General Properties of Quantum Bit Commitments

Jun Yan*

Jinan University

February 17, 2022

Abstract

While unconditionally-secure quantum bit commitment (allowing quantum computation and quantum communication) is impossible, in this work we study complexity-based quantum bit commitment. In particular, we will study its general properties through the lens of the so-called "canonical"[1] quantum bit commitment schemes. The reason why we can do this is that as will be shown in this work, any complexity-based quantum bit commitment scheme can be *converted* into the canonical form.

Both flavors of canonical quantum bit commitment schemes (i.e. computationally hiding and statistically binding, or statistically hiding and computationally binding), which will be shown *equivalent* in this work, can be based on quantum-secure one-way functions (or pseudorandom quantum states by more recent results). But in our opinion, the question of whether canonical quantum bit commitment schemes exist is interesting in its own right in quantum complexity theory and may serve as an alternative foundation of complexity-based quantum cryptography.

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

[1] In some prior work [FUYZ20, Yan21] and an earlier draft of this paper (back in 2020), it is called "generic" form. However, this name is misleading as pointed out by Ananth, Qian, and Yuen [AQY22], who also suggest the current name "canonical" to us. And we accept.

Contents

1 Introduction

In the classical world, bit commitment is an important cryptographic primitive. A bit commitment scheme defines a two-stage interactive protocol between a sender and a receiver. It provides two security guarantees, hiding and binding. Informally, the *hiding* property states that the committed bit is hidden from the receiver in the *commit* stage, while the *binding* property states that the sender can only open the commitment as at most one bit value (0 or 1, exclusively) in the *reveal* stage later. Unfortunately, unconditionally (or information-theoretically) secure bit commitment is impossible. As a compromise, we turn to consider complexity-based bit commitment. The one-way function assumption is a raw computational hardness assumption without any mathematical structure; it is the *minimum* assumption in complexity-based cryptography [IL89]. From the one-way function assumption we can construct two flavors of bit commitments: computationally-hiding (statistically-binding) bit commitment [Nao91] and (statistically-hiding) computationally-binding bit commitment [NOVY98, HNO+09]. However, a major disadvantage of these constructions is that they are *interactive*: at least two or even polynomial numbers of messages are needed to exchange, and which seems inherent [MP12, HHRS07].

As quantum technology develops, existing cryptosystems are facing possible quantum attacks in the near future. Regarding bit commitment, we thus have to study bit commitment secure against quantum attacks, a.k.a. *quantum bit commitment*. A *general* quantum bit commitment scheme itself (i.e. the construction) could be a hybrid of classical and quantum computation and communication. When it is purely classical (i.e. both the computation and the communication are classical), we will call it "(classical) bit commitment scheme secure against quantum attacks" or "post-quantum bit commitment scheme"[2].

The concept of quantum bit commitment was proposed almost three decades ago, aiming to make use of quantum mechanics to realize bit commitments [BB84, BC90]. Unfortunately, unconditionally secure quantum bit commitment is impossible either [May97, LC98]. Based on complexity assumptions such as quantum-secure one-way permutations or functions, we can also construct two flavors of quantum bit commitments [AC02, YWLQ15, DMS00, KO09, KO11, CLS01]. An interesting observation about these constructions is that almost all of them (except for the one in [CLS01]) are *non-interactive* (in both the commit and the reveal stages). This motivates us to ask the following question:

> *Is quantum bit commitment inherently non-interactive? That is, can any quantum bit commitment scheme be "compressed" into a non-interactive one?*

This possible non-interactivity of quantum bit commitment is intriguing: if it is true, then replacing post-quantum bit commitments with quantum bit commitments in applications can potentially reduce the *round complexity* of the whole construction.

Quantum commitments in applications. While the idea of using quantum bit commitments in applications sounds wonderful, unfortunately, it is well-known that the *general* binding property of quantum bit commitment, e.g. *sum-binding*, is much weaker than the classical-style binding (but secure against quantum attacks) [DMS00, CDMS04, YWLQ15, Unr16b], or *unique-binding* hereafter. This is because a quantum cheating sender may commit to a bit 0 and 1 in an arbitrary *superposition*, resulting in the committed value no longer unique[3]. Thus, it is questionable *a prior*

[2]Even in case, it is still legal to call it "quantum bit commitment scheme". This is because classical computation and communication can be simulated by quantum computation and communication, respectively, in a standard way.

[3]One may argue that in this case the committed value is still unique in that now the committed value is just a superposition rather than a classical bit. However, we highlight that the goal quantum a commitment is trying to

whether quantum bit commitments could be useful in cryptographic applications, let alone the notorious difficulty (or general impossibility) of quantum rewinding [vdG97] in security analysis. Moreover, in typical applications of bit commitments such as zero-knowledge [GMW91, Blu86], a binary string is committed in a bitwise fashion. In this regard, what can we say about the *general* binding property of the *parallel composition* of quantum bit commitments? Does it suffice for applications? These questions turn out to be notoriously hard since the concept of complexity-based quantum bit commitment was proposed more than two decades ago [DMS00]. As a compromise, we may ask specific to each application we are interested in, what (tailored) quantum (string) binding property is needed to establish its security? And can this quantum string binding property be reduced to the *general* quantum bit binding (e.g. sum-binding)?

Some progress towards answering questions mentioned above has been made in prior works. On the *positive* side, quantum bit commitment of the *canonical* (non-interactive) form (see Footnote 1) is proposed [YWLQ15, FUYZ20], which can be based on quantum-secure one-way functions [YWLQ15, KO09, KO11] or even pseudorandom quantum states by more recent results [MY21]. Though its binding property seems even weaker than sum-binding, it turns out to be useful in constructing quantum zero-knowledge [YWLQ15, FUYZ20, Yan21] and quantum oblivious transfer [FUYZ20]; but the corresponding security analysis based on quantum binding is more tricky than those based on unique-binding.

Other (classical or quantum) constructions of commitments may satisfy some stronger binding properties than sum-binding, such as commitments with unique-binding (e.g. [AC02, BB21] and those based on concrete complexity assumptions with *structure*), collapse-binding [Unr16b, Unr16a], and the recently established extractable property [GLSV21, BCKM21]. They may be more versatile than general quantum bit commitments in applications. However, these constructions suffer at least one of weaknesses listed as below:

1. Rely on stronger quantum complexity assumptions than quantum one-way functions;
2. Need some setup;
3. The construction is complex;
4. The construction is highly interactive (which is in contrast to our motivation of using quantum bit commitments in applications).

There are also some work in which certain strong enough quantum string binding properties were proposed for applications [DFS04, CDMS04], but no instantiations of the corresponding commitments based on well-founded complexity assumptions are known.

On the *negative* side, some black-box barriers towards using quantum commitments in applications are proved [ARU14].

This work. In this work, we put the applications of quantum bit commitments aside, while focusing on studying their *general* properties. In particular, we will study through the lens of quantum bit commitment schemes of the canonical form that ever appeared in prior work [CKR11, YWLQ15, FUYZ20, Yan21] and was motivated by the study of complete problems for quantum zero-knowledge [Wat02, Yan12] and more general quantum interactive proofs [RW05]. The reason why we can do this is because we will show (in this work) that any complexity-based quantum bit commitment scheme can be converted into the canonical form.

Based on previous results as well as results in this work, we propose to study quantum bit commitment in future no only as a cryptographic primitive in the MiniQCrypt world (named

secure a classical bit rather than a qubit. In this regard, the committed value is not unique any more.

after [GLSV21]), but also as a basic (quantum) complexity-theoretic object whose existence is an interesting open problem in its own right. (Refer to Section 1.4 for more discussion.)

In this paper, when we talk about statistical or computational binding without explicitly mentioning other properties of the binding, we mean sum-binding (or equivalently, honest-binding w.r.t. a canonical quantum bit commitment scheme, as will become clear shortly).

1.1 Our contribution

We first sketch what a *canonical* quantum bit commitment scheme looks like, which (we guess) are unfamiliar to most researchers; its formal definition, as well as its hiding and binding properties, are referred to Definition 4. Informally speaking, a canonical (non-interactive) quantum bit commitment scheme can be represented by an ensemble of unitary polynomial-time generated quantum circuit pair $\{(Q_0(n), Q_1(n))\}_n$, where n is the security parameter. For the moment, let us drop the security parameter n to simplify the notation. Both quantum circuits Q_0 and Q_1 perform on a quantum register pair (C, R), which are composed of a bunch of qubits. To commit a bit $b \in \{0, 1\}$, the sender (of bit commitment) first initializes the register pair (C, R) in all $|0\rangle$'s state and then performs the quantum circuit Q_b on them, sending the *commitment* register C to the receiver. In the reveal stage, the sender sends the bit b together with the *decommitment* register R to the receiver, who will first perform the *inverse* of the quantum circuit Q_b (since it is unitary) on the register pair (C, R), and then measure each qubit of (C, R) in the computational basis. The receiver will accept (i.e. the opening is successful) if and only if the measurement outcome of each qubit is 0.

We obtain *four* main results on properties of canonical quantum bit commitment schemes and general quantum bit commitments as follows:

1. Honest-binding is equivalent to sum-binding (w.r.t. the canonical form)

Among various binding properties proposed for quantum (including post-quantum) commitments [AC02, DMS00, CDMS04, DFS04, Unr16b, YWLQ15, Yan21], *honest-binding* [YWLQ15] is the weakest. Informally, it states that any cheating sender (in the reveal stage) cannot open an *honest* commitment to 0 (resp. 1) as 1 (resp. 0). Its formal definition w.r.t. a canonical quantum bit commitment scheme is referred to Definition 4. A prior, honest-binding seems too weak to be useful: it is unrealistic to restrict a cheating sender's behavior to be honest in the commit stage.

Sum-binding (which is mentioned several times before) is a general binding property of quantum bit commitment schemes (secure against quantum attacks) [DMS00]. It roughly states that any cheating sender (who may deviate from the scheme in both the commit and the reveal stages) cannot open a claimed bit commitment as 0 and 1 in such a way that the sum of their success probabilities is bounded by 1, with some additive negligible error. More formally, fix a bit commitment (not necessarily an honest commitment) first. Let p_0 (resp. p_1) denote the probability that a cheating sender in the reveal stage can open this commitment as 0 (resp. 1). Then sum-binding requires that $p_0 + p_1 < 1 + negl(n)$, where $negl(\cdot)$ is some negligible function of the security parameter. The formal definition of sum-binding w.r.t. a canonical quantum bit commitment scheme is referred to Definition 6.

While it is trivial that sum-binding implies honest-binding, in this work we show that the converse is also true w.r.t. a canonical quantum bit commitment scheme[4] (Theorem 1). This in turn establishes an *equivalence* between its semi-honest security (against an honest-but-curious attacker, i.e. honest-hiding and honest-binding; refer to Definition 4) and the full security (against

[4]We do not claim that this holds for a *general* quantum bit commitment scheme.

an arbitrary attacker) (Theorem 2). This equivalence not only explains at a high level why previous applications of a canonical quantum bit commitment scheme only make use of its honest-binding property [YWLQ15, FUYZ20, Yan21], but also enables us to simplify the security analysis of quantum bit commitment schemes of the canonical form[5]. As an application, we can significantly simplify the DMS construction of computationally-binding quantum bit commitment based on quantum-secure one-way permutations[6] [DMS00].

2. Quantum bit commitment is non-interactive inherently

We answer the motivating question raised before affirmatively, i.e. quantum bit commitment is inherently non-interacitve, by proving a *round-collapse* theorem (Theorem 3). This theorem can also be viewed as an extension of converting an arbitrary non-interactive quantum bit commitment scheme into the canonical form [YWLQ15, FUYZ20]. Its basic idea follows the non-interactive case, with the only *non-trivial* thing lying in identifying a sufficient yet as weak as possible condition under which the same idea works for such an extension. A prior, one may expect that for the compression of rounds, the original scheme itself should be firstly secure (against quantum attacks), with some additional structure requirements (if needed). Surprisingly, it turns out the condition for the round compression could be *extremely weak*: even the original quantum bit commitment scheme need not be fully secure; instead, it is sufficient that its *purification is semi-honest secure*! In greater detail, we construct a general *compiler* that can convert any (interactive) quantum bit commitment scheme whose purification is semi-honest secure into a quantum bit commitment scheme of the canonical form. This resulting scheme (of the canonical form), which will be referred to as the "compressed scheme", has *perfect completeness* and satisfies the *same flavor of hiding and binding properties* as the original scheme. This theorem is interesting by noting that we do not have a classical counterpart of it yet, which seems even unlikely [MP12, HHRS07]. An immediate consequence of the round-collapse theorem is that any known quantum bit commitment scheme (of either flavor and based on any complexity assumption) can be converted into the canonical form (Theorem 4).

If we want to apply the round-collapse theorem in applications, (seeing from its statement) the relationship between the semi-honest security of the original scheme and its purification becomes important. We thus initiate a study towards this relationship (in Section 7, 9, and 10). On one hand, we identify many situations in which the semi-honest security of the original scheme *extends* to its purification. On the other hand, we find two counterexamples for which such an extension is impossible (Appendix B). A *bridge* that connects these two notions of security is the security against a special kind of attack which we will refer to as the "purification attack", i.e. attacking by purifying all the party's (honest) operations prescribed by the protocol. A typical purification attack is *not* to perform the expected measurements. It turns out that an (interactive) quantum bit commitment scheme is secure against the purification attack *if and only if* its purification is semi-honest secure (Proposition 16). But in comparison, the security against the purification attack is more convenient to work with in security analysis than the semi-honest security of the purified scheme. We believe that this security against the purification attack as well as techniques developed to establish it (refer to "Technical overview") are of independent interest.

As an interesting application, we apply the round-collapse theorem to compress the classical NOVY scheme [NOVY98], obtaining yet another construction (besides ones given in [DMS00, KO09, KO11]) of non-interactive computationally-binding quantum bit commitment based on quantum-

[5]Then it suffices to show its semi-honest security.

[6]Strictly speaking, we simplify the security analysis of the DMS scheme *after* it is firstly converted into the canonical form (which is straightforward).

secure one-way permutations. This is interesting because we even do not know whether the original NOVY scheme itself is secure against quantum attacks (when the underlying quantum one-way permutation used is quantum secure). We also highlight that our quantum security analysis here is (interestingly) much simpler than the classical analysis of the NOVY scheme in [NOVY98]. This simplification mainly comes from that it suffices to show that the NOVY scheme is secure against the purification attack (for the purpose of round compression).

3. Quantum bit commitment is symmetric

The CLS scheme [CLS01] is an *interactive* computationally-binding quantum bit commitment scheme that builds on Naor's statistically-binding (interestingly, of the opposite flavor) classical bit commitment scheme (but secure against quantum attacks) [Nao91]. It gives a way of *converting* the flavor of quantum bit commitment. In this work, we generalize this result and push it to the *optimal*. Specifically, we show that quantum bit commitment is *symmetric*[7], in that two flavors of quantum bit commitments are *equivalent*. By the virtue of the round-collapse theorem, this is achieved by proving an equivalence between two flavors of quantum bit commitment schemes of the canonical form (Theorem 6).

The *high-level idea* of proving the equivalence above is as follows. Given a canonical quantum bit commitment scheme, we first feed it to a *somewhat simplified* CLS construction [CLS01] to convert its flavor, and then feed the resulting scheme to the general compiler guaranteed by the round-collapse theorem to obtain the final scheme (which is of the canonical form but with the opposite flavor). We highlight that both our construction and their analysis here are significantly simpler than the related ones in [CLS01, CDMS04]. Basically, the simplification comes from two aspects:

1. By the virtue of our round-collapse theorem (Theorem 3), the original CLS scheme (with a canonical quantum bit commitment scheme plugged in) can be firstly simplified to just satisfy the security against the purification attack *before* the compression.

2. Proving the security against the purification attack turns out to be much easier than the full security.

Towards proving this equivalence, we develop several techniques to establish the security against the purification attack. Among others, we develop a new technique to show a *computational collapse* caused by quantum computationally-binding commitments (Theorem 7), which might be of independent interest. In some more detail, in [CDMS04] authors try to show that using quantum computationally-binding commitments can force the receiver of quantum oblivious transfer [CK88] to measure its received BB84 qubits, like using ideal (i.e. perfectly unique-binding) commitments. However, their analysis is quite involved and relies on a tailored quantum string binding property that is not standard and no instantiations of the corresponding quantum commitments are known even today. In comparison, here we achieve a desired computational collapse based on the computational honest-binding property of canonical quantum bit commitment schemes but in a restrictive setting (i.e. proving the security against the purification attack rather than an arbitrary quantum attack). Our technique is inspired by techniques developed in [FUYZ20] and [Yan21]. It is interesting to explore whether our technique can be extended to show a similar computational collapse in the more general setting considered in [CK88, CDMS04].

