How to Base Security on the Perfect/Statistical Binding Property of Quantum Bit Commitment?

Junbin Fang
Jinan University, Guangzhou, China

Dominique Unruh ✉
University of Tartu, Estonia

Jun Yan[1] ✉
Jinan University, Guangzhou, China

Dehua Zhou
Jinan University, Guangzhou, China

Abstract

The concept of quantum bit commitment was introduced in the early 1980s for the purpose of basing bit commitments solely on principles of quantum theory. Unfortunately, such unconditional quantum bit commitments still turn out to be impossible. As a compromise like in classical cryptography, Dumais et al. [17] introduce the conditional quantum bit commitments that additionally rely on complexity assumptions. However, in contrast to classical bit commitments which are widely used in classical cryptography, up until now there is relatively little work towards studying the application of quantum bit commitments in quantum cryptography. This may be partly due to the well-known weakness of the general quantum binding that comes from the possible superposition attack of the sender of quantum commitments, making it unclear whether quantum commitments could be useful in quantum cryptography.

In this work, following Yan et al. [43] we continue studying using (canonical non-interactive) perfectly/statistically-binding quantum bit commitments as the drop-in replacement of classical bit commitments in some well-known constructions. Specifically, we show that the (quantum) security can still be established for zero-knowledge proof, oblivious transfer, and proof-of-knowledge. In spite of this, we stress that the corresponding security analyses are by no means trivial extensions of their classical analyses; new techniques are needed to handle possible superposition attacks by the cheating sender of quantum bit commitments.

Since (canonical non-interactive) statistically-binding quantum bit commitments can be constructed from quantum-secure one-way functions, we hope using them (as opposed to classical commitments) in cryptographic constructions can reduce the round complexity and weaken the complexity assumption simultaneously.

2012 ACM Subject Classification Theory of computation; Theory of computation → Cryptographic primitives

Keywords and phrases Quantum bit commitment, quantum zero-knowledge, quantum proof-of-knowledge, quantum oblivious transfer

Digital Object Identifier 10.4230/LIPIcs.ISAAC.2022.26

Related Version *Full Version*: https://eprint.iacr.org/2020/621

Funding *Junbin Fang*: Junbin Fang was supported by National Natural Science Foundation of China (Grant No. 62171202).
Dominique Unruh: Dominique Unruh was supported by the ERC consolidator grant CerQuS (Grant No. 819317), by the Estonian Centre of Exellence in IT (EXCITE) funded by ERDF, by PUT team grant PRG946 from the Estonian Research Council.

[1] The corresponding author

Jun Yan: Jun Yan 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).
Dehua Zhou: Dehua Zhou was supported by Science and Technology Project of Guangzhou City (Grant No. 201707010320).

1 Introduction

Bit commitment is an important cryptographic primitive. A bit commitment scheme can be viewed as a digital analogue of a non-transparent sealed envelope. Informally, a classical bit commitment scheme is a classical two-stage interactive protocol between a *sender* and a *receiver*, both of whom can be formalized by probabilistic polynomial-time algorithms. First in the *commit* stage, the sender commits to a bit b such that the receiver should not be able to guess its value better than a random guess; this is known as the *hiding* property. Later in the *reveal* stage, the sender opens the bit commitment and reveals the bit b to the receiver. The *binding* property guarantees that any cheating sender should not be able to open the bit commitment as $1 - b$.

As quantum technology develops quickly, in this work we study *quantum bit commitments* that allow both the sender and the receiver of commitments to run *quantum* polynomial-time algorithms and exchange *quantum* messages[2] (whereas still a *classical* bit is secured) [17, 13, 23, 24, 10, 43]. Unfortunately, neither *unconditional* quantum bit commitments are possible [28, 26]. Based on quantum complexity assumptions, there are also *two flavors* of quantum bit commitments: (computationally-hiding) *statistically-binding* quantum bit commitments [17, 23, 24] and *statistically-hiding* (computationally-binding) quantum bit commitments [43].

