General Properties of Quantum Bit Commitments

Jun Yan*

Jinan University

February 11, 2021

Abstract

The concept of quantum bit commitment was introduced more than three decades ago in a failed attempt to base unconditionally secure bit commitment solely on laws of quantum mechanics. In this work, we explore general properties of *conditional* quantum bit commitments that additionally rely on quantum computational hardness but without any mathematical structures, e.g. quantum-secure one-way functions. While in general quantum bit commitment can only guarantee a fairly weak binding property compared with its classical counterpart, we discover that it enjoys some other nice properties that classical bit commitment does not have. In particular, among others, it turns out that any interactive quantum bit commitment scheme can be compiled into a non-interactive one. These properties not only enable us to simplify both the construction and the security analysis of quantum bit commitment schemes significantly but also suggest a potential use of quantum bit commitments as a replacement of classical ones in quantum cryptography.

*Email: *tjunyan@jnu.edu.cn*

Contents

1 Introduction

(Classical) bit commitment is an important cryptographic primitive which provides two security guarantees, hiding and binding. Informally speaking, the *hiding* property states that the commitments to 0 respective 1 are indistinguishable, and the *binding* property states that any (claimed) bit commitment can be opened as at most one bit value (0 or 1, exclusively). Based on complexity assumptions, bit commitment come in two flavors, computationally-hiding (statistically-binding) bit commitment [Nao91] and (statistically-hiding) computationally-binding bit commitment [NOVY98, HNO+09]. Most bit commitment schemes are *interactive*, in particular those based on the existence of one-way functions [Nao91, NOVY98, HNO+09], which is also the minimum complexity assumption for almost all cryptographic applications [IL89]. The one-way function assumption is the minimum complexity assumption for almost all cryptographic applications [IL89]; it is also a raw computational hardness assumption without any mathematical structures.

Turning to the quantum world, quantum bit commitment was proposed more than three decades ago, aiming to make use of quantum mechanics to realize the commitment to a *classical* bit[1] [BB84, BC90]. Unfortunately, like in the classical setting, unconditionally secure quantum bit commitment is impossible either [May97, LC98]. Based on quantum-secure one-way functions/permutations, we also have two flavors of quantum bit commitments [AC02, YWLQ15, DMS00, KO09, KO11, CLS01]. It may sound counter-intuitive at the first glance but in general the binding property of quantum bit commitment (quantum bit binding) is inherently weaker than that of classical bit commitment (classical bit binding): formally, the quantum bit binding can only guarantee $p_0 + p_1 < 1 + negl(n)$, a.k.a. *sum-binding* [Unr16b], where p_b ($b \in \{0, 1\}$) denotes the success probability of opening a (claimed) quantum bit commitment as the bit value b, and $negl(\cdot)$ is some negligible function of the security parameter n. In comparison, by the same notation the classical bit binding guarantees $p_0 < negl(n)$ or $p_1 < negl(n)$. Roughly, the reason why the quantum bit binding is much weaker than its classical counterpart is because a malicious quantum sender can commit to an arbitrary *superposition* of 0 and 1. More discussion on quantum bit (and string) binding is referred to [DMS00, CDMS04].

In spite of its inherently weak binding property, quantum bit commitment still interests us for mainly two reasons. First, it turns out to be useful in several applications, notably quantum zero-knowledge [YWLQ15, FUYZ20, Yan20] and quantum oblivious transfer [CDMS04]. Second, [FUYZ20, Yan20] and this work show that quantum bit commitment enjoys some nice properties that classical bit commitment does not have (as to be introduced shortly below), which can help us to circumvent barriers proved only for classical commitments (e.g. [ARU14]). We expect that quantum bit commitment can serve as a useful primitive in quantum cryptography and finds more applications in future.

1.1 Our contribution

We obtain three main results on general properties of quantum bit commitments. Before stating them, we highlight that our results rely heavily on a *generic form* of non-interactive quantum bit commitment schemes (i.e. represented by an ensemble of unitary quantum circuit pair, r.f. Definition 2), though assuming this form does not lose generality [YWLQ15, FUYZ20].

[1] In some literature, the notion "quantum bit commitment" is referred to *post-quantum* secure classical bit commitment, or classical bit commitment secure against quantum attacks, which can be viewed as a special case of the quantum bit commitment whose construction (the communication and the computation of honest parties) is restricted to be classical.

1. Honest-binding is equivalent to sum-binding w.r.t. non-interactive quantum bit commitment schemes of the generic form

The honest-binding property of a (non-interactive or interactive) quantum bit commitment scheme is the security against the sender who is *semi-honest* (or *honest-but-curious*) in the commit stage but could be *arbitrary* in the reveal stage; it is the weakest binding property that any meaningful quantum bit commitment should satisfy. We show that the honest-binding property implies the seemingly stronger sum-binding property [DMS00] w.r.t. *non-interactive* quantum bit commitment schemes of the generic form (Theorem 1). Its proof is just a simple application of the *weak quantum rewinding lemma* once used in [YWLQ15, FUYZ20]. As an immediate corollary, we establish an equivalence between the semi-honest security and the full security (against an arbitrary quantum attack) w.r.t. a generic non-interactive quantum bit commitment scheme (Theorem 2). This equivalence enables us to simplify the security analysis of the DMS construction of computationally-binding quantum bit commitment [DMS00] significantly[2].

More interestingly, we observe that the binding property of a generic non-interactive quantum bit commitment scheme (of both flavors) turns out to be *information-theoretically strict*, or the scheme is automatically *strict-binding* that is in a similar sense to the one as introduced in [Unr12, ARU14], with the difference that the strict-binding here is through the *entanglement* (rather than the correlation) between a commitment and its decommitment. This inherent strictness of the quantum binding property has already proved crucial in some applications [FUYZ20].

Related work. Unruh [Unr16b] introduced a kind of quantum binding known as the *collapse-binding* for the *classical* commitments secure against quantum attacks, which has several nice properties and finds many applications in the post-quantum cryptography (e.g. [Unr16b, Mah18]). Compared with honest-binding/sum-binding, collapse-binding is strictly stronger [Unr16a]; but its realization in turn relies on stronger (than quantum-secure one-way functions) assumptions [Unr16a, Unr16b].

2. Interaction can be removed in realizing quantum bit commitment

Prior to this work, there already have several evidences suggesting that interaction may not be necessary in realizing quantum bit commitment: both flavors of non-interactive quantum bit commitment can be constructed from quantum-secure one-way functions [YWLQ15, DMS00, KO09, KO11]. Seeing from this, one may tend to conjecture that any (interactive) quantum bit commitment scheme can be complied into a non-interactive one. In this work, we confirm this conjecture by proving a *round-collapse* theorem (Theorem 4). This theorem is interesting by noting that we do not have a classical counterpart of it yet, which even seems unlikely [MP12, HHRS07]. This round-collapse theorem can also be viewed as a generalization of the *quantization* of Naor's bit commitment scheme in [YWLQ15].

At a high level, our *compiler* for the round compression is very simple: in the new (non-interactive) commit stage, the sender will simulate an *honest* execution of the commit stage of the original (interactive) scheme, and send the original receiver's system as the commitment at the end. Later in the reveal stage, the new sender will send its residual system to the new receiver, who will check the sender's whole computation in the commit stage via the *reversible* computation. At the first glance, this round-compression seems too good to be true: after all, a cheating sender may deviate from an honest simulation of the commit stage of the original interactive quantum bit

[2]Strictly speaking, we simplify the security analysis of the DMS scheme after it is firstly converted into the generic form.

scheme. But it turns out that as long as the original scheme is just secure against the *purification* attack (the full security is not even required), or put it another way, its purification (e.g. as done in [LC98]) is *semi-honest* secure, then it can be compressed into a non-interactive one (Theorem 3)!

For application of our round-collapse theorem, we provide yet another two constructions (besides the ones given in [DMS00, KO09, KO11]) of non-interactive computationally-binding quantum bit commitment. The first one is to compress the *CLS scheme* [CLS01], for which our security analysis is significantly easier than that of the original one. The second construction is to compress the *NOVY scheme* [NOVY98], whose classical security is not even known if can be lifted to the quantum setting (when the underlying one-way permutation is quantum secure). Also, our (quantum) security analysis for it is much easier than the classical one [NOVY98]. We highlight that in both applications, the simplification of the security analyses come from our strong round-collapse theorem: we just need to show the security against the purification attack of the original (interactive) scheme.

Our technique. Techniques to establish the security against the purification attack of the original interactive quantum bit commitment scheme, or the semi-honest security of its purification, will be crucial to our analysis. It turns out that the security against this special kind of attack is closely related to the semi-honest security, thus often much easier to establish than the full security. In particular, we show that in many interesting situations, the semi-honest security of the original scheme *extends* to its purification. For such an extension, the *basic idea* is to show that the collapses prescribed by the original scheme are *enforced* even *after* the purification. To see this, for example, messages sent through the classical channel automatically collapse; when a message is uniquely determined by some other collapsed messages, it can be viewed as collapsed; moreover, as argued in [FUYZ20], committing to a bit using a generic perfectly/statistically-binding quantum bit commitment scheme can be viewed as a way of measuring the committed bit (without leaking its value); and so on. In spite of this, we stress that the semi-honest security of an (interactive) quantum bit commitment scheme does *not* extend to its purification *generally*; two counterexamples are given in Subsection 5.4.

Related work. We would like to compare our compression of an interactive quantum bit commitment scheme with that of a quantum interactive proof system in [KW00]. The ideas in these two cases are similar: both of them rely heavily on the *reversibility* of quantum computation. The key difference is that for the latter, since (even) the honest prover could be computationally unbounded, an (interactive) *swap test* is introduced for the purpose of checking the computation. In comparison, in our case this test is not necessary because as typical in cryptography, both the honest sender and the honest receiver are polynomial-time bounded.

3. A generic statistically-binding quantum bit commitment scheme composed in parallel satisfies the strongest string sum-binding property

A natural way to commit a string is to commit it bitwisely using a quantum bit commitment scheme. Since a general quantum bit commitment scheme only guarantees a fairly weak sum-binding property, it is interesting and important to explore what binding property can be obtained if it is composed in parallel. Ideally, we may hope to prove such a strong quantum *string sum-binding* property as $\sum_{s\in\{0,1\}^m} p_s < 1 + negl(n)$, where p_s denotes the success probability that the cheating sender can open the claimed commitment as the m-bit string s, and $negl(\cdot)$ denotes some negligible function of the security parameter n. However, this string sum-binding property seems

too strong to be true generally when $m = poly(n)$ [CDMS04], in which case the sender may attack by committing to a superposition of exponentially many m-bit strings.

In spite of this, we are able to show that composing a generic *statistically-binding* quantum bit commitment scheme in parallel indeed gives rise to a quantum string commitment scheme satisfying such a strong statistical sum-binding property (Theorem 7). Its proof relies heavily on that the statistical binding error decreases *exponentially* w.r.t. the Hamming distance between the committed string and the string to reveal, which does not extend to the case of quantum computational binding.

This strong quantum statistical string sum-binding property in particular implies that the statistical CDMS-binding property[3] [CDMS04] holds w.r.t. any function on binary strings (Subsection 8.2). This in turn immediately implies that the quantum oblivious transfer protocol in [CDMS04] (a variant of the original one in [BBCS91, Cré94]) is secure when a generic non-interactive statistically-binding quantum bit commitment scheme is plugged in[4]. We expect this strong string sum-binding property to find more applications in future.

Organization. In Section 2, we review necessary preliminaries. In Section 3, we study the binding property of a generic non-interactive quantum bit commitment scheme. In particular, we prove that its honest-binding property is equivalent to the sum-binding property. This equivalence will later be used to simplify the security analysis of the DMS construction of computationally-binding bit commitment in Section 4. In Section 5, we define the semi-honest security of a general interactive quantum bit commitment scheme that is consistent with the intuition. Also, we sketch a general procedure to purify an arbitrary interactive quantum bit commitment scheme. Both of them will be crucial in establishing the round-collapse theorem in Section 6. In Section 7, we give yet another two constructions of non-interactive computationally-binding quantum bit commitment as applications of the round-collapse theorem. In Section 8, we establish a strong string sum-binding property of the parallel composition of a generic non-interactive statistically-binding quantum bit commitment scheme. Finally in Section 9, we conclude this work and raise some open questions.

2 Preliminaries

Notation. Denote $[n] = \{1, 2, \ldots, n\}$ for an integer n. Let U_n denote the uniform distribution/random variable ranging over the set $\{0,1\}^n$, i.e. all binary strings of length n. We use "$\xleftarrow{\$}$" to denote the action of choosing an element uniformly random from a given set, e.g. $x \xleftarrow{\$} U_n$. Let $negl(n)$ denote an arbitrary *negligible* (asymptotically smaller than any inverse polynomial) function of the security parameter n. Given two strings $s, s' \in \{0,1\}^n$, let $\mathrm{dist}(s, s')$ denote the Hamming distance between s and s'.

We sometimes explicitly write quantum register(s) as a *superscript* of an operator or a quantum state to indicate on which register(s) this operator performs or which register(s) hold this quantum state, respectively. For example, we may write U^A, $|\psi\rangle^A$ or ρ^A, highlighting that the operator U performs on the register A, and the register A is in pure state $|\psi\rangle$ or mixed state ρ, respectively. When it is clear from the context, we often drop the superscripts to simplify the notation.

[3] Actually, the original (computational) CDMS-binding introduced in [CDMS04] is only defined w.r.t. efficient cheating senders. But this definition extends straightforwardly to computationally unbounded cheating senders and gives rise to the *statistical* CDMS-binding.

[4] However, this application of the strong quantum string sum-binding property is not so appealing, since we already have a much simpler security analysis for the original (and simpler) quantum oblivious transfer protocol [FUYZ20].

Quantum stuffs. We use $\mathrm{F}(\cdot,\cdot)$ to denote the *fidelity* of two quantum states [Wat18]. Given a projector Π on a Hilbert space, we call $\{\Pi, \mathbb{1}-\Pi\}$ the *binary* measurement induced by Π; it is typically viewed as a *verification* for which we call it *succeeds*, *accepts*, or the outcome is *one*, if the measured quantum state collapses to the subspace on which Π projects.

For a bit $b \in \{0,1\}$, let $|b\rangle_+$ and $|b\rangle_\times$ be the qubits in the state $|b\rangle$ w.r.t. the standard basis and Hadamard basis, respectively. For the standard basis, we often drop "+" and just write $|b\rangle$.

We work with the standard *unitary* quantum circuit model. In this model, quantum algorithm can be formalized in terms of *uniformly generated* quantum circuit family, where the "uniformly generated" means the description of the quantum circuit coping with n-bit inputs can be output by *a single classical polynomial-time algorithm* on the input 1^n. We assume without loss of generality that each quantum circuit is composed of quantum gates chosen from some fixed universal, finite, and *unitary* quantum gate set [NC00]. Given a quantum circuit Q, we also abuse the notation to use Q to denote the corresponding *unitary transformation*, and $Q^\dagger$ to denote its *inverse*.

(In)distinguishability of quantum state ensembles

Definition 1 ((In)distinguishability of quantum state ensembles) Two quantum state ensembles $\{\rho_n\}_n$ and $\{\xi_n\}_n$ are *quantum statistically (resp. computationally) indistinguishable*, if for any quantum state ensemble $\{\sigma_n\}_n$ and any unbounded (resp. polynomial-time bounded) quantum algorithm D which outputs a single qubit,

$$|\Pr[D(1^n, \rho_n \otimes \sigma_n) = 1] - \Pr[D(1^n, \xi_n \otimes \sigma_n) = 1]| < negl(n)$$

for sufficiently large n.

Remark. The quantum state ensemble $\{\sigma_n\}_n$ in the definition above plays the role of the *non-uniformity* given to the distinguisher D. Since a mixed quantum state can always be purified, we can assume without loss of generality that the state σ_n is *pure*.

A generic non-interactive quantum bit commitment scheme

In [YWLQ15, FUYZ20], it is argued that any *non-interactive* statistically-binding quantum bit commitment scheme can be converted into a scheme of the generic form given by an ensemble of *unitary* quantum circuit pair. This argument extends to the case of non-interactive computationally-binding quantum bit commitment scheme in a straightforward way. We thus introduce the following definition.

Definition 2 A generic non-interactive quantum bit commitment scheme is represented by an ensemble of polynomial-time uniformly generated quantum circuit pair $\{(Q_0(n), Q_1(n))\}_n$ as follows.

- In the *commit* stage, to commit bit $b \in \{0,1\}$, the sender performs the quantum circuit $Q_b(n)$ on quantum registers (C, R) initialized in all $|0\rangle$'s state. Then the sender sends the *commitment* register C to the receiver, whose state at this moment denoted by $\rho_b(n)$.
- In the subsequent (canonical) *reveal* stage, the sender announces the bit b, and sends the *decommitment register* R to the receiver. The receiver then performs $Q_b(n)^\dagger$ on the registers (C, R), accepting if (C, R) return to all $|0\rangle$'s state.

The hiding (or concealing) and the binding properties of this generic scheme are defined as follows.

- **Hiding**. We say that the scheme is statistically (resp. computationally) hiding if the quantum state ensembles $\{\rho_0(n)\}_n$ and $\{\rho_1(n)\}_n$ are statistically (resp. computationally) indistinguishable.

- (Honest-)**binding**. We say that the scheme is computationally (resp. statistically) binding if for any state $|\psi\rangle$ in auxiliary register Z, and any polynomial-time realizable (resp. unbounded) unitary transformation U performing on (R, Z), the reduced state of $U(Q_0(n)|0\rangle \otimes |\psi\rangle)$ in the registers (C, R) is far from the state $Q_1(n)|0\rangle$, or formally,

$$\left\| \left(Q_1 |0\rangle \langle 0| Q_1^\dagger\right) U^{RZ} (Q_0 |0\rangle \otimes |\psi\rangle) \right\| < negl(n). \tag{1}$$

  By the *reversibility* of quantum computation, this binding property above can also be equivalently defined by swapping the roles of Q_0 and Q_1, in which case the inequality (1) becomes

$$\left\| \left(Q_0 |0\rangle \langle 0| Q_0^\dagger\right) U^{RZ} (Q_1 |0\rangle \otimes |\psi\rangle) \right\| < negl(n). \tag{2}$$

Remark.

1. In the sequel, we will focus on this non-interactive quantum bit commitment scheme of the generic form given above without loss of generality.

