Quantum Commitments and Signatures without One-Way Functions

Tomoyuki Morimae[1] and Takashi Yamakawa[1,2]

[1] Yukawa Institute for Theoretical Physics, Kyoto University, Japan
[2] NTT Corporation, Japan

Abstract. In the classical world, the existence of commitments is equivalent to the existence of one-way functions. In the quantum setting, on the other hand, commitments are not known to imply one-way functions, but all known constructions of quantum commitments use at least one-way functions. Are one-way functions really necessary for commitments in the quantum world? In this work, 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 their polynomially many copies are computationally indistinguishable from the same number of copies of Haar random states [Ji, Liu, and Song, CRYPTO 2018]. It is known that pseudorandom quantum states exist even if **BQP** = **QMA** (relative to a quantum oracle) [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. In this work, we also consider digital signatures, which are other fundamental primitives in cryptography. We show that one-time secure digital signatures with quantum public keys exist if pseudorandom quantum states exist. In the classical setting, the existence of digital signatures is equivalent to the existence of one-way functions. Our result, on the other hand, shows that quantum signatures can exist even if no quantum-secure classical cryptographic primitive (including quantum-secure one-way functions) exists.

1 Introduction

1.1 Background

Commitments [Blu81] are one of the most central primitives in cryptography. Assume that a sender wants to commit a message m to a receiver. The sender encrypts it and sends it to the receiver. Later, the sender sends a key so that the receiver can open the message m. Before the sender sends the key, the receiver should not be able to learn the message m, which is called *hiding*. Furthermore, the sender should not be able to change the message later once the

sender commits it, which is called *binding*. (Imagine that the sender's message is put in a safe box and sent to the receiver. The receiver cannot open it until the receiver receives the key, and the sender cannot change the message in the safe box once it is sent to the receiver.) 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, [3] and therefore one of them has to be based on a computational assumption. In other words, in a computationally hiding commitment scheme, a malicious receiver can learn the message m before the opening if its computational power is unbounded, and in a computationally binding commitment scheme, a malicious sender can change its committed message later if its 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 [Nao91, HILL99]. The existence of one-way functions is considered the weakest assumption in classical cryptography, because virtually all complexity-based classical cryptographic primitives are known to imply the existence of one-way functions [LR86, IL89, ILL89].

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 [BB84], although it is impossible classically. Furthermore, oblivious transfer is possible with only (quantum-secure) one-way functions when quantum states are transmitted [BCKM21, GLSV21, CK88, BBCS92, MS94, Yao95, DFL$^+$09]. Classically, it is known to be impossible to construct oblivious transfer from only one-way functions [IR90].[4]

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 [LC97, May97]. In fact, all known constructions of quantum commitments use at least (quantum-secure) one-way functions [DMS00, CLS01, KO09, KO11, YWLQ15, Yan20, BB21].

In this paper, we ask the following fundamental question:

Are one-way functions really necessary for commitments?

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

[4] [IR90] 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.

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 [BCKM21, GLSV21], but no construction is provided.

Digital signatures [DH76] 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 the pair (m, σ) of the message and the signature. 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 except for an negligible probability.

Obviously, statistically-secure digital 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. In the quantum setting, on the other hand, digital signatures are not known to imply one-way functions. Gottesman and Chuang introduced digital signatures with quantum public keys [GC01], but they considered information-theoretical security, and therefore the number of public keys should be bounded. Our second fundamental question in this paper is the following:

Are digital signatures possible without one-way functions?

1.2 Our Results

In this paper, we answer the above two fundamental questions affirmatively. The first result of this paper is a construction of quantum commitments from pseudorandom quantum states generators (PRSGs) [JLS18, BS19, BS20]. A PRSG is a quantum polynomial-time algorithm that, on input $k \in \{0,1\}^n$, outputs an m-qubit state $|\phi_k\rangle$ such that $|\phi_k\rangle^{\otimes t}$ over uniform random k is computationally indistinguishable from the same number of copies of Haar random states for any polynomial t. (The formal definition of PRSGs is given in Definition 2.1.)

Our first result is stated as follows:[5]

Theorem 1.1. *If a pseudorandom quantum states generator with $m \geq cn$ for a constant $c > 1$ exists, then non-interactive quantum commitments (for classical messages) with computational hiding and statistical binding exist.*

In [Kre21], it is shown that PRSGs exist even if $\mathbf{BQP} = \mathbf{QMA}$ relative to a quantum oracle. If $\mathbf{BQP} = \mathbf{QMA}$, no quantum-secure classical cryptographic primitive exists, because $\mathbf{BQP} = \mathbf{QMA}$ means $\mathbf{NP} \subseteq \mathbf{BQP}$. In particular, no quantum-secure one-way function exists. Our Theorem 1.1 therefore shows that quantum commitments can exist even if no quantum-secure classical cryptographic

[5] Our construction of commitments also satisfies perfect correctness, i.e., the probability that the honest receiver opens the correct bit committed by the honest sender is 1.

primitive exists.[6] In particular, quantum commitments can exist even if no quantum-secure one-way function exists.

As we will see later (Section 3), what we actually need is a weaker version of PRSGs where only the computational indistinguishability of a single copy of $|\phi_k\rangle$ from the Haar random state is required. We call such a weaker version of PRSGs *single-copy-secure PRSGs*. (See Definition 2.2. It is the $t = 1$ version of Definition 2.1.) Because a single copy of the Haar random state is equivalent to the maximally-mixed state, the single-copy security means the computational indistinguishability from the maximally-mixed state. It could be the case that the realization of single-copy-secure PRSGs is easier than that of (multi-copy-secure) PRSGs. (For more discussions, see Section 2.2.)

Non-interactive commitments are a special type of commitments. (See Definition 3.1.) 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 [YWLQ15], while it is subject to a black-box barrier in the classical case [MP12].

As the definition of binding, we choose a standard one, sum-binding [Unr16], which roughly means that $p_0+p_1 \leq 1+\mathsf{negl}(\lambda)$, where negl is a negligible function, λ is a security parameter, and 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 3.4.)