One reason that we are interested in quantum bit commitment is because it can be made *non-interactive* in both the commit and the reveal stages (i.e. both stages consist of just a single message from the sender to the receiver), even based on the seemingly minimum quantum-secure one-way function assumption [43, 23, 24]. In contrast, classical constructions of non-interactive statistically-binding bit commitments and constant-round statistically-hiding bit commitments are only known relying on stronger complexity assumptions [19]; some negative results suggest that the interactivity seems inherent [27, 21].

Since (classical) bit commitments are extremely useful in classical cryptography, we naturally will ask whether this is also true for quantum bit commitments in quantum cryptography. In particular, we ask the following question that is the main motivation of this work:

> **Motivating question:** *If we use non-interactive quantum bit commitments in existing (classical or quantum) cryptographic constructions, then can we still base the (quantum) security of those constructions on that of quantum bit commitment?*

If the answer to the question is "yes", then by turning to non-interactive quantum bit commitments, we may reduce the round complexity and keep the complexity assumption of cryptographic constructions to the minimum simultaneously.

---

[2] A special case of quantum bit commitments considered in the post-quantum setting [1, 34, 36, 35], a.k.a. classical bit commitments secure against quantum attacks, have classical construction; that is, honest parties' computation and communication are restricted to be classical.

Inspired by the study of complete problems for quantum zero-knowledge proofs [38, 22, 40] and more general quantum interactive proofs [33, 11], *canonical*[3] (non-interactive) quantum bit commitments are introduced in [43]. Roughly speaking, a canonical quantum bit commitment scheme can be represented by a quantum circuit pair ensemble $\{Q_0(n), Q_1(n)\}_n$. To commit a bit $b \in \{0,1\}$, perform the quantum circuit Q_b on the quantum registers (C, R) initialized in all $|0\rangle$'s state, and the quantum state of the commitment register C will be treated as the commitment. The binding property of the scheme $\{Q_0(n), Q_1(n)\}_n$, a.k.a. *honest-binding*, requires that no unitary operation performing on the decommitment register R can send the quantum state $Q_0|0\rangle$ to $Q_1|0\rangle$, and vice versa. This binding property appears even weaker than *sum-binding*[4] (which is considered as the general binding property of quantum bit commitments [17, 13, 35]). Canonical statistically-binding quantum bit commitments can be based on quantum-secure one-way functions [43].

This work. In this work, we answer the motivating question above *affirmatively* when canonical statistically-binding quantum bit commitments are used. We remark that restricting to consider quantum bit commitments of the canonical form in applications does not lose generality (in theory); refer to Subsection 1.2. We also remark that another flavor of quantum bit commitments, i.e. those that are *computationally* binding, turn out to be more exotic [13, 16, 2, 36, 35] and beyond the scope of this work.

To the best of our knowledge, we are aware of no prior work besides [43] studying the application of non-interactive quantum bit commitments solely based on quantum-secure one-way functions in quantum cryptography. Follow-up work and recent developments are referred to Subsection 1.5.

1.1 On the difficulty of basing security on that of quantum bit commitment

New difficulties will arise when we try to use quantum instead of classical bit commitments in cryptographic applications and establish their (quantum) security. This was already realized in some pioneer works on quantum commitments [17, 13, 16, 34, 36]. For the purpose of presenting this work, these new difficulties can be understood by examining Blum's zero-knowledge protocol for the **NP**-complete language Hamiltonian Cycle [8] with a general quantum bit commitment scheme plugged in; we would like to show that the resulting protocol is both zero-knowledge and sound against quantum attacks.

For *zero-knowledge*, recall that in the classical security analysis, it relies on the hiding property of bit commitment; moreover, the security reduction will rewind the possibly cheating verifier. Though quantum hiding is a straightforward generalization of classical hiding, we cannot rewind a quantum verifier freely in general [37]. Thus, the classical analysis does not extend to the quantum setting straightforwardly. Fortunately, this can be rescued by using Watrous's remarkable quantum rewinding technique [39].

