Quantum Computationally Predicate-Binding Commitment with Application in Quantum Zero-Knowledge Argument for **NP**

Jun Yan*

Jinan University

December 2, 2020

Abstract

A quantum bit commitment scheme is to realize bit (rather than qubit) commitment by exploiting quantum communication and quantum computation. In this work, we study the binding property of a generic quantum *computationally-binding* bit commitment scheme *composed in parallel*, which can be viewed as a quantum *string* commitment scheme. We show that the resulting scheme satisfies a stronger quantum computational binding property than the trivial honest-binding, which we call the *predicate-binding*. Intuitively and very roughly, the predicate-binding property guarantees that given any *inconsistent* predicate pair over a set of strings (i.e. no strings in this set can satisfy both predicates), if a (claimed) quantum commitment can be opened so that the revealed string satisfies one predicate with certainty, then the same commitment cannot be opened so that the revealed string satisfies the other predicate (except for a negligible probability).

As an application, we plug a generic quantum (perfectly/statistically-hiding) computationally-binding bit commitment scheme in Blum's zero-knowledge protocol for the **NP**-complete language Hamiltonian Cycle. Then the quantum computational predicate-binding property of the commitments immediately translates into the quantum computational soundness of the protocol. Combined with the perfect/statistical zero-knowledge property which can be similarly established as Watrous [Wat09], as well as known constructions of quantum computationally-binding bit commitment scheme, this gives rise to the first quantum perfect/statistical zero-knowledge *argument* system for all **NP** languages based solely on *quantum-secure one-way functions*.

*Email: tjunyan@jnu.edu.cn

Contents

1 Introduction

Bit commitment is an important cryptographic primitive; it can be viewed as an electronic realization of a locked box [Gol01]. Roughly speaking, a bit commitment scheme has two stages, the commit stage and the reveal stage, and satisfy two properties: hiding and binding. Intuitively, the hiding property requires that the commitments to 0 and 1 be indistinguishable in the commit stage, whereas the binding property requires that any (claimed) bit commitment cannot be opened (by the sender) as both 0 respective 1 (except for a negligible probability) in the reveal stage. Unfortunately, hiding and binding properties cannot be satisfied information-theoretically at the same time; one of them has to be *conditional*, e.g. based on some complexity assumption such as the existence of one-way functions.

Turning to the quantum setting, there are two *different* meanings of quantum bit commitment in the literature (depending on the context). The *first* meaning is the *classical* realization of bit commitment that is secure against *quantum* attacks, or the post-quantum secure (classical) bit commitment [AC02, Unr16b, Unr16a]. The *second* meaning refers to a realization of bit commitment by exploiting *quantum* features [BB84, BC90, DMS00, CLS01, CDMS04, KO09, KO11, CKR11, YWLQ15, FUYZ20, Yan20]. That is, now the honest parties in a bit commitment scheme are allowed to be quantum computers and exchange quantum messages. We highlight that for this second meaning it is still a classical bit that we are trying to secure, while the security should of course be against quantum attacks. Clearly, the first meaning of quantum bit commitment can be viewed as a special case of the second one. In this paper, the term "quantum bit commitment" will be reserved for the second, more general meaning.

The concept of quantum bit commitment is natural and sounds exciting. Unfortunately, contrary to its motivation, quantum bit commitment turns out still cannot be realized *unconditionally* either [May97, LC98]. Another bad news is that by today's quantum technology, the realization of a general (conditional) quantum bit commitment scheme still seems far beyond our reach. Even worse, and somewhat counter-intuitive at the first glance, the binding property of a general quantum bit commitment scheme is inherently *weaker* than its classical counterpart! In more detail, the weakness of the quantum binding property comes from that now a cheating sender may commit to an arbitrary *superposition* of bits 0 and 1, and later reveal this superposition (rather than a classical 0 or 1) with certainty [DMS00, CDMS04]. By this kind of quantum superposition attack, the sender is no longer bound to a unique classical bit any more after fixing a commitment like in the classical setting. As a consequence, it seems much harder to use quantum bit commitments in application [CDMS04, YWLQ15, FUYZ20].

Why quantum bit commitment is interesting? In spite of the bad news mentioned above, we are still interested in quantum bit commitment because it enjoys some intriguing features that classical bit commitment does not have [Yan20]. Notably, merely based on the raw quantum computational hardness, e.g. quantum-secure one-way functions:

1. Quantum bit commitment can be made *non-interactive* (i.e. the commitment consists of just one *quantum* message from the sender to the receiver), in contrast to the constant [MP12] or even polynomial number of rounds by classical constructions [HHRS07];

2. The (either statistical or computational) binding property of quantum bit commitment could be *information-theoretically strict* [FUYZ20, Yan20], which is generally impossible for classical bit commitment. Here, the strictness of the quantum binding property extends the one defined for classical bit commitment [Unr12, ARU14] in a straightforward way, which roughly requires

that not only the revealed value but also the decommitment state used in the opening of a quantum commitment should be unique.

By the first feature above, using quantum bit commitments instead of the classical one in applications can potentially reduce the number of rounds of the interaction[1] while keeping the complexity assumption to the minimum. By the second feature, using quantum bit commitments may circumvent existing barriers only known for classical constructions, as already confirmed in [FUYZ20].

In summary, if we are optimistic about the development of quantum technology and believe that general quantum computation and communication will become available one day, then *the application of quantum bit commitment as a primitive in quantum cryptography* is worthy of study.

New difficulties. If we replace classical bit commitments with quantum bit commitments in cryptographic applications, new difficulties will arise in security analysis. For example, note that since the quantum binding property is inherently weaker than the classical one as aforementioned[2], the security based on the classical binding property may deteriorate after the replacement. In greater detail, note that in applications we typically commit to a binary string by committing it *bitwisely*; later, a *subset* of bit commitments might be opened. The cheating sender may attack by making the opening information about *which* quantum bit commitments are to open as *what* value in an arbitrary superposition, while still be able to convince the receiver to accept with certainty. Henceforth, a (claimed) quantum commitment is no longer bound to a unique string, which makes the security analysis much harder than the classical one [CDMS04, YWLQ15, FUYZ20]. More detail about this difficulty is referred to subsection 1.4.

In the past two decades, there are only few works studying the security based on the *standard* binding (i.e. honest-binding, or equivalently, sum-binding) property [Yan20] of quantum bit commitment. Recently, some *general* techniques to exploit the quantum *statistical* binding property are developed in [FUYZ20], by which in many cases the security analysis based on the classical statistical binding property can be extended to the quantum setting. However, when it comes to the security based on the quantum *computational* binding property, the corresponding analysis turns out to be more elusive. Actually, to the best of our knowledge, we are aware of none of such results. Thus, in our opinion, the perhaps most important open question towards using quantum bit commitment as a primitive in quantum cryptography is:

> *Can we base quantum security on the standard computational binding property of quantum bit commitment?*

By the state-of-the-art knowledge, the answer to the question above is unclear. On one hand, intuitively it seems true, if we view the *superposition* of the committed value underlying quantum bit commitments as the corresponding *probability distribution*. Actually, this intuition is indeed correct in many cases when perfectly/statistically-binding quantum bit commitments are used [FUYZ20]. On the other hand, however, after a first attempt towards the security analysis, it turns out that a naive analysis (r.f. subsection 1.4) requires that the binding error be *sub-exponentially* or even *exponentially* small, rather than *negligiblly* small as typical in cryptography. We call this phenomena the "exponential curse", which at a high level arises from that the quantum state of polynomial number of qubits could be a superposition of exponentially many basis states. Moreover, the impossibility of general quantum rewinding [vdG97], as well as other related impossibility results

[1] The round complexity of the interaction might be one of the most important parameters of any cryptographic constructions.

[2] In this work, we neglect the analysis of the security based on the quantum hiding property, which is trivial for our application with the existing technique [Wat09].

known for classical constructions of bit commitment secure against quantum attacks [ARU14], may suggest a *negative* answer to the open question above.

1.1 Our contribution

One of our motivations of this work is to study the application of quantum computationally-binding bit commitments in constructing quantum zero-knowledge argument for **NP** languages. In spite of the technical difficulty and negative evidences mentioned above, we manage to base the quantum computational soundness of Blum's zero-knowledge protocol for the **NP**-complete language Hamiltonian Cycle [Blu86] on the standard computational binding property of quantum bit commitment, thus answering the main open question raised before *affirmatively*. More interestingly, the reason why this is possible turns out to be completely *different* from the aforementioned intuition (i.e. viewing the superposition as the corresponding probability distribution).

Specifically, our contribution is two-fold.

1. A *quantum* construction of perfect/statistical zero-knowledge *argument* system for all NP languages

We prove the following main theorem of this paper:

Theorem 1 *Plugging a generic quantum perfectly(resp. statistically)-hiding computationally-binding bit commitment scheme in Blum's protocol [Blu86] gives rise to a three-round quantum perfect(resp. statistical) zero-knowledge argument system for the **NP**-complete language Hamiltonian Cycle, with perfect completeness and soundness error* $1/2$.

Following [YWLQ15, Yan20], a generic quantum bit commitment scheme can be represented by an ensemble of quantum circuit pair $\{(Q_0(n), Q_1(n))\}_n$ (Definition 3). The theorem above gives the *first* quantum perfect/statistical zero-knowledge argument for all **NP** languages based on the *minimum* quantum complexity assumption. The quantum zero-knowledge argument given in [Unr16b] relies on a commitment scheme with a stronger quantum computational binding property (known as the *collapse-binding*), which in turn relies on much stronger assumptions [Unr16b, Unr16a]. Compared with its classical counterpart, our *quantum* construction reduces the rounds of the interaction *from polynomial to three*, thanks to the *non-interativeness* of a generic quantum computationally-binding bit commitment scheme [DMS00, KO09, KO11, Yan20].

We also highlight that our proof of the theorem above relies heavily on (though implicitly) that the (whether statistical or computational) binding property of a generic quantum bit commitment scheme is information-theoretically *strict* [Unr12, Yan20]; that is, for a successful opening of a (claimed) quantum bit commitment, the revealed value together with the decommitment state sent in the reveal stage for the opening is unique (through the *entanglement*). This strictness allows us to apply the quantum rewinding technique developed in [YWLQ15, FUYZ20] even in the quantum *computational* soundness analysis. Our quantum construction also circumvents the existing barrier which is only known for classical constructions. (We will discuss this in more detail later in subsection 1.3.)

2. A non-trivial computational binding property of the quantum *string* commitment obtained by composing quantum bit commitments in parallel

A natural way to obtain a string commitment scheme is to compose a bit commitment scheme in *parallel*, i.e. committing a string bitwisely using the bit commitment scheme. For the purpose of proving Theorem 1, we introduce a new binding property of quantum *string* commitment which we

call the *predicate-binding* property. We show that the parallel composition of a generic quantum bit commitment scheme with the standard *computational* binding property gives rise to a quantum computationally predicate-binding string commitment scheme (Theorem 3). It turns out that the quantum computational soundness of Blum's protocol in which a generic quantum computationally-binding bit commitment scheme is plugged in, as required in establishing Theorem 1, can be easily based on the predicate-binding property of the quantum string commitment obtained by composing quantum bit commitments in parallel.

Informally speaking, the predicate-binding property guarantees that given an arbitrary pair of *inconsistent* predicates on a set of strings of the same length (i.e. no strings in this set can satisfy both predicates), if a (claimed) quantum commitment can be opened such that the revealed string[3] satisfies one predicate with *certainty*, then the same commitment cannot be opened so as to satisfy the other predicate (except for a negligible probability). Clearly, this quantum predicate-binding property is *stronger* than the honest-binding property [YWLQ15], which roughly guarantees that the honest commitment to a string cannot be opened as any other string (except for a negligible probability).

We note that the parallel composition of classical bit commitments gives a string commitment that is trivially predicate-binding. While the parallel composition of quantum bit commitments trivially gives a quantum honest-binding string commitment [YWLQ15], it becomes highly non-trivial to show that it also satisfies the predicate-binding property. This is due to the fairly weak quantum bit binding property aforementioned. To the best of our knowledge, we are aware of no (quantum) security reduction from any non-trivial quantum computational string binding property to the quantum computational bit binding property in previous work. In [CDMS04], another non-trivial computational binding property of quantum string commitment is proposed for its application (i.e. quantum oblivious transfer). However, it is still open whether this quantum string commitment can be obtained by composing quantum bit commitments with standard computational binding property in parallel. (We will talk about this in more detail when we survey the search for the "right" definition of quantum computational binding in Subsection 1.2.)

Actually, in this work we did *not* prove the *full* quantum predicate-binding property (i.e. w.r.t. the most general inconsistent predicate pair). Instead, we only allow one predicate to be of the general form, whereas the other is subject to the restriction that it only depends on a *fixed* portion of the string. In spite of this restriction, the binding property we obtain is sufficient for establishing Theorem 1. Any extension of our result is left as an open problem. We believe that quantum predicate-binding string commitment could be of independent interest and will be found useful elsewhere.