Our first result, Theorem 1.1, 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 [FUYZ20] and quantum-secure oblivious transfer (and therefore multi-party computations (MPC)) [BCKM21, GLSV21]. Thus, those primitives can also exist even if **BQP** = **QMA** (and in particular quantum-secure one-way functions do not exist)[7] while classical constructions of them imply the existence of one-way functions. For more details, see Appendix B.

We also remark that there is no known construction of PRSGs 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 a PRSG from weaker assumptions than the

[6] It actually shows stronger things, because **BQP** = **QMA** also excludes the existence of some quantum-secure *quantum* cryptographic primitives where honest algorithms are quantum.

[7] Indeed, [BCKM21] 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.*"

existence of one-way functions without oracles. Such a construction immediately yields commitments (and more) by our result.

One might ask the following question: can we remove (or improve) the condition of $m \geq cn$ with a constant $c > 1$ in Theorem 1.1? The answer is no for single-copy-secure PRSGs, because if $m \leq n$, there is a trivial construction of a single-copy-secure PRSG without any assumption: $|\phi_k\rangle := |k_1, ..., k_m\rangle$ for any $k \in \{0,1\}^n$, where k_j is the jth bit of k. In fact, $\frac{1}{2^n}\sum_{k\in\{0,1\}^n} |\phi_k\rangle\langle\phi_k| = \frac{I^{\otimes m}}{2^m}$. If quantum commitments were constructed from such a single-copy-secure PRSG, we could realize quantum commitments without any assumption, which is known to be impossible [LC97, May97]. We note that [Kre21] considers only the case when $m = n$, but it is clear that the result holds for $m \geq cn$ with constant $c > 1$.

Finally, we do not know whether the opposite of Theorem 1.1 holds or not. Namely, do quantum commitments imply PRSGs (or single-copy-secure PRSGs)? It is an interesting open problem.

Now let us move on to our second subject, namely, digital signatures. Our second result in this paper is the following:

Theorem 1.2. *If a pseudorandom quantum states generator with $m \geq cn$ for a constant $c > 1$ exists, then one-time secure digital signatures with quantum public keys exist.*

One-time security means that the adversary can query the signing oracle at most once. (See Definition 4.2 and Definition 4.4.) In the classical setting, it is known how to construct many-time secure digital signatures from one-time secure digital signatures [Mer90], but we do not know how to generalize our one-time secure quantum signature scheme to a many-time secure one, because in our case public keys are quantum. It is an important open problem to construct many-time secure digital signatures from PRSGs.

Due to the oracle separation by [Kre21], Theorem 1.2 means that (at least one-time secure) digital signatures can exist even if no quantum-secure classical cryptographic primitive exists.[8] In particular, (one-time secure) digital 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 [DH76] by Gottesman and Chuang [GC01]. They consider information-theoretical security, and therefore the number of public keys should be bounded. On the other hand, our construction from PRSGs allows unbounded polynomial number of public keys. Quantum cryptography with quantum public keys are also studied in [KKNY12, Dol21].

We do not know whether the condition, $m \geq cn$ with a constant $c > 1$, can be improved or not in Theorem 1.2. Although it is possible to construct PRSGs without this restriction [BS20], this is satisfied in the construction of [Kre21], and therefore enough for our purpose of showing the existence of digital signatures without one-way functions.

As we will see later (Section 4), our construction of digital signatures is actually based on what we call *one-way quantum states generators (OWSGs)*

[8] Again, it also excludes some quantum-secure *quantum* cryptographic primitives.

(Definition 4.1). Intuitively, we say that a quantum polynomial-time algorithm that outputs an m-qubit quantum state $|\phi_k\rangle$ on input $k \in \{0,1\}^n$ is a OWSG if it is hard to find, given polynomially many copies of $|\phi_k\rangle$ (with uniformly random k), an n-bit string $\sigma \in \{0,1\}^n$ such that $|\phi_\sigma\rangle$ is close to $|\phi_k\rangle$. In other words, what we actually show is the following:

Theorem 1.3. *If a one-way quantum states generator exists, then one-time secure digital signatures with quantum public keys exist.*

We show that a PRSG is a OWSG (Lemma 4.1), and therefore, Theorem 1.2 is obtained as a corollary of Theorem 1.3. The concept of OWSGs itself seems to be of independent interest. In particular, we do not know whether OWSGs imply PRSGs or not, which is an interesting open problem.

Remember that for the construction of our commitment scheme we use only single-copy-secure PRSGs. Unlike our commitment scheme, on the other hand, our signature scheme uses the security of PRSGs for an unbounded polynomial number of copies, because the number of copies decides the number of quantum public keys. In other words, single-copy-secure PRSGs enable commitments but (multi-copy-secure) PRSGs enable signatures. There could be therefore a kind of hierarchy in PRSGs for different numbers of copies, which seems to be an interesting future research subject.

1.3 Technical Overviews

Here we provide intuitive explanations of our constructions given in Section 3 and Section 4.

Commitments The basic idea of our construction of commitments is, in some sense, a quantum generalization of the classical Naor's commitment scheme [Nao91].

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 pseudorandom state $|\phi_k\rangle$, and to replace the addition of η^b with the quantum one-time pad, which randomly applies Pauli X and Z. More precisely, the sender who wants to commit $b \in \{0,1\}$ generates the state

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

and sends the register C to the receiver, where $P_{x,z} \coloneqq \bigotimes_{j=1}^{m} X_j^{x_j} Z_j^{z_j}$. It is the commitment phase. At the end of the commitment phase, the receiver's state is $\rho_0 \coloneqq \frac{1}{2^n}\sum_k |\phi_k\rangle\langle\phi_k|$ when $b = 0$ and $\rho_1 \coloneqq \frac{1}{2^n}\frac{1}{4^m}\sum_k \sum_{x,z} P_{x,z}^b |\phi_k\rangle\langle\phi_k| P_{x,z}^b$ when $b = 1$. By the security of single-copy-secure PRSGs, ρ_0 is computationally indistinguishable from the m-qubit maximally-mixed state $\frac{I^{\otimes m}}{2^m}$, while $\rho_1 = \frac{I^{\otimes m}}{2^m}$ due to the quantum one-time pad (Lemma 2.1). The two states, ρ_0 and ρ_1, are therefore computationally indistinguishable, which shows computational hiding.