We finally remark that in the classical world, two flavors of bit commitments (secure against classical attacks) are also equivalent: both of them imply one-way functions, and from which both

[7]This symmetry is in the same sense as that of oblivious transfer [WW06].

of them can be constructed [Nao91, HNO+09]. In comparison, our quantum equivalence is stronger in that there is even no need of interaction in constructions of quantum bit commitment.

4. Quantum statistical string sum-binding (w.r.t. the canonical form)

A natural way to commit a string is to commit it in a bitwise fashion using a quantum bit commitment scheme. So it is interesting to explore what binding property can be obtained if a quantum bit commitment scheme is composed in parallel. Since a canonical quantum bit commitment scheme satisfies the sum-binding property, ideally, we may hope to prove such a dream version of the 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 a (claimed) string 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 $m = poly(n)$, in which case the sender can attack by committing to a superposition of *exponentially* many m-bit strings [CDMS04]. Then bounding the error induced by such a superposition by a negligible quantity becomes technically hard or even impossible[8].

In spite of the above, we manage to show that composing a canonical *statistically-binding* quantum bit commitment scheme in parallel indeed gives rise to a quantum string commitment scheme satisfying a dream version of the quantum statistical string sum-binding property (Theorem 8). Since our proof relies heavily on that the error (incurred by the statistical binding error) decreases *exponentially* in the Hamming distance between the committed string and the string to reveal, it does not extend to the case quantum computational binding.

1.2 A comparison with more recent work

More recently[9], Bitansky and Brakerski [BB21] construct a non-interactive statistically-binding quantum bit commitment scheme based on quantum-secure one-way functions, which deviates from the canonical form but manages to achieve *unique-binding* and make the sender's message in the reveal stage *classical*. However, compared with schemes of the canonical form constructed in [YWLQ15] and this work (Appendix C), their scheme is more complex. Moreover, since several generic techniques are already developed to handle quantum statistical binding [FUYZ20], it seems that the scheme in [BB21] is no more versatile in applications than schemes of the canonical form. Thus in our opinion, schemes in [YWLQ15] and this work (Appendix C) are superior to the scheme in [BB21] in that as a general rule in cryptography, it is better to keep the construction simple while leaving all complexity to the security analysis.

Morimae and Yamakawa [MY21] construct a statistically-binding quantum bit commitment scheme based on pseudorandom quantum states [JLS18], a quantum complexity assumption arguably weaker than quantum-secure one-way functions [Kre21]. Interestingly, we find their construction is just in the canonical form! So by results of this work, their security analysis of quantum statistical binding can be simplified to just show quantum statistical honest-binding (rather than sum-binding). Moreover, combining results in this work, it follows that both flavors of quantum bit commitment schemes of the canonical form can be constructed based on pseudorandom quantum states.

Ananth, Qian and Yuen [AQY21] also construct a statistically-binding quantum bit commitment scheme based on pseudorandom quantum states, which has *two* messages (thus interactive) in the

[8] To the best of our knowledge, however, no impossibility result is known yet. In [CDMS04], authors only vaguely argue that this seems impossible for quantum computationally-binding commitments.

[9] After the upload of the first preprint of this work to Cryptology ePrint Archive [Yan20] in 2020.

commit stage while the single message in the reveal stage is classical. This scheme is clearly not in the canonical form. But it satisfies a seemingly stronger (statistical) binding property than honest-binding or sum-binding: in its definition an explicit (but not necessarily efficient) extractor is required. This extractor can be used to extract (and thus collapse) the committed value from the commitment at the end of the commit stage. We find that this idea of introducing an extractor is very similar in spirit to the *commitment measurement* technique introduced in [FUYZ20] (which is used to collapse the committed value in analyzing the security based on the quantum statistical binding property of a canonical quantum bit commitment scheme). However, this idea of incorporating an extractor in the definition of quantum statistical binding seems cannot extend to the case of quantum computational binding (when the commitment is statistically hiding) *generally* in a straightforward way. This is because then since the quantum commitment to 0 and that to 1 are negligibly close (in trace distance), we cannot hope that there exists a similar extractor. In contrast, the formalization of a canonical quantum bit commitment scheme provides a *uniform* way to capture both flavors of quantum bit commitments (but without extractors).

Ananth, Qian and Yuen [AQY21] also propose studying pseudorandom quantum states, instead of quantum-secure one-way functions, as a basic quantum complexity assumption for quantum (rather than post-quantum) cryptography. In this regard, we feel that it would be equally interesting to study the existence of canonical quantum bit commitment schemes as a basic quantum complexity assumption for quantum cryptography. More discussion on this point is referred to Section 1.4.

1.3 Technical overview

Honest-binding implies sum-binding. The proof is just a simple application of the quantum rewinding lemma (Lemma 3) once used in [YWLQ15, FUYZ20, Yan21], which in a nutshell is another variant of the gentle measurement lemma [Win99] other than the one in [Unr12].

Round compression. At a high level, our compiler for the round compression is inspired by the equivalence between the semi-honest security and the full security w.r.t. a canonical quantum bit commitment scheme (Theorem 2). Specifically, the *compiler* itself is extremely simple: in the new (non-interactive) commit stage, the sender will simulate an *honest* execution of the commit stage of the original (possibly interactive) scheme, and then send the original receiver's system as the commitment to the new receiver. Later in the reveal stage, the new sender will send the residual system to the new receiver, who will check the new sender's whole computation in the commit stage via the quantum *reversible* computation. Note that here for the reveal stage to be legal, possible *irreversible* computation of both parties prescribed by the original scheme in the commit stage should be simulated by unitary computation (in a standard way) in the first place. This procedure of simulation is typically referred to as the "purification" (of a quantum protocol).

At the first glance, the compiler constructed as above seems too simple to be true: how can the idea of simply letting the new sender delegate all the computation in the commit stage of (the purification of) the original scheme work? After all, a cheating new sender can deviate arbitrarily, and there seems no way to restrict its behavior by just exchanging a single message in the (non-interactive) commit stage! Clearly, this idea of compression does not work for commitments in classical cryptography.

To see why our compiler works is by Theorem 2: it suffices to show that the resulting *compressed* quantum bit commitment scheme (which is just in the canonical form by our construction) is semi-honest secure! This also provides some intuition why in the formal statement of our round-collapse theorem (Theorem 3), it requires that the purification of the original scheme, or *purified scheme* hereafter, be semi-honest secure. As for the proof of the round-collapse theorem, while the honest-

hiding property of the compressed scheme is trivial, its honest-binding property can be argued as follows. Suppose (for contradiction) that at the beginning of the reveal stage, there is a cheating sender who can transform the quantum state of the whole system when a bit 0 is committed to the state when a bit 1 is committed, by just performing some unitary operation U on its own system. This will gives rise to an attack against the honest-binding property of the purified scheme as follows: the sender commits to the bit 0 honestly following the purified scheme in the commit stage. In the reveal stage, it first performs the operation U on its own system, transforming the whole system to a state that is close to the state when the bit 1 is committed, and then proceeds honestly to open the commitment as 1. While the intuition underlying this reduction is simple, to turn it to a formal proof, we need a large amount of (and tedious) work in formalizing an execution of (the commit stage of) a general (interactive) quantum bit commitment scheme and its purification (Section 6), as well as their semi-honest security (Section 7).

Last, we would like to compare our round compression of a general interactive quantum bit commitment scheme with that of a quantum interactive proof [KW00] or a zero-knowledge proof [Kob08]. Ideas in these two settings are very similar: both of them rely heavily on the *reversibility* of quantum computation. The *key difference* lies in 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 setting this test is not needed because (as typical in cryptography) both the honest sender and the honest receiver are polynomial-time bounded.

Arguing the security against the purification attack. To apply our round-collapse theorem, one needs first to show that the original (interacitve) quantum bit commitment scheme is secure against the purification attack (or equivalently, its purification is semi-honest secure). It turns out that this security 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 scenarios, the semi-honest security of the original scheme *extends* to its purification. For such an extension, the *basic idea* is to show that collapses prescribed by the original scheme are *enforced* even *after* the purification. To have a taste of how this is possible, note that messages sent through the classical channel automatically collapse; when a message is uniquely determined by some other collapsed messages, it can be viewed as having collapsed as well.

A non-trivial scenario in which collapses are enforced is by *quantum commitments*, as argued in [FUYZ20] and Section 10 of this paper. That is, committing to a bit in *superposition* using a canonical statistically- or computationally-binding quantum bit commitment scheme can be viewed as an *implicit* way of measuring it (but without leaking its value)! In greater detail, when statistically-binding quantum bit commitments are used, collapses can be shown using generic techniques (i.e. *perturbation* and *commitment measurement*) developed in [FUYZ20]. When computationally-binding quantum bit commitments are used, we will prove a *computational collapse theorem* (Theorem 7) in this work, which realizes a "computational collapse" (named after [CDMS04], but in proving a weaker security here). The technique used towards proving this theorem is inspired by the proof of the quantum computational string predicate-binding property in [Yan21], which basically is a clever way of bounding exponentially many negligible errors in superposition by a negligible quantity.

Last, we stress (again) that the semi-honest security of an arbitrary (interactive) quantum bit commitment scheme does *not* extend to its purification *generally*; two counterexamples are given in Section B.

Proving an equivalence between two flavors of quantum bit commitments. The basic

idea to convert the flavor of a quantum bit commitment scheme is to use the CLS construction [CLS01]. In a nutshell, the original CLS scheme in [CLS01] uses (classical) statistically unique-binding bit commitments (e.g. Naor's scheme [Nao91]) to realize a *quantum oblivious transfer* (QOT) [CK88], which in turn can be used to construct a computationally-binding quantum bit commitment scheme. This result can be extended to using a canonical statistically/perfectly-binding *quantum* bit commitment scheme within the CLS scheme [FUYZ20]. Combined with the round-collapse theorem (Theorem 3), this already proves one direction of the equivalence.

For the other direction of the equivalence, however, it is still open whether we can use computationally-binding quantum bit commitments in the CLS scheme to obtain a statistically-binding quantum bit commitment scheme. Roughly speaking, this is because we do not know whether using computationally-binding quantum bit commitments can cause a collapse like using statistically-binding quantum bit commitments [CDMS04]. Very recently, a quantum computationally-binding bit commitment that additionally satisfies extractable and equivocal properties is constructed based on (classical) statistically unique-binding bit commitments [BCKM21]. We conjecture that the same construction works as well if we use a canonical statistically-binding quantum bit commitment scheme instead, by generic techniques developed in [FUYZ20]. If this is true, then plugging the resulting computationally-binding quantum bit commitment scheme that additionally satisfies extractable and equivocal properties in the CLS scheme and applying the round-collapse theorem will prove the other direction of the equivalence.

In this work, however, we will take an alternative yet much simpler approach to prove the claimed equivalence. In particular, in proofs of both directions we will use the *same* construction to convert the flavor of quantum bit commitment, except that within which we will use canonical quantum bit commitment schemes of different flavors. Then the round-collapse theorem can be applied to finish the job.

In greater detail, we will use a *somewhat simplified CLS construction* to convert the flavor of quantum bit commitment, which basically removes all *intermediate verifications of quantum commitments* compared with the original CLS scheme. We can do this is by the virtue of the round-collapse theorem: we only need a scheme whose purification is semi-honest secure for the purpose of the round compression. In a nutshell, we only need (within our construction) a QOT satisfying the following security property: after the interaction, the purified receiver of QOT does not know the other bit that the honest sender is given as input, while the purified sender of QOT does not know which input bit the honest receiver is aware of. This security requirement is already much *weaker* than the security against an arbitrary quantum attack considered in [Yao95, CLS01, FUYZ20], let alone the recently achieved simulation security [DFL$^+$09, GLSV21, BCKM21]. Hence, it is much easier to establish.

In greater detail, for the security analysis we will first prove the semi-honest security of this somewhat simplified CLS scheme, and then extend it to its purification. For such an extension, a *crucial step* is to show that quantum commitments will cause an implicit collapse of the quantum state just like the measurements prescribed by the scheme were really performed. To this end, we will use techniques aforementioned.

1.4 Quantum bit commitments: seeing from both quantum cryptography and quantum complexity perspectives

Based on previous results and results in this paper, now let us give an overview of quantum bit commitments from quantum cryptography and quantum complexity perspectives, respectively.

Seeing from the *quantum cryptography perspective*, on one hand quantum bit commitment can

be constructed from quantum-secure one-way functions/permutations [AC02, YWLQ15, DMS00, KO09, KO11, CLS01, BB21], or pseudorandom quantum states [JLS18, MY21, AQY21]. It is interesting to explore whether quantum bit commitments imply pseudorandom quantum states conversely[10]. On the other hand, quantum bit commitments are useful, and may help reduce the round complexity of cryptographic constructions [YWLQ15, FUYZ20, Yan21]. In particular, there exists a certain *equivalence* between quantum bit commitment and quantum zero-knowledge [YWLQ15], and an equivalence between quantum bit commitment and quantum oblivious transfer [Yao95, CLS01, FUYZ20, BCKM21, AQY21]. Thus, quantum bit commitment is likely to be an important primitive living in the MiniQCrypt world [GLSV21]. It is interesting to explore more cryptographic applications of quantum bit commitments in future.

Seeing from the *quantum complexity perspective*, whether (complexity-based) quantum bit commitments exist is an interesting open problem. As mentioned, canonical quantum bit commitment schemes were motivated by the study of complete problems for quantum zero-knowledge [Wat02, Yan12] and more general quantum interactive proofs [RW05]. The existence of canonical statistically-hiding computationally-binding quantum bit commitment schemes is closely related to the *quantum complexity of unitaries* [Aar16]. In greater detail, suppose that (Q_0, Q_1) is a canonical statistically-hiding computationally-binding quantum bit commitment scheme. Then its statistical hiding property implies that quantum states $Q_0 |0\rangle^{CR}$ and $Q_1 |0\rangle^{CR}$ only differ up to a unitary U performing on the decommitment register R. This is because restricting to the commitment register C, the corresponding two reduced quantum states are negligibly close in trace distance. However, the computational binding property implies that this unitary U is *not* efficiently realizable!

We can motivate the study of a canonical computationally-hiding statistically-binding quantum bit commitment scheme by comparing it with a pair of efficiently constructible probability distributions that are *computationally indistinguishable* but *statistically far apart* in the classical setting. They look quit similar; we may view the former as the quantum counterpart of the latter. Goldreich shows that the existence of the latter implies one-way functions [Gol01, an exercise in Chapter 3] and pseudorandom generators [Gol90]. In a try to translate this result to the quantum setting, it brings us back to the question of whether quantum bit commitments imply pseudorandom quantum states (which are the quantum analog of pseudorandom generators) [JLS18, MY21, AQY21].

We finally remark that the round-collapse theorem and the equivalence between two flavors of quantum bit commitments established in this paper indicate that the open problem regarding the existence of (complexity-based) quantum bit commitments is very *robust*. And it will be more robust if the answer to the following open question, which concerns *quantum hardness amplification*, is "yes": can the computational binding error of a canonical quantum bit commitment scheme be reduced by parallel repetition, say from $1/2$ or even inverse polynomial to some negligible quantity? This question look very similar to the question of amplifying the hardness of inverting an arbitrary one-way function in classical cryptography [Yao82]. More interestingly, if the answer to this question is indeed "yes", then combining it with results in [Wat02, YWLQ15, FUYZ20, Yan21] will complete the proof for an equivalence between quantum bit commitment and quantum zero-knowledge like in the classical setting [OV08].

