General Properties of Quantum Bit Commitments (Extended Abstract)*

Jun Yan[1]

Jinan University, Guangzhou, China
tjunyan@jnu.edu.cn

Abstract. While unconditionally-secure quantum bit commitment (allowing both quantum computation and communication) is impossible, researchers turn to study the *complexity-based* one, a.k.a. *computational* quantum bit commitment. A computational *canonical* (non-interactive) quantum bit commitment scheme refers to a kind of schemes such that the commitment consists of just a single (quantum) message from the sender to the receiver that later can be opened by *uncomputing* the commit stage. In this work, we study general properties of computational quantum bit commitments through the lens of canonical quantum bit commitments. Among other results, we in particular obtain the following two:

1. Any computational quantum bit commitment scheme can be converted into the canonical (non-interactive) form (with its *sum-binding* property preserved).
2. Two flavors of canonical quantum bit commitments are *equivalent*; that is, canonical computationally-hiding statistically-binding quantum bit commitment exists if and only if the canonical statistically-hiding computationally-binding one exists. Combining this result with the first one, it immediately implies (unconditionally) that computational quantum bit commitment is *symmetric*.

Canonical quantum bit commitments can be based on quantum-secure one-way functions or pseudorandom quantum states. But in our opinion, the formulation of canonical quantum bit commitment is so clean and simple that itself can be viewed as a plausible complexity assumption as well. We propose to explore canonical quantum bit commitment from perspectives of both quantum cryptography and quantum complexity theory in the future.

Keywords: quantum bit commitment · quantum binding · round complexity · parallel composition.

1 Introduction

In the classical world, bit commitment is an important cryptographic primitive. A bit commitment scheme defines a two-stage interactive protocol between

* The full version of this paper is referred to [50].

a sender and a receiver, providing two security guarantees, hiding and binding. Informally, the *hiding* property states that the committed bit is hidden from the receiver during the *commit* stage and afterwards until it is opened, 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, a.k.a. *computational* bit commitment. The one-way function assumption is a basic computational hardness assumption without any mathematical structure; it is the *minimum* assumption in complexity-based cryptography [25]. From a one-way function we can construct two flavors of bit commitments: computationally-hiding (statistically-binding) bit commitment [37] and (statistically-hiding) computationally-binding bit commitment [38,24]. 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 in the commit stage, and which seems inherent [34,23].

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 could be a hybrid of classical and quantum computation and communication. When the construction is purely classical, we often call it "(classical) bit commitment scheme secure against quantum attacks" or "post-quantum bit commitment scheme"[1].

The concept of quantum bit commitment was proposed almost three decades ago, aiming to make use of quantum mechanics to realize bit commitments [6,10]. Unfortunately, unconditionally-secure quantum bit commitment is impossible either [35,33]. Based on complexity assumptions such as quantum-secure one-way permutations or functions, we can also construct two flavors of quantum bit commitments [2,52,17,30,31,14]. An interesting observation about these constructions is that almost all of them (except for the one in [14]) are *non-interactive* (in both the commit and the reveal stages). This is a great advantage over the classical bit commitment. And this motivates us to ask the following question:

> *Is quantum bit commitment inherently non-interactive? Or, can any quantum bit commitment scheme be "compressed" into a non-interactive one that is still useful in applications?*

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.

While the idea of using quantum bit commitments in applications sounds wonderful, unfortunately, it is well-known that the *general* binding property of

[1] 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.

quantum bit commitment, i.e. *sum-binding*, is much weaker than the classical-style binding[2] [17,12,52,44], 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. Thus, it is questionable *a priori* whether quantum bit commitments could be useful in cryptographic applications, let alone the notorious difficulty (or general impossibility) of quantum rewinding [21] in security analysis.

Canonical quantum bit commitment. Motivated by the study of complete problems for quantum zero-knowledge [45,28,49] and more general quantum interactive proofs [41,11], the so-called *canonical* (non-interactive) quantum bit commitment[3] was proposed [52,18].

Roughly speaking, by a canonical quantum bit commitment scheme, the commitment consists of just a single (quantum) message from the sender to the receiver, which can be opened later by *uncompute* the commit stage. Its definition is sketched at the beginning of "Our contributions" shortly and given in Definition 2 formally. A canonical quantum bit commitment scheme satisfies the so-called *honest-binding* property, which guarantees that any cheating sender in the *reveal* stage cannot open an *honest* commitment to the bit 0 as 1, and vice versa. This honest-binding property appears even weaker than sum-binding. Both flavors of canonical quantum bit commitments can be constructed from quantum-secure one-way functions [52,30,31], or pseudorandom quantum states by a more recent result [36] and this work.

Though its binding property appears extremely weak, interestingly, it turns out that canonical quantum bit commitment is sufficient to construct quantum zero-knowledge [52,18,51] and quantum oblivious transfer[4] [18]. However, the corresponding security (that will be based on quantum bit honest-binding) there are more tricky to establish than the corresponding security based on unique-binding.

Other quantum commitments and binding properties. There are also other (classical or quantum) constructions of commitments that satisfy some stronger binding properties (but which may not hold for *general* quantum bit commitments) than sum-binding, including *collapse-binding* commitments [44,43], and *extractable* commitments [22,5]; they are likely to be more versatile than general quantum bit commitments in applications. However, both of them need interactions in the standard model, losing the possible advantage of the non-interactivity of quantum bit commitments.

[2] That is, any quantum cheating sender cannot generate a commitment that can be opened as both 0 and 1 successfully with non-negligible probability.