For statistical sum-binding, we show that the fidelity between ρ_0 and ρ_1 is negligibly small. It is intuitively understood as follows: $\rho_0 = \frac{1}{2^n}\sum_{k\in\{0,1\}^n} |\phi_k\rangle\langle\phi_k|$ has a support in at most 2^n-dimensional space, while $\rho_1 = \frac{I^{\otimes m}}{2^m}$ has a support in the entire 2^m-dimensional space, where $m \geq cn$ with $c > 1$, and therefore the "overlap" between ρ_0 and ρ_1 is small.

A detailed explanation of our construction of commitments and its security proof are given in Section 3.

Digital Signatures Our construction of digital signatures is a quantum public key version of the classical Lamport signature. 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 $sk \coloneqq (sk_0, sk_1)$, where sk_0, sk_1 are uniform randomly chosen n-bit strings. The public key is $pk \coloneqq (pk_0, pk_1)$, where $pk_0 \coloneqq f(sk_0)$ and $pk_1 \coloneqq f(sk_1)$. 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, our key generation algorithm chooses $k_0, k_1 \leftarrow \{0,1\}^n$, and runs $|\phi_{k_b}\rangle \leftarrow \mathsf{StateGen}(k_b)$ for $b \in \{0,1\}$, where $\mathsf{StateGen}$ is a PRSG.[9] It outputs $sk \coloneqq (sk_0, sk_1)$ and $pk \coloneqq (pk_0, pk_1)$, where $sk_b \coloneqq k_b$ and $pk_b \coloneqq |\phi_{sk_b}\rangle$ for $b \in \{0,1\}$. To sign a bit $m \in \{0,1\}$, the signing algorithm outputs the signature $\sigma \coloneqq sk_m$. Given the message-signature pair (m, σ), the verification algorithm measures pk_m with $\{|\phi_\sigma\rangle\langle\phi_\sigma|, I - |\phi_\sigma\rangle\langle\phi_\sigma|\}$ and accepts if and only if the result is $|\phi_\sigma\rangle\langle\phi_\sigma|$.

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 contradicts the security of PRSGs. In order to formalize this intuition, we introduce what we call OWSGs (Definition 4.1), and show that PRSGs imply OWSGs (Lemma 4.1). For details of our construction of digital signatures and its security proof, see Section 4.

[9] It is not necessarily a PRSG. Any OWSG (Definition 4.1) is enough. For details, see Section 4.

1.4 Concurrent Work

Few days after the first version of this paper was made online, a concurrent work [AQY21] appeared. The concurrent work also constructs commitments from PRSGs. We give comparisons between our and their results.

1. For achieving the security level of $O(2^{-n})$ for binding, they rely on PRSGs with $m = 2\log n + \omega(\log\log n)$ and any t, or $m = 7n$ and $t = 1$. On the other hand, we rely on PRSGs with $m = 3n$ and $t = 1$. Thus, the required parameters seem incomparable though we cannot simply compare them due to the difference of definitions of binding. (See also Appendix B.)
2. 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.
3. They consider a more general definition of PRSGs than us that allows the state generation algorithm to sometimes fail. We do not take this into account since we can rely on PRSGs of [Kre21] whose state generation never fails for our primary goal to show that commitments and digital signatures can exist even if one-way functions do not exist. Moreover, the failure probability has to be anyway negligibly small due to the security of PRSGs, and therefore it would be simpler to ignore the failure.

Besides commitments, the result on digital signatures is unique to this paper. On the other hand, [AQY21] contains results that are not covered in this paper such as pseudorandom function-like states and symmetric key encryption. We remark that our result on digital signatures was added a few days after the initial version of [AQY21] was made online, but the result was obtained independently, and there is no overlap with [AQY21] in this part.

Though most part of this work was done independently of [AQY21], there are two part where we revised the paper based on [AQY21]. The first is the definition of PRSGs. As pointed out in the initial version of [AQY21], the initial version of this work implicitly assumed that PRSGs do not use any ancillary qubits, which is a very strong restriction. However, we found that all of our results can be based on PRSGs that use ancillary qubits with just notational adaptations. Thus, we regard this as a notational level issue and fixed it.

The second is the connection to oblivious transfer and MPC explained in Appendix B. In the initial version of this work, we only mentioned the idea of using the techniques of [FUYZ20] to instantiate oblivious transfer and MPC of [BCKM21] based on quantum commitments. On the other hand, [AQY21] shows it assuming that the base quantum commitment satisfies a newly introduced definition of statistical binding property, which we call AQY-binding. Interestingly, we found that it is already implicitly shown in [FUYZ20] that the sum-binding implies AQY-binding. As a result, our commitment scheme can also be used to instantiate oblivious transfer and MPC of [BCKM21]. See Appendix B for more detail.

2 Preliminaries

In this section, we provide preliminaries.

2.1 Basic Notations

We use standard notations in quantum information. For example, $I := |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator. For notational simplicity, we sometimes write the n-qubit identity operator $I^{\otimes n}$ 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 the jth qubit. Let ρ_{AB} be a quantum state over the subsystems A and B. Then $\mathrm{Tr}_A(\rho_{AB})$ is the partial trace of ρ_{AB} over subsystem A. For n-bit strings $x, z \in \{0,1\}^n$, $X^x := \bigotimes_{j=1}^n X_j^{x_j}$ and $Z^z := \bigotimes_{j=1}^n Z_j^{z_j}$, where x_j and z_j are the jth bit of x and z, respectively.

We also use standard notations in cryptography. 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.

In this paper, we use the following lemma. It can be shown by a straightforward calculation.

Lemma 2.1 (Quantum one-time pad). *For any m-qubit state ρ,*

$$\frac{1}{4^m}\sum_{x\in\{0,1\}^m}\sum_{z\in\{0,1\}^m} X^x Z^z \rho Z^z X^x = \frac{I^{\otimes m}}{2^m}.$$

2.2 Pseudorandom Quantum States Generators

Let us review pseudorandom quantum states generators (PRSGs) [JLS18, BS19, BS20]. The definition of PRSGs is given as follows.

