Quantum Bit Commitment with Application in Quantum Zero-Knowledge Proof

Dongdai Lin[2], Yujuan Quan[1], Jian Weng[1], and Jun Yan[1,2]

[1]Jinan University
quanyj@126.com, {*cryptjweng, complexityan*}*@gmail.com*
[2]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences
ddlin@iie.ac.cn

October 4, 2014

Abstract

Watrous (STOC 2006) proved that plugging classical bit commitment scheme that is secure against quantum attack into the GMW-type construction of zero-knowledge gives a classical zero-knowledge proof that is secure against quantum attack. In this paper, we showed that plugging quantum bit commitment scheme (allowing quantum computation and communication) into the GMW-type construction also gives a quantum zero-knowledge proof, as one expects. However, since the binding condition of quantum bit commitment scheme is inherently different from its classical counterpart, compared with Watrous' security proof, here we encounter new difficulty in soundness analysis. To overcome the difficulty, we take a geometric approach, managing to reduce quantum soundness analysis to classical soundness analysis.

We also propose a formalization of non-interactive quantum bit commitment scheme, which may come in handy in other places. Moreover, inspired by our formalization, we generalize Naor's construction of bit commitment scheme to the quantum setting, achieving non-interactive commit stage.

We hope quantum bit commitment scheme can find more applications in quantum cryptography.

1 Introduction

Zero-knowledge (**ZK**) is an important concept in both cryptography and complexity theory. Roughly speaking, compared with **NP** proof system (in which prover sends witness to verifier for verification), through zero-knowledge proof prover can convince verifier to accept without leaking anything that is hard to compute, i.e. *knowledge*, in particular the witness [1]. *Bit commitment scheme* (**BC**) is a two-stage (first a commit stage followed by a reveal stage) interactive cryptographic protocol between sender and receiver; its security consists of two aspects: the security against receiver, known as *hiding*, roughly says receiver cannot guess the committed bit during the commit stage. The security against sender, known as *binding*, says sender cannot open the bit commitment as both 0 and 1 later in the reveal stage. Bit commitment scheme is an important cryptographic

[1]In this paper, we focus on *proof* system, in which malicious prover could be computationally unbounded.

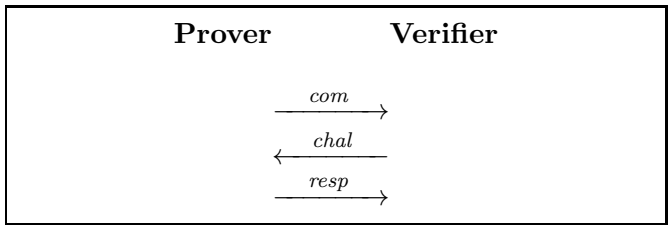

Figure 1: GMW-type zero-knowledge protocol

primitive, found many applications in the construction of cryptographic protocols. In particular, one can use bit commitment scheme to construct zero-knowledge protocols. A famous yet simple zero-knowledge protocol in the classical setting is GMW-type protocol [8], as depicted in Firgure 1. Specifically, in such type of protocol, prover first commits to a string *bit by bit* using bit commitment scheme. Next, verifier comes up with a random challenge. Last, prover responds by opening a subset of bit commitments as some values that will make verifier accept. Taking a concrete example, refer to the GMW-type protocol for Hamiltonian Cycle [2], as described in Figure 3. More detail about zero-knowledge and bit commitment scheme is referred to [7].

With the possible emergence of quantum computer and quantum communication, we are forced to study cryptography with quantum security, i.e. quantum cryptography. Generally, there are two sorts of quantum cryptography. The first one still uses classical mechanism in the construction (a.k.a. post-quantum cryptography), but even quantum computer cannot break it; the second one investigate the full power of quantum mechanism (including quantum computation and quantum communication) in the construction. We stress that one should be very careful about the security these two sorts of quantum cryptography provide, which may be inherently different (as we shall see in this paper). Likewise, there are two sorts of *quantum bit commitment scheme* (**QBC**) and *quantum zero-knowledge* (**QZK**). By convention, we usually call the first sort of **QBC** and **QZK** as (classical) **BC** and **ZK** *against quantum attack*, while the second just (general) **QBC** and **QZK**, respectively [2].

