exp*, between a challenger $\mathcal{C}$ and a QPT adversary $\mathcal{A}$:*

1. *$\mathcal{C}$ chooses $k \leftarrow \{0,1\}^n$.*
2. *$\mathcal{C}$ runs $|\phi_k\rangle \leftarrow G(k)$ $t+1$ times.*
3. *$\mathcal{C}$ sends $|\phi_k\rangle^{\otimes t}$ to $\mathcal{A}$.*

4. *$\mathcal{A}$ sends $\sigma \in \{0,1\}^n$ to $\mathcal{C}$.*

5. *$\mathcal{C}$ measures $|\phi_k\rangle$ with $\{|\phi_\sigma\rangle\langle\phi_\sigma|, I - |\phi_\sigma\rangle\langle\phi_\sigma|\}$. If the result is $|\phi_\sigma\rangle\langle\phi_\sigma|$, the output of the experiment is 1. Otherwise, the output of the experiment is 0.*

We say that G satisfies one-wayness if for any $t = poly(n)$ and for any QPT adversary $\mathcal{A}$ there exists a negligible function negl *such that*

$$\Pr[\mathsf{Exp} = 1] \le \mathsf{negl}(n).$$

Note that another natural definition of one-wayness is that given $|\phi_k\rangle^{\otimes t}$ it is hard to find k. However, as we will see later, it is not useful for our construction of signatures.

We can show the one-wayness for PRS generators:

Lemma 3 (One-wayness of PRS generators)**.** *A PRS generator,* $\mathsf{StateGen}$*, satisfies the one-wayness.*

Proof of Lemma 3. Assume that $\Pr[\mathsf{Exp} = 1]$ of the security game of Definition 5 with $G = \mathsf{StateGen}$ is non-negligible. Then we can construct an adversary $\mathcal{A}'$ that breaks the security of PRS as follows. Let $b' \in \{0,1\}$ be the parameter of the security game for PRS.

1. If $b' = 0$, the challenger $\mathcal{C}'$ of the security game for PRS chooses $k \leftarrow \{0,1\}^n$, runs $|\phi_k\rangle \leftarrow \mathsf{StateGen}(k)$ $t+1$ times, and sends $|\phi_k\rangle^{\otimes t+1}$ to $\mathcal{A}'$. If $b' = 1$, the challenger $\mathcal{C}'$ of the security game for PRS sends $t+1$ copies of Haar random state $|\psi\rangle^{\otimes t+1}$ to $\mathcal{A}'$. In other words, $\mathcal{A}'$ receives $\rho^{\otimes t+1}$, where $\rho = |\phi_k\rangle$ if $b' = 0$ and $\rho = |\psi\rangle$ if $b' = 1$.

2. $\mathcal{A}'$ sends $\rho^{\otimes t}$ to $\mathcal{A}$.

3. $\mathcal{A}$ outputs $\sigma \in \{0,1\}^n$.

4. $\mathcal{A}'$ measures ρ with $\{|\phi_\sigma\rangle\langle\phi_\sigma|, I - |\phi_\sigma\rangle\langle\phi_\sigma|\}$. If the result is $|\phi_\sigma\rangle\langle\phi_\sigma|$, $\mathcal{A}'$ outputs 1. Otherwise, $\mathcal{A}'$ outputs 0.

It is clear that

$$\Pr[\mathcal{A}' \to 1 | b' = 0] = \Pr[\mathsf{Exp} = 1].$$

By assumption, $\Pr[\mathsf{Exp} = 1]$ is non-negligible, and therefore $\Pr[\mathcal{A}' \to 1 | b' = 0]$ is also non-negligible. On the other hand,

$$\begin{aligned}
&\Pr[\mathcal{A}' \to 1 | b' = 1] \\
&= \int d\mu(\psi) \Big[\sum_{\sigma \in \{0,1\}^n} \Pr[\sigma \leftarrow \mathcal{A}(|\psi\rangle^{\otimes t})] |\langle\phi_\sigma|\psi\rangle|^2 \Big] \\
&\le \int d\mu(\psi) \Big[\sum_{\sigma \in \{0,1\}^n} |\langle\phi_\sigma|\psi\rangle|^2 \Big] \\
&= \sum_{\sigma \in \{0,1\}^n} \langle\phi_\sigma| \Big[\int d\mu(\psi) |\psi\rangle\langle\psi| \Big] |\phi_\sigma\rangle \\
&= \sum_{\sigma \in \{0,1\}^n} \langle\phi_\sigma| \frac{I^{\otimes m}}{2^m} |\phi_\sigma\rangle \\
&\le \frac{2^n}{2^m} \\
&\le \frac{1}{2^{(c-1)n}}.
\end{aligned}$$