The more challenging part of the security analysis lies in showing *soundness*, which is to be (if possible) based on the binding property of quantum bit commitment. This is because it is well-known that the *general* quantum *sum-binding* [17, 35] is much weaker than the classical-style binding (or *unique-binding* hereafter). Roughly speaking, sum-binding only

[3] Originally, it was called "generic" quantum bit commitment in [43] and early drafts of this work. The name "canonical" is suggested by Ananth, Qian and Yuen [4] later, which (we agree) is more appropriate.

[4] But this does not exclude the possibility that the seemingly weak honest-binding may imply stronger binding properties such as sum-binding.

guarantees that any cheating sender of bit commitment cannot open it such that $p_0 + p_1 - 1$ is non-negligible, where p_0 (resp. p_1) is the success probability of opening the commitment as 0 (resp. 1). The reason of sum-binding for quantum bit commitments can be seen such a superposition attack of the sender of bit commitment as follows. A cheating sender can commit to an arbitrary *superposition* of the bit 0 and 1, in such a way that with this superposition as the control, executes the commitment stage of the quantum bit commitment scheme *honestly* [17, 13]. In this scenario, the "committed value" will become a superposition (as opposed to a classical bit). Later in the reveal stage, the bit commitment can be opened as the same superposition. At this moment, if the (honest) receiver measures (thus collapses) this superposition, then the outcome will be a distribution over $\{0, 1\}$. In particular, both 0 and 1 could be revealed with a *noticeable* probability, e.g. when the superposition is $1/\sqrt{2}(|0\rangle + |1\rangle)$.

Even worse, when quantum bit commitments are composed in parallel (to commit a binary string) and used in some larger protocol, it is possibly the sender of commitments who decides which bit commitments will be opened. In this case, not only the revealed value but also the classical information about positions of bit commitments that will be opened could be in an arbitrary superposition. This will make the quantum security analysis (if possible) much more complicated than classical analysis.

Specific to the soundness of Blum's protocol, the cheating prover (who will play the role of the sender of commitments) may try to either open *all* quantum bit commitments as a superposition of permuted input graphs (when the verifier's challenge is 0), or open a *superposition* of subsets (each corresponding to a possible location of Hamiltonian cycles) of quantum bit commitments as all 1's (when the verifier's challenge is 1). A more formal treatment about the cheating sender's superposition attack is referred to the full paper [18, Appendix A].

For the soundness analysis of Blum's protocol, the most straightforward way is trying to argue that superpositions can somehow be viewed as *collapsed* to their corresponding probability distributions, so that the classical soundness analysis can be applied. This is possible in the post-quantum setting (where quantum-secure classical bit commitments are used) by introducing stronger (computational) *collapse-binding* commitments [36]. However, current known constructions of collapse-binding commitments are interactive and rely on stronger quantum complexity assumptions than quantum-secure one-way functions in the standard model [35]. We still do not know if any non-interactive quantum bit commitment based on quantum-secure one-way functions can satisfy some "meaningful" collapse-binding property that could be useful in applications yet.

Alternatively, one can assume without loss of generality that the verifier will measure nothing other than the qubit indicating whether to accept or not and then carries out a more direct calculation involving superpositions in the analysis, like in [43]. A technical difficulty towards this approach lies in that there could be exponentially many terms in superpositions (even only polynomial many bits are committed), and naive applications of the triangle inequality will cause an exponential blow-up of errors. One should try to avoid this potential exponential blow-up when the binding error of commitments is only guaranteed negligible (as typical in cryptography). In an earlier draft of [43], this difficulty was circumvented by composing the given commitment scheme in parallel to reduce the statistical binding error to be *exponentially* small. The technique to handle negligible binding errors is called *perturbation*, as claimed in the final conference version of [43]. However, for some reasons, the final full version of [43] has never appeared[5].