2. We call the binding property defined above the *honest-binding*, because informally it states that any cheating sender cannot open the *honest* commitment to a bit b (output by the sender who performs honestly in the commit stage) as $1 - b$. Clearly, this is the *weakest* binding property that any meaningful quantum bit commitment scheme should satisfy. We will also call this binding property *standard-binding*, for the additional reasons that: (1) it can be shown equivalent to the widely accepted *sum-binding* property; and (2) it has already proved useful in applications [FUYZ20, Yan20].

3. Seeing from our definition of the (honest-)binding property, we stress that the auxiliary state $|\psi\rangle$ is only provided to the (possibly cheating) sender at the *beginning* of the reveal stage.

4. As commented in [YWLQ15], this reveal stage is called *canonical* because it is similar to the *canonical* opening of classical bit commitment, where the sender sends all its *random coins* used in the commit stage to the receiver who then checks that these coins *explain* (i.e. are consistent with) the conversation generated in the commit stage.

5. In the sequel, to simplify the notation we often drop the security parameter n and just write (Q_0, Q_1) to represent a generic non-interactive quantum bit commitment scheme.

Useful lemmas

Lemma 3 (Uhlmann's theorem) *Let $\mathcal{X}$ and $\mathcal{Y}$ be two Hilber spaces. Density operators ρ and σ are in the space $\mathcal{X}$. Unit vector $|\psi\rangle$ is a purification of ρ in the space $\mathcal{X} \otimes \mathcal{Y}$, i.e. $Tr_Y(|\psi\rangle\langle\psi|) = \rho$. It holds that $\mathrm{F}(\rho, \sigma) = \max\{|\langle\psi|\eta\rangle| : \text{ unit vector } |\eta\rangle \in \mathcal{X} \otimes \mathcal{Y} \text{ s.t. } Tr_Y(|\eta\rangle\langle\eta|) = \sigma\}$.*

Lemma 4 (A weak quantum rewinding [FUYZ20]) *Let $\mathcal{X}$ and $\mathcal{Y}$ be two Hilbert spaces. Unit vector $|\psi\rangle \in \mathcal{X} \otimes \mathcal{Y}$. Orthogonal projectors $\Gamma_1, \ldots, \Gamma_k$ perform on the space $\mathcal{X} \otimes \mathcal{Y}$, while unitary*

transformations $U_1, \ldots, U_k$ *perform on the space* $\mathcal{Y}$. *If* $1/k \cdot \sum_{i=1}^{k} \left\|\Gamma_i(U_i \otimes \mathbb{1}^X) |\psi\rangle\right\|^2 \geq 1-\eta$, *where* $0 \leq \eta \leq 1$, *then*

$$\left\|(U_k^\dagger \otimes \mathbb{1}^X)\Gamma_k(U_k \otimes \mathbb{1}^X) \cdots (U_1^\dagger \otimes \mathbb{1}^X)\Gamma_1(U_1 \otimes \mathbb{1}^X) |\psi\rangle\right\| \geq 1 - \sqrt{k\eta}. \tag{3}$$

Proof: Deferred to Appendix A for convenience. ■

3 The binding property of a generic non-interactive quantum bit commitment scheme

3.1 Honest-binding is equivalent to sum-binding

A widely accepted binding property of quantum bit commitment is known as the *sum-binding*, which is exactly what can be guaranteed *generally* when the most general quantum attacks against the sender are considered. Its definition w.r.t. a generic non-interactive quantum bit commitment scheme is as follows.

Definition 5 (Sum-binding) In the commit stage, the cheating sender sends the commitment register C (which could be in an arbitrary state) to the receiver. In the reveal stage, to open the bit commitment as 0 (resp. 1), the sender performs U_0 (resp. U_1) on its system and then send the decommitment register R to the receiver. Let p_0 (resp. p_1) be the success probability that the sender opens the bit commitment as 0 (resp. 1). The sum-binding requires that $p_0 + p_1 < 1 + negl(n)$.

Clearly, sum-binding implies honest-binding, by noting that if we fix p_0 or p_1 in Definition 5 to be one, then we end up with the honest-binding. Interestingly, it turns out that the opposite direction is also true, i.e. the seemingly weaker honest-binding also implies sum-binding. This is fomally stated in the following theorem.

Theorem 1 *Honest-binding is equivalent to sum-binding w.r.t. a generic non-interactive quantum bit commitment scheme.*

Proof: We suffice to prove that honest-binding implies sum-binding. It turns out that an attack which breaks the sum-binding property can almost be directly used to break the honest-binding property without much modification. Detail follows.

Let n be the security parameter. An arbitrary attack of the sum-binding property of a generic non-interactive quantum bit commitment scheme $\{(Q_0(n), Q_1(n))\}_n$ can be modeled by $(U_0, U_1, |\psi\rangle)$, where U_0, U_1 are two unitary transformations and $|\psi\rangle$ an arbitrary quantum state. In more detail, at the beginning the whole system (C, R, Z) (refer to Definition 2 for their meanings) is initialized in the state $|\psi\rangle$. Then in the commit stage, the (possibly cheating) sender sends the commitment register C to the receiver. Later in the reveal stage, if a bit value $b \in \{0, 1\}$ is to reveal, then the sender first performs the unitary transformation U_b on the subsystem (R, Z), and then sends the decommitment register R to the receiver.

Now assume that an attack $(U_0, U_1, |\psi\rangle)$ breaks the sum-binding property; that is,

$$\left\|\left(Q_0 |0\rangle \langle 0| Q_0^\dagger\right)^{CR} \cdot U_0^{RZ} |\psi\rangle\right\|^2 + \left\|\left(Q_1 |0\rangle \langle 0| Q_1^\dagger\right)^{CR} \cdot U_1^{RZ} |\psi\rangle\right\|^2 > 1 + \frac{1}{p},$$

where p is some polynomial of the security parameter n. We apply the weak rewinding lemma (Lemma 4) to the inequality above, with the parameters $k, \eta, U_1, U_2, \Gamma_1$ and Γ_2 in the lemma replaced by $2, 1/2 - 1/(2p), U_0, U_1, Q_0 |0\rangle \langle 0| Q_0^\dagger$ and $Q_1 |0\rangle \langle 0| Q_1^\dagger$, respectively. We obtain

$$\left\| U_1^\dagger (Q_1 |0\rangle \langle 0| Q_1^\dagger) U_1 \cdot U_0^\dagger (Q_0 |0\rangle \langle 0| Q_0^\dagger) U_0 |\psi\rangle \right\| \geq 1 - \sqrt{1 - \frac{1}{p}} > \frac{1}{2p}. \tag{4}$$

We are next to devise an attack of the honest-binding property of the scheme (Q_0, Q_1) given the attack $(U_0, U_1, |\psi\rangle)$ of the sum-binding property. Recall the definition of honest-binding (Definition 2). Suppose in the commit stage, the sender honestly prepares the quantum state $Q_0 |0\rangle$ in the registers (C, R) and sends the register commitment C to the receiver. Later at the beginning of the reveal stage, the sender receives the quantum state $|\psi\rangle$, which is stored in quantum registers $(\mathsf{C}', \mathsf{R}', \mathsf{Z}')$ that are of the same size as the registers $(\mathsf{C}, \mathsf{R}, \mathsf{Z})$, respectively. Then the cheating sender S^* proceeds as follows to try to open the quantum bit commitment as 1:

1. Perform the unitary transformation U_0 on the quantum registers $(\mathsf{C}', \mathsf{R}', \mathsf{Z}')$.
2. Perform the binary measurement induced by the projector $Q_0 |0\rangle \langle 0| Q_0^\dagger$ on the registers $(\mathsf{C}', \mathsf{R}')$. (*Intuitively*, we expect that conditioned on the outcome being one, the reduced state of the register Z' will help the sender cheats.)
3. Perform the unitary transformation $U_1 U_0^\dagger$ on the registers $(\mathsf{R}, \mathsf{Z}')$.
4. Send the decommitment register R to the receiver, trying to open the quantum bit commitment as 1.

Note that the squared l.h.s. of the inequality (4) is exactly the probability of the event that the outcome of the measurement in step 2 above is one and S^* cheats (i.e. opens the quantum bit commitment as 1) successfully. This immediately yields a lower bound $1/4p^2$ (which is non-negligible) of the probability of S^* cheating successfully. (Note that S^* may also cheat successfully while the measurement outcome of step 2 is zero.) Hence, S^* breaks the honest-binding property. ■

Remark. We highlight that the security reduction above is *uniform*.

W.r.t. a generic non-interactive quantum bit commitment scheme, since the receiver sends nothing in the commit stage, its hiding property against the honest-but-curious receiver trivially extends to that against an arbitrary receiver. Combined with Theorem 1, we have the following theorem as an immediate corollary.

Theorem 2 *A generic non-interactive quantum bit commitment scheme* $\{(Q_0(n), Q_1(n)\}_n$ *is secure if and only if it is semi-honest secure (i.e. honest-hiding and honest-binding) .*

3.2 Honest-binding does not imply collapse-binding

In [Unr16a], Unruh proposed the so-called (computational) *collapse-binding* property of classical commitments against quantum attacks. Roughly speaking, collapse-binding requires that conditioned on the (possibly cheating) sender opening the commitment successfully, its views corresponding to whether the revealed value of the commitment is measured or not are *quantum polynomial-time indistinguishable*. Compared with general quantum bit commitments, collapse-binding bit

commitments behave closer to classical bit commitments secure against classical attacks and thus much easier to use in applications [Unr16b].

We can naturally generalize the collapse-binding property which was introduced for classical commitments to quantum commitments. Then we ask, *is a generic non-interactive quantum bit commitment scheme collapse-binding?* Unfortunately, it is not very hard to see that the answer is no; even perfect honest-binding does not imply collapse-binding. Intuitively, the reason is almost the same as that a *superposition* of 0 and 1 is distinguishable from its corresponding *mixture*. Consider the *counterexample* as follows.

A cheating sender may prepare the state

$$\frac{1}{\sqrt{2}}\Big(|0\rangle^B \otimes Q_0 |0\rangle^{CR} + |1\rangle^B \otimes Q_1 |0\rangle^{CR} \Big)$$

and sends the commitment register C to the receiver in the commit stage. Later, the sender sends the registers (B, R) to the receiver to open the commitment. Clearly, the receiver will accept with certainty. But the two quantum states corresponding to whether the opening register B is measured or not, i.e. $1/2\big(|0\rangle\langle 0| \otimes Q_0 |0\rangle\langle 0| Q_0^* + |1\rangle\langle 1| \otimes Q_1 |0\rangle\langle 0| Q_1^* \big)$ and $1/\sqrt{2}\big(|0\rangle Q_0 |0\rangle + |1\rangle Q_1 |0\rangle \big)$, respectively, are distinguishable. Indeed, to distinguish them, one can first uncompute the register pair (C, R) by performing $Q_b^\dagger$ controlled by the qubit B, which then allows us to discard the register pair (C, R) safely. Finally, one can perform the measurement which distinguishes the quantum states $1/2(|0\rangle\langle 0| + |1\rangle\langle 1|)$ and $1/\sqrt{2}(|0\rangle + |1\rangle)$ to finish the job.

3.3 Strict-binding

In [Unr12], Unruh proposed a strengthening of the ordinary binding property of classical commitments known as the *strict-binding*. Roughly speaking, the strict-binding property requires that the way to open a commitment be *unique*; that is, there cannot be two different pairs of the bit value to reveal together with the corresponding decommitment that will lead the receiver to accept in a canonical reveal stage. Quantum-secure classical strict-binding bit commitment can be constructed from quantum-secure injective one-way functions. Such commitments turn out to be crucial in constructing quantum-secure classical zero-knowledge proof-of-knowledge [Unr12, ARU14].

Interestingly, we note that a generic quantum bit commitment scheme of either flavors (computationally hiding or computationally binding) is automatically *strict-binding information-theoretically*. That is, the only way to open an honest quantum bit commitment with *certainty* is to send the decommitment register R, which should be untouched since the honest quantum bit commitment is prepared (i.e. by performing the quantum circuit Q_b for some $b \in \{0, 1\}$ on the quantum register pair (C, R) in the commit stage). This information-theoretic strict-binding property is originated to the *entanglement* between the decommitment register R and the commitment register C.

The observation that a generic non-interactive quantum bit commitment scheme is inherently strict-binding leads to a construction of quantum zero-knowledge proof-of-knowledge for **NP** statements based on general (rather than injective) quantum-secure one-way functions [FUYZ20].

4 Application: a simpler security analysis for the purified DMS construction of quantum bit commitment

Dumais, Mayers and Salvail [DMS00] gave a construction of non-interactive computationally-binding quantum bit commitment based on quantum-secure one-way permutation. The hard part

Commit stage: Let $b \in \{0,1\}$ be the bit to commit.

- The sender chooses $x \xleftarrow{\$} \{0,1\}^n$ and computes $y = f(x)$, where $f : \{0,1\}^n \to \{0,1\}^n$ is a quantum-secure one-way permutation. Then the sender sends $|y\rangle_{\theta(b)^n}$ to the receiver, where $\theta(b)$ denotes the standard basis "+" when $b = 0$ and the Hadamard basis "×" when $b = 1$.

Reveal stage:

- The sender sends the bit b and the string x to the receiver.
- The receiver measures each qubit (in total n) received in the commit stage in the basis $\theta(b)$, obtaining $y \in \{0,1\}^n$. Then the receiver checks that $y = f(x)$.

Figure 1: The DMS construction of non-interactive computationally-binding quantum bit commitment based on quantum-secure one-way permutation

of its security analysis lies in establishing the computational sum-binding property. Here, we simplify this analysis but w.r.t. the *purified* version of the DMS scheme using Theorem 1, which allows us to restrict to focus on its (computationally) honest-binding property.

For self-containment, we reproduce the DMS scheme following [DMS00] in Figure 1. It can be firstly purified and then converted into the generic form as given in Definition 2 such that

$$Q_0 |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle^R |f(x)\rangle^C_{+^n}, \qquad Q_1 |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle^R |f(x)\rangle^C_{\times^n}. \tag{5}$$

The lemma below establishes the quantum computational binding property of the purified DMS scheme.

Lemma 6 *The purified DMS scheme (Q_0, Q_1) given by the equation (5) is quantum computationally binding.*

Proof: By Theorem 1, it suffices to show that the purified DMS scheme is computationally honest-binding.

We first rewrite

$$\begin{aligned}
Q_1 |0\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle^R |f(x)\rangle^C_{\times^n} \\
&= \frac{1}{2^n} \sum_{x\in\{0,1\}^n} |x\rangle \Big(|0\rangle + (-1)^{f(x)_1} |1\rangle \Big) \cdots \Big(|0\rangle + (-1)^{f(x)_n} |1\rangle \Big) \\
&= \frac{1}{2^n} \sum_{x\in\{0,1\}^n} |x\rangle \sum_{y\in\{0,1\}^n} (-1)^{f(x)\cdot y} |y\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} \underbrace{\left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)\cdot y} |x\rangle^R \right)}_{(*)} |y\rangle^C,
\end{aligned}$$

and

$$Q_0 |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle^R |f(x)\rangle^C_{+^n} = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} \underbrace{\left|f^{-1}(y)\right\rangle^R}_{(**)} |y\rangle^C .$$

Intuitively, if any cheating sender breaks the (computational) honest-binding property, then it can sort of transform the quantum state represented by the expression $(*)$ into the expression represented by the term $(**)$ in the above. But this already implies some ability to invert the one-way permutation $f(\cdot)$ on input a uniformly random chosen image $y \in \{0,1\}^n$. We convert this intuition into a formal proof in the below.

For contradiction, suppose that there exists a cheating sender S^* who breaks the computational honest-binding property of the purified DMS scheme; that is, there exists a pair $(U, |\psi\rangle)$ (whose meaning is referred to Definition 2) such that

$$\left\| \left(Q_0 |0\rangle \langle 0| Q_0^\dagger\right)^{CR} U^{RZ} \left(Q_1 |0\rangle^{CR} \otimes |\psi\rangle^Z\right) \right\| \geq \frac{1}{p(n)}, \tag{6}$$

where $p(\cdot)$ is some polynomial. We construct an inverter I^* for the one-way permutation $f(\cdot)$ as follows: it operates on the system $(\mathsf{R}, \mathsf{Y}, \mathsf{Z})$, where the register Y holds the input $y \in \{0,1\}^n$, the register Z holds the auxiliary state $|\psi\rangle$, while the register R is initialized in the state $|0^n\rangle$. Then the inverter I^* proceeds in the following steps:

1. Transform the whole system $(\mathsf{R}, \mathsf{Y}, \mathsf{Z})$ into the state $1/\sqrt{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)\cdot y} |x\rangle^R |y\rangle^Y |\psi\rangle^Z$. Specifically, this step can be accomplished through the following steps:

   (a) Perform $H^{\otimes n}$ on the register R, where H is the Hadamard gate, to obtain the quantum state

   $$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle^R |y\rangle^Y |\psi\rangle^Z .$$

   (b) Perform the unitary quantum circuit that computes the function $f(\cdot)$, i.e. realizing $|x\rangle |0\rangle \mapsto |x\rangle |f(x)\rangle$ for each $x \in \{0,1\}^n$, to obtain the quantum state

   $$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle^R |y\rangle^Y |\psi\rangle^Z |f(x)\rangle .$$

   (c) For each pair of $f(x)_i$ and y_i, $i = 1, \ldots, n$, i.e. the i-th bit of $f(x)$ and y, respectively, perform the two-qubit unitary transformation that realizes $|a\rangle |b\rangle \mapsto (-1)^{ab} |a\rangle |b\rangle$. This unitary transformation can be realized by first performing the Hadamard gate on the second qubit $|b\rangle$, followed by performing the `CNOT` gate on the two qubits with the first qubit $|a\rangle$ as the control, and finally performing another Hadamard gate on the second qubit. After ths step, the state becomes

   $$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)\cdot y} |x\rangle^R |y\rangle^Y |\psi\rangle^Z |f(x)\rangle .$$

   (d) Uncompute the $f(x)$ for each $x \in \{0,1\}^n$ in the superposition above by performing the *inverse* of the unitary quantum circuit that computes the function $f(\cdot)$. We thus arrive at the desired quantum state.

2. Perform the unitary translation U on the register (R, Z).

3. Measure the register R in the standard basis and output the outcome.

It is not hard to see that the inverter I^* runs in polynomial time if the unitary transformation U is polynomial-time realizable. We are left to estimate the success probability of the inverter I^*.