Therefore, $\mathcal{A}'$ breaks the security of PRS. □

B. Definition of digital signatures with quantum public keys

We also have to formally define digital signatures with quantum public keys:

Definition 6 (Digital signatures with quantum public keys (Syntax))**.** *A signature scheme with quantum public keys is the set of algorithms* $(\mathsf{Gen}_1, \mathsf{Gen}_2, \mathsf{Sign}, \mathsf{Verify})$ *such that*

- $\mathsf{Gen}_1(1^\lambda)$*: It is a classical PPT algorithm that, on input the security parameter 1^λ, outputs a classical secret key sk.*
- $\mathsf{Gen}_2(sk)$*: It is a QPT algorithm that, on input the secret key sk, outputs a quantum public key pk.*
- $\mathsf{Sign}(sk, m)$*: It is a classical deterministic polynomial-time algorithm that, on input the secret key sk and a message m, outputs a classical signature σ.*
- $\mathsf{Verify}(pk, m, \sigma)$*: It is a QPT algorithm that, on input a public key pk, the message m, and the signature σ, outputs $\top/\bot$.*

The one-time security is defined as follows:

Definition 7 (One-time security of digital signatures with quantum public keys)**.** *Let us consider the following security game,* Exp*, between a challenger $\mathcal{C}$ and a QPT adversary $\mathcal{A}$:*

1. *$\mathcal{C}$ runs $sk \leftarrow \mathsf{Gen}_1(1^\lambda)$.*
2. *$\mathcal{A}$ can query $pk \leftarrow \mathsf{Gen}_2(sk)$ $poly(\lambda)$ times.*
3. *$\mathcal{A}$ sends a message m to $\mathcal{C}$.*

4. *$\mathcal{C}$ runs $\sigma \leftarrow \mathsf{Sign}(sk, m)$, and sends σ to $\mathcal{A}$.*

5. *$\mathcal{A}$ sends σ' and m' to $\mathcal{C}$.*

6. *$\mathcal{C}$ runs $v \leftarrow \mathsf{Verify}(pk, m', \sigma')$. If $m' \neq m$ and $v = \top$, $\mathcal{C}$ outputs 1. Otherwise, $\mathcal{C}$ outputs 0. This $\mathcal{C}$'s output is the output of the game.*

A signature scheme with quantum public keys is one-time secure if for any QPT adversary $\mathcal{A}$ there exists a negligible function negl *such that*

$$\Pr[\mathsf{Exp} = 1] \leq \mathsf{negl}(\lambda).$$

C. Construction

Let G be a quantum algorithm with one-wayness. Our construction of a one-time secure signature scheme with quantum public keys is as follows. (For simplicity, we consider the case when the message space is $\{0,1\}$.)

- $\mathsf{Gen}_1(1^n)$: Choose $k_0, k_1 \leftarrow \{0,1\}^n$. Output $sk \equiv (sk_0, sk_1)$, where $sk_b \equiv k_b$ for $b \in \{0,1\}$.
- $\mathsf{Gen}_2(sk)$: Run $|\phi_{k_b}\rangle \leftarrow G(k_b)$ for $b \in \{0,1\}$. Output $pk \equiv (pk_0, pk_1)$, where $pk_b \equiv |\phi_{k_b}\rangle$ for $b \in \{0,1\}$.
- $\mathsf{Sign}(sk, m)$: Output $\sigma \equiv sk_m$.
- $\mathsf{Verify}(pk, m, \sigma)$: Measure pk_m with $\{|\phi_\sigma\rangle\langle\phi_\sigma|, I - |\phi_\sigma\rangle\langle\phi_\sigma|\}$, and output $\top$ if the result is $|\phi_\sigma\rangle\langle\phi_\sigma|$. Otherwise, output $\bot$.

D. Security

Let us show the security of our construction.