QBC. Quantum bit commitment scheme is a quantum generalization of classical bit commitment scheme that is secure against quantum adversary. We remark that due to quantum mechanism, general **QBC** has inherently different binding condition from classical **BC** [6]. Briefly, this is because malicious sender in general **QBC** can deploy such a *superposition attack* as follows: he can realize a conversation with receiver that is an arbitrary superposition of conversations corresponding to honestly commit 0 and 1; then sender may open both 0 and 1 with non-negligible probability. In contrast, **BC** against quantum attack is "*unique*", just like classical **BC**, in that malicious sender can open at most one value (0 or 1) with non-negligible probability [3].

Since unconditional **QBC**, i.e. satisfying both statistically-hiding and statistically-binding conditions, does not exist [18, 17], a possible approach is to take some plausible quantum complexity assumptions and relax one condition to be computationally secure. As in classical setting, we have two flavors of **QBC**: (computationally-hiding) statistically-binding **QBC** and (computationally-binding) statistically-binding **QBC**. There have been several constructions in this regards, e.g. [1, 6, 15, 16]; interestingly, all these constructions have *non-interactive* commit stage (only one message sent from sender to receiver), in sharp contrast to the classical setting where interactivity

[2]The first sort of **QBC** and **QZK** can be viewed as a special case of the second by standard quantum simulation technique; see e.g. [28].

[3]Though in **BC** against quantum attack, malicious sender still can be quantum and thus can commit 0 and 1 in superposition, honest receiver will measure the commitment (upon receiving it) and collapse it into a classical one.

seems inherent [9].

QZK. Quantum zero-knowledge is a quantum generalization of classical zero-knowledge that is even secure against quantum adversary. *Rewinding* is an important technique in establishing classical zero-knowledge, which, however, seems generally impossible in the quantum setting [28]. Fortunately, Watrous in his breakthrough paper [31] showed that quantum rewinding is possible in some special case. In more detail, Watrous plugged a **BC** against quantum attack (i.e. **QBC** of the first sort) into the GMW-type zero-knowledge protocol for Graph 3-Coloring problem, showing it is quantum zero-knowledge by a new quantum rewinding technique, thus giving the first (classical) zero-knowledge proof against quantum attack (i.e. **QZK** of the first sort) for all **NP** languages.

1.1 Our motivation

The motivating question of this paper is natural: with general **QBC**, can we construct **QZK**? In particular, if we plug **QBC**, rather than classical **BC** against quantum attack as in [31], into the GMW-type zero-knowledge protocol, can we end up with a quantum zero-knowledge? Most previous studies of **QBC** (e.g. [3] and references therein) only treat it as a stand-alone scheme, failing to consider it as a building block of other protocols. Seeing from practice, one benefit of using **QBC** (rather than classical **BC** against quantum attack) is by noting that most constructions of **QBC** have non-interactive commit stage, which is of the most desired.

1.2 New difficulty with QBC in security proof

Compared with Watrous' proof, the new difficulty of the security proof for GMW-type protocol with **QBC** lies in soundness analysis. In more detail, in Watrous' case, we can let (honest) verifier measure prover's commitment upon receiving it, which then becomes classical and thus fixed. Then the same line of proof as in classical soundness analysis goes through. However, in our case with **QBC**, we cannot let verifier measure prover's commitment simply because it is quantum [4]. This difference turns out to be crucial in soundness analysis: now prover who plays the role of sender in **QBC** can deploy a much more elusive superposition attack than the sender in a stand-alone execution of **QBC**. For example, prover can let his commitment *com*, and response *resp*, which contains some classical information such as value or position of bit commitments to open, be entangled. Once verifier measures these classical information in *resp*, prover's commitment will collapse into possibly different subspaces due to verifier's different challenges. Therefore, classical soundness analysis where prover's commitment is fixed in the first place cannot be used here.