From the hypothesis (6),

$$\begin{aligned}
\frac{1}{p(n)} &\leq \left\| \left(Q_0 \left|0\right\rangle \left\langle 0\right| Q_0^\dagger\right)^{CR} U^{RZ} \left(Q_1 \left|0\right\rangle^{CR} \left|\psi\right\rangle^Z\right) \right\| \\
&= \frac{1}{2^n} \left\| Q_0 \left|0\right\rangle \otimes \sum_{y\in\{0,1\}^n} \left(\mathbb{1}^C \otimes \left\langle f^{-1}(y)\right|^R\right) \cdot U^{RZ} \left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)\cdot y} \left|x\right\rangle^R \left|\psi\right\rangle^Z\right) \right\| \\
&= \frac{1}{2^n} \left\| \sum_{y\in\{0,1\}^n} \left(\mathbb{1}^C \otimes \left\langle f^{-1}(y)\right|^R\right) \cdot U^{RZ} \left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)\cdot y} \left|x\right\rangle^R \left|\psi\right\rangle^Z\right) \right\| \\
&\leq \frac{1}{2^n} \sum_{y\in\{0,1\}^n} \left\| \left(\mathbb{1}^C \otimes \left\langle f^{-1}(y)\right|^R\right) \cdot U^{RZ} \left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)\cdot y} \left|x\right\rangle^R \left|\psi\right\rangle^Z\right) \right\| \\
&= \frac{1}{2^n} \sum_{y\in\{0,1\}^n} \left\| \left(\left|f^{-1}(y)\right\rangle \left\langle f^{-1}(y)\right|\right)^R \cdot U^{RZ} \left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)\cdot y} \left|x\right\rangle^R \left|\psi\right\rangle^Z\right) \right\| \\
&\leq \left(\frac{1}{2^n} \sum_{y\in\{0,1\}^n} \left\| \left(\left|f^{-1}(y)\right\rangle \left\langle f^{-1}(y)\right|\right)^R \cdot U^{RZ} \left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)\cdot y} \left|x\right\rangle^R \left|\psi\right\rangle^Z\right) \right\|^2 \right)^{\frac{1}{2}},
\end{aligned}$$

where the second "$\leq$" above uses the triangle inequality and the third "$\leq$" uses the Cauchy-Schwartz inequality. Squaring both sides of this inequality gives

$$\frac{1}{2^n} \sum_{y\in\{0,1\}^n} \left\| \left(\left|f^{-1}(y)\right\rangle \left\langle f^{-1}(y)\right|\right)^R \cdot U^{RZ} \left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)\cdot y} \left|x\right\rangle^R \left|\psi\right\rangle^Z\right) \right\|^2 \geq \frac{1}{p(n)^2}.$$

Note that the l.h.s. of the inequality above is exactly the success probability of the inverter I^* on input a uniformly random chosen image y. This probability is at least $1/p(n)^2$, which is non-negligible and thus contradicts the one-wayness of the function $f(\cdot)$.

This finishes the proof of the lemma. ■

5 The semi-honest security of an arbitrary interactive quantum bit commitment scheme and its purification

In this section, we turn to study the more general *interactive* quantum bit commitment schemes. For simplicity, we can assume without loss of generality that (1) all registers used by schemes are *two-dimensional* (i.e. composed of qubits), and (2) the operations used by schemes are restricted to unitary operations, measurements in the computational basis, random coin tosses, and exchanges of quantum or classical messages.

First, we try to define the semi-honest security of a general interactive quantum bit commitment scheme, which is generalized from that of classical protocols in a straightforward way. Then, we sketch a standard procedure of purifying an arbitrary interactive quantum bit commitment scheme. Next, we discuss the relationship between the semi-honest security of an arbitrary interactive quantum bit commitment scheme and its purification, which will be crucial for our applications in the sequel. Last, we study two inspiring schemes for the illustration of this relationship.

We remark that the material presented in this section is crucial for understanding and establishing the round-collapse theorem and its applications in the sequel.

5.1 Definitions of quantum honest-hiding and honest-binding

In this section, we turn to study the more general *interactive* quantum bit commitment schemes. For simplicity, we can assume without loss of generality that the operations used by schemes are restricted to unitary operations, measurements in the computational basis, random coin tosses, and exchanges of quantum or classical messages.

Recall that in the classical setting, the *semi-honest* security of a two-party protocol is defined w.r.t. the semi-honest, or *honest-but-curious* party. In a running of a two-party protocol, the semi-honest party will follow the protocol honestly, except that it will always record everything generated during the interaction. Only at the end of the running of the protocol, the semi-honest party may deviate to do something malicious based on its view.

In the same spirit as in the classical setting, we can generalize the semi-honest security to the quantum setting. For this purpose, we need first to prescribe a quantum semi-honest party's behavior in a running of an arbitrary quantum protocol, which is quite *different* from its classical counterpart due to the quantum no-cloning theorem.

A quantum semi-honest party's behavior. Intuitively, a quantum semi-honest party will also try to record everything that it can copy/clone but *without* disturbing the honest running of a quantum protocol. In greater detail, let us compare a running of the quantum protocol where one party is semi-honest while the other is honest, and a running where both parties are honest. We note that in the former the semi-honest party will use an additional quantum system for copying/cloning compared with the latter. But if we consider the residual quantum system in the former where this additional quantum system is removed, then the corresponding residual state should be identical to the state of the whole quantum system in the latter at *every* moment. Seeing from this intuition, in addition to always do exactly what the protocol prescribes, the semi-honest party will copy/clone the following things for a possible later use:

1. its measurement outcomes.
2. its random coin tosses.
3. *classical* messages it has sent and received.

We note that since a quantum state cannot be cloned generally, *intermediate* quantum states during a running of a quantum protocol can no longer be copied/cloned for a later use as in the classical setting.

To define the semi-honest security of an interactive quantum bit commitment scheme, we need first to define the semi-honest sender/receiver's *view* in a running of the *commit* stage of this scheme.

Definition 7 (The semi-honest sender/receiver's view) In a running of the *commit* stage of an interactive quantum bit commitment scheme where the sender (resp. receiver) is semi-honest while the receiver (resp. sender) is honest, the semi-honest sender's (resp. receiver's) view is given by the quantum state of its system at the *end* of the commit stage.

We have three remarks about the definition above:

1. The behavior of the semi-honest sender (resp. receiver) can be derived from our discussion w.r.t. a general quantum two-party protocol just above.

2. Since a quantum bit commitment scheme has two stages, namely the commit and the reveal stages, one may wonder why in the definition we only care about the commit stage. Basically, this is due to the honest-hiding and honest-binding properties of quantum bit commitment schemes we are interested in, whose definitions will be given shortly below.

3. We note that in the definition, *intermediate* quantum states of the semi-honest sender's (resp. receiver's) system during the commit stage do not account for its view; only the state at end of the commit stage matters. This is because quantum states cannot be cloned generally, as just discussed.

Now we are ready to define the semi-honest security of a general interactive quantum bit commitment scheme, i.e. its *honest-hiding* and the *honest-binding* properties. For the purpose of simplicity our definitions will be informal, yet clear enough so that experienced readers can easily work out the detail for a formal definition.

Intuitively, the honest-hiding property requires that at the end of a running of the commit stage of a quantum bit commitment scheme where the sender is honest while the receiver is semi-honest, the receiver cannot distinguish whether it is 0 or 1 that is committed. Thus, we have the following (informal) definition.

Definition 8 (Honest-hiding) An interactive quantum bit commitment scheme is *honest-hiding* if in a running of the commit stage of the scheme where the sender is honest while the receiver is semi-honest, the receiver's views corresponding to committing 0 respective 1 are indistinguishable.

Compared with the honest-hiding property which is defined w.r.t. the semi-honest receiver in the commit stage only, the honest-binding property is defined w.r.t. the *semi-honest* sender in the commit stage followed by an *arbitrary* sender in the reveal stage.

Definition 9 (Honest-binding) Consider the following honest-binding game w.r.t. an interactive quantum bit commitment scheme: a bit $b \in \{0, 1\}$ is committed in a running of the commit stage of the scheme where the sender is semi-honest while the receiver is honest. Later in the reveal stage, a possibly *cheating* sender will inherit the (semi-honest) sender's view (of the commit stage) and may additionally receive an auxiliary quantum state at the beginning of the reveal stage, attempting to open the (quantum) bit commitment as $1 - b$. If the sender succeeds, then we say that the sender wins the game. We say that the scheme is *honest-binding* if any cheating sender in the reveal stage cannot win the game with non-negligible probability, for both $b = 0$ and 1.

Remark. We note that our definitions of the honest-hiding and honest-binding properties of a general interactive quantum bit commitment scheme above are *consistent* with those of a generic non-interactive quantum bit commitment scheme (Definition 2), respectively. We highlight that compared with the definition of honest-binding in Definition 2, here we no longer claim that the inability to open an honest commitment to 0 as 1 is equivalent to the inability to open an honest commitment to 1 as 0. But in many situations, e.g. schemes studied in this paper (Section 7), the proofs of these two inabilities are symmetric.

5.2 Purify a general interactive quantum bit commitment scheme

For our purpose, we need first to normalize a general quantum bit commitment scheme by *purifying* it in such a way that all (classical and quantum) computations can be simulated by *unitary* quantum operations, and all classical communications can be simulated by quantum communications. The purification procedure presented below is standard, basically following Mayers [May97].

Recall that (for simplicity) we have already assumed without loss of generality that (1) all registers used by schemes are *two-dimensional* (i.e. composed of qubits), and (2) the operations used by schemes are restricted to unitary operations, measurements in the computational basis, random coin tosses, and exchanges of quantum or classical messages. To model a running of the *commit* stage of a general quantum bit commitment scheme, we introduce quantum registers $(\mathsf{A}, \mathsf{B}, \mathsf{E})$ as follows:

- A: the sender's workspace.
- B: the receiver's workspace.
- E: the environment $\mathsf{E} = (\mathsf{E}_S, \mathsf{E}_A, \mathsf{E}_B)$ is such that
  - $\mathsf{E}_S = (\mathsf{E}_{S,A}, \mathsf{E}_{S,B})$: both registers $\mathsf{E}_{S,A}$ and $\mathsf{E}_{S,B}$ store the classical bits transmitted between the sender and the receiver.
  - E_A: stores the *untransmitted* classical bits that are kept on the sender's side.
  - E_B: stores the *untransmitted* classical bits that are kept on the receiver's side.

For a party $P \in \{A, B\}$, where A and B stand for the sender and the receiver, respectively, we can purify each operation in the *commit* stage[5] of a general interactive quantum bit commitment scheme in the following way:

- *Measurement*: introduce an ancilla qubit in the state $|0\rangle$, and perform the quantum gate `CNOT` on the qubit to measure and this ancilla, with the former as the control. Then move this ancilla to the environment E_P.
- *A uniformly random coin toss*: introduce an ancilla qubit in the state $|0\rangle$, and perform the Hadamard gate `H` on it. Then move this ancilla to the environment E_P.
- *Transmission of a classical bit x from the sender to the receiver, and vice versa*: first move the qubit $|x\rangle$ from the environment E_A to $\mathsf{E}_{S,A}$, and then introduce an ancilla in the state $|0\rangle$ in the environment $\mathsf{E}_{S,B}$. Finally, perform the `CNOT` gate on the qubit $|x\rangle$ and this ancilla, with the former as the control. The opposite direction of the transmission is simulated symmetrically.
- *Unitary operation.* If P's unitary operation depends on any bit values in the environment $(E_P, E_{S,P})$, then first copy these bits into P's private workspace P before performing the corresponding unitary operation.

After the purification procedure above is applied, at any moment of a running of the *purified* commit stage of an interactive quantum bit commitment scheme the whole system will be in a state of the form

$$\sum_{s,a,b} \alpha_{s,a,b} \, |s\rangle^{E_{S,A}} \, |s\rangle^{E_{S,B}} \, |a\rangle^{E_A} \, |b\rangle^{E_B} \, |\psi_{s,a,b}\rangle^{AB} .$$

[5] For the purpose of this work, we only need to purify the commit stage, though the reveal stage can also be done in the same fashion.

That is, whenever each qubit in the environment E is measured in the standard basis (i.e. collapses occur like in a running of the commit stage of the original scheme), then $|\psi_{s,a,b}\rangle$ will be the state of the registers (A, B) associated with the occurrence of (s, a, b) with probability $|\alpha_{s,a,b}|^2$.

5.3 The semi-honest security before and after the purification

For the purpose of this work, we are especially interested in the relationship between the semi-honest security of an arbitrary interactive quantum bit commitment scheme and its purification. Towards this relationship we have the following observations:

Observation 1 Purifying an honest party's all operations in the commit stage of the original scheme will *not* affect the semi-honest security against the other party. This is simply because purifying the honest party's operations will not affect the other party's view.

Observation 2 By the standard purification procedure (Subsection 5.2), a semi-honest party will follow the *purified* scheme honestly. That is, in a running of the commit stage of the purified scheme, the semi-honest party's behavior will be the *same* as that of the corresponding honest party; no additional copies are needed.

Observation 3 The semi-honest security against one party of the purified scheme implies the semi-honest security against the same party of the original scheme. To see this, note that anything that can be copied/cloned, including the outcome of measurements, random coin tosses, as well as classical messages sent and received by the honest party, are all recorded in the environment by the standard purification procedure.

By Observation 1, the semi-honest security of the purified quantum bit commitment scheme can also as viewed as the security against the *purification attack* of the original scheme, where the "purification attack" refers to the attack by purifying the corresponding honest party's all operations. For this reason, in the sequel we will use the semi-honest security of the purified scheme and the security against the purification attack of the original scheme *interchangeably*.

Since the security against the purification attack will play a key role in our applications later, let us write out the corresponding definitions of what we will refer to as *purification-hiding* and *purification-binding* explicitly in the below, which are adapted from the definitions of honest-hiding (Definition 8) and honest-binding (Definition 9), respectively.

Definition 10 (Purification-hiding) Consider a running of the commit stage of an interactive quantum bit commitment scheme where the sender is honest while the receiver attacks by purifying all the honest receiver's operations. We say that this scheme is secure against the purification attack of the receiver, or *purification-hiding*, if the receiver's views corresponding to committing 0 respective 1 are indistinguishable.

Definition 11 (Purification-binding) Consider the following purification-binding game w.r.t. a general interactive quantum bit commitment scheme: a bit $b \in \{0, 1\}$ is committed in a running of the commit stage of the scheme where the receiver is *honest* while the sender attacks by purifying all the honest sender's operations. Later in the reveal stage, a possibly *cheating* sender will inherit the sender's view (of the commit stage) and may additionally receive an auxiliary quantum state at the beginning of the reveal stage, attempting to open the (quantum) bit commitment as $1 - b$. If the sender succeeds, then we say that the sender wins the game. We say that the scheme is secure against the purification attack of the sender, or *purification-binding*, if any cheating sender in the reveal stage cannot win the game with non-negligible probability, for both $b = 0$ and 1.

By definition, the security against the purification attack of an interactive quantum bit commitment scheme is *weaker* than the full security (against an arbitrary attack); generally, we do not expect that it can be equivalent to the full security[6]. Observation 3 above states that the security against the purification attack is *stronger* than the semi-honest security. But can these two notions of the security be equivalent, or equivalently, can the honest-hiding and honest-binding properties of an arbitrary interactive quantum bit commitment scheme be preserved after the purification?

To answer the question above, we note that compared with the honest party's behavior, after the purification some desired *collapses* (via measurements) by the honest party may no longer occur. This might compromise the semi-honest security of the purified scheme; one is referred to the next subsection for two such examples. In spite of this, the semi-honest security of some interactive quantum bit commitment schemes does extend to its purification. In Section 7, we develop several techniques for such an extension (which are illustrated by two applications). In the below, for illustration we identify a simple yet common scenario in which the semi-honest security against one party of a quantum bit commitment scheme extends its purification.

Specifically, we say that a party of a quantum bit commitment scheme is *public-coin* if its only action in the commit stage prescribed by the scheme is just sending a number of uniformly random bits. Then we have the following proposition.

Proposition 12 *If a party of a quantum bit commitment scheme is public-coin and this scheme is semi-honest secure against this party, then this scheme is also secure against the purification attack of this party.*

Proof Sketch: The (honest) receiver (who is the other party) of the random bits will measure immediately upon receiving them, which will collapse the state of the whole system to the one corresponding to this party *not* purifying its operation of tossing random coins. ■

5.4 Two simple schemes that are semi-honest secure but vulnerable to the purification attack

We present two schemes that are inspiring for the study of the relationship between the semi-honest security of a general interactive quantum bit commitment scheme and its purification. Both of these two schemes are unconditionally(information-theoretic) semi-honest secure, but vulnerable to the *purification attack*. We expect these two toy examples to give readers some idea of how the purification may compromise the semi-honest security of the original quantum bit commitment scheme. In particular, the security analysis of the second scheme (i.e. the simplified CLS scheme as we call) is helpful in understanding that of the correct one in subsection 7.1.

5.4.1 The BB84 scheme

The *non-interactive* BB84 scheme [BB84, May97] is described in Figure 2. We next informally argue that the BB84 scheme is unconditionally honest-hiding and unconditionally honest-binding.

The BB84 scheme is *unconditionally honest-hiding*, by noting that both honest commitments to 0 respective 1 are just the maximally mixed state. The scheme is *unconditionally honest-binding*, because almost a half of the bases $\hat{\theta}_i$'s chosen by the receiver are *not* equal to the basis θ that is determined by the bit b to commit. Thus, for each $\hat{\theta}_i \neq \theta$, any cheating sender cannot guess $\hat{x}_i$

[6]Restricting to the non-interactive quantum bit commitment scheme of the generic form, interestingly, we have shown that this is nevertheless true (Theorem 2).

Commit stage: Let $b \in \{0,1\}$ be the bit to commit.

1. The sender chooses a uniformly random string $x = x_1 \cdots x_n$, where each $x_i \xleftarrow{\$} \{0,1\}$. Choose the basis $\theta = +$ if $b = 0$, and $\theta = \times$ if $b = 1$. Send each qubit $|x_i\rangle_\theta$, $i = 1, 2, \ldots, n$, to the receiver.

2. For each $i = 1, \ldots, n$, the receiver chooses the basis $\hat{\theta}_i \xleftarrow{\$} \{+, \times\}$ and measures each qubit $|x_i\rangle_\theta$ in the basis $\hat{\theta}_i$, obtaining the outcome $\hat{x}_i$.

Reveal stage:

1. The sender sends the bit b and all x_i's to the receiver.

2. The receiver checks that for each $i = 1, 2, \ldots, n$, $\hat{x}_i = x_i$ whenever $\hat{\theta}_i = \theta$; reject otherwise.

Figure 2: The BB84 scheme

correctly with probability more than 1/2. It follows that the success probability of any cheating sender opening the honest commitment to the bit b as $1 - b$ is exponentially small.