Definition 2.1 (Pseudorandom quantum states generators (PRSGs) [JLS18, BS19, BS20]). *A pseudorandom quantum states generator (PRSG) 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.

Remark 2.1. In the most general case, $\mathsf{StateGen}$ is the following QPT algorithm: given an input $k \in \{0,1\}^n$, it first computes a classical description of a unitary quantum circuit U_k, and next applies U_k on the all zero state $|0...0\rangle$ to generate

$|\Phi_k\rangle_{AB} \coloneqq U_k|0...0\rangle$. It finally outputs the m-qubit state $\rho_k \coloneqq \mathrm{Tr}_B(|\Phi_k\rangle\langle\Phi_k|_{AB})$. However, ρ_k is, on average, almost pure, because otherwise the security is broken by a QPT adversary who runs the SWAP test on two copies.[10] In this paper, for simplicity, we assume that ρ_k is pure, and denote it by $|\phi_k\rangle$. The same results hold even if it is negligibly close to pure. What $\mathsf{StateGen}$ generates is therefore $|\Phi_k\rangle_{AB} = |\phi_k\rangle_A \otimes |\eta_k\rangle_B$ with an ancilla state $|\eta_k\rangle$. In this paper, for simplicity, we assume that there is no ancilla state in the final state generated by $\mathsf{StateGen}$, but actually the same results hold even if ancilla states exist. (See Section 3 and Section 4.) Moreover, [Kre21] considers the case with pure outputs and no ancilla state, and therefore restricting to the pure and no ancilla case is enough for our purpose of showing the existence of commitments and digital signatures without one-way functions.

Interestingly, what we actually need for our construction of commitments (Section 3) is a weaker version of PRSGs where the security is satisfied only for $t = 1$. We call them *single-copy-secure PRSGs*:

Definition 2.2 (Single-copy-secure PRSGs). *A single-copy-secure pseudorandom quantum states generator (PRSG) 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 non-uniform QPT adversary* $\mathcal{A}$*, there exists a negligible function* negl *such that for all* n*,*

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

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

Remark 2.2. Because a single copy of an m-qubit state sampled Haar randomly is equivalent to the m-qubit maximally-mixed state, $\frac{I^{\otimes m}}{2^m}$, the security of single-copy-secure PRSGs is in fact the computational indistinguishability of a single copy of $|\phi_k\rangle$ from $\frac{I^{\otimes m}}{2^m}$.

Remark 2.3. As we have explained in Remark 2.1, in the definition of PRSGs (Definition 2.1), the output state ρ_k of $\mathsf{StateGen}$ has to be negligibly close to pure (on average). When we consider single-copy-secure PRSGs (Definition 2.2), on the other hand, the SWAP-test attack does not work because only a single copy is available to adversaries. In fact, there is a trivial construction of a single-copy-secure PRSG whose output is not pure: $\mathsf{StateGen}(k) \to \frac{I^{\otimes m}}{2^m}$ for all $k \in \{0,1\}^n$. We therefore assume that the output of $\mathsf{StateGen}$ is pure, i.e., $\rho_k = |\phi_k\rangle\langle\phi_k|$, when we consider single-copy-secure PRSGs.

[10] Let us consider an adversary $\mathcal{A}$ that runs the SWAP test on two copies of the received state and outputs the result of the SWAP test. When $\rho_k^{\otimes t}$ is sent with uniformly random k, the probability that $\mathcal{A}$ outputs 1 is $(1 + \frac{1}{2^n}\sum_k \mathrm{Tr}(\rho_k^2))/2$. When the t copies of Haar random states $|\psi\rangle^{\otimes t}$ is sent, the probability that $\mathcal{A}$ outputs 1 is 1. For the security, $|(1 + \frac{1}{2^n}\sum_k \mathrm{Tr}(\rho_k^2))/2 - 1| \leq \mathsf{negl}(\lambda)$ has to be satisfied, which means the expected purity of ρ_k, $\frac{1}{2^n}\sum_k \mathrm{Tr}(\rho_k^2)$, has to be negligibly close to 1.

Remark 2.4. It could be the case that single-copy-secure PRSGs are easier to realize than (multi-copy-secure) PRSGs. In fact, the security proofs of the constructions of [JLS18, BS19] are simpler for $t = 1$. Furthermore, there is a simple construction of a single-copy-secure PRSG by using a pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^m$. In fact, we have only to take $|\phi_k\rangle = |G(k)\rangle$ for all $k \in \{0,1\}^n$.

Remark 2.5. One might think that a single-copy-secure PRSG with $m \geq n+1$ is a pseudorandom generator (PRG), because if the m-qubit state $|\phi_k\rangle$ is measured in the computational basis, the probability distribution of the measurement results is computationally indistinguishable from that (i.e., the m-bit uniform distribution) obtained when the m-qubit maximally mixed state $\frac{I^{\otimes m}}{2^m}$ is measured in the computational basis. It is, however, strange because if it was true then the existence of single-copy-secure PRSGs implies the existence of PRGs, which contradicts [Kre21]. The point is that measuring $|\phi_k\rangle$ in the computational basis does not work as PRGs because the output is not deterministically obtained. (Remember that PRGs are deterministic algorithms.)