Theorem 6. *Our construction of a signature scheme is one-time secure.*

Proof of Theorem 6. Let us consider the following security game, Exp, between the challenger $\mathcal{C}$ and a QPT adversary $\mathcal{A}$:

1. $\mathcal{C}$ chooses $k_0, k_1 \leftarrow \{0,1\}^n$.
2. $\mathcal{A}$ can query $|\phi_{k_b}\rangle \leftarrow G(k_b)$ $poly(n)$ times for $b \in \{0,1\}$.
3. $\mathcal{A}$ sends m to $\mathcal{C}$.
4. $\mathcal{C}$ sends k_m to $\mathcal{A}$.
5. $\mathcal{A}$ sends σ to $\mathcal{C}$.
6. $\mathcal{C}$ measures $|\phi_{k_{m\oplus 1}}\rangle$ with $\{|\phi_\sigma\rangle\langle\phi_\sigma|, I - |\phi_\sigma\rangle\langle\phi_\sigma|\}$. If the result is $|\phi_\sigma\rangle\langle\phi_\sigma|$, $\mathcal{C}$ outputs 1. Otherwise, $\mathcal{C}$ outputs 0. This $\mathcal{C}$'s output is the output of the game.

Assume that our construction is not one-time secure, which means that $\Pr[\mathsf{Exp} = 1]$ is non-negligible for an adversary $\mathcal{A}$ who queries both $\mathsf{Gen}_2(sk_0)$ and $\mathsf{Gen}_2(sk_1)$ $s = poly(n)$ times. (Without loss of generality, we can assume that the numbers of $\mathcal{A}$'s queries to $\mathsf{Gen}_2(sk_0)$ and $\mathsf{Gen}_2(sk_1)$ are the same. An adversary who queries to $\mathsf{Gen}_2(sk_0)$ s_0 times and to $\mathsf{Gen}_2(sk_1)$ s_1 times can be simulated by another adversary who queries to both $\mathsf{Gen}_2(sk_0)$ and $\mathsf{Gen}_2(sk_1)$ $s \equiv \max(s_0, s_1)$ times.) Then, we can construct an adversary that breaks the one-wayness of PRS as follows. Let $\mathcal{C}'$ and $\mathcal{A}'$ be the challenger and the adversary of the security game for the one-wayness of PRS, respectively.

1. $\mathcal{C}'$ chooses $k \leftarrow \{0,1\}^n$. $\mathcal{C}'$ runs $|\phi_k\rangle \leftarrow G(k)$ $s+1$ times. $\mathcal{C}'$ sends $|\phi_k\rangle^{\otimes s}$ to $\mathcal{A}'$.
2. $\mathcal{A}'$ chooses $r \leftarrow \{0,1\}$. $\mathcal{A}'$ chooses $k' \leftarrow \{0,1\}^n$. $\mathcal{A}'$ runs $|\phi_{k'}\rangle \leftarrow G(k')$ s times. If $r = 0$, $\mathcal{A}'$ returns $(|\phi_k\rangle^{\otimes s}, |\phi_{k'}\rangle^{\otimes s})$ to the query of $\mathcal{A}$. If $r = 1$, $\mathcal{A}'$ returns $(|\phi_{k'}\rangle^{\otimes s}, |\phi_k\rangle^{\otimes s})$ to the query of $\mathcal{A}$.
3. $\mathcal{A}$ sends $m \in \{0,1\}$ to $\mathcal{A}'$.
4. If $r = m$, $\mathcal{A}'$ aborts. If $r \neq m$, $\mathcal{A}'$ sends k' to $\mathcal{A}$.
5. $\mathcal{A}$ sends σ to $\mathcal{A}'$.
6. $\mathcal{A}'$ sends σ to $\mathcal{C}'$.
7. $\mathcal{C}'$ measures $|\phi_k\rangle$ with $\{|\phi_\sigma\rangle\langle\phi_\sigma|, I - |\phi_\sigma\rangle\langle\phi_\sigma|\}$. If the result is $|\phi_\sigma\rangle\langle\phi_\sigma|$, $\mathcal{C}'$ outputs 1. Otherwise, $\mathcal{C}'$ outputs 0.

By a streightforward calculation, which is given below,

$$\Pr[\mathcal{C}' \to 1] = \frac{1}{2}\Pr[\mathsf{Exp} = 1]. \tag{1}$$

Therefore, if $\Pr[\mathsf{Exp} = 1]$ is non-negligible, $\Pr[\mathcal{C}' \to 1]$ is also non-negligible, which means that $\mathcal{A}'$ breaks the one-wayness of PRS.