However, the BB84 scheme is vulnerable to the *purification attack* of the sender, or *not* purification-binding. To see this, note that the commit stage of the BB84 scheme can be *purified* in such a way that the sender prepares n EPR pairs and sends half of each EPR pair to the receiver as the commitment; another half is kept by the sender. Then the sender simulates the measurement of its halves of EPR pairs in the basis θ *unitarily*; we denote this unitary operation by U when a bit 0 is committed. As such, the cheating sender who performs as follows can open the honest commitment to 0 as 1 with certainty:

1. Perform $U^\dagger$ to roll its system back to the state at the moment just before the sender measuring its halves of EPR pairs in the commit stage.

2. Measure its halves of EPR pairs in the basis "$\times$". Denote the outcomes by $x_1, \ldots, x_n$.

3. Send the revealed bit 1, as well as all x_i's to the receiver.

In this way, it is not hard to see that the sender can open the bit commitment as 1 successfully with certainty.

5.4.2 A simplified CLS scheme

The simplified CLS scheme, which is adapted from [CLS01], is the *parallel* composition of the atomic scheme as described in Figure 3. Compared with the original CLS scheme, the sender additionally sends bases θ_i's in its first message, and the receiver removes commitments to all its random chosen bases and measurement outcomes in its first message. We are next to informally argue that this simplified CLS scheme is unconditionally honest-hiding and unconditionally honest-binding.

Unconditional honest-hiding. Consider a running of the commit stage of the *atomic* scheme in which the sender is honest whereas the receiver is semi-honest. Note that with an overwhelming probability, we have $\hat{\theta}_i \neq \theta_i$ for nearly *half* of indices i where $1 \leq i \leq n$. Since $|I_0| + |I_1| = 2n/3 >$

Commit stage: Let $b \in \{0,1\}$ be the bit to commit.

- (**S1**) For $i = 1, 2, \ldots, n$, the sender chooses a bit $x_i \xleftarrow{\$} \{0,1\}$ and a basis $\theta_i \xleftarrow{\$} \{+,\times\}$, sending $(|x_i\rangle_{\theta_i}, \theta_i)$ to the receiver.
- (**R2**) For $i = 1, 2, \ldots, n$, the receiver chooses each basis $\hat{\theta}_i \xleftarrow{\$} \{+,\times\}$ and measures each received BB84 qubit $|x_i\rangle_{\theta_i}$ in the basis $\hat{\theta}_i$, obtaining the outcome $\hat{x}_i$. Choose $c \xleftarrow{\$} \{0,1\}$. Choose at random two disjoint subsets of positions $I_0, I_1 \subset [n]$ of size $n/3$ such that for each $i \in I_c$, $\theta_i = \hat{\theta}_i$. Send (I_0, I_1) to the sender.
- (**S3**) The sender chooses $a_0 \xleftarrow{\$} \{0,1\}$ and sets $a_1 = a_0 \oplus b$. Then compute $\hat{a}_0 = \bigoplus_{i \in I_0} x_i \oplus a_0$, $\hat{a}_1 = \bigoplus_{i \in I_1} x_i \oplus a_1$, sending $(\hat{a}_0, \hat{a}_1)$ to the receiver.
- (**R4**) The receiver computes $d_c = \bigoplus_{i \in I_c} \hat{x}_i \oplus \hat{a}_c$.

Reveal stage:

- The sender sends the bit b and (a_0, a_1) to the receiver.
- The receiver checks that $b = a_0 \oplus a_1$ and $d_c = a_c$.

Figure 3: The atomic scheme which composes in parallel gives the simplified CLS scheme

$n/2$, it follows from the pigeon hole principle that there exists at least one index $j \in I_{1-c}$ such that $\hat{\theta}_j \neq \theta_j$. It is for this index j that the receiver's guess for the x_j can be no better than a random guess. In turn, the receiver's guess for a_{1-c}, and thus the committed bit b (which is equal to $a_0 \oplus a_1$), can be no better than a random guess. That is, the sender's messages contain no information about the committed bit b. And this should hold for each copy when there are n copies of the atomic scheme running in parallel. As such, the simplified CLS scheme is *unconditionally honest-hiding*.

Unconditional honest-binding. First consider the honest-binding game w.r.t. the *atomic* scheme in which a bit 0 is committed in the commit stage and the cheating sender is trying to open the commitment as 1 in the reveal stage; the case when a bit 1 is committed can be proved symmetrically.

A *key observation* here is that a cheating sender can win the game above if and only if it can guess the receiver's random choice of the bit c correctly. To see this, note that for the purpose of cheating successfully, in the reveal stage the sender must send $(a_0, 1-a_1)$ when $c = 0$, or $(1-a_0, a_1)$ when $c = 1$, to the receiver; this is because the receiver will check the correctness of a_c (but not a_{1-c}). This implies that a successful sender should guess the receiver's random choice of the bit c correctly. The converse holds trivially.

Since the receiver's only message in the commit stage, i.e. the subsets (I_0, I_1), contains no information about the bit c (the sender just saw two random disjoint subsets of size $n/3$), it follows that the probability of the sender winning the game is no more than $1/2$.

The honest-binding game w.r.t. the simplified CLS scheme consists of n copies of the atomic honest-binding game above running in parallel. Since the random bits c's corresponding to each copy of the atomic game are *independent*, the probability of the sender winning all copies of the atomic

game is no more than 2^{-n}. This establishes that the simplified CLS scheme is unconditionally honest-binding.

An attack against the purification-hiding property. Consider a running of the atomic scheme in which the receiver performs a unitary simulation of each of its non-unitary operation as prescribed by the scheme, including the measurement of each qubit $|x_i\rangle_{\theta_i}$ in the basis $\hat{\theta}_i$, as well as the random coin tosses corresponding to the choices of $\hat{\theta}_i, c$ and I_0, I_1. Note that the receiver's measurement of each received qubit in the bases $\hat{\theta}_i$'s is *independent* of its choices of the bit c and the subsets I_0, I_1. Thus, this measurement can be *postponed* to the *beginning* of step (R4) in commit stage; let U be the unitary transformation that simulates this new step. Once the commit stage is finished, the cheating receiver can perform as follows to guess the committed bit b:

1. Perform $U^\dagger$ to roll its system back to the state in which the received qubits $|x_i\rangle_{\theta_i}$'s have not yet been measured.

2. For each qubit $|x_i\rangle_{\theta_i}$, $i = 1, 2, \ldots, n$, measure it in the basis θ_i that is received in step (S1) to obtain x_i.

3. Compute a_0, a_1 from $\hat{a}_0, \hat{a}_1$ and $x_1, \ldots, x_n$; that is, let $a_0 = \bigoplus_{i \in I_0} x_i \oplus \hat{a}_0$, and $a_1 = \bigoplus_{i \in I_0} x_i \oplus \hat{a}_1$. Output $b = a_0 \oplus a_1$.

In this way, the receiver can guess the committed bit b correctly with certainty. The simplified CLS scheme is *not* purification-hiding.

6 A round-collapse theorem

In this section, we first prove a round-collapse theorem which roughly states that any interactive quantum bit commitment scheme can be compiled into a non-interactive one of the generic form (Definition 2). This can also be viewed as a generalization of transforming an arbitrary non-interactive quantum bit commitment scheme into the generic form [YWLQ15, FUYZ20]. As an immediate application, we can compile Naor's bit commitment scheme [Nao91] to get a non-interactive statistically-binding quantum bit commitment scheme, though this result was known before [YWLQ15]. Two more non-trivial applications of our round-collapse theorem are referred to the subsequent section.

The statement of our round-collapse theorem is as below.

Theorem 3 (Round-collapse) *If a quantum bit commitment scheme is secure against the purification attack (or equivalently, its purification is semi-honest secure), then it can be compressed into a non-interactive one of the generic form (Definition 2) with the same flavors of the hiding and binding properties.*

The core of the compiler to achieve the round-collapse is described in Figure 4. The *high-level idea* of its construction is to delegate all computations of the *purified* scheme in the commit stage to the new sender, while the new receiver can check the whole computation in the reveal stage later by the virtue of the *reversibility* of quantum computation.

Proof: We first consider a special case in which there are *no* intermediate verifications during the commit stage of the given interactive quantum bit commitment scheme. Generally, intermediate verifications may cause some party to abort prematurely (i.e. before completing the commit stage),

Assumption: there are *no* inner verifications within the commit stage of the given interactive quantum bit commitment scheme.

Commit stage: the new sender simulates the *honest* execution of the commit stage of the *purified* scheme in the way as stated in Subsection 5.2 such that the whole system is initialized in the all $|0\rangle$'s state. At the end, it sends the quantum registers $(\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B})$ to the receiver as the commitment.

Reveal stage: the new sender sends the remainder registers $(\mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A})$ to the receiver, who then does the *reverse computation* to check if the whole system returns to all $|0\rangle$'s state.

Figure 4: The core compiler for the round-collapse

which we do not take care for the moment for simplicity. In this special case, we construct a *compiler* as described in Figure 4 which can compress rounds of the given interactive quantum bit commitment scheme.

Formally, let Q_b ($b \in \{0,1\}$) denote the quantum circuit that simulates the honest execution of the commit stage of the purified scheme when the bit b is committed. It performs on quantum registers $(\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B}, \mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A})$, treating the first and the last triple quantum registers as the registers C and R in Definition 2, respectively.

We are next to prove the correctness of the compiler; that is, the scheme represented by the quantum circuit pair (Q_0, Q_1) indeed gives rise to a non-interactive quantum bit commitment scheme with the same flavors of hiding and binding properties as the original scheme.

Hiding. We show that the honest-hiding property of the purified scheme directly translates into that of the compressed scheme (Q_0, Q_1). Indeed, consider an honest execution of the commit stage of the purified scheme. If the purified scheme is statistically (resp. computationally) honest-hiding, then the states of the registers $(\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B})$ at the end of the commit stage when 0 respective 1 are committed will be statistically (resp. computationally) indistinguishable. This concludes that the scheme (Q_0, Q_1) is statistically (resp. computationally) hiding.

Binding. We show that the honest-binding property of the purified scheme translates into the binding property of the compressed scheme (Q_0, Q_1).

Consider the moment at the end of the commit stage in an honest execution of the purified scheme when a bit 0 is committed. The whole system $(\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B}, \mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A})$ will then be in the state $Q_0 |0\rangle$. The honest-binding property (Definition 9) of the purified scheme implies that *no cheating sender* — either computationally unbounded in case of statistically honest-binding or polynomial-time bounded in case of computationally honest-binding — can transform the quantum state $Q_0 |0\rangle$ into another one whose projection on the vector $Q_1 |0\rangle$ is non-negligible, by just operating on the subsystem $(\mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A})$. This is because for otherwise, a cheating sender would first transform the state $Q_0 |0\rangle$ into a state that is non-negligibly close to $Q_1 |0\rangle$ at the beginning of the reveal stage, and then proceed honestly to reveal the bit 1. But this should lead the receiver to accept with non-negligible probability, contradicting to the honest-binding property of the purified scheme. We note that the cheating sender may additionally use some auxiliary input state in the reveal stage (r.f. Definition 9), but almost the same argument as above goes through.

Henceforth, the scheme (Q_0, Q_1) is statistically (resp. computationally) binding if the purified scheme is statistically (resp. computationally) honest-binding.

Combining the hiding and binding properties established above, it follows that the non-interactive quantum bit commitment scheme (Q_0, Q_1) enjoys the same flavors of the hiding and binding properties as the given scheme.

Extension. We can extend the proof above to the case where there are intermediate *verifications* during the commit stage of the interactive quantum bit commitment scheme. In case that all verifications will always pass if both parties follow the scheme honestly — this is indeed the case when the *semi-honest* security is considered — we can safely remove these verifications without disturbing the state at the end of the commit stage and get back to the case as discussed above.

In case that some verifications may fail (and the corresponding party aborts) with *negligible* probability[7] even if both parties follow the scheme honestly, removing them will only cause a negligible disturbance to the state conditioned on neither parties aborting before the end of the commit stage. Such a disturbance will only affect the hiding and binding properties of the compressed scheme by a negligible additive factor. ■

Remark. In the proof above, we actually only proved that the compressed scheme (Q_0, Q_1) is *semi-honest* secure. But by the virtue of Theorem 2, it follows that the scheme (Q_0, Q_1) is fully secure against an arbitrary attack as well.

The proof of Theorem 3 actually gives a general explicit procedure to *compress* an arbitrary interactive quantum bit commitment scheme. We will refer to the scheme after the compression the "compressed scheme" hereafter. Let us highlight this in the following definition.

Definition 13 (Compressed scheme) Given an arbitrary interactive quantum bit commitment scheme, its associated *compressed scheme* is obtained by applying the compiler given in Figure 4.

Since the purification attack is a special kind of attack among all possible attacks, the following theorem is an immediate corollary of Theorem 3.

Theorem 4 *Any interactive quantum bit commitment scheme (secure against an arbitrary attack), in particular the post-quantum (classical) bit commitment scheme, can be compressed into a non-interactive one of the generic form (Definition 2) with the same flavors of the hiding and binding properties.*

6.1 Application: compress Naor's scheme

As the first application, we can apply the collapse theorem (Theorem 3) to Naor's construction of statistically-binding bit commitment [Nao91], obtaining a quantum computationally-hiding statistically-binding bit commitment scheme. Actually, similar result was already known before [YWLQ15]. Two more (involved) applications of the collapse theorem are referred to the next section.

Given a quantum-secure pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^{3n}$, a statistically-binding bit commitment scheme can be constructed in the following way [Nao91]. Its *commit* stage proceeds in two rounds: the receiver first sends a uniformly random string $r \in \{0,1\}^{3n}$ to the sender. In response, the sender chooses a uniformly random string $s \in \{0,1\}^n$, and if a bit 0 is to commit, then the sender sends $G(s)$ to the receiver; if a bit 1 is to commit, then the sender sends $G(s) \oplus r$ (the "$\oplus$" denotes the xor bitwisely) to the receiver. The *reveal* stage is canonical; namely, the sender sends its random coin tosses s to the receiver for verification.

[7] We always assume that the completeness error is negligible.

To compress Naor's scheme, we consider an honest execution of the commit stage of the *purified* Naor's scheme. At the end of the commit stage, when a bit 0 is committed the whole system will be in the state

$$Q_0 |0\rangle \stackrel{def}{=} \frac{1}{\sqrt{2^{4n}}} \sum_{\substack{s\in\{0,1\}^n,\\ r\in\{0,1\}^{3n}}} |s\rangle^{E_A} |G(s), r\rangle^{E_{S,A}} |G(s), r\rangle^{E_{S,B}} ; \tag{7}$$

and when a bit 1 is committed the whole system will be in the state

$$Q_1 |0\rangle \stackrel{def}{=} \frac{1}{\sqrt{2^{4n}}} \sum_{\substack{s\in\{0,1\}^n,\\ r\in\{0,1\}^{3n}}} |s\rangle^{E_A} |G(s)\oplus r, r\rangle^{E_{S,A}} |G(s)\oplus r, r\rangle^{E_{S,B}} \tag{8}$$

By the compiler within the proof of Theorem 3, the compressed scheme given by the quantum circuit pair (Q_0, Q_1) is as follows: in the commit stage the sender prepares the quantum state $Q_b |0\rangle$ when a bit $b \in \{0,1\}$ is to commit, and the quantum registers $\mathsf{E}_{S,B}$ will be sent to the receiver as the commitment; later in the reveal stage, the quantum register $(\mathsf{E}_A, \mathsf{E}_{S,A})$ will be sent as the decommitment to the receiver.

Since Naor's scheme is quantum-secure given that the pseudorandom generator $G(\cdot)$ is secure against any polynomial-time quantum distinguishers [HSS11], applying Theorem 3 we conclude that the scheme (Q_0, Q_1) is computationally hiding and statistically binding.

Remark. Compared with the scheme (Q_0, Q_1) given in the equations (7) and (8), the construction in [YWLQ15] is simpler and its proof is more direct. In spite of this, their ideas in the nutshell are nevertheless the same. Further, our approach via the round-collapse theorem here is more general, indicating that the quantization of Naor's scheme in [YWLQ15] is not an accident.

7 Application: yet another two constructions of non-interactive computationally-binding quantum bit commitment

In this section, we apply Theorem 3 to *compress* the CLS scheme [CLS01] and the NOVY scheme [NOVY98], obtaining yet another two constructions of non-interactive *computationally-binding* quantum bit commitment that are previously unknown. The main technical part of this section lies in showing that both the CLS and the NOVY schemes are secure against the purification attack, which will be proved in two separate subsections. Readers who are not interested in these two applications of the round-collapse theorem can safely skip this section.

To simplify the notation in our security analyses, we will drop the auxiliary quantum state that the adversary may receive (as specified, explicitly or implicitly, in Definitions 8 and 9). We can do this because our analyses will be black-box without rewinding; one can easily see that almost the same arguments go through even if the auxiliary quantum state is taken into account.

7.1 Compress the CLS scheme

The original CLS scheme [CLS01] is an *interactive* computationally-binding quantum bit commitment scheme; it is built on the statistically-binding (interestingly, of the opposite flavor) classical/quantum bit commitment [CLS01, FUYZ20]. Combined with Theorem 4, it immediately follows that the compressed CLS scheme (by the compiler specified within the proof of Theorem 3) is statistically hiding and computationally binding. However, showing that the CLS scheme is

Security parameter: n

Commit stage: Let $b \in \{0,1\}$ be the bit to commit.

- (**S1**) For $i = 1, 2, \ldots, n$, the sender chooses a bit $x_i \xleftarrow{\$} \{0,1\}$ and a basis $\theta_i \xleftarrow{\$} \{+, \times\}$, sending the qubit $|x_i\rangle_{\theta_i}$ to the receiver.
- (**R2**) For $i = 1, 2, \ldots, n$, the receiver chooses a basis $\hat{\theta}_i \xleftarrow{\$} \{+, \times\}$ and measures each received qubit $|x_i\rangle_{\theta_i}$ in the basis $\hat{\theta}_i$, obtaining the outcome $\hat{x}_i$. Then commit to $(\hat{\theta}_i, \hat{x}_i)$ bitwisely using a statistically-binding classical/quantum bit commitment scheme. (We assume that the bases "+" and "×" are encoded as 0 and 1, respectively.)
- (**S3**) The sender sends all θ_i's, $i = 1, 2, \ldots, n$, to the receiver.
- (**R4**) The receiver chooses a random bit $c \xleftarrow{\$} \{0,1\}$, as well as two random subsets of indices $I_0, I_1 \subset [n]$ such that $|I_0| = |I_1| = n/3$, $I_0 \cap I_1 = \emptyset$, and $\theta_i = \hat{\theta}_i$ for each $i \in I_c$. Then send (I_0, I_1) to the sender.
- (**S5**) The sender chooses a bit $a_0 \xleftarrow{\$} \{0,1\}$ and sets $a_1 = a_0 \oplus b$. Then compute $\hat{a}_0 = \bigoplus_{i \in I_0} x_i \oplus a_0$, $\hat{a}_1 = \bigoplus_{i \in I_1} x_i \oplus a_1$, and send $(\hat{a}_0, \hat{a}_1)$ to the receiver.
- (**R6**) The receiver computes the bit $d_c = \bigoplus_{i \in I_c} \hat{x}_i \oplus \hat{a}_c$.