[3] In the prior work (e.g. [52,18,51]) 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 [4], who also suggest the current name "canonical" to us. And we accept.

[4] In [18], a quantum oblivious transfer with a security that is weaker than the full simulation-security [22,5] but still very useful in many scenarios was achieved.

Restricting to quantum *statistically-binding* commitments, statistical *unique-binding* can be achieved based on quantum one-way permutations [2], or even functions by a recent result [7]. More recently, Ananth, Qian and Yuen [3] also propose an *extractor-based* quantum statistical-binding property, hereafter *AQY-binding*, and show that it can be satisfied by a construction of quantum bit commitment based on pseudorandom quantum states. Though these binding properties seem much stronger than the honest-binding property guaranteed by canonical statistically-binding quantum bit commitment (whose instantiations can be found either in [52], [50, Appendix D], or [36]), commitments satisfying these binding properties turn out to be *no more useful* (at least in theory, as far as we can tell) than canonical statistically-binding quantum bit commitments in applications [18]. More discussion on this point is referred to Subsection 1.2 (where we will discuss the extractor-based AQY-binding property in greater detail.)

Yet in some other work certain strong quantum binding properties are proposed for applications [16,12], but no instantiations of the corresponding commitments based on well-founded complexity assumptions are known even today.

This work. In this work, we show that the canonical quantum bit commitment *captures* the computational hardness underlying general computational quantum bit commitments, by providing a *compiler* that can transform any computational quantum bit commitment scheme into the canonical (non-interactive) form. This not only answer the motivating question aforementioned affirmatively, but also allows us to study general properties of quantum bit commitments through the lens of canonical quantum bit commitments.

We further propose to study canonical quantum bit commitment in the future not only as a cryptographic primitive in the MiniQCrypt world (named after [22]), but also as a basic (quantum) complexity-theoretic object whose existence is an interesting open problem in its own right. Our proposal is based on our current knowledge about canonical quantum bit commitment summarized as follows: (Refer to Subsection 1.3 for more detail.)

1. Its formulation is clean and simple (Definition 2), inducing two basic quantum complexity-theoretic open questions: one is on the existence of quantum state ensembles that are computationally indistinguishable but far apart in the trace distance, while the other on the existence of unitaries that cannot be efficiently realized.
2. It is robust (Theorem 6), implying that the two basic open questions mentioned in the 1st item above are essentially the same question.
3. It captures the computational hardness underlying general computational quantum bit commitments (Theorem 4).
4. It is useful in quantum cryptography [52,18,51,3,5].
5. Conversely, it is also implied by some basic quantum cryptographic primitives such as quantum zero-knowledge [52] and quantum oblivious transfer [14].

6. It is implied by quantum complexity assumptions such as quantum-secure one-way functions and pseudorandom quantum states in the MiniQCrypt world [52,30,31,14,36]. But the converse is unknown.

Before introducing our contribution of this work in greater detail, we stress that in this paper when we talk about statistical or computational binding without explicitly mentioning other properties of binding, we mean the most general *sum-binding* property (or equivalently, honest-binding w.r.t. canonical quantum bit commitments, as will become clear shortly). In spite of this, we have already known that canonical quantum bit commitments can satisfy some stronger binding properties than sum-binding that are interesting and useful in applications [18,50,51]. We expect further exploration on the binding properties of canonical quantum bit commitments in the future.

1.1 Our contribution

We first sketch what a *canonical* quantum bit commitment scheme looks like; its formal definition is given in Definition 2. 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 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 say that the scheme (Q_0, Q_1) is hiding if the reduced quantum state of $Q_0 |0\rangle$ in the register C and that of $Q_1 |0\rangle$ are indistinguishable, and that the scheme is binding if there does not exist a unitary performing on the register R that transforms the quantum state $Q_0 |0\rangle$ into $Q_1 |0\rangle$.

We obtain *four* main results on properties of canonical and more 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 [2,17,12,16,44,52,51], *honest-binding* [52] 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 given in Definition 2. A priori, honest-binding seems to be too weak to be useful: anyway, it is unrealistic to restrict a cheating sender's behavior to be honest in the commit stage!

Sum-binding is a general binding property of quantum bit commitment [17]. Roughly, let p_0 and p_1 denote the probability that a cheating sender (in the reveal stage) can open the commitment (generated in the commit stage in which the sender is also cheating) as 0 and 1, respectively. 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 given in Definition 3.

While it is trivial that sum-binding implies honest-binding, in this work we show that the converse is also true w.r.t. canonical quantum bit commitments[5] (Theorem 2). 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 2) and the full security (against an arbitrary attacker) (Theorem 3). This equivalence not only explains at a high level why previous applications of canonical quantum bit commitments only make use of its honest-binding property [52,18,51], but also enables us to simplify the security analysis of canonical quantum bit commitments schemes[6]. As an application, we can significantly simplify the DMS construction [17] of computationally-binding quantum bit commitment based on quantum-secure one-way permutations[7]. (The detail is referred to [50, Section 5]).

2. Quantum bit commitment is inherently non-interactive

We answer the motivating question raised before affirmatively, i.e. quantum bit commitment is inherently non-interacitve, by proving a *round-collapse* theorem (Theorem 4). This theorem can also be viewed as an extension of converting an arbitrary non-interactive quantum bit commitment scheme into the canonical form [52,18]. 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 priori, 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 un-

[5] We do not claim that this holds for a *general* quantum bit commitment; the two simple schemes presented in [50, Appendix C] also serve as two counterexamples in this regard.

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

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

likely [34,23]. 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 5).