Taking GMW-type protocol for Hamiltonian Cycle for example. Prover can commit a bunch of graphs in superposition as *com*. Classical information in prover's response *resp* include a graph or location of Hamiltonian cycle to open, depending on verifier's challenge bit, which could also be in superposition and entangled with *com*.

1.3 Our idea and technique

To prove soundness, i.e. the security of verifier against prover's possible superposition attack, we take a geometric approach to tackle this problem. First, we delay verifier's measurement of classical information within *resp* to the end, guaranteeing that prover's commitment *com* is fixed during the execution of the protocol. Note that now these classical information are not determined

[4] As pointed out by Unruh, since his proof-of-knowledge (a notion stronger than soundness) technique [26] also heavily relies on bit commitment scheme being classical, it cannot be used in our setting either.

(may be in superposition), so classical soundness analysis still cannot be applied. Second, at the end of the protocol, we really do not let verifier measure those classical information within *resp*; instead, for each verifier's challenge, we view verifier's corresponding measurement of classical information, as well as the subsequent procedure of checking whether to accept, as a single binary (0/1) measurement, where the projection subspace corresponding to outcome 1 can be viewed as verifier's *accepting subspace*. In other words, now we do not differentiate which particular classical information will be obtained if verifier measures them; we only care about whether they lead verifier to accept. By this viewpoint, it turns out that we can covert quantum soundness analysis into a *geometric problem* more or less like this: show that verifier's accepting subspaces corresponding to different challenges are (almost) mutually orthogonal.

For strict proof of soundness, we need a technical lemma whose geometric intuition is as follows: in a nutshell, it gives two equivalent yet simple characterizations of a bunch of complex Euclidean subspaces *almost having a non-trivial intersection*; that is, there exists a unit vector whose projections onto all the subspaces are almost one.

1.4 Our results

The main result of this paper is to give an affirmative answer to our motivating question.

Theorem 1 *All **NP** languages have quantum computational zero-knowledge proof given access to non-interactive (computationally-hiding) statistically-binding quantum bit commitment scheme.*

To prove this theorem, we first propose a *formalization* of non-interactive (statistically-binding) **QBC**. Here by "non-interactive" we mean in the commit stage, sender sends a quantum state to receiver as the bit commitment; later in the reveal stage, sender sends another quantum state for receiver to open the commitment; in both stages, receiver does not send any messages. Our formalization is motivated by Watrous' construction of **QSZK**-complete problem [30] as well as our intended application; it makes an essential use of the reversibility of quantum computation, and conceptually can encapsulate all constructions of non-interactive **QBC**, which could be of independent interest. Detail is referred to section 3.

Next, we plug such formalization of non-interactive **QBC** into GMW-type zero-knowledge protocols for **NP**-complete languages, e.g., Hamiltonian Cycle [2] or Graph 3-Coloring [8]. As for its security, quantum zero-knowledge follows similar to [31], using Watrous' quantum rewinding technique; the *novel* part lies in the soundness (section 5), as we have discussed.

Shortcoming. Our main result seems only of theoretic interests, since we still use GMW-type construction here, which is not much round-efficient (if we want to reduce soundness error to be negligible). Nevertheless, we believe that our novel use of **QBC** as building block, as well as corresponding soundness analysis, could be theoretically interest and found other applications in the future study of quantum cryptography.

Unconditional study of QZK. We also follow Watrous [30], generalizing unconditional study of classical zero-knowledge [27, 19, 23, 24] to the quantum setting. In particular, we show that **QBC** is also necessary for **QZK**.

Lemma 2 *If **NP** language A has quantum zero-knowledge proof, then it also has an instance-dependent non-interactive quantum bit commitment scheme.*

Here, the concept of instance-dependent **QBC** is a straightforward generalization of its classical counterpart [27]. The construction from **QZK** to **QBC** is just the same as Watrous' **QSZK**-

complete problem [30] (section 6). Combining with (a slight variant of) Theorem 1, we establish an equivalence between **QBC** and **QZK**.