Reveal stage:

- The sender sends the bits b and (a_0, a_1) to the receiver.
- The receiver verifies that $b = a_0 \oplus a_1$ and $d_c = a_c$.

Figure 5: The atomic scheme QBC, which composed in parallel gives the CLS scheme

secure against an arbitrary quantum attack a-prior, as done in [CLS01, FUYZ20], turns out to be quite involved.

Interestingly, Theorem 3 tells us that just for the purpose of the compression it suffices to restrict to consider the security against the purification attack of the CLS scheme, whose analysis turns out to be much simpler than the original one for the full security [CLS01, FUYZ20]. We thus achieve the least number of rounds and even simpler analysis simultaneously. In the rest of this subsection, we will focus on showing the security against the purification attack of a somewhat simplified CLS scheme. Detail follows.

The scheme. The CLS scheme is basically the *parallel composition* of the atomic (interactive) scheme as described in Figure 5, which we denote by $\mathrm{QBC}(n)$, with the security parameter n which we often drop to simplify the notation. Let $\mathrm{QBC}(n)^{\otimes n}$ denote the *parallel* composition of n copies of the scheme $\mathrm{QBC}(n)$. This scheme is almost the CLS scheme given in [CLS01], except that all *intermediate verifications* of the commitments by the sender are removed. In spite of this, we still call it CLS scheme in this paper.

To show that the compressed CLS scheme is secure, we suffice to prove that the CLS scheme $\mathrm{QBC}(n)^{\otimes n}$ is secure against the purification attack (Theorem 3), or the purified CLS scheme is

both unconditionally honest-hiding and computationally honest-binding. We will prove them in Lemma 14 and Lemma 15, respectively.

Remark. Since the atomic CLS scheme QBC is somewhat complex, we do not intend to explicitly write out the quantum circuit pair ensemble $\{Q_0(n), Q_1(n)\}_n$ corresponding to the compressed CLS scheme, though which is straightforward following the compiler described in Figure 4. Jumping ahead, we will do this for the comparably simpler NOVY scheme in the next subsection (Subsection 7.2).

Before giving formal proofs, let us first fix the bit commitment scheme used within the atomic scheme QBC (step (**R2**)). By Theorem 4, we can assume without loss of generality that the scheme is a generic non-interactive quantum bit commitment scheme represented by an ensemble of quantum circuit pair $\{(Q_0(n), Q_1(n))\}_n$ (Definition 2). To further simplify our security analysis, we can assume without loss of generality that this scheme is *perfectly* binding [FUYZ20].

Lemma 14 *The purification of the scheme QBC$(n)^{\otimes n}$ is unconditionally honest-hiding. (Or, the CLS scheme QBC$(n)^{\otimes n}$ is unconditionally purification-hiding.)*

Proof: We show that the CLS scheme QBC$(n)^{\otimes n}$ is unconditionally honest-hiding, and which extends to its purification.

The proof that the CLS scheme QBC$(n)^{\otimes n}$ is unconditionally honest-hiding follows almost the same line as the proof of that the simplified CLS scheme (r.f. Section 5.4) is unconditionally honest-hiding. This is because if we compare the two atomic schems described in Figure 5 and Figure 3, respectively, we find that the only difference lies in that in the former scheme the receiver additionally sends commitments to $(\hat{\theta}_i, \hat{x}_i)$'s to the sender in step (**R2**)[8]. But these commitments clearly *cannot* help the *semi-honest* receiver in cheating.

To show that the unconditional honest-hiding property of the scheme QBC$(n)^{\otimes n}$ is *preserved* after the purification, it suffices to show that all *collapses* caused by the receiver's *non-unitary* operations are still enforced even *after* the purification. Indeed, the receiver has two non-unitary operations prescribed by the atomic scheme QBC:

1. Measure each received qubit $|x_i\rangle_{\theta_i}$ in step (**R2**).
2. Randomly choose the bit c, as well as the subsets I_0, I_1, in step (**R4**).

For the first non-unitary operation, the commitment to each $(\hat{\theta}_i, \hat{x}_i)$ in step (**R2**) amounts to measuring $(\hat{\theta}_i, \hat{x}_i)$ (but without revealing them to the sender), by the virtue of the perfect binding property of the quantum bit commitment scheme (Q_0, Q_1) plugged in[9]. Thus, the state of the whole system still will collapse to the one associated with the occurrence of $(\hat{\theta}_i, \hat{x}_i)$, $i \in \{1, 2, \ldots, n\}$, even after the receiver's measurements are purified.

For the second non-unitary operation, with overwhelming probability, about half of $\hat{\theta}_i$'s are equal to θ_i's; that is, with probability exponentially close to one, $n/2.1 < \left|\left\{i \mid \theta_i = \hat{\theta}_i\right\}\right| < n/1.9$. Conditioned on this event happening, the receiver's private coin c can be *determined* from the subsets (I_0, I_1). In turn, the qubit storing the (private) coin c will collapse at the moment the subsets (I_0, I_1) are sent to the sender in step (**R4**). As such, the state of the whole system still

[8] If these commitments were removed from the scheme QBC, then its step (**S3**) could be merged into step (**S1**), resulting in the same atomic scheme as described in Figure 3.

[9] A hypothetical measurement known as the *commitment measurement* performed on each quantum bit commitment can be introduced without affecting the security; its detail is referred to [FUYZ20].

will collapse to the one associated with the occurrence of (I_0, I_1, c) before the purification of the receiver's random coin tosses.

Therefore, the unconditional honest-hiding property of the CLS scheme $\mathrm{QBC}(n)^{\otimes n}$ extends to its purification. This finishes the proof of the lemma. ■

As opposed to the proof of the unconditional purification-hiding property of the CLS scheme $\mathrm{QBC}(n)^{\otimes n}$, there seems no obvious way to show that the collapses caused by the honest sender's non-unitary operations, e.g. choosing the x_i's in step (**S1**) and choosing the a_0, a_1 in step (**S5**), still will be enforced after the purification. Thus, the unconditional honest-binding property of the CLS scheme $\mathrm{QBC}(n)^{\otimes n}$ (which follows similar to that of the simplified CLS scheme discussed in Section 5.4.) does not extend to its purification straightforwardly. In spite of this, we can take a similar analysis as the one in [CLS01]. But since now we are to argue the security against the purification rather than an arbitrary attack, the analysis can be greatly simplified.

Lemma 15 *The purification of the scheme $QBC(n)^{\otimes n}$ is computationally honest-binding. (Or, the CLS scheme $QBC(n)^{\otimes n}$ is computationally purification-binding.)*

Proof: For our analysis, we define a sequence of *atomic* schemes as follows[10]:

1. U-QBC. Obtained from the scheme QBC by letting the receiver commit to $2n$ *uniformly random* bits, rather than $(\hat{\theta}_i, \hat{x}_i)$'s, in step (**R2**).

2. S-QBC. Obtained from the scheme U-QBC by *removing* the receiver's commitments in step (**R2**). Now since step (**S3**) of the sender is independent of step (**R2**) of the receiver, we can first switch them, and then merge the former into step (**S1**), and the latter into step (**R2**). For clarity, the resultng scheme S-QBC is depicted in Figure 6.

3. M-QBC. Obtained from the scheme S-QBC by introducing measurements of each qubit $|x_i\rangle_{\theta_i}$ in the basis θ_i once it is sent in step (**S1**). These *hypothetical* measurements are introduced purely for the purpose of the security analysis.

The roadmap of our analysis is depicted as below:

$$\begin{array}{c}\text{The scheme } \mathrm{QBC}(n)^{\otimes n} \text{ is } \textit{computationally} \text{ purification-binding}\\ \Uparrow \boxed{\textbf{Reduction 1}}\\ \text{The scheme U-QBC}(n)^{\otimes n} \text{ is } \textit{unconditionally} \text{ purification-binding}\\ \Uparrow \boxed{\textbf{Reduction 2}}\\ \text{The scheme S-QBC}(n)^{\otimes n} \text{ is } \textit{unconditionally} \text{ purification-binding}\\ \Uparrow \boxed{\textbf{Reduction 3}}\\ \text{The scheme M-QBC}(n)^{\otimes n} \text{ is } \textit{unconditionally} \text{ purification-binding}\end{array}$$

To establish the purification-binding property of various schemes above, we consider the corresponding purification-binding games described in Definition 11. For simplification, in the analysis below we just focus on the case $b = 0$ (i.e. a bit 0 is committed) of each game without explicit mention; the case $b = 1$ can be established symmetrically.

Reduction 1. This is the most technical part of the whole analysis, which is deferred to Appendix B. Basically, we use the *hybrid* argument to replace all receiver's commitments one by one in step (**R2**) of the atomic scheme QBC.

[10]The notations of various schemes we introduced are *not* exactly the same as those in [Lég00, CLS01].

Security parameter: n

Commit stage: Let $b \in \{0,1\}$ be the bit to commit.

- (**S1**) For $i = 1, 2, \ldots, n$, the sender chooses a bit $x_i \xleftarrow{\$} \{0,1\}$ and a basis $\theta_i \xleftarrow{\$} \{+,\times\}$. Send the basis θ_i and the qubit $|x_i\rangle_{\theta_i}$ to the receiver.
- (**R2**) For $i = 1, 2, \ldots, n$, the receiver chooses a basis $\hat{\theta}_i \xleftarrow{\$} \{+,\times\}$ and measures each received qubit $|x_i\rangle_{\theta_i}$ in the basis $\hat{\theta}_i$, obtaining the outcome $\hat{x}_i$. Then choose a random bit $c \xleftarrow{\$} \{0,1\}$, as well as two random subsets of indices $I_0, I_1 \subset [n]$ such that $|I_0| = |I_1| = n/3$, $I_0 \cap I_1 = \emptyset$, and $\theta_i = \hat{\theta}_i$ for each $i \in I_c$. Send (I_0, I_1) to the sender.
- (**S3**) The sender chooses a bit $a_0 \xleftarrow{\$} \{0,1\}$ and sets $a_1 = a_0 \oplus b$. Then compute $\hat{a}_0 = \bigoplus_{i \in I_0} x_i \oplus a_0$, $\hat{a}_1 = \bigoplus_{i \in I_1} x_i \oplus a_1$, and send $(\hat{a}_0, \hat{a}_1)$ to the receiver.
- (**R4**) The receiver computes the bit $d_c = \bigoplus_{i \in I_c} \hat{x}_i \oplus \hat{a}_c$.

Reveal stage:

- The sender sends (b, a_0, a_1) to the receiver.
- The receiver verifies that $b = a_0 \oplus a_1$ and $d_c = a_c$.

Figure 6: The atomic scheme S-QBC

Reduction 2. Consider the purification-binding game w.r.t. the scheme U-QBC$(n)^{\otimes n}$, whose commit stage is just that of n copies of the purification-binding game w.r.t. the atomic scheme U-QBC running in parallel. Intuitively, the commitments described in step (**R2**) of the scheme U-QBC does not contain any information about the (honest) receiver's random bits c's (also chosen in step (**R2**); n bits in total) that can help the sender win the game, hence can be removed.

In more detail, a key observation is that whether for the purification-binding game w.r.t. the scheme U-QBC$(n)^{\otimes n}$ or the scheme S-QBC$(n)^{\otimes n}$, a cheating sender can win the game if and only if it can guess the (honest) receiver's all random bits c's correctly. To see this, note that for the purpose of cheating successfully, in the reveal stage of each copy of the purification-binding game w.r.t. the atomic scheme U-QBC or S-QBC, the cheating sender must send corresponding $(a_0, 1-a_1)$ when $c = 0$, or $(1-a_0, a_1)$ when $c = 1$, to the receiver; this is because the receiver will check the correctness of a_c (but not a_{1-c}). Combining this observation with that the receiver's commitments to random bits as described by step (**R2**) of the scheme U-QBC do not contain any information about the receiver's random bits c's, removing all these commitments in the purification-binding game w.r.t. the scheme U-QBC$(n)^{\otimes n}$ will not affect the sender's success probability of cheating. But removing these commitments gives exactly the same commit stage as that of the purification-binding game w.r.t. the scheme S-QBC$(n)^{\otimes n}$. Reduction 2 follows.

Reduction 3. Consider the purification-binding game w.r.t. the scheme S-QBC$(n)^{\otimes n}$, whose commit stage is just that of n copies of the purification-binding game w.r.t. the atomic scheme S-QBC running in parallel. Note that introducing the hypothetical measurements as in the description of the scheme M-QBC to this game will result in the purification-binding game w.r.t. the scheme M-QBC$(n)^{\otimes n}$, which will affect nothing but $\hat{x}_i$'s (i.e. the receiver's private measurement outcomes) where $i \in I_{1-c}$ (or $\hat{\theta}_i \neq \theta_i$) in the commit stage of each copy of the atomic game. Henceforth, neither the sender's view nor the receiver's verification (of d_c's, where only $\hat{x}_i$'s for $i \in I_c$ matter) in the subsequent reveal stage will change. This implies that the sender's probability of winning the game will not change after introducing the hypothetical measurements. Reduction 3 follows.

The scheme M-QBC$(n)^{\otimes n}$ **is unconditionally purification-binding**. We first argue that the scheme M-QBC$(n)^{\otimes n}$ is unconditionally honest-binding. Then we show that this binding property extends to the purified scheme; this is equivalent to say that the scheme M-QBC$(n)^{\otimes n}$ is unconditionally purification-binding.

First consider the honest-binding game w.r.t. the scheme M-QBC$(n)^{\otimes n}$, which is n copies of the honest-binding game w.r.t. the atomic scheme M-QBC running in parallel. Note that within each atomic game, the hypothetical measurements will become redundant; this is because each qubit $|x_i\rangle_{\theta_i}$ has already been collapsed by the honest-but-curious sender's measurement in the basis θ_i in step (**S1**). Hence, the honest-binding game w.r.t. the atomic scheme M-QBC is exactly the game w.r.t. the atomic scheme (of the simplified CLS scheme) described in Figure 3. Henceforth, as we have already argued in Subsubsection 5.4.2, the scheme M-QBC$(n))^{\otimes n}$ is unconditionally honest-binding.

Now we turn to consider the purification-binding game w.r.t. the scheme M-QBC$(n))^{\otimes n}$, which is n copies of the purification-binding game w.r.t. the atomic scheme M-QBC running in parallel. If we can show that all collapses of the sender's (quantum) messages in the corresponding honest-binding game are still enforced in this purification-binding game, then the probability that the sender can win the purification-binding game will be the same as that of the honest-binding game, and we are done. To see this, consider the atomic purification-binding game (w.r.t. the atomic scheme M-QBC). First, we note that the bases θ_i's chosen in the step (**S1**) will be collapsed by

the honest receiver. Second, the x_i's chosen in the same step will be collapsed by the hypothetical measurements. Third, in step (**S3**), since bits a_0, a_1 are uniquely determined by bits $\hat{a}_0, \hat{a}_1$ and $x_1, \ldots, x_n$, they will collapse after $\hat{a}_0, \hat{a}_1$ are collapsed by the honest receiver. As such, all collapses happened in the honest-binding game are still enforced in the corresponding purification-binding game.

This finishes the proof of that the scheme M-QBC$(n)^{\otimes n}$ is unconditionally purification-binding. Combining with Reduction 1, 2, and 3, this finishes the proof of the lemma. ■

Combing Lemma 14, Lemma 15, and Theorem 3, we have the following theorem as an immediate corollary.

Theorem 5 *The compressed CLS quantum bit commitment scheme is quantum statistically hiding and computationally binding.*

7.2 Compress the NOVY scheme

The *classical* NOVY scheme [NOVY98] gives a construction of computationally-binding bit commitment based on any one-way *permutation*. We naturally will ask, is the NOVY scheme secure against the quantum attack when the underlying one-way permutation is also *quantum-secure*? The main difficulty in extending the classical argument for the binding property [NOVY98] to the quantum setting lies in the *rewinding*, which is generally impossible in the quantum setting [vdG97]. Moreover, Brassard, Crépeau, Mayers, and Salvail [BCMS98] have shown an attack which indeed breaks the binding property that is common in the classical setting, but it *does not* break the well-accepted quantum *sum-binding* property. That is, the NOVY scheme with a quantum-secure one-way permutation plugged in is possibly sum-binding, but unfortunately we still do not know how to prove this. Instead, interestingly, a *quantum* construction of computationally-binding quantum bit commitment is given [DMS00]. This construction is intriguing in that its commit stage is *non-interactive*, in contrast to the polynomial rounds of the classical construction [NOVY98]. Its follow-up works finally manage to relax the complexity assumption to the quantum-secure one-way *function* [KO09, KO11].

In the below, we will show that the NOVY scheme with a quantum-secure one-way permutation plugged in is *secure against the purification attack*, which thus can be *compressed* into a non-interactive computationally-binding quantum bit commitment scheme by our round-collapse theorem (Theorem 3). The analysis here is much simpler than the one in [NOVY98].

Formally, we prove the following theorem. For self-containment, we reproduce the NOVY scheme [NOVY98] in Figure 7.

Theorem 6 *The compressed NOVY quantum bit commitment scheme with a quantum-secure one-way permutation plugged in is perfectly-hiding and computationally-binding. In particular, this scheme can be represented by the quantum circuit pair ensemble* $\{(Q_0(n), Q_1(n))\}_n$ *such that*

$$\begin{aligned} Q_0(n)\left|0\right\rangle &= \frac{1}{2^{\frac{n(n+1)}{4}}} \sum_{x,h^1,\ldots,h^{n-1}} \left|x, f(x), h^1, \ldots, h^{n-1}, h^1 f(x), \ldots, h^{n-1} f(x), a\right\rangle^R \\ &\qquad \otimes \left|h^1, \ldots, h^{n-1}, h^1 f(x), \ldots, h^{n-1} f(x), a\right\rangle^C, \qquad (9) \\ Q_1(n)\left|0\right\rangle &= \frac{1}{2^{\frac{n(n+1)}{4}}} \sum_{x,h^1,\ldots,h^{n-1}} \left|x, f(x), h^1, \ldots, h^{n-1}, h^1 f(x), \ldots, h^{n-1} f(x), 1-a\right\rangle^R \\ &\qquad \otimes \left|h^1, \ldots, h^{n-1}, h^1 f(x)_1, \ldots, h^{n-1} f(x), 1-a\right\rangle^C, \qquad (10) \end{aligned}$$

Commit stage: Let $b \in \{0,1\}$ be the bit to commit.