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. (The detail is referred to [50, 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. (The detail is referred to [50, Appendix C]). 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 [50, Proposition 15]. 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" for a discussion) are of independent interest.

As an interesting application, we apply the round-collapse theorem to compress the classical NOVY scheme [38], obtaining yet another construction (besides ones given in [17,30,31]) of non-interactive computationally-binding quantum bit commitment based on quantum-secure one-way permutations [50, Section 9]. 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 [38]. 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, or two flavors of quantum bit commitments are equivalent

Almost two decades ago, Crépeau, Légaré and Salvail [14] gave a way that virtually can transform any quantum bit commitment scheme that is computationally hiding and statistically unique-binding into another one of the opposite flavor, i.e. computationally binding and statistically hiding. In this work, we generalize this result significantly by proving a *symmetry*[8] in the sense as stated in the following (unconditional) theorem:

Theorem 1. *Computationally-hiding statistically-binding quantum bit commitments exist if and only if statistically-hiding computationally-binding quantum bit commitments exist.*

[8] This symmetry is in the same sense as that of oblivious transfer [48].

The *high-level idea* of proving the theorem above is as follows. By the virtue of the round-collapse theorem, it suffices to prove that the theorem holds w.r.t. canonical quantum bit commitments (Theorem 6). In greater detail, given a canonical quantum bit commitment scheme, we first feed it to a *somewhat simplified* CLS construction [14] 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 will be in the canonical form automatically).

Our security analysis are significantly simpler than the related ones given in [14,12]. Basically, the simplification comes from two aspects:

1. By the virtue of our round-collapse theorem (Theorem 4), the original CLS scheme (with a canonical quantum bit commitment scheme plugged in) can be simplified in the first place 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 Theorem 6, we develop several techniques to establish the security against the purification attack. Most of these techniques are adapted from those used in [18,51]. Among others, we in particular show a *computational collapse* caused by canonical quantum computationally-binding commitments [50, Appendix F], which might be of independent interest. More discussion on our techniques is referred to "Technical overview".

We finally remark that as a by-product of the symmetry, we automatically obtain a construction of canonical statistically-hiding computationally-binding quantum bit commitment based on quantum-secure one-way functions or pseudorandom quantum states. This is achieved by first plugging in the somewhat simplified CLS construction a canonical computationally-hiding statistically-binding quantum bit commitment scheme that is either based on quantum-secure one-way functions or pseudorandom quantum states, and then compressing the resulting scheme. We remark that the construction of statistically-hiding computationally-binding quantum bit commitment based on pseudorandom quantum states is previously unknown.

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 [12]. Then bounding the error induced by such a superposition by a negligible quantity becomes technically hard or even impossible[9].

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 7). 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 Related (more recent) work

More recently[10], Bitansky and Brakerski [7] construct a non-interactive statistically-binding quantum bit commitment scheme based on quantum-secure one-way functions. Their scheme deviates from the canonical one given in [52], managing to achieve *unique-binding* and the *classical* reveal stage, but at the cost of more complex construction and analysis.

Morimae and Yamakawa [36] construct a statistically-binding quantum bit commitment scheme based on pseudorandom quantum states [26], a quantum complexity assumption arguably weaker than quantum-secure one-way functions [32]. 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 the quantum statistical honest-binding (rather than sum-binding) property. Moreover, combining results in this work (Theorem 6), it follows that both flavors of canonical quantum bit commitments can be constructed based on pseudorandom quantum states.

Ananth, Qian and Yuen [3] also construct a statistically-binding quantum bit commitment scheme based on pseudorandom quantum states, which has *two* messages in the commit stage and a single *classical* message in the reveal stage. Clearly, this scheme is not in the canonical form. But they show that it satisfies a strong (statistical) binding property such that an (inefficient) extractor is associated with scheme, which can be used to extract (and thus collapse) the committed value from the commitment at the end of the commit stage. We find[11] that this idea of introducing an extractor to quantum statistically-binding commitments is very similar in spirit to the analysis framework introduced in [18] but only for canonical perfectly/statistically-binding quantum bit commitments. More discussion on the comparison between them is referred to [50, Appendix B], where by tweaking techniques used in [18], we in particular prove that canonical statistically-binding quantum bit commitments automatically satisfy the AQY-binding property.

[9] To the best of our knowledge, however, no impossibility result is known yet. In [12], authors only vaguely argue that this seems impossible for quantum computationally-binding commitments.

[10] After the upload of the first preprint of this work to Cryptology ePrint Archive [50] in 2020.

[11] This is also observed in [36, Appendix B].

While the extractor-based AQY-binding definition is more readily usable by cryptographers, there seems no obvious way to extend it to the case of quantum computational binding (when the commitment is statistically hiding). This is because then the quantum commitments to different values are negligibly close (in the trace distance); we cannot hope that a similar extractor exists. In contrast, the formalization of canonical quantum bit commitment schemes provide a *uniform* way to capture both flavors of quantum bit commitments.

Moreover, Ananth, Qian and Yuen [3] 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 the next subsection.

1.3 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 [2,52,17,30,31,14,7], or pseudorandom quantum states [26,36,3]. It is interesting to explore whether quantum bit commitments imply pseudorandom quantum states (of any sort) conversely[12]. On the other hand, quantum bit commitments are useful, and may help reduce the round complexity of cryptographic constructions [52,18,51]. In particular, there exists a certain *equivalence* between quantum bit commitment and quantum zero-knowledge [52], and an equivalence between quantum bit commitment and quantum oblivious transfer [54,14,18,5,3]. Thus, quantum bit commitment is likely to be an important primitive in the MiniQCrypt world [22]. It is interesting to explore more cryptographic applications of quantum bit commitments in the future.