Organization. In Section 2, we review necessary preliminaries. In Section 3, we formally introduce the definition of a canonical quantum bit commitment scheme and its honest-hiding and honest-binding properties In Section 4, we study the binding property of a canonical quantum bit commitment scheme. In particular, we prove that its honest-binding property is equivalent to

[10]We do not expect that quantum bit commitments can imply quantum-secure one-way functions, simply because a canonical quantum bit commitment scheme concerns quantum states rather than any function.

the sum-binding property, which will be used to simplify the security analysis of the DMS construction of computationally-binding bit commitment in Section 5. In Section 6, we fix a way of formalizing a quantum two-party interaction as well as a way to purify a quantum protocol. We also formally define a party's view of an interaction. Based on these formalizations, we define the semi-honest security of a general interactive quantum bit commitment scheme and its purification in the subsequent Section 7, where we also introduce the notion of the security against the purification attack. All formalizations and notions introduced in Section 6 and 7 will be crucial in the statement and the proof of the round-collapse theorem in Section 8. In Section 9, as an application of the round-collapse theorem we give yet another construction of non-interactive computationally-binding quantum bit commitment by compressing the classical NOVY scheme. In Section 10, we prove an equivalence between two flavors of quantum bit commitments as another application of the round-collapse theorem. In Section 11, we establish a very strong quantum string sum-binding property of the parallel composition of a canonical statistically-binding quantum bit commitment scheme. Finally in Section 12, we conclude this work and raise several open problems.

2 Preliminaries

Notation. Denote $[n] = \{1, 2, \ldots, n\}$ for an integer n. Denote by U_n 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* (i.e. 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'.

Quantum formalism. Quantum registers/systems we use in this paper are composed of multiple qubits. 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 superscripts to simplify the notation.

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. This binary measurement is typically induced by 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 former, we often drop "+" and just write $|b\rangle$.

We work with the standard *unitary* quantum circuit model. In this model, a 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 overload the notation to use Q to denote its corresponding *unitary transformation*; $Q^\dagger$ denotes 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*.

Useful lemmas

Lemma 2 (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 3 (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*

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

The proof of the lemma above is reproduced in Appendix A for convenience.

3 A canonical quantum bit commitment scheme

The definition of a canonical (non-interactive) quantum bit commitment scheme is as follows.

Definition 4 A canonical (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, where we drop the security parameter n to simplify the notation:

- In the *commit* stage, to commit a bit $b \in \{0, 1\}$, the sender performs the quantum circuit Q_b on the quantum register pair (C, R)[11] initialized in all $|0\rangle$'s state. Then the sender sends the *commitment register* C to the receiver, whose state at this moment is denoted by ρ_b.
- In the subsequent (canonical) *reveal* stage, the sender announces the bit b, and sends the *decommitment register* R to the receiver. The receiver will first perform $Q_b^\dagger$ on the quantum register pair (C, R) and then measure each qubit of (C, R) in the computational basis, accepting if measurement outcomes are all 0's.

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

[11] Their size depend on the security parameter n.

- (Honest)-**hiding**. We say that the scheme is statistically (resp. computationally) hiding if quantum states ρ_0 and ρ_1 are statistically (resp. computationally) indistinguishable[12].

- (Honest-)ϵ-**binding**. First prepare the quantum register pair (C, R) in the state $Q_0 |0\rangle$[13]. We say that the scheme is computationally (resp. statistically) ϵ-binding if for any state $|\psi\rangle$ of an auxiliary register Z, and any polynomial-time (resp. physically) realizable unitary transformation U performing on registers (R, Z), the reduced state of the quantum register pair (C, R) after the transformation U is performed is far from the state $Q_1 |0\rangle$. Or formally,

$$\left\| \left(Q_1 |0\rangle \langle 0| Q_1^\dagger\right)^{CR} U^{RZ} \left(\left(Q_0 |0\rangle\right)^{CR} |\psi\rangle^Z \right) \right\| < \epsilon. \tag{2}$$

  By the *reversibility* of quantum computation, this binding property can be equivalently defined by swapping the roles of Q_0 and Q_1, in which case the inequality (2) becomes

$$\left\| \left(Q_0 |0\rangle \langle 0| Q_0^\dagger\right)^{CR} U^{RZ} \left(\left(Q_1 |0\rangle\right)^{CR} |\psi\rangle^Z \right) \right\| < \epsilon. \tag{3}$$

  As typical in cryptography, We say that the scheme is computationally (resp. statistically) binding (without referring to the parameter ϵ) when the function $\epsilon(\cdot)$ is a negligible function (of the security parameter n).

Remark.

1. We call the binding property defined above *honest-binding*, because informally it states that any cheating sender cannot open the *honest* commitment to a bit b as $1 - b$. That is, in the definition of honest-binding, a cheating sender is honest in the commit stage but may deviate arbitrarily in the reveal stage. In this regard, the attack $(U, |\psi\rangle)$ of the sender just happens in the reveal stage. Honest-binding is the *weakest* binding property that any meaningful quantum bit commitment scheme should satisfy. This definition will be generalized to the case of *interactive* quantum bit commitment schemes later (Section 7).

2. The hiding property of a bit commitment scheme is only defined w.r.t. the commit stage. For the hiding property defined above, since the commit stage is non-interactive (so that the receiver will send nothing during the commit stage), the hiding against a semi-honest (i.e. honest-but-curious) receiver and that against an arbitrary receiver are just the same security property. In this regard, the honest-hiding is also the hiding against an arbitrary quantum receiver. However, in the sequel when we consider a general (interactive) quantum bit commitment scheme, these two notions are not necessarily equivalent.

3. As commented in [YWLQ15], the reveal stage in the definition above is *canonical* in the sense that it is similar to the canonical opening of a classical bit commitment: 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 during the commit stage.

[12] Strictly speaking, it should be understood as the corresponding two quantum state ensembles indexed by the security parameter n are indistinguishable.

[13] Here the notation $|0\rangle$ should be understood as multiple $|0\rangle$'s, the number of which depends on the security parameter; we just write a single $|0\rangle$ to simplify the notation. We will follow this rule throughout this paper.

4. In [YWLQ15, FUYZ20], it is argued informally that any *non-interactive* statistically-binding quantum bit commitment scheme can be converted into a scheme of the canonical form. Actually, the same argument extends to the setting of non-interactive computationally-binding quantum bit commitment schemes in a straightforward way. In this work, we will further extend it, showing that any (interactive) quantum bit commitment scheme can be converted into this canonical form (Theorem 3).

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 canonical quantum bit commitment scheme.

6. We can commit to a binary string $s \in \{0,1\}^m$ in a bitwise fashion using a canonical quantum bit commitment scheme (Q_0, Q_1). Then the corresponding quantum circuit is given by

$$Q_s \stackrel{def}{=} \bigotimes_{i=1}^{m} Q_{s_i}, \tag{4}$$

   where s_i is the i-th bit of the string s and each quantum circuit Q_{s_i} performs on one copy of the quantum register pair (C, R).

7. As discussed in "Introduction", this definition of a canonical quantum bit commitment scheme can also be viewed as a quantum complexity assumption that is weaker than quantum-secure one-way functions and pseudorandom quantum states [JLS18].

A generalized quantum honest-binding which turns out to be useful in security analysis is given below, whose proof is referred to [Yan21].

Lemma 5 (Generalized quantum honest-binding) *Inherit all notations in Definition 4. Let the operator $\Gamma = U_k \Pi_k \cdots U_1 \Pi_1$ be an arbitrary alternation of efficiently realizable (resp. unbounded) unitary transformations and projectors, where $k \geq 1$ is an integer, and for each i $(1 \leq i \leq k)$ both the unitary transformation U_i and the projector Π_i perform on the quantum registers (R, Z). If the inequality (2) holds, then*

$$\begin{aligned} \left\| (Q_1 |0\rangle \langle 0| Q_1^*)^{CR} \Gamma^{RZ} \left((Q_0 |0\rangle)^{CR} |\psi\rangle^Z \right) \right\| &< \epsilon(n), \\ \left\| (Q_0 |0\rangle \langle 0| Q_0^*)^{CR} \Gamma^{RZ} \left((Q_1 |0\rangle)^{CR} |\psi\rangle^Z \right) \right\| &< \epsilon(n). \end{aligned}$$

4 The binding of a canonical quantum bit commitment scheme

4.1 Honest-binding is equivalent to sum-binding

Sum-binding is a general binding property of quantum bit commitment schemes. Its definition w.r.t. a canonical quantum bit commitment scheme is as follows.

Definition 6 (Sum-binding) At the beginning of the commit stage, the cheating sender prepares the whole system $(\mathsf{C}, \mathsf{R}, \mathsf{Z})$ in an arbitrary quantum state $|\psi\rangle$. Then it sends the commitment register C 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 the system (R, Z) 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 $p_0 + p_1 < 1 + negl(n)$.

Compared with honest-binding (Definition 4), sum-binding is a security against an *arbitrary* quantum sender, who may deviate from the scheme in both the commit and the reveal stages. Clearly, sum-binding implies honest-binding, by noting that if we fix p_0 or p_1 in Definition 6 to be 1, 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. Combining them we have the following theorem.

Theorem 1 *Honest-binding is equivalent to sum-binding w.r.t. a canonical quantum bit commitment scheme (of either flavors).*

Proof: It is left to prove that honest-binding implies sum-binding. It turns out that an attack which breaks the sum-binding property can be directly used to break the honest-binding property without much modification. Detail follows. We remark that the proof below holds for either flavors of canonical quantum bit commitment schemes.

Let n be the security parameter. According to its definition (Definition 6), an arbitrary attack of the sum-binding property of a canonical quantum bit commitment scheme (Q_0, Q_1) can be modeled by $(U_0, U_1, |\psi\rangle)$. Now assume that the 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 $p(\cdot)$ is some polynomial of the security parameter n. We apply the quantum rewinding lemma (Lemma 3) 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

$$\left\| U_1^\dagger (Q_1 |0\rangle \langle 0| Q_1^\dagger) U_1 \cdot U_0^\dagger (Q_0 |0\rangle \langle 0| Q_0^\dagger) U_0 |\psi\rangle \right\| \geq 1 - \sqrt{1 - \frac{1}{p}} > \frac{1}{2p}. \tag{5}$$

We are next to devise an attack of the honest-binding property of the scheme (Q_0, Q_1) given the attack $(U_0, U_1, |\psi\rangle)$. Specifically, suppose that in the commit stage, the sender (honestly) prepares the quantum state $Q_0 |0\rangle$ in the quantum register pair (C, R) and sends the commitment register 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 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 quantum register pair $(\mathsf{C}', \mathsf{R}')$. (*Intuitively*, we expect that conditioned on the outcome being one, the reduced state of the register Z' will help the sender cheat.)
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.

Note that the squared l.h.s. of the inequality (5) is exactly the probability of the outcome of the binary measurement in step 2 above being one and S^* opening 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 0.) Hence, S^* breaks the honest-binding property of the scheme (Q_0, Q_1). ■

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

Combing the second remark following Definition 4 with Theorem 1, we have the following theorem as an immediate corollary.

Theorem 2 *A canonical quantum bit commitment scheme (Q_0, Q_1) (of either flavor) is secure if and only if it is semi-honest secure (i.e. honest-hiding and honest-binding) .*

4.2 A canonical quantum bit commitment scheme cannot be 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 computationally indistinguishable*. Collapse-binding commitments find many applications in quantum cryptography.

We can generalize the collapse-binding property that was introduced for classical commitments (but secure quantum attacks) to quantum commitments in a natural way. Adapted from [Unr16b], the collapse-binding property of a canonical quantum bit commitment scheme can be defined as follows.

Definition 7 (Collapse-binding) The workspace of a cheating sender is (C, R, B, Z), where registers (C, R, B) are initialized in all $|0\rangle$'s state and the register Z is in an arbitrary state that the sender may receive at the beginning of the commit stage. An attack of the sender of the scheme can be represented by a pair of physically (resp. efficiently) realizable unitary transformations (U_C, U_R). In the commit stage, the sender performs U_c on the whole system (C, R, B, Z), sending the register C to the receiver as the commitment. Later in the reveal stage, the sender performs U_R on the subsystem (R, B, Z), sending R as the decommitment and the single qubit B which stores the bit value to reveal (which could be in superposition). The receiver will decide whether to accept or not by checking via the reversible computation in superposition (controlled by the qubit B); that is, the receiver will perform the binary measurement $\{\Pi, \mathbb{1} - \Pi\}$, where

$$\Pi = (|0\rangle\langle 0|)^B \otimes \left(Q_0 |0\rangle\langle 0| Q_0^\dagger\right)^{CR} + (|1\rangle\langle 1|)^B \otimes \left(Q_1 |0\rangle\langle 0| Q_1^\dagger\right)^{CR}.$$

We say that the scheme is statistically (resp. computationally) collapse-binding if conditioned on the receiver accepting in the reveal stage, quantum states of the system (C, R, B, Z) corresponding to the qubit B is measured or not at the end of the reveal stage are quantum statistically (resp. computationally) indistinguishable.

Remark. We highlight that in the definition above, registers (B, C, R) are *not* in the sender's hands at the time of distinguishing whether the committed value collapses. Hence, now we cannot say any more that the sender's views corresponding to whether the committed value is measured or not are indistinguishable in defining collapse-binding like in the post-quantum setting [Unr16b]. Here, we define collapse-binding with the intuition in our minds that if a canonical quantum bit commitment scheme could replace (classical) collapse-binding commitments in applications straightforwardly, then we need it satisfy the property as defined above.

Then we naturally ask, *can a canonical quantum bit commitment scheme be collapse-binding?* If yes, then using quantum instead of classical bit commitments in cryptographic constructions

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

may reduce the round complexity by the virtue of the non-interactivity of a canonical quantum bit commitment scheme. 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 quantum computational distinguishable from its corresponding *mixture*. In greater detail, 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 of the qubit B corresponding to whether it is measured or not at the end of the reveal stage, 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. Next, 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.

5 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 permutations. The hard part of its security analysis lies in establishing the computational sum-binding property. Here, we can simplify this analysis but w.r.t. the *purified* DMS scheme using Theorem 1, which allows us to just show its (computational) 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 canonical form as given in Definition 4 such that

$$Q_0|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle^R |f(x)\rangle^C_{+^n}, \qquad Q_1|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle^R |f(x)\rangle^C_{\times^n}. \tag{6}$$

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

Lemma 8 *The purified DMS scheme (Q_0, Q_1) given by the equation (6) 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 4) such that

$$\left\| \left(Q_0|0\rangle\langle 0|Q_0^\dagger\right)^{CR} U^{RZ} \left(Q_1|0\rangle^{CR} \otimes |\psi\rangle^Z\right) \right\| \geq \frac{1}{p(n)}, \tag{7}$$

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 (7),

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

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. ■

6 Formalizations

In this section, we first fix a formalization for a general quantum two-party interaction, which basically follows Mayers [May97] but deviates a little bit. Based on this formalization, we formally define a party's view in an interaction and fix a way to purify a general quantum two-party protocol. Here, by "purify a quantum protocol" we mean all (classical and quantum) computations prescribed by the protocol will be simulated by *unitary* quantum operations, and all classical communications will be simulated by quantum communications. Formalizations and the definition of a party's view introduced in this section will be crucial for rigorous security definitions introduced in the subsequent Section 7 and the proof of the round-collapse theorem (Theorem 3) in Section 8.

To simplify the notation, we will drop the security parameter in this section.

Materials presented in this section are standard. Experienced readers may skip this section for the first reading of this paper and come back later when necessary.

6.1 An interaction between two parties

An interaction between two parties may be a hybrid of classical and quantum computations and communications. For simplicity, we can assume without loss of generality the following for a general two-party interaction:

- The interaction consists of multiple rounds, the number of which is bounded by some fixed polynomial of the security parameter;
- Both classical and quantum registers used are *two-dimensional*, i.e. composed of bits and qubits, respectively.
- Both parties can carry out classical and quantum computations. In particular, classical computation includes random coin tosses. Quantum computation includes quantum operations are those:
  1. either (which itself might not be unitary but) can be realized by polynomial-size quantum circuits composed of quantum gates from some fixed universal, finite, and unitary quantum gate set, or
  2. the measurement of a qubit in the computational basis.
- Both parties can send classical and quantum messages.

Formally, to model an interaction $\langle A, B\rangle$ between two parties A and B, we introduce *quantum* registers (A, B) and *classical* register E as follows:

- A: the party A's quantum workspace.
- B: the party B's quantum workspace.
- E: the "environment" $\mathsf{E} = (\mathsf{E}_S, \mathsf{E}_A, \mathsf{E}_B)$ 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 classical bits transmitted between the party A and the party B; that is, each party will keep a copy of them.
  - E_A: stores the *untransmitted* classical bits that are kept on the party A's side, which in particular includes A's inner coin tosses and measurement outcomes.
  - E_B: stores the *untransmitted* classical bits that are kept on the party B's side, which in particular includes B's inner coin tosses and measurement outcomes.

