General Non-interactive Quantum Commitments Are Compatible with Quantum Rewinding

Jun Yan[*]

Jinan University

August 29, 2023

Abstract

In this work, we show that *general* non-interactive quantum commitments (allowing quantum computation and communication) to *classical* messages are compatible with current-known quantum-rewinding techniques. Specifically, we first propose a definition of collapse-binding of quantum commitments which generalizes from its post-quantum counterpart and is shown to work well with quantum rewinding. Then we show that thus defined collapse-binding is equivalent to the conceivably minimal unique-message-binding. This in particular implies that canonical quantum bit commitments are collapse-binding and can be used to instantiate many cryptographic applications.

Additionally, we rephrase the flavor conversion of canonical quantum bit commitments as a hardness conversion, which then can be used to establish a stronger quantum indistinguishability that works well with quantum rewinding just like in the post-quantum setting. Such indistinguishability allows us to establish the security of the Goldreich-Kahan construction of constant-round zero-knowledge proofs for **NP** instantiated with canonical quantum bit commitments. We thus for the first time construct a *constant-round* (actually, four-round) quantum computational zero-knowledge proof for **NP** based on the *minimum* complexity assumption that is needed for the complexity-based quantum cryptography.

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

Contents

1 Introduction

Commitment is an important primitive in cryptography [Blu83, Gol01]. Intuitively, one can view the commitment as an electronic realization of an opaque box that can be locked with a key. A commitment scheme prescribes two stages of the commitment, a commit stage and a reveal stage. The commit stage corresponds to the sender sending an opaque box with the message to commit locked in to the receiver, while the reveal stage corresponds to the sender sending the key to the receiver to open the box and reveal the committed message. The scheme is hiding if any malicious receiver cannot guess the committed message correctly with advantage significantly larger than a random guess during the commit stage; this corresponds to that the box is opaque. The scheme is binding if any malicious sender cannot open the commitment as two different messages in the reveal stage; this corresponds to that the box is out of the sender's reach (who thus cannot change the message locked inside the box after it is sent).

Numerous cryptographic applications, notably zero-knowledge [Blu86, GMW91], can be based on commitments. Unfortunately, unconditional commitments do not exist; as a compromise, we can introduce computational complexity assumptions, studying computational commitments. In complexity-based cryptography, commitments can be constructed from the *minimum* assumption, i.e. one-way functions [IL89].

Turning to the quantum world, one natually tends to study quantum commitments, i.e. the quantum realization (allowing both quantum computation and communication, which in particular includes the classical realization as a special case) of commitments to *classical* messages secure against quantum attacks.[1] Unconditional quantum commitments are impossible either [May97, LC98]; we can similarly study computational quantum commitments. One of the original motivation for studying computational quantum commitment lies in its *non-interactivity* (i.e. just a single message in both the commit and the reveal stage) [DMS00, KO09, KO11, YWLQ15, Yan22, BB21, MY21, HMY22b], which is preferred in cryptography to reduce the round complexity [YWLQ15, FUYZ22, Yan21].

Apart from its cryptographic applications, recent studies suggest that quantum commitment is perhaps an even more fundamental notion than what one can see in the first place. Specifically, Yan [Yan22] discovers that (canonical) quantum bit commitment (QBC) can be reformulated as two *equivalent* quantum complexity-theoretic objects, EFI (named after [BCQ22]) and $\mathsf{Uhlmann}$, which may serve as the *minimum* assumption (rather than quantum-secure one-way functions [Kre21, KQST22]) of the complexity-based quantum cryptography [Yan22, BCQ22]. Seeing from this, QBC/EFI/$\mathsf{Uhlmann}$ may play an important role in MiniQCrypt [GLSV21] (the quantum analog of Minicrypt in classical cryptography [Imp95]), as important as one-way functions in Minicrypt. The relationship between QBC/EFI/$\mathsf{Uhlmann}$ and other candidate complexity assumptions proposed for MiniQCrypt is studied in [MY22]. More interestingly, EFI is also found useful and important in studying cosmology [Aar16, Bra22], and $\mathsf{Uhlmann}$ in quantum complexity theory [Aar16, MY23, BEM$^+$23].

In this work, we focus on cryptography. Seeing from the above, to explore MiniQCrypt, we would like to base more cryptographic applications on quantum commitments. However, previous studies indicate that this is not an easy job; simply using quantum commitments as the drop-in replacement of classical commitments in existing cryptographic constructions does not imply their quantum security immediately. Generally speaking, the difficulty of the quantum security analysis is

[1] Commitments to quantum states [GJMZ22], which are also of great interest, is *not* studied in this paper. We will briefly discuss the relation between [GJMZ22] and this work in "Related work" subsequently, and then in greater detail in Subsection 2.7.

rooted in the adversary's possible *superposition attacks*, which prevent us from extending classical rewinding techniques to the quantum setting in a straightforward way [vdG97, Wat09, Unr12, ARU14]. The similar difficulty even appears in the *post-quantum* security analysis (where post-quantum commitments, i.e. classical commitments secure against quantum attacks, are used).

Fortunately, we still can devise several quantum rewinding techniques to prove the security of many well-known constructions (or their variants) with post-quantum and even quantum commitments plugged in, respectively [Wat09, Unr12, FUYZ22, CMSZ21, LMS21]. Before comparing the corresponding post-quantum and quantum analysis and motivating this work, we point out that many previous studies of quantum commitments in cryptographic applications focus on *canonical* quantum bit commitments [YWLQ15, FUYZ22, Yan21], which does not lose much generality. This is because canonical quantum bit commitments can be viewed as *complete* for quantum bit commitments [YWLQ15, Yan22] and are easier to work with, just like the complexity class **NP** is often studied through the lens of its complete language SAT.

Post-quantum vs. quantum analysis. Generally speaking, techniques for the post-quantum and quantum analysis are very similar; most techniques devised for the former (often earlier) extend to that of the latter. For example, Watrous's quantum rewinding lemma for proving post-quantum statistical/computational zero-knowledge [Wat09] and Unruh's quantum rewinding lemma (Lemma 5) [Unr12, Unr16b] for proving post-quantum proof/argument-of-knowledge extend to the quantum security analysis straightforwardly [YWLQ15, FUYZ22, Yan21] (and refer to Section 10.3 of this paper). Though using similar techniques, however, post-quantum analysis often does not extend to quantum analysis directly; the latter is usually harder and needs more care.

In particular, consider the security analysis based on the binding of post-quantum and quantum commitments, respectively:

1. *Statistical* post-quantum analysis does not extend to quantum analysis straightforwardly [YWLQ15, FUYZ22]. A *framework* for such an extension is provided in [FUYZ22, AQY21, Yan22], also associated with several generic techniques to support this framework. Hence, the question on how to do the quantum statistical analysis based on quantum statistical binding is essentially settled.

2. Many *computational* post-quantum analysis (e.g. [Unr16b, CMSZ21, LMS21]) rely heavily on a seemingly strong yet strange computational binding property known as *collapse-binding* [Unr16b], which works well with several quantum-rewinding techniques and enables extractions. However, the straightforward generalization of collapse-binding to quantum commitments [DS23, GJMZ22] (which will be referred to as single-opening collapse-binding in this paper (Definition 7)) alone seems not so useful as its post-quantum counterpart in cryptographic applications; reasons are referred to Section 2.1.[2] Moreover, somewhat surprisingly, earlier study [Yan21, Yan22, BCQ22] indicates that Blum's zero-knowledge protocol [Blu86] and some variants of the well-known quantum oblivious transfer protocol [CK88, BBCS91, Cré94] instantiated with canonical computationally-binding quantum bit commitments can be proved computationally secure, where the security is based on the *honest-binding* (a security only against the semi-honest sender) of canonical quantum bit commitments. Hence, it is unclear what binding property of *general* quantum commitments is needed in cryptographic applications, and what is the relationship between it and other binding properties.

[2] But combined with an abstract technical lemma in [GJMZ22], it could be useful in the quantum security analysis [LMS23]. However, this point is not mentioned in [GJMZ22] and not obvious (in our opinion) seeing from there, where only applications of commitments to more general quantum states are studied. More details are referred to Section 2.7.

The motivation of this work. Seeing from the above, we naturally ask the following question that motivates the study in this work:

> Can we identify any *computational* collapse binding property (or any other fancier binding properties) of (general) quantum commitments that is compatible with (currently-known) quantum rewinding techniques and as useful as the collapse-binding of post-quantum commitments in cryptographic applications?

If the answer to the motivating question above is affirmative, then we expect that the security analysis based on the computational binding of quantum commitments can be done in a more *modular* way than the one in [Yan21] (which seems ad hoc); we even expect that the security of more well-known constructions instantiated with quantum computationally-binding commitments can be established (e.g. [FS90, GK96]), answering an open questions raised in [Yan21].

We also hope that the complexity assumption for the construction of quantum computationally-binding commitments can be as *weak* as possible, preferably no need of any structure (in contrast to [Unr16a, Zha22]). In particular, w.r.t. canonical quantum bit commitments, does honest-binding imply such (computational) binding property? If this is true, then it would be wonderful: quantum commitments that are useful in applications and achieve the *optimal* round complexity (i.e. non-interactive) can be based on the *minimum* complexity assumption for quantum cryptography!

Collapse-binding and the idea of collapsing. Intuitively, collapse-binding states that attacking the sender of commitments by committing to a *superposition* only gains negligible advantage over the attack by committing to the message that is distributed according to the probability distribution obtained by *collapsing* this superposition.[3] Collapse-binding is an extremely useful property in post-quantum security analysis: it works well with quantum rewinding and enables extractions [Unr16b, CMSZ21, LMS21]. Even for the quantum security analysis where collapse binding is not explicitly mentioned, after a closer look, one can find that the analysis indeed involve the idea of *collapsing* [Unr22]. For example, the *commitment-measurement* technique explicitly introduces (hypothetical) collapses in the security analysis based on quantum perfect/statistical binding [FUYZ22]; regarding the computation tree constructed in [Yan21], its root corresponds to the committed superposition, while all its leaves correspond to strings distributed according to the probability distribution obtained by collapsing this superposition.

Earlier study of (post-)quantum collapse-binding suggests that it seems to be stronger than sum-binding [Unr16b] and collision-resistance (w.r.t. hash-based commitments) [ARU14]. And constructions of post-quantum (computationally) collapse-binding commitments rely either on the random oracle [Unr16b] or complexity assumptions with structures [Unr16b, Zha22].

Very recent study of collapse-binding shows that it is equivalent to a seemingly weaker binding property [DS23]; in particular, w.r.t. post-quantum or quantum *bit* commitments, it is actually equivalent to sum-binding [DS23, GJMZ22].

1.1 Our contribution

In this work, we answer the motivating question mentioned above affirmatively. In particular, we identify a (computational) collapse-binding property of quantum commitments that extends the (single-opening) collapse-binding [DS23, GJMZ22] and can be used similarly as that of post-quantum commitments in the security analysis of cryptographic applications. What is more, we can

[3] When an arbitrary normalized superposition (or a unit vector) of the form $\sum_{s\in\{0,1\}^n} \alpha_s |s\rangle$ is measured in the computational basis, it will collapse to the state $|s\rangle$ with probability $|\alpha_s|^2$.

show that canonical quantum bit commitments already satisfy this desired collapse-binding property. This implies that non-interactive quantum (computationally) collapse-binding commitments can be based on the minimum complexity assumption for quantum cryptography.

Formally, we prove a more general *equivalence* theorem as stated below, which will imply what we just mentioned above immediately.

Theorem 1 *A general (non-interactive) quantum commitment scheme (with polynomial bounded message space, or equivalently, logarithmic message length) is collapse binding if and only if it is unique-message binding.*

Our definition of collapse-binding and the proof of the equivalence theorem above build on many ideas and techniques in the existing literature studying quantum and post-quantum commitments and zero-knowledge, including but not limited to [Unr16b, FUYZ22, Yan21, CMSZ21, LMS21, GJMZ22, DS23]. More detail is referred to "Technical overview".

Now let us give some explanation to the *unique-message binding* mentioned in our equivalence theorem. This binding property is firstly introduced in [LMS21];[4] informally speaking, it guarantees that any malicious sender cannot open the same commitment as two different messages *sequentially.* Compared with collapse-binding, unique-message-binding (Definition 3) is closer to the intuitive binding (i.e. the classical-style binding); it is conceivably the *minimum* binding property that any useful quantum commitment should satisfy.

Implications on quantum (computational) binding. Since single-opening collapse-binding is equivalent to sum-binding w.r.t. non-interactive quantum *bit* commitments [DS23, GJMZ22], combined with our equivalence theorem, it follows that unique-message-binding, sum-binding, and collapse-binding are all equivalent. (This holds even for interactive public-coin post-quantum bit commitments; refer to "Generalization" subsequently.) In particular, restricting to canonical quantum bit commitments, we observe that unique-message-binding is equivalent to honest-binding; hence, honest-binding is equivalent to collapse-binding! This improves various known equivalences among honest-binding, sum-binding, and single-opening collapse-binding [Yan22, DS23, GJMZ22].

Benefits. The benefit of our equivalence theorem is two-fold:

1. In constructing (non-interactive) quantum commitments (even *interactive post-quantum* commitments), the equivalence theorem allows us to focus on the minimal unique-message-binding (instead of collapse-binding) in the security analysis, which will greatly simplify the task both conceptually and technically. Additionally, when specifying a (non-interactive) quantum commitment scheme, we also only need to specify its unique-message-binding error (Definition 2); virtually all other binding (e.g. collapse-binding, sum-binding, and so on) errors can be derived from the unique-message-binding error. And in the security analysis of cryptographic applications, we will express the advantage achieved by the malicious sender of commitments in terms of this binding error.

2. It guarantees that any (non-interactive) quantum commitment is collapse-binding. W.r.t. cryptographic applications, this collapse-binding property enables quantum rewinding with extractions. Combined with the unique-message binding, it allows us to use (non-interactive) quantum commitments as the drop-in replacement of post-quantum commitments in cryptographic applications, where the post-quantum security can be lifted to the quantum security

[4] They introduce unique-message binding w.r.t. post-quantum commitments; but their definition extends to general quantum commitments straightforwardly (Definition 3).

immediately. Actually, for this purpose, we prove a parallel composition lemma (Lemma 11), a sequential composition lemma (Lemma 12), and culminate in proving a theorem (Theorem 3) that can be viewed as providing a general *template* for the security analysis based on the binding of quantum commitments; refer to Section 10 and Appendix C for some examples. Recall that using (non-interactive) quantum commitments can potentially reduce the round complexity while weakening the complexity assumption simultaneously [FUYZ22, Yan21].

A comment on the message space. We note that though the message space is restricted to be polynomially bounded in our equivalence theorem, in cryptographic applications, one can compose the corresponding quantum commitment scheme in *parallel* to commit any messages whose length is polynomially bounded (Lemma 11). However, this weakness of our equivalence theorem makes it does not apply to succinct commitments [Unr16b, GJMZ22].

Generalization. Though our equivalence theorem is stated w.r.t. *non-interactive* quantum commitments, it trivially extends to post-quantum *public-coin* commitments whose commit stage could even be *interactive* but the reveal stage remains *non-interactive.* Unfortunately, in a try to extend it to general interactive quantum commitments, we will encounter a new difficulty. Refer to "Technical overview" (Section 2) for more information about the generalization of our equivalence theorem.

Constant-round quantum zero-knowledge proofs for NP. We rephrase the flavor-conversion theorem for canonical quantum bit commitments [HMY22b, Yam22] as a *hardness-conversion* theorem (Theorem 7). Besides its independent interest in quantum complexity theory, it also finds an interesting cryptographic application.

Specifically, combining the hardness-conversion theorem with the useless oracle lemma (Lemma 6) that was once used in proving our equivalence theorem, we can prove a stronger quantum indistinguishability that is compatible with the new quantum rewinding technique [MW05, CMSZ21, LMS21]. In turn, we show that the post-quantum security analysis for the Goldreich-Kahan construction [LMS21] can be adapted to give a quantum security analysis. In particular, we prove the following theorem:

Theorem 2 *The Goldreich-Kahan construction [GK96] instantiated with canonical quantum bit commitments is statistically sound and quantum computational zero-knowledge. Hence, assuming the existence of canonical quantum bit commitments/*EFI*/*$\mathsf{Uhlmann}$*, all* $\mathbf{NP}$ *languages have a quantum computational zero-knowledge proof with just four rounds.*

Note that the classical Goldreich-Kahan construction based on one-way functions is unlikely to be of *constant* rounds; this is because classical constructions of statistically-hiding, computationally-binding bit commitments seem need *polynomial* number of rounds [NOVY98, HNO+09, HHRS07]. Theorem 2 once again proves that with quantum constructions, we may reduce the round complexity while weakening the complexity assumption simultaneously!

1.2 Related work

There are two recent works that are closely related to this one.

Comparison to [GJMZ22]. In [GJMZ22], commitments to more general quantum *states* are studied, where a binding property called *swap-binding* is introduced there and proved useful in cryptographic applications. One can view our study of collapse-binding as a special case of theirs: we encounter similar difficulties, and to overcome which we use similar techniques; even some of our results can be derived from theirs [LMS23] (though in different ways). However, this does not mean that our study is just a trivial specialization of theirs. Indeed, inspired by cryptographic applications of quantum commitments, we come up with new definitions (e.g. Definition 8) that we believe are useful; we also discover something new and exciting (Theorem 1) that can hardly be seen from the more general study in [GJMZ22]. Moreover, in cryptographic applications where commitments to *classical* messages (rather than quantum states) are sufficient, our study of collapse-binding formalizes a template (Theorem 3) for the security analysis that will come in handy in the future. A more detailed comparison between this work and [GJMZ22] is referred to Subsection 2.7 after we give a technical overview of this work.

Comparison to [DS23]. It is shown in [DS23] that collapse-binding is equivalent to the so-called *chosen-bit-binding* w.r.t. post-quantum commitments. This equivalence also extends to quantum commitments, but only w.r.t. single-opening collapse-binding (Definition 7) that cannot be used in cryptographic applications straightforwardly. Compared with our equivalence theorem (Theorem 1), for establishing equivalences, both of us use similar techniques, in particular Lemma 9. An advantage of their equivalence than ours lies in that there is no restriction on the dimension of the message space of commitment schemes. However, in our opinion, the main advantage of our equivalence than theirs is that the unique-message binding is a more intuitive and important (its importance in cryptographic applications is briefly discussed in Subsection 2.5) binding property than the chosen-bit binding. Finally, we believe that there is a more direct way (not via collapse-binding) to establish the equivalence between unique-message-binding and chosen-bit-binding when the message space (of the commitment scheme) is polynomially bounded.

Organization

The remainder of this paper is organized as follows. In Section 2, we give a technical overview of new definitions introduced in this work, as well as proofs of our main results. Section 3 provides some preliminaries. In Section 4, we generalize unique-message binding to allow interactions between the malicious sender of commitments and the challenger in the corresponding experiments, where in Section 5 we show that this generalization does not make the life significantly easier for the malicious sender to win the experiment. Next in Section 6, we give a definition of collapse binding of quantum commitments that is compatible with quantum rewinding, and we show that it is equivalent to the unique-message binding in the Section 7. In Section 8 and 9, we prove that thus defined collapse binding enjoys very nice composition properties. In Section 10, we establish the security of Blum's zero-knowledge protocol and its variants instantiated with general (non-interactive) quantum bit commitments. Later in Section 11, we prove a stronger quantum indistinguishability that is compatible with quantum rewinding, and using which we establish the security of the Goldreich-Kahan construction of zero-knowledge proofs for **NP** instantiated with canonical quantum bit commitments. Finally, we conclude with Section 12.

2 Technical overview

2.1 The pursuit for a good definition of collapse-binding

Good definitions are important in cryptography. For post-quantum commitments, collapse-binding is crucial in the security analysis of cryptographic applications [Unr16b, CMSZ21, LMS21]. However, its generalization to general quantum commitments is not straightforward. As noted in [YWLQ15, FUYZ22, Yan21] and recent in [GJMZ22], the *major difference* between post-quantum and (general) quantum commitments lies in that the opening of the former is via some *correlation* between the commitment and the decommitment, i.e. a check of some *classical* predicate; this can be seen from the opening of any post-quantum commitment schemes, e.g. hash-based commitment schemes [Unr16b]. In contrast, the opening of quantum commitments is via the *entanglement* between the commitment and the decommitment; e.g., consider the reveal stage of canonical quantum bit commitments [Yan22]. For this reason, the sender of post-quantum commitments can do the commitment check *by itself* with just the decommitment after the commit stage.[5] In contrast, the sender of quantum commitments cannot do the commitment check by itself with just the decommitment simply because the commitment register has been sent out (thus out of its reach).

A naive try of generalizing collapse binding to general quantum commitments is to allow the malicious sender to have *direct access* of the commitment register even *after* commitments are sent. After some thoughts, it turns out that canonical quantum bit commitments (Definition 4) cannot satisfy thus defined collapse-binding. In greater detail, consider the following attack of an arbitrary canonical quantum bit commitment scheme (Q_0, Q_1)[6]: the cheating sender may prepare the superposition

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

and then sends the commitment register $\mathcal{C}$ to the challenger. Later, the sender sends registers $(\mathcal{M}, \mathcal{R})$ to the challenger to open the commitment; clearly, the challenger will accept with certainty. But the two quantum states of registers $(\mathcal{C}, \mathcal{R}, \mathcal{M})$ corresponding to whether the message register $\mathcal{M}$ is measured or not by the challenger, i.e. $1/2\big(|0\rangle\langle 0| \otimes Q_0 |0\rangle\langle 0| Q_0^\dagger + |1\rangle\langle 1| \otimes Q_1 |0\rangle\langle 0| Q_1^\dagger \big)$ and $1/\sqrt{2}\big(|0\rangle Q_0 |0\rangle + |1\rangle Q_1 |0\rangle \big)$, respectively, are distinguishable. (Note that now the sender can access the commitment register $\mathcal{C}$ directly.) Indeed, to distinguish them, the sender can first uncompute the register pair $(\mathcal{C}, \mathcal{R})$ by performing $Q_b^\dagger$ controlled by the value b stored in the register $\mathcal{M}$, which will disentangle the register pair $(\mathcal{C}, \mathcal{R})$ from the register $\mathcal{M}$. Next, the sender can perform the measurement which distinguishes quantum states $1/2(|0\rangle\langle 0| + |1\rangle\langle 1|)$ and $1/\sqrt{2}(|0\rangle + |1\rangle)$ to finish the job. Actually, in earlier versions of [Yan22] where Yan informally argues that canonical quantum bit commitments cannot be collapse binding, it is this naive definition of collapse binding that is used.

However, after a closer look at the cryptographic applications where commitments are used (e.g. [Yan21, CMSZ21, LMS21]), one will find that it would be sufficient to prove the security against malicious senders of commitments who only have a very limited *oracle access* to the commitment register [GJMZ22]; in particular, malicious senders can only access the commitment register by performing verifications (i.e. binary measurements) that involve the check of opening commitments. After restricting the malicious sender's behavior, it is still possible that quantum commitments may satisfy some collapse-binding property that could be useful in security analysis like its post-quantum counterpart.

Actually, Gunn, Ju, Ma and Zhandry [GJMZ22] and independently Dall'Agnol and Spooner [DS23] have already defined a collapse-binding property for quantum commitments. However, their definition generalizes from Unruh's post-quantum collapse-binding [Unr16b] in a straightforward way without taking into account its direct cryptographic applications. Hence, this definition of collapse-binding is not so useful in cryptographic applications as its post-quantum counterpart. In this paper, we will refer to their definition of collapse-binding as *single-opening collapse-binding* (Definition 7).

In this work, based on the previous study, we propose a new definition of collapse-binding w.r.t. quantum commitments, which seems the "right" one; we hope that it can play the similar role

[5] The malicious sender will save *classical* messages exchanged during the commit stage.

[6] Here, we drop the security parameter for simplicity.

as collapse-binding for post-quantum commitments. Specifically, our definition of collapse-binding can be viewed as an extension of single-opening collapse-binding in two ways:

1. It allows the sender to access the commitment register via the challenger's verification *multiple times* in the experiment that defines collapse-binding. This can also be viewed as allowing the sender to access the commitment register via some *verification oracle*, which is in the same spirit as introducing a (unitary) oracle to swap-binding, obtaining the so-called *oracle swap-binding* [GJMZ22]. Moreover, in our definition we explicitly *quantify* how many verifications the challenger performs, in contrast to oracle swap-binding. This is very important, because in the security analysis of cryptographic applications, the advantage achieved by the malicious sender of commitments will depend on this quantity (Theorem 3).

2. The verifier's verification is more general than just the commitment check. In greater detail, following [FUYZ22, Yan21], the verification will be the "and" of the commitment check and an additional *predicate check*. This will capture most verifications in applications, in particular those in commit-and-open protocols.

Formally, our new definition of collapse binding is referred to Definition 8.

We note that in our try of formalizing collapse-binding above, we mainly focus on its cryptographic applications. The remaining question is: do such quantum collapse-binding commitments really exist based on plausible complexity assumptions? Of course, we hope that the underlying assumption used is as weak as possible, and preferably the minimum one [Yan22, BCQ22].

2.2 An equivalence between collapse-binding and unique-message-binding

Our equivalence theorem (Theorem 1) answers the remaining question raised at the end of last subsection affirmatively and almost optimally.

Our proof for the equivalence combines several previous results and techniques. Specifically, from collapse-binding to unique-message-binding, we adapt the proof in the post-quantum setting [LMS21] in a straightforward way; in particular, we show that single-opening collapse-binding implies unique-message-binding (Lemma 8).

For the other direction, i.e. from unique-message-binding to collapse-binding, we use a technique (Lemma 9) recently developed in [Zha22, CX22, DS23]. We actually prove that *reversible multi-verification* unique-message-binding (Definition 6) implies collapse-binding (Lemma 10), where in the experiment that defines the former the malicious sender of the commitment is allowed to access the commitment register multiple times via the challenger's verification that is similar to the one introduced in the experiment that defines collapse-binding. The word "reversible" means that the sender is also able to reverse its previous computation. We comment that the "polynomial message space" restriction in our equivalence theorem (Theorem 1) comes from the proof of this direction.

Since collapse-binding implies single-opening collapse-binding trivially by definition, for the equivalence we are left to show that the seemingly weaker unique-message-binding implies the reversible multi-verification unique-message-binding, i.e. rounds collapse w.r.t. the unique-message binding (Lemma 7). To this end, we extend a technical lemma proved in [GJMZ22, Lemma 6.8] to our setting, which will be referred to as the *useless oracle* lemma. Basically, this lemma enables us to show that allowing the sender to access the commitment register via any verification oracle will not make the transforming task (i.e. breaking the unique-message binding) significantly easier.

In summary, for our equivalence theorem we prove the following chain of implications: single-opening collapse-binding implies unique-message-binding (Lemma 8), which in turn implies reversible multi-verification unique-message-binding (Lemma 7), which in turn implies collapse-binding (Lemma 8), and which in turn implies single-opening collapse-binding (by definition).

2.3 Generalization

Note that another restriction (besides the polynomial message space) of our equivalence theorem (Theorem 1) is that it only holds w.r.t. *non-interactive* quantum commitments. Though any (interactive) quantum bit commitment scheme can be compiled into a non-interactive one of the canonical form [Yan22], it might be still preferred to use the original scheme in settings where some nice properties would have lost after the compilation. So it would be good if we can extend our equivalence theorem to more general interactive quantum commitments.[7]

However, after a careful examination of our proof, it turns out that we will encounter a new difficulty for a straightforward extension. In more detail, with non-interactive quantum commitments, the sender can do the commitment check by itself *before* sending the commitment register to the receiver. But for interactive quantum commitments, this becomes generally impossible. It is this difference that prevents us from extending proofs of Lemma 7 and 8 to the interactive setting.

In spite of the above, it is very interesting to note that our equivalence theorem extends to *interactive public-coin post-quantum* commitments (also with non-interactive reveal stage) trivially, by recalling that the sender of the commitment can do the commitment check by itself (without interacting with the receiver) w.r.t. general (interactive) public-coin post-quantum commitments.

2.4 Composition

The actual collapse binding property that is really useful in quantum cryptographic applications (Section 10 and Appendix C) is the one that is obtained from our definition by composing it first in *parallel* (Lemma 11) and then in *sequence* (Lemma 12). Intuitively, the parallel composition allows us to first commit to a long message (as long as of polynomial length) and later *partially* open the commitments; the sequential composition allows us to extract information polynomial number of times in the security analysis. Our sequential composition lemma can be viewed as an abstraction of the security analysis where the hybrid argument is applied to handle multiple extractions (e.g. [CMSZ21, LMS21]).

In the post-quantum setting, for the purpose of proving a parallel composition theorem w.r.t. collapse binding, Unruh imposes an additional requirement on the atomic commitment scheme [Unr16b].[8] In contrast, by the virtue of the introduction of the predicate check to the definition of collapse binding (Definition 8), this requirement is not necessary in our setting.

2.5 Application

We first highlight that *both* collapse-binding and unique-message-binding of quantum commitments are indispensable in security analysis of cryptographic constructions: the former enables quantum rewinding with extractions, while the latter ensures the binding in the common sense, i.e. multiple openings of the same commitment should reveal the identical message. Our analysis template (Theorem 3) formalizes these two guarantees in a quantitative way that turns out to be really useful in

[7] Here, by “interactive” quantum commitments we mean those whose commit stage is interactive, whereas the reveal stage is still non-interactive. Note that most commitment schemes in cryptography have non-interactive reveal stage.

[8] Specifically, this additional requirement states that it is possible to find an accepting triple (c, m, u), where c is the commitment, m the message, and u the opening/decommitment.

security analysis. Specifically, it gives a bound on the advantage that can be achieved by the malicious sender of commitments in terms of the unique-message binding error of the atomic scheme, the number of repetitions that the atomic scheme is composed in parallel, as well as the number of verifications performed by the challenger (or equivalently, rounds of the interaction) in the corresponding experiment. It in particular implies that the post-quantum security of commit-and-open protocols can be lifted to the quantum security immediately when one uses (non-interactive) quantum commitments as the drop-in replacement of post-quantum commitments within constructions.