1.2 Related work: towards the "right" definition for quantum computational binding

For years researchers have been seeking the "right" definition for quantum computational binding, where the "right" is in the following sense: on one hand, we hope that thus defined quantum computational binding property is strong enough so that on which the security of applications can be based. On the other hand, we hope that this quantum computational binding property is not too strong, so that the commitment can be based on relatively weak complexity assumption, e.g. quantum-secure one-way functions. In the past two decades, there have been several works towards coming up with a right definition for quantum computational binding, as discussed below for both

[3]Generally, the revealed value of a quantum string commitment could be a probability distribution over this set of strings.

quantum and classical constructions of commitment.

Quantum construction. Regarding quantum constructions of computationally-binding *bit* commitment, *sum-binding* was firstly proposed and established in [DMS00] for a non-interactive scheme based on an arbitrary quantum-secure one-way permutation. Follow-up works manage to relax the complexity assumption to quantum-secure one-way functions [CLS01] and even keep the non-interactiveness [KO09, KO11, Yan20]. Recently, Yan [Yan20] showed that w.r.t. a generic quantum bit commitment scheme, sum-binding is equivalent to *honest-binding* — the weakest binding property that any quantum bit commitment schemes should satisfy.

If we view the *parallel composition* of a computationally-binding bit commitment scheme as giving rise to a *string* commitment scheme, then what *string binding* property we can obtain remains a mystery. By a simple hybrid argument, it is easy to show that the resulting quantum string commitment scheme is *honest-binding*, which however seems not sufficient for any interesting applications. The first (and the only) quantum string binding property that is provably useful was introduced in [CDMS04], which will be referred to as the *CDMS-binding* hereafter. Unfortunately, we still do not know whether the corresponding string commitment scheme can be obtained from the parallel composition of a quantum bit commitment scheme with standard computational binding property.

In comparison, the quantum string commitment with computational predicate-binding property introduced in this paper not only suffices for quantum zero-knowledge argument, but also can be obtained from the parallel composition of quantum bit commitments with standard computational binding property. Seeing from this, the predicate-binding could serve as a candidate for the right definition of quantum computational string binding; more applications will be tested against it in future.

Classical construction. The classical construction can be viewed as a special case of the quantum construction such that the measurements of exchanged messages always take place. Due to the impossibility of general quantum rewinding [vdG97], we cannot generalize the definition of the computational binding against classical adversaries to that against quantum adversaries in a straightforward way. This is because the cheating sender's inability of outputting two different openings does not imply its inability to open the commitment as any value as its wish, as confirmed (though in a relatived world) in [ARU14]. On the positive side, Unruh [Unr16b] proposes a strong quantum computational binding property known as the *collapse-binding*. It turns out that collapse-binding commitment composes in parallel and enables a simple quantum rewinding, by which (classical) zero-knowledge argument-of-knowledge against quantum adversaries for **NP** can be constructed [Unr16b]. However, the collapse-binding property seems so strong that the concurrent known realization of collapse-binding commitments need either structure assumptions [Unr16a] or the quantum random oracle; we do not know whether it can be based on quantum-secure one-way functions. In comparison, everything we construct in this paper (though by quantum constructions) can be based solely on quantum-secure one-way functions.

1.3 How can our quantum construction circumvent a barrier for classical constructions?

In [Unr12], Unruh shows that plugging a perfectly-binding classical bit commitment scheme in a variant of Blum's protocol gives rise to a quantum zero-knowledge proof-of-knowledge. The perfect binding property of bit commitments there ensures that the resulting protocol have strict soundness, which guarantees that the last message the protocol is uniquely determined by the first two. It

is this strict soundness that makes a simple quantum rewinding work in establishing quantum proof-of-knowledge.

A natural way to extend the result above from the proof system to the argument system is to plug in a computationally-binding bit commitment scheme instead, which additionally satisfies the computational strict-binding property that can be defined in a similar way. And we expect that the resulting protocol gives rise to a quantum zero-knowledge argument or even argument-of-knowledge. Unfortunately, this possibility is refuted in a relativized world in [ARU14], where they show that a general Σ-protocol with computational strict soundness may not even sound!

So why the attack in [ARU14] does not extend to the quantum construction, in particular Blum's protocol with a generic quantum computationally-binding bit commitment scheme plugged in? After a few thought, it turns out that this is because, at a high level, a generic quantum computationally-binding bit commitment scheme satisfies a *information-theoretic* strict-binding property [Yan20], where the strictness comes from the *entanglement* between the commitment and its decommitment. It is this information-theoretic strictness of the quantum computational binding property that enables a simple quantum rewinding to work [YWLQ15, FUYZ20]. In comparison, we note that in the classical setting, the computational binding property cannot be information-theoretically strict: though it may be computationally hard to find an alternative opening, there actually *exists* a bunch of them!

1.4 Proof overview

We first sketch the soundness analysis of Blum's protocol in which a generic quantum computationally-binding bit commitment scheme is plugged in, the goal of which is to reduce its (computational) soundness to the predicate-binding property of quantum string commitment (Lemma 11). This is the key step in establishing Theorem 1.

We assume that readers are familar with Blum's protocol [Blu86], which is also sketched in Subsection 2.3. In its soundness analysis, the (possibly cheating) prover's first message constitutes a (claimed) quantum string commitment. The (honest) verifier's acceptance conditions corresponding to challenges 0 respective 1 induce two predicates on graphs with the same vertices as the input graph; when the input graph is not Hamiltonian, these two predicates should be *inconsistent*. Technically, at the heart of the reduction from the soundness of Blum's protocol to the predicate-binding property of the quantum string commitment lies in a simple quantum rewinding technique that is similar to [Unr12, YWLQ15, FUYZ20]. In particular, we can extend the quantum rewinding lemma that is suitable for the quantum statistical binding setting [FUYZ20] to the quantum computational binding setting (Lemma 1), which basically states that if the verifier's acceptance probability is high, then the direct rewinding via the reversible quantum computation works. We remark that though this extension is technically trivial, conceptually why it is possible relies heavily on that a generic quantum computationally-binding bit commitment scheme is *information-theoretically* strict-binding.

We are then left with showing that the parallel composition of a generic quantum computationally-binding *bit* commitment scheme indeed gives rise to a quantum computationally predicate-binding *string* commitment scheme (Theorem 3). This is the main technical part of this paper. In the below, we first explain a technical difficulty towards this goal by a naive try, and then sketch at a high level how to circumvent it. But before doing this, we set up some notations that are necessary for our exposition first.

Notations. A generic quantum bit commitment commitment scheme can be represented by a

quantum circuits pair (Q_0, Q_1)[4] performing on quantum registers (C, R). To commit a bit b, in the commit stage the sender performs the quantum circuit Q_b on quantum registers (C, R) initialized in the state $|0\rangle$, and then sends the *commitment* register C to the receiver; later in the reveal stage, the sender sends the bit b together with the *decommitment* register R to the receiver, who then does the reversible computation (i.e. performing $Q_b^\dagger$) to decide whether to accept or not (i.e. checking whether the registers return to the all $|0\rangle$ state). Informally, we say that the quantum bit commitment scheme (Q_0, Q_1) is *computationally binding* if for any polynomial-time realizable unitary transformation U performing on the register R, the inner product $\left| \langle 0| Q_1^\dagger U Q_0 |0\rangle \right|$ is negligible; that is, unit vectors $UQ_0|0\rangle$ and $Q_1|0\rangle$ are almost orthogonal[5].

To commit a string of length m, we commit it *bitwisely* using the scheme (Q_0, Q_1). Let Q_s denote the corresponding quantum circuit used to commit the string s; that is, $Q_s = \bigotimes_{i=1}^m Q_{s_i}$, which performs on m copies of the quantum register pair (C, R).

Let P_1, P_2 be two *predicates* on all m-bit strings. We use $s \in P_1$ (resp. P_2) to denote that the string $s \in \{0,1\}^m$ satisfies the predicate P_1 (resp. P_2). We say that two predicates P_1, P_2 are *inconsistent* if no string $s \in \{0,1\}^m$ can satisfy both P_1 and P_2. More detail about the formalization of predicates is referred to subsection 4.1.

A technical difficulty: exponential curse. We first consider the *simplest* scenario, in which an m-bit string is firstly committed and later *all* (bit) commitments are to open. Note that a cheating sender can first prepare an arbitrary superposition of the form $\sum_{s\in P_1} \alpha_s |s\rangle^D (Q_s|0\rangle)^{C^{\otimes m} R^{\otimes m}}$ (resp. $\sum_{s\in P_2} \beta_s |s\rangle Q_s|0\rangle$) in registers $(\mathsf{D}, \mathsf{C}^{\otimes m}, \mathsf{R}^{\otimes m})$, and then send the commiment registers $\mathsf{C}^{\otimes m}$ to the receiver in the commit stage. Later in the reveal stage, the sender sends the opening register D and the decommitment registers $\mathsf{R}^{\otimes m}$ to the receiver. By this strategy, the sender can open all commitments as a *distribution* (which is determined by all coefficients α_s's (resp. β_s's)) of strings that satisfy the predicate P_1 (resp. P_2) with *certainty*. To show predicate-binding, we are sufficient to show that up to any *polynomial-time* realizable unitary transformation U that does not touch the commitment registers $\mathsf{C}^{\otimes m}$ (which represents the sender's strategy in opening commitments), two arbitrary superpositions $\sum_{s\in P_1} \alpha_s |s\rangle Q_s|0\rangle$ and $\sum_{s\in P_2} \beta_s |s\rangle Q_s|0\rangle$ are almost *orthogonal*, i.e. their inner product is negligible, w.r.t. any inconsistent predicate pair (P_1, P_2). A technical difficulty in showing this lies in that a potential exponential blow-up may occur in bounding this inner product, which is called the "exponential curse" in [YWLQ15, FUYZ20]; similar phenomena also appear elsewhere [CDMS04]. Detail follows.

By the computational honest-binding property of the quantum bit commitment scheme (Q_0, Q_1), the inner product $|\langle 0| Q_{s'}^\dagger U Q_s |0\rangle|$ where $s \neq s'$ can be bounded by the binding error, which is negligible (as typical in cryptography). Thus, a naive way to bound the inner product (between the two superpositions) $\left| \sum_{s\in P_1} \alpha_s^* \langle s| (\langle 0| Q_s^\dagger) U \sum_{s'\in P_2} \beta_{s'} |s'\rangle (Q_{s'}|0\rangle) \right|$ is first to expand it and bound each term indexed by (s, s') using the binding error bound (while neglecting its coefficient, which can be bounded by 1), and then apply the triangle inequality. However, when there are *super-polynomial* (or even exponentially many) strings $s \in P_1$ or $s' \in P_2$, this naive approach will fail completely.

Actually, whether the inner product mentioned above could really be bounded by some negligible quantity is questionable. This is because generally, two superpositions of the form $\sum_x \alpha_x |\phi_x\rangle$ and $\sum_y \beta_y |\xi_y\rangle$, where $\{|\phi_x\rangle\}_x$ and $\{|\xi_y\rangle\}_y$ are two orthonormal bases, are *not* necessarily almost

[4]For the moment, we drop the security parameter to simplify the notation.

[5]The formal definitions of a generic quantum bit commitment scheme and its computational binding propery are referred to Definition 3, where the auxiliary input state that the cheating sender may receive is needed to be taken into account of.

orthogonal, even when $|\phi_x\rangle$ and $|\xi_y\rangle$ are almost orthogonal for each (x, y) pair. To see this, consider the following simple example. The Hilbert space is induced by m qubits, where $\{|x\rangle\}_{x\in\{0,1\}^m}$ is the standard basis and $\{H^{\otimes m}|y\rangle\}_{y\in\{0,1\}^m}$ is the Hadamard basis. Then consider an arbitrary vector in this space, which can be written as a superposition of basis vectors either in the standard basis or the Hadamard basis. Clearly, these two superpositions are actually the same vector, so that their inner product is one. But the inner product between $|x\rangle$ and $H^{\otimes m}|y\rangle$ for arbitrary $x, y \in \{0,1\}^m$ is exponentially small! This example tells us that to bound the inner product aforementioned, we need to exploit the *structures* of the two superpositions (which are induced by the structures of predicates P_1 and P_2).

Similar technical difficulty also appears in the quantum statistical binding setting, where two generic techniques were invented to circumvent this exponential curse: perturbation and commitment measurement [YWLQ15, FUYZ20]. Unfortunately, neither of them can extend to the quantum computational binding setting studied here straightforwardly. For the reason, the *fundamental difference* between these two settings lies in that in the quantum statistical binding setting, the bit commitments to 0 respective 1 (stored in the commitment register C) themselves are already *almost orthogonal*, and which will *never* be touched by the (possibly cheating) sender after they are sent. Thus, we can assume that commitments will *collapse* immediately by some hypothetical measurements at the moment they are sent; after the collapse, everything will behave similar to the classical perfect binding setting. However, in the quantum computational binding setting, commitments to 0 respective 1 could be *close or even identical*, where we are only guaranteed that in the reveal stage the *joint* states of the commitment register C and the decommitment register R are almost orthogonal. But the state of the decommitment register R can be affected by the sender's operation *after* the commitment stage. In turn, the hypothetical-collapse trick to handle quantum statistically-binding commitments [FUYZ20] fails completely here. New techniques are needed to establish the quantum computational predicate-binding property (if possible).