3 Commitments

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

3.1 Definition

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

Definition 3.1 (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 $\bot$. 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 perfect correctness is defined as follows:

Definition 3.2 (Perfect correctness). *A commitment scheme satisfies perfect correctness if the following is satisfied: when the honest sender commits $b \in \{0,1\}$, the probability that the honest receiver opens b is 1.*

The computational hiding is defined as follows:

Definition 3.3 (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,*

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

As the definition of binding, we consider sum-binding [Unr16] that is defined as follows:

Definition 3.4 (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* $U^{(b)}_{ER}$ *on the registers* E *and* R*.* $\mathcal{A}$ *sends* b *and the register* R *to* $\mathcal{C}$*.*
4. $\mathcal{C}$ *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* $|\psi_b\rangle\langle\psi_b|$ *is obtained,* $\mathcal{C}$ *accepts* b*. Otherwise,* $\mathcal{C}$ *outputs* $\bot$*.*

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

$$p_b := \langle\psi_b|_{RC}\mathrm{Tr}_E(U^{(b)}_{ER}|\Psi\rangle\langle\Psi|_{ERC}U^{(b)\dagger}_{ER})|\psi_b\rangle_{RC}.$$

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

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

3.2 Construction

Let us explain our construction of commitments.[11] Let $\mathsf{StateGen}$ be a single-copy-secure PRSG that, on input $k \in \{0,1\}^n$, outputs an m-qubit state $|\phi_k\rangle$. The commit phase is the following.

1. Let $b \in \{0,1\}$ be the bit to commit. The sender 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 receiver, where $P_{x,z} := \bigotimes_{j=1}^m X_j^{x_j} Z_j^{z_j}$.

[11] 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.

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.)

It is obvious that this construction satisfies perfect correctness (Definition 3.2).

Remark 3.1. 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. We will provide a detailed explanation of it in Appendix A. Here, we give an intuitive argument. In general non-interactive quantum commitments (Definition 3.1), 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 are 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 to the receiver before the reveal phase due to the quantum one-time pad. 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.

Remark 3.2. We also note that our construction of commitments can be extended to more general cases where ancilla qubits are used in PRSGs. Let us consider a more general PRSG that generates $|\phi_k\rangle \otimes |\eta_k\rangle$ and outputs $|\phi_k\rangle$, where $|\eta_k\rangle$ is an ancilla state. In that case, hiding and binding hold if we replace $|\psi_b\rangle$ with

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

3.3 Computational Hiding

We show computational hiding of our construction.

Theorem 3.1 (Computational hiding). *Our construction satisfies computational hiding.*

Proof of Theorem 3.1. 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 3.1.
$$|\Pr[\mathsf{Hyb}_0(b)=1] - \Pr[\mathsf{Hyb}_1(b)=1]| \leq \mathsf{negl}(\lambda)$$
for each $b \in \{0,1\}$.

Proof of Lemma 3.1. It is clear that
$$\Pr[\mathsf{Hyb}_0(1)=1] = \Pr[\mathsf{Hyb}_1(1)=1].$$
Let us show
$$|\Pr[\mathsf{Hyb}_0(0)=1] - \Pr[\mathsf{Hyb}_1(0)=1]| \leq \mathsf{negl}(\lambda).$$
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 PRSGs as follows. Let $b'' \in \{0,1\}$ be the parameter of the security game of PRSGs.

1. The challenger $\mathcal{C}'$ of the security game of PRSGs 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 PRSGs. □

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 3.2.

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

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

Proof of Lemma 3.2.

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

is clear. Let us show

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

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 PRSGs as follows. Let $b'' \in \{0,1\}$ be the parameter of the security game of PRSGs.

1. The challenger $\mathcal{C}'$ of the security game of PRSGs 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 PRSGs. □

It is obvious that

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

Therefore, from Lemma 3.1 and Lemma 3.2, we conclude

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

which shows Theorem 3.1. □

3.4 Statistical Binding

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

Theorem 3.2 (Statistical sum-binding). *Our construction satisfies statistical sum-binding.*

Proof of Theorem 3.2. Let

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

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

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

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}, $F(\rho_{AB},\sigma_{AB}) \leq F(\rho_A,\sigma_A)$, where $\rho_A = \mathrm{Tr}_B(\rho_{AB})$ and $\sigma_A = \mathrm{Tr}_B(\sigma_{AB})$.

Therefore,

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

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

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

is satisfied [NS03]. 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 $\xi \leq 2^n$. In the last inequality, we have used $m \geq cn$ for a constant $c > 1$. □

4 Digital Signatures

In this section, we provide our construction of digital signatures and show its security. For that goal, we first define OWSGs (Definition 4.1), and show that PRSGs imply OWSGs (Lemma 4.1).

4.1 One-way Quantum States Generators

For the construction of our signature scheme, we introduce OWSGs, which are defined as follows:

Definition 4.1 (One-way quantum states generators (OWSGs)). *Let G be 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 is a one-way quantum states generator (OWSG) if for any $t = poly(n)$ and for any QPT adversary $\mathcal{A}$ there exists a negligible function negl such that

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

Remark 4.1. 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 digital signatures.

Remark 4.2. The most general form of G is as follows: on input $k \in \{0,1\}^n$, it computes a classical description of a unitary quantum circuit U_k, and applies U_k on $|0...0\rangle$ to generate $|\Phi_k\rangle_{AB} := U_k|0...0\rangle$, and outputs $\rho_k := \mathrm{Tr}_B(|\Phi_k\rangle\langle\Phi_k|_{AB})$. However, because ρ_k plays the role of a public key in our construction of digital signatures, we assume that ρ_k is pure. (It is not natural if public keys and secret keys are entangled.) In that case, $U_k|0...0\rangle = |\phi_k\rangle_A \otimes |\eta_k\rangle_B$, where $|\eta_k\rangle$ is an ancilla state. For simplicity, we assume that there is no ancilla state: $U_k|0...0\rangle = |\phi_k\rangle$. In that case, the measurement $\{|\phi_\sigma\rangle\langle\phi_\sigma|, I - |\phi_\sigma\rangle\langle\phi_\sigma|\}$ by the challenger in Definition 4.1 can be done as follows: the challenger first applies $U_\sigma^\dagger$ on the state and then measures all qubits in the comptuational basis. The all zero measurement result corresponds to $|\phi_\sigma\rangle\langle\phi_\sigma|$ and other results correspond to $I - |\phi_\sigma\rangle\langle\phi_\sigma|$. Even if ancilla states exist, however, the same result holds. In that case, the verification of the challenger in Definition 4.1 is modified as follows: given σ, it generates $U_\sigma|0...0\rangle = |\phi_\sigma\rangle_A \otimes |\eta_\sigma\rangle_B$ to obtain $|\eta_\sigma\rangle$, applies $U_\sigma^\dagger$ on $|\phi_k\rangle \otimes |\eta_\sigma\rangle$, and measures all qubits in the computational basis. If the result is all zero, it accepts, i.e., the output of the experiment is 1. Otherwise, it rejects.