Now let us briefly mention our applications. Combining collapse-binding with the quantum rewinding lemma in [FUYZ22] (Lemma 4), we can prove the computational soundness of Blum's atomic zero-knowledge protocol for the **NP**-complete language Hamiltonian Cycle [Blu86] instantiated with non-interactive quantum bit commitments (Section 10.1); we can even prove argument-of-knowledge (w.r.t. Unruh's definition [Unr12, Unr16b]) for almost the same protocol with a slight modification (Section 10.2). The similar technique can also be used to show argument-of-knowledge of the GMW atomic zero-knowledge protocol for the **NP**-complete language Graph 3-Coloring [GMW91] (Appendix C).

Combining collapse-binding with Unruh's quantum rewinding lemma [Unr12] (Lemma 5), we can show that the parallel composition of yet another variant of Blum's atomic protocol can reduce the knowledge error (w.r.t. Unruh's definition) to be negligible (Section 10.3). Even more, using the recent new quantum rewinding technique (a.k.a. alternative projection) [MW05, CMSZ21, LMS21], the same protocol can also be shown argument-of-knowledge with *guaranteed extraction* (Section 10.4) (whose definition extends from its classical counterpart in a straightforward way [Gol01, Section 4.6]). Unfortunately, it seems that even this argument-of-knowledge (with guaranteed extraction) is still insufficient for the purpose of establishing the quantum security of the Fiat-Shamir construction of constant-round zero-knowledge arguments [FS90]: the trick to handle possibly multiple witnesses in the post-quantum setting [LMS21] does not extend here. We can only prove its quantum security for **UP** (rather than **NP**).

2.6 Constant-round quantum zero-knowledge proofs for NP

Our goal is to show the quantum security of the Goldreich-Kahan construction [GK96] instantiated with canonical quantum bit commitments. Our analysis will be almost the same as its post-quantum counterpart [LMS21], except that now we need to prove a technical lemma (Lemma 13) whose post-quantum counterpart [LMS21, Lemma 13.1] does not extend here in an obvious way.

At a high level, we need to show that quantum indistinguishability is preserved even when the distinghuisher is allowed to access a *purification* of the quantum state to distinghuish in a limited way. Specifically, the distinguisher's access will be given by an oracle which realizes the binary measurement induced by the *projection* on this purification. The reason why we need such a technical lemma is like that in the post-quantum analysis: it will enable us to apply the new quantum rewinding technique [MW05, CMSZ21, LMS21].

However, we will prove this technical lemma in a completely different approach than its post-quantum counterpart. Our proof is inspired by the *hardness-conversion* theorem (Theorem 7), which can be viewed as an reformulation and extension of the *flavor conversion* of canonical quantum bit commitments [HMY22b, Yam22, HMY22a]. In more detail, we observe that the *useless oracle lemma* (Lemma 6) already implies that the oracle access mentioned in the paragraph above does not make the task of *transforming* significantly easier. Then we apply the hardness-conversion theorem to convert the hardness of transforming to that of distinguishing.

For the hardness-conversion theorem itself (Theorem 7), in fact, the flavor-conversion in [HMY22b, Theorem 6.1] already implies one of its direction; the other direction can be proved similarly without much difficulty.

We expect that the hardness-conversion theorem may find more applications in both quantum cryptography and quantum complexity theory in the future.

2.7 A more detailed comparison to [GJMZ22]

Basically, our study of collapse-binding is inspired by that of swap-binding: we encounter similar difficulties in cryptographic applications of quantum commitments, and to overcome which we use similar techniques. This is not a surprise: after all, commitments to classical messages can be viewed as a special case of commitments to quantum states. In the following, let us compare our work with the work [GJMZ22] in more technical detail.

Comparison to their definitions. Recall that for the purpose of allowing the malicious sender to access the commitment in a limited way (which is necessary in the security analysis), our definition of collapse-binding (Definition 8) extends single-opening collapse-binding (Definition 7) by introducing additional interactions between the sender and the challenger in the corresponding experiment; in particular, each round of the interaction consists of a challenger's *verification* that is the "and" of a predicate check and a check of opening the commitment.

One can compare this verification with the *oracle* introduced in [GJMZ22] to extend swap-binding, obtaining *oracle swap-binding*; then one can think this verification as a special *verification oracle*. Though a binding property associated with a more general oracle is stronger than that associated with a verification oracle of some specific form, our definition of collapse-binding is sufficient for many cryptographic applications, in particular commit-and-open protocols. Actually, even in [GJMZ22], only security analysis of commit-and-open protocols are studied; we still do not know any cryptographic application for whose security analysis more general oracles (than verification oracles) are needed. We believe that our definition of collapse-binding is more understandable by cryptographers than that if the verification is replaced with a more general yet abstract oracle (as done in [GJMZ22] for oracle swap-binding).

Another major difference between our definition of collapse-binding and their oracle swap-binding is that in our definition, as aforementioned, we explicitly quantify how many verifications will be performed by the challenger in the corresponding experiment. This quantity is very important in the security analysis. Incorporating it in the definition of collapse-binding will ease cryptographers' job when they try to analyze the security of new commit-and-open protocols where quantum commitments to *classical* messages are used (as will be explained soon). The counterpart of this quantity in the study of (oracle) swap-binding is the number of queries made to the oracle, which, in contrast, is hidden inside the proof of the equivalence between swap-binding and oracle swap-binding [GJMZ22].

Yet another difference is that our definition is w.r.t. *general* (non-interactive) quantum commitments, whereas theirs restrict to quantum commitments of the "canonical" form that is similar to [Yan22].

Comparison in cryptographic applications. For cryptographic applications showcased in this work (Section 10 and Appendix C), similar results can also be derived from results in [GJMZ22] in two different ways (though both of which are not mentioned there).

The first way is to instantiate corresponding commit-and-open protocols with more general (computationally) swap-binding commitments to quantum states and analyze their security (based on swap-binding) in a similar way as that in [GJMZ22]. Such commitments can be based on canonical quantum bit commitments by a folklore construction [GJMZ22]. However, this way is no so appealing since it is an overkill: not only constructions of swap-binding commitments to quantum states are often more complex than those of collapse-binding commitments to classical messages,[9] but also the security analysis based on swap-binding [GJMZ22] is more complex than that based on collapse-binding.

The second and more efficient way, as communicated by [LMS23], is to instantiate corresponding commit-and-open protocols with quantum (computationally) *single-opening* collapse-binding commitments, e.g. canonical quantum bit commitments [DS23, GJMZ22]. For their security, one can prove by using a technical lemma called *admissible oracle lemma* (which will be discussed shortly) in [GJMZ22]. In greater detail, one can similarly introduce a notion called *oracle collapse-binding* that is similar to oracle swap-binding. Then the proof of swap-binding implying oracle swap-binding in [GJMZ22] can be slightly adapted to show that single-opening collapse-binding (Definition 7) implies oracle collapse-binding. Next, one can instantiate the oracle with the verification of the specific form as ours, which just recovers our definition of collapse-binding (Definition 8) that will be really used for the security analysis.

Seeing from above, our definition of collapse-binding is more ready to use (than both single-opening collapse-binding and oracle collapse-binding) by cryptographers in applications. In particular, since we explicitly quantify how many verifications the challenger will perform in the experiment that defines our collapse-binding, it allows us to formalize an *analysis template* (presented in the form of Theorem 3) for the security analysis of different cryptographic applications. This template can be instantiated directly *without* calling any additional abstract technical lemma (such as the admissible oracle lemma). We believe that this will further ease cryptographers' jobs in analyzing new commit-and-open protocols where quantum commitments to classical messages are used in the future.

Comparison to their admissible oracle lemma. In [GJMZ22], an important so-called "admissible oracle lemma" is proved. We would like to compare it with our equivalence theorem (Theorem 1).

For their statements, as aforementioned, the admissible oracle lemma implies an equivalence between single-opening collapse-binding and oracle collapse-binding. Similarly, our equivalence theorem also implies an equivalence between single-opening collapse-binding and collapse-binding; recall the implication chain mentioned in Subsection 2.2.

Comparing the proof of the admissible oracle lemma with our proof of Theorem 1, though looking quite different in many places, their underlying ideas are essentially the same. Specifically, both proofs roughly go in two steps (as presented in [GJMZ22]):

1. The distinghuishing task in equivalent to the transforming (or mapping in [GJMZ22]) task;

2. W.r.t. the transforming task, the very limited oracle access to the commitment register cannot help much.

For the proof of Step 1, they prove Lemma 6.6 in [GJMZ22], whereas we prove Lemma 8 and 10; both proofs use similar previous techniques (e.g. [Unr16b, LMS21, Zha22, CX22, DS23]).

For the proof of Step 2, they prove a key technical lemma, i.e. Lemma 6.8 in [GJMZ22]. Our proof of Step 2, namely, the round-collapse of the unique-message binding (Lemma 7), also relies heavily on a slightly stronger version of their Lemma 6.8, i.e. the useless oracle lemma (Lemma 6).

Despite similarities mentioned above, however, the equivalence revealed in Theorem 1 is not obvious given just the admissible oracle lemma, as far as we can see.

[9] Canonical quantum bit commitment itself is already collapse binding w.r.t. Definition 8.

3 Preliminaries

Notation. Given a binary string $d \in \{0,1\}^l$, we also abuse the notation to use d to denote the subset of $\{1,2,\ldots,l\}$ that consists of indices i's such that $d_i = 1$. Given a binary string $m \in \{0,1\}^l$, we use $m[d]$ to denote the substring obtained from m by projecting it on indices in the subset d.

We will write names of algorithms in sans serif font, e.g. $\mathsf{A}, \mathsf{D}, \mathsf{T}$, which could be either classical or quantum, either ordinary algorithms or interactive ones (used in an interactive protocol).

A *predicate* P over $\{0,1\}^l$ induces a subset of l-bit strings satisfying this predicate; abusing the notation, we also denote this subset by P.

3.1 Quantum preliminaries and notation

Quantum computational model. In this work, we focus on the *unitary* quantum circuit model (refer to textbooks such as [NC00, KSV02]) without loss of generality. Then *efficiently realizable* unitary transformations, or *quantum polynomial-time* (QPT) algorithms, can formalized by a family of quantum circuits $\{Q_\lambda\}_{\lambda \geq 1}$ such that:

1. The size of the quantum circuit Q_λ is bounded by some fixed polynomial of λ.

2. This quantum circuit family can be *uniformly generated*, i.e. there exists a polynomial-time classical algorithm which on input 1^λ, outputs the (classical) description of the quantum circuit Q_λ.

Since any *projective* measurement can be realized by a unitary transformation followed by a measurement in the *computational* basis, we say that a projective measurement is efficiently realizable if its corresponding unitary transformation is efficiently realizable. We say that a *projector* is efficient realizable if its induced binary projective measurement is efficiently realizable.

We will use *non-uniform* QPT algorithms to refer to QPT algorithms that may take quantum advice (as an extra input). Basically, *quantum advice* is a quantum state (which can be thought of pure without loss of generality) that only depend on the parameter λ.

Quantum notation. We use uppercase letters in calligraphic font, such as $\mathcal{A}, \mathcal{B}, \mathcal{X}$, to denote quantum registers. Abusing the notation, we will also use the same notation to denote Hilbert spaces induced by quantum registers; for example, we also use the notation $\mathcal{A}, \mathcal{B}, \mathcal{X}$ to denote the Hilbert spaces induced by quantum registers $\mathcal{A}, \mathcal{B}, \mathcal{X}$, respectively.

We often write quantum registers as the *superscript* of a quantum state or a quantum operation to indicate where this quantum state is stored or on which quantum registers this quantum operation acts, respectively.

When a quantum register $\mathcal{X}$ is composed of multiple (say l) copies of some particular register $\mathcal{A}$, we will write $\mathcal{X} = \mathcal{A}^{\otimes l}$. Given a subset $I \subseteq \{1,2,\ldots,l\}$, we will also use $\mathcal{X}[I]$, or $\mathcal{A}^{\otimes I}$, to denote the system composed of copies of the register $\mathcal{A}$ with indices in the subset I; in particular, the i-th copy of the register $\mathcal{A}$ will be denoted by $\mathcal{A}_i$.

We use Dirac notation $|\cdot\rangle$ such as $|\tau\rangle$ to denote a pure quantum state vector, while just τ to denote a mixed quantum state (or equivalently, density matrix).

We use *sub-normalized* quantum states frequently. Then the squared vector norm of a state vector or the trace of a density matrix can be viewed as giving the success probability of preparing the corresponding quantum states; this turns out to be more convenient to work with in our security analysis.

We write quantum operators in italic font, such as A, D, T. Quantum operators X, Y, Z will be reserved to denote corresponding Pauli matrices. An arbitrary *projector* Π induces a binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$, where Π is associated with the outcome 1, and $\mathbb{1} - \Pi$ associated with the outcome 0. We often use a projector and its induced binary projective measurement interchangeably.

We write such as $\mathsf{A}(x, \mathcal{Y}, \mathcal{Z})$ to indicate that the algorithm A performs on the *classical* input x and *quantum* registers $\mathcal{Y}, \mathcal{Z}$.

A quantum algorithm A is associated with a *unitary* operator denoted by A; we often use them interchangeably. A *distinguisher* is an algorithm which outputs a single classical bit. For a quantum distinguisher D, it induces a *unitary* operator D followed by a measurement of its output qubit $\mathcal{B}$ in the computational basis; the whole operation induces a *projector* given by $\Pi_{\mathsf{D}} = D(|1\rangle \langle 1|)^{\mathcal{B}} D^{\dagger}$.

The distance/closeness between two quantum states. Given two mixed quantum states (or density operators) ρ and σ, their *fidelity* and *trace distance* are denoted by $\mathrm{F}(\rho, \sigma)$ and $\mathrm{TD}(\rho, \sigma)$, respectively, where $\mathrm{F}(\rho, \sigma) \overset{def}{=} \left\| \sqrt{\rho}\sqrt{\sigma} \right\|_1$ and $\mathrm{TD}(\rho, \sigma) \overset{def}{=} 1/2 \left\| \rho - \sigma \right\|_1$. Fidelity and trace distance are two commonly used measures of the closeness/distance between two quantum states. Several facts about them that will be used in this paper (often without explicit reference) are listed as below, all of which can be found in standard textbook (e.g. [NC00, Wat18]).

Fact 1 (Uhlmann's Theorem) *Let ρ, σ be two density matrices of a Hilbert space $\mathcal{X}$. Then*

$$\mathrm{F}(\rho, \sigma) = \max\left\{ |\langle \psi | \phi \rangle| : \text{ unit vectors } |\psi\rangle, |\phi\rangle \in \mathcal{X} \otimes \mathcal{Y} \text{ s.t. } \mathrm{Tr}_{\mathcal{Y}}(|\psi\rangle\langle\psi|) = \rho,\ \mathrm{Tr}_{\mathcal{Y}}(|\phi\rangle\langle\phi|) = \sigma \right\}.$$

Fact 2 (Fuchs-van de Graaf inequalities) *Let ρ, σ be two density matrices of a Hilbert space $\mathcal{X}$. Then*

$$1 - \mathrm{TD}(\rho, \sigma) \leq \mathrm{F}(\rho, \sigma) \leq \sqrt{1 - \mathrm{TD}(\rho, \sigma)^2}.$$

Fact 3 *Tracing out a subsystem will only decrease the trace distance.*

Quantum (in)distinguishability.

Definition 1 (Statistically/computationally indistinguishable) Let $\{\rho_0(\lambda)\}_\lambda$ and $\{\rho_1(\lambda)\}_\lambda$ be two quantum state ensembles. Consider the following experiment between a non-uniform quantum distinghuisher D and a challenger:

1. The challenger chooses $b \overset{\$}{\leftarrow} \{0, 1\}$ uniformly random, and sends the quantum state ρ_b to the distinghuisher.

2. Upon receiving the quantum state from the challenger, the distinghuisher performs a quantum operation and outputs a guess $b' \in \{0, 1\}$.

We say that the distinghuisher wins the experiment if $b' = b$. The *advantage* (than a random guess) achieved by the distinghuisher is given by[10]

$$\left| \Pr_{b \overset{\$}{\leftarrow} \{0,1\}} [\mathsf{D}(\rho_b) = b] - \frac{1}{2} \right|.$$

[10] This definition of advantage differs from the one used in [AAS20, HMY22b] that is given by $|\Pr[\mathsf{D}(\rho_0) = 1] - \Pr[\mathsf{D}(\rho_1) = 1]|$ up to a multiplicative factor two. This constant factor is *not* important in security analysis. Here, we just fix a definition of the distinguishing advantage for a precise statement of lemmas and theorems that will be proved later in this paper. Hence, our statements might differ from the those of similar theorems in [AAS20, HMY22b] up to a multiplicative constant factor.

We say that these two quantum state ensembles are quantum statistically (resp. computationally) *indistinguishable* if any non-uniform QPT distinghuisher D can only win the experiment with negligible advantage. Quantitatively, we say that these two quantum state ensembles are quantum statistically (resp. computationally) *ϵ-indistinguishable* if for any non-uniform resp. QPT distinghuisher D:

$$\Pr_{b \xleftarrow{\$} \{0,1\}} [\mathsf{D}(\rho_b) = b] < \frac{1}{2} + \epsilon.$$

Two quantum rewinding lemmas. We state two simple quantum rewinding lemmas as below, one is suitable for GMW-type zero-knowledge protocols while the other is suitable for Σ-protocols.

The first quantum rewinding lemma is taken from [YWLQ15, FUYZ22].

Lemma 4 (Quantum rewinding w.r.t. GMW-type protocols) *Let $\mathcal{X}$ and $\mathcal{Y}$ be two Hilbert spaces. Unit vector $|\psi\rangle \in \mathcal{X} \otimes \mathcal{Y}$. Efficiently realizable projectors $\Gamma_1, \ldots, \Gamma_k$ perform on the space $\mathcal{X} \otimes \mathcal{Y}$, and efficiently realizable unitary transformations $U_1, \ldots, U_k$ perform on the space $\mathcal{Y}$. If $1/k \cdot \sum_{i=1}^{k} \left\| \Gamma_i (U_i \otimes \mathbb{1}^{\mathcal{X}}) |\psi\rangle \right\|^2 \geq 1 - \eta$, where $0 \leq \eta \leq 1$, then*

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

The second quantum rewinding lemma is taken from [Unr12]

Lemma 5 (Quantum rewinding w.r.t. Σ-protocols) *Let C be a set with $|C| = c$. Let $(\Gamma_i)_{i \in C}$ be orthogonal projectors on a Hilbert space $\mathcal{X}$. Let $|\psi\rangle \in \mathcal{X}$ be a unit vector. Let $V \overset{def}{=} 1/c \cdot \sum_{i \in C} \|\Gamma_i |\psi\rangle\|^2$ and $E \overset{def}{=} 1/c^2 \cdot \sum_{i,j \in C, i \neq j} \|\Gamma_i \Gamma_j |\psi\rangle\|^2$. Then, if $V \geq 1/\sqrt{c}$, we have $E \geq V(V^2 - 1/c)$.*

3.2 Non-interactive quantum commitments to classical messages

Definition 2 (Non-interactive quantum commitments) A generic *non-interactive* quantum commitment scheme $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ consists of two QPT algorithms. The QPT algorithm Commit describes the sender's operations to generate the commitment in the commit stage. The QPT algorithm Verify is run by the receiver to open the commitment later in the reveal stage.

In greater detail, to commit a *classical* message $m \in \{0,1\}^\ell$, the sender first chooses a proper security parameter λ and then runs the QPT algorithm $\mathsf{Commit}(1^\lambda, m)$, which outputs a quantum register pair $(\mathcal{C}, \mathcal{R})$. It then sends the *commitment register* $\mathcal{C}$ to the receiver as the commitment. Later, to open the commitment, the sender sends the classical message m stored in the *message register* $\mathcal{M}$, together with the decommitment register $\mathcal{R}$ to the receiver. Upon receiving them, the receiver will run the QPT algorithm $\mathsf{Verify}(1^\lambda, m, \mathcal{C}, \mathcal{R})$, outputting a single bit indicating whether to accept or not.

The verification algorithm Verify naturally induces a projector V_{com} corresponding to the *commitment check* of the following form:

$$V_{\mathsf{com}} = \sum_{m \in \{0,1\}^\ell} |m\rangle \langle m|^{\mathcal{M}} \otimes \Pi_m^{\mathcal{CR}}, \quad (2)$$

where Π_m is also a projector (that is determined by the revealed message m).

We say that the scheme Com is statistically (resp. computationally) *hiding* if for any messages $m \neq m'$ and computationally unbounded (resp. polynomial-time) non-uniform distinguisher D, the difference

$$\left|\Pr[\mathsf{D}(1^\lambda, \mathcal{C}) = 1 : (\mathcal{C}, \mathcal{R}) \leftarrow \mathsf{Commit}(1^\lambda, m)] - \Pr[\mathsf{D}(1^\lambda, \mathcal{C}) = 1 : (\mathcal{C}, \mathcal{R}) \leftarrow \mathsf{Commit}(1^\lambda, m')]\right| < negl(\lambda).$$

We say that the scheme Com is statistically (resp. computationally) *binding* if it satisfies the unique-message binding property as defined in Definition 3 shortly below.

Remark. Hereafter, when we refer to hiding/binding of commitments without explicitly mentioning it is computational or statistical hiding/binding, one can safely understand it as the computational hiding/binding without loss of generality. This is because proofs in the computational setting also apply to the statistical setting.[11]

The definition of unique-message binding stated as below is adapted from [LMS21].

Definition 3 (Unique-message binding) Let $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ be a generic non-interactive quantum commitment scheme (Definition 2). For a malicious sender $\mathsf{S}^* = (|\tau\rangle, \mathsf{T})$[12] and a security parameter λ, the *unique-message-binding experiment* $\mathsf{UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ proceeds as follows.[13]

$\underline{\mathsf{UniqBindExpt}_{\mathsf{S}^*}(\lambda)}$:

1. S^* receives/prepares a composite system $(\mathcal{C}, \mathcal{R}, \mathcal{M})$ in the quantum state $|\tau\rangle$,[14] and sends this system to the challenger.

2. The challenger performs the binary projective measurement $\{V_{\mathsf{com}}, \mathbb{1} - V_{\mathsf{com}}\}$ on the system $(\mathcal{C}, \mathcal{R}, \mathcal{M})$, where the projector V_{com} is given by Eq. (2). If the outcome is 0, then it aborts and the experiment outputs 0. Otherwise, the challenger returns registers $(\mathcal{R}, \mathcal{M})$ (without the commitment register $\mathcal{C}$) to the sender S^*.

3. S^* measures the message register $\mathcal{M}$ in the computational basis, obtaining the first message m_1.

4. Now S^* will try to open the commitment as another message other than m_1 by running a *transformer* T, which is a QPT algorithm that can be represented by a unitary T, on its own system. Then it sends registers $(\mathcal{R}, \mathcal{M})$ to the challenger.

5. The challenger performs (again) the binary projective measurement $\{V_{\mathsf{com}}, \mathbb{1} - V_{\mathsf{com}}\}$. If the outcome is 0, then it aborts and the experiment outputs 0. Otherwise, the challenger sends registers $(\mathcal{R}, \mathcal{M})$ back to the sender S^*.

6. S^* measures the message register $\mathcal{M}$ to obtain the second message m_2: If $m_2 = m_1$, then it aborts and the experiment outputs 0; otherwise, the experiment outputs 1.

[11] Actually, proofs in the statistical setting are usually much simpler than those in the computational setting, where information-theoretic tools can be used [FUYZ22, AQY21].

[12] Recall that by $|\tau\rangle$ we refer to a pure quantum state, or a state vector. Though a mixed quantum state is more general, in which case we will denote just by τ, restricting to pure states do not lose any generality (by purification). This convention also applies to defining attacks subsequently.

[13] To simplify the notation, we will drop the security parameter λ in the description of the experiment. We will follow this convention in subsequent definitions in this paper.

[14] The sender may also use an additional system as its private workspace; we suppress it here for simplicity.

We say that the quantum commitment scheme Com is *unique-message binding* if for any non-uniform QPT sender S^*,

$$\Pr[\mathsf{UniqBindExpt}_{\mathsf{S}^*}(\lambda) = 1] < negl(\lambda).$$

Quantitatively, we say that the quantum commitment scheme Com is ϵ*-unique-message binding* if for any non-uniform QPT malicious sender S^*,

$$\Pr[\mathsf{UniqBindExpt}_{\mathsf{S}^*}(\lambda) = 1] \leq \epsilon(\lambda).$$

Remark. Compared with the definition of unique-message binding in the post-quantum setting [LMS21], here we let the sender, as opposed to the challenger, measure the message register $\mathcal{M}$. This is because in a try to generalize it to the case where multiple verifications are allowed (Definition 6) later, the challenger does not know when the sender will stop and measure the register $\mathcal{M}$ to obtain another message m_2.

The definition of canonical quantum bit commitments below is taken from [Yan22]. It clearly satisfies the syntax of Definition 2.

Definition 4 (Canonical quantum bit commitment) A canonical (non-interactive) quantum bit commitment scheme is represented by an ensemble of polynomial-time uniformly-generated quantum circuit pair $\{(Q_0(\lambda), Q_1(\lambda))\}_\lambda$ and proceeds as follows:

- 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[15] $(\mathcal{C}, \mathcal{R})$ initialized in all $|0\rangle$'s state. Then the sender sends the *commitment register* $\mathcal{C}$ to the receiver, whose state at this moment is denoted by ρ_b.

- In the subsequent (canonical) *reveal* stage, the sender announces the bit b, and sends the *decommitment register* $\mathcal{R}$ to the receiver. The receiver will first perform $Q_b^\dagger$ on the quantum register pair $(\mathcal{C}, \mathcal{R})$, and then measure each qubit of $(\mathcal{C}, \mathcal{R})$ in the computational basis, accepting if measurement outcomes are *all* 0's.

The hiding (or concealing) and the honest-binding properties of the scheme are defined in the below:

- ϵ-**hiding**. We say that the scheme is statistically (resp. computationally) ϵ-hiding if quantum states ρ_0 and ρ_1 are statistically (resp. computationally) ϵ-indistinguishable (w.r.t. Definition 1).

- ϵ-honest-**binding**. First prepare the quantum register pair $(\mathcal{C}, \mathcal{R})$ in the state $Q_0 |0\rangle$.[16] We say that the scheme is statistically (resp. computationally) ϵ-binding if for any state $|\psi\rangle$ of an auxiliary register $\mathcal{Z}$, and any time-unbounded (resp. QPT) realizable unitary transformation T performing on registers $(\mathcal{R}, \mathcal{Z})$,

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

  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 Inequality (3) becomes

$$\left\| \left(Q_0 |0\rangle \langle 0| Q_0^\dagger\right)^{\mathcal{CR}} T^{\mathcal{RZ}} \left((Q_1 |0\rangle)^{\mathcal{CR}} |\tau\rangle^{\mathcal{Z}} \right) \right\| < \epsilon. \tag{4}$$

[15] Their size will depend on the security parameter λ.

[16] 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 convention throughout this paper.

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

Remark. It is easy to see that the honest-binding property of canonical quantum bit commitments implies the unique-message binding property (Definition 3). In particular, if a canonical quantum bit commitment scheme is ϵ-honest-binding, then it is ϵ^2-unique-message-binding.

3.3 Verifications involving opening quantum commitments

When quantum commitments are used in cryptographic applications, notably quantum zero-knowledge and quantum oblivious transfer, there are usually verifications involving opening quantum commitments within larger protocols. Now let us formalize these verifications for a general study of quantum commitments in applications.

Following [FUYZ22], a general (polynomial-time) verification involving opening quantum commitments includes two checks: a *commitment check* and a *predicate check*. It induces a projector as follows:

$$\Pi = \left(|0\rangle \langle 0|^{\mathcal{A}} \otimes \mathbb{1}^{\mathcal{CRMD}} + |1\rangle \langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}} \right) \cdot P^{\mathcal{MAD}}, \tag{5}$$

where the projector V_{com} is given by Eq. (2) and P is induced by a *classical predicate* that can be checked in polynomial time with the form

$$P = \sum_{(m,a,d)\in P} |m,a,d\rangle \langle m,a,d| \,. \tag{6}$$

Note that projectors P and V_{com} *commute*. Hence, the projector Π is well-defined; that is, it is indeed a projector.

Intuitively, the register $\mathcal{D}$ holds some classical information that will be checked by the predicate P, and the qubit $\mathcal{A}$ indicates whether the commitment will be opened or not. The importance of introducing the qubit $\mathcal{A}$ can be seen when the commitment scheme are composed in parallel in applications, where not all commitments will be opened each time;[17] this will become clear in Section 8.

4 Unique-message binding that admits multiple verifications

In this section, we generalize the definition of unique-message binding (Definition 3) in such a way that the malicious sender and the challenger can exchange multiple messages in the corresponding experiment. It turns out that this generalization is not only necessary for establishing the security of cryptographic constructions using quantum commitments, but also crucial in establishing the equivalence between unique-message binding and collapse binding.

Specifically, we will define two versions of *multi-verification* unique-message binding, where the second version additionally allows the *reversible* computation compared with the first one. Though the second definition is (literally) stronger than the first one,[18] it seems no more useful than the first one in applications. Actually, the reversible version will only be used in establishing the equivalence between unique-message binding and collapse binding later in this paper (Section 7).

The first definition of multi-verification unique-message binding is given as below, which is inspired by [FUYZ22].

[17] Which commitments will be opened depend on the execution of the larger protocol.

[18] They turn out to be actually equivalent, as established later in this paper.

Definition 5 (Multi-verification unique-message binding) Let $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ be a non-interactive quantum commitment scheme w.r.t. Definition 2. Let λ be the security parameter. For a malicious $t(\lambda)$-*verification* sender $\mathsf{S}^* = (|\tau\rangle, P, \mathsf{T})$ of commitments who may interact with the challenger for the verification given by Eq. (5) at most $t(\lambda)$ times,[19] the *multi-verification unique-message-binding experiment* $\mathsf{MV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ between S^* and the challenger is defined as follows.