Our approach. Instead of considering the aforementioned inner product of two arbitrary superpositions, now we equivalently consider the projection of an arbitrary superposition of the form $\sum_{s\in P_1}\alpha_s|s\rangle Q_s|0\rangle$, up to any polynomial-time realizable unitary transformation U that does not touch the commitment registers $\mathsf{C}^{\otimes m}$, on the subspace induced by the predicate P_2, i.e. $\sum_{s\in P_2}|s\rangle\langle s|\otimes(Q_s|0\rangle\langle 0|Q_s^\dagger)$, which we also denote by P_2. Our goal then becomes to show that this projection is negligible. Our idea is based on the following *key observation*: when the predicate P_1 is *sparse*, i.e. the number of the m-bit strings satisfying it is *polynomially* bounded[6], then combining a new *perturbation* technique (which looks similar but actually inherently different from the one developed in the quantum statistical binding setting [YWLQ15, FUYZ20]) and the triangle inequality, we can bound the aforementioned projection by a negligible quantity. However, to remove this sparsity requirement, we still need to overcome the exponential curse. To this end, we take into account of the *coefficients* of the superposition, and make an essential use of the following *structure* of predicates P_1 and P_2: to check whether a string satisfies P_1 (resp. P_2), *all* its bits are to examine.

For more technical detail, we are to bound the norm $\left\|\sum_{s\in P_1}\alpha_s P_2 U(|s\rangle Q_s|0\rangle)\right\|$, where in the summation there could be exponentially many terms. At a high level, our *trick* is to order these terms properly so as to treat them as *leaves of a binary tree*, whose internal nodes will correspond to the summation of leaves of the subtree it determines; in particular, the root of the tree will correspond to the summation of all leaves, whose norm is just what we want to bound. We will actually bound the norm of all internal nodes, including the root, in a *bottom-up* fashion. It turns

[6]In this case, the number of terms in the superposition $\sum_{s\in P_1}\alpha_s Q_s|0\rangle$ is polynomially bounded.

out that the accumulated error will grow only *linearly* in the *depth* of the tree, which is just m. The formal proof (of Lemma 9) is by induction on the depth of internal nodes.

As a final remark, we note that our security analysis did *not* achieve a totally *uniform* security reduction (from the quantum computational string predicate-binding property to the quantum computational binding property of a generic quantum bit commitment scheme); rather, we make an essential use of a certain amount of both classical and quantum *non-uniformity*. (More detail about this is referred to the discussion at the end of Subsection 4.3.)

Extension. However, the (simplest) scenario considered above is usually *not* sufficient for applications. This is because in many cases where bit commitments are used in a larger protocol, *not* all bit commitments are required to open for a verification. Even worse, positions of which bit commitments are to open are not fixed; they depend on the party who plays the role of the (cheating) sender. (For example, consider an execution of Blum's protocol in which a Hamiltonian cycle is challenged to open.)

Fortunately, we can extend the predicate-binding property established above to a more general case in which it holds that for at least one predicate (P_1 or P_2), the positions of which bit commitments are to open for its verification are fixed, while the other predicate could be arbitrary (Theorem 3). It turns out that this extension already suffices for our purpose of establishing Theorem 1.

For the formal proof of such extension, there are some new technical difficulties we need to handle. (More detail is referred to the proof of Theorem 3 (in Appendix A)). Among others, we would like to highlight that the standard computational binding property of a generic quantum bit commitment scheme needs to be strengthened (Lemma 4) for use in our security analysis. We believe that this generalization could be of independent interest.

Organization. We first give preliminaries in Section 2. In Section 3, we derive a more general computational binding property of a generic quantum bit commitment scheme from the standard one, which will be useful in the subsequent Section 4, where we establish the computational predicate-binding property of the quantum string commitment scheme obtained by composing a generic quantum computationally-binding bit commitment scheme in parallel. As an application of the predicate-binding property, in Section 5 we show that Blum's zero-knowledge protocol for the **NP**-complete language Hamiltonian Cycle with a generic quantum computationally-binding bit commitment scheme plugged in is sound against any quantum computationally bounded prover. We conclude with Section 6.

2 Preliminaries

A quantum system or register induces a Hilbert space, while a quantum operation performing on a quantum system induces an operator acting on the Hilbert space associated with the system. In particular, a unitary operation induces a unitary transformation, and a binary projective measurement induces a projector (corresponding to the outcome one). We will *interchangeably* use quantum system and its induced Hilbert space, quantum operation and its induced operator. For example, we may say that a unitary transformation or a projector perform on or do not touch a quantum register.

Notations. We will explicitly write quantum register(s) as a *superscript* of an operator to indicate or highlight on which register(s) this operator performs. Similarly, we will also explicitly write quantum register(s) as a *superscript* of a quantum state to indicate or highlight in which register(s)

this quantum state is stored. For example, let A be a quantum register. Then we may write U^A, $|\psi\rangle^A$ (resp. ρ^A), to indicate that the operator U performs on the register A, the quantum pure (resp. mixed) state $|\psi\rangle$ (resp. ρ) is stored in the register A, respectively. We may also write $U \otimes \mathbb{1}^A$ to highlight that the operation U does *not* touch the register A. But when it is clear from the context, we often drop such superscripts or the tensor product with the identity to simplify the notation; this in particular happens in many of derivations within our proofs, where we often write out registers as superscripts or the tensor product with the identity explicitly in the first step, while dropping them subsequently. When there are m copies of register A, and a unitary transformation U performs on the copies of the register A indexed by the subset $T \subseteq \{1, 2, \ldots, m\}$, then we write $\otimes T$ as the superscript, i.e. $U^{\mathsf{A}^{\otimes T}}$; in particular, when the subset T is the whole set, we then just write $\mathsf{A}^{\otimes m}$ to simplify the notation.

Efficiently realizable quantum computation. In this work, without loss of generality, we restrict to consider the following quantum computational model:

1. Quantum systems or registers are constituted of *qubits*.
2. There are only two kinds of quantum operations: *unitary* transformation and *projective* measurement.

We also need to formalize *efficiently realizable* quantum operations. By [Yao93], any efficiently realizable quantum algorithm or unitary transformation can be formalized by a family of quantum circuits $\{Q_n\}_{n\geq 1}$ such that:

1. Each gate of the quantum circuit Q_n comes from a pre-fixed finite, unitary, and universal quantum gate set, e.g. $\{\text{Hadamard}, \text{phase}, \text{CNOT}, \pi/8\}$ [NC00].
2. Quantum circuit Q_n is of *polynomial* size (w.r.t. the index n).
3. The quantum circuit family $\{Q_n\}_{n\geq 1}$ can be uniformly generated, i.e. there exists a polynomial-time classical algorithm A which on input 1^n outputs the description of the quantum circuit Q_n.

Since any *projective* measurement can be realized by first performing a unitary transformation, followed by a measurement of all qubits in the *standard* basis, we say that a projective measurement is *efficiently realizable* if the corresponding unitary transformation is efficiently realizable.

Any projector Π induces a binary measurement $\{\Pi, \mathbb{1} - \Pi\}$, which produces the outcome 1 (resp. 0) when the quantum state collapses into the subspace induced the projector Π (resp. $\mathbb{1} - \Pi$). We say that the projector Π is *efficient realizable* if its induced binary measurement is efficiently realizable.

Quantum rewinding. A quantum rewinding technique as stated in the lemma below is adapted from the one given in [FUYZ20] directly, where now we restrict to consider projectors and unitary transformations that are efficiently realizable. In spite of this, its proof follows the same line as the one in [FUYZ20].

Lemma 1 (A quantum rewinding) *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 $1/k \cdot \sum_{i=1}^{k} \left\|\Gamma_i(U_i \otimes \mathbb{1}^X) |\psi\rangle\right\|^2 \geq 1 - \eta$, where $0 \leq \eta \leq 1$, then*

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

2.1 A generic quantum bit commitment scheme

We first need to define quantum *(in)distinguishability* based on the efficiently realizable quantum computation we fixed above. Our definition follows [Wat09].

Definition 2 ((In)distinguishability of quantum state ensembles) Two quantum state ensembles $\{\rho_n\}_{n\geq 1}$ and $\{\xi_n\}_{n\geq 1}$ are *quantum statistically (resp. computationally) indistinguishable* if for any quantum state ensemble $\{\sigma_n\}_{n\geq 1}$ and any unbounded (resp. efficiently realizable) quantum algorithm D which outputs a single qubit that will be measured in the standard basis, it holds that

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

for sufficiently large n, where $negl(\cdot)$ is some negligible function.

Following Yan [Yan20], the definition of a generic quantum computationally-binding bit commitment scheme is given as below.

Definition 3 (Quantum bit commitment scheme, QBC) A *non-interactive* quantum bit commitment scheme is a two-party, two-stage protocol. It can be represented by an ensemble of polynomial-time uniformly generated quantum circuit pair $\{(Q_0(n), Q_1(n))\}_{n\geq 1}$. Specifically,

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

We are next to define the hiding (or concealing) and the binding properties of the scheme $\{(Q_0(n), Q_1(n))\}_{n\geq 1}$.

- **Statistically hiding**. We say that the scheme is statistically hiding if the quantum state ensembles $\{\rho_0(n)\}_{n\geq 1}$ and $\{\rho_1(n)\}_{n\geq 1}$ are quantum statistically indistinguishable.
- **Computationally $\epsilon(n)$-binding**. We say that the scheme is quantum computationally $\epsilon(n)$-binding if for any state $|\psi\rangle$ in auxiliary register Z, and any efficiently realizable unitary transformation U performing on (R, Z),

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

  By the *reversibility* of quantum computation, the binding property can also be equivalently defined by swapping the roles of Q_0 and Q_1 in the above. Then the inequality (2) becomes

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

  We call $\epsilon(n)$ the *binding error*. When $\epsilon(n)$ is some negligible function, we usually drop it and just say that the scheme is computationally binding.

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

We will use the scheme (Q_0, Q_1) to commit a binary string bitwisely. Namely, the quantum circuit to commit a string $s = s_1 s_2 \cdots s_m \in \{0,1\}^m$ is given by

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

which performs on m copies of the quantum register pair (C, R).

2.2 Modeling an attack of the sender of quantum commitments

When a quantum bit commitment scheme is used within a larger protocol, we consider the following scenario: suppose that the cheating party in a running of the larger protocol plays the role of the sender in the quantum bit commitment scheme. This cheating party is supposed to first commit to a string in $\{0,1\}^m$ bitwisely, and later try to open the commitments in a way as determined by the larger protocol. Then the behavior of this cheating party, or an *attack* of the sender, can be modeled by $(U, |\psi\rangle)$ such that:

1. The sender prepares the whole system $(\mathsf{C}^{\otimes m}, \mathsf{R}^{\otimes m}, \mathsf{D}, \mathsf{Z})$ in the quantum state $|\psi\rangle$ at the *end* of the commit stage, and sends the commitment registers $\mathsf{C}^{\otimes m}$ to the receiver.

2. Later in the reveal stage, the sender first performs the *unitary* transformation U on the system in its hands, which in particular includes registers $(\mathsf{R}^{\otimes m}, \mathsf{D})$, and then sends registers $(\mathsf{R}^{\otimes m}, \mathsf{D})$ to the receiver. Intuitively, the register D contains the classical information indicating *which* quantum bit commitments are to open as *what* value, and the register $\mathsf{R}^{\otimes m}$ are decommitment registers.

We remark that in the second item above, we assume without loss of generality that *all* decommitment registers $\mathsf{R}^{\otimes m}$ are sent to the receiver in the reveal stage, though sometimes only a proper subset of commitments are required to open[7]. Briefly, we can do this because the receiver is *honest*. The detail is referred to [FUYZ20].

2.3 Blum's zero-knowledge protocol for Hamiltonian Cycle

Basically, Blum's protocol [Blu86] proceeds as follows: on input a graph G (assuming it is represented by its adjacency matrix) with n vertices:

1. The prover first chooses a random permutation $\Pi \in S_n$, where S_n consists of all permutations over the set $\{1, 2, \ldots, n\}$. Then it commits to the graph $\pi(G)$, sending all n^2 (quantum) bit commitments to the verifier.

2. Upon receiving the prover's commitments, the verifier tosses a random coin to obtain the challenge bit $b \in \{0,1\}$ and sends it to the prover.

3. If the challenge $b = 0$, then the prover sends the permutation π together with the decommitment registers for *all* bit commitments to the verifier. If the challenge $b = 1$, then the prover sends the location of a Hamiltonian cycle H together with the decommitment registers for the commitments of all edges of the cycle H to the verifier.

[7] For example, consider a running of Blum's zero-knowledge protocol for the language Hamiltonian Cycle in which the cheating prover responds to the challenge 1 of the verifier.