Now let us describe possible operations of a party $\mathrm{P} \in \{\mathrm{A}, \mathrm{B}\}$:

- The party P's classical operations will perform on the register E_P.
- The party P's quantum operations will perform on the register P.
- If the party P's classical operations depend on the classical messages stored in the register $\mathsf{E}_{S,P}$, then it will first copy the corresponding bits to the register E_P.
- If the party P's quantum operations depend on the classical information stored in the register $(\mathsf{E}_P, \mathsf{E}_{S,P})$, then it will first copy the corresponding bits to the register E_P.
- If the party P's quantum operations output classical bits, then move these bits to the register E_P.
- When the party A (resp. B) wants to send a *quantum* message to the party B (resp. A), it will send the part of the register A (resp. B) which holds this message to the party B (resp. A), who will then incorporate this register into its own workspace B (resp. A).
- When the party A (resp. B) wants to send a *classical* message to the party B (resp. A), it will first move this message from the part of the register E_A (resp. E_B) which holds this message to the register $\mathsf{E}_{S,A}$ (resp. $\mathsf{E}_{S,B}$), and then copy it to the register $\mathsf{E}_{S,B}$ (resp. $\mathsf{E}_{S,A}$).

By the formalization introduced above, at any moment of the interaction the whole system will be in a (mixed) state of the form

$$\sum_{s,a,b} |\alpha_{s,a,b}|^2 \left(|s\rangle \langle s|\right)^{E_{S,A}} \left(|s\rangle \langle s|\right)^{E_{S,B}} \left(|a\rangle \langle a|\right)^{E_A} \left(|b\rangle \langle b|\right)^{E_B} \left(|\psi_{s,a,b}\rangle \langle \psi_{s,a,b}|\right)^{AB}. \tag{8}$$

Remark. We have two remarks about the formalization above.

1. We actually implicitly assume that each party will record all *classical* messages (in classical registers $\mathsf{E}_{S,A}$ for the party A and $\mathsf{E}_{S,B}$ for the party B) it has sent and received. And we can assume w.o.l.g. that even *honest* parties (whose behaviors are prescribed in a quantum protocol) will do this. This could be crucial for attacking a quantum protocol.
2. We note that quantum registers introduced above are *not* fixed during the execution of the protocol; they are subject to *change* as the quantum computation and communication go on.

6.2 A party's view of an interaction

For the purpose of defining the semi-honest security of a quantum protocol in the subsequent section (Section 7), we introduce a party's view of an interaction, which is natural and accords with our intuition.

Definition 9 (A party's view of an interaction) A party's view of a two-party interaction is given by the state of its system at the *end* of the interaction. Formally, with the formalization fixed in Section 6.1, the party A's view is given by the state of the subsystem $(\mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A})$ at the end of the interaction, which is of the form

$$\sum_{s,a,b} |\alpha_{s,a,b}|^2 \left(|s\rangle \langle s|\right)^{E_{S,A}} \left(|a\rangle \langle a|\right)^{E_A} \mathrm{Tr}_B \left(|\psi_{s,a,b}\rangle \langle \psi_{s,a,b}|\right)^{AB} \tag{9}$$

that is obtained from the expression (8) by tracing out the subsystem $(\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B})$. The expression for the party B's view can be written down symmetrically:

$$\sum_{s,a,b} |\alpha_{s,a,b}|^2 \left(|s\rangle \langle s|\right)^{E_{S,B}} \left(|b\rangle \langle b|\right)^{E_B} \mathrm{Tr}_A \left(|\psi_{s,a,b}\rangle \langle \psi_{s,a,b}|\right)^{AB}. \tag{10}$$

Remark. We have two remarks about the definition above:

1. Seeing from the formalization of a party's view, we actually implicitly assume w.o.l.g. that any (honest or cheating) party will copy all classical messages generated during the interaction (for a possible later use).

2. *Intermediate* quantum states of a party's system during the interaction do not account for its view; only the state at *end* matters. There are two reasons to justify this: First, general intermediate quantum states cannot be cloned for the use after the interaction. Second, thus defined view fits our applications later.

6.3 The purification of a general quantum protocol

A general quantum protocol could be a hybrid of classical and quantum computations and communications. We can *purify* it so that the resulting protocol consists of only unitary quantum computation and communication (but the security might be compromised). In the below, We fix a way to purify a general quantum protocol based on the formalization of a two-party interaction (Section 6.1), which is almost standard.

Given a general quantum protocol, its *purification* prescribes an interaction between two parties A and B formalized as follows:

- The whole system consists of quantum registers (A, B, E) as described in Section 6.1, except that now the register E is a quantum (rather than classical) register (by abusing the notation).

- For a party $\mathrm{P} \in \{\mathrm{A}, \mathrm{B}\}$, we can purify each operation prescribed by the protocol in the following way, depending on the operation:

    1. *Measurement in the computational basis*: move the qubit that will be measured to the environment E_P.
    2. *A uniformly random coin toss*: introduce an ancilla qubit in the state $|0\rangle$, and perform the Hadamard gate on it. Then move it to the register E_P.

3. *Transmission of a classical bit x from the party A to the party B, and vice versa*: first move the qubit $|x\rangle$ from the register E_A to $\mathsf{E}_{S,A}$, and then copy it to the register $\mathsf{E}_{S,B}$ w.r.t. the computational basis (i.e. introducing an ancilla in the state $|0\rangle$ in the environment $\mathsf{E}_{S,B}$, and then 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.
4. *Non-unitary quantum operation*: it can be simulated by a unitary quantum operations followed by a measurement in the computational basis. The measurement in turn can be simulated in the way as described in item 1.
5. *Classical operation other than a random coin toss.* It can be simulated by a unitary quantum operation in a standard way [NC00, KSV02].

After the purification, the whole system will be in a state of the form

$$\sum_{s,a,b} \alpha_{s,a,b} \, |s\rangle^{E_{S,A}} \, |s\rangle^{E_{S,B}} \, |a\rangle^{E_A} \, |b\rangle^{E_B} \, |\psi_{s,a,b}\rangle^{AB} \tag{11}$$

at any moment of a running of the purified protocol. Compared with the expression (8), here qubits in the environment are no longer collapsed.

By the definition of a party's view of an interaction (Definition 9), the party A's view of a running of a purified (quantum) protocol is given by the state of the subsystem $(\mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A})$ at the end of the interaction, which is of the form

$$\sum_{s,a,a',b} \alpha^*_{s,a',b} \alpha_{s,a,b} \, (|s\rangle \langle s|)^{E_{S,A}} (|a\rangle \langle a'|)^{E_A} \mathrm{Tr}_B (|\psi_{s,a,b}\rangle \langle \psi_{s,a',b}|)^{AB}. \tag{12}$$

It is obtained from the expression (11) by tracing out the subsystem $(\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B})$. The expression for the party B's view can be written down symmetrically, i.e.:

$$\sum_{s,a,b,b'} \alpha^*_{s,a,b,b'} \alpha_{s,a,b,b'} \, (|s\rangle \langle s|)^{E_{S,B}} (|b\rangle \langle b'|)^{E_B} \mathrm{Tr}_A (|\psi_{s,a,b}\rangle \langle \psi_{s,a,b'}|)^{AB} \tag{13}$$

7 The semi-honest security and the security against the purification attack

Based on formalizations of a general quantum two-party interaction and the definition of a party's view during the interaction introduced in the previous section, we formally define the semi-honest security of an *interactive* quantum bit commitment scheme and its purification in this section. They extend from the case of non-interactive quantum bit commitment scheme in a straightforward way, and will be crucial for both the statement and the proof of the round-collapse theorem later in Section 8. Further, for our purpose we initiate a study towards the relationship between the semi-honest security of an interactive quantum bit commitment scheme and its purification. A bridge that connects these two notions of security is a special kind of security that we will refer to as the "security against the purification attack".

The organization of this section is as follows. We formally define the semi-honest security of an interactive quantum bit commitment scheme and its purification in Section 7.1 and Section 7.2, respectively. Also in Section 7.2, we introduce the notion of the security against the purification attack and show its equivalence to the semi-honest security of the purified scheme. Last in Section 7.3, we study the strength of the security against the purification attack.

7.1 The semi-honest security: honest-hiding and honest-binding

We will define the semi-honest security of a general (interactive) quantum bit commitment scheme against the receiver and the sender, which will be referred to as honest-hiding and honest-binding. Specifically, we specialize the formalization of a two-party interaction fixed in Section 6.1 to an (honest) running of the commit stage of the scheme, where we identify the party A (resp. B) with the (honest) sender (resp. receiver). Then the sender's and the receiver's views of the commit stage can be defined correspondingly according to Definition 9. Formally, we introduce the following two definitions.

Definition 10 (Honest-hiding) Consider an honest running of the *commit* stage of an interactive quantum bit commitment scheme. We say that the scheme is statistically (resp. computationally) *honest-hiding* if the (honest) receiver's view of the commit stage corresponding to committing 0 and that corresponding to committing 1 are statistically (resp. computationally) indistinguishable. Or equivalently, consider an honest running of the *commit* stage of an interactive quantum bit commitment scheme in which a uniformly random bit b is committed. We say that the scheme is statistically (resp. computationally) *honest-hiding* if *after* the commit stage, any (possibly cheating) computationally unbounded (resp. polynomial-time) receiver cannot guess the bit b correctly with a non-negligible advantage than just a random guess.

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

Definition 11 (Honest-binding) Consider the following honest-binding game w.r.t. an interactive quantum bit commitment scheme: an arbitrary bit $b \in \{0, 1\}$ is committed in an honest running of the commit stage of the scheme. Later in the reveal stage, a possibly *cheating* sender attempts to open the (quantum) bit commitment as $1 - b$. For doing this, this cheating sender will inherit the (honest) sender's view of the commit stage and may additionally receive an auxiliary quantum state at the beginning of the reveal stage. If this cheating sender succeeds, then we say that it wins the game. We say that the scheme is statistically (resp. computationally) *honest-binding* if any computationally unbounded (resp. polynomial-time) cheating sender in the reveal stage cannot win the game with non-negligible probability.

Remark. We note that our definitions of honest-hiding and honest-binding properties (of a general interactive quantum bit commitment scheme) as above are *consistent* with those of a canonical quantum bit commitment scheme (Definition 4), respectively. However, in the definition of honest-binding in Definition 4, the inability of opening an honest commitment to 0 as 1 is equivalent to that of opening an honest commitment to 1 as 0, which we do not claim here. In spite of this, it turns out for schemes studied in this paper (Section 9 and 10), proofs for these two directions are symmetric.

7.2 The semi-honest security of purified quantum bit commitment schemes and the security against the purification attack

Quantum bit commitment schemes have two stages, the commit stage and the reveal stage. For our purpose, by "purifying an interactive quantum bit commitment scheme" we mean purify only its commit stage.

Definition 12 (The purification of an interactive quantum bit commitment scheme) Given an interactive quantum bit commitment scheme, we can purify its commit stage in the way as described in Section 6.3. We will call the resulting scheme the "purified scheme", or the "purification of the original scheme". Correspondingly, the sender and the receiver of the purified scheme will be referred to as the "purified sender" and "purified receiver" (w.r.t. the original scheme), respectively.

For the purpose of this work, we are especially interested in the relationship between the semi-honest security of the original quantum bit commitment scheme and its purification. Towards studying this relationship, we will first introduce a special kind of attack of an interactive quantum bit commitment scheme which we will refer to as the *purification attack*. Informally, we can view the purification of one party in an interaction as a kind of attack of this party, i.e. the purification attack. Then we establish an equivalence between the security against the purification attack of the original scheme and the semi-honest security of its purification.

The purification attack against the receiver, or *purification-hiding* for short, is formally defined as follows. This definition is adapted straightforwardly from that of honest-hiding w.r.t. an interactive quantum bit commitment scheme (Definition 10).

Definition 13 (Purification-hiding) Given an interactive quantum bit commitment scheme, consider an interaction between the *honest* sender and the *purified* receiver of the commit stage. We say that this scheme is statistically (resp. computationally) secure against the purification attack of the receiver, or statistically (resp. computationally) *purification-hiding*, if the purified receiver's view corresponding to committing 0 and that corresponding to committing 1 are statistically (resp. computationally) indistinguishable. Or equivalently, consider an interaction between the *honest* sender and the *purified* receiver of the commit stage in which a uniformly random bit b is committed. We say that the scheme is statistically (resp. computationally) *purification-hiding* if *after* the commit stage, any (possibly cheating) computationally unbounded (resp. polynomial-time) receiver cannot guess the bit b correctly with a non-negligible advantage than just a random guess.

We define the security against the purification attack of the sender of the original scheme, or *purification-binding* for short, as follows. The definition is adapted straightforwardly from that of honest-binding w.r.t. an interactive quantum bit commitment scheme (Definition 11).

Definition 14 (Purification-binding) Given an interactive quantum bit commitment scheme, we define a purification-binding game w.r.t. this scheme as follows: The purified sender first interacts with the honest receiver in the commit stage when an arbitrary bit $b \in \{0, 1\}$ is committed. Later in the reveal stage, a possibly *cheating* sender attempts to open the (quantum) bit commitment as $1 - b$. For doing this, this cheating sender will inherit the purified sender's view of the commit stage and may additionally receive an auxiliary quantum state at the beginning of the reveal stage. If this cheating sender succeeds, then we say that it wins the game. We say that the scheme is statistically (resp. computationally) secure against the purification attack of the sender, or statistically (resp. computationally) *purification-binding*, if any computationally unbounded (resp. polynomial-time) sender in the reveal stage cannot win the game with non-negligible probability.

The following simple observation is crucial for establishing the equivalence between the security against the purification attack of the original scheme and the semi-honest security of the purified scheme.

Proposition 15 *Purifying an honest party's all operations in a running of a two-party quantum protocol will not affect the other party's view.*

PROOF SKETCH: This is simply because the honest party's behavior can be equivalently viewed as that of its purification after some collapses caused by projective measurements in the computational basis. But whether these collapses really occur or not cannot be observed by the other party. Hence, the other party's views are identical in either cases. ■

Proposition 16 *The security against the purification attack of an interactive quantum bit commitment scheme is equivalent to the semi-honest security of its purification.*

PROOF: Given an interactive quantum bit commitment scheme, we consider the following two interactions:

1. The interaction between the purified sender and the purified receiver of the commit stage, i.e. an (honest) running of the commit stage of the purified scheme;

2. The interaction between the (honest) sender and the purified receiver of the commit stage.

By Proposition 15, the purified receiver's views of the two interactions above are identical. Thus, the purification-hiding property of the original scheme is equivalent to the honest-hiding property of the purified scheme.

Similarly, it is not hard to see the purification-binding property of the original scheme is equivalent to the honest-binding property of its purification by comparing the following two interactions:

1. The interaction between the purified sender and the purified receiver of the commit stage, i.e. an (honest) running of the commit stage of the purified scheme;

2. The interaction between the purified sender and the (honest) receiver of the commit stage.

Note that the purified sender's views of these two interactions are also identical. ■

Due to Proposition 16, in the sequel we will use the security against the purification attack of the original scheme and the semi-honest security of the purified scheme *interchangeably*. In many cases of security analysis, the former is often easier to work with than the latter. This is because we only need to consider the purification of just one (other than two) party with the former.

7.3 The strength of the security against the purification attack

We will show that the security against the purification of a general interactive quantum bit commitment scheme lies *between* the semi-honest security and the full security (i.e. against an arbitrary attack).

First, clearly the security against the purification attack of a general interactive quantum bit commitment scheme is implied by the full security. However, we do not expect the opposite direction to hold[14], because in the definition of the full security a cheating sender can deviate arbitrarily rather than just purifying the honest sender's behavior.

Second, the security against the purification attack implies the semi-honest security, as formally stated in the following proposition.

Proposition 17 *The security against the purification attack of one party of an interactive quantum bit commitment scheme implies its semi-honest security against the same party.*

[14]Specific to quantum bit commitment schemes of the canonical form, interestingly, we have shown that these two notions of security are equivalent (Theorem 2).

PROOF SKETCH: This is simply because the honest party's view can be viewed as that of its purification after some collapses caused by projective measurements in the computational basis. ■

But can the opposite direction of the proposition above hold, or put it in another way, can the honest-hiding and honest-binding properties of any interactive quantum bit commitment scheme be preserved after the purification?