$\underline{\mathsf{MV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)}$:

1. The malicious sender S^* receives/prepares a joint system $(\mathcal{C}, \mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$ in the quantum state $|\tau\rangle$. It then measures the qubit $\mathcal{A}$ in the computational basis: if the qubit $\mathcal{A}$ contains 0, then it aborts and the experiment outputs 0. Otherwise, it sends the system $(\mathcal{C}, \mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$, together with the description of the predicate P, to the challenger.

2. The challenger performs the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ where the projector Π is given by Eq. (5) with the predicate P plugged in. If the outcome is 0, i.e. the verification fails, then the challenger aborts and the experiment outputs 0. Otherwise, the challenger returns registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$ (but without the commitment register $\mathcal{C}$) to the sender S^*.

3. The sender S^* measures the message register $\mathcal{M}$ in the computational basis, obtaining the first message m_1.

4. Now the sender S^* will try to open the commitment as another message other than m_1 by running an interactive QPT *transformer* T, which may *interact* with the challenger at most t rounds.[20] Specifically, each round of the interaction between the transformer T and the challenger will take the following form:

   (a) The transformer T performs a unitary T on its system, and sends registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$ to the challenger.

   (b) The challenger performs the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ as in Step 2, and then sends registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$ together with the measurement outcome back to the transformer.

5. If the verification in the last round of Step 4 fails, then S^* aborts and the experiment outputs 0; otherwise, S^* measures the qubit $\mathcal{A}$. If the outcome is 0, then S^* aborts and the experiment outputs 0; otherwise, S^* further measures the message register $\mathcal{M}$ to obtain the second message m_2. If $m_2 = m_1$, then S^* aborts and the experiment outputs 0; otherwise, the experiment outputs 1.

We say that the quantum commitment scheme Com is *multi-verification unique-message binding* if for any non-uniform QPT sender S^*,

$$\Pr[\mathsf{MV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda) = 1] = negl(\lambda).$$

Quantitatively, we say that the quantum commitment scheme Com is $t(\lambda)$-*verification* $\epsilon(\lambda)$-*unique-message-binding* if for any $t(\lambda)$-verification non-uniform QPT sender S^*,

$$\Pr[\mathsf{MV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda) = 1] \leq \epsilon(\lambda).$$

[19] In subsequent security analysis, we will assume that the function $t(\cdot) = \omega(1)$ without loss of generality to simplify the asymptotic analysis.

[20] Here, by one round we mean the exchange of two (quantum) messages: one from the sender (who plays the role of the transformer) to the challenger, followed by another message of the opposite direction.

Remark. Note that in Step 4 of the multi-verification unique-message binding experiment, we restrict the sender to use the same unitary T (as induced by the transformer T) and the predicate P in each round; this will simplify the proof of our round-collapse lemma for unique-message binding (Lemma 7). However, one should note that this is actually not a restriction because if in each round i, a different unitary T_i and a different predicate P_i are used, then we can incorporate all T_i's and P_i's into a single unitary T and a single predicate P that additionally depend on a clock register (which counts how many rounds that have passed), respectively. This argument also applies to various definitions of quantum binding properties that allow multiple verifications subsequent in this paper (i.e. Definition 6, 8, 9 and 10). This also justifies that in the subsequent security proofs of cryptographic constructions (Section 10 and Appendix C), we may construct round-dependent unitaries T_i's and predicates P_i's.

Note that in the multi-verification unique-message binding experiment as defined above, the challenger's verifications in Step 4 is *not* reversible. Next, we are going to define a variant of the multi-verification unique-message binding which in particular allows the malicious sender to reverse verifications in Step 4 of the corresponding experiment. In greater detail, compared with the multi-verification unique-message binding experiment, in the experiment of this variant the challenger will *simulate* its verification unitarily and send the qubit containing the outcome back to the sender in each round of Step 4. Clearly, this variant is stronger than the multi-verification unique-message binding by definition.

Definition 6 (Reversible multi-verification unique-message binding) Let $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ be a non-interactive quantum commitment scheme w.r.t. Definition 2. Let λ be the security parameter. For a malicious $t(\lambda)$-*verification* sender $\mathsf{S}^* = (|\tau\rangle, P, \mathsf{T})$ of commitments who may interact with the challenger for the verification given by Eq. (5) at most $t(\lambda)$ times, the *reversible multi-verification unique-message-binding experiment* $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ between S^* and the challenger is defined as follows.

$\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$:

1. The malicious sender S^* receives/prepares a joint system $(\mathcal{C}, \mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$ in the quantum state $|\tau\rangle$. It then measures the qubit $\mathcal{A}$ in the computational basis: if the outcome is 0, then S^* aborts and the experiment outputs 0. Otherwise, it uses a fresh qubit $\mathcal{E}$ initialized in the state $|0\rangle$, and sends the system $(\mathcal{C}, \mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$, together with the description of the predicate P, to the challenger.

2. The challenger *simulates* the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ using the qubit $\mathcal{E}$ in the standard way (i.e. controlled by the measurement outcome, it flips the value of the qubit $\mathcal{E}$), where the projector Π is given by Eq. (5) with the predicate P plugged in. Then the challenger measures the qubit $\mathcal{E}$ in the computational basis. If the outcome is 0, i.e. the verification fails, then the challenger aborts and the experiment outputs 0; otherwise, the challenger returns registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ (but without the commitment register $\mathcal{C}$) to the sender S^*.

3. The sender S^* measures the message register $\mathcal{M}$ in the computational basis, obtaining the first message m_1.

4. Now the sender S^* will try to open the commitment as another message other than m_1 by running an interactive QPT *transformer* T, which may *interact* with the challenger at most

$t-1$ rounds.[21] Each round of the interaction between the transformer T and the challenger will take the following form:

(a) The transformer T performs a unitary T on its system, and then sends registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ to the challenger.

(b) The challenger first simulates the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ as in Step 2 (but never measures the qubit $\mathcal{E}$), and then sends registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ back to the transformer.

5. The transformer T performs the unitary T on its system once more, and re-initializes the qubit $\mathcal{E}$ in the state $|0\rangle$. Then it sends registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ to the challenger.

6. The challenger first simulates the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ as in Step 2 (but no longer measures the qubit $\mathcal{E}$), and then sends registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ back to the sender S^*.

7. The sender S^* measures the qubit $\mathcal{E}$. If it is 0, then S^* aborts and the experiment outputs 0; otherwise, S^* measures the qubit $\mathcal{A}$. If the qubit $\mathcal{A}$ contains 0, then S^* aborts and the experiment outputs 0; otherwise, S^* further measures the message register $\mathcal{M}$ to obtain the second message m_2. If $m_2 = m_1$, then S^* aborts and the experiment outputs 0; otherwise, the experiment outputs 1.

We say that the quantum commitment scheme Com is *reversible multi-verification unique-message binding* if for any non-uniform QPT sender S^*,

$$\Pr[\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda) = 1] = negl(\lambda).$$

Quantitatively, we say that the quantum commitment scheme Com is reversible $t(\lambda)$-*verification* ϵ-*unique-message-binding* if for any $t(\lambda)$-verification non-uniform QPT malicious sender S^*,

$$\Pr[\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda) = 1] \leq \epsilon(\lambda).$$

Remark. Several remarks about the definition above are in order:

1. Similar to Definition 5 (refer to the remark immediately after it), we can assume that the transformer T induces a unitary T that is identical for each round in Step 4 as well as Step 5 of the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$.

2. Step 5 and 6 of the reversible multi-verification unique-message binding experiment can also be viewed as the last round of Step 4 (like the multi-verification unique-message binding experiment), except that reversing any previous verification is explicitly prohibited by requiring use a fresh new qubit $\mathcal{E}$ in the state $|0\rangle$. This guarantees that the message m_2 obtained in Step 7 is indeed a message that is successfully opened by S^*. In comparison, note that in Step 4(a) the qubit $\mathcal{E}$ may *not* be in the state $|0\rangle$ when it is sent to the challenger.

3. Note that the sender in the reversible multi-verification unique-message binding experiment can swap out the content of the qubit $\mathcal{E}$ for a later use upon receiving registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ back from the challenger in Step 4(b).

[21] Added with another round consisting of Step 5 and 6 later, there are t rounds in total at most. Refer to the second remark immediately after the definition for some explanation about why the last round is singled out from Step 4 compared with the multi-verification unique-message binding experiment (Definition 5).

5 A round collapse of unique-message binding

In this section, we prove a round collapse of unique-message binding. Specifically, we show that the unique-message binding (Definition 3) implies the seemingly stronger reversible multi-verification unique-message binding (Definition 6).

Our proof relies heavily on a technical lemma as below, which is an extension and a slight refinement of [GJMZ22, Lemma 6.8] in that the subspace Π_1 now is not necessarily the orthogonal complement of the subspace Π_0 w.r.t. the larger space Π. Its proof is also adapted from the proof in [GJMZ22], which is moved to Appendix A.

Lemma 6 (Useless oracle lemma) *Fix a unitary U, a state $|\tau\rangle$, and three orthogonal projectors Π_0, Π_1, Π_2. Let $\Pi = \Pi_0+\Pi_1+\Pi_2$. Let G be a unitary of the form $G = \Pi_0 G_0+\Pi_1 G_1+\Pi_2 G_2+(\mathbb{1}-\Pi)$, where G_0, G_1, G_2 are unitaries that commute with Π_0, Π_1, Π_2, respectively. Define $\tilde{G_0} = \Pi_0 G_0 + \Pi_2 G_2 + (\mathbb{1} - \Pi_0 - \Pi_2)$ and*

$$\epsilon(t) \overset{def}{=} \max_{\substack{r\in\{0,1\},\\ 0\le q,s\le t}} \|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^q \cdot \Pi_0(\tilde{G_0})^r (U\tilde{G_0})^s \Pi_0 |\tau\rangle \|$$

for all integers $t \ge 0$. Then for all integers $t \ge 0$,

$$\|\Pi_1(UG)^t \Pi_0 |\tau\rangle \| \le 4t^2 \cdot \epsilon(t).$$

The round collapse of unique-message binding is formally stated as the following lemma.

Lemma 7 *Let* $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ *be a non-interactive quantum commitment scheme w.r.t. Definition 2. Then its unique-message binding property (Definition 3) is equivalent to the reversible multi-verification unique-message binding property (Definition 6).*

In particular, given a malicious $t(\lambda)$-verification sender S^* *who can win the reversible multi-verification unique-message binding experiment* $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ *with advantage ϵ, there exists another sender* S' *who can win the unique-message binding experiment* $\mathsf{UniqBindExpt}_{\mathsf{S}'}(\lambda)$ *with advantage at least $\epsilon/(50t^6)$.*

Proof: By definition, the reversible multi-verification unique-message binding (Definition 6) trivially implies the unique-message binding (Definition 3). We only need to show that the seemingly weaker unique-message binding conversely also implies the reversible multi-verification unique-message binding.

According to Definition 6, suppose that $\mathsf{S}^* = (|\tau\rangle, P, \mathsf{T})$ is a malicious $t(\lambda)$-verification sender against the reversible multi-verification unique-message binding property of the quantum commitment scheme $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ with advantage $\epsilon(\lambda)$. Our goal is to construct another sender S' who breaks the unique-message binding property (Definition 3) of the scheme Com with advantage $\epsilon/(50t^6)$.

First consider a running of the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$. We inherit all notations introduced in the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ within Definition 6. We can assume without loss of generality that exact t rounds are executed in Step 4.[22] Suppose that a message m_1 is

[22] This is because if the interaction stops before t rounds, then we can let the transformer T continue interacting with the challenger while performing the identity (i.e. $T_i = \mathbb{1}$) on its system in subsequent rounds until t rounds are reached.

revealed in Step 3. Let p_{m_1} denote the probability that the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ outputs 1. Introduce projectors:

$$\begin{aligned}
W_0 &= (|m_1\rangle\langle m_1|)^{\mathcal{M}} \otimes (|1\rangle\langle 1|)^{\mathcal{A}}, \\
W_1 &= \sum_{m_2 \neq m_1} (|m_1\rangle\langle m_1|)^{\mathcal{M}} \otimes (|1\rangle\langle 1|)^{\mathcal{A}}, \\
W_2 &= \mathbb{1} - W_0 - W_1 = (|0\rangle\langle 0|)^{\mathcal{A}}.
\end{aligned}$$

Note that both projectors W_0 and W_1 commute with the projector Π (given by Eq. (5)):

$$\begin{aligned}
W_0\Pi = \Pi W_0 &= (|1\rangle\langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}}) \cdot \sum_{(m_1,1,d)\in P} |m_1,1,d\rangle\langle m_1,1,d|^{\mathcal{MAD}}, \\
W_1\Pi = \Pi W_1 &= (|1\rangle\langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}}) \cdot \sum_{\substack{m_2\neq m_1,\\ (m_2,1,d)\in P}} |m_2,1,d\rangle\langle m_2,1,d|^{\mathcal{MAD}}.
\end{aligned}$$

Thus, we can introduce more projectors (which are well-defined):

$$\Pi_0 = W_0\Pi, \qquad \Pi_1 = W_1\Pi, \qquad \Pi_2 = W_2\Pi = |0\rangle\langle 0|^{\mathcal{A}} \cdot P^{\mathcal{MAD}}. \tag{7}$$

Note that $\Pi = \Pi_0 + \Pi_1 + \Pi_2$. The challenger's operation in each round of Step 4 of the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ can be represented by the unitary G as follows:

$$G = \Pi^{\mathcal{CRMAD}} \otimes X^{\mathcal{E}} + \mathbb{1} - \Pi^{\mathcal{CRMAD}}. \tag{8}$$

Since the operation Pauli-X performs on a different register (i.e. the qubit $\mathcal{E}$) than Π and W_0, W_1, W_2, it follows that G commutes with all Π_0, Π_1, Π_2.

With our notations, we have

$$p_{m_1} = \|\Pi_1 GT(GT)^{t-1}\Pi_0 G|\tau\rangle\|^2 = \|(\Pi_1 \otimes X)(TG)^t \Pi_0 |\tau\rangle\|^2 = \|\Pi_1 (TG)^t \Pi_0 |\tau\rangle\|^2,$$

where in the second "=" above we use equalities $\Pi_0 G = G\Pi_0$ and $\Pi_1 G = G\Pi_1$. Next, we invoke Lemma 6 in the contrapositive way by doing the following replacements:

- Replace projectors Π and Π_0, Π_1, Π_2 in the statement of Lemma 6 with projectors Π and Π_0, Π_1, Π_2 here given by Eq. (5) and Eq. (7), respectively.
- Replace G_0, G_1, G_2 in the statement of Lemma 6 with Pauli-X performing on the qubit $\mathcal{E}$; thus, the unitary G is given by Eq. (8).
- Replace the unitary U in the statement of Lemma 6 with the unitary T that is induced by the transformer T.

Then one can conclude from Lemma 6 that for some $r \in \{0,1\}$ and $0 \leq q, s \leq t$,

$$\left\|\Pi_1 (T(\Pi_2 G + \mathbb{1} - \Pi_2))^q \cdot \Pi_0 (\tilde{G}_0)^r (T\tilde{G}_0)^s \Pi_0 |\tau\rangle\right\|^2 \geq \frac{p_{m_1}}{17t^4}. \tag{9}$$

Inequality (9) inspires us to construct such a malicious sender $\mathsf{S}' = (\tau', \mathsf{T}')$ against the unique-message binding property (Definition 3) that the experiment $\mathsf{UniqBindExpt}_{\mathsf{S}'}(\lambda)$ proceeds as follows:

1. This step is further divided into several steps:

(a) Using the quantum state $|\tau\rangle$ as used by S^*, S' internally simulates the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ until Step 3 is finished: if S^* aborts before Step 3, then S' also aborts and the experiment outputs 0; otherwise, let m_1 be the message obtained in Step 3.

(b) S' chooses $r \xleftarrow{\$} \{0,1\}$ and $q, s \xleftarrow{\$} \{0,1,\dots,t\}$ uniformly random.

(c) S' performs the operation $\Pi_0(\tilde{G}_0)^r(T\tilde{G}_0)^s$, where the projector Π_0 represents the operation that performs the binary projective measurement $\{\Pi_0, \mathbb{1} - \Pi_0\}$, and simply aborts when the outcome is 0 (in which case the experiment outputs 0). If S' does not abort, then denote the residual (sub-normalized) state of the whole system by $\left|\tau'_{m_1}\right\rangle$; that is,

$$\left|\tau'_{m_1}\right\rangle = \Pi_0(\tilde{G}_0)^r(T\tilde{G}_0)^s\Pi_0\left|\tau\right\rangle. \tag{10}$$

Note the expression of the state $\left|\tau'_{m_1}\right\rangle$ is just a sub-expression of the expression on the l.h.s. of "$\geq$" in Inequality (9). Let $\tau' = \sum_{m_1} |\tau'_{m_1}\rangle\langle\tau'_{m_1}|$.

(d) S' sends registers $(\mathcal{C}, \mathcal{R}, \mathcal{M})$ to the challenger.

2. The challenger performs the binary projective measurement $\{V_{\mathsf{com}}, \mathbb{1} - V_{\mathsf{com}}\}$ on the system $(\mathcal{C}, \mathcal{R}, \mathcal{M})$, where the projector V_{com} is given by Eq. (2). If the outcome is 0, then it aborts and the experiment outputs 0. Otherwise, the challenger returns registers $(\mathcal{R}, \mathcal{M})$ (without the commitment register $\mathcal{C}$) to the sender S'.

3. S' measures the message register $\mathcal{M}$ in the computational basis, obtaining the message m_1 (again).

4. Let the transformer T' be the QPT algorithm which realizes the unitary $T' = ((\Pi_2 G + \mathbb{1} - \Pi_2)T)^q$. S' runs T'. Note that the operation $\Pi_2 G + \mathbb{1} - \Pi_2$ is just a unitary simulation of the binary projective measurement $\{\Pi_2, \mathbb{1} - \Pi_2\}$, where the expression of Π_2 is given in Eq. (7); it can be performed *without* interacting with the challenger. Then S' sends registers $(\mathcal{R}, \mathcal{M})$ to the challenger.

5. The challenger performs the binary projective measurement $\{V_{\mathsf{com}}, \mathbb{1} - V_{\mathsf{com}}\}$. If the outcome is 0, then it aborts and the experiment outputs 0. Otherwise, the challenger sends registers $(\mathcal{R}, \mathcal{M})$ back to the sender S'.

6. S' measures the message register $\mathcal{M}$ to obtain the second message m_2: If $m_2 = m_1$, then it aborts and the experiment outputs 0; otherwise, the experiment outputs 1.

Now we estimate the probability that the experiment $\mathsf{UniqBindExpt}_{\mathsf{S}'}(\lambda)$ outputs 1. Consider a running of the experiment $\mathsf{UniqBindExpt}_{\mathsf{S}'}(\lambda)$. If S' succeeds in preparing the *sub-normalized* state $\left|\tau'_{m_1}\right\rangle$ (given in Eq. (10)), then the commitment check $\{V_{\mathsf{com}}, \mathbb{1} - V_{\mathsf{com}}\}$ by the challenger in Step 2 will pass with certainty, the message m_1 obtained in Step 3 will be identical to the one obtained in Step 1(a). Moreover, the whole system will remain in the state $\left|\tau'_{m_1}\right\rangle$ at the end of Step 3.

Motivated by Inequality (9), we call the state $\left|\tau'_{m_1}\right\rangle$ "good" if

$$\left\|\Pi_1(T(\Pi_2 G + \mathbb{1} - \Pi_2))^q|\tau'_{m_1}\rangle\right\|^2 \geq \frac{p_{m_1}}{17t^4}.$$

Since the triple (q, r, s) is chosen uniformly random, with probability at least $1/(2(t+1)^2)$ the state $\left|\tau'_{m_1}\right\rangle$ will be good. Then it follows that

$$\begin{aligned}
& \Pr[\mathsf{UniqBindExpt}_{\mathsf{S}'}(\lambda) = 1 \wedge m_1 \text{ is revealed in Step 3}] \\
\geq\ & \Pr[\mathsf{UniqBindExpt}_{\mathsf{S}'}(\lambda) = 1 \wedge m_1 \text{ is revealed in Step 3} \mid |\tau'_{m_1}\rangle \text{ is good}] \cdot \Pr[|\tau'_{m_1}\rangle \text{ is good}] \\
\geq\ & \Pr[\mathsf{UniqBindExpt}_{\mathsf{S}'}(\lambda) = 1 \wedge m_1 \text{ is revealed in Step 3} \mid |\tau'_{m_1}\rangle \text{ is good}] \cdot \frac{1}{2(t+1)^2} \\
\geq\ & \left\| \Pi_1 (T(\Pi_2 G + \mathbb{1} - \Pi_2))^q |\tau'_{m_1}\rangle \right\|^2 \cdot \frac{1}{2(t+1)^2} \\
\geq\ & \frac{p_{m_1}}{50t^6}.
\end{aligned}$$

The third "$\geq$" in the above is due to that in the experiment $\mathsf{UniqBindExpt}_{\mathsf{S}'}(\lambda)$, the challenger will only do the commitment check; it will neither do the predicate check nor check whether the qubit $\mathcal{A}$ contains 1 (both of which will be checked by the projector Π_1).

Summing over all possible message m_1's gives

$$\Pr[\mathsf{UniqBindExpt}_{\mathsf{S}'}(\lambda) = 1] \geq \frac{\epsilon}{50t^6},$$

which is also non-negligible when ϵ is.

This finishes the proof of the lemma. ■

6 Collapse binding that admits multiple verifications

In this section, we first adapt existing definitions of collapse binding to be suitable for (non-interactive) quantum commitments w.r.t. Definition 2 in a straightforward way. However, this definition is not so useful as its post-quantum counterpart [Unr16b, Unr16a] in cryptographic applications. To remedy this, we propose a second seemingly stronger definition of collapse binding that is more ready to use in applications. In the next section, we will show that these two definitions are actually equivalent.

The first definition is adapted from [Unr16b, Unr16a, GJMZ22].

Definition 7 (Single-opening collapse binding) Let $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ be a non-interactive quantum commitment scheme w.r.t. Definition 2 and λ the security parameter. For a malicious sender $\mathsf{S}^* = (|\tau\rangle, \mathsf{D})$ of commitments and a challenge bit $b \in \{0, 1\}$, the *single-opening collapse-binding experiment* $\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ proceeds as follows.

$\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$:

1. The malicious sender S^* receives/prepares a joint system $(\mathcal{C}, \mathcal{R}, \mathcal{M})$ in the quantum state $|\tau\rangle$, and sends it to the challenger.

2. The challenger performs the binary projective measurement $\{V_{\mathsf{com}}, \mathbb{1} - V_{\mathsf{com}}\}$, where the projector V_{com} is given by Eq. (2). If the measurement outcome is 0, then the challenger aborts and the experiment outputs a uniformly random bit b'. Otherwise, i.e. the outcome is 1, if further $\underline{b = 1}$, then the challenger measures the register $\mathcal{M}$ in the computational basis; if $b = 0$, then it does nothing. Return registers $(\mathcal{R}, \mathcal{M})$ to the sender S^* (without the commitment register $\mathcal{C}$).

3. Now the sender S^* will try to guess the challenge bit b by running a *distinguisher* D. The measurement (in the computational basis) of a designated qubit gives a bit b' that will be treated as the output of the whole experiment.

We say that the quantum commitment scheme Com is *single-opening collapse binding* if for all non-uniform QPT sender S^*,

$$\Pr_{b \xleftarrow{\$} \{0,1\}} [\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda) = b] \leq \frac{1}{2} + negl(\lambda).$$

Quantitatively, we say that the quantum commitment scheme Com is *single-opening ϵ-collapse-binding* if for any non-uniform QPT malicious sender S^*,

$$\Pr_{b \xleftarrow{\$} \{0,1\}} [\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda) = b] \leq \frac{1}{2} + \epsilon(\lambda).$$

The second definition of collapse binding which allows multiple verifications is inspired by [FUYZ22]. It turns out to be more ready to use in applications.

Definition 8 (Collapse binding) Let $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ be a non-interactive quantum commitment scheme w.r.t. Definition 2 and λ the security parameter. For a malicious $t(\lambda)$-verification sender $\mathsf{S}^* = (|\tau\rangle, P, \mathsf{D})$ of commitments and a challenge bit $b \in \{0,1\}$, where the sender may interact with the challenger at most $t(\lambda)$ rounds, consider the *collapse-binding experiment* $\mathsf{ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ as follows.

$\underline{\mathsf{ColBindExpt}_{\mathsf{S}^*,b}(\lambda)}$:

1. The malicious sender S^* receives/prepares a joint system $(\mathcal{C}, \mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$ in the state $|\tau\rangle$, and measures the qubit $\mathcal{A}$ in the computational basis: if the outcome is 0, then S^* aborts and the experiment outputs a uniformly random bit b'; otherwise, it sends the system $(\mathcal{C}, \mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$, together with the description of the predicate P, to the challenger.

2. The challenger performs the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$, where the expression of the projector Π is given by Eq. (5). If the measurement outcome is 0, then the challenger aborts and the experiment outputs a uniformly random bit b'. Otherwise, i.e. the outcome is 1, if further $\underline{b = 1}$, then the challenger measures the register $\mathcal{M}$ in the computational basis; if $b = 0$, then it does nothing. The challenger returns registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$ to the sender S^* (without the commitment register $\mathcal{C}$).

3. Now the sender S^* will try to guess the challenge bit b by running the *distinguisher* D, which may *interact* with the challenger at most $t(\lambda)$ rounds before outputting a guess $b' \in \{0,1\}$. In particular, each round of the interaction between the distinguisher D and the challenger will take the following form:

   (a) The distinguisher D performs the induced unitary D on its system, and sends registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$ to the challenger.

   (b) The challenger performs the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ that is the same as the one in Step 2, and sends registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$ together with the measurement outcome back to the distinguisher.

4. The distinguisher D performs the unitary D on its system once more and then measures a designated qubit, with the outcome b' that will be treated as the output of the whole experiment.

We say that the quantum commitment scheme Com is *collapse binding* if for all non-uniform QPT sender S^*,

$$\Pr_{b \overset{\$}{\leftarrow} \{0,1\}} [\mathsf{ColBindExpt}_{\mathsf{S}^*,b}(\lambda) = b] \leq \frac{1}{2} + negl(\lambda).$$

Quantitatively, we say that the quantum commitment scheme Com is *$t(\lambda)$-verification $\epsilon(\lambda)$-collapse-binding* if for any $t(\lambda)$-verification non-uniform QPT malicious sender S^*,

$$\Pr_{b \overset{\$}{\leftarrow} \{0,1\}} [\mathsf{ColBindExpt}_{\mathsf{S}^*,b}(\lambda) = b] \leq \frac{1}{2} + \epsilon(\lambda).$$

Remark. Two remarks on the definition above are in order:

1. We highlight that Step 2 and Step 3(b) are almost the identical, except that in Step 2 the message register $\mathcal{M}$ will be measured in case $b = 1$.

2. For the same reason as mentioned in the remark immediately following the definition of reversible multi-verification unique-message binding (Definition 6), we can also assume that here the same unitary D and predicate P are used in each round of Step 3 without any loss of generality.

7 Collapse binding and unique-message binding are equivalent

In this section, we prove that various definitions of collapse binding (Definition 7, 8) and those of unique-message binding (Definition 3, 5, 6) are actually equivalent. This will prove the informal Theorem 1.

Specifically, we will prove that

1. Single-opening collapse binding (Definition 7) implies unique-message binding (Definition 3) (Lemma 8).

2. Reversible multi-verification unique-message binding (Definition 6) implies collapse binding (Definition 8) (Lemma 10).

This will be sufficient for our purpose because:

- Collapse binding (Definition 8) implies single-opening collapse binding (Definition 7) by definition;

- Unique-message binding (Definition 3) is equivalent to reversible multi-verification unique-message binding (Definition 6) (Lemma 7), in turn multi-verification unique message binding (Definition 5) by definition.

7.1 Collapse binding implies unique-message binding

The proof of this lemma is adapted from the one in [LMS21].

Lemma 8 *Let* $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ *be a non-interactive quantum commitment scheme (Definition 2). If the scheme is single-opening collapse binding (Definition 7), then it is also unique-message binding (Definition 3).*

In particular, given a malicious sender S^* *who can win the unique-message binding experiment* $\mathsf{UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ *with advantage* ϵ*, there exists another sender* S' *who can win the single-opening collapse-binding experiment* $\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',b}(\lambda)$ *for a uniformly random bit* b *with advantage at least* $\epsilon/4$*.*

Proof: Suppose that there is a malicious sender $\mathsf{S}^* = (|\tau\rangle, \mathsf{T})$ who can win the unique-message binding experiment $\mathsf{UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ with advantage at least $\epsilon(\lambda)$; that is,

$$\Pr[\mathsf{UniqBindExpt}_{\mathsf{S}^*}(\lambda) = 1] = \epsilon(\lambda).$$

We will construct another sender S' who can win the single-opening collapse binding experiment $\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',b}(\lambda)$ (Definition 7) for a uniformly random challenge bit $b \in \{0,1\}$ with advantage $\epsilon/4$.

Specifically, we construct $\mathsf{S}' = (|\tau'\rangle, \mathsf{D})$ such that the experiment $\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',b}(\lambda)$ proceeds as follows:

1. This step is further divided into several steps:

   (a) S' performs the binary projective measurement $\{V_{\mathsf{com}}, \mathbb{1} - V_{\mathsf{com}}\}$ (Eq. (2)) on the system $(\mathcal{C}, \mathcal{R}, \mathcal{M})$ initialized in the state $|\tau\rangle$ to verify the opening of the commitment. If the opening succeeds, then measure the message register $\mathcal{M}$ to obtain a message m_1; otherwise, it aborts and the experiment outputs a uniformly random bit b'.