[5] This is partly because its technique will be generalized and its main result will be reproved (in a conceptually much simpler way) in this paper. This will become clear later.

Besides collapse-binding commitments [36] just mentioned, two other works [13, 16] also try to base the security of cryptographic constructions on other binding properties of quantum commitments. However, it is still open whether these quantum commitments can be realized based on standard complexity assumptions.

1.2 Our contribution

In this work, we propose an *analysis framework* for basing security of cryptographic constructions on the *perfect/statistical* binding property of *canonical* (non-interactive) quantum bit commitment used within, and devise several techniques/tricks for this purpose. For *applications*, we plug canonical perfectly/statistically-binding quantum bit commitments in three well-known constructions, including zero-knowledge, oblivious transfer, and (zero-knowledge) proof-of-knowledge, and establish their (quantum) security. Our results exemplify that (statistically-binding) quantum bit commitment could be a useful primitive in quantum cryptography.

We remark that restricting to consider quantum bit commitments of the *canonical* form does not lose generality (in theory) for two reasons: (1) It turns out that any quantum bit commitment scheme can be compiled into the canonical form [41]; (2) We believe that statistically-binding quantum bit commitments of other forms can be handled similarly (as demonstrated by a more recent work [3]; refer to Subsection 1.5).

The analysis framework. It proceeds in *two* steps:

1. Lift the *classical or quantum* security of the construction based on the *perfect/statistical* unique-binding property of bit commitment to the *quantum* security that is based on the *perfect* binding property of canonical quantum bit commitment. This step may vary from application to application, but the *basic idea* is the same: introduce what we will call "commitment measurements" to collapse the potential superposition of the committed value underlying quantum bit commitments.
2. Extend the security based on quantum *perfect* binding to quantum *statistical* binding. We highlight that this step is *not* trivial, due to the potential exponential blow-up of the error aforementioned. This is in contrast to the classical setting, where such an extension is trivial by a simple union bound. The basic idea of this step is *perturbation*, as inspired by [43]. Specifically, by perturbation it can be shown that the error also (like in the classical setting, but for a completely different reason) grows *linearly* in the number of bit commitments that will be opened. We remark this second step is *standard*, almost the same for all applications. Hence, it allows us to focus on the first step of the analysis framework for the whole security analysis.

Techniques/tricks supporting the analysis framework will be introduced in Subsection 1.3.

Applications. We will apply the analysis framework in three applications listed as below:

1. Quantum zero-knowledge proof. We plug a canonical statistically-binding quantum bit commitment scheme in Blum's protocol for the **NP**-complete language Hamiltonian Cycle and establish its quantum security. The hard part of the security analysis lies in showing its soundness, which was firstly established in [43]. Here, we give an *alternative* proof following the analysis framework [18, Lemma 11, Corollary 12], which we believe is conceptually simpler. We also note that this analysis can be easily extended to any other GMW-type zero-knowledge protocols, which in particular include the GMW protocol for Graph 3-Coloring [20].

As an immediate corollary, we reprove the following theorem (also firstly proved in [43]):

▶ **Theorem 1.** *If quantum-secure one-way functions exist, then every language in* ***NP*** *has a three-round public-coin quantum (computational) zero-knowledge proof with perfect completeness and soundness error* $1/2 + o(1)$.

By the virtue of non-interactive (quantum) commitments used, the protocol guaranteed by the theorem above reduces one round compared with the classical protocol which uses interactive bit commitments [31].