Seeing from the *quantum complexity perspective*, whether computational quantum bit commitments exist is an interesting open problem. As mentioned, canonical quantum bit commitment are motivated by the study of complete problems for quantum zero-knowledge [45,49] and more general quantum interactive proofs [41,11]. The existence of canonical statistically-hiding computationally-binding quantum bit commitment schemes is closely related to the *quantum complexity of unitaries* [1]. 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

[12] 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 sort of functions.

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 the trace distance. However, the computational binding property implies that this unitary U is *not* efficiently realizable!

We can motivate the study of canonical computationally-hiding statistically-binding quantum bit commitment 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 quite 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 [20, an exercise in Chapter 3] and pseudorandom generators [19]. In a try to translate this result to the quantum setting, it brings us back to the open question of whether quantum bit commitments imply pseudorandom quantum states (which are the quantum analog of pseudorandom generators) [26,36,3].

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 question regarding the existence of computational 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 looks very similar to the amplification of the hardness of inverting an arbitrary one-way function in classical cryptography [53]. More interestingly, if the answer to this question is indeed "yes", then combining it with results in [45,52,18,51] will complete a proof for an equivalence between quantum bit commitment and quantum zero-knowledge like in the classical setting [40].

1.4 Technical overview

Honest-binding implies sum-binding. The proof is just a simple application of the quantum rewinding lemma (Lemma 1) once used in [52,18,51], which in a nutshell is another variant (other than the one used in [42] that is designed specific for sigma protocols) of the gentle measurement lemma [47].

Round compression. Our compiler for the round compression is inspired by the equivalence between the semi-honest security and the full security w.r.t. canonical quantum bit commitments (Theorem 3).

Informally speaking, 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. For this construction to be legal, possible *irreversible* computation of both parties in the commit stage prescribed by the

original scheme should be simulated by corresponding 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, the new sender may deviate arbitrarily, and there seems no way of restricting 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.

The reason why our compiler works is by the virtue of Theorem 3: 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 4), it requires that the *(*purification) of the original scheme (rather than the original scheme itself), 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 roughly argued in the below.

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 into 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 [50, Section 6], as well as their semi-honest security [50, 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 [27] or a zero-knowledge proof [29]. 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 necessary; this is because (as typical in cryptography) both the honest sender and the honest receiver of bit commitment are polynomial-time bounded.

Proving an equivalence between two flavors of canonical quantum bit commitments. The basic idea to *convert* the flavor of a canonical quantum bit commitment scheme is to use the CLS construction [14]. In a nutshell, the

original CLS scheme in [14] uses *classical* statistically unique-binding bit commitments (e.g. Naor's scheme [37]) to realize a 1-out-of-2 *quantum oblivious transfer* (QOT) [13], which in turn can be used to construct a computationally-binding quantum bit commitment scheme. In [18], it is shown that commitments used in the CLS scheme, or QOT subprotocol more precisely, can be replaced with canonical statistically/perfectly-binding quantum bit commitments. Then combined with the round-collapse theorem (Theorem 4), this already proves one direction of the equivalence.

For the other direction of the equivalence, however, it is still open whether one can use computationally-binding quantum bit commitments in the CLS scheme to obtain a statistically-binding quantum bit commitment scheme. Technically, this is because we do not know whether using computationally-binding quantum bit commitments can force the receiver of BB84 qubits in the QOT subprotocol to measure these qubits upon receiving them. (We note that this is not a big problem when statistically-binding quantum bit commitments are used [14,18].) To overcome this difficulty, in [12] a tailored quantum string binding property is proposed, by which they show that quantum commitments satisfying such binding property are sufficient to show the security of the QOT protocol. Unfortunately, we do not know whether quantum commitments satisfying such binding property are instantiatable even today. In this work, we overcome this technical difficulty by proving a *computational collapse theorem* [50, Appendix F], as will be discussed shortly.

Actually, for our purpose of converting the flavor of canonical quantum bit commitments, it suffices for us to use a *somewhat simplified CLS construction*: all *intermediate verifications of quantum commitments* within the original CLS scheme can be removed. We can do this is by the virtue of the round-collapse theorem, namely, we only need a scheme whose purification is semi-honest secure for the purpose of the round compression. In particular, we only need such a QOT that satisfies 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 is already much *weaker* than the security against an arbitrary quantum attack considered in [54,14,18], let alone the recently achieved simulation security [15,22,5]. Hence, one can imagine that it is much easier to establish.

For the formal security analysis, we will first prove the semi-honest security of this somewhat simplified CLS scheme, and then manage to 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 QOT subprotocol were really performed. To this end, we will use techniques introduced in the below.

Arguing the security against the purification attack. Seeing from the statement of our round-collapse theorem, to apply it, one needs first to show that the purification of the original (interactive) quantum bit commitment scheme is semi-honest secure, or equivalently, the original scheme is secure against the

purification attack. 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 to do this, 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 case in which collapses are enforced is by *quantum commitments*, as argued in [18] and within the proof of Theorem 6 in this paper. That is, committing to a *superposition* using canonical statistically- or computationally-binding quantum bit commitments (in a bitwise fashing) can be viewed as an *implicit* way of measuring it (but without leaking its value)! In greater detail, when canonical statistically-binding quantum bit commitments are used, collapses can be shown using techniques (i.e. *perturbation* and *commitment measurement*) developed in [18]. When canonical computationally-binding quantum bit commitments are used, we will show a "computational collapse" (named after [12]) by proving a *computational collapse theorem* [50, Appendix F] in this work. The technique used towards proving this theorem is inspired by the proof of the quantum computational string predicate-binding property in [51], which basically is a way of bounding exponentially many negligible errors in an arbitrary superposition by a negligible quantity. We remark that currently, this computational collapse theorem is only known to be suitable to apply when the security against the purification attack is considered; whether it can be extended to be suitable for the security analysis against an arbitrary quantum attack (like in [12]) is left as an interesting open problem.