   (b) S' appends a fresh qubit $\mathcal{B}$ in the state $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ to its system.

   (c) Controlled by the qubit $\mathcal{B}$, S' performs the unitary T induced by the transformer T. That is, it performs the controlled unitary

   $$\textit{ctrl-}T = |0\rangle\langle 0|^{\mathcal{B}} \otimes \mathbb{1}^{\mathcal{R}\mathcal{M}} + |1\rangle\langle 1|^{\mathcal{B}} \otimes T^{\mathcal{R}\mathcal{M}}. \tag{11}$$

   (d) Controlled by the qubit $\mathcal{B}$, S' performs the binary projective measurement $\{P_{m_1}, \mathbb{1} - P_{m_1}\}$ to verify whether the commitment is opened as some message other than m_1 successfully, where the projector

   $$P_{m_1} = |0\rangle\langle 0|^{\mathcal{B}} \otimes \mathbb{1}^{\mathcal{C}\mathcal{R}\mathcal{M}} + |1\rangle\langle 1|^{\mathcal{B}} \otimes V_{\mathsf{com}}^{\mathcal{C}\mathcal{R}\mathcal{M}} \sum_{m_2 \neq m_1} |m_2\rangle\langle m_2|^{\mathcal{M}}.$$

   If yes, then the (sub-normalized) quantum state at this moment will be treated as the state $|\tau'\rangle$. Otherwise, S' aborts and the experiment outputs a uniformly random bit b'.

   (e) S' sends the system $(\mathcal{C}, \mathcal{R}, \mathcal{M})$ to the challenger.

2. The challenger performs the binary projective measurement $\{V_{\mathsf{com}}, \mathbb{1} - V_{\mathsf{com}}\}$. If the outcome is 0, then it aborts and the experiment outputs a uniformly random bit b'. Otherwise, i.e. the outcome is 1, then measure the register $\mathcal{M}$ in the computational basis if $b = 1$. Return registers $(\mathcal{R}, \mathcal{M})$ to the sender S' (without the commitment register $\mathcal{C}$).

3. After receiving registers $(\mathcal{R}, \mathcal{M})$ back from the challenger, the sender S' calls the distinguisher D which proceeds in two steps:
    (a) Perform the unitary *ctrl-*$T^\dagger$, the inverse of the unitary *ctrl-*T given by Eq. (11);
    (b) Perform the binary projective measurement $\{|+\rangle\langle+|, \mathbb{1} - |+\rangle\langle+|\}$ on the qubit $\mathcal{B}$. Its output b' will be treated as the output of the experiment.

Now let us calculate the probability

$$\Pr[\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',b}(\lambda) = 1 \ \wedge \ \mathsf{S}' \text{ does not abort prematurely}]$$

for both $b = 0$ and $b = 1$.

Denote the (sub-normalized) quantum state of the whole system at the end of Step 1(a) by $|\tau_{m_1}\rangle$ (if S' does not abort); note that the quantum state $|\tau_{m_1}\rangle$ after the renormalization will result in the opening of the commitment as m_1 succeeding with certainty.

The (sub-normalized) quantum state at the end of Step 1(d) (when S' does not abort) is given by

$$\frac{1}{\sqrt{2}} |0\rangle^{\mathcal{B}} |\tau_{m_1}\rangle^{\mathcal{CRM}} + \frac{1}{\sqrt{2}} |1\rangle^{\mathcal{B}} P_{m_1} T |\tau_{m_1}\rangle^{\mathcal{CRM}}. \tag{12}$$

For convenience, we introduce shorthands:

$$\gamma_{m_1} \overset{def}{=} \| \, |\tau_{m_1}\rangle \, \|^2, \qquad \gamma \overset{def}{=} \sum_{m_1} \gamma_{m_1},$$

and

$$\epsilon_{m_1} \overset{def}{=} \left\| P_{m_1} T |\tau_{m_1}\rangle \right\|^2.$$

By the assumption of S^*, we have $\sum_{m_1} \epsilon_{m_1} = \epsilon$, i.e. the advantage that S^* can win the unique-message binding experiment $\mathsf{UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ is ϵ.

We first calculate $\Pr[\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',1}(\lambda) = 1 \wedge \mathsf{S}' \text{ does not abort prematurely}]$. In a running of the experiment $\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',1}(\lambda)$, the challenger will measure the message register $\mathcal{M}$ in Step 2 once the opening of the commitment succeeds. Note that in the superposition (12), the register $\mathcal{M}$ could be an arbitrary superposition of all possible m_2's *other than* m_1 associated with the state $|1\rangle$ of the qubit $\mathcal{B}$. So the measurement of the register $\mathcal{M}$ by the challenger will *collapse* the superposition (12). But either collapsed to the (sub-normalized) quantum states with 0 or 1 in the qubit $\mathcal{B}$, the measurement of the qubit $\mathcal{B}$ in the Hadamard basis $\{|+\rangle\langle+|, \mathbb{1} - |+\rangle\langle+|\}$ on the qubit $\mathcal{B}$ will output 1 with probability exactly 1/2. Thus,

$$\Pr[\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',1}(\lambda) = 1 \ \wedge \ \mathsf{S}' \text{ does not abort prematurely}] = \frac{1}{2} \sum_{m_1} \frac{\gamma_{m_1} + \epsilon_{m_1}}{2} = \frac{\gamma + \epsilon}{4}.$$

We next calculate $\Pr[\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',0}(\lambda) = 1 \ \wedge \ \mathsf{S}' \text{ does not abort prematurely}]$. In the experiment $\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',0}(\lambda)$, the message register $\mathcal{M}$ will not be measured by the challenger in Step 2 even the opening of the commitment succeeds. Then the state of the whole system before performing the binary projective measurement $\{|+\rangle\langle+|, \mathbb{1} - |+\rangle\langle+|\}$ by the distinguisher D (in Step 3(b)) is

$$\frac{1}{\sqrt{2}} |0\rangle^{\mathcal{B}} |\tau_{m_1}\rangle^{\mathcal{CRM}} + \frac{1}{\sqrt{2}} |1\rangle^{\mathcal{B}} T^\dagger P_{m_1} T |\tau_{m_1}\rangle^{\mathcal{CRM}},$$

which can be rewritten as:

$$\begin{aligned} & \frac{1}{\sqrt{2}} \frac{|+\rangle + |-\rangle}{\sqrt{2}} |\tau_{m_1}\rangle + \frac{1}{\sqrt{2}} \frac{|+\rangle - |-\rangle}{\sqrt{2}} T^\dagger P_{m_1} T |\tau_{m_1}\rangle \\ = \ & \frac{1}{2}\Big(|+\rangle \left(|\tau_{m_1}\rangle + T^\dagger P_{m_1} T |\tau_{m_1}\rangle \right) + |-\rangle \left(|\tau_{m_1}\rangle - T^\dagger P_{m_1} T |\tau_{m_1}\rangle \right) \Big). \end{aligned}$$

Thus, the binary projective measurement $\{|+\rangle\langle+|, \mathbb{1} - |+\rangle\langle+|\}$ by the distinguisher D in Step 3(b) will output 1 with probability

$$\frac{1}{4} \big\| \, |\tau_{m_1}\rangle + T^\dagger P_{m_1} T |\tau_{m_1}\rangle \, \big\|^2 = \frac{\| |\tau_1\rangle \|^2 + 3 \, \| P_{m_1} T |\tau_{m_1}\rangle \|^2}{4} = \frac{\gamma_{m_1} + 3\epsilon_{m_1}}{4}.$$

Summing over all m_1 gives

$$\Pr[\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',0}(\lambda) = 1 \ \wedge \ \mathsf{S}' \text{ does not abort prematurely}] = \frac{\gamma + 3\epsilon}{4}.$$

Since when S' aborts prematurely, both experiments $\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',0}(\lambda)$ and $\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',1}(\lambda)$ will output a uniformly random bit b'. It follows that

$$\Pr[\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',0}(\lambda) = 1] - \Pr[\mathsf{SO\text{-}ColBindExpt}_{\mathsf{S}',1}(\lambda) = 1] = \frac{\gamma + 3\epsilon}{4} - \frac{\gamma + \epsilon}{4} = \frac{\epsilon}{2}.$$

This means that the malicious sender S' can achieve the advantage $\epsilon/4$, which is also non-negligible when ϵ is. But this contradicts the single-opening collapse-binding property of the scheme Com.

This finishes the proof of the lemma. ■

7.2 Unique-message binding implies collapse binding

Our proof will rely on the following technical lemma, which is taken from [DS23, Claim 3.5]; similar technical lemmas were proved even earlier [CX22, Zha22].

Lemma 9 *Let Π_{D} be the projector corresponding to a distinguisher D, $\mathsf{M} = (\Pi_i)_{i\in[N]}$ be a projective submeasurement (meaning Π_i's are projectors and $\sum_i \Pi_i \leq \mathbb{1}$) and ρ be a (possibly sub-normalized) quantum state such that $\sum_i \mathrm{Tr}(\Pi_i \rho) = \mathrm{Tr}(\rho)$. Then*

$$\sum_j \sum_{i \neq j} \mathrm{Tr}(\Pi_i \Pi_{\mathsf{D}} \Pi_j \rho \Pi_j \Pi_{\mathsf{D}}) \geq \frac{\mathrm{Tr}(\Pi_{\mathsf{D}}(\rho - \mathsf{M}(\rho)))^2}{N \cdot \mathrm{Tr}(\rho)}.$$

Remark. In order that the r.h.s. of the inequality above is non-negligible, N has to be polynomially bounded. The requirement in Lemma 10 and Theorem 1 that the dimension of the message space has to be polynomially bounded is rooted in this restriction of the technical lemma above.

Lemma 10 *Let $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ be a non-interactive quantum commitment scheme (Definition 2) with the dimension of the message space N that is bounded by some polynomial of the security parameter λ. If the scheme Com is reversible multi-verification unique-message binding (Definition 6), then it is also collapse binding (Definition 8).*

In particular, given a $t(\lambda)$-verification malicious sender S^* who can win the collapse-binding experiment $\mathsf{ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ for a uniformly random bit b with advantage ϵ, then there exists another $(2t(\lambda)+1)$-verification malicious sender S' who can win the reversible multi-verification unique-message binding experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$ with advantage $8\epsilon^2/N$.

Proof: Suppose that $\mathsf{S}^* = (|\tau\rangle, P, \mathsf{D})$ is a t-verification malicious sender who can win the collapse-binding experiment (Definition 8) with advantage ϵ; that is,

$$\Pr_{b \xleftarrow{\$} \{0,1\}} [\mathsf{ColBindExpt}_{\mathsf{S}^*,b}(\lambda) = b] \geq \frac{1}{2} + \epsilon(\lambda).$$

We can assume without loss of generality that in the experiment $\mathsf{ColBindExpt}_{\mathsf{S}^*,b}$, for both $b = 0$ and 1, S^* interacts with the challenger in exactly t rounds. Given access to S^*, we will construct another sender $\mathsf{S}' = (\tau', P, \mathsf{T})$ who (using the same predicate P as S^*) can win the reversible multi-verification unique-message binding experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}^*}(\lambda)$ (Definition 6) with advantage $\Omega(\epsilon^2/N)$;[23] that is,

$$\Pr[\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda) = 1] \geq \frac{8\epsilon^2}{N}.$$

Specifically, we construct the malicious sender $\mathsf{S}' = (\tau', P, \mathsf{T})$ such that the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$ proceeds as follows:

1. This step is further divided into two steps:

   (a) S' internally simulates the collapse-binding experiment $\mathsf{ColBindExpt}_{\mathsf{S}^*,0}(\lambda)$ until the end of Step 2, using the same auxiliary input quantum state $|\tau\rangle$ and the predicate P as used by S^*: If either S^* aborts in Step 1 or the challenger aborts in Step 2, then S' aborts and the experiment outputs 0. Otherwise, the resulting (sub-normalized) *mixed* quantum state will be treated as the auxiliary input quantum state τ' used by the attack S'.

   (b) S' proceeds as described by Step 1 of reversible multi-verification unique-message-binding experiments (Definition 6). Namely, it uses a fresh qubit $\mathcal{E}$ initialized in the state $|0\rangle$, and sends the system $(\mathcal{C}, \mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$, together with the description of the predicate P, to the challenger.[24]

2. The challenger proceeds as described by Step 2 of reversible multi-verification unique-message-binding experiments. Namely, the challenger *simulates* the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ using the qubit $\mathcal{E}$ in the standard way, where the projector Π is given by Eq. (5) with the predicate P plugged in. If the outcome is 0, i.e. the verification fails, then it aborts and the experiment outputs 0; otherwise, the challenger returns registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ (but without the commitment register $\mathcal{C}$) to the sender S'.

3. The sender S' measures the message register $\mathcal{M}$ in the computational basis, obtaining the first message m_1.

4. This step is further divided into three steps:

   (a) S' interacts with the challenger to simulate the interaction between S^* and the corresponding challenger as described in Step 3 of the collapse-binding experiment $\mathsf{ColBindExpt}_{\mathsf{S}^*,0}(\lambda)$. That is, the unitary T performed in each round induced by the transformer T is just the unitary D induced by the distinguisher D used by the sender S^* in the collapse-binding experiment $\mathsf{ColBindExpt}_{\mathsf{S}^*,0}(\lambda)$, with the only difference that now the sender S' and the

[23] Here, we use the notation τ' rather than $|\tau'\rangle$ to indicate that it could be a *mixed* quantum state.

[24] By the construction of the (sub-normalized) quantum state τ', now there is actually no need for the sender S' to measure the qubit A and check the opening of the commitment.

challenger will simulate the challenger's verification in the experiment $\mathsf{ColBindExpt}_{\mathsf{S}^*,0}(\lambda)$ *unitarily* in the standard way using additional qubits $\mathcal{E}_i$'s and the qubit $\mathcal{E}$. Detail follows. Specifically, for the simulation in each round, a fresh new qubit initialized in the state $|0\rangle$ will be used to record the challenger's verification outcome; in the i-th round ($1 \leq i \leq t$), the qubit used will be denoted by $\mathcal{E}_i$. After applying the unitary D, the sender S' will swap the content of the qubit $\mathcal{E}_i$ and $\mathcal{E}$ before sending registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ to the challenger. Then the challenger will first simulate the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ as in Step 2, and then send registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ back to the sender S'. Upon receiving registers back from the challenger, the sender S' will swap the content of the qubit $\mathcal{E}_i$ and $\mathcal{E}$ once more.

(b) The transformer T simulates Step 4 of the experiment $\mathsf{ColBindExpt}_{\mathsf{S}^*,0}(\lambda)$ unitarily, i.e. first performs the unitary D and then simulate measuring a designated output qubit unitarily.

(c) S' first performs the unitary $D^\dagger$ to reverse part of the computation as described in Step 4(b); measuring the designated qubit will *not* be reversed. Then it reverses the whole computation as described in Step 4(a).

5. The transformer T's operation in this step will be the identity. Then it re-initializes the qubit $\mathcal{E}$ in the state $|0\rangle$, and sends registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ to the challenger.

6. The challenger first simulates the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ as in Step 2, and then sends registers $(\mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D}, \mathcal{E})$ back to the sender S'.

7. S' proceeds as described in Step 7 of reversible multi-verification unique-message-binding experiments. That is, it measures qubits $\mathcal{A}, \mathcal{E}$, and measures the message register $\mathcal{M}$ to obtain the second message m_2: If either of qubits $\mathcal{A}$ or $\mathcal{E}$ contain 0, or $m_2 = m_1$, then S' aborts and the experiment outputs 0; otherwise, the experiment outputs 1.

In the experiment above, since both Step 4(a) and 4(c) take t rounds, plus an additional round taking in Step 5 and 6, the malicious sender S' interacts with the challenger $2t + 1$ rounds in total. We are next to prove that the malicious sender S' can win the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$ with advantage at least $8\epsilon^2/N$.

By our construction of S', the system $(\mathcal{C}, \mathcal{R}, \mathcal{M}, \mathcal{A}, \mathcal{D})$ will remain in the (sub-normalized) mixed quantum state τ' at the end of Step 2 of the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$. Step 4 of the experiment actually implements the binary projective measurement $\{\Pi_{\mathsf{D}}, \mathbb{1} - \Pi_{\mathsf{D}}\}$ that is induced by the distinguisher D. Let M denote the submeasurement $\{\Pi_m\}_{m \in \{1,2,\ldots,N\}}$, where the projector

$$\Pi_m = \Pi \cdot |m\rangle\langle m|^{\mathcal{M}} \cdot |1\rangle\langle 1|^{\mathcal{A}}. \tag{13}$$

By the assumption that the malicious sender S^* can win the collapse-binding experiment $\mathsf{ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ where $b \overset{\$}{\leftarrow} \{0, 1\}$ with advantage ϵ, we have:

$$|\mathrm{Tr}(\Pi_{\mathsf{D}}(\tau' - \mathsf{M}(\tau')))| \geq 2\epsilon, \qquad |\mathrm{Tr}((\mathbb{1} - \Pi_{\mathsf{D}})(\tau' - \mathsf{M}(\tau')))| \geq 2\epsilon.$$

This is because conditioned on the experiment $\mathsf{ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ aborting prematurely in Step 1 or 2, the distinghuishing advantage will be 0. Since $\sum_m \mathrm{Tr}(\Pi_m \tau') = \mathrm{Tr}(\tau')$, it follows from Lemma 9 that

$$\sum_{m_1} \sum_{m_2 \neq m_1} \mathrm{Tr}(\Pi_{m_2} \Pi_{\mathsf{D}} \Pi_{m_1} \tau' \Pi_{m_1} \Pi_{\mathsf{D}}) \geq \frac{\mathrm{Tr}(\Pi_{\mathsf{D}}(\tau' - \mathsf{M}(\tau')))^2}{N \cdot \mathrm{Tr}(\tau')} \geq \frac{4\epsilon^2}{N}.$$

We can prove a similar inequality as above if we replace the projector Π_{D} with $\mathbb{1} - \Pi_{\mathsf{D}}$. Note that the probability that the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$ outputting 1 is exactly given by

$$\sum_{m_1} \sum_{m_2 \neq m_1} \mathrm{Tr}(\Pi_{m_2} \Pi_{\mathsf{D}} \Pi_{m_1} \tau' \Pi_{m_1} \Pi_{\mathsf{D}}) + \sum_{m_1} \sum_{m_2 \neq m_1} \mathrm{Tr}(\Pi_{m_2} (\mathbb{1} - \Pi_{\mathsf{D}}) \Pi_{m_1} \tau' \Pi_{m_1} (\mathbb{1} - \Pi_{\mathsf{D}})).$$

This implies that S' can win the experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$ with advantage at least $8\epsilon^2/N$, which is non-negligible when $N = O(\mathrm{poly}(\lambda))$. But this breaks the reversible multi-verification unique-message binding property (Definition 6) of the scheme Com.

This finishes the proof of the lemma. ■

8 The parallel composition of collapse binding

In applications, we often compose a commitment scheme in parallel to commit a long message. In this section, we show that parallelized non-interactive quantum commitment schemes satisfy a collapse binding property that extends naturally from that of the atomic scheme.

Definition 9 (Parallel collapse-binding) Let $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ be a non-interactive quantum commitment scheme w.r.t. Definition 2. Consider the *parallel collapse-binding experiment* $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ defined as below, where the challenge bit $b \in \{0, 1\}$ and the malicious sender $\mathsf{S}^* = (|\tau\rangle, P, \mathsf{D})$ is a non-uniform QPT interactive algorithm. We say that the sender S^* is $l(\lambda)$-fold,[25] $t(\lambda)$-verification, if it attacks l folds of the scheme Com running in parallel by interacting with the challenger at most $t(\lambda)$ rounds.

$\underline{\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)}$:

1. The malicious sender S^* receives/prepares a joint system $(\mathcal{C}^{\otimes l}, \mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D})$ in the state $|\tau\rangle$, and sends the system $(\mathcal{C}^{\otimes l}, \mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D})$, together with the description of the predicate P to the challenger.

2. The challenger performs the binary projective measurement $\{\Pi_{\mathsf{par}}, \mathbb{1} - \Pi_{\mathsf{par}}\}$, with

$$\Pi_{\mathsf{par}} \overset{def}{=} \left(|0\rangle \langle 0|^{\mathcal{A}} \otimes \mathbb{1}^{\mathcal{CRM}} + |1\rangle \langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}} \right)^{\otimes l} \cdot P^{\mathcal{M}^{\otimes l} \mathcal{A}^{\otimes l} \mathcal{D}}, \tag{14}$$

   where the projector V_{com} is given by Eq. (2). If the measurement outcome is 0, then the challenger aborts and the experiment outputs a uniformly random bit b'. Otherwise, if the outcome is 1 and $\underline{b = 1}$, then the challenger first measures all l copies of the qubit $\mathcal{A}$ in the computational basis. Let $I \subseteq \{1, 2, \ldots, l\}$ be the subset consisting of all indices i's such that the measurement outcomes of the qubit $\mathcal{A}_i$ is 1.

   > Two *restrictions* on the state of qubits $\mathcal{A}^{\otimes l}$:[26] First, we require that the value of qubits $\mathcal{A}^{\otimes l}$ is *deterministic*; that is, measuring qubits $\mathcal{A}^{\otimes l}$ will cause *no* collapse of the quantum state. We point out that this restriction can be circumvented in many interesting scenarios, as remarked subsequent to the definition. Second, we

[25] In subsequent security analysis, we will assume that the function $l(\cdot) = \omega(1)$ without loss of generality to simplify the asymptotic analysis.

[26] These restrictions are imposed for a technical reason: it will be crucial for proving our parallel and sequential composition lemmas (Lemma 11, 12) later.

additionally require that $|I|$ is efficiently computable and at least 1 (i.e. the subset I is non-empty).[27] We also point out that this condition is often automatically satisfied in applications.

The challenger then measures message registers $\mathcal{M}_i$'s in the computational basis if the qubit $\mathcal{A}_i$ contains 1. It returns registers $(\mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D})$ to the sender S^* (without commitment registers $\mathcal{C}^{\otimes l}$).

3. Now the sender S^* will try to guess the challenge bit b by running the *distinguisher* D, which may *interact* with the challenger at most $t(\lambda)$ rounds before outputting a guess $b' \in \{0,1\}$. In particular, each round of the interaction between the distinguisher D and the challenger will take the following form:
   (a) The distinguisher D performs a unitary D on its system, and sends registers $(\mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D})$ to the challenger.
   (b) The challenger performs the binary projective measurement $\{\Pi_{\mathsf{par}}, \mathbb{1} - \Pi_{\mathsf{par}}\}$ that is the same as the one in Step 2, and sends registers $(\mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D})$ together with the measurement outcome back to the distinguisher.
4. The distinguisher D performs the unitary D on its system once more and then measures a designated qubit, with the outcome b' that will be treated as the output of the whole experiment.

We say that the quantum commitment scheme Com is *parallel collapse-binding* if for all non-uniform QPT sender S^*,

$$\Pr_{b \overset{\$}{\leftarrow} \{0,1\}} [\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda) = b] \leq \frac{1}{2} + negl(\lambda).$$

Quantitatively, we say that the quantum commitment scheme Com is $l(\lambda)$*-fold,* $t(\lambda)$*-verification,* $\epsilon(\lambda)$*-parallel-collapse-binding* if for any $l(\lambda)$-fold, $t(\lambda)$-verification non-uniform QPT malicious sender S^*,

$$\Pr_{b \overset{\$}{\leftarrow} \{0,1\}} [\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda) = b] \leq \frac{1}{2} + \epsilon(\lambda).$$

Remark. We have two remarks on the first restriction on the state of qubits $\mathcal{A}^{\otimes l}$ in the definition above.

1. A typical scenario in cryptographic applications where this restriction is satisfied is that *all* commitments will be opened. This is exactly the case where the parallel composition of collapse binding is studied in previous literature [Unr16b, GJMZ22].

2. This restriction can be circumvented by a simple trick following Unruh [Unr12, Unr16b]. Specifically, we can let the sender of commitments additionally commit to the value of qubits $\mathcal{A}^{\otimes l}$. Then conditioned on tis commitment is opened successfully (whose check can be incorporated in to Π_{par}), whether the challenger measuring qubits $\mathcal{A}^{\otimes l}$ or not will be undetectable seeing from the viewpoint of the sender (by the virtue of the collapse-binding property of the commitment). And this will be sufficient for proving the parallel composition lemma (Lemma 11); refer to the remark subsequent to the proof of this lemma.

[27] Alternatively, this restriction can be incorporated into the predicate P: if the size of the subset I is not equal to some efficiently computable value, then the challenger will abort.

Lemma 11 (Parallel composition) *Let* $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ *be a non-interactive quantum commitment scheme w.r.t. Definition 2. If this scheme is collapse binding w.r.t. Definition 8, then it is also parallel collapse-binding w.r.t. Definition 9.*

In particular, if there is a malicious $l(\lambda)$*-fold,* $t(\lambda)$*-verification sender* S^* *who can win the parallel collapse-binding experiment* $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ *(for a uniformly random bit* b*) with advantage* $\epsilon(\lambda)$*, then there exists another malicious* $t(\lambda)$*-verification sender* S' *who can win the collapse-binding experiment* $\mathsf{ColBindExpt}_{\mathsf{S}',b}(\lambda)$ *(for a uniformly random bit* b*) with advantage at least* ϵ/l*.*

Proof: Suppose that $\mathsf{S}^* = (|\tau\rangle, P, \mathsf{D})$ is a malicious $l(\lambda)$-fold, $t(\lambda)$-verification sender who can win the parallel collapse-binding experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ (for a uniformly random bit b) with advantage $\epsilon(\lambda)$. Let $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,1/2}(\lambda)$ denote the experiment that is almost identical to the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,0}(\lambda)$, except that the challenger also measures qubits $\mathcal{A}^{\otimes l}$ (but not $\mathcal{M}^{\otimes l}$ as opposed to the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$; this is why we use the subscript $1/2$ for its notation) in Step 2.

Without loss of generality, assume that S^* will always cause the challenger to accept for its verification $\{\Pi_{\mathsf{par}}, \mathbb{1} - \Pi_{\mathsf{par}}\}$ in Step 2 of the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ (for both $b = 0$ and 1). This is because S^* can do this verification by itself in Step 1; we can let it simply abort (and output a uniformly random bit b') without affecting its distinghuishing advantage.

Due to the restriction on the state of qubits $\mathcal{A}^{\otimes l}$ (recall Definition 9), it follows that the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,0}(\lambda)$ and the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,1/2}(\lambda)$ are equivalent. Thus, the sender S^* can distinghuish the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,1/2}(\lambda)$ and the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$ with advantage at least ϵ.

Now we construct another malicious $t(\lambda)$-verification sender $\mathsf{S}' = (\tau', P', \mathsf{D}')$ such that the collapse-binding experiment $\mathsf{ColBindExpt}_{\mathsf{S}',b}(\lambda)$ proceeds as follows:

1. This step is further divided into several steps:

   (a) The malicious sender S' simulates S^* to receive a joint system $(\mathcal{C}^{\otimes l}, \mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D})$ in the state $|\tau\rangle$, and measures all l copies of the qubit $\mathcal{A}$ in the computational basis. Denote by I the subset of $\{1, 2, \ldots, l\}$ consisting of all indices i's such that the measurement outcome of the qubit $\mathcal{A}_i$ is 1.

   (b) S' chooses an index $i \xleftarrow{\$} I$.

   (c) S' performs the binary projective measurement $\left\{\Pi'_{\mathsf{par}}, \mathbb{1} - \Pi'_{\mathsf{par}}\right\}$, where the projector Π'_{par} corresponds to the verification of the opening of commitments with indices in $I \setminus \{i\}$. That is,

   $$\Pi'_{\mathsf{par}} \overset{def}{=} \big(|0\rangle \langle 0|^{\mathcal{A}} \otimes \mathbb{1}^{\mathcal{CRM}} + |1\rangle \langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}} \big)^{\otimes (l-1)}. \tag{15}$$

   The measurement outcome will be recorded in a fresh qubit $\mathcal{F}$.

   (d) If the qubit $\mathcal{F}$ contains 0, then S' aborts and the experiment outputs a uniformly random bit b'. Otherwise, S' measures copies of the message register $\mathcal{M}$ with indices in I and whose values are less than i. The resulting (sub-normalized) quantum state of the whole system will be denoted by τ'.

   (e) S' sets the predicate P' to be equal to the predicate P *anded* with the value stored in the qubit $\mathcal{F}$.

   (f) S' sends registers $(\mathcal{C}_i, \mathcal{R}_i, \mathcal{M}_i, \mathcal{A}_i)$, registers $(\mathcal{D}, \mathcal{F})$, together with the description of the predicate P' to the challenger.

2. The challenger performs the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ on the system $(\mathcal{C}_i, \mathcal{R}_i, \mathcal{M}_i, \mathcal{A}_i, \mathcal{D}, \mathcal{F})$, where the expression of the projector Π is given by Eq. (5), with the predicate P' plugged in and the composite system $(\mathcal{D}, \mathcal{F})$ here identified as the register $\mathcal{D}$ in Eq. (5). If the measurement outcome is 0, then the challenger aborts and the experiment outputs a uniformly random bit b'. Otherwise, if the outcome is 1 and $\underline{b = 1}$, then the challenger measures the register $\mathcal{M}_i$ in the computational basis. It then returns registers $(\mathcal{R}_i, \mathcal{M}_i, \mathcal{A}_i, \mathcal{D}, \mathcal{F})$ to the sender S' (without the commitment register $\mathcal{C}_i$), who will flip the value of the qubit $\mathcal{F}$ to set it back to the state $|0\rangle$.[28]

3. Now the sender S' will try to guess the challenge bit b by running the distinguisher D used by the sender S^* as a subroutine, which may *interact* with the challenger at most $t(\lambda)$ rounds before outputting a guess $b' \in \{0, 1\}$. In particular, each round of the interaction between the distinguisher D' and the challenger will take the following form:

   (a) The distinguisher D' first performs the unitary D induced by the distinguisher D on its system, and then *simulates* the binary projective measurement $\left\{\Pi'_{\mathsf{par}}, \mathbb{1} - \Pi'_{\mathsf{par}}\right\}$ unitarily in the standard way, using the qubit $\mathcal{F}$ to record the measurement outcome. It sends registers $(\mathcal{R}_i, \mathcal{M}_i, \mathcal{A}_i, \mathcal{D}, \mathcal{F})$ to the challenger.