4. If the challenge $b = 0$, then the verifier accepts if all bit commitments are opened as $\pi(G)$ successfully. If the challenge $b = 1$, then the verifier accepts if the H is a possible location of a Hamiltonian cycle and all commitments to the edges of H are opened as 1 successfully.

3 Generalized quantum computational binding

In our definition of quantum computational binding (inequalities (2) and (3) within Definition 3), we quantify over all efficiently realizable unitary transformations that do not touch the commitment. In this section, we show that we can generalize the quantum computational binding property by additionally quantifying over all efficiently realizable projectors. (Recall that we call a *projector* Π efficiently realizable if its induced binary measurement $\{\Pi, \mathbb{1} - \Pi\}$ is efficiently realizable).

We remark that such a generalization is introduced mainly for a technical reason. (Refer to the subsequent section for its application.) Intuitively, such a generalization is needed because a larger quantum protocol within which quantum bit commitments are used may involve not only unitary transformations but also (projective) measurements. For its proof, it makes an essential use of the *arbitrarity* of the efficiently realizable unitary transformation U and the auxiliary input state $|\psi\rangle$ in the definition of quantum computational binding (Definition 3).

Lemma 4 *Inherit all notations in Definition 3. Let the operator $\Gamma = U_k \Pi_k \cdots U_1 \Pi_1$ be an arbitrary alternation of efficiently realizable unitary transformations and projectors, where $k \geq 1$ is an integer, and for each i $(1 \leq i \leq k)$ both the unitary transformation U_i and the projector Π_i perform on the quantum registers (R, Z). If the inequality (2) holds, then*

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

Proof: We just prove the first inequality; the second one can be proved symmetrically.

By the definition of quantum computationally binding (Definition 3), the first inequality trivially holds when the operator Γ is a unitary transformation. To handle projectors, the basic idea is *simulation*: namely, each binary projective measurement $\{\Pi_i, \mathbb{1} - \Pi_i\}$ $(1 \leq i \leq k)$ performing on the registers (R, Z) can be simulated by a unitary transformation V_i performing on registers $(\mathsf{R}, \mathsf{Z}, \mathsf{Y}_i)$ in the standard way, where the register Y_i is a single qubit register initialized in the state $|0\rangle$. Note that if the binary measurement $\{\Pi_i, \mathbb{1} - \Pi_i\}$ is efficiently realizable, then so is V_i. Put it formally,

$$V_i^{RZY_i} \big(|0\rangle^{Y_i} (Q_0 |0\rangle)^{CR} |\psi\rangle^Z \big) = |1\rangle^{Y_i} \otimes \Pi_i^{RZ} \big((Q_0 |0\rangle)^{CR} |\psi\rangle^Z \big) + |0\rangle^{Y_i} \otimes (\mathbb{1} - \Pi_i)^{RZ} \big((Q_0 |0\rangle)^{CR} |\psi\rangle^Z \big).$$

For each index i $(1 \leq i \leq k)$ and each bit $b \in \{0, 1\}$, we introduce the projector

$$\Pi_i^b \stackrel{def}{=} \begin{cases} \Pi_i, & \text{if } b = 1 \\ \mathbb{1} - \Pi_i, & \text{if } b = 0 \end{cases},$$

and the register $\mathsf{Y} = (\mathsf{Y}_1, \ldots, \mathsf{Y}_k)$. Then

$$(U_k^{RZ} V_k^{RZY_k} \cdots U_1^{RZ} V_1^{RZY_1}) \big(|0^k\rangle^Y (Q_0 |0\rangle)^{CR} |\psi\rangle^Z \big) = \sum_{s \in \{0,1\}^k} |s\rangle^Y \otimes U_k \Pi_k^{s_k} \cdots U_1 \Pi_1^{s_1} \big((Q_0 |0\rangle) |\psi\rangle \big).$$

Hence,

$$\begin{aligned}
& \left\| (Q_1 |0\rangle \langle 0| Q_1^*)^{CR} (U_k^{RZ} V_k^{RZY_k} \cdots U_1^{RZ} V_1^{RZY_1}) \left(|0^k\rangle^Y Q_0 |0\rangle^{CR} |\psi\rangle^Z \right) \right\|^2 \\
= & \left\| \sum_{s\in\{0,1\}^k} |s\rangle^Y \otimes (Q_1 |0\rangle \langle 0| Q_1^*) U_k \Pi_k^{s_k} \cdots U_1 \Pi_1^{s_1} \left((Q_0 |0\rangle) |\psi\rangle \right) \right\|^2 \\
= & \sum_{s\in\{0,1\}^k} \left\| |s\rangle \otimes (Q_1 |0\rangle \langle 0| Q_1^*) U_k \Pi_k^{s_k} \cdots U_1 \Pi_1^{s_1} \left((Q_0 |0\rangle) |\psi\rangle \right) \right\|^2 \\
\geq & \left\| |1^k\rangle \otimes (Q_1 |0\rangle \langle 0| Q_1^*) U_k \Pi_k^1 \cdots U_1 \Pi_1^1 \left((Q_0 |0\rangle) |\psi\rangle \right) \right\|^2 \\
= & \left\| (Q_1 |0\rangle \langle 0| Q_1^*) U_k \Pi_k \cdots U_1 \Pi_1 \left((Q_0 |0\rangle) |\psi\rangle \right) \right\|^2 \\
= & \left\| (Q_1 |0\rangle \langle 0| Q_1^*) \Gamma \left((Q_0 |0\rangle) |\psi\rangle \right) \right\|^2 .
\end{aligned}$$

While the r.h.s. of the inequality above is exactly what we want to bound, the l.h.s. can be bounded by ϵ^2 due to the inequality (2) (which holds for any efficiently realizable unitary transformation and any auxiliary input state, in particular the unitary $U_k V_k \cdots U_1 V_1$ and the state $|0^k\rangle |\psi\rangle$, respectively). Then take the square root of both sides will finish the proof of the first inequality. ■

A straightforward corollary of the lemma above in the following will also be useful in our security analysis.

Corollary 5 *Inherit all notations in Definition 3. Operator Γ is the same as introduced in Lemma 4. Quantum states $|\psi_0\rangle, |\psi_1\rangle$ are two possible states of the register Z. Then*

$$\left| ((\langle 0| Q_1^\dagger)^{CR} \langle \psi_1|^Z) \Gamma^{RZ} \left((Q_0 |0\rangle)^{CR} |\psi_0\rangle^Z \right) \right| < \epsilon(n).$$

Proof:

$$\left| ((\langle 0| Q_1^\dagger)^{CR} \langle \psi_1|^Z) \Gamma^{RZ} \left((Q_0 |0\rangle)^{CR} |\psi_0\rangle^Z \right) \right| \leq \left\| (Q_1 |0\rangle \langle 0| Q_1^*)^{CR} \Gamma^{RZ} \left((Q_0 |0\rangle)^{CR} |\psi_0\rangle^Z \right) \right\| < \epsilon(n).$$

■

4 The predicate-binding property of quantum string commitment

In this section, we first introduce the notion of **NP**-predicate and then the predicate-binding property of quantum string commitments. Next, we show that the parallel composition of a generic quantum computationally-binding bit commitment scheme gives rise to a quantum string commitment scheme that is predicate-binding w.r.t. a pair of inconsistent **NP**-predicates of a special form. Last, we extend this predicate-binding property to a setting that is sufficient for our application, i.e. quantum zero-knowledge argument for **NP**.

4.1 NP-predicate

Informally, the **NP**-predicate defined in the below states that for a string to satisfy some predicate, it should exhibit a certain "pattern" somewhere. The intuition underlying our definition is that in typical applications of bit commitments, the receiver will check whether the opened commitments will cause it to accept.

Definition 6 (NP-predicate) An ***NP****-predicate* P on binary strings $\{0,1\}^m$ ($m \geq 1$) can be represented by a pair of functions $(T(\cdot), s(\cdot))$, where: given a witness $w \in \{0,1\}^{\mathrm{poly}(m)}$, $T(w)$ is a subset of $\{1,2,\ldots,m\}$ and $s(w)$ is a string of length $|T(w)|$; both $T(w)$ and $s(w)$ can be computed in $\mathrm{poly}(m)$ time. A string $str \in \{0,1\}^m$ *satisfies* the predicate P if there exists a *witness* $w \in \{0,1\}^{\mathrm{poly}(m)}$ satisfying $str[T(w)] = s(w)$, where $str[T(w)]$ denotes the substring obtained from the string str by projecting it on coordinates in the subset $T(w)$.

In this work, for convenience we often drop the prefix "**NP**" and just write the "predicate" to refer to an **NP**-predicate. For a predicate P, it induces a subset P (by abusing the notation) of strings in $\{0,1\}^m$ such that a string $s \in P$ if and only if it *satisfies* the predicate P; we will identify a predicate as the subset induced by it. We say that two predicates P_1, P_2 on the set $\{0,1\}^m$ are *inconsistent* if $P_1 \cap P_2 = \emptyset$; that is, no strings in $\{0,1\}^m$ can satisfy both P_1 and P_2 simultaneously.

Consider a larger protocol within which commitments are used. At some stage of a running of this protocol, the party who plays the role of the possibly *cheating* sender of commitments will open commitments, and the party who plays the role of the *honest* receiver of commitments will do some verification. It is this verification that natually induces an **NP**-predicate, which will be referred to as the *predicate induced by openig commitments*. See the following example.

Example. Consider a running of Blum's zero-knowledge protocol for the **NP**-complete language Hamiltonian Cycle, in which the verifier is *honest* while the prover might be *cheating*, and the common input graph G has n vertices. Let $m = n^2$. Graphs of n vertices can be represented by strings of length m. This running of Blum's protocol induces two predicates on strings over $\{0,1\}^m$, corresponding to the verifier's verifications w.r.t. two possible challenges, respectively. In more detail, when the verifier's challenge is 0, it will check that all bit commitments are opened as a graph that is isomorphic to the input graph. This induces a predicate P_0 which consists of all graphs that are isomorphic to the input graph. Moreover, for each graph in P_0, any isomorphism π between this graph and the input graph can serve as its witness; in particular, $T(\cdot) \equiv \{1,2,\ldots,m\}$ and $s(\pi) = \pi(G)$. When the verifier's challenge is 1, it will check that n (out of n^2) bit commitments are opened as all 1's; moreover, these n positions (of bit commitments to open) should correspond to a possible location of a Hamiltonian cycle. This induces a predicate P_1 which consists of all graphs containing a Hamiltonian cycle. Moreover, for each graph in P_1, the location of any of its Hamiltonian cycle H can serve as its witness; in particular, $T(H)$ is set of coordinates corresponding to edges of H and $s(\cdot) \equiv 1^n$. If the input graph is *not* Hamiltonian, then the two predicates P_0 and P_1 are clearly inconsistent.

4.2 String predicate-binding

We first give an informal definition of the predicate-binding property of a quantum string commitment scheme, and then make it formal w.r.t. the scheme obtained by composing a generic quantum bit commitment scheme in parallel.

Definition 7 (Predicate-binding, informal) Let P_1, P_2 be two *inconsistent* **NP**-predicates. We say that a quantum string commitment scheme is *predicate-binding w.r.t.* (P_1, P_2) if any cheating sender, who can succeed in convincing the receiver that the committed value of the (claimed) quantum string commitment satisfies the predicate P_1 with *certainty*, will fail to convince the receiver that the committed value satisfies the predicate P_2 (except for a *negligible* probability). We say that a quantum string commitment scheme is *predicate-binding* if it is predicate-binding w.r.t. any pair of inconsistent predicates.

Remark. Classical commitment secure against classical attacks is trivially predicate-binding, simply because there is at most one string (i.e. the committed value) associated with each (claimed) commitment. However, this no longer holds w.r.t. either classical or quantum commitment secure against quantum attacks.

Now we restrict to consider the quantum string commitment scheme obtained by composing a generic quantum bit commitment scheme (Q_0, Q_1) in parallel. We know that this resulting quantum string commitment scheme is honest-binding [Yan20]. Our goal is to show that it also satisfies the predicate-binding property, which is *stronger* than honest-binding property and turns out to be more useful in security analysis of quantum cryptography.

Suppose that a cheating sender who is modeled as in Section 2.2 tries to convince the (honest) receiver that the committed value of a (claimed) quantum string commitment satisfies a predicate P, i.e. the (claimed) commitment can be opened in such a way that if the witness is w then the bit commitments indexed by the subset $T(w)$ are opened as the string $s(w)$. The predicate P natually induces a *projector* P (also by abusing the notation) whose expression is given by

$$P = \sum_{w} \left(|w\rangle \langle w| \right)^{D} \otimes \left(Q_{s(w)} |0\rangle \langle 0| Q_{s(w)}^{\dagger} \right)^{C^{\otimes T(w)} R^{\otimes T(w)}}, \tag{5}$$

where the summation is over all legal witnesses for m-bit strings in P_1 and the quantum circuit $Q_{s(w)}$ (whose meaning is referred to the equation (4)) performs on the copies of the quantum register pair (C, R) indexed by the subset $T(w)$; in the reveal stage, the receiver will perform the binary *measurement* $\{P, \mathbb{1} - P\}$ to decide whether to accept or not. Hence, the sender's success probability of convincing the receiver to accept is given by $\|PU |\psi\rangle\|^2$, where recall that the $|\psi\rangle$ is the quantum state of the whole system at the end of the commit stage and the U is the sender's operation in the reveal stage.