2. Quantum oblivious transfer. We plug a canonical perfectly/statistically-binding quantum bit commitment scheme in the quantum oblivious transfer protocol [6, 12, 15] and establish its quantum security. The hard part of the security analysis lies in establishing the security against Bob, who is the receiver of oblivious transfer and plays the role of the sender of quantum bit commitments in this larger protocol. Following our analysis framework, we lift the security against Bob in the case where classical perfect unique-binding bit commitments are used [6, 12, 29, 44, 9] to our setting [18, Lemma 13, Corollary 14]. As an immediate corollary, we reprove the following well-known theorem:

▶ **Theorem 2.** *If quantum-secure one-way functions exist, then there exists a constant-round 1-out-of-2 quantum oblivious transfer that is computationally secure against Alice and unconditionally secure against Bob, with the security is in the following sense: after the interaction, Alice cannot guess Bob's choice bit, while Bob is not aware of the other bit owned by Alice.*

We stress that the security achieved by the theorem above is *not* the full *simulation-security* (as mostly desired in cryptography). However, it still could be useful in some applications. For example, it can be used to construct statistically-hiding (computationally-binding) quantum bit commitment [14, 41].

We also remark that there is no gain in the round complexity by using non-interactive quantum bit commitments in the quantum oblivious transfer protocol. This is because, for example when Naor's bit commitment scheme [31] is used, the first message of the bit commitment scheme can be absorbed into earlier Alice's messages prescribed by the larger quantum oblivious transfer protocol.

3. Quantum (zero-knowledge) proof-of-knowledge. Unruh [34] shows that if commitments satisfying some specific binding property exists, then plugging it in a variant of Blum's protocol gives rise to a quantum (computational) zero-knowledge proof-of-knowledge for the **NP**-complete language Hamiltonian Cycle [8]. Moreover, Unruh shows that such commitments can be based on *injective* quantum-secure one-way functions. Here we plug a canonical *perfectly/statistically*-binding quantum bit commitment in the same variant of Blum's protocol and show that the quantum proof-of-knowledge can also be fulfilled [18, Corollary 17, Corollary 18]. As an immediate corollary, we arrive at the following *new* theorem that is previously unknown:

▶ **Theorem 3.** *If quantum-secure one-way functions exist, then every language in* ***NP*** *has a three-round public-coin quantum (computational) zero-knowledge proof-of-knowledge with perfect completeness and knowledge error* $1/2$.

Compared with Unruh's (post-quantum) result, we make use of *quantum* construction and succeed in reducing the complexity assumption to general (removing the requirement of injectiveness) quantum-secure one-way functions. This answers an open question raised by Unruh [34] affirmatively.

Our analysis of quantum proof-of-knowledge is interesting. In some detail, in the analysis we will construct a canonical knowledge extractor like the one constructed in [34], which will make use of a quantum rewinding that is also similar to the one used in [34]. However, commitments used in [34] ensure that the whole quantum system is only slightly perturbed before the rewinding, whereas in our case the system may have collapsed significantly due to the possible superposition attack of the cheating prover (who will play the role of the sender of commitments). So why the quantum rewinding works in our setting seems for a *different* reason than that in [34]. Interestingly, it turns out that the underlying reason is also the same; but how to interpret it will be different, and not clear at all as it appears. Basically, it will only become clear if one views sending a bit commitment to a superposition (using a canonical (computationally-hiding) perfectly-binding quantum bit commitment scheme) as an *implicit measurement* of this committed superposition without leaking the outcome. More discussion on this point is referred to Subsection 1.4.

1.3 Our techniques/tricks

We give a brief overview of our techniques/tricks used in this work. Their formal treatment is referred to the full paper [18, Section 4].

(Imaginary) commitment measurement. In the case that the canonical quantum bit commitment scheme used is perfectly binding, we can introduce an *imaginary* binary projective measurement performed on each claimed quantum bit commitment; we will call it "commitment measurement" hereafter. It turns out that in many interesting situations, introducing commitment measurements will *not* affect the receiver's acceptance probability of opening quantum bit commitments later. In more detail, the *commitment measurement* is just the measurement that perfectly distinguishes the *honest* commitment (meaning the sender will follow the scheme in the commit stage) to 0 and that to 1, which is *not* efficiently realizable (otherwise, the commitment scheme is not computationally hiding). In spite of this, we can introduce it for the purpose of the security analysis. The *benefit* of doing so is that the superposition of the committed value underlying quantum bit commitments will then *collapse* to its corresponding probability distribution. In turn, by averaging over all possible committed values, it suffices for us to prove the security w.r.t. an arbitrary committed value. But now the analysis is similar to the one based on perfect unique-binding. In summation, this technique is useful in realizing Step 1 of the analysis framework. Similar techniques were also used in [32, 14].