We can show the following:

Lemma 4.1 (PRSGs imply OWSGs). *If a pseudorandom quantum states generator with $m \geq cn$ for a constant $c > 1$ exists, then a one-way quantum states generator exists.*

Proof of Lemma 4.1. Assume that $\Pr[\mathsf{Exp} = 1]$ of the security game of Definition 4.1 with $G = \mathsf{StateGen}$ is non-negligible. Then we can construct an adversary $\mathcal{A}'$ that breaks the security of PRSGs as follows. Let $b' \in \{0,1\}$ be the parameter of the security game for PRSGs.

1. If $b' = 0$, the challenger $\mathcal{C}'$ of the security game for PRSGs 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 PRSGs 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,

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

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

Remark 4.3. For simplicity, Lemma 4.1 considers the case when no ancilla state exists in PRSGs. It is easy to see that Lemma 4.1 can be generalized to the case when PRSGs have ancilla states: on input $k \in \{0,1\}^n$, a PRSG applies U_k on

$|0...0\rangle$ to generate $U_k|0...0\rangle = |\phi_k\rangle \otimes |\eta_k\rangle$, where $|\phi_k\rangle$ is the output of the PRSG and $|\eta_k\rangle$ is an ancilla state. In that case, we modify Definition 4.1 in such a way that the verification of the challenger is modified as follows: given σ, it generates $U_\sigma|0...0\rangle = |\phi_\sigma\rangle \otimes |\eta_\sigma\rangle$ to obtain $|\eta_\sigma\rangle$, applies $U_\sigma^\dagger$ on $|\phi_k\rangle \otimes |\eta_\sigma\rangle$, and measures all qubits in the computational basis. If the result is all zero, it accepts, i.e., the output of the experiment is 1.

4.2 Definition of Digital Signatures with Quantum Public Keys

We now formally define digital signatures with quantum public keys:

Definition 4.2 (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 perfect correctness is defines as follows:

Definition 4.3 (Perfect correctness). *We say that a signature scheme satisfies perfect correctness if*

$$\Pr[\top \leftarrow \mathsf{Verify}(pk, m, \sigma) : sk \leftarrow \mathsf{Gen}_1(1^\lambda), pk \leftarrow \mathsf{Gen}_2(sk), \sigma \leftarrow \mathsf{Sign}(sk, m)] = 1$$

for all messages m*.*

The one-time security is defined as follows:

Definition 4.4 (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*

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

4.3 Construction

Let G be a OWSG. 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 $sk := (sk_0, sk_1)$, where $sk_b := k_b$ for $b \in \{0,1\}$.
- $\mathsf{Gen}_2(sk)$: Run $|\phi_{k_b}\rangle \leftarrow G(k_b)$ for $b \in \{0,1\}$. Output $pk := (pk_0, pk_1)$, where $pk_b := |\phi_{k_b}\rangle$ for $b \in \{0,1\}$.
- $\mathsf{Sign}(sk, m)$: Output $\sigma := sk_m$.
- $\mathsf{Verify}(pk, m, \sigma)$: 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 $\bot$.

It is clear that this construction satisfies perfect correctness (Definition 4.3).

4.4 Security

Let us show the security of our construction.

Theorem 4.1. *Our construction of a signature scheme is one-time secure.*

Proof of Theorem 4.1. 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 $\mathsf{Gen}_2(sk_1)$ $s := \max(s_0, s_1)$ times.) Then, we can construct an adversary that breaks the security of OWSG G as follows. Let $\mathcal{C}'$ and $\mathcal{A}'$ be the challenger and the adversary of the security game of G, 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 straightforward 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 security of G.

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

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

□

Remark 4.4. For simplicity, we have assumed that the OWSG G does not have any ancilla state. We can extend the result to the case when G has ancilla states. In that case, the verification algorithm in our construction of digital signatures is 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 this generalized version.

Acknowledgements. TM is supported by JST Moonshot R&D JPMJMS2061-5-1-1, JST FOREST, MEXT QLEAP, the Grant-in-Aid for Scientific Research (B) No.JP19H04066, the Grant-in Aid for Transformative Research Areas (A) 21H05183, and the Grant-in-Aid for Scientific Research (A) No.22H00522.

References

AQY21. P. Ananth, L. Qian, and H. Yuen. Cryptography from pseudorandom quantum states. *IACR Cryptol. ePrint Arch.*, 2021:1663, 2021.

BB84. 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.

BB21. N. Bitansky and Z. Brakerski. Classical Binding for Quantum Commitments. In *TCC*, pages 273–298. Springer, 2021.

BBCS92. C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical Quantum Oblivious Transfer. In *CRYPTO'91*, volume 576 of *LNCS*, pages 351–366. 1992.

BCKM21. J. Bartusek, A. Coladangelo, D. Khurana, and F. Ma. One-Way Functions Imply Secure Computation in a Quantum World. LNCS, pages 467–496. 2021.

Blu81. M. Blum. Coin Flipping by Telephone. In *CRYPTO'81*, volume ECE Report 82-04, pages 11–15. 1981.

BS19. Z. Brakerski and O. Shmueli. (Pseudo) Random Quantum States with Binary Phase. In *TCC 2019, Part I*, volume 11891 of *LNCS*, pages 229–250. 2019.

BS20. Z. Brakerski and O. Shmueli. Scalable Pseudorandom Quantum States. In *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 417–440. 2020.

CK88. C. Crépeau and J. Kilian. Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract). In *29th FOCS*, pages 42–52. 1988.

CLS01. C. Crépeau, F. Légaré, and L. Salvail. How to Convert the Flavor of a Quantum Bit Commitment. In *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 60–77. 2001.

DFL+09. I. Damgård, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner. Improving the Security of Quantum Protocols via Commit-and-Open. In *CRYPTO 2009*, volume 5677 of *LNCS*, pages 408–427. 2009.