Theorem 3 *Non-interactive statistically-binding quantum bit commitment scheme is not only sufficient but also necessary for quantum zero-knowledge proof for **NP** languages.*

We point out two difference between our equivalence theorem above and its classical counterpart in [24]:

1. The constructions and security proofs in the quantum setting are inherently different from [24].

2. Here we only obtain the equivalence with regard to proof system; whether it holds for argument system where malicious prover are polynomial-time bounded is an interesting open question.

From such equivalence, mimicing unconditional conditional study of classical zero-knowledge, we can also prove many properties about quantum zero-knowledge proof for **NP** languages *unconditionally* (does not rely on any complexity assumption); refer to section 7 for detail.

QBC from QOWF. Inspired by our formalization of non-interactive (statistically-binding) **QBC**, we provides a construction based on a complexity assumption likely to be equivalent to quantum one-way function (**QOWF**). It can be viewed as a quantum generalization of Naor' scheme [20] in the classical setting, but with only one message in the commit stage; detail is referred to section 4. We highlight that a straightforward quantum generalization of Naor's scheme gives a **BC** against quantum attack [10], but with two-messages in the commit stage rather than one; another construction is however assuming quantum one-way permutation (**QOWP**) [1], which is believed to be much stronger than **QOWF**.

1.5 Related work

We prove a technical lemma (Lemma 6) in soundness analysis that is similar to Unruh's proof-of-knowledge technique [26, Lemma 6]. For the difference, it seems that Unruh got better bound than ours, whereas our technique can handle **QBC** (more general than **BC** against quantum attack) and conceptually any GMW-type zero-knowledge protocols for **NP**-complete languages, including Graph 3-Coloring (Appendix F).

Compared with Kobayashi's work on **QZK** proof [13], here we restrict to **NP** languages. We remark that zero-knowledge for **NP** languages is of the most interest from cryptographic view: we expect (honest) prover can be implemented in polynomial time given access to a witness; this is actually what we have achieved. In comparison, Kobayashi assumes honest prover has unbounded computational power. We highlight that we prove many properties of **QZK** proof that are similar to Kobayashi, but with such subtle difference in prover's efficiency. Of course, Kobayashi's proof and ours are completely different; actually, our study meet Kobayashi's call for unconditional study of **QZK** proof in [13].

To the best of our knowledge, the only previous work we know using **QBC** as a building block is [5], where **QBC** is used to construct quantum oblivious transfer (**QOT**). But the security analysis there and ours are also completely different.

We note that our idea of formalizing non-interactive **QBC** is similar to [4], but with different motivations and assumptions.

1.6 Organization

In section 2 we give some preliminary materials. In section 3, we propose a formalization of **QBC**. Inspired by this formalization, we give a construction of **QBC** in section 4. Following is section 5, where we prove the soundness of the GMW-type protocol for Hamiltonian Cycle when we plug in **QBC**; this is the main technical part of the paper. In sections 6 and 7, we prove an equivalence between **QBC** and **QZK**, and several immediate consequences following from such equivalence, respectively. We conclude with section 8.

2 Preliminaries

In this paper, we assume readers are familiar with classical GMW-type zero-knowledge protocol and its security proof, in particular the soundness analysis. Refer to [7] for detail.

Most of terminologies and notations in quantum information we are using here are standard and can be found in [29]; for self-containment, we give a quick overview in Appendix 2. In addition, given a projector Π, we also abuse the notation to use Π to denote the subspace it projects onto. We shall use quantum register and a sequence of qubits interchangeably; when we say Hilbert space induced by the quantum register, we mean the Hilbert space induced by qubits stored in the quantum register.

We also adopt the definition of *quantum indistinguishability* from Watrous [31], which is a straightforward generalization of its classical counterpart. For self-containment, we give it in Appendix B.

Quantum algorithm can be formalized in terms of *uniformly generated* quantum circuit family, whereas quantum circuit is composed of quantum gates chosen from some fixed universal, finite, and *unitary* quantum gate set [22, 31].

3 Formalization of QBC

In this section, we shall give a formalization of non-interactive statistically-binding **QBC**. Before doing this, we need to introduce a notion known as *quantum state defined by quantum circuit*, as firstly defined by Watrous [30].