- The sender chooses a string $x \xleftarrow{\$} \{0,1\}^n$ and computes $y = f(x)$, where $f : \{0,1\}^n \to \{0,1\}^n$ is an aribitrary one-way permutation.
- For $k = 1, 2, \ldots, n-1$, the receiver chooses a string $h^k \xleftarrow{\$} 0^{k-1}1\{0,1\}^{n-k}$ and sends it to the sender, who replies with the bit $c_k = h^k y$, i.e. the inner product of h^k and y if we view them as vectors over the field $\mathbb{F}_2$.
- Let $(y_0, y_1) \in \{0,1\}^n$ be the two solutions in the lexicographical order of the equation system $h^k y = c_k$, $k = 1, \ldots, n-1$. Let the bit $a \in \{0,1\}$ be such that $y = y_a$. The sender then sends the bit $d = a \oplus b$ to the receiver.

Reveal stage:

- The sender sends the bit b and the string x to the receiver.
- The receiver first determines the bit a from $f(x)$: 0 if $f(x)$ is the lexicographically smaller solution of the equation system $h^k y = c_k$, $k = 1, \ldots, n-1$, and 1 otherwise. Then the receiver checks that $d = a \oplus b$; accept if yes, reject otherwise.

Figure 7: The NOVY scheme

where the x is summing over $\{0,1\}^n$, and h^k (for $k = 1, 2, \ldots, n-1$) over $0^{k-1}1\{0,1\}^{n-k}$.

Proof: The expressions of $Q_0(n)$ and $Q_1(n)$ are obtained by applying the compiler described in Figure 4 to the NOVY scheme described in Figure 7. By the round-collapse theorem (Theorem 3), the correctness of the scheme $\{(Q_0(n), Q_1(n))\}_n$ follows by combining Lemma 17 and Lemma 16 that are to be proved shortly below. ■

Lemma 16 *The NOVY scheme with a quantum-secure one-way permutation plugged in is perfectly honest-hiding and computationally honest-binding.*

Proof: The *perfect* honest-hiding property follows by exactly the same argument as the one in the classical setting. At a high level, this is because the two distributions of the messages exchanged during the commit stage corresponding to $f(x) = y_0$ and $f(x) = y_1$ are *identical*; we ommit the detail here, which is trivial. In the below, we will focus on showing the *computational* honest-binding property of the scheme, whose proof is also almost a reproduction of the classical one (which is folklore).

Consider the honest-binding game w.r.t. the NOVY scheme in which a bit 0 is committed; the case when a bit 1 is committed can be proved symmetrically. For contradiction, suppose that a cheating sender S^* of the reveal stage succeeds in opening the commitment as 1 with non-negligible probability. Given the oracle access to S^*, we construct an *inverter* I^* of the quantum-secure one-way permutation $f(\cdot)$ as follows: on input $y' \in \{0,1\}^n$,

1. Choose $y \xleftarrow{\$} \{0,1\}^{n-1} \circ (1 - y'_n)$, where the y'_n denotes the n-th bit of the y' and the operator "$\circ$" denotes the concatenation of two binary strings.

2. For $k = 1, 2, \ldots, n-1$ do: $h^k \stackrel{\$}{\leftarrow} 0^{k-1}1 \circ \{0,1\}^{n-k}$ subject to $h^k y = h^k y'$; let $c_k = h^k y$.

3. If $y < y'$, then $a \leftarrow 0$; otherwise, $a \leftarrow 1$.

4. Output $x' \leftarrow S^*(y, h^1, \ldots, h^{n-1}, c_1, \ldots, c_{n-1}, 1-a)$.

We are left to show that this inverter indeed breaks the security of the one-way permutation $f(\cdot)$.

Let $H = (H^1, H^2, \ldots, H^{n-1})$, where the random variable $H^k = 0^{k-1}1 \circ U_{n-k}$ and U_{n-k} is uniformly distributed over $\{0,1\}^{n-k}$. We introduce an *experiment* $\mathcal{E}_1$ as: $x \stackrel{\$}{\leftarrow} \{0,1\}^n$, $y = f(x)$, $h \stackrel{\$}{\leftarrow} H$. *Intuitively*, the experiment $\mathcal{E}_1$ is to simulte the commit stage of the honest-binding game w.r.t. the NOVY scheme. Let y' be the unique vector such that $hy = hy'$ and $y' \neq y$. We claim that $y_n = 1 - y'_n$. Indeed, let $j = \max\{i \mid 1 \leq i \leq n,\ y_i \neq y'_i\}$; our goal is to show that $j = n$. Suppose for contradiction that $j \leq n-1$. Then for any $h^j \in 0^{j-1}1 \circ \{0,1\}^{n-j}$, since the last $n-j+1$ bits of $y - y'$ are 10^{n-j}, we must have $h^j(y - y') = 1$. But this contradicts with the equation $h^j y = h^j y'$.

We introduce another *experiment* $\mathcal{E}_2$ as: $y' \stackrel{\$}{\leftarrow} \{0,1\}^n$, $y \stackrel{\$}{\leftarrow} \{0,1\}^{n-1} \circ (1 - y'_n)$, $h \stackrel{\$}{\leftarrow} H$ subject to $hy = hy'$. *Intuitively*, the experiment $\mathcal{E}_2$ is to simulate an execution of the first two steps of the inverter I^*.

We claim that the distribution of (y, y', h) in the experiment $\mathcal{E}_1$ is *identical* to that in the experiment $\mathcal{E}_2$; that is, for any (y, y', h),

$$\Pr_{\mathcal{E}_1}[y, y', h] = \Pr_{\mathcal{E}_2}[y, y', h]. \tag{11}$$

Assuming for the moment that this is true, then the success probability of the inverter I^* is exactly that of the cheating sender S^*. But since this probability is non-negligible by our hypothesis, the inverter I^* thus breaks the one-wayness of the one-way permutation $f(\cdot)$. We arrive at a contradiction. Henceforth, the NOVY scheme is computationally honest-binding.

We are left to prove the equation (11). Regarding the experiment $\mathcal{E}_1$, since both the y and h are uniformly distributed, and the y' is uniquely determined by the y and h, we have

$$\Pr_{\mathcal{E}_1}[y, y', h] = \Pr_{\mathcal{E}_1}[y] \cdot \Pr_{\mathcal{E}_1}[h] = \frac{1}{2^n} \cdot \frac{1}{2^{n-1}} \frac{1}{2^{n-2}} \cdots \frac{1}{2}. \tag{12}$$

Regarding the experiment $\mathcal{E}_2$, we have

$$\Pr_{\mathcal{E}_2}[y, y', h] = \Pr_{\mathcal{E}_2}[y'] \cdot \Pr_{\mathcal{E}_2}[y \mid y'] \cdot \Pr_{\mathcal{E}_2}[h \mid y, y'] = \frac{1}{2^n} \cdot \frac{1}{2^{n-1}} \cdot \Pr_{\mathcal{E}_2}[h \mid y, y']. \tag{13}$$

To calculate the $\Pr_{\mathcal{E}_2}[h \mid y, y']$, since the h is chosen uniformly random such that $hy = hy'$ in the experiment $\mathcal{E}_2$, we are to calculate it via of the cardinaliy of the set $\{h \mid h(y - y') = 0\}$. Since $y_n - y'_n = 1$, there are exactly *half* of $h^k \in 0^{k-1}1 \circ \{0,1\}^{n-k}$, for each $1 \leq k \leq n-1$, such that $h^k(y - y') = 0$. It then follows that there are $2^{n-2} \cdot 2^{n-1} \cdots 2 \cdot 1$ h's satisfying $h(y - y') = 0$. As such,

$$\Pr_{\mathcal{E}_2}[h \mid y, y'] = \frac{1}{2^{n-2}} \cdots \frac{1}{2}.$$

Combined with equations (12) and (13), the equation (11) holds.

This finishes the proof of the lemma. ■

Lemma 17 *If the NOVY scheme is quantum semi-honest secure (i.e. honest-hiding and honest-binding), then it is also secure against the purification attack.*

PROOF: We first prove that the NOVY scheme is secure against the purification attack of the receiver; or, the purification of the NOVY scheme is honest-hiding. This follows from the assumption that the NOVY scheme is honest-hiding together with that the receiver is public-coin, in which case Proposition 12 can be applied.

We next prove that the NOVY scheme secure against the purification of the sender; or, the purification of the NOVY scheme is honest-binding. Consider the purification-binding game w.r.t. the NOVY scheme in which a bit 0 is committed. By the purification attack the cheating sender may not meausre the quantum states storing x and $f(x)$ at the beginning of the commit stage. Since the classical messages $(h_1, \ldots, h_{n-1}; c_1, \ldots, c_{n-1}; a)$ exchanged in the commit stage will uniquely determine the x chosen by the sender at the beginning of the commit stage, the corresponding quantum states storing x and $f(x)$ will be enforced to collapse at the end of the commit stage. The case when a bit 1 is committed in the purification-binding game can be proved symmetrically. Hence, the honest-binding property of the NOVY scheme extends to its purification. ■

8 Parallel composition of statistically-binding quantum bit commitments

We know that a general quantum bit commitment scheme can only guarantee the *sum-binding* property (Definition 5). In cryptography, a typical way to commit a string is to commit it *bitwisely* using a bit commitment scheme. We naturally will ask, what binding property can we obtain if we commit a string bitwisely using a generic *quantum* bit commitment scheme? The answer to this question on the *parallel* composition of quantum bit commitments turns out to be elusive, especially w.r.t. the *computationally-binding* quantum bit commitment [CDMS04].

In this section, we study the parallel composition of a generic *statistically-binding* quantum bit commitment scheme, establishing the (almost) strongest binding property that we may hope for. We also show that this binding property implies the CDMS-binding property of quantum string commitment, which is useful in quantum cryptography [CDMS04]. In spite of this, we do not expect the same binding property extends to a generic *computationally-binding* quantum bit commitment scheme [CDMS04].

8.1 Quantum string sum-binding

We first define the sum-binding property of a general quantum string commitment scheme.

Definition 18 (Sum-binding) Suppose that a possibly cheating sender interacts with an honest receiver prescribed by a quantum string commitment scheme, and completes the commit stage. For any string $s \in \{0,1\}^{m(n)}$, where $m(\cdot)$ is a polynomial of the security parameter n, let p_s denote the success probability that the sender can open the commitment as the string s in the reveal stage. We say that this quantum string commitment scheme is *sum-binding* if

$$\sum_{s \in \{0,1\}^m} p_s < 1 + negl(n). \tag{14}$$

Remark. The sum-binding property defined above is very *strong* for quantum string commitment in the following sense. Note that a cheating sender can trivially achieve $\sum_{s \in \{0,1\}^m} p_s = 1$, by committing to an arbitrary superposition of the strings in $\{0,1\}^m$ honestly and then open the

commitment honestly. But showing that the advantage of any cheating sender in opening a commitment is negligible is likely to be hard or even impossible [CDMS04]. The difficulty comes from that there are *exponentially* many strings (2^m, exactly) in $\{0,1\}^m$.

For our purpose, we first extend the honest-binding property of a non-interactive quantum bit commitment scheme (in Definition 2) to a quantitative form.

Definition 19 (ϵ-binding) We say that a generic non-interactive quantum bit commitment scheme $\{(Q_0(n), Q_1(n))\}_n$ as stated in Definition 2 is $\epsilon(n)$-*binding* if the r.h.s. of both inequalities (1) and (2) are replaced with the function $\epsilon(n)$.

We can prove the following theorem.

Theorem 7 *Suppose that a generic non-interactive quantum bit commitment scheme $\{(Q_0(n), Q_1(n))\}_n$ is statistically binding. Then the quantum string commitment scheme obtained by composing it in parallel is sum-binding. Specifically, if the scheme $\{(Q_0(n), Q_1(n))\}_n$ is statistically $\epsilon(n)$-binding where the function $\epsilon(\cdot)$ is negligible, then*

$$\sum_{s\in\{0,1\}^m} p_s \leq 1 + O(m^2\epsilon). \tag{15}$$

The proof of the theorem above will be information-theoretic, thus does not extend to the computational setting. Before giving the proof, we provide some preliminaries first.

When we use the quantum bit commitment scheme $\{Q_0(n), Q_1(n)\}_n$ to commit an m-bit string s bitwisely, the quantum (string) commitment (stored in the quantum register $\mathsf{C}^{\otimes m}$) is given by the quantum state

$$\rho_s = \bigotimes_{i=1}^{m} \rho_{s_i}, \tag{16}$$

where the "s_i" denotes the i-th bit of the string s. The fact below gives an information-theoretic characterization of the success probability of opening a claimed quantum commitment as an arbitrary string.

Fact 20 ([YWLQ15]) *Let $\{Q_0(n), Q_1(n)\}_n$ be a generic non-interactive statistically-binding quantum bit commitment scheme. Given an arbitrary quantum state $\rho \in \mathcal{C}^{\otimes m}$ which is claimed to be the commitment to an m-bit string by a (possible cheating) computationally-unbounded sender, the success probability of opening this commitment as an arbitrary string $s \in \{0,1\}^m$ is at most $\mathrm{F}(\rho, \rho_s)^2$.*

The following lemma states that the honest-binding error decreases *exponentially* w.r.t. the *Hamming distance* between the committed string and the string to reveal.

Lemma 21 ([YWLQ15]) *Let $\{Q_0(n), Q_1(n)\}_n$ be a generic non-interactive quantum bit commitment scheme that is statistically ϵ-binding. Given the honest commitment to a string $s \in \{0,1\}^m$, the success probability of opening it as $s' \in \{0,1\}^m$ by any computationally-unbounded sender is at most $\epsilon^{2\cdot\mathrm{dist}(s,s')}$.*

Proof Sketch: Combining Fact 20 and the equation (16), the success probability

$$\mathrm{F}(\rho_s, \rho_{s'})^2 = \prod_{i=1}^{m} \mathrm{F}(\rho_{s_i}, \rho_{s'_i})^2 \leq \epsilon^{2\cdot\mathrm{dist}(s,s')}.$$

■

We also need a technical lemma as below, whose name comes from the fact that the inequality (17) trivially holds by the Pythagorean theorem in the special case in which vectors $|\psi_s\rangle$ and $|\psi_{s'}\rangle$ are *orthogonal* whenever $s \neq s'$. Its proof is deferred to Appendix C.

Lemma 22 (An approximate Pythagorean theorem) *Let $\{|\psi_s\rangle \in \mathcal{X}\}_{s\in\{0,1\}^{m(n)}}$ be an ensemble of unnormalized vectors, where $\mathcal{X}$ is a Hilbert space, $m(\cdot)$ is a polynomial, and n is the security parameter. For each pair of indices $s, s' \in \{0,1\}^m$ such that $s \neq s'$, the inner product $|\langle\psi_{s'}|\,\psi_s\rangle| \leq \epsilon(n)^{\mathrm{dist}(s,s')}$ for some fixed function $\epsilon(\cdot)$ such that $0 < \epsilon(n) < 1/m(n)$ when n is sufficiently large. Fix coefficients $\alpha_s \geq 0$ for all $s \in \{0,1\}^m$. Then it holds that*

$$\left| \left\| \sum_{s\in\{0,1\}^m} \alpha_s |\psi_s\rangle \right\|^2 - \sum_{s\in\{0,1\}^m} \alpha_s^2 \||\psi_s\rangle\|^2 \right| \leq m^2\epsilon \sum_{s\in\{0,1\}^m} \alpha_s^2. \tag{17}$$

Now we are ready to prove Theorem 7.