   (b) The challenger performs the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ that is the same as the one in Step 2, and sends registers $(\mathcal{R}_i, \mathcal{M}_i, \mathcal{A}_i, \mathcal{D}, \mathcal{F})$ together with the measurement outcome back to the distinguisher. Upon receiving them, the distinghuisher will *uncompute* the qubit $\mathcal{F}$, i.e. performing the inverse of the unitary simulation of the binary projective measurement $\left\{\Pi'_{\mathsf{par}}, \mathbb{1} - \Pi'_{\mathsf{par}}\right\}$ as done in Step 3(a).[29]

4. The distinguisher D' performs the unitary D on its system once more and then measures a designated qubit, with the outcome b' that will be treated as the output of the whole experiment.

Next, we will use a standard hybrid argument to show that the malicious sender S' can win the collapse-binding experiment $\mathsf{ColBindExpt}_{\mathsf{S}',b}(\lambda)$, for a uniformly chosen bit b, with advantage at least ϵ/l.

Consider the parallel collapse-binding experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,0}(\lambda)$ when an arbitrary subset I of $\{1, 2, \ldots, l\}$ is obtained in Step 1, which consists of all indices with which the measurement outcome of corresponding copies of the qubit $\mathcal{A}$ is 1. Denote by $|\tau'_I\rangle$ the corresponding (subnormalized) quantum state at the end of Step 1, with the corresponding malicious sender denoted by S'_I; thus, $\tau' = \sum_I |\tau'_I\rangle \langle \tau'_I|$.[30]

Order indices in I in the increasing order. We construct the i-th hybrid $\mathsf{H}_i(\lambda)$, for $i = 0, 1, \ldots |I|$, by modifying the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*_I,1/2}(\lambda)$ in the following way: if the verification $\{\Pi, \mathbb{1} - \Pi\}$ succeeds in Step 2, then the challenger will measure the first i copies of the message register $\mathcal{M}$ with indices in I. Henceforth, $\mathsf{H}_0(\lambda)$ is just the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*_I,1/2}(\lambda)$, and

[28] To satisfy the syntax of collapse-binding experiments, this flip operation can be moved to the beginning of Step 3.

[29] To satisfy the syntax of collapse-binding experiments, this uncomputing operation of S' can be moved to Step 3(a) of the next round.

[30] With the restriction on qubits $\mathcal{A}^{\otimes l}$ presented within Definition 9, the subset I here will be some deterministic subset. In spite of this, in the analysis below we still treat I as a more general random subset. This is because then our analysis below extends to the case where the trick mentioned in the remark subsequent to Definition 9 is applied (to circumvent the restriction). Refer to the remark subsequent to our proof of this lemma for a greater detail.

$\mathsf{H}_{|I|}(\lambda)$ is just the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*_I,1}(\lambda)$. Let

$$\epsilon_I \overset{def}{=} \frac{1}{2}(\Pr[\mathsf{H}_0(\lambda) = 1] - \Pr[\mathsf{H}_{|I|}(\lambda) = 1]);$$

we have $\sum_I |\epsilon_I| \geq \epsilon$.

Now consider the experiment $\mathsf{ColBindExpt}_{\mathsf{S}',b}(\lambda)$. For each index $i \in I$, let $\mathsf{ord}(i)$ denote the order of i in the subset I; that is, there are exactly $\mathsf{ord}(i)$ indices in I that are less than or equal to i. A key observation is that experiments $\mathsf{ColBindExpt}_{\mathsf{S}'_I,0}(\lambda)$ and $\mathsf{ColBindExpt}_{\mathsf{S}'_I,1}(\lambda)$ conditioned on an index i is chosen in Step 1(b) are identical to $\mathsf{H}_{\mathsf{ord}(i)-1}$ and $\mathsf{H}_{\mathsf{ord}(i)}$, respectively. Thus,

$$\begin{aligned}
& \Pr[\mathsf{ColBindExpt}_{\mathsf{S}'_I,0}(\lambda) = 1] - \Pr[\mathsf{ColBindExpt}_{\mathsf{S}'_I,1}(\lambda) = 1] \\
= \quad & \frac{1}{|I|}\sum_{i \in I}\Big(\Pr[\mathsf{ColBindExpt}_{\mathsf{S}'_I,0}(\lambda) = 1 \mid i \text{ is chosen is Step 1(b)}] \\
& \qquad -\Pr[\mathsf{ColBindExpt}_{\mathsf{S}'_I,1}(\lambda) = 1 \mid i \text{ is chosen is Step 1(b)}]\Big) \\
= \quad & \frac{1}{|I|}\sum_{i \in I}\big(\Pr[\mathsf{H}_{\mathsf{ord}(i)-1}(\lambda) = 1] - \Pr[\mathsf{H}_{\mathsf{ord}(i)}(\lambda) = 1]\big) \\
= \quad & \frac{1}{|I|}\big(\Pr[\mathsf{H}_0(\lambda) = 1] - \Pr[\mathsf{H}_{|I|}(\lambda) = 1]\big) \\
= \quad & \frac{2\epsilon_I}{|I|}.
\end{aligned}$$

It follows that

$$\begin{aligned}
& |\Pr[\mathsf{ColBindExpt}_{\mathsf{S}',0}(\lambda) = 1] - \Pr[\mathsf{ColBindExpt}_{\mathsf{S}',1}(\lambda) = 1]| \\
= \quad & \Big|\sum_I \Pr[\mathsf{ColBindExpt}_{\mathsf{S}'_I,0}(\lambda) = 1] - \sum_I \Pr[\mathsf{ColBindExpt}_{\mathsf{S}'_I,1}(\lambda) = 1]\Big| \\
= \quad & \Big|\sum_I (\Pr[\mathsf{ColBindExpt}_{\mathsf{S}'_I,0}(\lambda) = 1] - \Pr[\mathsf{ColBindExpt}_{\mathsf{S}'_I,1}(\lambda)] = 1)\Big| \\
= \quad & \frac{2\big|\sum_I \epsilon_I\big|}{|I|} \\
\geq \quad & \frac{2\epsilon}{l}.
\end{aligned}$$

Hence, the sender S' breaks the collapse-binding property of the scheme Com with advantage at least ϵ/l. ■

Remark. We note that the parallel composition lemma above still holds when the trick mentioned in the remark subsequent to Definition 9 is applied (to circumvent the restriction on qubits $\mathcal{A}^{\otimes l}$). To see this, note that now the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,0}(\lambda)$ and the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}^*,1/2}(\lambda)$ are indistinguishable (instead of identical in the proof above with restrictions on $\mathcal{A}^{\otimes l}$).

9 A useful (parallel-and-sequential) collapse-binding property in applications

In the security analysis of cryptographic applications which use quantum commitments, some commitments may be opened multiple times due to the quantum rewinding; in turn, the corresponding message registers might be measured multiple times (conditioned on the openings succeeding), too. To formalize this scenario, we modify the definition of the parallel collapse-binding property by introducing an indicator qubit $\mathcal{O}$, giving rise to a definition of parallel-and-sequential collapse binding; this will be the actual collapse binding property that is really useful in cryptographic applications. Moreover, this introduction of the indicator $\mathcal{O}$ even allows us to absorb Step 2 of parallel collapse-binding into its Step 3, giving the following cleaner definition:

Definition 10 (Parallel-and-sequential collapse-binding) Let $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ be a non-interactive quantum commitment scheme w.r.t. Definition 2. Consider the parallel-and-sequential collapse-binding experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ defined as below, where the challenge bit $b \in \{0,1\}$ and the malicious sender $\mathsf{S}^* = (|\tau\rangle, P, \mathsf{D})$ is a non-uniform QPT interactive algorithm. We say that the sender S^* is $l(\lambda)$-fold, $t(\lambda)$-verification, if it attacks l folds of the scheme Com running in parallel and may interact with the challenger at most $t(\lambda)$ rounds.

$\underline{\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)}$:

1. The malicious sender S^* receives/prepares a joint system $(\mathcal{C}^{\otimes l}, \mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D}, \mathcal{O})$ in the state $|\tau\rangle$. Then it sends the commitment register $\mathcal{C}^{\otimes l}$, together with the description of the predicate P to the challenger.

2. Now the sender S^* will try to guess the challenge bit b by running the *distinguisher* D, which may *interact* with the challenger at most $t(\lambda)$ rounds before outputting a guess $b' \in \{0,1\}$. In particular, each round of the interaction between the distinguisher D and the challenger will take the following form:

   (a) The distinguisher D performs a unitary D on its system, and sends registers $(\mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D}, \mathcal{O})$ to the challenger.

   (b) The challenger performs the binary projective measurement $\{\Pi_{\mathsf{par}}, \mathbb{1} - \Pi_{\mathsf{par}}\}$, where the expression of the projector Π_{par} is given by Eq. (14). If the measurement outcome is 1 and $\underline{b = 1}$, then measure the qubit $\mathcal{O}$: if the outcome is 1, then further measure qubits $\mathcal{A}^{\otimes l}$ and registers $\mathcal{M}_i$'s such that the qubit $\mathcal{A}_i$ contains 1.

      Restrictions on the state of qubits $\mathcal{A}^{\otimes l}$:[31] the same as those introduced in the definition of parallel collapse-binding (Definition 9).

      The challenger sends registers $(\mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D}, \mathcal{O})$ together with the outcome of the binary measurement $\{\Pi_{\mathsf{par}}, \mathbb{1} - \Pi_{\mathsf{par}}\}$ back to the distinguisher.

3. The distinguisher D performs the unitary D on its system once more and then measures a designated qubit, with the outcome b' that will be treated as the output of the whole experiment.

[31] Note that in the case where the measurement outcome of the qubit $\mathcal{O}$ is 0, qubits $\mathcal{A}^{\otimes l}$ and registers $\mathcal{M}_i$'s will *not* be measured. Then the restrictions on the state of qubits $\mathcal{A}^{\otimes l}$ can be removed. This will be very important for applications.

We say that the quantum commitment scheme Com is *parallel-and-sequential collapse-binding* if for all non-uniform QPT sender S^*,

$$\Pr_{b \xleftarrow{\$} \{0,1\}}[\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda) = b] \leq \frac{1}{2} + negl(\lambda).$$

Quantitatively, we say that the quantum commitment scheme Com is *$l(\lambda)$-fold, $t(\lambda)$-verification $\epsilon(\lambda)$-parallel-and-sequential collapse-binding* if for any $l(\lambda)$-fold, $t(\lambda)$-verification non-uniform QPT malicious sender S^*,

$$\Pr_{b \xleftarrow{\$} \{0,1\}}[\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,0}(\lambda) = b] \leq \frac{1}{2} + \epsilon(\lambda).$$

Remark. Restrictions on qubits $\mathcal{A}^{\otimes l}$ can also be circumvented by the same trick as mentioned in the remark subsequent to Definition 9 for the purpose of proving the following sequential composition lemma.

Now we are ready to prove the sequential composition lemma as below, which has two items. We highlight that the second item is typically needed to ensure that the extraction (say, by the special soundness) be correct in applications.

Lemma 12 (Sequential composition) *Let* $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ *be a non-interactive quantum commitment scheme w.r.t. Definition 2.*

1. *If the scheme is parallel collapse-binding w.r.t. Definition 9, then it is also parallel-and-sequential collapse binding w.r.t. Definition 10.*

   In particular, if there is a malicious $l(\lambda)$-fold, $t(\lambda)$-verification sender S^* *who can win the parallel-and-sequential collapse-binding experiment* $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ *(for a uniformly random bit b) with advantage $\epsilon(\lambda)$, then there exists another malicious $l(\lambda)$-fold, $(t(\lambda) - 1)$-verification sender* S' *who can win the parallel collapse-binding experiment* $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',b}(\lambda)$ *(for a uniformly random bit b) with advantage at least ϵ/t.*

2. *For any copy of the message register $\mathcal{M}$ that is measured multiple times during the experiment* $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$*, all outcomes will be identical except for a negligible probability.*

   In particular, if for some $l(\lambda)$-fold, $t(\lambda)$-verification malicious sender S^**, the probability is at least $\epsilon(\lambda)$ that there are two measurements of some copy of the message register $\mathcal{M}$ whose outcomes are different in the experiment* $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$*, then there exists another $l(\lambda)$-fold, $(t(\lambda)-1)$-verification malicious sender* S' *who can win the multi-verification unique-message binding experiment* $\mathsf{MV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$ *with advantage at least $\epsilon/(lt)$.*

PROOF: We prove Item 1 first.

Given a malicious l-fold, t-verification sender $\mathsf{S}^* = (|\tau\rangle, P, \mathsf{D})$ who can win the parallel-and-sequential collapse-binding experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ (for a uniformly random bit b) with advantage ϵ, we will construct another malicious l-fold, $(t-1)$-verification sender S' who can win the parallel collapse-binding experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',b}(\lambda)$ (also for a uniformly random bit b) with advantage ϵ/t.

Basically, the sender S' will simulate S^* in the parallel collapse-binding experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',b}(\lambda)$ (for a uniformly random bit b), except that now S', as opposed to the challenger in the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$, will measure the qubit $\mathcal{O}$ in each round. In greater detail, the parallel collapse-binding experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',b}(\lambda)$ proceeds as follows:

1. This step is further divided into several steps:

   (a) S' chooses $i \xleftarrow{\$} \{1, 2, \ldots, t\}$ uniformly random.

   (b) S' *internally* simulates from the beginning the interaction between S^* and the challenger in the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$, until the i-th time when the qubit $\mathcal{O}$ is measured with the outcome 1, but qubits $\mathcal{A}^{\otimes l}$ and the corresponding message registers $\mathcal{M}_i$'s have not yet been measured by the challenger. If this does not happen before the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$ ends, then the experiment will output whatever the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$ outputs.

   (c) S' sends the system $(\mathcal{C}^{\otimes l}, \mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D})$ (while keeping the qubit $\mathcal{O}$), together with the description of the predicate P, to the challenger.

2. The challenger performs the binary projective measurement $\{\Pi_{\mathsf{par}}, \mathbb{1} - \Pi_{\mathsf{par}}\}$, where the expression of the projector Π_{par} is given by Eq. (14). If the measurement outcome is 1[32] and $\underline{b = 1}$, then the challenger measures qubits $\mathcal{A}^{\otimes l}$ in the computational basis to obtain a subset I which consists of all indices with the corresponding qubit $\mathcal{A}$ containing 1. It then measures register $\mathcal{M}_i$'s with the index $i \in I$ in the computational basis. It returns registers $(\mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D})$ to the sender S' (without the commitment register $\mathcal{C}^{\otimes l}$).

3. Now the sender S' will try to guess the challenge bit b by running almost the same distinguisher D as used by the sender S^* (except for the measurements of the qubit $\mathcal{O}$), which may *interact* with the challenger at most $t - i$ rounds before outputting a guess $b' \in \{0, 1\}$. In particular, each round of the interaction between the distinguisher D and the challenger will take the following form:

   (a) The distinguisher D performs the unitary D on its system, and sends registers $(\mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D})$ to the challenger.

   (b) The challenger performs the binary projective measurement $\{\Pi_{\mathsf{par}}, \mathbb{1} - \Pi_{\mathsf{par}}\}$, and then sends registers $(\mathcal{R}^{\otimes l}, \mathcal{M}^{\otimes l}, \mathcal{A}^{\otimes l}, \mathcal{D})$ together with the measurement outcome back to the distinghuisher D.

   (c) If the challenger's measurement outcome is 1, then the distinguisher D will measure the qubit $\mathcal{O}$ in the computational basis.[33] (If the outcome is 0, then the qubit $\mathcal{O}$ will not be measured.)

4. The distinguisher D performs the unitary D on its system once more and then measures a designated qubit, with the outcome b' that will be treated as the output of the whole experiment.

We prove by a hybrid argument that the sender S' can win the parallel collapse-binding experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',b}(\lambda)$ (for a uniformly random bit b) with advantage ϵ/t. Specifically, for $i = 1, \ldots, t$, the i-th hybrid $\mathsf{H}_i(\lambda)$ is defined as the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',1}(\lambda)$ conditioned on the index i is chosen in Step 1(a). It is easy to see that $\mathsf{H}_t(\lambda)$ is just the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$. We define $\mathsf{H}_0(\lambda)$ as the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,0}(\lambda)$. Thus,

$$|\Pr[\mathsf{H}_0(\lambda) = 1] - \Pr[\mathsf{H}_t(\lambda) = 1]| > 2\epsilon.$$

[32] The measurement outcome cannot be 0 by our construction of S'.

[33] This step can be absorbed into Step 3(a) of the next round to satisfy the syntax of the parallel collapse-binding experiment.

Also observe that the experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',0}(\lambda)$ conditioned on an index i $(1 \leq i \leq t)$ chosen in Step 1(a) is just the hybrid $\mathsf{H}_{i-1}(\lambda)$. It follows that

$$\begin{aligned}
& |\Pr[\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',0}(\lambda) = 1] - \Pr[\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',1}(\lambda) = 1]| \\
= \; & \frac{1}{t}\Big|\sum_{i=1}^{t}\big(\Pr[\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',0}(\lambda) = 1 \mid i \text{ is chosen in Step 1(a)}] \\
& \quad -\Pr[\mathsf{P\text{-}ColBindExpt}_{\mathsf{S}',1}(\lambda) = 1 \mid i \text{ is chosen in Step 1(a)}]\big)\Big| \\
= \; & \frac{1}{t}\Big|\sum_{i=1}^{t}\big(\Pr[\mathsf{H}_{i-1}(\lambda) = 1] - \Pr[\mathsf{H}_{i}(\lambda) = 1]\big)\Big| \\
= \; & \frac{1}{t}|\Pr[\mathsf{H}_{0}(\lambda) = 1] - \Pr[\mathsf{H}_{n}(\lambda) = 1]| \\
> \; & \frac{2\epsilon}{t}.
\end{aligned}$$

But this breaks the parallel collapse-binding property of the commitment scheme.

This finishes the proof of Item 1.

We next prove Item 2.

Given a malicious l-fold, t-verification sender $\mathsf{S}^* = (|\tau\rangle, P, \mathsf{D})$, we construct another malicious $(t-1)$-verification sender $\mathsf{S}' = (\tau', P', \mathsf{T}')$ such that the multiple-verification unique-message binding experiment (Definition 5) $\mathsf{MV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$ proceeds as follows:

1. This step is further divided into several steps:
   (a) S' chooses $r \xleftarrow{\$} \{1, 2, \ldots, t-1\}$.
   (b) S' internally simulates the interaction between S^* and the challenger in the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$ from the beginning, until the *end* of the round in which the r-th time when the qubit $\mathcal{O}$ is measured with the outcome 1: if the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$ ends before this happening, or any inconsistency (of the measurement outcomes of copies of the register $\mathcal{M}$) occurs during the simulation, then S' aborts and the experiment outputs 0. The resulting (sub-normalized) quantum state of the whole system will be denoted by τ'.
   (c) S' initializes a fresh qubit $\mathcal{F}$ in the state $|1\rangle$. Denote by I_1 the subset of $\{1, 2, \ldots, l\}$ consisting of all indices with which the measurement outcomes of corresponding copies of the qubit $\mathcal{A}$ are 1's. Choose $i \xleftarrow{\$} I_1$.
   (d) S' sets the predicate P' to be equal to the value of the qubit $\mathcal{F}$.
   (e) S' sends the i-th copy of registers $(\mathcal{C}_i, \mathcal{R}_i, \mathcal{M}_i, \mathcal{A}_i, \mathcal{F})$, together with the description of the predicate P' to the challenger.

2. The challenger performs the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ where the projector Π is given by Eq. (5) with the predicate P' plugged in. If the outcome is 0, i.e. the verification fails, then the challenger aborts and the experiment outputs 0; otherwise, the challenger returns registers $(\mathcal{R}_i, \mathcal{M}_i, \mathcal{A}_i, \mathcal{F})$ to the sender S' (without the commitment register $\mathcal{C}_i$), who will flip the value of the qubit $\mathcal{F}$ to set it back to 0.

3. The sender S' measures the message register $\mathcal{M}_i$ in the computational basis, obtaining the first message m_1.

4. Now the sender S' will try to open the i-th commitment as another message $m_2 \neq m_1$ by running the distinguisher D used by the sender S^* as a subroutine, which may *interact* with the challenger at most $t-1$ rounds. In particular, each round of the interaction between the transformer T' and the challenger will take the following form:

   (a) The transformer T' first performs the unitary D induced by the distinguisher D on its system, and then simulates the binary projective measurement $\left\{\Pi'_{\mathsf{par}}, \mathbb{1} - \Pi'_{\mathsf{par}}\right\}$ (Eq. (15)) unitarily in the standard way, using the qubit $\mathcal{F}$ to record the measurement outcome. It then sends registers $(\mathcal{R}_i, \mathcal{M}_i, \mathcal{A}_i, \mathcal{F})$ to the challenger.

   (b) The challenger performs the binary projective measurement $\{\Pi, \mathbb{1} - \Pi\}$ that is the same as the one in Step 2, and sends registers $(\mathcal{R}_i, \mathcal{M}_i, \mathcal{A}_i, \mathcal{F})$, together with the measurement outcome, back to the transformer, who will then *uncomputes* the qubit $\mathcal{F}$, i.e. performing the inverse of the unitary simulation of the binary projective measurement $\left\{\Pi'_{\mathsf{par}}, \mathbb{1} - \Pi'_{\mathsf{par}}\right\}$ that is done in Step 3(a).

   (c) If the challenger's verification succeeds, then the transformer T' measures the qubit $\mathcal{O}$. If the outcome is 1, then further measures qubits $\mathcal{A}^{\otimes l}$ to obtain a subset I_2, and measures copies of the message registers $\mathcal{M}$ with indices in I_2. If $i \in I_2$, jump to Step 5.

5. If the verification in the last round of Step 4 fails, then S' aborts and the experiment outputs 0. Otherwise, S' measures the qubit $\mathcal{A}_i$, as well as the message registers $\mathcal{M}_i$ to obtain the second message m_2: If either the qubit $\mathcal{A}_i$ contains 0, or $m_2 = m_1$, then S' aborts and the experiment outputs 0; otherwise, the experiment outputs 1.

Now we estimate the advantage achieved by the malicious sender S' in the multi-verification unique-message binding experiment $\mathsf{MV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$. In a running of the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$, we call that an *inconsistency* (i^*, r_1^*, r_2^*) occurs if the message register $\mathcal{M}_{i^*}$ is measured in both rounds r_1^* and r_2^*, but not in the between; moreover, the corresponding two measurement outcomes are different.

Consider the moment when the first time an inconsistency (i^*, r_1^*, r_2^*) occurs in a running of the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$.[34] In Step 1(a) of the experiment $\mathsf{MV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$, the chosen index pair (i, r) will hit (i^*, r_1^*) with probability at least $1/lt$. And conditioned on this event happening, the experiment $\mathsf{MV\text{-}UniqBindExpt}_{\mathsf{S}'}(\lambda)$ will be just a simulation of the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$ from the beginning to the moment when the first time an inconsistency occurs.

Since the probability that an inconsistency occurs in the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$ is at least ϵ, it follows that S' can win the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$ with advantage at least $\epsilon/(lt)$.

This proves Item 2. ■

Remark. We note that the proofs above (for both items) really do not use the restrictions on qubits $\mathcal{A}^{\otimes}$ that are presented within Definition 10 (or Definition 9). Henceforth, the sequential composition lemma holds in both the case where the restrictions are imposed on qubits $\mathcal{A}^{\otimes}$ and the case where the trick to circumvent the first restriction (refer to the remark subsequent to Definition 9) is applied.

[34] This occurs in the round r_2^*; if there are multiple inconsistencies occur simultaneously, then just choose an arbitrary one.

The following theorem is an immediate corollary of many lemmas established before; it connects the unique-message binding error of non-interactive quantum commitments in constructions with the sequential-and-parallel collapse-binding error in cryptographic applications in a quantitative way.

Theorem 3 *Let* $\mathsf{Com} = (\mathsf{Commit}, \mathsf{Verify})$ *be a non-interactive quantum commitment scheme (Definition 2) that is* ϵ*-unique-message binding (Definition 3). Then for the parallel-and-sequential collapse-binding experiment* $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$ *w.r.t. any* l*-fold,* t*-verification sender* S^* *and a uniformly random bit* b*:*

1. S^* *can only win the experiment with advantage at most* $O(\sqrt{\epsilon N} \cdot lt^4)$*;*

2. *The probability of any inconsistency of measurement outcomes occurring in the experiment* $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$ *is at most* $O(\epsilon l t^7)$*.*

Proof: We first prove Item 1. For contradiction, suppose that there is an l-fold, t-verification sender S^* who can win the parallel-and-sequential collapse-binding experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,b}(\lambda)$, for a uniformly random bit b, with advantage, say $100\sqrt{\epsilon N} \cdot lt^4$.

By Item 1 of Lemma 12, there exists another l-fold, t-verification sender S_1' who can win the corresponding parallel collapse-binding experiment $\mathsf{P\text{-}ColBindExpt}_{\mathsf{S_1}',b}(\lambda)$ (for a uniformly random bit b) with advantage at least $100\sqrt{\epsilon N} \cdot lt^3$.

Then by Lemma 11, there exists another malicious t-verification sender S_2' who can win the collapse-binding experiment $\mathsf{ColBindExpt}_{\mathsf{S}_2',b}(\lambda)$ (for a uniformly random bit b) with advantage at least $100\sqrt{\epsilon N} \cdot t^3$.

Then by Lemma 10, there exists another $2t$-verification malicious sender S_3' who can win the reversible multi-verification unique-message binding experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}_3'}(\lambda)$ with advantage $80000\epsilon t^6$.

Finally by Lemma 7, there exists yet another sender S_4' who can win the unique-message binding experiment $\mathsf{UniqBindExpt}_{\mathsf{S}_4'}(\lambda)$ with advantage at least 2ϵ. But this breaks the ϵ-unique-message binding property of the scheme Com. This proves Item 1.

We next prove Item 2.

For contradiction, suppose that there exists an l-fold, t-verification sender S^* such that in the parallel-and-sequential collapse-binding experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(\lambda)$, inconsistencies occur with probability at least, say, $100\epsilon l t^7$. By Item 2 of Lemma 12, there exists another l-fold, t-verification malicious sender S_1' who can win the multi-verification unique-message binding experiment $\mathsf{MV\text{-}UniqBindExpt}_{\mathsf{S}_1'}(\lambda)$ with advantage at least $100\epsilon t^6$. Since each multi-verification unique-message binding experiment can be simulated by a reversible one in the standard way, it follows that there exists another l-fold, t-verification malicious sender S_2' who can win the reversible multi-verification unique-message binding experiment $\mathsf{RMV\text{-}UniqBindExpt}_{\mathsf{S}_2'}(\lambda)$ with advantage at least $100\epsilon t^6$.

Then by Lemma 7, there exists yet another sender S_3' who can win the unique-message binding experiment $\mathsf{UniqBindExpt}_{\mathsf{S}_3'}(\lambda)$ with advantage at least 2ϵ. But this breaks the ϵ-unique-message binding property of the scheme Com. This proves Item 2. ■

Remark. One may use the trick mentioned in the remark subsequent to Definition 9 to circumvent the restriction on qubits $\mathcal{A}^{\otimes l}$. However, this will only introduce a constant factor to estimations in the two items of the theorem above.

10 Application: the security against the prover in Blum's protocol for Hamiltonian Cycle and its variants

In this section, we plug a generic non-interactive quantum *bit* commitment scheme w.r.t. Definition 2 in Blum's protocol for Hamiltonian Cycle and its variants, showing how to base the computational soundness or argument-of-knowledge of resulting protocols on its computational binding property.

Similar techniques can also be used to cope with the GMW zero-knowledge protocol for Graph 3-Coloring; refer to Appendix C for the detail.

10.1 Soundness

In this subsection, we show that the original Blum's protocol with a generic non-interactive quantum *bit* commitment scheme plugged in is sound against any non-uniform QPT prover. This improves one of the main result in [Yan21].

We first recap Blum's protocol.

Blum's protocol. Suppose that the common input graph G has n vertices, which can be represented by an $n \times n$ adjacency matrix. Informally, Blum's protocol instantiated with a generic quantum bit commitment scheme proceeds as follows:

P1 The prover chooses a random permutation π over the set $\{1, 2, \ldots, n\}$, and commits to the permuated graph $\pi(G)$ in a bitwise fashion using a generic non-interactive quantum bit commitment scheme.

V1 The verifier chooses a challenge bit $b \in \{0, 1\}$ uniformly random.

P2 If $b = 0$, then the prover sends π, together with the decommitments for *all* (quantum) bit commitments to the verifier. Otherwise, i.e. if $b = 1$, then the prover sends the location of a Hamiltonian cycle of the graph $\pi(G)$, together with the decommitments for the n bit commitments to the n edges of the Hamiltonian cycle.

V2 If $b = 0$, then the verifier checks that all n^2 bit commitments are opened as $\pi(G)$ successfully. If $b = 1$, then the verifier checks that the n edges indeed form a Hamiltonian cycle, and all corresponding n bit commitments are opened as 1 successfully.

We formalize an arbitrary attack $(|\tau\rangle, U)$ of the prover in Blum's protocol as follows, where registers for the prover's workspace are suppressed to simplify the notation:

- In Step P1, the prover prepares/receives a system $(\mathcal{C}^{\otimes n^2}, \mathcal{R}^{\otimes n^2}, \mathcal{M}^{\otimes n^2}, \mathcal{A}^{\otimes n^2}, \mathcal{D})$ in the state $|\tau\rangle$, sending the commitment registers $\mathcal{C}^{\otimes n^2}$ to the verifier.
- In Step P2, if $b = 0$, then the prover does nothing; otherwise, if $b = 1$, then it performs the unitary U on its system. It then sends the system $(\mathcal{R}^{\otimes n^2}, \mathcal{M}^{\otimes n^2}, \mathcal{A}^{\otimes n^2}, \mathcal{D})$ to the verifier.