Before answering 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. But this might compromise the semi-honest security of the purified scheme; one is referred to Appendix B for two such examples.

In spite of the above, the semi-honest security of some interactive quantum bit commitment schemes does extend to their purifications. In Section 9 and 10, we develop several techniques for such an extension. In the below, for illustration we identify a simple yet common scenario in which such an extension is possible.

Specifically, we say that one party of an interactive 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 18 *If one party of an interactive 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 of random bits[15] will measure immediately upon receiving them, which will collapse the state of the whole system to the one corresponding to the sender of random bits *not* purifying its operation of tossing random coins. ■

8 A round-collapse theorem

In this section, we will prove a round-collapse theorem as below, which can be viewed as an extension of converting an arbitrary *non-interactive* quantum bit commitment scheme into the canonical form [YWLQ15, FUYZ20].

Theorem 3 (Round-collapse) *If a quantum bit commitment scheme is secure against the purification attack (or equivalently, its purification is semi-honest secure; refer to Definition 13 and 14), then it can be compressed into a scheme of the canonical form (Definition 4) such that:*

1. *It has perfect completeness. That is, if both the sender and the receiver follow the scheme honestly, then the receiver will not reject or abort in both the commit and the reveal stages.*

2. *Both the hiding and binding properties of the original scheme are preserved after the compression. That is, if the original scheme is statistically (resp. computationally) hiding (resp. binding), then the new scheme is also statistically (resp. computationally) hiding (resp. binding) as well.*

[15] Not the receiver of the bit commitment.

At a high level, our *compiler* achieves the round-collapse by delegating the computation of both parties in the commit stage prescribed by the *purification* of the original scheme to the new sender. Later in the reveal stage, the new receiver will check this computation in the commit stage via the *reversible* quantum computation. We will formally prove the round-collapse theorem (Theorem 3) shortly below, by constructing a compiler for the round-compression. The proof relies heavily on the formalization introduced in Section 6.

As a simple application of the round-collapse theorem, we can compress Naor's bit commitment scheme [Nao91] to get a non-interactive one. Nevertheless, this application seems not a big deal, since there already exists a more straightforward (and somewhat simpler) construction (also inspired by Naor's scheme [YWLQ15]). Two non-trivial applications are referred to the next two sections.

Proof of Theorem 3: We first give a compiler for the round-compression that is easier to understand. Then we explain how to simplify it a little bit to make it cleaner. To prove the correctness of the compiler, it suffices to prove that the resulting scheme, which will be in the canonical form, is *semi-honest* secure: by the virtue of Theorem 2, it follows that the resulting scheme will be fully secure (against an arbitrary quantum attack) as well.

For simplicity, we can assume w.o.l.g. that in the first place the original scheme is *normalized* in such a way that in any running of the commit stage, the number of rounds of the interaction is fixed by adding dummy rounds, and each exchanged message (whether classical, quantum, or a hybrid) is of fixed length by padding dummy qubits or bits. As such, the number of rounds of the interaction and the length of each exchanged message in the commit stage only depend on the security parameter.

We will call the given quantum bit commitment scheme the *original scheme*, while its purification the *purified scheme*. Their *commit* stages (*not* including the reveal stages) will be formalized in the way as described in Section 6.1 and Section 6.3, respectively, with the party A identified as the sender and the party B as the receiver. Our *compiler* to achieve the round-collapse is described in Figure 2 (with the security parameter dropped to simplify the notation). We will call this resulting scheme the *compressed scheme*. We are next to prove the correctness of our compiler; that is, the compressed scheme represented by the quantum circuit pair (Q_0, Q_1), which is already in the canonical form, has perfect completeness and satisfies the same flavors of the hiding and binding properties as the original scheme. In the first place, note that by the normalization of the original scheme, the size of each quantum register of $(\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B}, \mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A})$ *at the end of the commit stage* in an execution of the purified scheme only depends on the security parameter[16].

Completeness. The perfect completeness of the compressed scheme comes from the reversibility of the quantum computation directly.

Honest-hiding. We show that the honest-hiding property of the purified scheme translates directly 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 state of the register $\mathsf{C} = (\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B})$ at the end of the commit stage (i.e. the receiver's view) when a bit 0 is committed, and that when a bit 1 is committed, will be statistically (resp. computationally) indistinguishable. This concludes that the scheme (Q_0, Q_1) is statistically (resp. computationally) hiding.

[16]But by our formalization, their sizes are subject to change *during* the commit stage. In spite of this, their total size is fixed and also only depends on the security parameter. In this sense, it is legal to say that quantum circuits Q_0, Q_1 perform on quantum registers $(\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B}, \mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A})$ in our construction of the compiler described in Figure 2.

Commit stage: The new sender simulates an *honest* execution of the commit stage of the *purified* scheme, and then sends the system that corresponds to the receiver of the purified scheme as the *commitment*. Formally, let Q_b ($b \in \{0,1\}$) denote the unitary quantum circuit that simulates an honest execution of the commit stage of the purified scheme when the bit b is committed. This quantum circuit performs on quantum registers $(\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B}, \mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A})$ that are initialized in all $|0\rangle$'s state. After the quantum circuit Q_b is applied, the system of the new sender will be in the state of the form given by the expression (11). Then the new sender sends the quantum register $\mathsf{C} = (\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B})$ (which is in the state of the form given by the expression (13)) to the receiver as the commitment.

Reveal stage: The new sender sends the bit b to reveal, together with all the residual system in its hands, i.e. the quantum register $\mathsf{R} = (\mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A})$, to the receiver. Upon receiving them, the new receiver will perform $Q_b^\dagger$, i.e. the inverse of Q_b, on the whole system (C, R) $(= (\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B}, \mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A}))$ to check if it returns to *all* $|0\rangle$'s state. If yes, then accept; reject otherwise.

Figure 2: A general compiler for the round-compression of quantum bit commitment schemes

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

Consider the moment at the beginning of the reveal stage after an honest execution of the commit stage of the purified scheme when a bit 0 is committed. Then the system (C, R) $(= (\mathsf{E}_{S,B}, \mathsf{E}_B, \mathsf{B}, \mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A}))$ will be in the state $Q_0 |0\rangle$. An arbitrary quantum state $|\psi\rangle$, which is stored in an auxiliary system Z, might also be fed to the cheating sender at this moment.

The honest-binding property (Definition 11) of the purified scheme implies that by just operating on the subsystem (R, Z) $(= (\mathsf{E}_{S,A}, \mathsf{E}_A, \mathsf{A}, \mathsf{Z}))$, *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 $Q_0 |0\rangle$ of the system (C, R) into a (possibly mixed) state whose projection on the vector $Q_1 |0\rangle$ is non-negligible. This is because for otherwise, a cheating sender in the reveal stage could have first transformed the state $Q_0 |0\rangle$ of the system (C, R) into a state that is non-negligibly close (in trace distance) to $Q_1 |0\rangle$ by performing on the system (R, Z), and then proceed *honestly* as prescribed by the purified scheme to try to open the commitment as 1. But this should lead the receiver to accept with non-negligible probability, contradicting to the honest-binding property of the purified scheme.

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

Combining all the above, it follows that the canonical quantum bit commitment scheme (Q_0, Q_1) has perfect completeness and satisfies the same flavors of the hiding and binding properties as the original scheme.

Simplification. We note that there is some redundancy in our construction of the compiler given in Figure 2: the content of the register $\mathsf{E}_{S,A}$ and $\mathsf{E}_{S,B}$ are identical; they both record the classical messages communicated by the two party. It turns out in the construction of the compiler for the round-compression, it suffices to keep track of just one copy of classical messages. In greater detail, in the constructions of quantum circuits Q_0 and Q_1 as described in Figure 2, we can just keep the register $\mathsf{E}_{S,B}$ while dropping the register $\mathsf{E}_{S,A}$. Alternatively, this can be done at the end of the

Commit stage: Let Q_b ($b \in \{0,1\}$) denote the unitary quantum circuit that first simulates the honest execution of the commit stage of the purified scheme when a bit b is committed and then uncomputes the register $\mathsf{E}_{S,A}$. This quantum circuit can also be equivalently viewed as just performing on quantum registers $(\mathsf{E}_S, \mathsf{E}_B, \mathsf{B}, \mathsf{E}_A, \mathsf{A})$ that are initialized in all $|0\rangle$'s state, where the register E_S is just the register $\mathsf{E}_{S,B}$ after renaming. The new sender will send the quantum register $\mathsf{C} = (\mathsf{E}_S, \mathsf{E}_B, \mathsf{B})$ to the receiver as the commitment.

Reveal stage: The new sender will send the bit b to reveal, together with all the residual system in its hands, i.e. the quantum register $\mathsf{R} = (\mathsf{E}_A, \mathsf{A})$, to the receiver. Upon receiving them, the new receiver will perform $Q_b^\dagger$, i.e. the inverse of Q_b, on the whole system (C, R) $(= (\mathsf{E}_S, \mathsf{E}_B, \mathsf{B}, \mathsf{E}_A, \mathsf{A}))$, to check if it returns to *all* $|0\rangle$'s state. If yes, then accept; reject otherwise.

Figure 3: A simplified compiler for the round-compression of quantum bit commitment schemes

construction by uncomputing the register $\mathsf{E}_{S,A}$ given the register $\mathsf{E}_{S,B}$. Now we rename the register $\mathsf{E}_{S,B}$ as E_S. Then the quantum circuit pair (Q_0, Q_1) which represent a new compressed scheme performing on the registers (C, R), where $\mathsf{C} = (\mathsf{E}_S, \mathsf{E}_B, \mathsf{B})$ and $\mathsf{R} = (\mathsf{E}_A, \mathsf{A})$. This simplified compiler is summarized in Figure 3 for convenience.

For the correctness of this simplified compiler, proofs of the perfect completeness and the honest-hiding property of the compressed scheme follow almost the same line as those when the compiler described in Figure 2 is used. For the proof of the honest-binding property, we can first recover the dropped register $\mathsf{E}_{S,A}$ and then argue in the same way as the analysis when the compiler described in Figure 2 is used. We omit the detail here. ■

Remark. One may wonder why the proof of the round-collapse theorem as above does not go through if we only require that the original scheme (rather than its purification) be semi-honest secure. Literally, this is because the system (C, R) is then no longer guaranteed to be in a *pure* state at the end of the commit stage; in turn, we cannot make use of the reversibility of quantum computation.

Hereafter, we will call the scheme after the compression (by feeding it into the compiler described in Figure 3) as the "compressed scheme", as stated in the definition below formally.

Definition 19 (Compressed scheme) Given an arbitrary interactive quantum bit commitment scheme, its associated *compressed scheme* is obtained by feeding it into the compiler described in Figure 3.

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

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

Remark. We stress again that in this work we consider *general* quantum binding properties that *all* quantum bit commitment schemes can satisfy, for which sum-binding is likely to be the strongest.

A specific quantum bit commitment scheme may satisfy even stronger binding properties (e.g. [AC02, Unr16b, Unr16a, GLSV21, BCKM21, BB21]) than sum-binding. But if we feed it into our compiler for the round-compression, these stronger binding properties may be lost; the compressed scheme is only guaranteed sum-binding (or equivalently honest-binding, since it is of the canonical form).

9 Application: compress the NOVY scheme

In this section, we apply the round-collapse theorem (Theorem 3) to *compress* the NOVY scheme [NOVY98], obtaining yet another construction of non-interactive *computationally-binding* quantum bit commitment. The main technical part of this section lies in showing that the NOVY scheme is secure against the purification attack.

In greater detail, 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 a superposition attack which breaks the unique-binding property, but it *does not* break the quantum *sum-binding* property. That is, the NOVY scheme instantiated with a quantum-secure one-way permutation is still possibly sum-binding, but unfortunately we do not have a proof of it yet. In the below, we show that the NOVY scheme instantiated with a quantum-secure one-way permutation is *secure against the purification attack*, which in turn can be *compressed* into a computationally-binding quantum bit commitment scheme of the canonical form by our round-collapse theorem (Theorem 3). The (quantum) analysis here is much simpler than the classical one in [NOVY98].

Formally, we prove the following theorem. And for self-containment, we reproduce the NOVY scheme [NOVY98] in Figure 4.

Theorem 5 *The compressed NOVY quantum bit commitment scheme is perfectly-hiding and computationally-binding if the one-way permutation used within it is quantum-secure. In particular, this compressed scheme can be represented by the quantum circuit pair ensemble* (Q_0, Q_1) *such that*

$$Q_0(n)\left|0\right\rangle = \frac{1}{2^{\frac{n(n+1)}{4}}} \sum_{x,h^1,\ldots,h^{n-1}} \left|x\right\rangle^R \left|h^1,\ldots,h^{n-1},h^1f(x),\ldots,h^{n-1}f(x),a\right\rangle^C, \tag{14}$$

$$Q_1(n)\left|0\right\rangle = \frac{1}{2^{\frac{n(n+1)}{4}}} \sum_{x,h^1,\ldots,h^{n-1}} \left|x\right\rangle^R \left|h^1,\ldots,h^{n-1},h^1f(x),\ldots,h^{n-1}f(x),1-a\right\rangle^C, \tag{15}$$

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: We can purify the NOVY scheme (described in Figure 4) in the way as fixed in Section 6 so that the whole system will be in the quantum state

$$\frac{1}{2^{\frac{n(n+1)}{4}}} \sum_{x,h^1,\ldots,h^{n-1}} \left|x\right\rangle^{E_A} \left|h^1,\ldots,h^{n-1},h^1f(x),\ldots,h^{n-1}f(x),a\right\rangle^{E_S}$$

when a bit 0 is committed honestly, and in the quantum state

$$\frac{1}{2^{\frac{n(n+1)}{4}}} \sum_{x,h^1,\ldots,h^{n-1}} \left|x\right\rangle^{E_A} \left|h^1,\ldots,h^{n-1},h^1f(x),\ldots,h^{n-1}f(x),1-a\right\rangle^{E_S}$$

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 4: The NOVY scheme

when a bit 0 is committed honestly. The expressions of $Q_0(n)$ and $Q_1(n)$ are obtained by the general compiler as described in Figure 3. By the round-collapse theorem (Theorem 3), the correctness of the scheme (Q_0, Q_1) follows by combining Lemma 20 and Lemma 21 that will be proved shortly below. ■

To simplify the notation in our security analysis, we will drop the auxiliary quantum state that the adversary may receive (as specified, explicitly or implicitly, in Definitions 10 and 11). We can do this because our analysis 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. We will also follow this rule in the subsequent sections.

Lemma 20 *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 distribution of the bit a is uniform; we omit the detail here. 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[17] (which we believe 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

[17] We highlight that this is the analysis of the security against a sender who is honest in the commit stage, rather than the NOVY analysis of the security against an arbitrary sender [NOVY98].

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: $h^k \xleftarrow{\$} 0^{k-1}1 \circ \{0,1\}^{n-k}$ 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: $x \xleftarrow{\$} \{0,1\}^n$, $y = f(x)$, $h \xleftarrow{\$} H$. *Intuitively*, the experiment $\mathcal{E}_1$ is to simulate 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: $y' \xleftarrow{\$} \{0,1\}^n$, $y \xleftarrow{\$} \{0,1\}^{n-1} \circ (1 - y'_n)$, $h \xleftarrow{\$} H$ 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),

$$\Pr_{\mathcal{E}_1}[y, y', h] = \Pr_{\mathcal{E}_2}[y, y', h]. \tag{16}$$

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 (16). 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

$$\Pr_{\mathcal{E}_1}[y, y', h] = \Pr_{\mathcal{E}_1}[y] \cdot \Pr_{\mathcal{E}_1}[h] = \frac{1}{2^n} \cdot \frac{1}{2^{n-1}} \frac{1}{2^{n-2}} \cdots \frac{1}{2}. \tag{17}$$

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

$$\Pr_{\mathcal{E}_2}[y, y', h] = \Pr_{\mathcal{E}_2}[y'] \cdot \Pr_{\mathcal{E}_2}[y \mid y'] \cdot \Pr_{\mathcal{E}_2}[h \mid y, y'] = \frac{1}{2^n} \cdot \frac{1}{2^{n-1}} \cdot \Pr_{\mathcal{E}_2}[h \mid y, y']. \tag{18}$$

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 (17) and (18), the equation (16) holds.