Proof of Theorem 7: Let $\rho \in \mathcal{C}^{\otimes m}$ be an arbitrary quantum state which is claimed as the commitment to an m-bit string sent by a cheating sender. Let ρ_s be the quantum state corresponding to the honest commitment to the string $s \in \{0,1\}^m$. By Fact 20, it suffices to prove $\sum_{s\in\{0,1\}^m} \mathrm{F}(\rho,\rho_s)^2 \leq 1 + O(m^2\epsilon)$. Denote by $|\varphi\rangle$ to be an arbitrary purification of ρ. Fact 3 allows us to choose a unit vector $|\psi_s\rangle$ to be a purification of ρ_s such $|\langle\varphi|\psi_s\rangle| = \mathrm{F}(\rho,\rho_s)$. In turn, our goal becomes to prove

$$\sum_{s\in\{0,1\}^n} |\langle\varphi|\psi_s\rangle|^2 \leq 1 + O(m^2\epsilon).$$

Since the projection of the vector $|\varphi\rangle$ on the orthogonal complement of the subspace spanned by $\{|\psi_s\rangle\}_{s\in\{0,1\}^m}$ contributes zero to the summation on the r.h.s. of the inequality above, we can assume without loss of generality that $|\varphi\rangle \in \mathrm{span}\,\{|\psi_s\rangle\}_{s\in\{0,1\}^m}$; that is, we can write

$$|\varphi\rangle = \sum_{t\in\{0,1\}^m} \alpha_t |\psi_t\rangle\,.$$

(We note that the $|\psi_t\rangle$ in the equation above is *not* necessarily orthogonal to $|\psi_{t'}\rangle$ for $t' \neq t$, and $\sum_{t\in\{0,1\}^m} |\alpha_t|^2$ is *not* necessarily equal to one.) Moreover, again without loss of generality we can assume that the α_t's are non-negative reals; for otherwise, we can absorb the corresponding

normalization (complex) phases into $|\psi_t\rangle$'s without affecting other settings. Thus,

$$\begin{aligned}
\sum_{s\in\{0,1\}^m} |\langle\varphi|\psi_s\rangle|^2 &= \sum_{s\in\{0,1\}^m} \Big| \sum_{t\in\{0,1\}^m} \alpha_t \langle\psi_t|\psi_s\rangle \Big|^2 \\
&\le \sum_{s\in\{0,1\}^m} \sum_{t\in\{0,1\}^m} \alpha_t^2 \, |\langle\psi_t|\psi_s\rangle|^2 \qquad \text{(triangle inequality)} \\
&= \sum_{t\in\{0,1\}^m} \alpha_t^2 \sum_{j=0}^{m} \sum_{\substack{s\in\{0,1\}^m: \\ \mathrm{dist}(s,t)=j}} |\langle\psi_t|\psi_s\rangle|^2 \\
&\le \sum_{t\in\{0,1\}^m} \alpha_t^2 \sum_{j=0}^{m} \sum_{\substack{s\in\{0,1\}^m: \\ \mathrm{dist}(s,t)=j}} \mathrm{F}(\rho_s,\rho_t)^2 \qquad \text{(Fact 3)} \\
&\le \sum_{t\in\{0,1\}^m} \alpha_t^2 \sum_{j=0}^{m} \sum_{\substack{s\in\{0,1\}^m: \\ \mathrm{dist}(s,t)=j}} \epsilon^{2j} \qquad \text{(Lemma 21)} \\
&= \sum_{t\in\{0,1\}^m} \alpha_t^2 \sum_{j=0}^{m} \binom{m}{j} \epsilon^{2j} \\
&= (1+\epsilon^2)^m \sum_{t\in\{0,1\}^m} \alpha_t^2. \qquad (18)
\end{aligned}$$

We are left to bound $\sum_{t\in\{0,1\}^m} \alpha_t^2$. To this end, we apply the approximate Pythagorean theorem; specifically, we replace $|\psi_s\rangle$ and $\sum_{s\in\{0,1\}^m} \alpha_s |\psi_s\rangle$ in Lemma 22 with $|\psi_t\rangle$ and $|\varphi\rangle$, respectively. We note that all $|\psi_t\rangle$'s and $|\varphi\rangle$ are now *unit* vectors, and the condition $|\langle\psi_{t'}|\,|\psi_t\rangle| \le \epsilon^{\mathrm{dist}(t,t')}$ is guaranteed by Lemma 21. Hence,

$$m^2\epsilon \sum_{t\in\{0,1\}^m} \alpha_t^2 \ge \left| \Big\| \sum_{t\in\{0,1\}^m} \alpha_t \, |\psi_t\rangle \Big\|^2 - \sum_{t\in\{0,1\}^m} \alpha_t^2 \, \||\psi_t\rangle\|^2 \right| = \Big|1 - \sum_{t\in\{0,1\}^m} \alpha_t^2\Big|.$$

Then there are two cases:

1. $\sum_{t\in\{0,1\}^m} \alpha_t^2 < 1$. In this case, 1 serves as a good upper bound.
2. $\sum_{t\in\{0,1\}^m} \alpha_t^2 \ge 1$. In this case, we have $m^2\epsilon \sum_{t\in\{0,1\}^m} \alpha_t^2 \ge \sum_{t\in\{0,1\}^m} \alpha_t^2 - 1$. Rewritting terms, we have $\sum_{t\in\{0,1\}^m} \alpha_t^2 \le 1/(1-m^2\epsilon)$.

It follows that in either cases, we have

$$\sum_{t\in\{0,1\}^m} \alpha_t^2 \le \frac{1}{1-m^2\epsilon}.$$

Plugging the upper bound above in the inequality (18), we have

$$\sum_{s\in\{0,1\}^m} |\langle\varphi|\psi_s\rangle|^2 \le \frac{(1+\epsilon^2)^m}{1-m^2\epsilon} = 1 + m^2\epsilon + O((m+m^4)\epsilon^2) = 1 + O(m^2\epsilon).$$

This completes the proof of the theorem. ■

8.2 Relationship with other quantum string binding properties

We show that the quantum string sum-binding property established above is *stronger* than two other quantum string binding properties that have been previously studied.

Honest-binding

Informally, we say that a quantum string commitment scheme is *honest-binding* if the honest commitment to an arbitrary string s cannot be opened as $s' \neq s$ with non-negligible probability (implicit in [YWLQ15]). By a simple hybrid argument, it is not hard to see that any quantum non-interactive (statistically-binding or computationally-binding) bit commitment scheme composed in parallel gives an honest-binding quantum string commitment scheme.

To see that the quantum string sum-binding implies the quantum string honest-binding, we just fix the $p_s = 1$ in the inequality (15) for an arbitrary string $s \in \{0,1\}^m$; it then follows that $p_{s'} < O(m^2\epsilon)$ for any $s' \neq t$.

CDMS-binding

The CDMS-binding is defined w.r.t. a function or a set of functions. The following definition is adapted from [CDMS04].

Definition 23 (CDMS-binding) Function $f : \{0,1\}^m \to \{0,1\}^l$, where $m(\cdot)$ and $l(\cdot)$ are two polynomials of the security parameter n. A possibly cheating sender interacts with an honest receiver prescribed by a quantum string commitment scheme and completes the commit stage. Let $\tilde{p}_y^f$ be the success probability that the sender can open the string commitment as *any* string $s \in \{0,1\}^m$ in the reveal stage such that $f(s) = y$, where $y \in \{0,1\}^l$. We say that this (string) commitment scheme is *binding w.r.t. the function* $f(\cdot)$ (or f-*binding* as in [CDMS04]) if

$$\sum_{y\in\{0,1\}^l} \tilde{p}_y^f < 1 + negl(n).$$

When a set of functions $\mathcal{F}$ is considered, we say that a quantum string commitment scheme is $\mathcal{F}$-binding if it is f-binding for each $f \in \mathcal{F}$.

The (string) sum-binding property (Definition 18) can be viewed as a special case of the CDMS-binding property, by noting that when the function f is fixed to be the *identity* function, then the f-binding becomes the sum-binding.

Conversely, it is also not hard to see that the (string) sum-binding property implies the f-binding property *whatever* the function f is. To see this, a *key observation* is that

$$\tilde{p}_y^f \leq \sum_{s:f(s)=y} p_s,$$

where p_s denotes the success probability that the sender can open a claimed commitment as the string $s \in \{0,1\}^m$ (as in Definition 18). This follows straightforwardly from definitons of $\tilde{p}_y^f$ and p_s: while the cheating sender uses the *same* strategy to open the commitment as each preimage of y in the definition of $\tilde{p}_y^f$, it may reveal each preimage of y *adaptively* in the definition of p_s. Hence, given the sum-binding we have

$$\sum_{y\in\{0,1\}^l} \tilde{p}_y^f \leq \sum_{y\in\{0,1\}^l} \sum_{s:f(s)=y} p_s = \sum_{s\in\{0,1\}^m} p_s < 1 + negl(n),$$

which establishes the f-binding property.

Therefore, the (string) sum-binding property implies the CDMS-binding property w.r.t. any function or set of functions.

9 Conclusion and open questions

In this work, we study general properties of quantum bit commitments based on the raw quantum computational hardness. Notably, we show that it is sufficient to focus on the *non-interactive* quantum bit commitment of a generic scheme (Theorem 3), whose semi-honest security implies the full security (Theorem 2). This yields several applications (Section 4 and 7), allowing us to not only obtain new constructions of quantum bit commitment but also simplify the security analyses of some existing ones. We also establish the strongest sum-binding property of the quantum string commitment scheme obtained by composing a generic non-interactive statistically-binding quantum bit commitment scheme in parallel (Theorem 7).

Two open questions following this work that interest us most are as follows:

1. In previous applications of statistically-binding quantum bit commitments [YWLQ15, FUYZ20], a string is committed bitwisely. If we view this as giving rise to a quantum string commitment, then after taking a closer look at those security analyses, we find that the security of corressponding constructions essentially only relies on the string *honest-binding* property. An interesting open question is, can we find any applications whose security will make an essential use of the (strongest) string sum-binding property that we have established?

2. What binding property (stronger than honest-binding) can we obtain if we compose *computationally-binding* quantum bit commitments in parallel? Can it yield any interesting applications? If yes, then the corresponding construction is likely to reduce the round complexity significantly compared with its classical counterpart (by the virtue of the non-interactiveness of quantum bit commitment). However, as pointed out in [FUYZ20], the security analysis based on the quantum statistical binding property does not extend to the computational setting straightforwardly. In spite of this, an initial step towards this goal is taken in [Yan20], where a so-called "predicate-binding" property is established and turns out to be useful.

Acknowledgements. We thank Dominique Unruh for inspiring discussions with him about the strictness of the quantum binding property. We are also grateful to Dominique Unruh and Takeshi Koshiba for their valuable comments on the early draft of this paper.

References

[AC02] Mark Adcock and Richard Cleve. A quantum Goldreich-Levin theorem with cryptographic applications. In *STACS*, pages 323–334. Springer, 2002. 3

[ARU14] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *FOCS*, pages 474–483, 2014. 3, 4, 11

[BB84] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, 1984. 3, 19

[BBCS91] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In *CRYPTO*, pages 351–366, 1991. 6

[BC90] Gilles Brassard and Claude Crépeau. Quantum bit commitment and coin tossing protocols. In *CRYPTO*, pages 49–61, 1990. 3

[BCMS98] Gilles Brassard, Claude Crépeau, Dominic Mayers, and Louis Salvail. Defeating classical bit commitments with a quantum computer. *arXiv preprint quant-ph/9806031*, 1998. 31

[CDMS04] Claude Crépeau, Paul Dumais, Dominic Mayers, and Louis Salvail. Computational collapse of quantum state with application to oblivious transfer. In *TCC*, pages 374–393, 2004. 3, 6, 34, 35, 38

[CLS01] Claude Crépeau, Frédéric Légaré, and Louis Salvail. How to convert the flavor of a quantum bit commitment. In *EUROCRYPT*, pages 60–77, 2001. 3, 5, 20, 25, 26, 28

[Cré94] Claude Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, 1994. 6

[DMS00] Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *EUROCRYPT*, pages 300–315, 2000. 3, 4, 5, 11, 12, 31

[FUYZ20] Junbin Fang, Dominique Unruh, Jun Yan, and Dehua Zhou. How to base security on the perfect/statistical binding property of quantum bit commitment? 2020. https://eprint.iacr.org/2020/621. 2, 3, 4, 5, 6, 7, 8, 11, 22, 25, 26, 27, 39, 42

[HHRS07] Iftach Haitner, Jonathan J. Hoch, Omer Reingold, and Gil Segev. Finding collisions in interactive protocols - a tight lower bound on the round complexity of statistically-hiding commitments. In *FOCS*, pages 669–679, 2007. 4

[HNO+09] Iftach Haitner, Minh-Huyen Nguyen, Shien Jin Ong, Omer Reingold, and Salil P. Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM J. Comput.*, 39(3):1153–1218, 2009. 3

[HSS11] Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. In *CRYPTO*, pages 411–428, 2011. 25

[IL89] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *FOCS*, pages 230–235, 1989. 3

[KO09] Takeshi Koshiba and Takanori Odaira. Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. In *TQC*, pages 33–46, 2009. 3, 4, 5, 31

[KO11] Takeshi Koshiba and Takanori Odaira. Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function. *arXiv:1102.3441*, 2011. 3, 4, 5, 31

[KW00] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *STOC*, pages 608–617, 2000. 5

[LC98] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1):177–187, 1998. 3, 5

[Lég00] Frédéric Légaré. *Converting the flavor of a quantum bit commitment.* PhD thesis, McGill University, 2000. 28

[Mah18] Urmila Mahadev. Classical verification of quantum computations. In *FOCS*, pages 259–267, 2018. 4

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, 1997. 3, 17, 19

[MP12] Mohammad Mahmoody and Rafael Pass. The curious case of non-interactive commitments - on the power of black-box vs. non-black-box use of primitives. In *CRYPTO 2012*, pages 701–718, 2012. 4

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *J. Cryptology*, 4(2):151–158, 1991. 3, 22, 24

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and Quantum Informatioin.* Cambridge University Press, 2000. 7

[NOVY98] Moni Naor, Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Perfect zero-knowledge arguments for NP using any one-way permutation. *J. Cryptology*, 11(2):87–108, 1998. 3, 5, 25, 31

[Unr12] Dominique Unruh. Quantum proofs of knowledge. In *EUROCRYPT*, pages 135–152, 2012. 4, 11

[Unr16a] Dominique Unruh. Collapse-binding quantum commitments without random oracles. In *ASIACRYPT*, pages 166–195, 2016. 4, 10

[Unr16b] Dominique Unruh. Computationally binding quantum commitments. In *EUROCRYPT*, pages 497–527, 2016. 3, 4, 11

[vdG97] Jeroen van de Graaf. *Towards a formal definition of security for quantum protocols.* PhD thesis, Université de Montréal, 1997. 31

[Wat18] John Watrous. *Theory of Quantum Information.* Cambridge University Press, 2018. 7

[Yan20] Jun Yan. Quantum computationally predicate-binding commitment with application in quantum zero-knowledge argument for np. Cryptology ePrint Archive, Report 2020/1510, 2020. https://eprint.iacr.org/2020/1510. 3, 8, 39

[YWLQ15] Jun Yan, Jian Weng, Dongdai Lin, and Yujuan Quan. Quantum bit commitment with application in quantum zero-knowledge proof (extended abstract). In *ISAAC*, pages 555–565, 2015. 3, 4, 7, 8, 22, 24, 25, 35, 38, 39

A The proof of the weak quantum rewinding lemma in [FUYZ20]

Lemma 24 (The restatement of Lemma 4) *Let $\mathcal{X}$ and $\mathcal{Y}$ be two Hilbert spaces. Unit vector $|\psi\rangle \in \mathcal{X} \otimes \mathcal{Y}$. Orthogonal projectors $\Gamma_1, \ldots, \Gamma_k$ perform on the space $\mathcal{X} \otimes \mathcal{Y}$, while unitaries $U_1, \ldots, U_k$ perform on the space $\mathcal{Y}$. If $1/k \cdot \sum_{i=1}^{k} \left\|\Gamma_i (U_i \otimes \mathbb{1}^X) |\psi\rangle\right\|^2 \geq 1 - \eta$, where $0 \leq \eta \leq 1$, then*

$$\left\|(U_k^\dagger \otimes \mathbb{1}^X)\Gamma_k(U_k \otimes \mathbb{1}^X) \cdots (U_1^\dagger \otimes \mathbb{1}^X)\Gamma_1(U_1 \otimes \mathbb{1}^X) |\psi\rangle\right\| \geq 1 - \sqrt{k\eta}.$$

Proof: From the assumption $1/k \cdot \sum_{i=1}^{k} \|\Gamma_i U_i |\psi\rangle\|^2 \geq 1 - \eta$, we have

$$\begin{aligned} \eta &\geq 1 - \frac{1}{k}\sum_{i=1}^{k} \|\Gamma_i U_i |\psi\rangle\|^2 = \frac{1}{k}\sum_{i=1}^{k} \left(1 - \|\Gamma_i U_i |\psi\rangle\|^2\right) \\ &= \frac{1}{k}\sum_{i=1}^{k} \|\Gamma_i U_i |\psi\rangle - U_i |\psi\rangle\|^2 \\ &= \frac{1}{k}\sum_{i=1}^{k} \left\|U_i^\dagger \Gamma_i U_i |\psi\rangle - |\psi\rangle\right\|^2, \end{aligned}$$

where the second "=" is by noting that $1 - \|\Gamma_i U_i |\psi\rangle\|^2$ is equal to the square of the projection of $U_i |\psi\rangle$ on the subspace $\mathbb{1} - \Gamma_i$. Rearranging terms, we get

$$\sum_{i=1}^{k} \left\|U_i^\dagger \Gamma_i U_i |\psi\rangle - |\psi\rangle\right\|^2 \leq k\eta. \tag{19}$$

We claim that

$$\left\||\psi\rangle - (U_k^\dagger \Gamma_k U_k) \cdots (U_1^\dagger \Gamma_1 U_1) |\psi\rangle\right\|^2 \leq \sum_{i=1}^{k} \left\|U_i^\dagger \Gamma_i U_i |\psi\rangle - |\psi\rangle\right\|^2. \tag{20}$$

If this is true, then combining the inequalities (19) and (20), we have

$$\left\||\psi\rangle - (U_1^\dagger \Gamma_1 U_1) \cdots (U_k^\dagger \Gamma_k U_k) |\psi\rangle\right\| \leq \sqrt{k\eta}.$$

Applying the triangle inequality to the left hand side of the inequality above and rearranging terms, we arrive at

$$\left\|(U_1^\dagger \Gamma_1 U_1) \cdots (U_k^\dagger \Gamma_k U_k) |\psi\rangle\right\| \geq 1 - \sqrt{k\eta},$$

as desired.

We are left to prove the inequality (20), which will be done by induction on k.

1. $\underline{k = 1}$. The "=" of inequality (20) holds trivially.

2. Suppose that the inequality (20) holds for $k-1$. We now prove that it also holds for k.

$$\begin{aligned}
& \left\| |\psi\rangle - (U_k^\dagger \Gamma_k U_k) \cdots (U_1^\dagger \Gamma_1 U_1) |\psi\rangle \right\|^2 \\
= & \left\| |\psi\rangle - (U_k^\dagger \Gamma_k U_k) |\psi\rangle \right\|^2 + \left\| (U_k^\dagger \Gamma_k U_k) |\psi\rangle - (U_k^\dagger \Gamma_k U_k) \cdots (U_1^\dagger \Gamma_1 U_1) |\psi\rangle \right\|^2 \\
\leq & \left\| |\psi\rangle - (U_k^\dagger \Gamma_k U_k) |\psi\rangle \right\|^2 + \left\| |\psi\rangle - (U_{k-1}^\dagger \Gamma_{k-1} U_{k-1}) \cdots (U_1^* \Gamma_1 U_1) |\psi\rangle \right\|^2 \\
\leq & \left\| |\psi\rangle - (U_k^\dagger \Gamma_k U_k) |\psi\rangle \right\|^2 + \sum_{i=1}^{k-1} \left\| U_i^\dagger \Gamma_i U_i |\psi\rangle - |\psi\rangle \right\|^2 \\
= & \sum_{i=1}^{k} \left\| U_i^\dagger \Gamma_i U_i |\psi\rangle - |\psi\rangle \right\|^2 .
\end{aligned}$$

where the first "=" follows from Pythagorean theorem by observing that the subspaces $U_k^\dagger \Gamma_k U_k$ and $\mathbb{1} - U_k^\dagger \Gamma_k U_k$ are orthogonal; in the second "$\leq$", we apply the induction hypothesis. This finishes the proof of the inequality (20), and in turn the proof of the lemma. ■

B Reduction 1 in Lemma 15

We inherit all notations in Subsection 7.1. Additionally, for convenience and to avoid ambiguity here, let us call the sender and the receiver of the inner quantum bit commitment scheme (Q_0, Q_1) Alice and Bob, respectively, while "the sender" and "the receiver" are reserved for the scheme $\mathrm{QBC}(n)^{\otimes n}$ and other outer schemes.