Let us show Eq. (1). In fact,

$$
\begin{aligned}
\Pr[\mathcal{C}' \to 1] &= \frac{1}{2^{2n}} \sum_{k,k' \in \{0,1\}^n} \frac{1}{2} \Pr[1 \leftarrow \mathcal{A}(|\phi_k\rangle^{\otimes s}, |\phi_{k'}\rangle^{\otimes s})] \Pr[\sigma \leftarrow \mathcal{A}(k')] |\langle \phi_\sigma | \phi_k \rangle|^2 \\
&\quad + \frac{1}{2^{2n}} \sum_{k,k' \in \{0,1\}^n} \frac{1}{2} \Pr[0 \leftarrow \mathcal{A}(|\phi_{k'}\rangle^{\otimes s}, |\phi_k\rangle^{\otimes s})] \Pr[\sigma \leftarrow \mathcal{A}(k')] |\langle \phi_\sigma | \phi_k \rangle|^2 \\
&= \frac{1}{2^{2n}} \sum_{k,k' \in \{0,1\}^n} \frac{1}{2} \Pr[1 \leftarrow \mathcal{A}(|\phi_k\rangle^{\otimes s}, |\phi_{k'}\rangle^{\otimes s})] \Pr[\sigma \leftarrow \mathcal{A}(k')] |\langle \phi_\sigma | \phi_k \rangle|^2 \\
&\quad + \frac{1}{2^{2n}} \sum_{k,k' \in \{0,1\}^n} \frac{1}{2} \Pr[0 \leftarrow \mathcal{A}(|\phi_k\rangle^{\otimes s}, |\phi_{k'}\rangle^{\otimes s})] \Pr[\sigma \leftarrow \mathcal{A}(k)] |\langle \phi_\sigma | \phi_{k'} \rangle|^2 \\
&= \frac{1}{2} \Pr[\mathsf{Exp} = 1].
\end{aligned}
$$

□

E. Remark

For simplicity, we have considered the case when there is no ancilla qubits in the output of PRS generators. We note that the same results hold for more general cases when the output contains ancilla qubits.

First, let us consider the definition of one-wayness (Definition 5). Let G be a QPT algorithm such that, on input $k \in \{0,1\}^n$, it outputs a classical description of a unitary U_k, and applies a unitary U_k on $|0...0\rangle$ to generate $U_k|0...0\rangle = |\phi_k\rangle \otimes |\eta_k\rangle$, where $|\eta_k\rangle$ is an ancilla state and $|\phi_k\rangle$ is the main output of G. We modify the final verification of $\mathcal{C}$ in Definition 5 as follows: Given σ, $\mathcal{C}$ generates $U_\sigma|0...0\rangle = |\phi_\sigma\rangle \otimes |\eta_\sigma\rangle$. $\mathcal{C}$ then runs $U_\sigma^\dagger$ on $|\phi_k\rangle \otimes |\eta_\sigma\rangle$, and measures all qubits in the computational basis. If all results are zero, the output of the experiment is 1. Otherwise, it is 0. (This verification is actually the one explained in Ref. [43].)

It is easy to verify that the one-wayness of PRS generators (Lemma 3) holds for a PRS generator that, on input $k \in \{0,1\}^n$, outputs a classical description of a unitary U_k, and applies U_k on $|0...0\rangle$ to generate $U_k|0...0\rangle = |\phi_k\rangle \otimes |\eta_k\rangle$, where $|\phi_k\rangle$ works as a PRS and $|\eta_k\rangle$ is an ancilla state.

The verification algorithm in our construction of digital signatures is also modified as follows: Given σ, first generate $U_\sigma|0...0\rangle = |\phi_\sigma\rangle \otimes |\eta_\sigma\rangle$. Then run $U_\sigma^\dagger$ on $pk_m \otimes |\eta_\sigma\rangle$, and measures all qubits in the computational basis. If all results are zero, output $\top$. Otherwise, output $\bot$. It is easy to check that a similar proof holds for the security of our construction.

ACKNOWLEDGMENTS

We thank W. Kretschmer and Y. Nakata for answering our questions. We thank P. Ananth, L. Qian, and H. Yuen for comments on our paper. TM is supported by the JST Moonshot R&D JPMJMS2061-5-1-1, JST FOREST, MEXT Q-LEAP, the Grant-in-Aid for Scientific Research (B) No.JP19H04066, and the Grant-in-Aid for Transformative Research Areas (A) No.JP21H05183.

[1] M. Blum, Coin flipping by telephone. In Allen Gersho, editor, Advances in Cryptology: A Report on CRYPTO 81, CRYPTO 81, IEEE Workshop on Communications Security, Santa Barbara, California, USA, August 24-26, 1981, pages 11–15. U. C. Santa Barbara, Dept. of Elec. and Computer Eng., ECE Report No 82-04, 1981.