This finishes the proof of the lemma. ■

Lemma 21 *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 18 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 will not measure the quantum register in which x and $f(x)$ are stored 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 during the commit stage will uniquely determine the x chosen by the sender, the quantum state is enforced to collapse at the end of the commit stage to the one as if x and $f(x)$ were really measured (at the beginning 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. ■

10 Application: an equivalence between two flavors of quantum bit commitments

In this section, we show that two flavors of quantum bit commitments are *equivalent*, or quantum bit commitment is *symmetric*, through the following theorem.

Theorem 6 *Canonical computationally-hiding statistically-binding quantum bit commitment schemes exist if and only if canonical statistically-hiding computationally-binding quantum bit commitment schemes exist.*

Towards establishing the equivalence above, our basic idea is first using a construction that is a simplification of the CLS scheme [CLS01] to convert the flavor of the given quantum bit commitment scheme, and then compressing the resulting (interactive) scheme into a canonical one using the round-collapse theorem (Theorem 3).

In greater detail, our construction for the purpose of converting the flavor of quantum bit commitments 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 construction is almost the CLS scheme given in [CLS01], but with a significant simplification: all *intermediate verifications* of the commitments by the sender are removed. In spite of this, we will still call it the *CLS scheme* in this paper. Intuitively, these intermediate verifications can be removed because by the virtue of the round-collapse theorem (Theorem 3), we only need a scheme that is just secure against the purification attack for the purpose of the compression. That is, we only need to show that the CLS scheme $\mathrm{QBC}(n)^{\otimes n}$ is secure against the purification attack, or the purified CLS scheme is both honest-hiding and honest-binding. This

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 $(\hat{\theta}_i, \hat{x}_i)$ in a bitwise fashion using a canonical quantum bit commitment scheme (Q_0, Q_1). (We can 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 a scheme that is a somewhat simplification of the original CLS scheme

simplification of the construction will induce a significant simplification of the analysis of the original CLS scheme [CLS01], which is for the full security and quite technically involved.

Remark. Since here our purpose is to show the equivalence between two flavors of quantum bit commitments, we do not intend to explicitly write out the quantum circuit pair (Q_0, Q_1) corresponding to the compressed CLS scheme, though which is straightforward following the compiler described in Figure 3.

We will prove two directions of Theorem 6 in two separate subsections. Specifically, in Section 10.1 we show that instantiating the CLS scheme with a canonical computationally-hiding statistically-binding quantum bit commitment scheme gives rise to a scheme that is statistically purification-hiding and computationally purification-binding. In Section 10.2 we prove the other direction of Theorem 6, namely, instantiating the CLS scheme with a canonical statistically-hiding computationally-binding quantum bit commitment scheme gives rise to a scheme that is computationally purification-hiding and statistically purification-binding.

10.1 The forward direction

Applying the round-collapse theorem (Theorem 3), the forward direction of Theorem 6 follows immediately from Lemma 22 and Lemma 23 that will be stated and proved in the remainder of this subsection.

Lemma 22 *If the canonical quantum bit commitment scheme (Q_0, Q_1) is statistically-binding, then the purification of the CLS scheme $QBC(n)^{\otimes n}$ is statistically honest-hiding (or, the CLS scheme $QBC(n)^{\otimes n}$ is statistically purification-hiding).*

Proof: To simplify our security analysis, by the *perturbation technique* developed in [FUYZ20], we can assume without loss of generality that the canonical quantum bit commitment scheme (Q_0, Q_1) plugged in the atomic scheme QBC (described in Figure 5) is *perfectly* binding.

We first show that the CLS scheme $\mathrm{QBC}(n)^{\otimes n}$ is statistically honest-hiding. Then we show that this statistical honest-hiding property extends to its purification.

The proof that the CLS scheme $\mathrm{QBC}(n)^{\otimes n}$ is statistically honest-hiding follows almost the same line as the proof of that the oversimplified CLS scheme (r.f. Section B) is statistically honest-hiding. This is because if we compare the two atomic schems described in Figure 5 and Figure 8, 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**)[18]. But these commitments clearly *cannot* help the *semi-honest* receiver in cheating.

To show that the statistical honest-hiding property of the scheme $\mathrm{QBC}(n)^{\otimes n}$ 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, note that the scheme (Q_0, Q_1) plugged in is perfectly binding. Then applying the *commitment measurement technique* technique developed in [FUYZ20], the commitment to each pair $(\hat{\theta}_i, \hat{x}_i)$ in step (**R2**) amounts to measure them (but without revealing their values to the sender)[19]. Thus, even the receiver's measurements are purified, the state of the whole system can be equivalently viewed as collapsed to the one corresponding to that each pair $(\hat{\theta}_i, \hat{x}_i)$ is really measured.

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 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.

[18] 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 8.

[19] A hypothetical measurement called "commitment measurement" performed on each quantum bit commitment can be introduced to collapse the committed value without affecting the security; its detail is referred to [FUYZ20]. Anyway, if one is not satisfied with this informal argument, then one is referred to the proof of the backward direction of Theorem 6 in Section 10.2. There, a computational collapse (caused by computationally-binding quantum commitments) is formally established. And arguments for this computational collapse extends to the (information-theoretic) collapse (caused by perfectly-binding quantum commitments) here straightforwardly.

Therefore, the statistical 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 statistical 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 statistical honest-binding property of the CLS scheme $\mathrm{QBC}(n)^{\otimes n}$ (which follows similar to that of the oversimplified CLS scheme discussed in Section B) 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 23 *If the canonical quantum bit commitment scheme (Q_0, Q_1) is computationally-hiding, then the purification of the CLS 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[20]:

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:

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

To establish the purification-binding property of various schemes above, we consider the corresponding purification-binding games described in Definition 14. 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 D. Basically, we use the *hybrid* argument to replace all receiver's commitments with commitments to uniformly random bits in step (**R2**) of the atomic scheme QBC.

[20]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 statistically purification-binding**. We first argue that the scheme M-QBC$(n)^{\otimes n}$ is statistically 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 statistically 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 8. Henceforth, as we have already argued in Subsubsection B.2, the scheme M-QBC$(n))^{\otimes n}$ is statistically 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 statistically purification-binding. Combining with Reduction 1, 2, and 3, this finishes the proof of the lemma. ■

10.2 The backward direction

Now the canonical quantum bit commitment scheme (Q_0, Q_1) plugged in the scheme QBC (described in Figure 5) will be statistically-hiding and computationally-binding.

To prove the backward direction of Theorem 6, after a few thoughts, it turns out that the proof of the forward direction almost extends here in a straightforward way except for one place: namely, in arguing the statistical purification-hiding property (the proof of Lemma 22), we use a technique developed in [FUYZ20] which allows us to view quantum bit commitments with perfect binding as implicit measurements of the committed value. However, here we will use instead quantum bit commitments that are only guaranteed computationally binding, in which case the same technique cannot be applied. Actually, this is just where the analysis of quantum oblivious transfer gets stuck when computationally-binding quantum bit commitments are used [CDMS04], where the difficulty was circumvented by turning to a stronger yet "non-standard" quantum computational string binding property. However, even today there is still no instantiation of quantum commitments with such binding property based on well-founded quantum complexity assumptions.

Fortunately, our situation seems inherently easier than that is considered in [CDMS04], because we only need to take into account of the purification attack (as opposed to an arbitrary attack). It turns out that in our situation we can show that quantum commitments with just the computational honest-binding property indeed can realize a *computational collapse* that is similar to the one caused by statistically-binding quantum commitments as argued in the proof of Lemma 22.

Formally, the proof of the backward direction of Theorem 6 relies on a what we will refer to as the *computational collapse theorem*, which might be of independent interest. Its proof, which is deferred to Appendix E, is inspired by the technique developed in [Yan21] to establish the quantum computational string predicate-binding property.

Theorem 7 (Computational collapse) *Suppose that (Q_0, Q_1) is a computationally ϵ-binding quantum bit commitment scheme. Then for each $b \in \{0,1\}$,*

$$\left\| \Pi_b U \sum_{s\in\{0,1\}^m} \alpha_s |s\rangle (Q_s |0\rangle)^{C^{\otimes m} R^{\otimes m}} |\psi_s\rangle |0\rangle^B \right\|^2 \leq \sum_{s\in\{0,1\}^m} |\alpha_s|^2 \left\| \Pi_b U |s\rangle (Q_s |0\rangle)^{C^{\otimes m} R^{\otimes m}} |\psi_s\rangle |0\rangle^B \right\|^2 + m\epsilon,$$

where the projector $\Pi_b = |b\rangle\langle b|$ acts on the qubit B; the efficiently realizable unitary transformation U is arbitrary and acts on the whole system other than the system $C^{\otimes m}$; complex coefficients α_s's satisfy $\sum_{s\in\{0,1\}^m} |\alpha_s|^2 = 1$; $|\psi_s\rangle$ is a unit vector; and the quantum circuit Q_s is given by the equation (4).

Now we are ready to sketch a proof of the backward direction of Theorem 6 using Theorem 7.

Proof of Theorem 6 (the backward direction): It suffices to prove that the CLS scheme QBC$(n)^{\otimes n}$, i.e. the parallelization of the atomic scheme QBC described in Figure 5 with a canonical statistically-

hiding computationally-binding quantum bit commitment scheme plugged in, is both computationally purification-hiding and statistically purification-binding.

The proof of the statistical purification-binding property follows almost the same line as that of Lemma 23, except thatwhere "computationally hiding" is replaced with "statistically hiding" literally.

For the proof of the computational purification-hiding property, we will adapt the proof of Lemma 22. As discussed, it suffices to show that using computationally-binding quantum commitments will result in a similar collapse of the quantum state as that is caused by using perfectly-binding quantum commitments. We are left to elaborate how to apply the *computational collapse theorem* (Theorem 7) to justify this.

Recall that in the proof of Lemma 22, we argue that although the cheating receiver will not measure each pair $(\hat{\theta}_i, \hat{x}_i)$, the corresponding collapse is enforced by perfectly-binding quantum bit commitments. Now we are going to argue that using computationally-binding quantum bit commitments will cause a similar effect. Specifically, suppose that a uniformly random bit $b \in \{0,1\}$ has been chosen by the sender to commit. The quantum state of the whole system at the end of the commit stage can be written in the following form:

$$\sum_{\hat{\theta},\hat{x}\in\{0,1\}^n} \frac{1}{2^n} |\hat{\theta}\rangle|\hat{x}\rangle \otimes \left(Q_{\hat{\theta}} |0\rangle\right)^{C^{\otimes n}R^{\otimes n}} \left(Q_{\hat{x}} |0\rangle\right)^{C^{\otimes n}R^{\otimes n}} \otimes |\psi_{\hat{\theta},\hat{x}}\rangle |0\rangle^B , \tag{19}$$

where quantum circuits $Q_{\hat{\theta}}$ and $Q_{\hat{x}}$ are circuits used to commit the chosen bases $\hat{\theta}$ and the measurement outcomes $\hat{x}$, respectively; the qubit B will be used to store the guess for the bit b that is committed by the sender; and $|\psi_{\hat{\theta},\hat{x}}\rangle$ is the state of the residual system. Note that the quantum state corresponding to $(\hat{\theta}, \hat{x})$ being measured at this moment is given by the uniform mixture of the quantum state ensemble

$$\left\{ |\hat{\theta}\rangle|\hat{x}\rangle \otimes \left(Q_{\hat{\theta}} |0\rangle\right)^{C^{\otimes n}R^{\otimes n}} \left(Q_{\hat{x}} |0\rangle\right)^{C^{\otimes n}R^{\otimes n}} \otimes |\psi_{\hat{\theta},\hat{x}}\rangle |0\rangle^B \right\}_{\hat{\theta},\hat{x}\in\{0,1\}^n} . \tag{20}$$

Next, the cheating receiver may attack by performing a polynomial-time realizable unitary operation U on its system, which in particular does *not* touch the commitment registers $\mathsf{C}^{\otimes 2n}$. (It may also additionally receives a quantum state for the attack, but which will not affect the analysis below; so we omit it.) After the attack, seeing from the expression (19) the success probability of the receiver guessing the random bit b correctly is given by

$$\left\| \Pi_b U \sum_{\hat{\theta},\hat{x}\in\{0,1\}^n} \frac{1}{2^n} |\hat{\theta}\rangle|\hat{x}\rangle \otimes \left(Q_{\hat{\theta}} |0\rangle\right)\left(Q_{\hat{x}} |0\rangle\right) \otimes |\psi_{\hat{\theta},\hat{x}}\rangle |0\rangle^B \right\|^2 . \tag{21}$$

In comparison, seeing from the expression (20) the success probability when the attack U performs on the collapsed quantum state (i.e. obtained by measuring $(\hat{\theta}, \hat{x})$ of the quantum state (19)) is given by

$$\sum_{\hat{\theta},\hat{x}\in\{0,1\}^n} \frac{1}{2^{2n}} \left\| \Pi_b U \left(|\hat{\theta}\rangle|\hat{x}\rangle \otimes \left(Q_{\hat{\theta}} |0\rangle\right)\left(Q_{\hat{x}} |0\rangle\right) \otimes |\psi_{\hat{\theta},\hat{x}}\rangle |0\rangle^B \right) \right\|^2 , \tag{22}$$

Now we are ready to apply the computational collapse theorem. Specifically, we instantiate parameters $m, s, |\psi_s\rangle, \Pi_b, U$ and α_s for each $s \in \{0,1\}^m$ in Theorem 7 with $2n, (\hat{\theta}, \hat{x}), |\psi_{\hat{\theta},\hat{x}}\rangle, \Pi_b, U$ and $1/2^{2n}$, respectively. It follows that if the *real* quantum state (given by the expression (19)) of the whole system at the end of the commit stage is replaced by the *collapsed* one corresponding to

$(\hat{\theta}, \hat{x})$ is measured (given by the expression (20)), then the receiver's success probability of guessing the committed bit b correctly decreases at most $2n\epsilon$ (which is negligible).

Hence, the proof Lemma 22 can be modified to establish the computational purification-hiding property here by just replacing the information-theoretic collapse caused by perfectly-binding quantum bit commitments with the computational collapse caused by computationally-binding quantum bit commitments. ■

11 Parallel composition of a canonical statistically-binding quantum bit commitment scheme

In cryptography, a typical way to commit a string is to commit it in a *bitwise* fashion using a bit commitment scheme. We naturally ask, what binding property can we obtain if we commit a string in a bitwise fashion using a canonical *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 will the parallel composition of a canonical *statistically-binding* quantum bit commitment scheme, establishing the (almost) strongest quantum string 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 canonical *computationally-binding* quantum bit commitment scheme.

11.1 Quantum string sum-binding

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

Definition 24 (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

$$\sum_{s \in \{0,1\}^m} p_s < 1 + negl(n). \tag{23}$$

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]. Roughly speaking, the main difficulty comes from that there are *exponentially* many strings (2^m, exactly) in $\{0,1\}^m$, but we still hope bound the sum of exponentially many advantages by a negligible quantity. In spite of this, we can prove the following parallel composition theorem w.r.t. a canonical statistically-binding quantum bit commitment scheme.

Theorem 8 (Parallel composition) *Suppose that a canonical quantum bit commitment scheme (Q_0, Q_1) is statistically binding. Then the quantum string commitment scheme obtained by composing it in parallel is statistically sum-binding. Formally, if the scheme (Q_0, Q_1) is statistically*

$\epsilon(n)$-*binding where the function* $\epsilon(\cdot)$ *is negligible, then*

$$\sum_{s\in\{0,1\}^m} p_s \leq 1 + O(m^2\epsilon). \tag{24}$$

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, Q_1) to commit an m-bit string s in a bitwise fashion, the quantum (string) commitment (stored in the quantum register $\mathsf{C}^{\otimes m}$) is given by the quantum state

$$\rho_s = \bigotimes_{i=1}^{m} \rho_{s_i}, \tag{25}$$

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 25 ([YWLQ15]) *Let* (Q_0, Q_1) *be a 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 26 ([YWLQ15]) *Let* (Q_0, Q_1) *be a canonical 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 25 and the equation (25), 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 (26) 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 F.

Lemma 27 *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*

$$\left| \left\| \sum_{s\in\{0,1\}^m} \alpha_s |\psi_s\rangle \right\|^2 - \sum_{s\in\{0,1\}^m} \alpha_s^2 \||\psi_s\rangle\|^2 \right| \leq m^2\epsilon \sum_{s\in\{0,1\}^m} \alpha_s^2. \tag{26}$$

Now we are ready to prove Theorem 8.