DH76. W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

DMS00. P. Dumais, D. Mayers, and L. Salvail. Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation. In *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 300–315. 2000.

Dol21. J. Doliskani. Efficient quantum public-key encryption from learning with errors. *arXiv:2105.12790*, 2021.

FUYZ20. 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.

GC01. D. Gottesman and I. L. Chuang. Quantum digital signatures. *arXiv:quant-ph/0105032*, 2001.

GLSV21. A. B. Grilo, H. Lin, F. Song, and V. Vaikuntanathan. Oblivious Transfer Is in MiniQCrypt. LNCS, pages 531–561. 2021.

HILL99. J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A Pseudorandom Generator from any One-way Function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

IL89. R. Impagliazzo and M. Luby. One-way Functions are Essential for Complexity Based Cryptography (Extended Abstract). In *30th FOCS*, pages 230–235. 1989.

ILL89. R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random Generation from one-way functions (Extended Abstracts). In *21st ACM STOC*, pages 12–24. 1989.

IR90. R. Impagliazzo and S. Rudich. Limits on the Provable Consequences of One-way Permutations. In *CRYPTO'88*, volume 403 of *LNCS*, pages 8–26. 1990.

JLS18. Z. Ji, Y.-K. Liu, and F. Song. Pseudorandom Quantum States. In *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 126–152. 2018.

KKNY12. A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami. Computational Indistinguishability Between Quantum States and Its Cryptographic Application. *Journal of Cryptology*, 25(3):528–555, 2012.

KO09. T. Koshiba and T. Odaira. Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. *TQC 2009*, 2009.

KO11. T. Koshiba and T. Odaira. Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function. *arXiv:1102.3441, 2011*, 2011.

Kre21. W. Kretschmer. Quantum pseudorandomness and classical complexity. *TQC 2021*, 2021.

LC97. H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78:3410–3413, 1997.

LR86. M. Luby and C. Rackoff. Pseudo-random Permutation Generators and Cryptographic Composition. In *18th ACM STOC*, pages 356–363. 1986.

May97. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78:3414–3417, 1997.

Mer90. R. C. Merkle. A Certified Digital Signature. In *CRYPTO'89*, volume 435 of *LNCS*, pages 218–238. 1990.

MP12. D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *EUROCRYPT*, pages 700–718. Springer, 2012.

MS94. 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.*, 1994.

Nao91. M. Naor. Bit commitment using pseudorandomness. *Journal of cryptology*, pages 151–158, 1991.

NS03. A. Nayak and P. Shor. Bit-commitment-based quantum coin flipping. *Physical Review A*, 67:012304, 2003.

Unr16. D. Unruh. Collapse-Binding Quantum Commitments Without Random Oracles. In *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 166–195. 2016.

Yan20. J. Yan. General properties of quantum bit commitments. *Cryptology ePrint Archive: Report 2020/1488*, 2020.

Yao95. A. C.-C. Yao. Security of quantum protocols against coherent measurements. In *27th ACM STOC*, pages 67–75. 1995.

YWLQ15. J. Yan, J. Weng, D. Lin, and Y. Quan. Quantum bit commitment with application in quantum zero-knowledge proof. *ISAAC 2015*, 2015.

A Making Opening Message Classical

In this Appendix, we show that general quantum non-interactive commitments can be modified so that the opening message is classical.

Let us consider the following general non-interactive quantum commitments:

– **Commit phase:** The sender who wants to commit $b \in \{0,1\}$ generates a certain state $|\psi_b\rangle_{RC}$ on the registers R and C. The sender sends the register C to the receiver.
– **Reveal phase:** The sender sends b and the register R to the receiver. The receiver runs a certain verification algorithm on the registers R and C.

Let us modify it as follows:

– **Commit phase:** The sender who wants to commit $b \in \{0,1\}$ chooses $x, z \leftarrow \{0,1\}^{|R|}$, and generates the state

$$[(X^x Z^z)_R \otimes I_C]|\psi_b\rangle_{RC},$$

where $|R|$ is the size of the register R. The sender sends the registers R and C to the receiver.
– **Reveal phase:** The sender sends (x, z) and b to the receiver. The receiver applies $(X^x Z^z)_R \otimes I_C$ on the state, and runs the original verification algorithm on the registers R and C.

Theorem A.1. *If the original commitment scheme is computationally hiding and statistically sum-binding, then the modified commitment scheme is also computationally hiding and statistically sum-binding.*

Proof. Let us first show hiding. Hiding is clear because what the receiver has after the commit phase in the modified scheme is $\frac{I^{\otimes|R|}}{2^{|R|}} \otimes \mathrm{Tr}_R(|\psi_b\rangle\langle\psi_b|_{RC})$, which is the same as that in the original scheme.

Next let us show binding. Biding is also easy to understand. The most general action of a malicious sender in the modified scheme is as follows.

1. The sender generates a state $|\Psi\rangle_{ERC}$ on the three registers E, R, and C. The sender sends the registers R and C to the receiver.
2. Given $b \in \{0,1\}$, the sender computes $(x, z) \in \{0,1\}^{|R|} \times \{0,1\}^{|R|}$. The sender sends (x, z) and b to the receiver.
3. The receiver applies $X^x Z^z$ on the register R.
4. The receiver runs the verification algorithm on the registers R and C.

Assume that this attack breaks sum-binding of the modified scheme. Then we can construct an attack that breaks sum-binding of the original scheme as follows:

1. The sender generates a state $|\Psi\rangle_{ERC}$ on the three registers E, R, and C. The sender sends the register C to the receiver.
2. Given $b \in \{0,1\}$, the sender computes (x, z) and applies $X^x Z^z$ on the register R. The sender sends the register R, b, and (x, z) to the receiver.
3. The receiver runs the verification algorithm on the registers R and C.