[2] If a commitment scheme is statistically binding, there exists at most one message to which a commitment can be opened except for negligible probability. This unique message can be found by a brute-force search, which means that the scheme is not statistically hiding.

[3] M. Naor, Bit commitment using pseudorandomness. Journal of cryptology, pages 151–158, 1991.

[4] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, A Pseudorandom Generator from any One-way Function. SIAM J. Comput. **28**(4) pages 1364-1396, 1999.

[5] O. Goldreich, Foundations of Cryptography. Cambridge University Press. 2004.

[6] M. Luby and C. Rackoff, Pseudo-random permutation generators and cryptographic composition. In 18th ACM STOC, pages 356–363. ACM Press, May 1986.

[7] R. Impagliazzo and M. Luby, One-way functions are essential for complexity based cryptography (extended abstract). In 30th FOCS, pages 230–235. IEEE Computer Society Press, October / November 1989.

[8] R. Impagliazzo, L. A. Levin, and M. Luby, Pseudo-random generation from one-way functions (extended abstracts). In 21st ACM STOC, pages 12–24. ACM Press, May 1989.

[9] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing. In IEEE International Conference on Computers Systems and Signal Processing, pages 175–179. IEEE, 1984.

[10] Oblivious transfer is the following task: Alice has two messages m_0, m_1. Bob can learn one of them, but he cannot learn the other. Alice cannot learn which message Bob learns.

[11] J. Bartusek, A. Coladangelo, D. Khurana, and F. Ma, One-way functions imply secure computation in a quantum world. In Tal Malkin and Chris Peikert, editors, CRYPTO 2021, Part I, volume 12825 of LNCS, pages 467–496, Virtual Event, August 2021. Springer, Heidelberg.

[12] A. B. Grilo, H. Lin, F. Song, and V. Vaikuntanathan, Oblivious Transfer Is in MiniQCrypt. In: Canteaut and Standaert (eds) Advances in Cryptology - EUROCRYPT 2021. EUROCRYPT 2021. Lecture Notes in Computer Science, vol 12697. Springer, Cham.

[13] C. Crépeau and J. Kilian, Achieving oblivious transfer using weakened security assumptions (extended abstract). In 29th FOCS, pages 42-52. IEEE Computer Society Press, October 1988.

[14] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, Practical quantum oblivious transfer. In Joan Feigenbaum, editor, CRYPTO'91, volume 576 of LNCS, pages 351-366. Springer, Heidelberg, August 1992.

[15] D. Mayers and L. Salvail, Quantum oblivious transfer is secure against all individual measurements. In Proceedings Workshop on Physics and Computation. PhysComp'94, pages 69-77. IEEE, 1994.

[16] A. C.-C. Yao, Security of quantum protocols against coherent measurements. In 27th ACM STOC, pages 67-75. ACM Press, May / June 1995.

[17] I. Damgard, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner, Improving the security of quantum protocols via commit-and-open. In Shai Halevi, editor, CRYPTO 2009, volume 5677 of LNCS, pages 408-427. Springer, Heidelberg, August 2009.

[18] R. Impagliazzo and S. Rudich, Limits on the provable consequences of one-way permutations. In Shafi Goldwasser, editor, CRYPTO'88, volume 403 of LNCS, pages 8-26. Springer, Heidelberg, August 1990.

[19] Ref. [18] showed the impossibility of *relativizing constructions* of key exchange from one-way functions, and oblivious transfer is stronger than key exchange. Since most cryptographic constructions are relativizing, this gives a strong negative result on constructing oblivious transfer from one-way functions in the classical setting.

[20] H.-K. Lo and H. F. Chau, Is quantum bit commitment really possible? Phys. Rev. Lett. **78**, 3410–3413 (1997).

[21] D. Mayers, Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**, 3414–3417 (1997).

[22] J. Yan, J. Weng, D. Lin, and Y. Quan, Quantum bit commitment with application in quantum zero-knowledge proof (extended abstract). In Khaled M. Elbassioni and Kazuhisa Makino, editors, Algorithms and Computation - 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings, volume 9472 of Lecture Notes in Computer Science, pages 555–565. Springer, 2015.

[23] P. Dumais, D. Mayers, and L. Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In EUROCRYPT, pages 300-315, 2000.

[24] C. Crépeau, F. Légaré and L. Salvail, How to convert the flavor of a quantum bit commitment. In EUROCRYPT, pages 60-77, 2001.