Based on the expression (5), we can formalize the predicate-binding property of the parallelization of a generic quantum bit commitment scheme as follows.

Definition 8 (Predicate-binding w.r.t. the parallel composition of QBC) Let P_1, P_2 be two *inconsistent* **NP**-predicates. We say that the quantum string commitment scheme obtained by composing a generic quantum bit commitment scheme (Q_0, Q_1) in parallel is *predicate-binding w.r.t.* (P_1, P_2) if $\|P_2 U P_1 |\psi\rangle\|^2$ is negligible, where $|\psi\rangle$ is an arbitrary state of registers $(\mathsf{C}^{\otimes m}, \mathsf{R}^{\otimes m}, \mathsf{D}, \mathsf{Z})$, and U could be any efficiently realizable unitary transformations that do not touch the quantum commitment (i.e. the quantum register $\mathsf{C}^{\otimes m}$). We say that this quantum string commitment scheme is *predicate-binding* if it is predicate-binding w.r.t. any pair of inconsistent predicates.

4.3 A special case

We first restrict to consider a special kind of predicates which arise in the setting where a generic quantum bit commitment scheme is run *stand-alone* to commit a string bitwisely, and later *all* (bit) commitments are to open. Thus, the witness for any string over $\{0,1\}^m$ that satisfies such kind of predicates could be the string itself. That is, for such a predicate $P = (T(\cdot), s(\cdot))$, it holds that $T(\cdot) \equiv \{1, 2, \ldots, m\}$, and $s(\cdot)$ is the identity function. Imposing these restrictions on the equation (5), the expression of the projector P becomes

$$P = \sum_{s \in P} \left(|s\rangle \langle s| \right)^{D} \otimes \left(Q_s |0\rangle \langle 0| Q_s^{\dagger} \right)^{C^{\otimes m} R^{\otimes m}}. \tag{6}$$

For any inconsistent predicate pair (P_1, P_2) such that both predicates P_1 and P_2 are of the form (6), we have the following main technical lemma of this work.

Lemma 9 *Suppose that the scheme (Q_0, Q_1) is computationally ϵ-binding for some arbitrary negligible function $\epsilon(\cdot)$. Both predicates P_1 and P_2 are of the form given by the expression (6). Then for any quantum state $|\psi\rangle$ of registers $(\mathsf{C}^{\otimes m}, \mathsf{R}^{\otimes m}, \mathsf{D}, \mathsf{Z})$, and any efficiently realizable unitary transformation U that does not touch the commitment registers $\mathsf{C}^{\otimes m}$, we have $\|P_2 U P_1 |\psi\rangle\|^2 \leq m^2\epsilon^2 + 2m\epsilon$.*

Proof: According to the expression (6), we can write

$$P_1 |\psi\rangle = \sum_{s \in P_1} \alpha_s |s\rangle^D \otimes Q_s |0\rangle^{C^{\otimes m} R^{\otimes m}} \otimes |\phi_s\rangle^Z \tag{7}$$

$$= \sum_{s \in \{0,1\}^m} \alpha_s |s\rangle^D \otimes Q_s |0\rangle^{C^{\otimes m} R^{\otimes m}} \otimes |\phi_s\rangle^Z , \tag{8}$$

where for $s \notin P_1$, we let $\alpha_s = 0$ and $|\phi_s\rangle$ be arbitrary; moreover, the complex coefficients α_s's satisfy $\sum_{s\in\{0,1\}^m} |\alpha_s|^2 \leq 1$. For convenience, we introduce the shorthand

$$|\psi_s\rangle \stackrel{def}{=} |s\rangle \otimes Q_s |0\rangle \otimes |\phi_s\rangle \tag{9}$$

for each $s \in \{0,1\}^m$. With these notations, our goal becomes to show

$$\Big\| P_2 U \sum_{s\in\{0,1\}^m} \alpha_s |\psi_s\rangle \Big\|^2 \leq m^2\epsilon^2 + 2m\epsilon. \tag{10}$$

We will actually prove a strengthening of the inequality (10) by induction. Specifically, we will prove that for each k $(0 \leq k \leq m)$ and each string $x \in \{0,1\}^{m-k}$, it holds that

$$\Big\| P_2 U \sum_{s\in\{0,1\}^k \circ x} \alpha_s |\psi_s\rangle \Big\|^2 \leq (m^2\epsilon^2 + 2k\epsilon) \sum_{s\in\{0,1\}^k \circ x} |\alpha_s|^2 , \tag{11}$$

where $\{0,1\}^k \circ x$ denotes the set of all m-bit strings with a suffix x of length $m-k$. If we view for each $x \in \{0,1\}^{m-k}$, where $0 \leq k \leq m$, it induces an internal node/leaf of a binarty tree which corresponds to the summation $P_2 U \sum_{s\in\{0,1\}^k \circ x} \alpha_s |\psi_s\rangle$, then we will bound the (squared) norm of each internal node in a bottom-up way. Thus, the root of the tree will correspond to the case where $k = m$ (then x becomes an empty string), i.e. l.h.s. of the inequality (10) without the squred norm. If we can prove the inequality (11), then plugging in $k = m$ and the inequality $\sum_{s\in\{0,1\}^m} |\alpha_s|^2 \leq 1$, we will arrive at the inequality (10).

Now we are ready to prove the inequality (11) by induction on k, where $0 \leq k \leq m$.

Base. We show that the inequality (11) holds when $k = 0$. In this case, x is a string of length m. Since the coefficient $\alpha_x = 0$ for $x \notin P_1$, in which case the inequality (11) holds trivially, we suffice to fix an arbitrary $x \in P_1$ and show that $\|P_2 U |\psi_x\rangle\| \leq m\epsilon$. To this end, our technique is the *perturbation* that is similar to the quantum statistical binding setting [FUYZ20]. Specifically, we will first show that the unit vector $U |\psi_x\rangle$ is *negligibly close* to the (unnormalized) vector

$$|\tilde{\psi}_x\rangle \stackrel{def}{=} \bigotimes_{i=1}^{m} \big(\mathbb{1} - (Q_{\bar{x}_i} |0\rangle \langle 0| Q_{\bar{x}_i}^\dagger)\big) U |\psi_x\rangle , \tag{12}$$

where $\bar{x}_i = 1 - x_i$, and the projector $Q_{\bar{x}_i} |0\rangle \langle 0| Q_{\bar{x}_i}^\dagger$ performs on the i-the copy of the register pair (C, R). Second, we show that from the inconsistency of the predicate pair (P_1, P_2), it follows

that the vector $|\tilde{\psi}_x\rangle$ is *orthogonal* to the subspace P_2. Combining these two facts, we know that $\|P_2U|\psi_x\rangle\|$ is negligible. Detail follows.

We first show that $\big\||\psi_x\rangle - |\tilde{\psi}_x\rangle\big\| < m\epsilon$ via a simple hybrid argument. Specifically, we introduce hybrids for each $0 \le j \le m$ such that $\mathsf{H}_j \stackrel{def}{=} \bigotimes_{i=1}^{j}(\mathbb{1} - Q_{\bar{x}_i}|0\rangle\langle 0|Q_{\bar{x}_i}^\dagger)U|\psi_x\rangle$; then $U|\psi_x\rangle = \mathsf{H}_0$ and $|\tilde{\psi}_x\rangle = \mathsf{H}_m$. We suffice to show that any two adjacent hybrids are negligibly close: if this is true, then applying the triangle inequality of the operator norm m times will yield the desired bound.

Indeed, for each $1 \le j \le m$,

$$\begin{aligned}
& \|\mathsf{H}_j - \mathsf{H}_{j-1}\| \\
= & \left\| \bigotimes_{i=1}^{j}(\mathbb{1} - Q_{\bar{x}_i}|0\rangle\langle 0|Q_{\bar{x}_i}^\dagger)U|\psi_x\rangle - \bigotimes_{i=1}^{j-1}(\mathbb{1} - Q_{\bar{x}_i}|0\rangle\langle 0|Q_{\bar{x}_i}^\dagger)U|\psi_x\rangle \right\| \\
\le & \left\| (\mathbb{1} - Q_{\bar{x}_j}|0\rangle\langle 0|Q_{\bar{x}_j}^\dagger)U|\psi_x\rangle - U|\psi_x\rangle \right\| \\
= & \left\| (Q_{\bar{x}_j}|0\rangle\langle 0|Q_{\bar{x}_j}^\dagger)U(|x\rangle Q_x|0\rangle|\phi_x\rangle) \right\| \\
< & \ \epsilon,
\end{aligned}$$

where the last "<" follows from Lemma 4 by considering the j-th quantum bit commitment. In greater detail, to apply Lemma 4 we replace the $|\psi\rangle$ and T in Lemma 4 with $|x\rangle\left(\bigotimes_{i\neq j} Q_{x_i}|0\rangle\right)|\phi_x\rangle$ and U here, respectively.

We then show that the (unnormalized) vector $|\tilde{\psi}_x\rangle$ is orthogonal to the subspace P_2, i.e. $\big\|P_2|\tilde{\psi}_x\rangle\big\| = 0$. This follows straightforwardly from the assumption that the predicate P_2 is *inconsistent* with the predicate P_1. In greater detail, for each $s \in P_2$, we know that it is *different* from the string $x \in P_1$; that is, there exists some index j ($1 \le j \le m$) such that $s_j = \bar{x}_j$. Combining this with the equation (12), it follows that

$$\begin{aligned}
& \left\| (|s\rangle\langle s| \otimes Q_s|0\rangle\langle 0|Q_s^\dagger)|\tilde{\psi}_x\rangle \right\| \le \left\| (Q_s|0\rangle\langle 0|Q_s^\dagger)|\tilde{\psi}_x\rangle \right\| \\
\le & \left\| (Q_{\bar{x}_j}|0\rangle\langle 0|Q_{\bar{x}_j}^\dagger)\Big(\bigotimes_{i=1}^{m}(\mathbb{1} - (Q_{\bar{x}_i}|0\rangle\langle 0|Q_{\bar{x}_i}^\dagger))U|\psi_x\rangle\Big) \right\| \\
= & \ 0.
\end{aligned}$$

Then summing over all $s \in P_2$, we obtain

$$\Big\| \sum_{s\in P_2} (|s\rangle\langle s| \otimes Q_s|0\rangle\langle 0|Q_s^\dagger)|\tilde{\psi}_x\rangle \Big\| = \big\|P_2|\tilde{\psi}_x\rangle\big\| = 0.$$

Combining $\big\||\psi_x\rangle - |\tilde{\psi}_x\rangle\big\| < m\epsilon$ with $\big\|P_2|\tilde{\psi}_x\rangle\big\| = 0$, we arrive at $\|P_2U|\psi_x\rangle\| \le m\epsilon$.

Induction. Now suppose that the inequality (11) holds for $k-1$ and each binary string x of length $m-(k-1)$. We are to show that it also holds for k and an arbitrary binary string x of length of $m-k$.

For an arbitrary $x \in \{0,1\}^{m-k}$, we first expand the l.h.s. of the inequality (11):

$$\begin{aligned}
&\left\| P_2 U \sum_{s\in\{0,1\}^k \circ x} \alpha_s |\psi_s\rangle \right\|^2 = \left\| P_2 U \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s |\psi_s\rangle + P_2 U \sum_{s'\in\{0,1\}^{k-1}\circ 1x} \alpha_{s'} |\psi_{s'}\rangle \right\|^2 \\
\leq\ & \left\| P_2 U \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s |\psi_s\rangle \right\|^2 + \left\| P_2 U \sum_{s'\in\{0,1\}^{k-1}\circ 1x} \alpha_{s'} |\psi_{s'}\rangle \right\|^2 \qquad (13) \\
&+2 \left| \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s \langle\psi_s| \cdot U^\dagger P_2 U \cdot \sum_{s'\in\{0,1\}^{k-1}\circ 1x} \alpha_{s'} |\psi_{s'}\rangle \right|.
\end{aligned}$$

For convenience, we introduce shorthands

$$\alpha_{0x}^2 \stackrel{def}{=} \sum_{s\in\{0,1\}^{k-1}\circ 0x} |\alpha_s|^2, \qquad \alpha_{1x}^2 \stackrel{def}{=} \sum_{s'\in\{0,1\}^{k-1}\circ 1x} |\alpha_{s'}|^2, \qquad \alpha_x^2 \stackrel{def}{=} \alpha_{0x}^2 + \alpha_{1x}^2.$$

Without loss of generality, we can assume that all $\alpha_{0x}, \alpha_{1x}, \alpha_x \geq 0$. With these notations, our goal (i.e. inequality (11)) becomes to show

$$\left\| P_2 U \sum_{s\in\{0,1\}^k \circ x} \alpha_s |\psi_s\rangle \right\|^2 \leq \alpha_x^2 (m^2\epsilon^2 + 2k\epsilon),$$

and the induction hypothesis implies

$$\left\| P_2 U \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s |\psi_s\rangle \right\|^2 \leq \alpha_{0x}^2 (m^2\epsilon^2 + 2(k-1)\epsilon),$$

$$\left\| P_2 U \sum_{s\in\{0,1\}^{k-1}\circ 1x} \alpha_s |\psi_s\rangle \right\|^2 \leq \alpha_{1x}^2 (m^2\epsilon^2 + 2(k-1)\epsilon).$$

The remainder of the analysis splits into two cases.