It is easy to check that the two states on which the receiver applies the verification algorithm are the same. □

B Equivalence of Binding Properties

In this paper, we adopt sum-binding (Definition 3.4) as a definition of binding property of commitment schemes. On the other hand, the concurrent work by Ananth et al. [AQY21] introduces a seemingly stronger definition of binding, which we call AQY-binding, and shows that their commitment scheme satisfies it. The advantage of the AQY-binding is that it naturally fits into the security analysis of oblivious transfer in [BCKM21]. That is, a straightforward adaptation of the proofs in [BCKM21] enables us to prove that a commitment scheme satisfying AQY-binding and computational hiding implies the existence of oblivious transfer and multi-party computation (MPC). Combined with their construction of an AQY-binding and computational hiding commitment scheme from PRSGs, they show that PRSGs imply oblivious transfer and MPC.

We found that it is already implicitly shown in [FUYZ20] that the sum-binding and AQY-binding are equivalent for non-interactive commitment schemes in a certain form called the *generic form* as defined in [YWLQ15, Yan20, FUYZ20].[12] Since our commitment scheme is in the generic form, we can conclude that our commitment scheme also satisfies AQY-binding, and thus can be used for constructing oblivious transfer and MPC based on [BCKM21]. We explain this in more detail below.

Commitment schemes in the general form. We say that a commitment scheme is in the general form if it works as follows over registers (C, R).

1. In the commit phase, for generating a commitment to $b \in \{0,1\}$, the sender applies a unitary Q_b on $|0...0\rangle_C \otimes |0...0\rangle_R$ and sends the C register to the receiver.
2. In the reveal phase, the sender sends the R register along with the revealed bit b. Then, the receiver applies $Q_b^\dagger$, measures both C and R in the computational basis, and accepts if the measurement outcome is $0...0$.

See [Yan20, Definition 2] for the more formal definition. Yan [Yan20, Theorem 1] showed that for commitment schemes in the general form, the sum-binding is equivalent to the *honest-binding*, which means $F(\sigma_0, \sigma_1) = \mathsf{negl}(\lambda)$, where F is the fidelity and σ_b is the honestly generated commitment to b for $b \in \{0,1\}$, i.e., $\sigma_b := \mathrm{Tr}_R(Q_b|0...0\rangle\langle 0...0|_{RC}Q_b^\dagger)$.

AQY-binding. Roughly speaking, the AQY-binding requires that there is an (inefficient) extractor $\mathcal{E}$ that extracts a committed message from the commitment and satisfies the following: We define the following two experiments between a (possibly dishonest) sender and the honest receiver:

Real Experiment: In this experiment, the sender and receiver run the commit and reveal phases, and the experiment returns the sender's final state ρ_S and the revealed bit b, which is defined to be $\bot$ if the receiver rejects.

[12] We remark that it is also noted in [AQY21, Remark 6.2] that they are "probably equivalent".

Ideal Experiment: In this experiment, after the sender sends a commitment, the extractor $\mathcal{E}$ extracts b' from the commitment. After that, the sender reveals the commitment and the receiver verifiers it. Let b be the revealed bit, which is defined to be $\bot$ if the receiver rejects. The experiment returns (ρ_S, b) if $b = b'$ and otherwise $(\rho_S, \bot)$ where ρ_S is sender's final state.

Then we require that for any (unbounded-time) malicious sender, outputs of the real and ideal experiments are statistically indistinguishable. See [AQY21, Definition 6.1] for the formal definition.

Sum-binding and AQY-binding are equivalent.

First, it is easy to see that AQY-binding implies sum-binding. By the AQY-binding, we can see that a malicious sender can reveal a commitment to $b \in \{0,1\}$ only if $\mathcal{E}$ extracts b except for a negligible probability. Moreover, it is clear that $\Pr[\mathcal{E} \text{ extracts } 0] + \Pr[\mathcal{E} \text{ extracts } 1] \leq 1$ for any fixed commitment. Thus, the sum-binding follows.

We observe that the other direction is implicitly shown in [FUYZ20] as explained below. As already mentioned, the sum-binding is equivalent to honest-binding. For simplicity, we start by considering the case of perfectly honest-binding, i.e., $F(\sigma_0, \sigma_1) = 0$.

First, as shown in [FUYZ20, Corollary 4], there is an (inefficient) measurement $(\mathit{\Pi}_0, \mathit{\Pi}_1)$ that perfectly distinguishes σ_0 and σ_1 since we assume $F(\sigma_0, \sigma_1) = 0$. Then, we can define the extractor $\mathcal{E}$ for the AQY-binding as an algorithm that just applies the measurement $(\mathit{\Pi}_0, \mathit{\Pi}_1)$ and outputs the corresponding bit b. It is shown in [FUYZ20, Lemma 6] that the final joint state over sender's and receiver's registers does not change even if we apply the measurement $(\mathit{\Pi}_0, \mathit{\Pi}_1)$ to the commitment before the reveal phase conditioned on that the receiver accepts. In the case of rejection, note that the revealed bit is treated as $\bot$ in the experiment for the AQY-binding. Moreover, the measurement on the commitment register does not affect sender's final state since no information is sent from the receiver to the sender. By combining the above observations, the joint distribution of the sender's final state and the revealed bit does not change even if we measure the commitment in $(\mathit{\Pi}_0, \mathit{\Pi}_1)$. This means that the AQY-binding is satisfied.

For the non-perfectly honest-binding case, i.e., $F(\sigma_0, \sigma_1) = \mathsf{negl}(\lambda)$, we can rely on the perturbation technique. It is shown in [FUYZ20, Lemma 8] that for a non-perfectly honest-binding commitments characterized by unitaries (Q_0, Q_1), there exist unitaries $(\tilde{Q}_0, \tilde{Q}_1)$ that characterize a perfectly honest-binding commitment scheme and are close to (Q_0, Q_1) in the sense that replacing (Q_0, Q_1) with $(\tilde{Q}_0, \tilde{Q}_1)$ in any experiment only negligibly changes the output as long as the experiment calls (Q_0, Q_1) or $(\tilde{Q}_0, \tilde{Q}_1)$ polynomially many times. By using this, we can reduce the AQY-binding property of non-perfectly honest-binding commitment schemes to that of perfectly honest-binding commitment schemes with a negligible security loss.