[25] T. Koshiba and T. Odaira, Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. In Andrew M. Childs and Michele Mosca, editors, Theory of Quantum Computation, Communication, and Cryptography, 4th Workshop, TQC 2009, Waterloo, Canada, May 11-13, 2009, Revised Selected Papers, volume 5906 of Lecture Notes in Computer Science, pages 33–46. Springer, 2009.

[26] T. Koshiba and T. Odaira, Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function. arXiv:1102.3441, 2011.

[27] J. Yan, General Properties of Quantum Bit Commitments. Cryptology ePrint Archive: Report 2020/1488

[28] N. Bitansky and Z. Brakerski, Classical Binding for Quantum Commitments. TCC 2021

[29] W. Diffie and M. Hellman, New directions in cryptography, in IEEE Transactions on Information Theory, vol.22, no.6, pp.644-654, November 1976.

[30] D. Gottesman and I. L. Chuang, Quantum Digital Signatures. arXiv:quant-ph/0105032.

[31] Z. Ji, Y.-K. Liu, and F. Song, Pseudo-random quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, CRYPTO 2018, Part III, volume 10993 of LNCS, pages 126–152. Springer, Heidelberg, August 2018.

[32] Z. Brakerski and O. Shmueli, (Pseudo) Random Quantum States with Binary Phase. In: Hofheinz and Rosen (eds) Theory of Cryptography. TCC 2019. Lecture Notes in Computer Science, vol 11891. Springer, Cham.

[33] Z. Brakerski and O. Shmueli, Scalable Pseudorandom Quantum States. In: Micciancio and Ristenpart (eds) Advances in Cryptology - CRYPTO 2020. Lecture Notes in Computer Science, vol 12171. Springer, Cham.

[34] W. Kretschmer, Quantum pseudorandomness and classical complexity. 16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021), Leibniz International Proceedings inInformatics (LIPIcs), 197:2:1–2:20, 2021

[35] M. Mahmoody and R. Pass, The curious case of non-interactive commitments - on the power of black-box vs. non-black-box use of primitives. In Reihaneh SafaviNaini and Ran Canetti, editors, CRYPTO 2012, volume 7417 of LNCS, pages 701–718. Springer, Heidelberg, August 2012.

[36] D. Unruh, Collapse-binding quantum commitments without random oracles. Asiacrypt 2016.

[37] J. Fang, D. Unruh, J. Yan, and D. Zhou, How to Base Security on the Perfect/Statistical Binding Property of Quantum Bit Commitment? Cryptology ePrint Archive, Report 2020/621, 2020

[38] Indeed, Ref. [11] states as follows: "*Moreover if in the future, new constructions of statistically binding, quantum computationally hiding commitments involving quantum communication are discovered based on assumptions weaker than quantum-hard one-way functions, it would be possible to plug those into our protocol compilers to obtain QOT.*" Unfortunately, our commitment scheme cannot be directly plugged into their construction since they require *classical binding* property [28], which is stronger than the standard notion of binding for quantum commitments proven in this paper.

[39] Ref. [34] gives only the case when $m = n$, but it is clear that the result holds for $m \geq cn$ with constant $c > 1$.

[40] L. Lamport, Constructing Digital Signatures from a One Way Function. SRI International (CSL-98). Retrieved 17

February 2021.

[41] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami, Computational Indistinguishability Between Quantum States and Its Cryptographic Application. J. Cryptol. 25: 528–555 (2012).

[42] J. Doliskani, Efficient Quantum Public-Key Encryption From Learning With Errors. arXiv:2105.12790.

[43] P. Ananth, L. Qian, and H. Yuen, Cryptography from pseudorandom quantum states. Cryptology ePrint Archive: Report 2021/1663

[44] P. Ananth, L. Qian, and H. Yuen, personal communication

[45] In fact, the security proofs of the constructions of Refs. [31, 32] are simpler for $t = 1$. Furthermore, there is a simple construction of PRS for $t = 1$ by using a pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^m$. In fact, we have only to take $|\phi_k\rangle = |G(k)\rangle$.

[46] Another example of constructions is $|\psi_0\rangle = \sum_{k\in\{0,1\}^n} |k\rangle|\phi_k\rangle$ and $|\psi_1\rangle = \sum_{r\in\{0,1\}^m} |r\rangle|r\rangle$. We have chosen the one we have explained, because the analogy to Naor's commitment scheme is clearer.

[47] M. Wilde, From Classical to Quantum Shannon Theory. arXiv:1106.1445

[48] A. Nayak and P. Shor, Bit-commitment-based quantum coin flipping. Phys. Rev. A **67**, 012304 (2003).