Last, we stress that the semi-honest security of an arbitrary (interactive) quantum bit commitment scheme does *not* extend to its purification *generally*; two counterexamples are presented in [50, Appedix C].

1.5 Follow-up work

In preparing the camera-ready version of this extended abstract, we notice that there is a follow-up work [9].

After reading an earlier draft of the full version of this extended abstract [50] (the version uploaded to Cryptology ePrint Archive this February, 2022), authors of [9] call the two ensembles of efficiently-generated quantum state that are far in the trace distance but quantum computationally indistinguishable the "EFI pair". (As we have argued in this extended abstract, EFI pair and canonical statistically-binding quantum bit commitment are actually the same object seen from different perspectives.) They further explore the connections between EFI pairs and some other cryptographic applications that are not discussed in this extended abstract, in particular multiparty secure computations for classical functionalities and quantum zero-knowledge proofs for languages *beyond* **NP**. (Note that within **NP**, an equivalence between (instance-dependent) canonical

statistically-binding quantum bit commitments (hence EFI pairs) and quantum zero-knowledge proofs has already been established in [52] back in 2015.)

Organization. The remainder of this paper is organized as follows. 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 show that w.r.t. canonical quantum bit commitment, its honest-binding property is equivalent to the sum-binding property. This equivalence will be used to prove the round-collapse theorem in Section 5. As an application of the round-collapse theorem, in Section 6 we prove an equivalence between two flavors of quantum bit commitments. In Section 7, a very strong quantum string sum-binding property of the parallel composition of canonical statistically-binding quantum bit commitments is established. We conclude with Section 8, where several open problems are also raised.

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}, $|\psi\rangle^{\mathsf{A}}$ 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 [46]. 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 [39]. 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 classical bit,*

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

for sufficiently large n.

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

A quantum rewinding lemma

Lemma 1 (A quantum rewinding [18]). *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*

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

3 Canonical (non-interactive) quantum bit commitment

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

Definition 2. *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)[13] 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.*

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

– *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:

– *(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*[14].
– *ϵ-(honest-)**binding**. First prepare the quantum register pair (C, R) in the state $Q_0 |0\rangle$*[15]*. 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 in [50, Section 7].

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

[15] 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.

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 [52], 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.
4. In [52,18], 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 4).
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 [26].

4 Honest-binding is equivalent to sum-binding

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

Definition 3 (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 2), 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 3 to be 1, then we end up with 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 2. *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 3), 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 1) 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

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

An intuitive interpretation of this inequality is that the success probability of first opening the bit commitment as 0 and then as 1 is at least some non-negligible quantity.

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 $(\mathsf{R}', \mathsf{Z}')$.
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 its outcome being 1, the reduced state of the register Z' will help the sender S^* 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.

To show that S^* breaks the honest-binding property of the scheme (Q_0, Q_1), it suffices to prove a lower bound of the probability of both the following two events happening simultaneously: (1) the measurement outcome in the step 2 being 1; and (2) the cheating sender S^* succeeds. (Note that S^* may also cheat successfully while the measurement outcome of the step 2 is 0; but its probability can be ignored for a lower bound of S^*'s success probability.) This probability is given by the expression

$$\left\| (U_1^\dagger)^{RZ'} \left(Q_1 |0\rangle \langle 0| Q_1^\dagger\right)^{CR} U_1^{RZ'} \cdot (U_0^\dagger)^{RZ'} \left(Q_0 |0\rangle \langle 0| Q_0^\dagger\right)^{C'R'} U_0^{R'Z'} \left((Q_0 |0\rangle)^{CR} |\psi\rangle^{C'R'Z'} \right) \right\|^2 .$$

A key observation is that conditioned on the measurement outcome in the step 2 being 1, both the quantum register pair (C, R) and $(\mathsf{C}', \mathsf{R}')$ will be in the state $Q_0 |0\rangle$ at the end of the step 2. Thus, from then on, switching to perform unitaries U_0, U_1 on registers $(\mathsf{R}', \mathsf{Z}')$ (as opposed to $(\mathsf{R}, \mathsf{Z}')$) and opening the commitment in the register C' will result in the same success probability. That is, the expression above is equal to

$$\left\| (U_1^\dagger)^{R'Z'} \left(Q_1 |0\rangle \langle 0| Q_1^\dagger\right)^{C'R'} U_1^{R'Z'} (U_0^\dagger)^{R'Z'} \cdot \left(Q_0 |0\rangle \langle 0| Q_0^\dagger\right)^{C'R'} U_0^{R'Z'} \left((Q_0 |0\rangle)^{CR} |\psi\rangle^{C'R'Z'} \right) \right\|^2 .$$

Since now the quantum registers (C, R) are untouched, this expression will simplify to

$$\left\| (U_1^\dagger)^{R'Z'} \left(Q_1 |0\rangle \langle 0| Q_1^\dagger\right)^{C'R'} U_1^{R'Z'} (U_0^\dagger)^{R'Z'} \cdot \left(Q_0 |0\rangle \langle 0| Q_0^\dagger\right)^{C'R'} U_0^{R'Z'} |\psi\rangle^{C'R'Z'} \right\|^2 .$$

But this final expression can be lowerbounded by applying the inequality (5), if we identify registers $(\mathsf{C}, \mathsf{R}, \mathsf{Z})$ in the l.h.s. of the inequality (5) with registers $(\mathsf{C}', \mathsf{R}', \mathsf{Z}')$ here, respectively. This will yield a lower bound $1/4p^2$, which is non-negligible.