Case 1: either $\alpha_{0x} = 0$ or $\alpha_{1x} = 0$. Without loss of generality, we can assume that $\alpha_{1x} = 0$. This implies that $\alpha_{s'} = 0$ for each $s' \in \{0,1\}^{k-1} \circ 1x$. Thus,

$$\left\| P_2 U \sum_{s\in\{0,1\}^k \circ x} \alpha_s |\psi_s\rangle \right\|^2 = \left\| P_2 U \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s |\psi_s\rangle \right\|^2 \leq \alpha_{0x}^2 (m^2\epsilon^2 + 2(k-1)\epsilon) \leq \alpha_x^2 (m^2\epsilon^2 + 2k\epsilon),$$

where the first "$\leq$" uses the induction hypothesis.

Case 2: both $\alpha_{0x} > 0$ and $\alpha_{1x} > 0$. Following the inequality (13) and using the induction hypothesis, we have

$$\begin{aligned}
\left\| P_2 U \sum_{s\in\{0,1\}^k \circ x} \alpha_s |\psi_s\rangle \right\|^2 \ \leq\ & \alpha_{0x}^2 (m^2\epsilon^2 + (k-1)\epsilon) + \alpha_{1x}^2 (m^2\epsilon^2 + 2(k-1)\epsilon) \\
& + 2\alpha_{0x}\alpha_{1x} \cdot \underbrace{\left| \frac{1}{\alpha_{0x}} \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s \langle\psi_s| \cdot U^\dagger P_2 U \cdot \frac{1}{\alpha_{1x}} \sum_{s'\in\{0,1\}^{k-1}\circ 1x} \alpha_{s'} |\psi_{s'}\rangle \right|}_{(*)}.
\end{aligned}$$

We claim (refer to Claim 10 in the below) that the absolute value $(*)$ in the above can be bounded by 2ϵ. Then

$$\begin{aligned}\left\| P_2 U \sum_{s\in\{0,1\}^k \circ x} \alpha_s |\psi_s\rangle \right\|^2 &\leq (\alpha_{0x}^2 + \alpha_{1x}^2)(m^2\epsilon^2 + 2(k-1)\epsilon) + 2\alpha_{0x}\alpha_{1x}\cdot 2\epsilon \\ &\leq (\alpha_{0x}^2 + \alpha_{1x}^2)(m^2\epsilon^2 + 2(k-1)\epsilon) + (\alpha_{0x}^2 + \alpha_{1x}^2)\cdot 2\epsilon \\ &= \alpha_x^2(m^2\epsilon^2 + 2k\epsilon).\end{aligned}$$

The induction step is thus completed in both cases.

We finish the proof the inequality (11), and in turn the whole lemma. ■

We are left to prove the following claim.

Claim 10 *The absolute value* $(*)$ *is less than* 2ϵ.

Proof: Inherit all notations introduced within the statement and the proof of Lemma 9. Our idea is (again) using perturbation. Detail follows.

Plugging in the equation (9), *unit* vectors

$$1/\alpha_{0x} \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s |\psi_s\rangle \qquad \text{and} \qquad 1/\alpha_{1x} \sum_{s'\in\{0,1\}^{k-1}\circ 1x} \alpha_{s'} |\psi_{s'}\rangle$$

can be written in the form

$$Q_0|0\rangle \otimes |\xi_0\rangle \qquad \text{and} \qquad Q_1|0\rangle \otimes |\xi_1\rangle,$$

respectively, where both $Q_0|0\rangle$ and $Q_1|0\rangle$ are the states of the k-th quantum register pair (C, R), and

$$\begin{aligned}|\xi_0\rangle &= \frac{1}{\alpha_{0x}} \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s |s\rangle \otimes Q_{s[\bar{k}]}|0\rangle \otimes |\phi_s\rangle, \\ |\xi_1\rangle &= \frac{1}{\alpha_{1x}} \sum_{s'\in\{0,1\}^{k-1}\circ 1x} \alpha_{s'} |s'\rangle \otimes Q_{s'[\bar{k}]}|0\rangle \otimes |\phi_{s'}\rangle;\end{aligned}$$

here $s[\bar{k}]$ and $s'[\bar{k}]$ denote the substrings of s and s' with the k-th bit dropped, respectively.

We introduce more shorthands as follows:

$$\begin{aligned}|\eta_0\rangle &\stackrel{def}{=} U(Q_0|0\rangle \otimes |\xi_0\rangle), \quad |\tilde{\eta}_0\rangle \stackrel{def}{=} \big(\mathbb{1} - (Q_1|0\rangle\langle 0|Q_1^\dagger)\big)U(Q_0|0\rangle \otimes |\xi_0\rangle), \\ |\eta_1\rangle &\stackrel{def}{=} U(Q_1|0\rangle \otimes |\xi_0\rangle), \quad |\tilde{\eta}_1\rangle \stackrel{def}{=} \big(\mathbb{1} - (Q_0|0\rangle\langle 0|Q_0^\dagger)\big)U(Q_1|0\rangle \otimes |\xi_0\rangle),\end{aligned} \tag{14}$$

where both projectors $\mathbb{1} - (Q_1|0\rangle\langle 0|Q_1^\dagger)$ and $\mathbb{1} - (Q_0|0\rangle\langle 0|Q_0^\dagger)$ perform on the k-th quantum register pair (C, R). With these notations, our goal becomes to show

$$|\langle\eta_0| P_2 |\eta_1\rangle| < 2\epsilon.$$

To this end, it suffices to show:

1. $\| |\eta_0\rangle - |\tilde{\eta}_0\rangle \| < \epsilon$;
2. $\| |\eta_1\rangle - |\tilde{\eta}_1\rangle \| < \epsilon$;
3. $\langle \tilde{\eta}_0 | P_2 | \tilde{\eta}_1 \rangle = 0$.

This is because if all of the three items above hold, then a simple triangle inequality will finish the job.

Indeed, for the first item,

$$\| |\eta_0\rangle - |\tilde{\eta}_0\rangle \| = \left\| \left(Q_1 |0\rangle \langle 0| Q_1^\dagger\right) U \left(Q_0 |0\rangle \otimes |\xi_0\rangle\right) \right\| < \epsilon,$$

which follows immediately from the quantum computational binding property (Lemma 4).

Symmetrically, we can prove the second item.

For the third item, according to the equation (6),

$$\begin{aligned} P_2 &= \sum_{s \in P_2} \left(|s\rangle \langle s| \right)^D \otimes \left(Q_s |0\rangle \langle 0| Q_s^\dagger \right)^{C^{\otimes m} R^{\otimes m}} \\ &= \sum_{s \in P_2} \left(|s\rangle \langle s| \right)^D \otimes \left(Q_{s_k} |0\rangle \langle 0| Q_{s_k}^* \right) \otimes \left(Q_{s[\bar{k}]} |0\rangle \langle 0| Q_{s[\bar{k}]}^* \right), \end{aligned}$$

where the projector $Q_{s_k} |0\rangle \langle 0| Q_{s_k}^*$ performs on the k-th quantum register pair (C, R), and the projector $Q_{s[\bar{k}]} |0\rangle \langle 0| Q_{s[\bar{k}]}^*$ performs on the remaining $m-1$ copies of the quantum register pair (C, R). Whether $s_k = 0$ or 1, following from the equations in (14),

$$\langle \tilde{\eta}_0 | \left(Q_{s_k} |0\rangle \langle 0| Q_{s_k}^\dagger \right) | \tilde{\eta}_1 \rangle = 0.$$

Thus, $\langle \tilde{\eta}_0 | \left(|s\rangle \langle s| \otimes Q_{s_k} |0\rangle \langle 0| Q_{s_k}^\dagger \right) | \tilde{\eta}_1 \rangle = 0$. Summing over all $s \in P_2$ will yield $\langle \tilde{\eta}_0 | P_2 | \tilde{\eta}_1 \rangle = 0$.

This finishes the proof of the claim. ■

A closer look at our security reduction. In our security analysis above, we did *not* achieve a *uniform* security reduction; rather, we make an essential use of a certain amount of both classical and quantum *non-uniformity*. In greater detail, note that the only places we use the computational binding property of quantum *bit* commitment lies in the base step and in bounding the absolute value $(*)$ within the induction step (Claim 10). Thus, if there were a successful attack $(U, |\psi\rangle)$ of the predicate-binding property w.r.t. an inconsistent predicate pair (P_1, P_2), then by contradiction there are two possibilities:

1. The inequality (11) fails for $k = 0$, some $x \in \{0,1\}^m$, and the quantum state $|\psi_x\rangle$.
2. Claim 10 fails for some k where $1 \leq k \leq m$, some $x \in \{0,1\}^{m-k}$, and quantum states $1/\alpha_{0x} \sum_{s \in \{0,1\}^{k-1} \circ 0x} \alpha_s |\psi_s\rangle$ and $1/\alpha_{1x} \sum_{s' \in \{0,1\}^{k-1} \circ 1x} \alpha_{s'} |\psi_{s'}\rangle$.

Given the classical and quantum non-uniformity in either of the items above, we can construct an attack against the computational binding property of the scheme (Q_0, Q_1).

4.4 Extension

By slightly adapting its proof, we can extend Lemma 9 to hold for a more general inconsistent predicate pair (P_1, P_2) so as to be useful in cryptographic applications. Specifically, we can prove the following theorem, whose formal statement is referred to Theorem 3.

Theorem 2 *Suppose that the quantum bit commitment scheme (Q_0, Q_1) is computationally binding. Let P_1, P_2 be two inconsistent predicates on the set $\{0,1\}^m$ such that for (at least) one of them, the verification of whether an m-bit string satisfies it needs to examine the bits at some fixed positions of the string (regardless of the given witness). Then the parallel composition of the scheme (Q_0, Q_1) gives rise to a quantum string commitment scheme that is computationally predicate-binding w.r.t. (P_1, P_2).*

In the remainder of this subsection, we will first sketch why such an extension as described in the theorem above is possible, and then state this theorem in a more formal way.

The generalization of the predicate P_2. It is not hard to extend Lemma 9 to the case in which the predicate P_2 is of the most *general* form as described by the equation (5) (while the restriction on the predicate P_1 remains the same). This extension turns out to be already sufficient for our application (section 5). Now let us briefly mention how to adapt the proof of Lemma 9 to this case in the below.

The proof of Lemma 9 is by induction. For the base step, which essentially relies on that the inconsistency of the two predicates P_1 and P_2 (without any restrictions on them), almost the same proof goes through. For the induction step, however, we will encounter new difficulty in bounding $\langle\tilde{\eta}_0| P_2 |\tilde{\eta}_1\rangle$ within the proof of Claim 10: now it may happen that some projectors of the form $|w\rangle\langle w| \otimes \left(Q_{s(w)} |0\rangle\langle 0| Q^\dagger_{s(w)}\right)$ in the summation over all legal witnesses of the equation (5) do not touch the k-th register pair (C, R). Thus, new technique is needed to handle such projectors for the purpose of bounding the absolute value $(*)$. Actually, this is where we really need to generalize the (standard) quantum computational binding property (refer to Definition 3) so that it can cope with not only unitary transformations but also projectors (Lemma 4).

In further detail, to bound the absolute value $(*)$ now we divide the summation over all legal witnesses in the equation (5) into two parts: the summations of those projectors that touch the k-th register pair (C, R), and those do not. Correspondingly, we can first bound the absolute value of each of these two parts separately, and then use the triangle inequality to get a bound of the absolute value $(*)$. In particular, the absolute value of the former part can be bounded by 2ϵ in a similar way as that of the proof of Claim 10, whereas the absolute value of the latter part can be bounded by ϵ, thanks to the generalized computational binding property (Lemma 4). Combing them we obtain a 3ϵ bound of the absolute value $(*)$ in case of the generalized predicate P_2.

The generalization of the predicate P_1. Unfortunately, it seems unlikely that we can generalize the predicate P_1 to the most general form (5) like the predicate P_2 above by our technique. This is because the special form of the projector P_1 (equation (6)) seem to play an important role in bounding the absolute value $(*)$ in the induction proof of Lemma 9. In more detail, it seems that we make an essential of the following *structure* of the superposition (8) (which is induced by the projector P_1): for distinct $s, s' \in \{0,1\}^m$, say $s_i \neq s'_i$, the projections of unit vectors $|s\rangle^D \otimes Q_s |0\rangle^{C^{\otimes m} R^{\otimes m}} \otimes |\phi_s\rangle^Z$ and $|s'\rangle^D \otimes Q_{s'} |0\rangle^{C^{\otimes m} R^{\otimes m}} \otimes |\phi_{s'}\rangle^Z$ on the i-th quantum register pair (C, R) correspond to commitments to different bit value. It is this structure that makes our strategy of bounding the norm of the summation $P_2 U \sum_{s\in\{0,1\}^m} \alpha_s |\psi_s\rangle$ (i.e. the l.h.s. of the inequality (10)) work.