Measurement manipulation. In our quantum security analysis, we may *add* or *remove* a measurement, or *replace* a measurement with other ones. This may seem tricky, but it turns out useful. For example, without affecting the security, sometimes we may try to collapse the quantum system as much as we can by introducing new measurements, so that the analysis based on perfect unique-binding can be lifted to the our setting where canonical perfectly-binding quantum bit commitments are used; in other situations, we may try to collapse less by removing measurements, so that some quantum-specific techniques can be applied, including the *perturbation* and the *quantum rewinding* that will be introduced shortly below. In summation, this technique is useful in realizing Step 1 of the analysis framework.

Commit to secret coins. The trick of letting a cheating party commit to secret coins it used in quantum cryptographic constructions was introduced by Unruh [34, 36]. It enables a quantum rewinding to work in the security analysis, where the commitments used there are unique binding. We find that the same trick also enables a similar quantum rewinding even if canonical statistically-binding quantum bit commitments (whose binding property is much weaker than unique-binding) are used. More detail is referred to the proof overview of quantum proof-of-knowledge in Subsection 1.4.

Perturbation. We devise a generic procedure for realizing Step 2 of the analysis framework. Our basic idea is to *perturb* the quantum circuit pair (Q_0, Q_1) that represents a canonical statistically-binding quantum bit commitment scheme. The resulting perturbed scheme, denoted by $(\tilde{Q}_0, \tilde{Q}_1)$, will be sort of *perfectly binding*. We note that quantum circuits $\tilde{Q}_0, \tilde{Q}_1$ may be of *super-polynomial* size; but this is not a problem for the purpose of security analysis. A *key observation* is that the error incurred by replacing the scheme (Q_0, Q_1) with the scheme $(\tilde{Q}_0, \tilde{Q}_1)$ in any quantum computation only grows *linearly* in the number of such replacements. The *zero-binding-error* guaranteed by the quantum perfect binding property of the scheme $(\tilde{Q}_0, \tilde{Q}_1)$ can help us avoid the potential exponential blow-up of errors in the security analysis as mentioned before. Similar techniques were also used in [11, 39].

A quantum rewinding lemma with improved bound. The quantum rewinding lemma in [43] enables a similar quantum rewinding as the one used in [34]. In this work, we will use the same lemma but with an *improved* lower bound on the success probability of the quantum rewinding. It allows us to obtain the asymptotically optimal knowledge error in the analysis of quantum proof-of-knowledge [18, Section 7].

1.4 Proof overview of our applications

While Step 2 of the analysis framework is standard, in the below we give an overview of Step 1 of applying the analysis framework to the three applications aforementioned (i.e. lifting the classical/quantum security based on the perfect unique-binding property of bit commitment to the quantum security based on the perfect binding property of canonical quantum bit commitment).

Zero-knowledge proof. Perform the commitment measurement on each claimed quantum bit commitment sent by the cheating prover. Then the classical soundness analysis can be lifted to our setting straightforwardly.

Quantum oblivious transfer. Call the sender of oblivious transfer Alice and the receiver Bob. Consider the security against Bob, who will play the role of sender of commitments. Compared with the GMW-type quantum zero-knowledge proof protocols, the quantum oblivious transfer protocol will continue after Alice's opening of quantum bit commitments. Thus, compared with the soundness analysis of quantum zero-knowledge proof, we need to take into account not only Alice's acceptance probability of its verification but also the *post-verification state* of the whole system. To show the security against Bob, we also perform the commitment measurement to each claimed quantum bit commitment sent by Bob. It turns out that via a simple reduction, the (quantum) analysis for the same quantum oblivious transfer protocol but with perfect unique-binding commitments plugged in [44, 9] can be lifted to our setting straightforwardly.