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 2 with Theorem 2, we have the following theorem as an immediate corollary.

Theorem 3. *A canonical quantum bit commitment scheme (Q_0, Q_1) (of either flavor) is secure if and only if it is semi-honest secure.*

5 A round-collapse theorem

In this section, we will prove a round-collapse theorem (Theorem 4), which can be viewed as an extension of converting an arbitrary *non-interactive* quantum bit commitment scheme into the canonical form [52,18]. To understand the statement and the proof of this theorem, in the first place we should have given a formal treatment of a general quantum two-party interactive protocols, their purifications, as well as their semi-honest and related security. However, we cannot do this in this extended abstract due to the limited space. Now let us informally introduce these notions, while moving their formal treatments to [50, Section 6, 7].

Roughly, a *general quantum two-party interactive protocols* allows both classical and quantum computation and communication. We can assume without loss of generality that quantum computation is limited to measurements in the computational basis, as well as quantum operations realized by polynomial-size quantum circuits composed of unitary quantum gates. A *purification* of an interactive protocol refers to the protocol obtained by simulating all classical computation and communication, as well as quantum measurements of the original protocol, by unitary quantum operations in a standard way. The *purification attack* against one party of the protocol refers to the attack by *purifying* all this party's operations.

Restricting to quantum bit commitment schemes, for our purpose we will define their *semi-honest security* as that both the semi-honest sender and receiver will *follow* the protocol in the commit stage; but in the reveal stage later, the semi-honest sender may *deviate* the protocol. Correspondingly, the *purification attack against the receiver* refers to the attack by purifying all the honest receiver's operations in the commit stage. And the *purification attack against the sender* refers to the attack by purifying all the honest sender's operations in the commit stage; but the attack in the reveal stage could be arbitrary.

Theorem 4 (Round-collapse). *If a quantum bit commitment scheme is secure against the purification attack (or equivalently, its purification is semi-honest secure), then it can be compressed into a scheme of the canonical form (Definition 2) 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.*

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.

Due to the space limitation, the proof of the round-collapse theorem can be found in [50].

As a simple application of the round-collapse theorem, we can compress Naor's bit commitment scheme [37] to get a non-interactive one [50, Appendix D]. 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 [52]). Two non-trivial applications are referred to the subsequent section and [50, Section 9], respectively.

Since the purification attack is just a special kind of attack among all possible attacks, the following theorem is an immediate corollary of Theorem 4.

Theorem 5. *Any secure (against an arbitrary quantum attack) interactive quantum bit commitment scheme, in particular post-quantum secure (classical) bit commitment scheme, can be compressed into a non-interactive one of the canonical form (Definition 2) 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. [2,44,43,22,5,7]) than sum-binding. But if we feed it into our compiler for the round-compression, these stronger binding properties may be lost; the resulting/compressed scheme is only guaranteed sum-binding (or equivalently honest-binding, since it is of the canonical form).

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

In this section, we show that quantum bit commitment is *symmetric*, or two flavors of quantum bit commitments are *equivalent* (Theorem 1). This is an immediate corollary of the following theorem combined with the round-collapse theorem (Theorem 4).

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

Towards establishing the equivalence above, our basic idea is first using a construction that is a simplification of the CLS scheme [14] 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 4).

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 Fig. 1, which we denote by QBC(n), with the security parameter n (which we often drop to simplify the notation). Let QBC$(n)^{\otimes n}$ denote the *parallel* composition of n copies of the scheme QBC(n). This construction is almost the CLS scheme given in [14], 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 *CLS scheme* in this paper. Intuitively, these intermediate verifications can be removed because by the virtue of the round-collapse theorem (Theorem 4), 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 QBC$(n)^{\otimes n}$ is secure against the purification attack, or the purified CLS scheme is both honest-hiding and honest-binding. This simplification of the construction will induce a significant simplification of the analysis of the original CLS scheme [14], which is for the full security and quite technically involved.

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 $d_c = a_c$.

Fig. 1. The atomic scheme QBC, which composed in parallel gives a scheme that is a somewhat simplification of the original CLS scheme

Due to the space limitation, the proof of Theorem 6 is referred to [50, Section 10].

7 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. *computationally-binding* quantum bit commitment [12].

In this section, we will study the parallel composition of a canonical *statistically-binding* quantum bit commitment scheme, establishing a very strong quantum string binding property. We also show that this binding property implies the CDMS-binding property of quantum string commitment (referred to [50, Section 11]), which is useful in quantum cryptography [12]. However, we do not expect the same binding property extends to canonical *computationally-binding* quantum bit commitment schemes.

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

Definition 4 (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*

$$\sum_{s\in\{0,1\}^m} p_s < 1 + negl(n). \tag{6}$$

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 [12]. Roughly speaking, the main difficulty comes from that there are *exponentially* many strings (2^m, exactly) in $\{0,1\}^m$, but we still hope to bound the sum of exponentially many advantages by a negligible quantity.

In spite of the difficulty mentioned above, we can prove the following parallel composition theorem w.r.t. a canonical statistically-binding quantum bit commitment scheme.