In spite of the difficulty mentioned above, we still can generalize the predicate P_1 to the case in which the associated function $T(\cdot)$ is any *constant* function; that is, which bits are to examine for the verification of P_1 are fixed. In comparison, in the special form given by the equation (6), the function $T(\cdot)$ is fixed to output the whole set and the function $s(\cdot)$ is fixed to be the identity function.

To have a glimpse of why such a generalization of P_1 is possible, we first rewrite its expression in a proper form. Specifically, let T_1 be the fixed subset that prescribes which bits are to examine for the verification of P_1. In this case whether a string $s \in \{0,1\}^m$ satisfies the predicate P_1 actually only depends on its substring $s[T_1]$. Let $l = |T_1|$. The predicate P_1 in turn induces a predicate $P_1[T_1]$ on the set $\{0,1\}^l$ such that all l bits are needed to be examined to check whether an l-bit string satisfies the predicate $P_1[T_1]$. Following the equation (5), the projector P_1 can be written as

$$P_1 = \sum_w \left(|w\rangle \langle w| \right)^D \otimes \left(Q_{s(w)} |0\rangle \langle 0| Q_{s(w)}^\dagger \right)^{C^{\otimes T_1} R^{\otimes T_1}} \tag{15}$$

$$= \sum_{s \in P_1[T_1]} \sum_{w:s(w)=s} \left(|w\rangle \langle w| \right)^D \otimes \left(Q_s |0\rangle \langle 0| Q_s^\dagger \right)^{C^{\otimes T_1} R^{\otimes T_1}}. \tag{16}$$

Note that for distinct $s, s' \in P_1[T_1]$, the two projectors $\sum_{w:s(w)=s} |w\rangle \langle w|$ and $\sum_{w:s(w)=s'} |w\rangle \langle w|$ are *orthogonal*. Then similar to the equation (7), we can write

$$P_1 |\psi\rangle = \sum_{s \in P_1[T_1]} \alpha_s |\omega_s\rangle^D \otimes Q_s |0\rangle^{C^{\otimes T_1} R^{\otimes T_1}} \otimes |\phi_s\rangle^{C^{\otimes (m-l)} R^{\otimes (m-l)} Z}, \tag{17}$$

where the unit vector $|\omega_s\rangle$ is of the form $\sum_{w:s(w)=s} \alpha_w |w\rangle^D$, vectors $|\omega_s\rangle$ and $|\omega_{s'}\rangle$ are orthogonal for distinct $s, s' \in P_1[T_1]$.

It is not hard to verify that if we replace this $P_1 |\psi\rangle$ given by the equation (17) with the one given by the equation (7) in the proof of Lemma 9, then almost the same proof goes through.

A formal statement of Theorem 2. It turns out that predicates P_1 and P_2 in Lemma 9 can be generalized in the way as discussed above *simultaneously*. Thus, Theorem 2 can be stated in a more formal way as in the theorem below, whose proof is deferred to Appendix A.

Theorem 3 *Suppose that the scheme (Q_0, Q_1) is computationally ϵ-binding. Let P_1, P_2 be two inconsistent predicates on the set $\{0,1\}^m$, which induce two projectors of the form (16) and (5), respectively. Then for any quantum state $|\psi\rangle$ of registers $(C^{\otimes m}, R^{\otimes m}, D, Z)$, and any efficiently realizable unitary transformation U that does not touch the commitment registers $C^{\otimes m}$, we have $\| P_2 U P_1 |\psi\rangle \|^2 \leq m^2 \epsilon^2 + 3m\epsilon$.*

5 Application: quantum zero-knowledge argument

In this section, we give an application of the quantum computationally predicate-binding string commitment scheme as shown in the proceeding section. Specifically, we show that Blum's protocol for the **NP**-complete language Hamiltonian Cycle [Blu86] with a generic quantum computationally-binding bit commitment scheme plugged in gives rise to a quantum zero-knowledge *argument* system. While its quantum (perfect or statistical) zero-knowledge property can be obtained by a straightforward application of Watrous's quantum rewinding technique [Wat09, Unr12, Unr16b, YWLQ15], its quantum computational soundness is established by Lemma 11 as stated below. Combing them we arrive at Theorem 1.

Lemma 11 *Blum's protocol for the language* Hamiltonian Cycle *with a generic quantum computationally-binding bit commitment scheme* (Q_0, Q_1) *plugged in is sound against any quantum provers who are polynomial-time bounded, with soundness error* $1/2 + negl(\cdot)$.

PROOF: This can be proved by instantiating Theorem 3 with proper predicates induced by Blum's protocol. Detail follows.

Suppose that the binding error of the scheme (Q_0, Q_1) is $\epsilon(\cdot)$, which is a negligible function. We inherit notations as introduced in Subsection 2.3. Following Subsection 2.2, we can model a generic attack of the prover of Blum's protocol in the following way. The combined (quantum) system of the (cheating) prover and the (honest) verifier is given by $(\mathsf{P}, \mathsf{D}, \mathsf{C}^{\otimes n^2}, \mathsf{R}^{\otimes n^2})$, where the n^2 copies of the register pair (C, R) are used for (in total n^2) quantum bit commitments; the register D will hold the classical information of the prover's response (i.e. the permutation π when the challenge $b = 0$ or the location of a Hamiltonian cycle H when $b = 1$); the register P is the prover's (private) workspace. Suppose that the whole system is initialized in the state $|\psi\rangle$. The prover sends the quantum register $\mathsf{C}^{\otimes n^2}$ to the verifier as its first message. Then depending on the challenge b, the prover will perform some polynomial-time realizable unitary transformation U_b on the registers $(\mathsf{P}, \mathsf{D}, \mathsf{R}^{\otimes n^2})$. After receiving the prover's response, the verifier will perform some binary measurement, which also depends on the challenge b (as prescribed in the below), to decide to whether accept or not.

Formally, depending on the challenge b, the verifier's accepting conditions induce two **NP**-predicates, which in turn induces two efficiently realizable projectors/binary measurements as follows:

1. The projector corresponding to $b = 0$ is given by

$$P_0 = \sum_{\pi \in S_n} \left(|\pi\rangle \langle \pi| \right)^D \otimes \left(Q_{\pi(G)} |0\rangle \langle 0| Q^\dagger_{\pi(G)} \right)^{C^{\otimes n^2} R^{\otimes n^2}}.$$

2. The projector corresponding to $b = 1$ is given by

$$P_1 = \sum_{H: n \text{ cycle}} \left(|H\rangle \langle H| \right)^D \otimes \left(Q_{1^n} |0\rangle \langle 0| Q^\dagger_{1^n} \right)^{C^{\otimes H} R^{\otimes H}},$$

   where the projector $Q_{1^n} |0\rangle \langle 0| Q^\dagger_{1^n}$ performs on the n copies of the register pair (C, R) that are determined by the location of the Hamiltonian cycle H.

We highlight that here we implicitly assume that the verifier just performs a big binary measurement (induced by either P_0 or P_1) to decide whether to accept or not; it in particular does not measure the register D to extract any classical information. It is easy to see that whether measuring the register D or not will not change the verifier's acceptance probability. But by doing this, we are then allowed to apply the quantum rewinding lemma (Lemma 1).

Now we are ready to argue the quantum computational soundness of Blum's protocol. Suppose for contradiction that there exists a efficiently realizable cheating prover given by $(|\psi\rangle, U_0, U_1)$ as aforementioned who can break the quantum computational soundness. Namely,

$$\frac{1}{2} \sum_{b \in \{0,1\}} \| P_b U_b |\psi\rangle \|^2 > \frac{1}{2} + n^{-c},$$

where c is some constant. Then applying the quantum rewinding lemma (Lemma 1), it follows that

$$\left\| P_1 U_1 U_0^\dagger P_0 U_0 \left|\psi\right\rangle \right\| > n^{-c}. \tag{18}$$

On the other hand, we invoke Theorem 3 by doing the replacements as summarized in the following table:

Theorem 3	Blum's protocol
m	n^2
Registers $(\mathsf{C}^{\otimes m}, \mathsf{R}^{\otimes m})$	Registers $(\mathsf{C}^{\otimes m}, \mathsf{R}^{\otimes m})$
Register D	Register D
Register Z	Register P
Projector P_1	Projector P_0
Projector P_2	Projector P_1
Quantum state $\left|\psi\right\rangle$	Quantum state $U_0 \left|\psi\right\rangle$
Unitary transformation U	Unitary transformation $U_1 U_0^\dagger$

In case that the input graph G is not Hamiltonian, the two predicates P_0 and P_1 are inconsistent. Applying Theorem 3 will yield an upper bound $n^4\epsilon^2 + 3n^2\epsilon$ of the squared norm $\left\| P_1 U_1 U_0^\dagger P_0 U_0 \left|\psi\right\rangle \right\|^2$, which is negligible. But this contradicts with the inequality (18).

We finish the proof of the lemma. ■

6 Conclusion and open problems

In this work, we show that the parallel composition of a generic quantum computationally-binding bit commitment scheme gives rise to a quantum *string* commitment scheme that is computationally predicate-binding. This new notion of quantum computational string binding property is stronger than the trivial honest-binding property, and turns out to be useful in constructing quantum zero-knowledge argument for **NP** languages. The main technical part of this work lies in establishing this quantum computational predicate-binding property, which is non-trivial.

There are many open problems following our work. In the below, we just mention some that interest us most:

1. Can we extend our technique to prove predicate-binding w.r.t. more general inconsistent predicate pair than the one stated in Theorem 3? Can we prove predicate-binding w.r.t. other inconsistent predicate pairs with inherently different *structures*?

2. Can we extend our technique to prove predicate-binding w.r.t. multiple (≥ 3) inconsistent predicates? If we can do this, then we may show that the GMW zero-knowledge protocol for the **NP**-complete language Graph 3-Coloring [GMW91] with a generic quantum computationally-binding bit commitment scheme plugged in gives rise to a quantum zero-knowledge argument.

3. Can we prove even stronger binding (than the predicate-binding) property of the quantum string commitment scheme obtained by composing a generic quantum computationally-binding bit commitment scheme in parallel? Further, if this is possible, then can it yield any interesting applications? In [CDMS04], a so-called computational f-*binding* property of

quantum string commitment scheme w.r.t. a function $f : \{0,1\}^m \to \{0,1\}^l$ is proposed, where integers $l \leq m$. Such binding property w.r.t. some particular functions turns out to be useful in constructing quantum oblivious transfer. Can we extend our technique to show f-binding of a generic quantum computationally-binding bit commitment scheme composed in parallel w.r.t. any interesting functions, in particular those needed in [CDMS04]? We note that the string predicate-binding property we established can also be viewed as f-binding w.r.t. to the efficiently computable function f whose image is just the set $\{0,1\}$, and the preimages mapped to 1 induce the prediate P_1 while the preimages mapped to 0 induce the prediate P_2.

We also note that in the case of quantum *statistical* binding, the strongest string binding property, so called the *string sum-binding*, can be established; it implies the statistical f-binding w.r.t. *any* function f [FUYZ20].

4. Can we show that plugging a generic quantum computationally-binding bit commitment scheme in a variant of Blum's protocol [Unr12, FUYZ20] gives rise to a quantum zero-knowledge argument-of-knowledge for the **NP**-complete language Hamiltonian Cycle?

5. How about plugging a generic computationally-binding quantum bit commitment scheme in [GK96] to obtain a quantum ϵ-zero-knowledge proof in constant rounds like in [CCY20]? If this is true, then we can relax the complexity assumption required in [CCY20] to quantum-secure one-way functions by a quantum construction.

Acknowledgements. We thank Dominique Unruh for helpful and inspiring discussions on the strictness of the quantum binding property and the possibility of basing quantum zero-knowledge argument for **NP** on computationally-binding quantum bit commitments at the early stage of this work.