Quantum proof-of-knowledge. Compared with the two applications above, the main difficulty here comes from the quantum rewinding: our quantum rewinding lemma ([18, Lemma 10], which is similar to the one used in [34]) only allows us to measure the qubit indicating whether the verifier accepts or not; but for the purpose of extracting a witness, we need to measure more!

In [34], the difficulty caused by quantum rewinding as mentioned above was circumvented by a simple trick: let the prover additionally commit (using perfect unique-binding commitments) to its secret random coins used in its first message. In this way, the prover's second message will become "unique" for the verifier to accept. In turn, removing the measurement for extracting other classical information (than the single qubit just mentioned) will not affect the success probability of the quantum rewinding. However, this argument seems not to extend straightforwardly to our setting where canonical perfectly-binding quantum bit commitments are used. This is because the potential superposition of the committed value underlying commitments may collapse *significantly* by measurements for extracting other classical information.

Interestingly, after a few thought, it turns out that the trick used in [34] to enable quantum rewinding still works in our setting, and for a similar reason! But this is not clear at all at first glance; one can only see this after one has come to realize that sending a commitment to a superposition using a canonical (computationally-hiding) perfectly-binding quantum bit commitment scheme amounts to an *implicit measurement* of this committed superposition (due to perfect binding) without leaking the outcome (due to computational hiding). Here, the "implicit measurement" is in a similar sense as the standard unitary simulation of measuring a qubit in the computational basis[6]. Intuitively, one can view commitments in this way is because the commitment to 0 and that to 1 are orthogonal, and they will never be touched by the sender of commitments after they are sent.

In the analysis of quantum proof-of-knowledge, now that the prover has already *collapsed* the quantum state by additionally sending commitments to its secret random coins used in its first message, the (explicit) measurement of its response (i.e. its second message) by the knowledge extractor to extract classical information will cause no more collapses. Therefore, removing this measurement will enable us to apply our quantum rewinding lemma like in [34].

1.5 Follow-up work and recent developments

Since the first preprint of this paper uploaded to Cryptology ePrint Archive [18] back in 2020, significant progress has been made towards studying quantum commitments and their applications. Now let us mention some of them that are most relavant to this work.

In two follow-up works, Yan [41] study general properties of quantum bit commitments through the lens of canonical quantum bit commitments. Somewhat surprisingly, it turns out that any interactive (as opposed to just non-interactive, which is already known in [43]) quantum bit commitment scheme can be compiled into the canonical form. Yan [42] manages to base the computational soundness of Blum's zero-knowledge protocol on the computational binding property of canonical quantum bit commitment (when it is used in Blum's protocol). In its analysis, different techniques are used.

Also starting from Naor's scheme [31] like [43], Bitansky and Brakerski [7] construct another non-interactive statistically-binding quantum bit commitment scheme that achieves the unique-binding; Ananth, Qian and Yuen [3] construct a two-message statistically-binding

[6] That is, initialize an ancilla qubit in the state $|0\rangle$, and then store the measurement outcome in this qubit without further disturbed afterwards.

quantum bit commitment scheme but based on pseudorandom quantum states, an arguably weaker complexity assumption than quantum-secure one-way functions [25]. A common benefit of these two constructions is that their reveal stage consists of just a single *classical* message. The latter AQY scheme is also shown to satisfy a stronger quantum statistical binding property (*AQY-binding* hereafter) that turns out useful in applications (e.g. [5]).

After a careful examination, we find that the underlying idea of AQY-binding is almost the same as that of the analysis framework introduced in this work; this is also observed in a recent work by Morimae and Yamakawa [30, Appendix B]. Roughly speaking, AQY-binding is a quantum statistical binding property for *general* (as opposed to canonical) quantum commitments that is used in a similar way as our analysis framework in applications; and it can be shown by combining similar techniques as *commitment measurement* and *perturbation* introduced in this work. Actually, by tweaking these two techniques one can show that the statistical binding property of canonical quantum bit commitment implies the AQY-binding property [41, Appendix B]. As a consequence, following [3] canonical statistically-binding quantum bit commitments can also be used to instantiate the construction in [5] to achieve the *full simulation-secure* quantum oblivious transfer[7] (as opposed to the weaker one presented in Section 6 of this paper).