The verifier's verifications corresponding to $b = 0$ and $b = 1$ will be of the form given by Eq. (14), with different predicates plugged in. Specifically, the predicate corresponding to $b = 0$ induces the following projector:

$$P_0 \overset{def}{=} \sum_{\pi} |\pi\rangle\langle\pi|^{\mathcal{D}} \otimes |\pi(G)\rangle\langle\pi(G)|^{\mathcal{M}^{\otimes n^2}} \otimes |1^{n^2}\rangle\langle 1^{n^2}|^{\mathcal{A}^{\otimes n^2}}. \tag{16}$$

In turn, the corresponding verification induces the projector:

$$V_0 \overset{def}{=} \big(|0\rangle \langle 0|^{\mathcal{A}} \otimes \mathbb{1}^{\mathcal{CRM}} + |1\rangle \langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}} \big)^{\otimes n^2} \cdot P_0. \tag{17}$$

The predicate corresponding to $b = 1$ induces the following projector:

$$P_1 \overset{def}{=} \sum_H |H\rangle \langle H|^{\mathcal{D}} \otimes |1^n\rangle \langle 1^n|^{\mathcal{M}^{\otimes H}} \otimes |H\rangle \langle H|^{\mathcal{A}^{\otimes n^2}}, \tag{18}$$

where H denotes the adjacency matrix representation of the Hamiltonian cycle H, and the register $\mathcal{M}^{\otimes H}$ denotes copies of the register $\mathcal{M}$ (in total n) with indices corresponding to 1-entries (i.e. edges) of H. In turn, the corresponding verification induces the projector:

$$V_1 \overset{def}{=} \big(|0\rangle \langle 0|^{\mathcal{A}} \otimes \mathbb{1}^{\mathcal{CRM}} + |1\rangle \langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}} \big)^{\otimes n^2} \cdot P_1. \tag{19}$$

Theorem 4 *Using non-interactive statistically-hiding, computationally-binding quantum bit commitments (Definition 2) in Blum's protocol gives rise to a three-round, quantum statistical zero-knowledge argument for the* ***NP****-complete language* Hamiltonian Cycle *with perfect completeness and soundness error* $1/2$.

Proof: Suppose that the (unique-message) binding error of the quantum bit commitment scheme used is bounded by ϵ, which is negligible. Suppose that the common input graph G with n vertices does not have a Hamiltonian cycle.

For contradiction, suppose that there exists an attack $P^* = (|\tau\rangle, U)$ of the prover which can convince the verifier to accept with probability $1/2 + 1/p$, where $p(\cdot)$ is a polynomial of $n \overset{def}{=} |V(G)|$ (i.e. the number of vertices of the common input graph G). That is,

$$\frac{1}{2}\big(\|V_0 |\tau\rangle\|^2 + \|V_1(U \otimes \mathbb{1}^{\mathcal{C}^{\otimes n^2}}) |\tau\rangle \|^2 \big) = \frac{1}{2} + \frac{1}{p}.$$

Applying the quantum rewinding lemma (Lemma 4), we have:

$$\|V_1(U \otimes \mathbb{1}^{\mathcal{C}^{\otimes n^2}}) V_0 |\tau\rangle \| \geq 1 - \sqrt{2\Big(\frac{1}{2} - \frac{1}{p}\Big)} \geq \frac{1}{p}.$$

Consider the parallel-and-sequential collapse-binding experiment (Definition 9) $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,b}(n)$ w.r.t. the n^2-fold, 2-verification malicious sender $\mathsf{S}^* = (|\tau\rangle, (P_0, P_1), U)$ and a uniformly random bit b as follows:

1. S^* receives/prepares a system $(\mathcal{C}^{\otimes n^2}, \mathcal{R}^{\otimes n^2}, \mathcal{M}^{\otimes n^2}, \mathcal{A}^{\otimes n^2}, \mathcal{D}, \mathcal{O})$ in the state $|\tau\rangle |1\rangle^{\mathcal{O}}$. Then it sends the commitment registers $\mathcal{C}^{\otimes n^2}$, together with the descriptions of predicates[35] (P_0, P_1) to the verifier.

2. S^* does nothing and sends registers $(\mathcal{R}^{\otimes n^2}, \mathcal{M}^{\otimes n^2}, \mathcal{A}^{\otimes n^2}, \mathcal{D}, \mathcal{O})$ to the challenger.

3. The challenger performs the binary projective measurement $\{V_0, \mathbb{1} - V_0\}$. If the measurement outcome is 1, then it measures the qubit $\mathcal{O}$: if the outcome is 1, then it further measures qubits $\mathcal{A}^{\otimes n^2}$. If the measurement of the qubit $\mathcal{O}$ outputs 1 and $b = 1$, then it measures the copies of the register $\mathcal{M}$ with the corresponding qubit $\mathcal{A}$ containing 1, i.e. all copies of the register $\mathcal{M}$. The challenger returns registers $(\mathcal{R}^{\otimes n^2}, \mathcal{M}^{\otimes n^2}, \mathcal{A}^{\otimes n^2}, \mathcal{D}, \mathcal{O})$ to the sender S^* (without the commitment register $\mathcal{C}^{\otimes n^2}$).

[35] They can be viewed as a single predicate that depends on the counting of rounds of the interaction between the sender and the challenger; refer to the remark immediately following Definition 5

4. If the challenger's verification fails, then S^* aborts and the experiment outputs 0.[36] Otherwise, S^* performs the unitary U on its system other than $\mathcal{O}$, and flips the value of $\mathcal{O}$ (i.e. performs the Pauli-X on $\mathcal{O}$). Then it sends registers $(\mathcal{R}^{\otimes n^2}, \mathcal{M}^{\otimes n^2}, \mathcal{A}^{\otimes n^2}, \mathcal{D}, \mathcal{O})$ to the challenger.

5. The challenger performs the binary projective measurement $\{V_1, \mathbb{1} - V_1\}$. If the measurement outcome is 1, then it measures the qubit $\mathcal{O}$: if the outcome is 1, then it further measures qubits $\mathcal{A}^{\otimes n^2}$. If the measurement of the qubit $\mathcal{O}$ outputs 1 and $b = 1$, then it measures the copies of the register $\mathcal{M}$ with the corresponding qubit $\mathcal{A}$ containing 1. The challenger returns registers $(\mathcal{R}^{\otimes n^2}, \mathcal{M}^{\otimes n^2}, \mathcal{A}^{\otimes n^2}, \mathcal{D}, \mathcal{O})$ to the sender S^*.

6. If the challenger's verification fails, then the experiment outputs 0. Otherwise, the experiment outputs 1.

It is easy to check that

$$\Pr[\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,0}(n) = 1] = \| V_1 (U \otimes \mathbb{1}^{\mathcal{C}^{\otimes n^2}}) V_0 \left|\tau\right\rangle \|^2 \geq \frac{1}{p^2}.$$

The experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(n)$ differs from the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,0}(n)$ in that conditioned on the challenger's verification passes in Step 3, the challenger will measure registers $\mathcal{M}^{\otimes n^2}$ to obtain a graph that is isomorphic to the graph G. By Item 1 of Theorem 3 where we plug in $l = n^2$, $t = 2$ and $N = 2$, it follows that

$$\Pr[\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(n) = 1] \geq \frac{1}{p^2} - O(\sqrt{\epsilon} n^2).$$

Now let us modify S^* slightly: it no longer flips the qubit $\mathcal{O}$ in Step 4; we call the resulting sender S'. Then the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}',1}(n)$ only differs from the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(n)$ in that conditioned on the challenger's verification passing in Step 5, the challenge will further measure to obtain a Hamiltonian cycle. Since this (conditional) measurement will not affect the probability that the experiment outputting 1, we have

$$\Pr[\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}',1}(n) = 1] = \Pr[\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(n) = 1] \geq \frac{1}{p^2} - O(\sqrt{\epsilon} n^2). \tag{20}$$

Moreover, by Item 2 of Theorem 3 where we plug in $l = n^2$, $t = 2$ and $N = 2$, the probability that a graph obtained in Step 3 and a Hamiltonian cycle obtained in Step 5 is *inconsistent* in the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}',1}(n)$ is at most $O(\epsilon n^2)$. Combined with Inequality (20), it follows that in the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}',1}(n)$, with probability at least $1/p^2 - O(\sqrt{\epsilon} n^2) - O(\epsilon n^2)$ (which is positive), the graph obtained in Step 3 is isomorphic to the the original graph G and the Hamiltonian cycle obtained in Step 5 is consistent with this graph. This implies that there is a Hamiltonian cycle in the original graph G, contradicting to that G is not Hamiltonian.

This finishes the proof of the theorem. ■

10.2 Argument-of-knowledge

In this subsection, we will use the definition of quantum argument-of-knowledge [Unr16b] that is similar to quantum proof-of-knowledge defined by Unruh [Unr12], with the only difference that now

[36] To satisfy the syntax of parallel-and-sequential collapse-binding experiments given in Definition 10, this can be viewed as S^* proceeding arbitrarily subsequently until the end of the experiment when the bit 0 is output.

the malicious prover is modelled by a non-uniform QPT (as opposed to computationally unbounded) algorithm.[37] Informally speaking, for quantum argument-of-knowledge, we require that there exists a *knowledg error* k such that for any non-uniform QPT sender who can convince the verifier to accept with probability p, there exists another non-uniform QPT extraction algorithm that can output the witness with probability at least $(p-k)^d/q$ for some polynomial q and constant d.

To obtain quantum argument-of-knowledge, we need to modify the original Blum's protocol slightly by letting the prover additionally commit to its responses corresponding to the challenge bit 0 in its firstmessage. Technically, this is because generally measuring the message register $\mathcal{M}$ does *not* uniquely determine the measurement outcome of the register $\mathcal{D}$, which stores the permutation used by the prover: it is possible that a superposition of several different permutations is stored in the register $\mathcal{D}$ such that all these permutations will mapy the input graph to the same graph! Intuitively, the collapse of the quantum state caused by the measurement of the register $\mathcal{D}$ may perturb the state significantly, deteriorating the success probability of quantum rewinding.

A variant of Blum's protocol. This *first* variant[38] does the following modification to Blum's original protocol: in addition to commit to the graph $\pi(G)$ in its first message, the prover also commits to the random permutation π. Correspondingly, when the verifier's challenge bit is 0, the prover will additionally open the commitment to the random permutation π.

Specifically, the permutation π can be represented by its corresponding $n \times n$ permutation matrix. Thus, the whole system becomes $(\mathcal{C}^{\otimes 2n^2}, \mathcal{R}^{\otimes 2n^2}, \mathcal{M}^{\otimes 2n^2}, \mathcal{A}^{\otimes 2n^2}, \mathcal{D})$.

The predicate P_0 corresponding to the challenge bit 0 becomes

$$P_0' \overset{def}{=} \sum_{\pi} |\pi\rangle\langle\pi|^{\mathcal{D}} \otimes |\pi, \pi(G)\rangle\langle\pi, \pi(G)|^{\mathcal{M}^{\otimes 2n^2}} \otimes |1^{2n^2}\rangle\langle 1^{2n^2}|^{\mathcal{A}^{\otimes 2n^2}}, \tag{21}$$

and the corresponding verification

$$V_0' \overset{def}{=} \left(|0\rangle\langle 0|^{\mathcal{A}} \otimes \mathbb{1}^{\mathcal{CRM}} + |1\rangle\langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}} \right)^{\otimes 2n^2} \cdot P_0'. \tag{22}$$

Expressions for the predicate P_1 and the verification V_1 corresponding to the challenge bit 1 remain almost the same as those introduced in soundness analysis before, except that now H denotes the concatenation of the string 0^{n^2} and the encoding of the adjacency matrix representation of the Hamiltonian cycle H.[39] Specifically,

$$\begin{aligned} P_1' &\overset{def}{=} \sum_{H} |H\rangle\langle H|^{\mathcal{D}} \otimes |1^n\rangle\langle 1^n|^{\mathcal{M}^{\otimes H}} \otimes |H\rangle\langle H|^{\mathcal{A}^{\otimes 2n^2}}, & (23) \\ V_1' &\overset{def}{=} \left(|0\rangle\langle 0|^{\mathcal{A}} \otimes \mathbb{1}^{\mathcal{CRM}} + |1\rangle\langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}} \right)^{\otimes 2n^2} \cdot P_1'. & (24) \end{aligned}$$

Theorem 5 *Using non-interactive statistically-hiding, computationally-binding quantum bit commitments (Definition 2) in the first variant of Blum's protocol as above gives rise to a quantum statistical zero-knowledge argument-of-knowledge for the* ***NP****-complete language* Hamiltonian Cycle *with perfect completeness and knowledge error* 1/2.

[37] Strictly speaking, the definition of quantum argument-of-knowledge used here is also slightly different from Unruh's [Unr12, Unr16b]. Specifically, Unruh actually defines *post-quantum* proof/argument-of-knowledge (i.e. protocols are restricted to be classical), whereas here both quantum computation and communication are allowed. In spite of this, extending the definition from the post-quantum to the quantum setting is straightforward, as previously studied in [FUYZ22].

[38] In the next subsection, we will present another variant for a slightly different purpose.

[39] The string 0^{n^2} indicates that the commitments to the permutation π will not be opened.

Proof: We just sketch how to modify our proof for the soundness above (i.e. Theorem 4) to that for the argument-of-knowledge here.

The knowledge extractor we construct essentially follows the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}',1}(n)$ constructed in the soundness analysis in the previous subsection. Specifically, the *knowledge extractor* proceeds as follows:

1. Receive/prepare a system $(\mathcal{C}^{\otimes 2n^2}, \mathcal{R}^{\otimes 2n^2}, \mathcal{M}^{\otimes 2n^2}, \mathcal{A}^{\otimes 2n^2}, \mathcal{D})$ in the state $|\tau\rangle$, as P^* does.
2. Perform the binary projective measurement $\{V_0', \mathbb{1} - V_0'\}$, where V_0' is given by the expression (22). If the measurement outcome is 1, then measure the register $\mathcal{D}$ to obtain a permutation π; otherwise, abort.
3. Perform the unitary U on the system other than $\mathcal{C}^{\otimes 2n^2}$.
4. Perform the binary projective measurement $\{V_1', \mathbb{1} - V_1'\}$, where V_1' is given by the expression (24). If the measurement outcome is 1, then measure the register $\mathcal{D}$ to obtain a Hamiltonian cycle H; otherwise, abort.
5. Check if the graph $\pi(G)$ and the Hamiltonian cycle H are consistent. If yes, then output $\pi^{-1}(H)$; otherwise, abort.

To see why the knowledge extractor works, a key observation is that in its Step 2, the measurement of the register $\mathcal{D}$ can be *replaced* with that of registers $\mathcal{M}^{\otimes 2n^2}$: the outcome of the former will uniquely determine that of the latter, and vice versa. After this replacement, one can check that the knowledge extractor is essentially the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}',1}(n)$ constructed in the proof of soundness before (except that predicates P_0, P_1 and verifications V_0, V_1 will be replaced with P_0', P_1' and V_0', V_1', respectively). ■

10.3 Reducing the knowledge error by parallel composition

The knowledge error of the first variant of Blum's protocol given above is 1/2, which is too large for applications. One would like to reduce it to be negligible. A possible way to achieve this is by *parallel composition*, which preserves the round complexity. However, for the purpose of extraction, we need to compose yet another variant of Blum's original protocol given as below.

Yet another variant of Blum's protocol. Briefly, compared with the first variant given in the previous subsection, in this *second* variant we let the prover additionally commit to its response corresponding to the challenge 1. In greater detail, now the whole system becomes $(\mathcal{C}^{\otimes 3n^2}, \mathcal{R}^{\otimes 3n^2}, \mathcal{M}^{\otimes 3n^2}, \mathcal{A}^{\otimes 3n^2}, \mathcal{D})$. There are in total $3n^2$ quantum bit commitments, n^2 of which are commitments to the permutated graph $\pi(G)$, the permutation π, and the Hamiltonian cycle H, respectively.

Now the predicate corresponding to the challenge 0 becomes

$$P_0'' \overset{def}{=} \sum_\pi |\pi\rangle\langle\pi|^{\mathcal{D}} \otimes |\pi, \pi(G)\rangle\langle\pi, \pi(G)|^{\mathcal{M}^{\otimes 2n^2}} \otimes |0^{n^2}1^{2n^2}\rangle\langle 0^{n^2}1^{2n^2}|^{\mathcal{A}^{\otimes 3n^2}}, \qquad (25)$$

where the string $0^{n^2}1^{2n^2}$ stored in the registers $\mathcal{A}^{\otimes 3n^2}$ indicates that all but commitments to the Hamiltonian cycle H will be opened. The corresponding verification

$$V_0'' \overset{def}{=} \left(|0\rangle\langle 0|^{\mathcal{A}} \otimes \mathbb{1}^{\mathcal{CRM}} + |1\rangle\langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}}\right)^{\otimes 3n^2} \cdot P_0'. \qquad (26)$$

The predicate and the verification corresponding to the challenge 1 are given by

$$P_1'' \overset{def}{=} \sum_H |H\rangle \langle H|^{\mathcal{D}} \otimes |H\rangle \langle H|^{\mathcal{M}^{\otimes n^2}} \otimes |1^n\rangle \langle 1^n|^{\mathcal{M}^{\otimes H}} \otimes |1^{n^2}0^{n^2}H\rangle\langle 1^{n^2}0^{n^2}H|^{\mathcal{A}^{\otimes 3n^2}}, \tag{27}$$

$$V_1'' \overset{def}{=} \left(|0\rangle \langle 0|^{\mathcal{A}} \otimes \mathbb{1}^{\mathcal{CRM}} + |1\rangle \langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}} \right)^{\otimes 3n^2} \cdot P_1', \tag{28}$$

where the string $1^{n^2}0^{n^2}H$ stored in the registers $\mathcal{A}^{\otimes 3n^2}$ indicates that commitments to the Hamiltonian cycle H and those to entries of $\pi(G)$ corresponding to edges of H will be opened.

Theorem 6 *The parallel composition of the second variant of Blum's protocol given above with non-interactive statistically-hiding, computationally-binding quantum bit commitments (Definition 2) plugged in gives rise to a quantum argument-of-knowledge for the* ***NP****-complete language* Hamiltonian Cycle *with perfect completeness and negligible knowledge error.*

Proof: When l copies of the atomic protocol are composed, the size of the verifier's challenge space becomes 2^l. For an arbitrary challenge $r \in \{0,1\}^l$, the verifier's verification induces the projector

$$V_r'' \overset{def}{=} \bigotimes_{i=1}^{l} V_{r_i}'',$$

where V_0'' and V_1'' are given by expressions (26) and (28), respectively.

Given an attack $P^* = (|\tau\rangle, U)$ of the prover of the parallelized protocol, we sketch the knowledge extractor as below:

1. Receive/prepare a system $(\mathcal{C}^{\otimes 3n^2}, \mathcal{R}^{\otimes 3n^2}, \mathcal{M}^{\otimes 3n^2}, \mathcal{A}^{\otimes 3n^2}, \mathcal{D})^{\otimes l}$ in the state $|\tau\rangle$, as P^* does.

2. Choose $r \overset{\$}{\leftarrow} \{0,1\}^l$

3. Perform the unitary U_r, the unitary U with r as part of the input, on the system other than commitment registers $\mathcal{C}^{\otimes 3n^2 l}$.

4. Perform the binary projective measurement $\{V_r'', \mathbb{1} - V_r''\}'$. If the measurement outcome is 1, then measure registers $\mathcal{D}^{\otimes l}$; otherwise, abort. For each $i \in \{1, \ldots, l\}$, if $r_i = 0$, then the measurement of the corresponding copy of the register $\mathcal{D}$ will output a permutation π_i; if $r_i = 1$, then the measurement will output a Hamiltonian cycle H_i.

5. Perform the unitary $U_r^\dagger$.

6. Choose $r' \overset{\$}{\leftarrow} \{0,1\}^l$. If $r' = r$, abort.

7. Perform the unitary $U_{r'}$ on the system other than $\mathcal{C}^{\otimes 3n^2 l}$.

8. Perform the binary projective measurement $\left\{V_{r'}'', \mathbb{1} - V_{r'}''\right\}$. If the measurement outcome is 1, then measure registers $\mathcal{D}^{\otimes l}$; otherwise, abort. For each $i \in \{1, \ldots, l\}$, if $r_i' = 0$, then the measurement of the corresponding copy of the register $\mathcal{D}$ will output a permutation π_i; if $r_i' = 1$, then the measurement will output a Hamiltonian cycle H_i.

9. Let i be any position such that $r_i \neq r_i'$. Check if the graph $\pi_i(G)$ and the Hamiltonian cycle H_i are consistent. If yes, then output $\pi_i^{-1}(H_i)$; otherwise, abort.

We next sketch the proof that the extractor constructed above indeed works. Suppose that the (unique-message) binding error of the quantum bit commitment scheme used is bounded by ϵ (which is negligible).

As long as we compose the atomic protocol super-logarithmic number of times, i.e. $l = \omega(\log n)$, then the size of the challenge space C (with the size 2^l) is super-polynomial. Suppose that the prover P^* can convince the verifier to accept with some non-negligible probability $1/p$ (for some polynomial p) in the parallelized protocol. Now invoking the quantum rewinding lemma w.r.t. Σ-protocols (Lemma 5) with the super-polynomial $|C| = 2^l$ and the non-negligible $V = 1/p$, it follows that the knowledge extractor without measurements of registers $\mathcal{D}^{\otimes l}$ (in both Step 4 and 8) will not abort before Step 8 with probability at least $V(V^2 - 1/2^l)$, which is at least $1/(2p^3)$.

Note that for each fold i, regardless of the value of r_i, the measurement of the register $\mathcal{D}_i$ within the extractor is *equivalent* to that of corresponding copies of the message register $\mathcal{M}$. (The argument here is similar to the analysis of the argument-of-knowledge in the previous subsection.) Thus, the knowledge extractor can be equivalently modified to be the same construction but with the measurement of the register $\mathcal{D}^{\otimes l}$ replaced with that of corresponding message registers. We refer to this latter construction as the modified knowledge extractor.

Now we are ready to apply Theorem 3 with $N = 2$, $t = 2$, and l polynomially bounded. By its Item 1, the probability that the modified knowledge extractor will not abort before Step 8 differs from that of the same construction but without measurements of message registers up to an additive factor $O(\sqrt{\epsilon} l)$. Hence, the modified knowledge extractor will not abort before Step 8 with probability at least $1/(2p^3) - O(\sqrt{\epsilon} l)$. Further, by Item 2, the modified knowledge extractor will not abort in Step 8 with probability at most $O(\epsilon l)$. Putting it together, the modified knowledge extractor, in turn the (original) knowledge extractor, will output a Hamiltonian cycle with probability at least $1/(2p^3) - O(\sqrt{\epsilon} l) - O(\epsilon l) \geq 1/(3p^3)$. ■

10.4 Guaranteed extraction via a new quantum rewinding technique

In cryptographic applications, proof/argument-of-knowledge is often used as a building block of larger protocols, e.g. [FS90], where the *guaranteed extraction* is desired. However, the success probability of the knowledge extraction that we obtained is only guaranteed *non-negligible* (Theorem 6), which is insufficient. We note that in the classical setting, two definitions of proof/argument-of-knowledge, i.e. the one which we extend (following [Unr12, Unr16b]) to the quantum setting at the beginning of Subsection 10.2 and the one with guaranteed extraction, are actually equivalent [Gol01, Section 4.7]. However, the classical proof for the former definition implying the latter does not extend to the quantum setting straightforwardly; this is due to the general impossibility of quantum rewinding.

In spite of this, we believe that the new quantum rewinding technique recently developed [CMSZ21, LMS21], which builds on [MW05], can be used here to achieve the guaranteed extraction. In particular, the second variant of Blum's protocol present in the previous subsection can be shown argument-of-knowledge with *negligible* knowledge error, in that given any prover who can convince the verifier to accept with non-negligible probability, there exists a knowledge extractor running in the *coherent-runtime expected polynomial time* (in the sense given in [LMS21], i.e. EQPT_c) that can output a witness (i.e. a Hamiltonian cycle) almost sure.

To see this, the construction of the knowledge extractor will be almost the same as that in the post-quantum setting [LMS21] with $k = 2$,[40] except that now non-interactive quantum commit-

[40] The parallelization of (variants of) Blum's protocol satisies the 2-special soundness property as introduced in

ments will be used as the drop-in replacement of post-quantum collapse-binding commitments. The analysis will also be almost the same as the post-quantum analysis, except that now we can apply the parallel-and-sequential collapse binding property (Definition 10) directly: the hybrid argument for applying the collapse-binding property multiple times in the post-quantum security analysis will be hidden in our proof of Theorem 3. As a result, now the failure probability of the extraction will be expressed in terms of the unique-message binding (as opposed to the collapse-binding) error of commitments; in particular, performing measurements (for the purpose of the extraction) will only introduce an *additive* error that is the unique-message-binding error multiplied by some polynomial of *constant* degree (Theorem 3), which is still negligible.

However, even with guaranteed extraction, it is still unknown whether the Feige-Shamir construction [FS90] instantiated with a generic non-interactive quantum bit commitment scheme can be proven quantum zero-knowledge. The *difficulty* was firstly observed in the *post-quantum* setting [LMS21] that also extends to the quantum setting: the verifier (who plays the role of the prover in argument-of-knowledge) may use *different* witness in different folds of the parallel repetition of the atomic (variant of) Blum's protocol. Hence, the measurement of the witness may collapse the quantum state noticeably. For the purpose of *state-preserving* extraction, authors of [LMS21] tweaks the argument-of-knowledge construction, but at the cost of introducing *super-polynomial* complexity assumptions. Unfortunately, this tweak fails completely for quantum commitments.

Anyway, for languages in **UP**, one still can follow the template as given in [LMS21] to obtain a state-preserving extraction from the guaranteed extraction when quantum commitments are used. And with this state-preserving extraction, the Feige-Shamir construction instantiated with non-interactive quantum commitments can be shown secure.

11 A stronger quantum indistinguishability compatible with quantum rewinding

The typical indistinguishability of two quantum states is against adversaries who do *not* have access to the rest system which may be entangled with the quantum state to distinghuish. However, it turns out that in some applications, e.g. the Goldreich-Kahan construction of constant-round zero-knowledge proofs [GK96] instiantiated with quantum commitments, this indistinguishability is not sufficient for establishing the security. Instead, we need to establish a stronger quantum indistinguishability against adversaries who are even given oracle access to the binary measurement induced by the *projection* onto an arbitrary purification of the given quantum state to distinguish.

In this section, for our cryptographic purpose we prove the following lemma, which can be viewed as the extension of a similar result in the *post-quantum* setting [LMS21]. However, our proof will use a completely different strategy than that in the post-quantum analysis. In greater detail, our proofs combine a hardness-conversion theorem (Theorem 7, as stated immediately after Lemma 13) with the useless oracle lemma (Lemma 6) established before.

Lemma 13 *Let $|\phi_0\rangle$ and $|\phi_1\rangle$ be two arbitrary (not necessarily efficiently preparable) unit vectors of the Hilbert space induced by a joint quantum system $(\mathcal{X}, \mathcal{Y})$. The unitary operation G_b ($b = 0, 1$) performs on registers $(\mathcal{X}, \mathcal{Y})$ and a qubit $\mathcal{E}$ such that*

$$G_b \overset{def}{=} |\phi_b\rangle\langle\phi_b|^{\mathcal{X}\mathcal{Y}} \otimes X^{\mathcal{E}} + (\mathbb{1} - |\phi_b\rangle\langle\phi_b|^{\mathcal{X}\mathcal{Y}}) \otimes \mathbb{1}^{\mathcal{E}},$$

where $X^{\mathcal{E}}$ denotes the Pauli-X operator performed on the qubit $\mathcal{E}$. If there exists a non-uniform QPT oracle distinguisher D^{G_b} achieving the advantage ϵ and such that:

[LMS21].

1. *It uses some quantum advice $|\tau\rangle$ and calls the oracle G_b at most t times;*

2. *It has direct access to the register $\mathcal{X}$ and the qubit $\mathcal{E}$, but only oracle access (through G_0 or G_1) to the register $\mathcal{Y}$.*

That is,

$$\Big|\Pr[\mathsf{D}^{G_0}(|\phi_0\rangle^{\mathcal{X}\mathcal{Y}}|0\rangle^{\mathcal{E}}|\tau\rangle^{\mathcal{Z}})=1]-\Pr[\mathsf{D}^{G_1}(|\phi_1\rangle^{\mathcal{X}\mathcal{Y}}|0\rangle^{\mathcal{E}}|\tau\rangle^{\mathcal{Z}})=1]\Big|>2\epsilon.$$

Then there exists another non-uniform QPT distinguisher D' with just the direct access to the register $\mathcal{X}$ such that

$$\big|\Pr[\mathsf{D}'(\mathrm{Tr}_{\mathcal{Y}}(|\phi_0\rangle\langle\phi_0|)\otimes|\tau'\rangle\langle\tau'|)=1]-\Pr[\mathsf{D}'(\mathrm{Tr}_{\mathcal{Y}}(|\phi_1\rangle\langle\phi_1|)\otimes|\tau'\rangle\langle\tau'|)=1]\big|>\epsilon^2/(32t^4),$$

where the quantum advice $|\tau'\rangle$ may correlate with $|\tau\rangle, |\phi_0\rangle$ and $|\phi_1\rangle$.

The theorem below can be viewed as rephrasing an extension of the flavor-conversion of canonical quantum bit commitments [HMY22b].