Theorem 7 (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

$$\sum_{s\in\{0,1\}^m} p_s \leq 1 + O(m^2\epsilon). \tag{7}$$

The proof of the theorem above will be information-theoretic, thus does not extend to the computational setting. Due to the space limitation, its proof is referred to [50, Section 11].

8 Conclusion and open problems

In this work, we study general properties of complexity-based/computational quantum bit commitments. Specifically, we show that any quantum bit commitment scheme can be compressed into the canonical form (Theorem 4), which is non-interactive and whose semi-honest security implies the full security (Theorem 3). This yields several applications [50, Appendix D and Section 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 a very strong quantum statistical string sum-binding property by composing a canonical statistically-binding quantum bit commitment scheme in parallel (Theorem 7).

We propose to study quantum bit commitments in the 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. Can canonical quantum bit commitments satisfy any stronger binding properties than sum-binding that are interesting? The answer to this question is "yes" ([18,51] and [50, Appendix B]). We expect further exploration towards this open question in the future.
2. 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 6). 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* [22,5] that is preferable in cryptography. Recall that we prove a computational collapse theorem ([50, Appendix F]) 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 [12]) with a canonical computationally-binding quantum bit commitment scheme plugged in [13]? Possibly combine it with the quantum sampling technique devised in [8]? 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 [14] and here for the purpose of converting the flavor of quantum bit commitment.

3. In this work, we show that the NOVY bit commitment scheme can be compressed into the canonical form and shown secure against quantum attacks [50, Section 9]. A natural and interesting extension of this result would be compressing the construction of statistically-hiding computationally-binding (classical) bit commitment scheme based on one-way functions [24] into the canonical form and showing its quantum security (when the underlying one-way function used is quantum secure).
4. As mentioned in Section 1.3, it is interesting to explore whether quantum bit commitments conversely imply pseudorandom quantum states (of any sort).
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* [52]. 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 [53]. If the answer to this question is "yes", then combining it with results in [45,52,18,51] will complete the proof for an equivalence between quantum bit commitment and quantum zero-knowledge like in the classical setting [40].
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 computational quantum bit commitments really exist?

Acknowledgements. We thank Dominique Unruh and Takeshi Koshiba for bringing the reference [48] 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, Crypto 2022 and Asiacrypt 2022 for their useful suggestions and valuable comments on earlier drafts of this paper.

This work was supported by National Natural Science Foundation of China (Grant No. 61602208), by PhD Start-up Fund of Natural Science Foundation of Guangdong Province, China (Grant No. 2014A030310333), by Major Program of Guangdong Basic and Applied Research Project (Grant No. 2019B030302008), by National Joint Engineering Research Center of Network Security Detection and Protection Technology, and by Guangdong Key Laboratory of Data Security and Privacy Preserving. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of funding agencies.

References

1. Aaronson, S.: The complexity of quantum states and transformations: From quantum money to black holes. arXiv:1607.05256 (2016)
2. Adcock, M., Cleve, R.: A quantum Goldreich-Levin theorem with cryptographic applications. In: STACS, pp. 323–334. Springer (2002)
3. Ananth, P., Qian, L., Yuen, H.: Cryptography from pseudorandom quantum states. Cryptology ePrint Archive, Report 2021/1663 (2021), https://ia.cr/2021/1663
4. Ananth, P., Qian, L., Yuen, H.: (2022), private communication
5. Bartusek, J., Coladangelo, A., Khurana, D., Ma, F.: One-way functions imply secure computation in a quantum world. In: Malkin, T., Peikert, C. (eds.) CRYPTO. Lecture Notes in Computer Science, vol. 12825, pp. 467–496. Springer (2021)
6. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. vol. 175 (1984)
7. Bitansky, N., Brakerski, Z.: Classical binding for quantum commitments. In: Nissim, K., Waters, B. (eds.) TCC. Lecture Notes in Computer Science, vol. 13042, pp. 273–298. Springer (2021)
8. Bouman, N.J., Fehr, S.: Sampling in a quantum population, and applications. In: CRYPTO. pp. 724–741 (2010)
9. Brakerski, Z., Canetti, R., Qian, L.: On the computational hardness needed for quantum cryptography. Cryptology ePrint Archive, Paper 2022/1181 (2022), https://eprint.iacr.org/2022/1181, https://eprint.iacr.org/2022/1181
10. Brassard, G., Crépeau, C.: Quantum bit commitment and coin tossing protocols. In: CRYPTO. pp. 49–61 (1990)
11. Chailloux, A., Kerenidis, I., Rosgen, B.: Quantum commitments from complexity assumptions. In: ICALP (1). pp. 73–85 (2011)
12. Crépeau, C., Dumais, P., Mayers, D., Salvail, L.: Computational collapse of quantum state with application to oblivious transfer. In: TCC. pp. 374–393 (2004)
13. Crépeau, C., Kilian, J.: Achieving oblivious transfer using weakened security assumptions (extended abstract). In: FOCS. pp. 42–52 (1988)
14. Crépeau, C., Légaré, F., Salvail, L.: How to convert the flavor of a quantum bit commitment. In: EUROCRYPT. pp. 60–77 (2001)
15. Damgård, I., Fehr, S., Lunemann, C., Salvail, L., Schaffner, C.: Improving the security of quantum protocols via commit-and-open. In: CRYPTO. pp. 408–427 (2009)