For contradiction, suppose that the scheme $\text{U-QBC}(n)^{\otimes n}$ is unconditionally purification-binding whereas the scheme $\mathrm{QBC}(n)^{\otimes n}$ is *not* computationally purification-binding; in particular, let S^* be a cheating sender in the reveal stage[11] who breaks the computational purification-binding property of the latter. That is, consider the purification-game w.r.t. the scheme $\mathrm{QBC}(n)^{\otimes n}$, where in the reveal stage the cheating sender S^* attempts to open the commitment as 1. By our hypothesis, the probability of the S^* cheating (revealing 1) successfully is non-negligible. We shall construct a cheating Bob B^*, with oracle access to S^*, who can break the computational hiding property of the inner quantum bit commitment scheme (Q_0, Q_1), thus arriving at a contradiction. To this end, we use the *hybrid* argument. Detail follows.

As prescribed by the atomic scheme QBC, there are $2n$ bit commitments (to (θ_i, x_i), for $i = 1, 2, \ldots, n$) sent in step (**R2**); thus, there are in total $2n^2$ bit commitments sent in the parallelized scheme $\mathrm{QBC}(n)^{\otimes n}$. For $k = 0, 1, 2, \ldots, 2n^2$, we define *hybrid* scheme H_k as follows: it is basically the parallelized scheme $\mathrm{QBC}(n)^{\otimes n}$, except that in step (**R2**) in place of the first k (when $k \geq 1$) bits the receiver would have committed, it picks k fresh uniformly random bits and commits to them. It is easy to check that the hybrids H_0 and H_{2n^2} are just the parallelized scheme $\mathrm{QBC}(n)^{\otimes n}$ and $\text{U-QBC}(n)^{\otimes n}$, respectively.

Now for each hybrid H_k ($0 \leq k \leq 2n^2$), consider the corresponding purification-binding game such that in the reveal stage the cheating sender runs S^*. We define event succ as the sender cheating (revealing 1) successfully. From our hypothesis that the scheme $\text{U-QBC}(n)^{\otimes n}$ is unconditionally

[11] Recall that regarding the purification-binding (Definition 11), the sender's operation is fixed to be the purification of that of the honest sender in the commit stage.

purification-binding and S^* breaks the computational purification-binding property of the scheme $\mathrm{QBC}(n)^{\otimes n}$, we have

$$\Pr_{\mathrm{H}_0}[\mathsf{succ}] - \Pr_{\mathrm{H}_{2n^2}}[\mathsf{succ}] > \frac{1}{q(n)}, \tag{21}$$

where $q(\cdot)$ is some fixed polynomial.

Now we are ready to construct a cheating Bob B^*, with oracle access to S^*, who can break the computational hiding property of the inner quantum bit commitment scheme (Q_0, Q_1). Specifically, B^* operates as follows after receiving the commitment to a *random* bit $b \in \{0,1\}$ from Alice:

1. Choose $k \xleftarrow{\$} \{0, 1, \ldots, 2n^2 - 1\}$.
2. *Internally* simulate the commit stage of the purification-binding game w.r.t. the hybrid H_k, except that in step (**R2**) replace the commitment to the $(k+1)$-th bit, which we denote by b_{k+1}, with the commitment to the bit b (which is received from Alice *externally*).
3. Invoke the S^* in the reveal stage of the purification-game. If the opening is successful, i.e. the event succ happens, then let $\tilde{b} = b_{k+1}$; otherwise, choose $\tilde{b} \xleftarrow{\$} \{0,1\}$.
4. Output the guess $\tilde{b}$.

Clearly, B^* runs in polynomial time if S^* does. We are left to lowerbound the probability of the B^* guessing the bit b correctly.

Averaging over all choices of the random $k \in \{0, 1, \ldots, 2n^2 - 1\}$,

$$\Pr_{b \leftarrow \{0,1\}, B^*}[\tilde{b} = b] = \frac{1}{2n^2} \sum_{k=0}^{2n^2-1} \Pr_{b \leftarrow \{0,1\}, B_k^*}\left[\tilde{b} = b\right], \tag{22}$$

where the B^* under the "Pr" indicates the experiment induced by the cheating Bob B^*, and B_k^* indicates the same experiment conditioned on the k is chosen. For the summand on the r.h.s. of the equation above,

$$\begin{aligned}
\Pr_{b \leftarrow \{0,1\}, B_k^*}\left[\tilde{b} = b\right] &= \Pr_{b \leftarrow \{0,1\}, B_k^*}\left[(\tilde{b} = b) \wedge \mathsf{succ}\right] + \Pr_{b \leftarrow \{0,1\}, B_k^*}\left[(\tilde{b} = b) \wedge \overline{\mathsf{succ}}\right] \\
&\geq \Pr\left[(\tilde{b} = b) \wedge \mathsf{succ} | b = b_{k+1}\right] \cdot \Pr\left[b = b_{k+1}\right] + \Pr\left[(\tilde{b} = b) | \overline{\mathsf{succ}}\right] \cdot \Pr[\overline{\mathsf{succ}}] \\
&= \frac{1}{2} \Pr\left[\mathsf{succ} | b = b_{k+1}\right] + \frac{1}{2} \Pr[\overline{\mathsf{succ}}],
\end{aligned} \tag{23}$$

where the last "=" follows from the following:

- The first "1/2" is due to that the bit b is chosen uniformly random by Alice, and thus with probability 1/2 equal to the $(k+1)$-th bit (i.e. b_{k+1}) that the receiver would have committed in a semi-honest execution of the commit stage of the hybrid H_k.
- Conditioned on both the events succ and $b = b_{k+1}$ happening, according to step 3 of the B^*, we must have $\tilde{b} = b_{k+1} = b$. Thus,

$$\Pr_{b \leftarrow \{0,1\}, B_k^*}\left[(\tilde{b} = b) \wedge \mathsf{succ} | b = b_{k+1}\right] = \Pr_{b \leftarrow \{0,1\}, B_k^*}\left[\mathsf{succ} | b = b_{k+1}\right].$$

- The second "1/2" is due to that conditioned on that the opening of the commitment (as 1) fails, B^* (step 3) will output a random guess $\tilde{b}$.

Another important observation is that

$$\Pr_{b\leftarrow\{0,1\},B_k^*}\left[\mathsf{succ}|b=b_{k+1}\right]=\Pr_{\mathrm{H}_k}\left[\mathsf{succ}\right],\qquad \Pr_{b\leftarrow\{0,1\},B_k^*}[\mathsf{succ}]=\Pr_{\mathrm{H}_{k+1}}[\mathsf{succ}], \tag{24}$$

where the H_k and H_{k+1} under the "Pr" indicate the experiments induced by a semi-honest execution of the hybrids H_k and H_{k+1}, respectively.

Combing equations (23) and (24), we have

$$\begin{aligned}\Pr_{b\leftarrow\{0,1\},B_k^*}[\tilde{b}=b] &\geq \frac{1}{2}\Pr_{\mathrm{H}_k}\left[\mathsf{succ}\right]+\frac{1}{2}\Big(1-\Pr_{\mathrm{H}_{k+1}}\left[\mathsf{succ}\right]\Big)\\ &= \frac{1}{2}+\frac{1}{2}\Big(\Pr_{\mathrm{H}_k}\left[\mathsf{succ}\right]-\Pr_{\mathrm{H}_{k+1}}\left[\mathsf{succ}\right]\Big).\end{aligned}$$

Plug this inequality in the equation (22),

$$\begin{aligned}\Pr_{b\leftarrow\{0,1\},B^*}[\tilde{b}=b] &\geq \frac{1}{2n^2}\sum_{k=0}^{2n^2-1}\left(\frac{1}{2}+\frac{1}{2}\Big(\Pr_{\mathrm{H}_k}\left[\mathsf{succ}\right]-\Pr_{\mathrm{H}_{k+1}}\left[\mathsf{succ}\right]\Big)\right)\\ &= \frac{1}{2}+\frac{1}{4n^2}\Big(\Pr_{\mathrm{H}_0}\left[\mathsf{succ}\right]-\Pr_{\mathrm{H}_{2n^2}}\left[\mathsf{succ}\right]\Big)\\ &\geq \frac{1}{2}+\frac{1}{4n^2q(n)},\end{aligned}$$

where the last "$\geq$" follows from the inequality (21). But this violates the computational hiding property of the quantum bit commitment scheme (Q_0,Q_1). Thus, if the scheme U-QBC$(n)^{\otimes n}$ is unconditionally purification-binding, then the scheme QBC$(n)^{\otimes n}$ computationally purification-binding.

C A proof of the approximate Pythagorean theorem

For convenience, we restate the approximate Pythagorean theorem as below.

Lemma 25 (A restatement of Lemma 22) *Let $\{|\psi_s\rangle\in\mathcal{X}\}_{s\in\{0,1\}^{m(n)}}$ be an essemble of unnormalized vectors, where $\mathcal{X}$ is a Hilbert space, $m(\cdot)$ is a polynomial, and n is the security parameter. For each pair of indices $s,s'\in\{0,1\}^m$ such that $s\neq s'$, the inner product $|\langle\psi_{s'}|\,\psi_s\rangle|\leq\epsilon(n)^{\mathrm{dist}(s,s')}$ for some fixed function $\epsilon(\cdot)$ such that $0<\epsilon(n)<1/m(n)$ when n is sufficiently large. Fix coefficients $\alpha_s\geq 0$ for all $s\in\{0,1\}^m$. Then it holds that*

$$\left|\left\|\sum_{s\in\{0,1\}^m}\alpha_s\,|\psi_s\rangle\,\right\|^2-\sum_{s\in\{0,1\}^m}\alpha_s^2\,\||\psi_s\rangle\|^2\right|\leq m^2\epsilon\sum_{s\in\{0,1\}^m}\alpha_s^2. \tag{25}$$

Proof: We prove the lemma by induction on m.

1. $\underline{m=1}$. We first expand $\|\alpha_0\,|\psi_0\rangle+\alpha_1\,|\psi_1\rangle\|^2$ as

$$\alpha_0^2\,\||\psi_0\rangle\|^2+\alpha_1^2\,\||\psi_1\rangle\|^2+\alpha_0\alpha_1\langle\psi_0|\psi_1\rangle+\alpha_1\alpha_0\langle\psi_1|\psi_0\rangle.$$

Thus,

$$\begin{aligned}
& \left| \|\alpha_0 |\psi_0\rangle + \alpha_1 |\psi_1\rangle\|^2 - (\alpha_0^2 \||\psi_0\rangle\|^2 + \alpha_1^2 \||\psi_1\rangle\|^2) \right| \\
= \; & |\alpha_0\alpha_1\langle\psi_0|\psi_1\rangle + \alpha_1\alpha_0\langle\psi_1|\psi_0\rangle| \\
\leq \; & 2\epsilon \cdot \alpha_0\alpha_1 \leq 2\epsilon \cdot \frac{\alpha_0^2 + \alpha_1^2}{2} \\
= \; & \epsilon(\alpha_0^2 + \alpha_1^2).
\end{aligned}$$

The lemma holds for $m = 1$.

2. Assume that the theorem holds for $m-1$, where $m \geq 2$. We then prove it also holds for m. First, one can expand $\left\| \sum_{s\in\{0,1\}^m} \alpha_s |\psi_s\rangle \right\|^2$ as

$$\begin{aligned}
& \left\| \sum_{t\in\{0,1\}^{m-1}} \alpha_{t0} |\psi_{t0}\rangle + \sum_{t'\in\{0,1\}^{m-1}} \alpha_{t'1} |\psi_{t'1}\rangle \right\|^2 \\
= \; & \left\| \sum_{t\in\{0,1\}^{m-1}} \alpha_{t0} |\psi_{t0}\rangle \right\|^2 + \left\| \sum_{t'\in\{0,1\}^{m-1}} \alpha_{t'1} |\psi_{t'1}\rangle \right\|^2 \\
& + \sum_{t,t'\in\{0,1\}^{m-1}} \alpha_{t0}\alpha_{t'1}\langle\psi_{t0}|\psi_{t'1}\rangle + \sum_{t,t'\in\{0,1\}^{m-1}} \alpha_{t'1}\alpha_{t0}\langle\psi_{t'1}|\psi_{t0}\rangle.
\end{aligned}$$

Thus, the left hand side of the inequality (25)

$$\begin{aligned}
& \left| \left\| \sum_{s\in\{0,1\}^m} \alpha_s |\psi_s\rangle \right\|^2 - \sum_{s\in\{0,1\}^m} \alpha_s^2 \|\psi_s\|^2 \right| \\
= \; & \left| \left\| \sum_{t\in\{0,1\}^{m-1}} \alpha_{t0} |\psi_{t0}\rangle \right\|^2 + \left\| \sum_{t'\in\{0,1\}^{m-1}} \alpha_{t'1} |\psi_{t'1}\rangle \right\|^2 - \sum_{s\in\{0,1\}^m} \alpha_s^2 \|\psi_s\|^2 \right. \\
& \left. + \sum_{t,t'\in\{0,1\}^{m-1}} \alpha_{t0}\alpha_{t'1}\langle\psi_{t0}|\psi_{t'1}\rangle + \sum_{t,t'\in\{0,1\}^{m-1}} \alpha_{t'1}\alpha_{t0}\langle\psi_{t'1}|\psi_{t0}\rangle \right| \\
\leq \; & \left| \left\| \sum_{t\in\{0,1\}^{m-1}} \alpha_{t0} |\psi_{t0}\rangle \right\|^2 - \sum_{t\in\{0,1\}^{m-1}} \alpha_{t0}^2 \||\psi_{t0}\rangle\|^2 \right| + \left| \left\| \sum_{t'\in\{0,1\}^{m-1}} \alpha_{t'1} |\psi_{t'1}\rangle \right\|^2 - \sum_{t'\in\{0,1\}^{m-1}} \alpha_{t'1}^2 \||\psi_{t'1}\rangle\|^2 \right| \\
& + 2 \sum_{t,t'\in\{0,1\}^{m-1}} |\alpha_{t0}\alpha_{t'1}\langle\psi_{t'1}|\psi_{t0}\rangle| \qquad \text{(triangle inequality)} \\
\leq \; & (m-1)^2\epsilon \sum_{t\in\{0,1\}^{m-1}} \alpha_{t0}^2 + (m-1)^2\epsilon \sum_{t'\in\{0,1\}^{m-1}} \alpha_{t'1}^2 + 2 \sum_{t,t'\in\{0,1\}^{m-1}} |\alpha_{t0}\alpha_{t'1}\langle\psi_{t'1}|\psi_{t0}\rangle| \\
= \; & (m-1)^2\epsilon \sum_{s\in\{0,1\}^m} \alpha_s^2 + 2 \sum_{t,t'\in\{0,1\}^{m-1}} |\alpha_{t0}\alpha_{t'1}\langle\psi_{t'1}|\psi_{t0}\rangle|,
\end{aligned}$$

where the last "$\leq$" is by the induction hypothesis. We are left to bound the second term in the above.

Indeed,

$$\begin{aligned}
& 2 \sum_{t,t' \in \{0,1\}^{m-1}} |\alpha_{t0}\alpha_{t'1}\langle\psi_{t'1}|\psi_{t0}\rangle| \\
= \; & 2 \sum_{j=0}^{m-1} \sum_{\substack{t,t' \in \{0,1\}^{m-1}: \\ \mathrm{dist}(t,t')=j}} \alpha_{t0}\alpha_{t'1} \cdot |\langle\psi_{t'1}|\psi_{t0}\rangle| \\
\leq \; & \sum_{j=0}^{m-1} \epsilon^{j+1} \sum_{\substack{t,t' \in \{0,1\}^{m-1}: \\ \mathrm{dist}(t,t')=j}} 2\alpha_{t0}\alpha_{t'1} \qquad \Big(\text{by the assumption } |\langle\psi_{s'}|\psi_s\rangle| < \epsilon^{\mathrm{dist}(s,s')}\Big) \\
\leq \; & \sum_{j=0}^{m-1} \epsilon^{j+1} \sum_{\substack{t,t' \in \{0,1\}^{m-1}: \\ \mathrm{dist}(t,t')=j}} (\alpha_{t0}^2 + \alpha_{t'1}^2).
\end{aligned}$$

We next count how many times each α_{t0}^2 (resp. $\alpha_{t'1}^2$) is added up in the inner summation above. Since for each t (resp. t'), there are exactly $\binom{m-1}{j}$ t''s (resp. t's) such that $\mathrm{dist}(t,t') = j$, it follows that there are in total $\binom{m-1}{j}$ α_{t0}^2's (resp. $\alpha_{t'1}^2$'s) appearing in the inner summation. Therefore,

$$\sum_{\substack{t,t' \in \{0,1\}^{m-1}: \\ \mathrm{dist}(t,t')=j}} (\alpha_{t0}^2 + \alpha_{t'1}^2) = \binom{m-1}{j} \left(\sum_{t \in \{0,1\}^{m-1}} \alpha_{t0}^2 + \sum_{t' \in \{0,1\}^{m-1}} \alpha_{t'1}^2 \right) = \binom{m-1}{j} \sum_{s \in \{0,1\}^m} \alpha_s^2.$$

Hence,

$$2 \sum_{t,t' \in \{0,1\}^{m-1}} |\alpha_{t0}\alpha_{t'1}\langle\psi_{t'1}|\psi_{t0}\rangle| \leq \sum_{j=0}^{m-1} \epsilon^{j+1} \binom{m-1}{j} \sum_{s \in \{0,1\}^m} \alpha_s^2 = \epsilon(1+\epsilon)^{m-1} \sum_{s \in \{0,1\}^m} \alpha_s^2.$$

Putting it together,

$$\begin{aligned}
\left| \Big\| \sum_{s \in \{0,1\}^m} \alpha_s |\psi_s\rangle \Big\|^2 - \sum_{s \in \{0,1\}^m} {\alpha_s}^2 \||\psi_s\rangle\|^2 \right| \; & \leq \; (m-1)^2\epsilon \sum_{s \in \{0,1\}^m} \alpha_s^2 + \epsilon(1+\epsilon)^{m-1} \sum_{s \in \{0,1\}^m} \alpha_s^2 \\
& = \; \big((m-1)^2 + (1+\epsilon)^{m-1}\big)\epsilon \sum_{s \in \{0,1\}^m} \alpha_s^2 \\
& \leq \; m^2\epsilon \sum_{s \in \{0,1\}^m} \alpha_s^2.
\end{aligned}$$

This completes the proof of the lemma. ■