Theorem 7 (Hardness conversion) *Given a pair of quantum states $(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{X}\mathcal{Y}}, |1\rangle^{\mathcal{B}}|\phi_1\rangle^{\mathcal{X}\mathcal{Y}})$ of a joint quantum system $(\mathcal{B},\mathcal{X},\mathcal{Y})$, where $\mathcal{B}$ is a single qubit and quantum states $|\phi_0\rangle$ and $|\phi_1\rangle$ may be neither orthogonal nor efficiently preparable, its dual pair*[41] *is given by $(|\psi_0\rangle, |\psi_1\rangle)$ such that*

$$|\psi_0\rangle \overset{def}{=} \frac{1}{\sqrt{2}}\big(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{X}\mathcal{Y}}+|1\rangle^{\mathcal{B}}|\phi_1\rangle^{\mathcal{X}\mathcal{Y}}\big),\qquad |\psi_1\rangle \overset{def}{=} \frac{1}{\sqrt{2}}\big(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{X}\mathcal{Y}}-|1\rangle^{\mathcal{B}}|\phi_1\rangle^{\mathcal{X}\mathcal{Y}}\big).$$

We have:

1. *If there exists a QPT transformer T, possibly using some quantum advice $|\tau\rangle$ that is stored in the register $\mathcal{Z}$, who performs on registers $(\mathcal{X},\mathcal{Z})$ and achieves*

   $$\big\|(|\psi_1\rangle\langle\psi_1|)^{\mathcal{B}\mathcal{X}\mathcal{Y}}T^{\mathcal{X}\mathcal{Z}}\big(|\psi_0\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}|\tau\rangle^{\mathcal{Z}}\big)\big\|\geq\epsilon,$$

   then there exists another QPT distinguisher D who uses the same quantum state $|\tau\rangle$, together with another state stored in the register $\mathcal{Z}'$ that is disentangled from but correlated with $|\tau\rangle$ as advice, performs on registers $(\mathcal{X},\mathcal{Z},\mathcal{Z}')$, and makes a single oracle access to both the unitary transformation ctrl-ctrl-T and its inverse ctrl-ctrl-$T^\dagger$, such that it can distinguish $\mathrm{Tr}_{\mathcal{Y}}(|\phi_0\rangle\langle\phi_0|)$ and $\mathrm{Tr}_{\mathcal{Y}}(|\phi_1\rangle\langle\phi_1|)$ with advantage at least $\epsilon^2/8$.

2. *Conversely, if there exists a QPT distinguisher D, possibly using some quantum advice $|\tau\rangle$ that is stored in the register $\mathcal{Z}$, who can distinguish $\mathrm{Tr}_{\mathcal{Y}}(|\phi_0\rangle\langle\phi_0|)$ and $\mathrm{Tr}_{\mathcal{Y}}(|\phi_1\rangle\langle\phi_1|)$ with advantage η, then there exists another QPT transformer T who uses a quantum advice $|\tau'\rangle$ with the same size as $|\tau\rangle$ that is stored in the register $\mathcal{Z}$, performs on registers $(\mathcal{X},\mathcal{Z})$, makes a single oracle access to both D (i.e. the unitary operator induced by the unitary part of the distinguisher D) and its inverse $D^\dagger$, such that*

   $$\big\|(|\psi_1\rangle\langle\psi_1|)^{\mathcal{B}\mathcal{X}\mathcal{Y}}T^{\mathcal{X}\mathcal{Z}}\big(|\psi_0\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}|\tau'\rangle^{\mathcal{Z}}\big)\big\|\geq 2\eta.$$

[41] We call it "dual pair" is seeing from the hiding-binding duality observed in [GJMZ22].

Note that

$$|0\rangle|\phi_0\rangle = \frac{1}{\sqrt{2}}\big(|\psi_0\rangle^{\mathcal{BXY}} + |\psi_1\rangle^{\mathcal{BXY}}\big), \qquad |1\rangle|\phi_1\rangle = \frac{1}{\sqrt{2}}\big(|\psi_0\rangle^{\mathcal{BXY}} - |\psi_1\rangle^{\mathcal{BXY}}\big).$$

The two items above also hold if we exchange the role of $(|0\rangle|\phi_0\rangle, |1\rangle|\phi_1\rangle)$ *and* $(|\psi_0\rangle, |\psi_1\rangle)$*, and that of registers* $\mathcal{X}$ *and* $(\mathcal{B}, \mathcal{Y})$*.*

The proof of the hardness-conversion theorem above is moved to Appendix B. Now we are ready to prove Lemma 13 using this theorem.

Proof: Define the projector

$$\Pi = (|0\rangle\langle 0|)^{\mathcal{B}} \otimes |\phi_0\rangle\langle\phi_0|^{\mathcal{XY}} + (|1\rangle\langle 1|)^{\mathcal{B}} \otimes |\phi_1\rangle\langle\phi_1|^{\mathcal{XY}}. \tag{29}$$

Introduce the unitary

$$G = (|0\rangle\langle 0|)^{\mathcal{B}} \otimes G_0^{\mathcal{XYE}} + (|1\rangle\langle 1|)^{\mathcal{B}} \otimes G_1^{\mathcal{XYE}} = \Pi^{\mathcal{BXY}} \otimes X^{\mathcal{E}} + (\mathbb{1} - \Pi)^{\mathcal{BXY}} \otimes \mathbb{1}^{\mathcal{E}}.$$

Now we use the oracle G to replace oracles G_0, G_1 used in the assumption of the lemma, obtaining

$$\left|\Pr[\mathsf{D}^G(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{XY}}|0\rangle^{\mathcal{E}}|\tau\rangle^{\mathcal{Z}}) = 1] - \Pr[\mathsf{D}^G(|1\rangle^{\mathcal{B}}|\phi_1\rangle^{\mathcal{XY}}|0\rangle^{\mathcal{E}}|\tau\rangle^{\mathcal{Z}}) = 1]\right| > 2\epsilon.$$

That is, the distinghuisher D, with oracle access to G but without direct access to registers $(\mathcal{B}, \mathcal{Y})$, can distinguish quantum states $\mathrm{Tr}_{\mathcal{Y}}(|\phi_0\rangle\langle\phi_0|)$ and $\mathrm{Tr}_{\mathcal{Y}}(|\phi_1\rangle\langle\phi_1|)$ with advantage at least ϵ.

Now we are ready to apply Item 2 of Theorem 7. Specifically, by replacing $|\phi_0\rangle$, $|\phi_1\rangle$, and $|\tau\rangle$ in Theorem 7 with $|\phi_0\rangle$, $|\phi_1\rangle$ and $|\tau\rangle$ here, respectively, it follows that there exists a non-uniform QPT transformer T that does not have direct access to registers $(\mathcal{B}, \mathcal{Y})$ and uses some quantum advice $|\tau_1\rangle$ such that

$$\|(|\psi_1\rangle\langle\psi_1|)^{\mathcal{BXY}}(T^G)^{\mathcal{XZ}}(|\psi_0\rangle^{\mathcal{BXY}}|0\rangle^{\mathcal{E}}|\tau_1\rangle^{\mathcal{Z}})\| > \epsilon, \tag{30}$$

where

$$\begin{aligned}
|\psi_0\rangle &\overset{def}{=} \frac{1}{\sqrt{2}}\big(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{XY}} + |1\rangle^{\mathcal{B}}|\phi_1\rangle^{\mathcal{XY}}\big),\\
|\psi_1\rangle &\overset{def}{=} \frac{1}{\sqrt{2}}\big(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{XY}} - |1\rangle^{\mathcal{B}}|\phi_1\rangle^{\mathcal{XY}}\big).
\end{aligned}$$

Moreover, note that the transformer T calls the oracle G at most $2t$ times: it makes a single oracle access to the unitary D that is the unitary part of the distinghuisher and that to its inverse $D^\dagger$, which calls G and $G^\dagger$ at most t times, respectively. But note that $G = G^\dagger$, the transformer T calls the oracle G at most $2t$ times.

Now we introduce two more projectors to simplify the notation:

$$\Pi_0 \overset{def}{=} |\psi_0\rangle\langle\psi_0|, \qquad \Pi_1 \overset{def}{=} |\psi_1\rangle\langle\psi_1|.$$

It is easy to check that $\Pi = \Pi_0 + \Pi_1$, where the expression of Π is given in Eq. (29). Moreover, the unitary T^G can be written in the form $(UG)^{2t}$ for some QPT unitary U performing on registers $(\mathcal{X}, \mathcal{Z}, \mathcal{E})$. Hence, Inequality (30) can be rewritten as

$$\|\Pi_1(UG)^{2t}\Pi_0(|\psi_0\rangle|0\rangle|\tau_1\rangle)\| > 2\epsilon.$$

Now we are ready to apply Lemma 6. Specifically, replacing Π_0, Π_1, Π_2, G_0, and G_1 in Lemma 6 with Π_0, Π_1, 0, X and X here, respectively, where X performs on the qubit $\mathcal{E}$, we have

$$\|\Pi_1 U^q \Pi_0 |\tau_2\rangle^{\mathcal{BXYEZ}}\| > \frac{\epsilon}{2t^2}$$

for some $0 \leq q \leq 2t$ and sub-normalized vector $|\tau_2\rangle$ (which is correlated with $|\tau_1\rangle$). Rewriting $\Pi_0 |\tau_2\rangle$ as $|\psi_0\rangle |\tau_3\rangle$, it becomes

$$\|(|\psi_1\rangle \langle\psi_1|)^{\mathcal{BXY}}(U^{\mathcal{XZE}})^q(|\psi_0\rangle^{\mathcal{BXY}} |\tau_3\rangle^{\mathcal{EZ}})\| > \frac{\epsilon}{2t^2}.$$

Now apply Item 1 of Theorem 7, there exists a non-uniform QPT distinguisher who uses some quantum advice $|\tau'\rangle$ that is correlated with $|\tau_3\rangle$, $|\psi_0\rangle$ and $|\psi_1\rangle$, in turn $|\tau\rangle$, $|\phi_0\rangle$ and $|\phi_1\rangle$, and can distinguish quantum states $\mathrm{Tr}_{\mathcal{Y}}(|\phi_0\rangle \langle\phi_0|)$ and $\mathrm{Tr}_{\mathcal{Y}}(|\phi_1\rangle \langle\phi_1|)$ with advantage at least $\epsilon^2/(32t^4)$. ■

11.1 Application in quantum security analysis of the Goldreich-Kahan construction

In this subsection, we sketch how to prove that the Goldreich-Kahan construction of constant-round quantum computational zero-knowledge proofs for **NP** [GK96] instantiated with canonical quantum bit commitments is secure.[42] In particular, we will show how to adapt the security analysis for post-quantum zero-knowledge in [LMS21] to that in the quantum setting by using Lemma 13.

We first sketch the Goldreich-Kahan protocol that is adapted from [LMS21]. Suppose that L is an **NP** language and $x \in L$ is a common input to both the prover and the verifier; w is a witness for $x \in L$ that is given to the prover as a private input. Let Σ_L be a quantum Σ-protocol for the language L,[43] whose three messages can be described by a triple $(\mathcal{A}, r, \mathcal{Z})$, where registers $\mathcal{A}$ and $\mathcal{Z}$ contain the prover's first and second (quantum) messages, respectively. For example, Σ_L could be the parallelized Blum's protocol instantiated with statistically-binding canonical quantum bit commitments.[44] The Goldreich-Kahan protocol proceeds as follows:

V1 The verifier commits to a uniformly random string r using statistically-hiding canonical quantum bit commitments in a bitwise fashion.

P1 The prover sends the register $\mathcal{A}$ to the verifier.

V2 The verifier opens its commitments as r that will be treated as the challenge to the prover.

P2 The prover sends the register $\mathcal{Z}$ to the verifier as the response to $(\mathcal{A}, r)$.

[42] We point out that general non-interactive quantum bit commitments (Definition 2) work equally well here, like in Section 10 and Appendix C. Here, we restrict to consider canonical quantum bit commitments for two reasons: First, in the statement of Theorem 2, we want to highlight that the security of the Goldreich-Kahan construction can be based on the minimum complexity assumption for computational quantum cryptography. Second, the statistical soundness of the construction will become straightforward using the analysis framework in [FUYZ22] when canonical statistically-binding quantum bit commitments are used (by the prover).

[43] Quantum Σ-protocols generalize Σ-protocols (in the common sense) by allowing the prover's two messages to be quantum.

[44] Actually, to use Blum's protocol, in the first place we have to reduce the language L to the **NP**-complete language Hamiltonian Cycle using some witness-preserving Karp-reduction [Gol01]. Moreover, for the purpose of just proving the statistical soundness, there is no need to use the extraction property (or strict soundness) of general Σ protocols. Thus, using Blum's original atomic protocol (as opposed to variants introduced in Section 10) will be sufficient here.

V3 The verifier checks that the triple $(\mathcal{A}, r, \mathcal{Z})$ will convince the verifier of the protocol Σ_L to accept.

The (statistical) soundness of the Goldreich-Kahan protocol is easy: the verifier's commitments (sent in Step V1) are statistically hiding, which only leak negligible information about its challenge r. Then using the analysis framework in [FUYZ22], one can lift the statistical soundness when post-quantum statistically-binding quantum bit commitments are used to the current quantum setting.

In the remainder of this subsection, we focus on how to prove quantum zero-knowledge. In particular, we show how to modify the post-quantum analysis elaborated in [LMS21, Section 2.4] to the quantum setting. We recommend readers to first read their exposition to get a general idea of the analysis; our presentation below will be based on their exposition and also inherit notations introduced there.

The simulator we construct here will be almost identical to the one in [LMS21], except that it will be modified correspondingly to satisfy the syntax of canonical quantum bit commitments. To prove the correctness of the simulator, we will also introduce the same two hybrids as in [LMS21].

To show that the original simulator is indistinguishable from the first hybird, we need to prove that quantum states $|\mathsf{Sim}_0\rangle$ and $|P\rangle$ *remain* indistinguishable given just the reduced quantum states of the sub-register $\mathcal{A}$ (i.e. the register containing the prover's first message in Step P1 of the protocol), even after operations taken within Step 4*(a). Here, $|\mathsf{Sim}_0\rangle$ denotes the quantum state generated by running the honest-verifier simulator of the protocol Σ_L w.r.t. the challenge all 0's, and $|P\rangle$ denotes the quantum state generated by running the honest prover. However, the desired indistinguishability does not follow immediately from that quantum states $|\mathsf{Sim}_0\rangle$ and $|P\rangle$ are indistinguishable (in the common sense) w.r.t. the sub-register $\mathcal{A}$ at the beginning. This is because operations in Step 4*(a) include (the unitary simulation of) the binary measurement induced by *projections* (hidden in the corresponding big unitary U) on $|\mathsf{Sim}_0\rangle$ (for the simulator) or $|P\rangle$ (for the first hybrid) that are introduced by quantum rewinding. Note that these two projections allow the distinghuisher to access registers beyond the sub-register $\mathcal{A}$ (but in a very restricted way).

Hence, we need to prove that quantum states $|\mathsf{Sim}_0\rangle$ and $|P\rangle$ are indistinguishable w.r.t. the sub-register $\mathcal{A}$ even the distinghuisher is allowed to access binary measurements induced by projections on $|\mathsf{Sim}_0\rangle$ and $|P\rangle$, respectively. This is where our Lemma 13 comes in. In greater detail, to apply Lemma 13, we just replace quantum states $|\phi_0\rangle, |\phi_1\rangle$ in the lemma with $|\mathsf{Sim}_0\rangle$ and $|P\rangle$ here, respectively; replace the register $\mathcal{X}$ in the lemma with the register $\mathcal{A}$, and the register $\mathcal{Y}$ there with the rest of the system; correspondingly, G_0, G_1 in the lemma will be replaced with the unitary simulation of binary measurements induced by projections on $|\mathsf{Sim}_0\rangle$ and $|P\rangle$, respectively.

We point out that there is a subtlety here in applying Lemma 13: there are *multiple* binary measurements within the big unitary U (i.e. the operation taken in Step 4*(a)); and all their outcomes are needed to be recorded. However, in the statement of Lemma 13, there is only a *single* qubit $\mathcal{E}$ provided to record the measurement outcome. Actually, this is not a big issue: after each measurement, the outcome stored in the qubit $\mathcal{E}$ can be swapped out for a possible later use; and this swap operation can be incorporated into the unitary U. (Note that this situation is very similar to that is considered in defining reversible multi-verification unique-message binding. Refer to remarks immediately after Definition 6.)

Showing that the first hybrid and the second hybrid are indistinguishable is similar, only this time we need to show that quantum states $|\mathsf{Sim}_{r'}\rangle$ and $|P_{r'}\rangle$ are indistinguishable w.r.t. the sub-registers $(\mathcal{A}, \mathcal{Z})$ even the distinghuisher is allowed to access binary measurements induced by projections on $|\mathsf{Sim}_{r'}\rangle$ and $|P_{r'}\rangle$, respectively. Here, $|\mathsf{Sim}_{r'}\rangle$ denotes the quantum state generated by running the honest-verifier simulator of the protocol Σ_L w.r.t. the challenge r', and $|P_{r'}\rangle$ denotes the quantum state generated by running the honest prover with its response to the challenge r' contained in the register $\mathcal{Z}$. This will guarantee that even after operations taken within Step 4*(c) (in which projections on $|\mathsf{Sim}_{r'}\rangle$ or $|P_{r'}\rangle$ are hidden inside the big unitary $U^\dagger$), quantum states $|\mathsf{Sim}_{r'}\rangle$ and $|P_{r'}\rangle$ remain indistinguishable w.r.t. the sub-registers $(\mathcal{A}, \mathcal{Z})$ (i.e. registers containing prover's two messages sent in Step P1 and Step P2 of the protocol, respectively). To this end, we can apply Lemma 13 in a similar way as discussed above. In greater detail, we just replace quantum states $|\phi_0\rangle, |\phi_1\rangle$ in Lemma 13 with $|\mathsf{Sim}_{r'}\rangle$ and $|P_{r'}\rangle$ here, respectively; replace the register $\mathcal{X}$ in the lemma with registers $(\mathcal{A}, \mathcal{Z})$, and the register $\mathcal{Y}$ there with the rest of the system; correspondingly, G_0, G_1 in the lemma will be replaced with the unitary simulation of binary measurements induced by projections on $|\mathsf{Sim}_{r'}\rangle$ and $|P_{r'}\rangle$, respectively.

12 Conclusion and open problems

In this work, we propose a definition of collapse binding w.r.t. *general* non-interactive quantum commitments (Definition 8), which is compatible with quantum rewinding and as useful as its post-quantum counterpart in cryptographic applications (Section 10, Appendix C). This collapse binding is provably equivalent to unique-message binding (Theorem 1), which in particular implies that canonical quantum bit commitments are collapse binding.

Additionally, we rephrase the flavor conversion of canonical quantum bit commitments as a hardness conversion, which can be used to prove a stronger quantum indistinguishability that is compatible with quantum rewinding (Lemma 13). This indistinguishability is found useful in constructing constant-round quantum computational zero-knowledge proofs for **NP** (Theorem 2).

Two main questions left open by this work are on the extension of our equivalence theorem: can it extend to more general *interactive* quantum commitments? Can the restriction on the message space (i.e. polynomially bounded) in our equivalence theorem be removed?

Acknowledgement. We first thank Dominique Unruh for the decade-long discussion on quantum binding; it is Dominique's insight that virtually all security analysis based on quantum binding make essential use of collapse-binding that inspires this work. We thank Alex Lombardi, Fermi Ma, and Nicholas Spooner for patiently explaining to us how to apply the collapse-binding property in the security analysis of their astonishing paper [LMS21]; their feedback to an early draft of this paper is also valuable. We thank Marcel Dall'Agnol and Nicholas Spooner for clarifying a technical detail within their proof of Lemma 9. Thanks also go to Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa for the inspiring discussion on rephrasing the flavor conversion of canonical quantum bit commitments as the hardness conversion and related topics.

References

[Aar16] Scott Aaronson. The complexity of quantum states and transformations: From quantum money to black holes. *arXiv:1607.05256*, 2016. 4

[AAS20] Scott Aaronson, Yosi Atia, and Leonard Susskind. On the hardness of detecting macroscopic superpositions. *Electron. Colloquium Comput. Complex.*, TR20-146, 2020. 17, 66

[AQY21] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. Cryptology ePrint Archive, Report 2021/1663, 2021. https://ia.cr/2021/1663. 5, 19

[ARU14] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *FOCS*, pages 474–483, 2014. 5, 6

[BB21] Nir Bitansky and Zvika Brakerski. Classical binding for quantum commitments. In Kobbi Nissim and Brent Waters, editors, *TCC*, volume 13042 of *Lecture Notes in Computer Science*, pages 273–298. Springer, 2021. 4

[BBCS91] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In *CRYPTO*, pages 351–366, 1991. 5

[BCQ22] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. Cryptology ePrint Archive, Paper 2022/1181, 2022. https://eprint.iacr.org/2022/1181. 4, 5, 11

[BEM$^+$23] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. Unitary complexity and the uhlmann transformation problem, 2023. 4

[Blu83] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *ACM SIGACT News*, 15(1):23–27, 1983. 4

[Blu86] Manuel Blum. How to prove a theorem so no one else can claim it. In *Proceedings of the International Congress of Mathematicians*, volume 1, page 2, 1986. 4, 5, 13

[Bra22] Zvika Brakerski. Black-hole radiation decoding is quantum cryptography, 2022. 4

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *FOCS*, pages 42–52, 1988. 5

[CMSZ21] Alessandro Chiesa, Fermi Ma, Nicholas Spooner, and Mark Zhandry. Post-quantum succinct arguments: Breaking the quantum rewinding barrier. In *FOCS*, pages 49–58. IEEE, 2021. 5, 6, 7, 8, 9, 10, 12, 13, 53

[Cré94] Claude Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, 1994. 5

[CX22] Shujiao Cao and Rui Xue. The gap is sensitive to size of preimages: Collapsing property doesn't go beyond quantum collision-resistance for preimages bounded hash functions. In *CRYPTO 2022*, volume 13509 of *Lecture Notes in Computer Science*, pages 564–595. Springer, 2022. 11, 15, 33

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

[DS23] Marcel Dall'Agnol and Nicholas Spooner. On the necessity of collapsing for post-quantum and quantum commitments. In *TQC*, volume 266 of *LIPIcs*, pages 2:1–2:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023. 5, 6, 7, 9, 10, 11, 15, 33

[FS90] Uriel Feige and Adi Shamir. Witness indistinguishable and witness hiding protocols. In *STOC*, pages 416–426, 1990. 6, 13, 53, 54

[FUYZ22] Junbin Fang, Dominique Unruh, Jun Yan, and Dehua Zhou. How to base security on the perfect/statistical binding property of quantum bit commitment? In Sang Won Bae and Heejin Park, editors, *33rd International Symposium on Algorithms and Computation, ISAAC 2022, December 19-21, 2022, Seoul, Korea*, volume 248 of *LIPIcs*, pages 26:1–26:12. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. https://ia.cr/2020/621. 4, 5, 6, 7, 8, 9, 11, 13, 18, 19, 21, 29, 50, 57, 58

[GJMZ22] Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. Commitments to quantum states. Cryptology ePrint Archive, Paper 2022/1358, 2022. https://eprint.iacr.org/2022/1358. 2, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15, 25, 28, 37, 55, 63, 66

[GK96] Oded Goldreich and Ariel Kahan. How to construct constant-round zero-knowledge proof systems for NP. *J. Cryptol.*, 9(3):167–190, 1996. 6, 8, 13, 54, 57

[GLSV21] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT*, volume 12697 of *Lecture Notes in Computer Science*, pages 531–561. Springer, 2021. 4

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991. 4, 13, 68

[Gol01] Oded Goldreich. *Foundations of Cryptography, Basic Tools*, volume I. Cambridge University Press, 2001. 4, 13, 53, 57

[HHRS07] Iftach Haitner, Jonathan J. Hoch, Omer Reingold, and Gil Segev. Finding collisions in interactive protocols - a tight lower bound on the round complexity of statistically-hiding commitments. In *FOCS*, pages 669–679, 2007. 8

[HMY22a] Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. Private communication, 2022. 13

[HMY22b] Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. From the hardness of detecting superpositions to cryptography: Quantum public key encryption and commitments. Cryptology ePrint Archive, Paper 2022/1375, 2022. https://eprint.iacr.org/2022/1375. 4, 8, 13, 14, 17, 55, 66, 67, 68

[HNO$^+$09] Iftach Haitner, Minh-Huyen Nguyen, Shien Jin Ong, Omer Reingold, and Salil P. Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM J. Comput.*, 39(3):1153–1218, 2009. 8

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

[Imp95] Russell Impagliazzo. A personal view of average-case complexity. In *Proceedings of the Tenth Annual Structure in Complexity Theory Conference, Minneapolis, Minnesota, USA, June 19-22, 1995*, pages 134–147. IEEE Computer Society, 1995. 4

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

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

[KQST22] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. *CoRR*, abs/2212.00879, 2022. 4

[Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. In Min-Hsiu Hsieh, editor, *TQC*, volume 197 of *LIPIcs*, pages 2:1–2:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. 4

[KSV02] Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation, volume 47 of Graduate Studies in Mathematics.* American Mathematical Society, 2002. 16

[LC98] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1):177–187, 1998. 4

[LMS21] Alex Lombardi, Fermi Ma, and Nicholas Spooner. Post-quantum zero knowledge, revisited (or: How to do quantum rewinding undetectably). Cryptology ePrint Archive, Report 2021/1543, 2021. https://ia.cr/2021/1543. 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 19, 20, 31, 53, 54, 57, 58, 59

[LMS23] Alex Lombardi, Fermi Ma, and Nicholas Spooner. Private communication, 2023. 5, 8, 15

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

[MW05] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005. 8, 13, 53

[MY21] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. 2021. https://ia.cr/2021/1691. 4

[MY22] Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. Cryptology ePrint Archive, Paper 2022/1336, 2022. https://eprint.iacr.org/2022/1336. 4

[MY23] Tony Metger and Henry Yuen. stateqip = statepspace, 2023. 4

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and Quantum Informatioin.* Cambridge University Press, 2000. 16, 17

[NOVY98] Moni Naor, Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. Perfect zero-knowledge arguments for NP using any one-way permutation. *J. Cryptology*, 11(2):87–108, 1998. 8

[Reg06] Oded Regev. Witness-preserving amplification of QMA, 2006. Lecture notes of course Quantum Computation. 68

[Unr12] Dominique Unruh. Quantum proofs of knowledge. In *EUROCRYPT*, pages 135–152, 2012. 5, 13, 18, 37, 49, 50, 53

[Unr16a] Dominique Unruh. Collapse-binding quantum commitments without random oracles. In *ASIACRYPT*, pages 166–195, 2016. 6, 28

[Unr16b] Dominique Unruh. Computationally binding quantum commitments. In *EUROCRYPT 2016*, pages 497–527, 2016. 5, 6, 7, 8, 9, 10, 12, 13, 15, 28, 37, 49, 50, 53

[Unr22] Dominique Unruh. Private communication, 2022. 6

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

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. 5

[Wat18] John Watrous. *Theory of Quantum Information.* Cambridge University Press, 2018. 17

[Yam22] Takashi Yamakawa. Private communication, 2022. 8, 13

[Yan21] Jun Yan. Quantum computationally predicate-binding commitments with application in quantum zero-knowledge arguments for NP. In *ASIACRYPT 2021*, volume 13090 of *Lecture Notes in Computer Science*, pages 575–605. Springer, 2021. 4, 5, 6, 7, 8, 9, 10, 11, 47

[Yan22] Jun Yan. General properties of quantum bit commitments (extended abstract). In *ASIACRYPT 2022*, volume 13794 of *Lecture Notes in Computer Science*, pages 628–657. Springer, 2022. The full version is referred to https://eprint.iacr.org/2020/1488. 4, 5, 7, 10, 11, 12, 14, 20

[YWLQ15] Jun Yan, Jian Weng, Dongdai Lin, and Yujuan Quan. Quantum bit commitment with application in quantum zero-knowledge proof (extended abstract). In *ISAAC*, pages 555–565, 2015. 4, 5, 9, 18

[Zha22] Mark Zhandry. New constructions of collapsing hashes. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part III*, volume 13509 of *LNCS*, pages 596–624. Springer, Heidelberg, August 2022. 6, 11, 15, 33

A A proof of Lemma 6

Our proof of is adapted from that of Lemma 6.8 in [GJMZ22] with minor modifications.

Lemma 14 (A restatement of Lemma 6) *Fix a unitary U, a state $|\tau\rangle$, and a triple of orthogonal projectors Π_0, Π_1, Π_2. Let $\Pi = \Pi_0 + \Pi_1 + \Pi_2$. Let G be a unitary of the form $G =$*

$\Pi_0 G_0 + \Pi_1 G_1 + \Pi_2 G_2 + (\mathbb{1} - \Pi)$, *where* G_0, G_1, G_2 *are unitaries that commute with* Π_0, Π_1, Π_2, *respectively. Define* $\tilde{G}_0 = \Pi_0 G_0 + \Pi_2 G_2 + (\mathbb{1} - \Pi_0 - \Pi_2)$ *and*

$$\epsilon(t) \overset{def}{=} \max_{\substack{r\in\{0,1\},\\ 0\le q,s\le t}} \|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^q \cdot \Pi_0(\tilde{G}_0)^r(U\tilde{G}_0)^s\Pi_0 \left|\tau\right\rangle \|$$

for all integers $t \ge 0$. *Then for all integers* $t \ge 0$,

$$\|\Pi_1(UG)^t\Pi_0 \left|\tau\right\rangle \| \le 4t^2 \cdot \epsilon(t).$$

Proof: The lemma follows immediately from two claims that will be proved subsequently by a simple triangle inequality:

$$\begin{aligned} \|\Pi_1(UG)^t\Pi_0 \left|\tau\right\rangle \| &\le \|\Pi_1(U\tilde{G}_0)^t\Pi_0 \left|\tau\right\rangle \| + 2t^2\epsilon(t) \qquad \text{(Claim 16)} \\ &\le 2t\cdot\epsilon(t) + 2t^2\epsilon(t) \qquad \text{(Claim 15)} \\ &\le 4t^2\cdot\epsilon(t). \end{aligned}$$

■

Claim 15 $\|\Pi_1(U\tilde{G}_0)^t\Pi_0 \left|\tau\right\rangle \| \le 2t \cdot \epsilon(t)$.