Comparing our analysis framework and the AQY-binding property in applications, all the technical detail in the former analysis will be hidden in establishing the latter binding property. Thus, AQY-binding is more readily usable by cryptographers. Another advantage of AQY-binding is that it is more general, i.e. not necessarily requires canonical quantum bit commitments. In spite of this, as argued at the beginning of Subsection 1.2, restricting to consider canonical statistically-binding bit commitments and use our analysis framework does not lose generality. Moreover, our analysis framework *explicitly* allows us to ignore the statistical binding error while focusing on perfectly-binding (canonical) quantum bit commitments in general. This will often make the security analysis conceptually simpler.

References

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

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

3 Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. Cryptology ePrint Archive, Report 2021/1663, 2021. URL: `https://ia.cr/2021/1663`.

4 Prabhanjan Ananth, Luowen Qian, and Henry Yuen, 2022. Private communication.

5 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.

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

7 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.

8 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.

[7] We believe that techniques/tricks introduced in this work suffices for this job, too.

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

10 André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In *FOCS*, pages 354–362, 2011.

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

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

13 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.

14 Claude Crépeau, Frédéric Légaré, and Louis Salvail. How to convert the flavor of a quantum bit commitment. In *EUROCRYPT*, pages 60–77, 2001.

15 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.

16 Ivan Damgård, Serge Fehr, and Louis Salvail. Zero-knowledge proofs and string commitments withstanding quantum attacks. In *CRYPTO*, pages 254–272, 2004.

17 Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *EUROCRYPT*, pages 300–315, 2000.

18 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. URL: `https://ia.cr/2020/621`.

19 Oded Goldreich. *Foundations of Cryptography, Basic Tools*, volume I. Cambridge University Press, 2001.

20 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.

21 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.

22 Hirotada Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In *ISAAC*, pages 178–188, 2003.

23 Takeshi Koshiba and Takanori Odaira. Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. In *TQC*, pages 33–46, 2009.

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

25 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.

26 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.

27 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.

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

29 Dominic Mayers and Louis Salvail. Quantum oblivious transfer is secure against all individual measurements. In *Physics and Computation, 1994. PhysComp'94, Proceedings., Workshop on*, pages 69–77. IEEE, 1994.

30 Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. *Cryptology ePrint Archive, Report 2021/1691*, 2021. URL: `https://ia.cr/2021/1691`.

31 Moni Naor. Bit commitment using pseudorandomness. *J. Cryptology*, 4(2):151–158, 1991.

32 Oded Regev. Witness-preserving amplification of QMA, 2006. Lecture notes of course Quantum Computation.

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

34 Dominique Unruh. Quantum proofs of knowledge. In *EUROCRYPT*, pages 135–152, 2012.

35 Dominique Unruh. Collapse-binding quantum commitments without random oracles. In *ASIACRYPT*, pages 166–195, 2016.

36 Dominique Unruh. Computationally binding quantum commitments. In *EUROCRYPT*, pages 497–527, 2016.

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

38 John Watrous. Limits on the power of quantum statistical zero-knowledge. In *FOCS*, pages 459–468, 2002.

39 John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. Preliminary version appears in *STOC* 2006.

40 Jun Yan. Complete problem for perfect zero-knowledge quantum proof. In *SOFSEM*, pages 419–430, 2012.

41 Jun Yan. General properties of quantum bit commitments. Cryptology ePrint Archive, Report 2020/1488, 2020. URL: `https://ia.cr/2020/1488`.

42 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.

43 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.

44 Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *STOC*, pages 67–75, 1995.