PROOF of Theorem 8: 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 25, 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 2 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,

$$\begin{aligned}
\sum_{s\in\{0,1\}^m} |\langle\varphi|\psi_s\rangle|^2 &= \sum_{s\in\{0,1\}^m} \Big|\sum_{t\in\{0,1\}^m} \alpha_t\langle\psi_t|\psi_s\rangle\Big|^2 \\
&\leq \sum_{s\in\{0,1\}^m}\sum_{t\in\{0,1\}^m} \alpha_t^2\,|\langle\psi_t|\psi_s\rangle|^2 \qquad \text{(triangle inequality)} \\
&= \sum_{t\in\{0,1\}^m} \alpha_t^2 \sum_{j=0}^{m} \sum_{\substack{s\in\{0,1\}^m:\\ \mathrm{dist}(s,t)=j}} |\langle\psi_t|\psi_s\rangle|^2 \\
&\leq \sum_{t\in\{0,1\}^m} \alpha_t^2 \sum_{j=0}^{m} \sum_{\substack{s\in\{0,1\}^m:\\ \mathrm{dist}(s,t)=j}} \mathrm{F}(\rho_s,\rho_t)^2 \qquad \text{(Fact 2)} \\
&\leq \sum_{t\in\{0,1\}^m} \alpha_t^2 \sum_{j=0}^{m} \sum_{\substack{s\in\{0,1\}^m:\\ \mathrm{dist}(s,t)=j}} \epsilon^{2j} \qquad \text{(Lemma 26)} \\
&= \sum_{t\in\{0,1\}^m} \alpha_t^2 \sum_{j=0}^{m} \binom{m}{j} \epsilon^{2j} \\
&= (1+\epsilon^2)^m \sum_{t\in\{0,1\}^m} \alpha_t^2. \qquad (27)
\end{aligned}$$

We are left to bound $\sum_{t\in\{0,1\}^m} \alpha_t^2$. To this end, we apply Lemma 27; specifically, we replace $|\psi_s\rangle$ and $\sum_{s\in\{0,1\}^m} \alpha_s\,|\psi_s\rangle$ in Lemma 27 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 $|\langle\psi_{t'}|\,\psi_t\rangle| \leq \epsilon^{\mathrm{dist}(t,t')}$ is guaranteed by Lemma 26.

Hence,

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

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. $\sum_{t\in\{0,1\}^m} \alpha_t^2 \geq 1$. In this case, we have $m^2\epsilon \sum_{t\in\{0,1\}^m} \alpha_t^2 \geq \sum_{t\in\{0,1\}^m} \alpha_t^2 - 1$. Rewritting terms, we have $\sum_{t\in\{0,1\}^m} \alpha_t^2 \leq 1/(1-m^2\epsilon)$.

It follows that in either cases, we have

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

Plugging the upper bound above in the inequality (27), we have

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

This completes the proof of the theorem. ■

11.2 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 (24) 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 28 (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 24) 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 24). 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.

12 Conclusion and open problems

In this work, we study general properties of complexity-based quantum bit commitments. Specifically, we show that any quantum bit commitment scheme can be compressed into the canonical form (Theorem 3), which is non-interactive and whose semi-honest security implies the full security (Theorem 2). This yields several applications (Section 5 and 9), allowing us to not only obtain new constructions of quantum bit commitment but also simplify the security analysis of existing ones. Moreover, it also enables us to establish an equivalence between two flavors of quantum bit commitments (Theorem 6). Regarding the parallel composition, we establish the strongest quantum statistical string sum-binding property by composing a canonical statistically-binding quantum bit commitment scheme in parallel (Theorem 8).

We propose to study quantum bit commitments in future from both quantum cryptography and quantum complexity theory perspectives. In the below, we summarize and raise some open problems that are related to this work and beyond:

1. In previous applications of statistically-binding quantum bit commitments [YWLQ15, FUYZ20], a string is committed in a bitwise fashion. If we view this as giving rise to a quantum string commitment, then after taking a closer look at those security analysis, we find that the

security of corresponding constructions essentially only relies on the string *honest-binding* property. Informally, the string honest-binding property states that an honest commitment to a binary string cannot be opened as any other string except for a negligible probability. Then an interesting open question is, can we find any applications whose security will make an essential use of the quantum string sum-binding property as proved in Section 11, something like that is done in [CDMS04]?

2. In Section 11, we only discuss the parallel composition of of a canonical statistically-binding quantum bit commitment scheme. But what string binding property (preferably stronger than honest-binding) can we obtain if we compose a canonical *computationally-binding* quantum bit commitment scheme 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-interactivity of quantum bit commitments). 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 [Yan21], where a so-called "predicate-binding" property is established and turns out to be useful. We expect more positive results in this regard in future.

3. In this work, we plug a canonical computationally-binding quantum bit commitment scheme in a somewhat simplified CLS scheme for the purpose of converting its flavor (Section 10.2). This construction essentially realizes a quantum oblivious transfer (QOT) that satisfies the following security requirements: the purified receiver of QOT does not know the other bit that the honest sender is given as input , while the purified sender of QOT does not know which input bit the honest receiver is aware of. We highlight that this security is neither the security against an arbitrary quantum attack nor the *simulation security* [GLSV21, BCKM21] that is preferable in cryptography. Recall that we prove a computational collapse theorem (Theorem 7) for the analysis this security. So a natural open question is, can this computational-collapse technique be extended to show the same security but against an arbitrary quantum attack (as opposed to against the purification attack) for the original QOT protocol (or some of its variant like the one considered in [CDMS04]) with a canonical computationally-binding quantum bit commitment scheme plugged in [CK88]? Possibly combine it with the quanum sampling technique devised in [BF10]? Though this security is not as good as the simulation security, the corresponding construction is much simpler (in particular, consisting of constant number of rounds). And it might be sufficient in some interesting applications, just like [CLS01] and here for the purpose of converting the flavor of quantum bit commitment.

4. As mentioned in Section 1.4, it is interesting to explore whether quantum bit commitments conversely imply pseudorandom quantum states.

5. This open question regards *quantum hardness amplification*. The big question here is, if a unitary operation U is hard to realize (e.g. requires super-polynomial number of elementary quantum gates), then is the unitary operation $U^{\otimes n}$ (i.e. perform the unitary operation U n times in parallel) harder? Specific to a canonical quantum bit commitment scheme, we ask: can the parallel composition of quantum bit commitments reduce the binding error? The answer is a trivial "yes" w.r.t. a canonical statistically-binding quantum bit commitment scheme, whose binding error can be captured by an information-theoretic notion known as *fidelity* [YWLQ15]. However, the answer becomes unclear when it comes to a canonical computationally-binding quantum bit commitment scheme. In particular, can the parallel

composition reduce the *computational* binding error from, say 1/2 or even inverse polynomial, to a negligible quantity? This question looks very similar to the question of amplifying the one-wayness of one-way functions in classical cryptography [Yao82]. If the answer to this question is "yes", then combining it with results in [Wat02, YWLQ15, FUYZ20, Yan21] will complete the proof for an equivalence between quantum bit commitment and quantum zero-knowledge like in the classical setting [OV08].

6. Some fancier open questions include: can quantum bit commitment find more applications in quantum cryptography? Are there any other quantum cryptographic applications (besides quantum zero-knowledge and quantum oblivious transfer) that also imply quantum bit commitment? That is, can quantum bit commitment serve as the foundation of quantum cryptography?

7. Finally, the perhaps biggest open question that is related to the quantum complexity theory is: do complexity-based quantum bit commitments really exist?

Acknowledgements. We thank Dominique Unruh and Takeshi Koshiba for bringing the reference [WW06] to our attention. Many thanks also go to Dominique Unruh, Takeshi Koshiba, Prabhanjan Ananth, Luowen Qian, Henry Yuen, and the anonymous referees of ICALP 2021 for their useful suggestions and valuable comments on earlier drafts of this paper.

References

[Aar16] Scott Aaronson. The complexity of quantum states and transformations: From quantum money to black holes. *arXiv:1607.05256*, 2016. 13

[AC02] Mark Adcock and Richard Cleve. A quantum Goldreich-Levin theorem with cryptographic applications. In *STACS*, pages 323–334. Springer, 2002. 4, 5, 6, 13, 34

[AQY21] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. Cryptology ePrint Archive, Report 2021/1663, 2021. https://ia.cr/2021/1663. 9, 10, 13

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Private communication, 2022. 1

[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. 5

[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. 4, 56

[BB21] Nir Bitansky and Zvika Brakerski. Classical binding for quantum commitments. In Kobbi Nissim and Brent Waters, editors, *TCC*, volume 13042 of *Lecture Notes in Computer Science*, pages 273–298. Springer, 2021. 5, 9, 13, 34

[BC90] Gilles Brassard and Claude Crépeau. Quantum bit commitment and coin tossing protocols. In *CRYPTO*, pages 49–61, 1990. 4

[BCKM21] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In Tal Malkin and Chris Peikert, editors, *CRYPTO*, volume 12825 of *Lecture Notes in Computer Science*, pages 467–496. Springer, 2021. 5, 12, 13, 34, 50

[BCMS98] Gilles Brassard, Claude Crépeau, Dominic Mayers, and Louis Salvail. Defeating classical bit commitments with a quantum computer. *arXiv preprint quant-ph/9806031*, 1998. 34

[BF10] Niek J. Bouman and Serge Fehr. Sampling in a quantum population, and applications. In *CRYPTO*, pages 724–741, 2010. 50

[Blu86] Manuel Blum. How to prove a theorem so no one else can claim it. In *Proceedings of the International Congress of Mathematicians*, volume 1, page 2, 1986. 5

[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. 4, 5, 6, 8, 9, 11, 12, 43, 45, 48, 49, 50

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *FOCS*, pages 42–52, 1988. 8, 12, 50

[CKR11] André Chailloux, Iordanis Kerenidis, and Bill Rosgen. Quantum commitments from complexity assumptions. In *ICALP (1)*, pages 73–85, 2011. 5

[CLS01] Claude Crépeau, Frédéric Légaré, and Louis Salvail. How to convert the flavor of a quantum bit commitment. In *EUROCRYPT*, pages 60–77, 2001. 4, 8, 12, 13, 37, 38, 40, 50, 57

[DFL+09] Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols via commit-and-open. In *CRYPTO*, pages 408–427, 2009. 12

[DFS04] Ivan Damgård, Serge Fehr, and Louis Salvail. Zero-knowledge proofs and string commitments withstanding quantum attacks. In *CRYPTO*, pages 254–272, 2004. 5, 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. 4, 5, 6, 7, 13, 20

[FUYZ20] Junbin Fang, Dominique Unruh, Jun Yan, and Dehua Zhou. How to base security on the perfect/statistical binding property of quantum bit commitment? Cryptology ePrint Archive, Report 2020/621, 2020. https://ia.cr/2020/621. 1, 2, 5, 7, 8, 9, 10, 11, 12, 13, 15, 17, 30, 39, 43, 49, 50, 51, 55

[GLSV21] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT*, volume 12697 of *Lecture Notes in Computer Science*, pages 531–561. Springer, 2021. 5, 6, 12, 13, 34, 50

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991. 5

[Gol90] Oded Goldreich. A note on computational indistinguishability. *Inf. Process. Lett.*, 34(6):277–281, 1990. 13

[Gol01] Oded Goldreich. *Foundations of Cryptography, Basic Tools*, volume I. Cambridge University Press, 2001. 13

[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, 7

[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. 4, 9

[HSS11] Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. In *CRYPTO*, pages 411–428, 2011. 60

[IL89] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *FOCS*, pages 230–235, 1989. 4

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO*, volume 10993 of *Lecture Notes in Computer Science*, pages 126–152. Springer, 2018. 9, 13, 17

[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. 4, 5, 7, 13

[KO11] Takeshi Koshiba and Takanori Odaira. Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function. *arXiv:1102.3441*, 2011. 4, 5, 7, 13

[Kob08] Hirotada Kobayashi. General properties of quantum zero-knowledge proofs. In *TCC*, pages 107–124, 2008. arXiv.org:0705.1129. 11

[Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. In Min-Hsiu Hsieh, editor, *TQC*, volume 197 of *LIPIcs*, pages 2:1–2:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. 9

[KSV02] Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation, volume 47 of Graduate Studies in Mathematics*. American Mathematical Society, 2002. 26

[KW00] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *STOC*, pages 608–617, 2000. 11

[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. 4

[Lég00] Frédéric Légaré. *Converting the flavor of a quantum bit commitment*. PhD thesis, McGill University, 2000. 40

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, 1997. 4, 23, 56

[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, 7

[MY21] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments without one-way functions. *arXiv preprint arXiv:2112.06369*, 2021. 5, 9, 13

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *J. Cryptology*, 4(2):151–158, 1991. 4, 8, 9, 12, 31, 59

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and Quantum Informatioin*. Cambridge University Press, 2000. 14, 26

[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. 4, 7, 8, 34, 35

[OV08] Shien Jin Ong and Salil P. Vadhan. An equivalence between zero knowledge and commitments. In *TCC*, pages 482–500, 2008. 13, 51

[RW05] Bill Rosgen and John Watrous. On the hardness of distinguishing mixed-state quantum computations. In *CCC*, pages 344–354. IEEE Computer Society, 2005. 5, 13

[Unr12] Dominique Unruh. Quantum proofs of knowledge. In *EUROCRYPT*, pages 135–152, 2012. 10

[Unr16a] Dominique Unruh. Collapse-binding quantum commitments without random oracles. In *ASIACRYPT*, pages 166–195, 2016. 5, 19, 34

[Unr16b] Dominique Unruh. Computationally binding quantum commitments. In *EUROCRYPT*, pages 497–527, 2016. 4, 5, 6, 19, 34

[vdG97] Jeroen van de Graaf. *Towards a formal definition of security for quantum protocols*. PhD thesis, Université de Montréal, 1997. 5, 34

[Wat02] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *FOCS*, pages 459–468, 2002. 5, 13, 51

[Wat18] John Watrous. *Theory of Quantum Information*. Cambridge University Press, 2018. 14

[Win99] Andreas J. Winter. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inf. Theory*, 45(7):2481–2485, 1999. 10

[WW06] Stefan Wolf and Jürg Wullschleger. Oblivious transfer is symmetric. In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 222–232. Springer, 2006. 8, 51

[Yan12] Jun Yan. Complete problem for perfect zero-knowledge quantum proof. In *SOFSEM*, pages 419–430, 2012. 5, 13

[Yan20] Jun Yan. General properties of quantum bit commitments. Cryptology ePrint Archive, Report 2020/1488, 2020. https://ia.cr/2020/1488. 9

[Yan21] Jun Yan. Quantum computationally predicate-binding commitments with application in quantum zero-knowledge arguments for NP. In *ASIACRYPT*, volume 13090 of *Lecture Notes in Computer Science*, pages 575–605. Springer, 2021. 1, 5, 6, 7, 8, 10, 11, 13, 17, 43, 50, 51

[Yao82] Andrew Chi-Chih Yao. Theory and applications of trapdoor functions (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982*, pages 80–91, 1982. 13, 51

[Yao95] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *STOC*, pages 67–75, 1995. 12, 13

[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. 4, 5, 6, 7, 9, 10, 13, 16, 17, 30, 31, 46, 48, 49, 50, 51, 59, 60

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

Lemma 29 (The restatement of Lemma 3) *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 $1/k\cdot\sum_{i=1}^{k}\|\Gamma_iU_i|\psi\rangle\|^2\geq 1-\eta$, we have

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

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

$$\sum_{i=1}^{k}\left\|U_i^\dagger\Gamma_iU_i|\psi\rangle-|\psi\rangle\right\|^2\leq k\eta. \tag{28}$$

We claim that

$$\left\||\psi\rangle-(U_k^\dagger\Gamma_kU_k)\cdots(U_1^\dagger\Gamma_1U_1)|\psi\rangle\right\|^2\leq\sum_{i=1}^{k}\left\|U_i^\dagger\Gamma_iU_i|\psi\rangle-|\psi\rangle\right\|^2. \tag{29}$$

If this is true, then combining the inequalities (28) and (29), 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 (29), which will be done by induction on k.