Proof: By the definition of $\tilde{G}_0$, we have

$$\begin{aligned} U\tilde{G}_0 &= U(\Pi_0 G_0 + \Pi_2 G_2 + \mathbb{1} - \Pi_0 - \Pi_2) \\ &= U(\Pi_2 G_2 + \mathbb{1} - \Pi_2) + U\Pi_0(G_0 - \mathbb{1}). \end{aligned}$$

Then $\Pi_1(U\tilde{G}_0)^t\Pi_0 \left|\tau\right\rangle$ can be written in the form:

$$\Pi_1(U\tilde{G}_0)^t\Pi_0 \left|\tau\right\rangle = \sum_{i=0}^{t} \Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^i \cdot F_{t-i}\Pi_0 \left|\tau\right\rangle, \tag{31}$$

where

$$F_i \overset{def}{=} \begin{cases} \mathbb{1} & i = 0, \\ U\Pi_0(G_0 - \mathbb{1})(U\tilde{G}_0)^{i-1}, & 1 \le i \le t. \end{cases}$$

To see this, note that $(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^i \cdot F_{t-i}$ is just the sum of the terms in the binomial expansion of $(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2) + U\Pi_0(G_0 - \mathbb{1}))^t$ that, when going from left to right, consist of exactly i times of $U(\Pi_2 G_2 + \mathbb{1} - \Pi_2)$'s before the first $U\Pi_0(G_0 - \mathbb{1})$.

We are next to bound the vector norm of each term in the summation on the right of Eq. (31); in particular, we are going to show that for each $0 \le i \le t$,

$$\left\|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^i \cdot F_{t-i}\Pi_0 \left|\tau\right\rangle\right\| \le 2\epsilon(t).$$

For the $i = t$ case, $F_0 = \mathbb{1}$. We have

$$\left\|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^t\Pi_0 \left|\tau\right\rangle\right\| \le \epsilon(t)$$

by the definition of the $\epsilon(t)$.

For any $i \leq t-1$ case, plugging in the expression of F_i, we have:

$$\begin{aligned}
& \left\|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^i \cdot F_{t-i}\Pi_0 \left|\tau\right\rangle\right\| \\
= & \left\|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^i U\Pi_0 G_0 (U\tilde{G}_0)^{t-i-1}\Pi_0 \left|\tau\right\rangle - \Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^i U\Pi_0 (U\tilde{G}_0)^{t-i-1}\Pi_0 \left|\tau\right\rangle\right\| \\
\leq & \left\|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^i U\Pi_0 G_0 (U\tilde{G}_0)^{t-i-1}\Pi_0 \left|\tau\right\rangle\right\| + \left\|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^i U\Pi_0 (U\tilde{G}_0)^{t-i-1}\Pi_0 \left|\tau\right\rangle\right\| \\
= & \left\|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^{i+1}\Pi_0 G_0 (U\tilde{G}_0)^{t-i-1}\Pi_0 \left|\tau\right\rangle\right\| \\
& + \left\|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^{i+1}\Pi_0 (U\tilde{G}_0)^{t-i-1}\Pi_0 \left|\tau\right\rangle\right\| \qquad \text{(using } (\Pi_2 G_2 + \mathbb{1} - \Pi_2)\Pi_0 = \Pi_0 \text{ since } \Pi_0\Pi_2 = 0) \\
\leq & \left\|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^{i+1}\Pi_0 G_0 (U\tilde{G}_0)^{t-i-1}\Pi_0 \left|\tau\right\rangle\right\| + \epsilon(t) \qquad \text{(by the definition of } \epsilon(t)) \\
= & \left\|\Pi_1(U(\Pi_2 G_2 + \mathbb{1} - \Pi_2))^{i+1}\Pi_0 \tilde{G}_0 (U\tilde{G}_0)^{t-i-1}\Pi_0 \left|\tau\right\rangle\right\| + \epsilon(t) \qquad \text{(using } \Pi_0 G_0 = \Pi_0\tilde{G}_0 \text{ since } \Pi_0\Pi_2 = 0) \\
\leq & 2\epsilon(t). \qquad \text{(by the definition of } \epsilon(t))
\end{aligned}$$

The claim follows immediately by the triangle inequality of the vector norm. ■

Claim 16 $\|(UG)^t\Pi_0 \left|\tau\right\rangle - (U\tilde{G}_0)^t\Pi_0 \left|\tau\right\rangle\| \leq 2t^2 \cdot \epsilon(t)$.

PROOF: We prove by induction on t. The case $t = 0$ is trivial.

When $t \geq 1$, we introduce the hybrid $UG \cdot (U\tilde{G}_0)^{t-1}\Pi_0 \left|\tau\right\rangle$. On one hand,

$$\begin{aligned}
\left\|(UG)^t\Pi_0 \left|\tau\right\rangle - UG \cdot (U\tilde{G}_0)^{t-1}\Pi_0 \left|\tau\right\rangle\right\| &= \left\|(UG)^{t-1}\Pi_0 \left|\tau\right\rangle - (U\tilde{G}_0)^{t-1}\Pi_0 \left|\tau\right\rangle\right\| \\
&\leq 2(t-1)^2 \cdot \epsilon(t-1),
\end{aligned}$$

where we use the induction hypothesis. On the other hand,

$$\begin{aligned}
& \left\|UG \cdot (U\tilde{G}_0)^{t-1}\Pi_0 \left|\tau\right\rangle - (U\tilde{G}_0)^t\Pi_0 \left|\tau\right\rangle\right\| \\
= & \left\|(UG - U\tilde{G}_0)(U\tilde{G}_0)^{t-1}\Pi_0 \left|\tau\right\rangle\right\| \\
= & \left\|(G_1 - \mathbb{1})\Pi_1(U\tilde{G}_0)^{t-1}\Pi_0 \left|\tau\right\rangle\right\| \\
\leq & 2\left\|\Pi_1(U\tilde{G}_0)^{t-1}\Pi_0 \left|\tau\right\rangle\right\| \qquad \text{(The triangle inequality w.r.t. the operator norm)} \\
\leq & 4(t-1) \cdot \epsilon(t-1). \qquad \text{(Claim 15)}
\end{aligned}$$

Using the triangle inequality,

$$\begin{aligned}
& \left\|(UG)^t\Pi_0 \left|\tau\right\rangle - (U\tilde{G}_0)^t\Pi_0 \left|\tau\right\rangle\right\| \\
\leq & \left\|(UG)^t\Pi_0 \left|\tau\right\rangle - UG \cdot (U\tilde{G}_0)^{t-1}\Pi_0 \left|\tau\right\rangle\right\| + \left\|UG \cdot (U\tilde{G}_0)^{t-1}\Pi_0 \left|\tau\right\rangle - (U\tilde{G}_0)^t\Pi_0 \left|\tau\right\rangle\right\| \\
\leq & 2(t-1)^2 \cdot \epsilon(t-1) + 4(t-1) \cdot \epsilon(t-1) \\
\leq & 2t^2 \cdot \epsilon(t). \qquad \text{(The function } \epsilon(\cdot) \text{ is increasing)}
\end{aligned}$$

This finishes the proof of the claim. ■

B A proof of the hardness-conversion Theorem

Before stating and proving the hardness-conversion theorem (Theorem 7), we first state a refinement of a technical lemma proved in [HMY22b] that can be viewed as an extension of the equivalence between swapping and distinghuishing established in [AAS20].

Lemma 17 (A refinement of Lemma 5.1 in [HMY22b]) *Let $|x\rangle, |y\rangle$ be orthogonal n-qubit states and $|\tau\rangle$ be an m-qubit state. Let U be a polynomial-time computable unitary over $(n+m)$-qubit states and define Γ as*

$$\Gamma \overset{def}{=} \|(\langle y| \otimes \mathbb{1}^{\otimes m})U|x\rangle|\tau\rangle + (\langle x| \otimes \mathbb{1}^{\otimes m})U|y\rangle|\tau\rangle\|.$$

Then, there exists a non-uniform QPT distinguisher A with advice $|\tau'\rangle \overset{def}{=} |\tau\rangle \otimes (|x\rangle|0\rangle + |y\rangle|1\rangle)/\sqrt{2}$ that distinguishes $|\psi\rangle \overset{def}{=} (|x\rangle + |y\rangle)/\sqrt{2}$ and $|\phi\rangle \overset{def}{=} (|x\rangle - |y\rangle)/\sqrt{2}$ with advantage $\Gamma^2/8$. Moreover, the distinghuisher A makes a single oracle access to both ctrl-U and ctrl-$U^\dagger$, and only acts on the n-qubit state via the oracle access to ctrl-U. (The oracle access to ctrl-$U^\dagger$ does not act on the n-quit state.)

Conversely, let $|\psi\rangle, |\phi\rangle$ be orthogonal n-qubit states, and suppose that a non-uniform QPT distinguisher A with an m-qubit advice $|\tau\rangle$ distinguishes $|\psi\rangle$ and $|\phi\rangle$ with advantage Δ without using additional ancilla qubits besides $|\tau\rangle$. Then, there exists a polynomial-time computable unitary U over $(n+m)$-qubit states such that

$$|\langle y|\langle\tau|U|x\rangle|\tau\rangle + \langle x|\langle\tau|U|y\rangle|\tau\rangle| = 4\Delta,$$

where $|x\rangle \overset{def}{=} (|\psi\rangle + |\phi\rangle)/\sqrt{2}$ and $|y\rangle \overset{def}{=} (|\psi\rangle - |\phi\rangle)/\sqrt{2}$. Moreover, U makes a single oracle access to both A and $A^\dagger$ (where recall that A is the uniary induced by the distinghuisher A) that act on the same quantum system, and U only acts on the n-qubit state via oracle accesses to A and $A^\dagger$.

Remark. We highlight that the definition of the distinguishing advantage we are using in this paper (Definition 1) is *half* of the one used in [HMY22b, AAS20].

The hardness-conversion theorem extends the flavor-conversion of canonical quantum bit commitments established in [HMY22b] and is rephrased in a way that is suitable for our application (Section 11).

Theorem 8 (A restatement of Theorem 7) *Given a pair of quantum states $(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{XY}}, |1\rangle^{\mathcal{B}}|\phi_1\rangle^{\mathcal{XY}})$ of a joint quantum system $(\mathcal{B}, \mathcal{X}, \mathcal{Y})$, where $\mathcal{B}$ is a single qubit and quantum states $|\phi_0\rangle$ and $|\phi_1\rangle$ may be neither orthogonal nor efficiently preparable, its dual pair*[45] *is given by $(|\psi_0\rangle, |\psi_1\rangle)$ such that*

$$|\psi_0\rangle \overset{def}{=} \frac{1}{\sqrt{2}}\big(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{XY}} + |1\rangle^{\mathcal{B}}|\phi_1\rangle^{\mathcal{XY}}\big), \qquad |\psi_1\rangle \overset{def}{=} \frac{1}{\sqrt{2}}\big(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{XY}} - |1\rangle^{\mathcal{B}}|\phi_1\rangle^{\mathcal{XY}}\big).$$

We have:

1. *If there exists a QPT transformer T, possibly using some quantum advice $|\tau\rangle$ that is stored in the register $\mathcal{Z}$, who performs on registers $(\mathcal{X}, \mathcal{Z})$ and achieves*

$$\big\|(|\psi_1\rangle\langle\psi_1|)^{\mathcal{BXY}}T^{\mathcal{XZ}}\big(|\psi_0\rangle^{\mathcal{BXY}}|\tau\rangle^{\mathcal{Z}}\big)\big\| \geq \epsilon,$$

[45] We call it "dual pair" is seeing from the hiding-binding duality observed in [GJMZ22].

then there exists another QPT distinguisher D *who uses the same quantum state* $|\tau\rangle$*, together with another state stored in the register* $\mathcal{Z}'$ *that is disentangled from but correlated with* $|\tau\rangle$ *as advice, performs on registers* $(\mathcal{X}, \mathcal{Z}, \mathcal{Z}')$*, and makes a single oracle access to both the unitary transformation ctrl-ctrl-T and its inverse ctrl-ctrl-*$T^\dagger$*, such that it can distinguish* $\mathrm{Tr}_{\mathcal{Y}}(|\phi_0\rangle\langle\phi_0|)$ *and* $\mathrm{Tr}_{\mathcal{Y}}(|\phi_1\rangle\langle\phi_1|)$ *with advantage at least* $\epsilon^2/8$*.*

2. *Conversely, if there exists a QPT distinguisher* D*, possibly using some quantum advice* $|\tau\rangle$ *that is stored in the register* $\mathcal{Z}$*, who can distinguish* $\mathrm{Tr}_{\mathcal{Y}}(|\phi_0\rangle\langle\phi_0|)$ *and* $\mathrm{Tr}_{\mathcal{Y}}(|\phi_1\rangle\langle\phi_1|)$ *with advantage* η*, then there exists another QPT transformer* T *who uses a quantum advice* $|\tau'\rangle$ *with the same size as* $|\tau\rangle$ *that is stored in the register* $\mathcal{Z}$*, performs on registers* $(\mathcal{X}, \mathcal{Z})$*, makes a single oracle access to both D (i.e. the unitary operator induced by the unitary part of the distinguisher* D*) and its inverse* $D^\dagger$*, such that*

$$\big\|(|\psi_1\rangle\langle\psi_1|)^{\mathcal{B}\mathcal{X}\mathcal{Y}}T^{\mathcal{X}\mathcal{Z}}\big(|\psi_0\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}|\tau'\rangle^{\mathcal{Z}}\big)\big\| \geq 2\eta.$$

Note that

$$|0\rangle|\phi_0\rangle = \frac{1}{\sqrt{2}}\big(|\psi_0\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}} + |\psi_1\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}\big), \qquad |1\rangle|\phi_1\rangle = \frac{1}{\sqrt{2}}\big(|\psi_0\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}} - |\psi_1\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}\big).$$

The two items above also hold if we exchange the role of $(|0\rangle|\phi_0\rangle, |1\rangle|\phi_1\rangle)$ *and* $(|\psi_0\rangle, |\psi_1\rangle)$*, and that of registers* $\mathcal{X}$ *and* $(\mathcal{B}, \mathcal{Y})$*.*

Proof: The two items in the statement of the theorem have already been proved in [HMY22b] in terms of the flavor conversion of canonical quantum bit commitments. However, the same two items but with the role of $(|0\rangle|\phi_0\rangle, |1\rangle|\phi_1\rangle)$ and $(|\psi_0\rangle, |\psi_1\rangle)$ exchanged are not proved in [HMY22b], though they can be proved similarly as presented below.

For Item 1, for completeness we first sketch its proof in [HMY22b] and then specify how to modify it to prove the same item but with the role of $(|0\rangle|\phi_0\rangle, |1\rangle|\phi_1\rangle)$ and $(|\psi_0\rangle, |\psi_1\rangle)$ exchanged.

It is noted in [HMY22b] that

$$\begin{aligned}&\langle\psi_1|^{\mathcal{B}\mathcal{X}\mathcal{Y}}T^{\mathcal{X}\mathcal{Z}}\big(|\psi_0\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}|\tau\rangle^{\mathcal{Z}}\big) = \langle\psi_0|^{\mathcal{B}\mathcal{X}\mathcal{Y}}T^{\mathcal{X}\mathcal{Z}}\big(|\psi_1\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}|\tau\rangle^{\mathcal{Z}}\big)\\ =\ &\frac{1}{2}\big(\langle 0|^{\mathcal{B}}\langle\phi_0|^{\mathcal{X}\mathcal{Y}}\big)T^{\mathcal{X}\mathcal{Z}}\big(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{X}\mathcal{Y}}|\tau\rangle^{\mathcal{Z}}\big) - \frac{1}{2}\big(\langle 1|^{\mathcal{B}}\langle\phi_1|^{\mathcal{X}\mathcal{Y}}\big)T^{\mathcal{X}\mathcal{Z}}\big(|1\rangle^{\mathcal{B}}|\phi_1\rangle^{\mathcal{X}\mathcal{Y}}|\tau\rangle^{\mathcal{Z}}\big).\end{aligned}$$

Thus, from the assumption that the transforming advantage

$$\big\|(|\psi_1\rangle\langle\psi_1|)^{\mathcal{B}\mathcal{X}\mathcal{Y}}T^{\mathcal{X}\mathcal{Z}}\big(|\psi_0\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}|\tau\rangle^{\mathcal{Z}}\big)\big\| \geq \epsilon,$$

it follows that the swapping advantage

$$\begin{aligned}&\|\langle\psi_1|^{\mathcal{B}\mathcal{X}\mathcal{Y}}T^{\mathcal{X}\mathcal{Z}}\big(|\psi_0\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}|\tau\rangle^{\mathcal{Z}}\big) + \langle\psi_0|^{\mathcal{B}\mathcal{X}\mathcal{Y}}T^{\mathcal{X}\mathcal{Z}}\big(|\psi_1\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}|\tau\rangle^{\mathcal{Z}}\big)\|\\ =\ &2\big\|(|\psi_1\rangle\langle\psi_1|)^{\mathcal{B}\mathcal{X}\mathcal{Y}}T^{\mathcal{X}\mathcal{Z}}\big(|\psi_0\rangle^{\mathcal{B}\mathcal{X}\mathcal{Y}}|\tau\rangle^{\mathcal{Z}}\big)\big\|\\ \geq\ &2\epsilon.\end{aligned}$$

Based on this T and applying the forward direction of Lemma 17, one can construct a distinghuisher that distinghuishes $|\phi_0\rangle$ and $|\phi_1\rangle$ w.r.t. the register $\mathcal{X}$ with advantage $\epsilon^2/2$. Note that in this case, a single oracle access to ctrl-T and that to ctrl-$T^\dagger$ are sufficient.

In the case when the role of $(|0\rangle|\phi_0\rangle, |1\rangle|\phi_1\rangle)$ and $(|\psi_0\rangle, |\psi_1\rangle)$ are exchanged, the assumption of Item 1 becomes

$$\big\|(|1\rangle|\phi_1\rangle\langle 1|\langle\phi_1|)^{\mathcal{B}\mathcal{X}\mathcal{Y}}T^{\mathcal{B}\mathcal{Y}\mathcal{Z}}\big(|0\rangle^{\mathcal{B}}|\phi_0\rangle^{\mathcal{X}\mathcal{Y}}|\tau\rangle^{\mathcal{Z}}\big)\big\| \geq \epsilon.$$

Then consider the following unitary T' which uses an additional ancilla qubit $\mathcal{B}'$ initialized in the state $|0\rangle$:

$$T' = \text{ctrl-}T^{\mathcal{B}'\mathcal{B}\mathcal{Y}\mathcal{Z}} \cdot X^{\mathcal{B}'} \cdot \mathsf{CNOT}^{\mathcal{B}\mathcal{B}'},$$

where the gate CNOT uses the qubit $\mathcal{B}$ and the unitary ctrl-T uses the qubit $\mathcal{B}'$ as the control, respectively. It is easy to check that the swapping advantage

$$\| \langle 0| \langle \phi_0| T' |1\rangle |\phi_1\rangle |\tau\rangle |0\rangle^{\mathcal{B}'} + \langle 1| \langle \phi_1| T' |0\rangle |\phi_0\rangle |\tau\rangle |0\rangle^{\mathcal{B}'} \| = \|0 + \langle 1| \langle \phi_1| T' |0\rangle |\phi_0\rangle |0\rangle^{\mathcal{B}'} \| \geq \epsilon.$$

Then applying the forward direction of Lemma 17, there exists a distinghuisher who can distinghuishes $|\psi_0\rangle$ and $|\psi_1\rangle$ w.r.t. registers $(\mathcal{B}, \mathcal{Y})$ with advantage at least $\epsilon^2/8$. Moreover, since the distinghuisher will make a single query to both ctrl-T' and ctrl-$(T')^\dagger$, it will make a single query to both ctrl-ctrl-T and ctrl-ctrl-$T^\dagger$.

The proof of Item 2 roughly proceeds as follows in [HMY22b]. That is, a lower bound of the distinghuishing advantage implies a lower bound of the swapping advantage (by the backward direction of Lemma 17), which in turn trivially implies a lower bound of the transforming advantage. Its detail is omitted here; one can check the proof of the same item but with the role of $(|0\rangle |\phi_0\rangle, |1\rangle |\phi_1\rangle)$ and $(|\psi_0\rangle, |\psi_1\rangle)$ exchanged below, which follows almost the same line as that for Item 2.

Suppose that there exists a non-uniform QPT distinguisher D who can distinguish $|\psi_0\rangle$ and $|\psi_1\rangle$ w.r.t. registers $(\mathcal{B}, \mathcal{Y})$ with advantage η using a quantum advice $|\tau\rangle$. Then applying the backward direction of Lemma 17, there exists a unitary T performing on registers $(\mathcal{B}, \mathcal{Y}, \mathcal{Z})$ that achieves the swapping advantage

$$| \langle 1| \langle \phi_1| \langle \tau| T |0\rangle |\phi_0\rangle |\tau\rangle + \langle 0| \langle \phi_0| \langle \tau| T |1\rangle |\phi_1\rangle |\tau\rangle | = 4\eta.$$

By the triangle inequality, either $| \langle 1| \langle \phi_1| \langle \tau| T |0\rangle |\phi_0\rangle |\tau\rangle |$ or $| \langle 0| \langle \phi_0| \langle \tau| T |1\rangle |\phi_1\rangle |\tau\rangle |$ are at least 2η. If the former happens, then we are done: the transforming advantage is at least 2η and $|\tau'\rangle = |\tau\rangle$. Otherwise, if only the latter happens, applying Jordan's lemma (e.g. refer to [Reg06]) we know that there exists a state $|\tau'\rangle$ with the same dimension as $|\tau\rangle$ such that

$$\|(|1\rangle \langle 1| \otimes |\phi_1\rangle \langle \phi_1|) T^\dagger |0\rangle |\phi_0\rangle |\tau'\rangle \| \geq 2\eta,$$

by considering projectors $T^\dagger(|0\rangle \langle 0| \otimes |\phi_0\rangle \langle \phi_0|)T$ and $|1\rangle \langle 1| \otimes |\phi_1\rangle \langle \phi_1|$. ■

C Application: the security against the prover in the GMW protocol for Graph 3-Coloring

In this section, we show that the GMW protocol for Graph 3-Coloring [GMW91] with a generic non-interactive quantum computationally-binding bit commitment scheme (Definition 2) plugged in is an argument-of-knowledge.

Informally, the GMW protocol proceeds as follows. On an input common graph G:

P1 The prover commits to the color of each vertex of the graph G.

V1 The verifier chooses an edge of the graph G uniformly random.

P2 The prover opens the commitments to the two vertices adjacent to the edge chosen by the verifier.

V2 The verifier checks that the commitments are opened successfully and the two revealed colors are different.

Now let us formalize an execution of the GMW protocol between a malicious prover $P^* = (|\tau\rangle, P, U)$ and the honest verifier V instantiated with a generic non-interactive quantum computationally-binding bit commitment scheme as follows:

1. P^* receives/prepares the system $(\mathcal{C}^{\otimes 2n}, \mathcal{R}^{\otimes 2n}, \mathcal{M}^{\otimes 2n}, \mathcal{A}^{\otimes 2n}, \mathcal{D})$ in the state $|\tau\rangle$, and sends the commitment registers $\mathcal{C}^{\otimes 2n}$ (which are supposed to store commitments to colors of all vertices) to the verifier. (Note that the color of each vertex can be encoded by two bits.)

2. V chooses a uniformly random edge $e \overset{\$}{\leftarrow} \{1, 2, \ldots, m\}$ as the challenge, where $m = O(n^2)$ is the number of edges of the graph G.

3. P^* performs the unitary U_e on the system $(\mathcal{R}^{\otimes 2n}, \mathcal{M}^{\otimes 2n}, \mathcal{A}^{\otimes 2n}, \mathcal{D})$, where the unitary U_e is the unitary U with e as the control.

4. Suppose that the edge $e = (e_u, e_v)$, where e_u, e_v are the two vertices adjacent to the edge e. The verifier V checks that commitments to colors of e_u and e_v are opened successfully, and that colors of e_u and e_v are different. Formally, the projector P_e corresponding to the predicate check induced by the challenge e is given by

$$P_e \overset{def}{=} \sum_{c(e_u) \neq c(e_v)} |c(e_u), c(e_v)\rangle \langle c(e_u), c(e_v)|^{\mathcal{D}} \otimes |c(e_u), c(e_v)\rangle \langle c(e_u), c(e_v)|^{\mathcal{M}^{\otimes 4}} \otimes |e\rangle^{\mathcal{A}^{\otimes 2n}}, \quad (32)$$

where $c(e_u), c(e_v)$ denote the color of vertices e_u, e_v, respectively; the register $\mathcal{A}^{\otimes 2n}$ contains a binary string, which is also denoted by e to overload notation for simplification, indicating which four (out of $2n$) bit commitments will be opened. Hence, the verifier's verification corresponding to the challenge e is given by the projector

$$V_e \overset{def}{=} \big(|0\rangle \langle 0|^{\mathcal{A}} \otimes \mathbb{1}^{\mathcal{CRM}} + |1\rangle \langle 1|^{\mathcal{A}} \otimes V_{\mathsf{com}}^{\mathcal{CRM}} \big)^{\otimes 2n} \cdot P_e. \quad (33)$$

We prove the following theorem.

Theorem 9 *Using non-interactive statistically-hiding, computationally-binding quantum bit commitments (Definition 2) in the GMW protocol gives rise to a three-round, quantum statistical zero-knowledge argument-of-knowledge for the* ***NP****-complete language* Graph 3-Coloring *with perfect completeness and knowledge error noticeably less than* 1.

Proof: Suppose that the input graph G has n vertices, $m = O(n^2)$ edges.

Given an arbitrary prover $P^* = (|\tau\rangle, U)$, we construct a canonical knowledge extractor as follows:

1. Receiver/prepare the system $(\mathcal{C}^{\otimes 2n}, \mathcal{R}^{\otimes 2n}, \mathcal{M}^{\otimes 2n}, \mathcal{A}^{\otimes 2n}, \mathcal{D})$ in the state $|\tau\rangle$, as P^* does.

2. For each edge $e = 1, 2, \ldots, m$:

   (a) Perform U_e on the system $(\mathcal{R}^{\otimes 2n}, \mathcal{M}^{\otimes 2n}, \mathcal{A}^{\otimes 2n}, \mathcal{D})$.

   (b) Suppose that $e = (e_u, e_v)$. Perform the binary measurement $\{V_e, \mathbb{1} - V_e\}$, where the projector V_e is given by Eq. (32). If the verification fails, then abort; otherwise, measure the register $\mathcal{D}$ to obtain colors of e_u and e_v.

(c) Perform $U_e^\dagger$.

3. Check that all colors obtained in Step 2 are consistent. If not, then abort; otherwise, output colors for each vertex.

Now we prove that the canonical knowledge extractor constructed as above indeed works. Suppose that the (unique-message) binding error of the quantum bit commitment scheme used is ϵ. Suppose that the prover P^* can convince the verifier to accept with probability larger than $1 - 1/m + \delta$; that is,

$$\frac{1}{m} \sum_{e} \| V_e U_e |\tau\rangle \|^2 \geq 1 - \frac{1}{m} + \delta.$$

Applying Lemma 4 with Γ_i, U_i $(1 \leq i \leq k)$ replaced with V_e, U_e $(e \in \{1, 2, \ldots, m\})$ here, respectively, it follows that

$$\left\| (U_m^\dagger \otimes \mathbb{1}^{\mathcal{C}^{\otimes 2n}}) V_m (U_m \otimes \mathbb{1}^{\mathcal{C}^{\otimes 2n}}) \cdots (U_1^\dagger \otimes \mathbb{1}^{\mathcal{C}^{\otimes 2n}}) V_1 (U_1 \otimes \mathbb{1}^{\mathcal{C}^{\otimes 2n}}) |\tau\rangle \right\| \geq 1 - \sqrt{m \left(\frac{1}{m} - \delta \right)} \geq \frac{m\delta}{2}. \tag{34}$$

By identifying the prover as the sender and the verifier as the challenger, we view the knowledge extractor as inducing a parallel-and-sequential collapse-binding experiment (Definition 9) $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(n)$, except that:

1. Conditioned on the verification in Step 2(b) succeeding, the challenger will measure registers $\mathcal{M}^{\otimes 4}$ (which four copies of the register $\mathcal{M}$ is determined by the edge e) rather than $\mathcal{D}$. But seeing from the expression of the predicate P_e (Eq. (32)), these two measurements are equivalent.

2. The experiment excludes Step 3 of the knowledge extractor; instead, it will simply output 1 at the end if it does not abort previously.

It is easy to see that the probability that the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(n)$ outputting 1 is equal to that of the knowledge extractor not aborting before Step 3.

The experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,0}(n)$ differs from $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(n)$ in that the challenger will not measure registers $\mathcal{M}^{\otimes 4}$ when the verification induced by the projector V_e succeeds. One can see that the probability of the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,0}(n)$ outputting 1 is just given by the square of the l.h.s. of Inequality (34), which is at least $m^2\delta^2/4$.

Now we are ready to apply Theorem 3 with $N = 2, l = 2n, t = m = O(n^2)$. By its Item 1, the probability that the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(n)$ outputs 1 is at least $m^2\delta^2/4 - O(\sqrt{\epsilon} n^9)$. By Item 2, the probability that some commitment is opened as different values in the experiment $\mathsf{PS\text{-}ColBindExpt}_{\mathsf{S}^*,1}(n)$ is at most $O(\epsilon n^{15})$. Thus, the probability that the knowledge extractor aborts in Step 3 is at most $O(\epsilon n^{15})$. Putting it together, the knowledge extractor will succeed with probability at least $m^2\delta^2/4 - O(\sqrt{\epsilon} n^9) - O(\epsilon n^{15}) = m^2\delta^2/4 - O(\sqrt{\epsilon} n^9)$. ■