16. Damgård, I., Fehr, S., Salvail, L.: Zero-knowledge proofs and string commitments withstanding quantum attacks. In: CRYPTO. pp. 254–272 (2004)
17. Dumais, P., Mayers, D., Salvail, L.: Perfectly concealing quantum bit commitment from any quantum one-way permutation. In: EUROCRYPT. pp. 300–315 (2000)
18. Fang, J., Unruh, D., Yan, J., Zhou, D.: 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
19. Goldreich, O.: A note on computational indistinguishability. Inf. Process. Lett. **34**(6), 277–281 (1990)
20. Goldreich, O.: Foundations of Cryptography, Basic Tools, vol. I. Cambridge University Press (2001)
21. van de Graaf, J.: Towards a formal definition of security for quantum protocols. PhD thesis, Université de Montréal (1997)
22. Grilo, A.B., Lin, H., Song, F., Vaikuntanathan, V.: Oblivious transfer is in miniqcrypt. In: Canteaut, A., Standaert, F. (eds.) EUROCRYPT. Lecture Notes in Computer Science, vol. 12697, pp. 531–561. Springer (2021)
23. Haitner, I., Hoch, J.J., Reingold, O., Segev, G.: Finding collisions in interactive protocols - a tight lower bound on the round complexity of statistically-hiding commitments. In: FOCS. pp. 669–679 (2007)
24. Haitner, I., Nguyen, M.H., Ong, S.J., Reingold, O., Vadhan, S.P.: Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. SIAM J. Comput. **39**(3), 1153–1218 (2009)
25. Impagliazzo, R., Luby, M.: One-way functions are essential for complexity based cryptography (extended abstract). In: FOCS. pp. 230–235 (1989)
26. Ji, Z., Liu, Y., Song, F.: Pseudorandom quantum states. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO. Lecture Notes in Computer Science, vol. 10993, pp. 126–152. Springer (2018)
27. Kitaev, A., Watrous, J.: Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In: STOC. pp. 608–617 (2000)
28. Kobayashi, H.: Non-interactive quantum perfect and statistical zero-knowledge. In: ISAAC. pp. 178–188 (2003)
29. Kobayashi, H.: General properties of quantum zero-knowledge proofs. In: TCC. pp. 107–124 (2008), arXiv.org:0705.1129
30. Koshiba, T., Odaira, T.: Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. In: TQC. pp. 33–46 (2009)
31. Koshiba, T., Odaira, T.: Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function. arXiv:1102.3441 (2011)
32. Kretschmer, W.: Quantum pseudorandomness and classical complexity. In: Hsieh, M. (ed.) TQC. LIPIcs, vol. 197, pp. 2:1–2:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2021)
33. Lo, H.K., Chau, H.F.: Why quantum bit commitment and ideal quantum coin tossing are impossible. Physica D: Nonlinear Phenomena **120**(1), 177–187 (1998)
34. Mahmoody, M., Pass, R.: The curious case of non-interactive commitments - on the power of black-box vs. non-black-box use of primitives. In: CRYPTO 2012. pp. 701–718 (2012)
35. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Physical Review Letters **78**(17), 3414–3417 (1997)
36. Morimae, T., Yamakawa, T.: Quantum commitments and signatures without one-way functions (2021), https://ia.cr/2021/1691
37. Naor, M.: Bit commitment using pseudorandomness. J. Cryptology **4**(2), 151–158 (1991)

38. Naor, M., Ostrovsky, R., Venkatesan, R., Yung, M.: Perfect zero-knowledge arguments for NP using any one-way permutation. J. Cryptology **11**(2), 87–108 (1998)
39. Nielsen, M.A., Chuang, I.L.: Quantum computation and Quantum Informatioin. Cambridge University Press (2000)
40. Ong, S.J., Vadhan, S.P.: An equivalence between zero knowledge and commitments. In: TCC. pp. 482–500 (2008)
41. Rosgen, B., Watrous, J.: On the hardness of distinguishing mixed-state quantum computations. In: CCC. pp. 344–354. IEEE Computer Society (2005)
42. Unruh, D.: Quantum proofs of knowledge. In: EUROCRYPT. pp. 135–152 (2012)
43. Unruh, D.: Collapse-binding quantum commitments without random oracles. In: ASIACRYPT. pp. 166–195 (2016)
44. Unruh, D.: Computationally binding quantum commitments. In: EUROCRYPT. pp. 497–527 (2016)
45. Watrous, J.: Limits on the power of quantum statistical zero-knowledge. In: FOCS. pp. 459–468 (2002)
46. Watrous, J.: Theory of Quantum Information. Cambridge University Press (2018)
47. Winter, A.J.: Coding theorem and strong converse for quantum channels. IEEE Trans. Inf. Theory **45**(7), 2481–2485 (1999)
48. Wolf, S., Wullschleger, J.: Oblivious transfer is symmetric. In: Vaudenay, S. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 4004, pp. 222–232. Springer (2006)
49. Yan, J.: Complete problem for perfect zero-knowledge quantum proof. In: SOFSEM. pp. 419–430 (2012)
50. Yan, J.: General properties of quantum bit commitments. Cryptology ePrint Archive, Report 2020/1488 (2020), `https://ia.cr/2020/1488`
51. Yan, J.: Quantum computationally predicate-binding commitments with application in quantum zero-knowledge arguments for NP. In: ASIACRYPT. Lecture Notes in Computer Science, vol. 13090, pp. 575–605. Springer (2021)
52. Yan, J., Weng, J., Lin, D., Quan, Y.: Quantum bit commitment with application in quantum zero-knowledge proof (extended abstract). In: ISAAC. pp. 555–565 (2015)
53. Yao, A.C.: Theory and applications of trapdoor functions (extended abstract). In: 23rd Annual Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982. pp. 80–91 (1982)
54. Yao, A.C.C.: Security of quantum protocols against coherent measurements. In: STOC. pp. 67–75 (1995)