References

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

[ARU14] Andris Ambainis, Ansis Rosmanis, and Dominique Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *FOCS*, pages 474–483, 2014. 3, 5, 7, 8

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

[BC90] Gilles Brassard and Claude Crépeau. Quantum bit commitment and coin tossing protocols. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 49–61. Springer, 1990. 3

[Blu86] Manuel Blum. How to prove a theorem so no one else can claim it. In *Proceedings of the International Congress of Mathematicians*, volume 1, page 2, 1986. 5, 8, 14, 25

[CCY20] Nai-Hui Chia, Kai-Min Chung, and Takashi Yamakawa. A black-box approach to post-quantum zero-knowledge in constant rounds. Cryptology ePrint Archive, Report 2020/1384, 2020. https://eprint.iacr.org/2020/1384. 28

[CDMS04] Claude Crépeau, Paul Dumais, Dominic Mayers, and Louis Salvail. Computational collapse of quantum state with application to oblivious transfer. In *TCC*, pages 374–393, 2004. 3, 4, 6, 7, 9, 27, 28

[CKR11] André Chailloux, Iordanis Kerenidis, and Bill Rosgen. Quantum commitments from complexity assumptions. In *ICALP (1)*, pages 73–85, 2011. 3

[CLS01] Claude Crépeau, Frédéric Légaré, and Louis Salvail. How to convert the flavor of a quantum bit commitment. In *EUROCRYPT*, pages 60–77, 2001. 3, 7

[DMS00] Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *EUROCRYPT*, pages 300–315, 2000. 3, 5, 7

[FUYZ20] Junbin Fang, Dominique Unruh, Jun Yan, and Dehua Zhou. How to base security on the perfect/statistical binding property of quantum bit commitment? 2020. https://eprint.iacr.org/2020/621. 3, 4, 5, 8, 9, 10, 12, 14, 19, 28

[GK96] Oded Goldreich and Ariel Kahan. How to construct constant-round zero-knowledge proof systems for NP. *J. Cryptol.*, 9(3):167–190, 1996. 28

[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. 27

[Gol01] Oded Goldreich. *Foundations of Cryptography, Basic Tools*, volume I. Cambridge University Press, 2001. 3

[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. 3

[KO09] Takeshi Koshiba and Takanori Odaira. Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. In *TQC*, pages 33–46, 2009. 3, 5, 7

[KO11] Takeshi Koshiba and Takanori Odaira. Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function. *arXiv:1102.3441*, 2011. 3, 5, 7

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

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

[MP12] Mohammad Mahmoody and Rafael Pass. The curious case of non-interactive commitments - on the power of black-box vs. non-black-box use of primitives. In *CRYPTO 2012*, pages 701–718, 2012. 3

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and Quantum Information*. Cambridge University Press, 2000. 12

[Unr12] Dominique Unruh. Quantum proofs of knowledge. In *EUROCRYPT*, pages 135–152, 2012. 3, 5, 7, 8, 25, 28

[Unr16a] Dominique Unruh. Collapse-binding quantum commitments without random oracles. In *ASIACRYPT*, pages 166–195, 2016. 3, 5, 7

[Unr16b] Dominique Unruh. Computationally binding quantum commitments. In *EUROCRYPT*, pages 497–527, 2016. 3, 5, 7, 25

[vdG97] Jeroen van de Graaf. *Towards a formal definition of security for quantum protocols*. PhD thesis, Université de Montréal, 1997. 4, 7

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. Preliminary version appears in *STOC* 2006. 1, 4, 13, 25

[Yan20] Jun Yan. General properties of quantum bit commitment. 2020. https://eprint.iacr.org/2020/1488. 3, 4, 5, 7, 8, 13, 18

[Yao93] Andrew Chi-Chih Yao. Quantum circuit complexity. In *FOCS*, pages 352–361, 1993. 12

[YWLQ15] Jun Yan, Jian Weng, Dongdai Lin, and Yujuan Quan. Quantum bit commitment with application in quantum zero-knowledge proof (extended abstract). In *ISAAC*, pages 555–565, 2015. 3, 4, 5, 6, 8, 9, 10, 25

A A proof of Theorem 3

We just highlight how to adapt the proof of Lemma 9 to the setting of Theorem 3, in which both predicates P_1 and P_2 are generalized in the way as stated in Section 4.4.

According to the equation (17), we can replace the equations (7), (8) in the proof of Lemma 9 with

$$\begin{aligned} P_1 |\psi\rangle &= \sum_{s\in P_1[T_1]} \alpha_s |\omega_s\rangle^D \otimes Q_s |0\rangle^{C^{\otimes T_1} R^{\otimes T_1}} \otimes |\phi_s\rangle^{C^{\otimes (m-l)} R^{\otimes (m-l)} Z} \\ &= \sum_{s\in\{0,1\}^l} \alpha_s |\omega_s\rangle^D \otimes Q_s |0\rangle^{C^{\otimes T_1} R^{\otimes T_1}} \otimes |\phi_s\rangle^{C^{\otimes (m-l)} R^{\otimes (m-l)} Z}, \end{aligned}$$

where for $s \notin P_1[T_1]$, we let $\alpha_s = 0$, and the corresponding $|\omega_s\rangle$ and $|\phi_s\rangle$ be arbitrary[8]; moreover, the complex coefficients α_s's satisfy $\sum_{s\in\{0,1\}^l} |\alpha_s|^2 \leq 1$. We similarly introduce the shorthand

$$|\psi_s\rangle \stackrel{def}{=} |\omega_s\rangle \otimes Q_s |0\rangle \otimes |\phi_s\rangle,$$

[8] We stress that our purpose of introducing $\alpha_s, |\omega_s\rangle, |\phi_s\rangle$ for $s \notin P_1[T_1]$ is mainly for a cleaner way of writing the proof; it will *not* affect the places in our proof where the (generalized) quantum computational binding property (Lemma 4) is applied.

and our goal becomes to show

$$\left\| P_2 U \sum_{s\in\{0,1\}^l} \alpha_s |\psi_s\rangle \right\|^2 \leq m^2\epsilon^2 + 3m\epsilon.$$

We are to strengthen the inequality above and prove by induction that for each k $(0 \leq k \leq l)$ and each string $x \in \{0,1\}^{l-k}$, it holds that

$$\left\| P_2 U \sum_{s\in\{0,1\}^k \circ x} \alpha_s |\psi_s\rangle \right\|^2 \leq (l^2\epsilon^2 + 3k\epsilon) \sum_{s\in\{0,1\}^k\circ x} |\alpha_s|^2 , \tag{19}$$

Base. We first show that the inequality (19) holds when $k = 0$. In this case, $x \in \{0,1\}^l$. Since the coefficient $\alpha_x = 0$ when $x \notin P_1[T_1]$, in which case the inequality (19) trivially hold, we suffice to fix an arbitrary $x \in P_1[T_1]$ and show that $\|P_2 U |\psi_x\rangle\| \leq l\epsilon$.

It is not hard to see that the proof of the base step of Lemma 9 almost goes through here, except that now we apply the perturbation $\bigotimes_{i=1}^{l} \left(\mathbb{1} - (Q_{\bar{x}_i} |0\rangle \langle 0| Q_{\bar{x}_i}^\dagger)\right)$ to the subspace induced by the l copies of the quantum register pair (C, R) indexed by the subset T_1. In more detail, we introduce the (unnormalized) vector

$$|\tilde{\psi}_x\rangle \stackrel{def}{=} \bigotimes_{i=1}^{l} \left(\mathbb{1} - Q_{\bar{x}_i} |0\rangle \langle 0| Q_{\bar{x}_i}^\dagger\right) U |\psi_x\rangle ,$$

which will play the same role of the equation (12) in the proof of the base step of Lemma 9. We remark that here we will make an essential use of the fact that predicates P_1 and P_2 are *inconsistent*, so that the string $s(w)$ w.r.t. each witness w within the expression of the projector P_2 (refer to the equation (5)) must differ with the string $x \in P_1[T_1]$ in at least one common coordinate $i \in T_1 \cap T_2(w)$.

Induction step. Now suppose that the inequality (19) holds for $k-1$ and each binary string x of the length $l-(k-1)$. We are to show that it also holds for k and an arbitrary binary string x of the length of $l-k$.

Similar to the induction step of the proof of Lemma 9, now for each $x \in \{0,1\}^{l-k}$, we similarly introduce shorthands

$$\alpha_{0x}^2 \stackrel{def}{=} \sum_{s\in\{0,1\}^{k-1}\circ 0x} |\alpha_s|^2 , \qquad \alpha_{1x}^2 \stackrel{def}{=} \sum_{s'\in\{0,1\}^{k-1}\circ 1x} |\alpha_{s'}|^2 , \qquad \alpha_x^2 \stackrel{def}{=} \alpha_{0x}^2 + \alpha_{1x}^2,$$

where $\alpha_{0x}, \alpha_{1x}, \alpha_x \geq 0$. Then our goal becomes to show that

$$\left\| P_2 U \sum_{s\in\{0,1\}^k\circ x} \alpha_s |\psi_s\rangle \right\|^2 \leq \alpha_x^2 (l^2\epsilon^2 + 3k\epsilon).$$

Indeed,

$$\begin{aligned}
&\left\| P_2 U \sum_{s\in\{0,1\}^k\circ x} \alpha_s |\psi_s\rangle \right\|^2 = \left\| P_2 U \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s |\psi_s\rangle + P_2 U \sum_{s'\in\{0,1\}^{k-1}\circ 1x} \alpha_{s'} |\psi_{s'}\rangle \right\|^2 \\
\leq\ &\left\| P_2 U \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s |\psi_s\rangle \right\|^2 + \left\| P_2 U \sum_{s'\in\{0,1\}^{k-1}\circ 1x} \alpha_{s'} |\psi_{s'}\rangle \right\|^2 \\
&+2\left| \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s \langle\psi_s| \cdot U^\dagger P_2 U \cdot \sum_{s'\in\{0,1\}^{k-1}\circ 1x} \alpha_{s'} |\psi_{s'}\rangle \right|.
\end{aligned}$$

The remaining analysis also splits into two cases like that of the proof of Lemma 9, depending on whether at least one of α_{0x} or α_{1x} are zero. Now in the case that both $\alpha_{0x} > 0$ and $\alpha_{1x} > 0$, we will encounter new difficulty in bounding the absolute value

$$\Big|\frac{1}{\alpha_{0x}} \sum_{s\in\{0,1\}^{k-1}\circ 0x} \alpha_s \langle\psi_s| \cdot U^\dagger P_2 U \cdot \frac{1}{\alpha_{1x}} \sum_{s'\in\{0,1\}^{k-1}\circ 1x} \alpha_{s'} |\psi_{s'}\rangle \Big|, \tag{20}$$

the counterpart of the absolute value $(*)$ within the proof of Lemma 9.

We will bound the expression (20) by 3ϵ in the following claim, which can be viewed as the counterpart of Claim 10. Once this is done, then we can complete the induction step similarly to that of the proof of Lemma 9 and establish Theorem 3.

We are left to prove the following claim.

Claim 12 *The expression (20) is less than* 3ϵ.

Proof Sketch: We just highlight how to adapt the proof of Claim 10 to the setting here.

Compared with the proof of Claim 10, the new difficulty is: since now the projector P_2 is of the most general form as given by the equation (5), it could happen that for some projector $|w\rangle\langle w| \otimes Q_{s(w)} |0\rangle\langle 0| Q^\dagger_{s(w)}$ in the summation of P_2, $k \notin T(w)$; that is, this projector does not touch the k-th quantum register pair (C, R). This will cause our argument for the equality $\langle\tilde{\eta}_0| P_2 |\tilde{\eta}_1\rangle = 0$ within the proof of Claim 10 to fail.

To overcome this new difficulty, our idea is to split the projector P_2 into two parts: the sum of projectors that touch the k-th quantum register pair (C, R), i.e. $k \in T(w)$, which we denote by P_2^1, and the sum of those do not, which we denote by P_2^2. Then for the projector P_2^1, almost the same proof as that of Claim 10 will yield an upper bound 2ϵ, whereas for the projector P_2^2, we will use the generalized quantum computational binding property (Lemma 4) to obtain an upper bound ϵ.

In more detail, after introducing similar notations $|\xi_0\rangle, |\xi_1\rangle, |\eta_0\rangle, |\eta_1\rangle, |\tilde{\eta}_0\rangle, |\tilde{\eta}_1\rangle$ as in the proof of Claim 10, our goal is to show that $|\langle\eta_0| P_2 |\eta_1\rangle| < 3\epsilon$. Plugging in $P_2 = P_2^1 + P_2^2$, we will prove that

1. $\big|\langle\eta_0| P_2^1 |\eta_1\rangle\big| < 2\epsilon$, and
2. $\big|\langle\eta_0| P_2^2 |\eta_1\rangle\big| < \epsilon$.

For the item 1, by the property of the projector P_2^1, i.e. each projector in the summation of P_2^1 touches the k-th quantum register pair (C, R), almost the same proof as that of Claim 10 will yield the same upper bound 2ϵ.

For the item 2, the projector P_2^2 does *not* touch the k-th quantum register pair (C, R). We then apply Corollary 5, with the operator Γ replaced by $UP_2^2U^\dagger$, which will yield $\big|\langle\eta_0| P_2^2 |\eta_1\rangle\big| < \epsilon$. We additionally highlight that to apply Corollary 5, we need to show that the projector P_2^2 is efficiently realizable given that the projector P_2 is. This is indeed the case: conditioned on a quantum state collapsing to the subspace induced by the projector P_2, we can further compute the function $T(w)$ given the witness w and check that $k \notin T(w)$.

Combining items 1 and 2 above, the absolute value (20) can be bound by 3ϵ. This finishes the proof of the claim. ■