1. $\underline{k = 1}$. The "=" of inequality (29) holds trivially.
2. Suppose that the inequality (29) holds for $\underline{k-1}$. 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 (29), and in turn the proof of the lemma. ■

B Two simple quantum bit commitment 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 statistically (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 oversimplified CLS scheme as we call) is helpful in understanding that of the correct one in Section 10.1.

B.1 The BB84 scheme

The *non-interactive* BB84 scheme [BB84, May97] is described in Figure 7. We next informally argue that the BB84 scheme is statistically honest-hiding and statistically honest-binding.

The BB84 scheme is *statistically honest-hiding*, by noting that both the honest commitment to 0 and that to 1 are just the maximally mixed state. The scheme is *statistically honest-binding*,

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 7: The BB84 scheme

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 $\hat{x}_i$ 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.

B.2 An oversimplified CLS scheme

The oversimplified CLS scheme, which is adapted from [CLS01], is the *parallel* composition of the atomic scheme as described in Figure 8. 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 argue that this oversimplified CLS scheme is statistically honest-hiding and statistically honest-binding.

Statistical honest-hiding. Consider an honest running of the commit stage of the *atomic* scheme. Note that with an overwhelming probability, we have $\hat{\theta}_i \neq \theta_i$ for nearly *half* of indices i where

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 8: The atomic scheme which composes in parallel gives the oversimplified CLS scheme

$1 \leq i \leq n$. Since $|I_0| + |I_1| = 2n/3 > n/2$, 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 oversimplified CLS scheme is *statistically honest-hiding*.

Statistical 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 oversimplified 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 oversimplified CLS scheme is statistically 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 the 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 been measured yet.

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 oversimplified CLS scheme is *not* purification-hiding.

C 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].

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 bitwise xor) to the receiver. The *reveal* stage is canonical; namely, the sender sends its random coin tosses s to the receiver for verification.

To compress Naor's scheme, we consider an honest execution of the commit stage of the *purified* Naor's scheme, which can be formalized in the way as described in Section 6. At the end of the commit stage, when a bit 0 is committed the whole system will be in the state

$$\frac{1}{\sqrt{2^{4n}}} \sum_{\substack{s \in \{0,1\}^n, \\ r \in \{0,1\}^{3n}}} |s\rangle^{E_A} |G(s), r\rangle^{E_{S,A}} |G(s), r\rangle^{E_{S,B}} ; \tag{30}$$

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

$$\frac{1}{\sqrt{2^{4n}}} \sum_{\substack{s \in \{0,1\}^n, \\ r \in \{0,1\}^{3n}}} |s\rangle^{E_A} |G(s) \oplus r, r\rangle^{E_{S,A}} |G(s) \oplus r, r\rangle^{E_{S,B}} . \tag{31}$$

By the general compiler (Figure 3, within the proof of Theorem 3), the compressed scheme is given by the quantum circuit pair (Q_0, Q_1) as follows:

$$Q_0 |0\rangle \stackrel{def}{=} \frac{1}{\sqrt{2^{4n}}} \sum_{\substack{s\in\{0,1\}^n,\\ r\in\{0,1\}^{3n}}} |s\rangle^R |G(s), r\rangle^C , \tag{32}$$

$$Q_1 |0\rangle \stackrel{def}{=} \frac{1}{\sqrt{2^{4n}}} \sum_{\substack{s\in\{0,1\}^n,\\ r\in\{0,1\}^{3n}}} |s\rangle^R |G(s) \oplus r, r\rangle^C . \tag{33}$$

Since Naor's scheme is quantum-secure given that the pseudorandom generator $G(\cdot)$ is secure against any polynomial-time quantum distinguisher [HSS11], applying Theorem 3 concludes that the scheme (Q_0, Q_1) is computationally hiding and statistically binding. Its security can also be established in a more direct way like that in [YWLQ15].

D Reduction 1 in Lemma 23

We inherit all notations in Section 10.1. 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 statistically 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[21] 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 statistically purification-binding and S^* breaks the computational purification-binding property of the scheme $\mathrm{QBC}(n)^{\otimes n}$, we have

$$\Pr_{\mathrm{H}_0}[\mathsf{succ}] - \Pr_{\mathrm{H}_{2n^2}}[\mathsf{succ}] > \frac{1}{q(n)}, \tag{34}$$

[21] Recall that regarding the purification-binding (Definition 14), the sender's operation is fixed to be the purification of that of the honest sender in the commit stage.

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 $k \in \{0, 1, \ldots, 2n^2 - 1\}$,

$$\Pr_{b \leftarrow \{0,1\}, B^*}[\tilde{b} = b] = \frac{1}{2n^2} \sum_{k=0}^{2n^2-1} \Pr_{b \leftarrow \{0,1\}, B_k^*}\big[\tilde{b} = b\big], \tag{35}$$

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,

$$\begin{aligned}
\Pr_{b \leftarrow \{0,1\}, B_k^*}\big[\tilde{b} = b\big] &= \Pr_{b \leftarrow \{0,1\}, B_k^*}\big[(\tilde{b} = b) \wedge \mathsf{succ}\big] + \Pr_{b \leftarrow \{0,1\}, B_k^*}\big[(\tilde{b} = b) \wedge \overline{\mathsf{succ}}\big] \\
&\geq \Pr\big[(\tilde{b} = b) \wedge \mathsf{succ} | b = b_{k+1}\big] \cdot \Pr\big[b = b_{k+1}\big] + \Pr\big[(\tilde{b} = b) | \overline{\mathsf{succ}}\big] \cdot \Pr[\overline{\mathsf{succ}}] \\
&= \frac{1}{2} \Pr\big[\mathsf{succ} | b = b_{k+1}\big] + \frac{1}{2} \Pr[\overline{\mathsf{succ}}],
\end{aligned} \tag{36}$$

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,

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

- 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

$$\Pr_{b \leftarrow \{0,1\}, B_k^*}\big[\mathsf{succ} | b = b_{k+1}\big] = \Pr_{\mathrm{H}_k}\big[\mathsf{succ}\big], \qquad \Pr_{b \leftarrow \{0,1\}, B_k^*}[\mathsf{succ}] = \Pr_{\mathrm{H}_{k+1}}[\mathsf{succ}], \tag{37}$$

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 (36) and (37), we have

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

Plug this inequality in the equation (35),

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

where the last "$\geq$" follows from the inequality (34). 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 statistically purification-binding, then the scheme QBC$(n)^{\otimes n}$ computationally purification-binding.

E A proof of the computational collapse theorem

Theorem 9 (A restatement of Theorem 7) *Suppose that (Q_0,Q_1) is a computationally ϵ-binding quantum bit commitment scheme. Then for each $b\in\{0,1\}$,*

$$\left\|\Pi_b U\sum_{s\in\{0,1\}^m}\alpha_s|s\rangle\left(Q_s|0\rangle\right)^{C^{\otimes m}R^{\otimes m}}|\psi_s\rangle|0\rangle^B\right\|^2\leq\sum_{s\in\{0,1\}^m}|\alpha_s|^2\left\|\Pi_b U|s\rangle\left(Q_s|0\rangle\right)^{C^{\otimes m}R^{\otimes m}}|\psi_s\rangle|0\rangle^B\right\|^2+m\epsilon,$$

where the projector $\Pi_b=|b\rangle\langle b|$ acts on the qubit B; the efficiently realizable unitary transformation U is arbitrary and acts on the whole system other than the system $C^{\otimes m}$; complex coefficients α_s's satisfy $\sum_{s\in\{0,1\}^m}|\alpha_s|^2=1$; $|\psi_s\rangle$ is a unit vector; and the quantum circuit Q_s is given by the equation (4).

Proof: Actually, we will prove a strengthening of the theorem as follows: for each k $(0\leq k\leq m)$ and each $x\in\{0,1\}^{m-k}$, it holds that

$$\left\|\Pi_b U\sum_{s\in\{0,1\}^k\circ x}\alpha_s|s\rangle\left(Q_s|0\rangle\right)^{C^{\otimes m}R^{\otimes m}}|\psi_s\rangle|0\rangle^B\right\|^2\leq\sum_{s\in\{0,1\}^k\circ x}|\alpha_s|^2\left(\left\|\Pi_b U|s\rangle\left(Q_s|0\rangle\right)^{C^{\otimes m}R^{\otimes m}}|\psi_s\rangle|0\rangle^B\right\|^2+k\epsilon\right),\tag{38}$$

where $\{0,1\}^k\circ x$ denotes the set of all m-bit strings with the suffix x. Then what the theorem states is just a special case of the inequality above when $k=m$ and x is an empty string.

We will prove by induction.

Base. $k=0$. In this case, fix an arbitrary $x\in\{0,1\}^m$. Then the inequality (38) holds trivially.

Induction. Suppose that the inequality (38) holds for $k-1$ and each string $x\in\{0,1\}^{m-(k-1)}$. We will prove that it also holds for k and an arbitrary string $x\in\{0,1\}^{m-k}$.

Without loss of generality, we assume that the complex number $\alpha_s \geq 0$ for each $s \in \{0,1\}^m$; otherwise, we can absorb its phase into the quantum state. We also introduce a shorthand $|\phi_s\rangle \stackrel{def}{=} |s\rangle (Q_s |0\rangle) |\psi_s\rangle |0\rangle$ to simplify the notation. Then our goal becomes to show

$$\Big\| \Pi_b U \sum_{s \in \{0,1\}^k \circ x} \alpha_s |\phi_s\rangle \Big\|^2 \leq \sum_{s \in \{0,1\}^k \circ x} \alpha_s^2 \big(\| \Pi_b U |\phi_s\rangle \|^2 + k\epsilon \big).$$

We first expand the l.h.s. of the inequality above:

$$\begin{aligned} \Big\| \Pi_b U \sum_{s \in \{0,1\}^k \circ x} \alpha_s |\phi_s\rangle \Big\|^2 &= \Big\| \Pi_b U \sum_{s \in \{0,1\}^{k-1} \circ 0x} \alpha_s |\phi_s\rangle + \Pi_b U \sum_{s \in \{0,1\}^{k-1} \circ 1x} \alpha_s |\phi_s\rangle \Big\|^2 \\ &\leq \Big\| \Pi_b U \sum_{s \in \{0,1\}^{k-1} \circ 0x} \alpha_s |\phi_s\rangle \Big\|^2 + \Big\| \Pi_b U \sum_{s \in \{0,1\}^{k-1} \circ 1x} \alpha_s |\phi_s\rangle \Big\|^2 \quad (39) \\ &\quad + 2 \Big| \sum_{s \in \{0,1\}^{k-1} \circ 0x} \alpha_s \langle \phi_s | \cdot U^\dagger \Pi_b U \cdot \sum_{s \in \{0,1\}^{k-1} \circ 1x} \alpha_s |\phi_s\rangle \Big|. \end{aligned}$$

For convenience, we introduce additional shorthands $\alpha_{0x}, \alpha_{1x}, \alpha_x$ such that

$$\alpha_{0x}^2 \stackrel{def}{=} \sum_{s \in \{0,1\}^{k-1} \circ 0x} \alpha_s^2, \qquad \alpha_{1x}^2 \stackrel{def}{=} \sum_{s \in \{0,1\}^{k-1} \circ 1x} \alpha_s^2. \quad (40)$$

The remainder of the analysis splits into two cases:

Case 1: either $\alpha_{0x} = 0$ or $\alpha_{1x} = 0$. Without loss of generality, we assume $\alpha_{1x} = 0$. This implies $\alpha_s = 0$ for all $s \in \{0,1\}^{k-1} \circ 1x$. Hence, from the inequality (39) we have

$$\begin{aligned} \Big\| \Pi_b U \sum_{s \in \{0,1\}^k \circ x} \alpha_s |\phi_s\rangle \Big\|^2 &\leq \Big\| \Pi_b U \sum_{s \in \{0,1\}^{k-1} \circ 0x} \alpha_s |\phi_s\rangle \Big\|^2 \\ &\leq \sum_{s \in \{0,1\}^{k-1} \circ 0x} \alpha_s^2 \big(\| \Pi_b U |\phi_s\rangle \|^2 + (k-1)\epsilon \big) \qquad \text{(induction hypothesis)} \\ &= \sum_{s \in \{0,1\}^k \circ x} \alpha_s^2 \big(\| \Pi_b U |\phi_s\rangle \|^2 + (k-1)\epsilon \big) \\ &\leq \sum_{s \in \{0,1\}^k \circ x} \alpha_s^2 \big(\| \Pi_b U |\phi_s\rangle \|^2 + k\epsilon \big). \end{aligned}$$

Case 2: both $\alpha_{0x}, \alpha_{1x} > 0$. From the inequality (39) we have

$$\begin{aligned}
\Big\| \Pi_b U \sum_{s\in\{0,1\}^k\circ x} \alpha_s |\phi_s\rangle \Big\|^2 \;\leq\; & \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s^2 \big(\|\Pi_b U |\phi_s\rangle\|^2 + (k-1)\epsilon \big) \qquad \text{(induction hypothesis)} \\
& + \sum_{s\in\{0,1\}^{k-1}\circ 1x} \alpha_s^2 \big(\|\Pi_b U |\phi_s\rangle\|^2 + (k-1)\epsilon \big) \qquad \text{(induction hypothesis)} \\
& + 2\alpha_{0x}\alpha_{1x} \underbrace{\Big| \frac{1}{\alpha_{0x}} \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s \langle\phi_s| \cdot U^\dagger \Pi_b U \cdot \frac{1}{\alpha_{1x}} \sum_{s\in\{0,1\}^{k-1}\circ 1x} \alpha_s |\phi_s\rangle \Big|}_{(*)} \\
\leq\; & \sum_{s\in\{0,1\}^k\circ x} \alpha_s^2 \big(\|\Pi_b U |\phi_s\rangle\|^2 + (k-1)\epsilon \big) + 2\alpha_{0x}\alpha_{1x}\cdot\epsilon \qquad \text{(Claim 30)} \\
\leq\; & \sum_{s\in\{0,1\}^k\circ x} \alpha_s^2 \big(\|\Pi_b U |\phi_s\rangle\|^2 + (k-1)\epsilon \big) + \big(\alpha_{0x}^2 + \alpha_{1x}^2\big)\epsilon \\
=\; & \sum_{s\in\{0,1\}^k\circ x} \alpha_s^2 \big(\|\Pi_b U |\phi_s\rangle\|^2 + k\epsilon \big). \qquad \text{(recall shorthands (40))}
\end{aligned}$$

This completes the proof of the induction step, and hence the theorem. ■

We are left to prove the following claim.

Claim 30 *The absolute value $(*)$ in the proof of Theorem 7 above is less than ϵ.*

PROOF: Inherit all notations introduced within the statement and the proof of Theorem 7. Recall that the shorthand $|\phi_s\rangle \stackrel{def}{=} |s\rangle (Q_s |0\rangle) |\psi_s\rangle |0\rangle$, where the (unitary) quantum circuit $Q_s = \otimes_{i=1}^m Q_{s_i}$ performs on n copies of the quantum register pair (C, R). Then the proof of the claim is just a simple application of the quantum computational ϵ-binding property of the quantum bit commitment scheme (Q_0, Q_1).

In greater detail, note that w.r.t. the unit quantum state vector $1/\alpha_{0x} \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s |\phi_s\rangle$, the $(k+1)$-th quantum register pair (C, R) is in the state $Q_0 |0\rangle$ that is *unentangled* with the rest of the system; similarly, w.r.t. the unit quantum state vector $1/\alpha_{1x} \sum_{s\in\{0,1\}^{k-1}\circ 1x} \alpha_s |\phi_s\rangle$, the $(k+1)$-th quantum register pair (C, R) is in the state $Q_1 |0\rangle$ that is *unentangled* with the rest of the system. Then the absolute value $(*)$ can be bounded by ϵ by applying Lemma 5 straightforwardly; we omit further details here. ■

F A proof of Lemma 27

For convenience, we restate Lemma 27 as below.

Lemma 31 (A restatement of Lemma 27) *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*

$$\Big| \Big\| \sum_{s\in\{0,1\}^m} \alpha_s |\psi_s\rangle \Big\|^2 - \sum_{s\in\{0,1\}^m} \alpha_s^2 \||\psi_s\rangle\|^2 \Big| \leq m^2\epsilon \sum_{s\in\{0,1\}^m} \alpha_s^2. \tag{41}$$

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 $\underline{m-1}$, 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 (41)

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

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. ■