Definition 4 (Quantum state defined by quantum circuit) We can view a quantum circuit Q with designated output as encoding a quantum state in the following way: imagine we apply quantum circuit Q on a pair of quantum registers (O, G) initialized in all 0's state, where quantum register O corresponds to output qubits and G corresponds to non-output qubits (or garbage qubits, which will be implicitly discarded after applying Q); we call the resulting state of quantum register O as the *quantum state defined by quantum circuit* Q. That is, the quantum state defined by quantum circuit Q is given by $\mathrm{Tr}_{\mathcal{G}}(Q|0\rangle\langle 0|Q^*)$, where $\mathcal{G}$ is the subspace induced by register G.

Our formalization of **QBC** is as follows.

Definition 5 A *non-interactive* quantum bit commitment scheme, represented by an ensemble of a pair of quantum circuits $\{(Q_0(n), Q_1(n))\}_n$ with security parameter n, is a two-party, two-stage protocol with following properties:

- The protocol consists of two parties, sender and receiver, proceeding in two stages: first a *commit* stage and later a *reveal* stage.

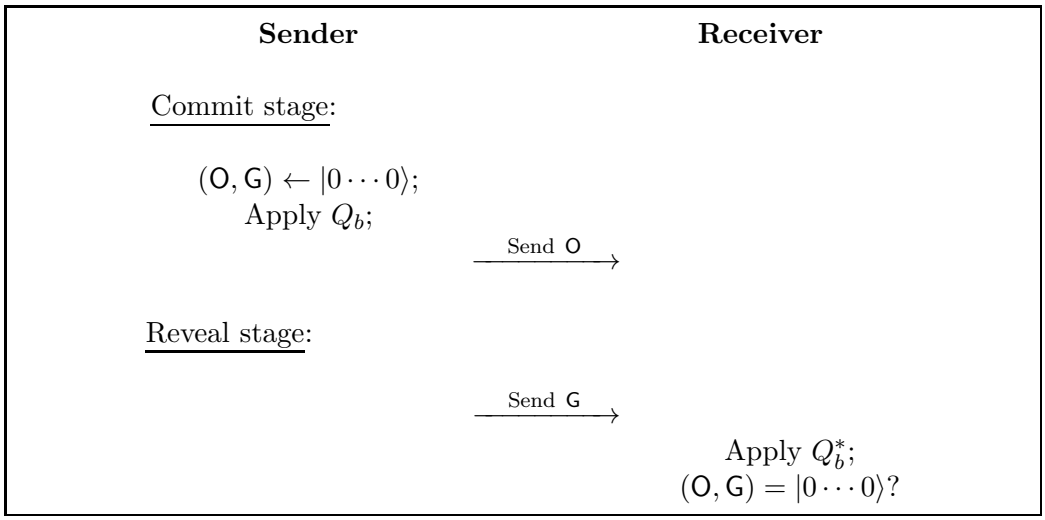

Figure 2: Commit and open procedures of non-interactive **QBC**

- Both sender and receiver's operations can be represented by a pair of (unitary) quantum circuits $(Q_0(n), Q_1(n))$, defining a pair of quantum states $(\rho_0(n), \rho_1(n))$.
- At the beginning of commit stage, sender receives a private bit $b \in \{0,1\}$. To commit bit b, sender applies quantum circuit $Q_b(n)$ on quantum registers (O,G), which is initialized in all 0's state. Then sender sends register O to receiver; register G is kept.
- In the reveal stage, sender sends b, together with quantum register G to receiver R. Receiver first measures b to get the value to open, and then applies $Q_b(n)^*$ on $(\mathsf{O},\ \mathsf{G})$, the inverse of $Q_b(n)$; accept if these quantum registers return to all 0's state.

The commit and open procedures are depicted in Figure 2. We are next to define hiding (or concealing) and binding conditions of quantum bit commitment scheme.

- **Hiding**. We say the scheme $\{(Q_0(n), Q_1(n))\}_n$ is statistically (resp. computationally) hiding if quantum state ensembles $\{\rho_0(n)\}_n$ and $\{\rho_1(n)\}_n$ are statistically (resp. computationally) indistinguishable.
- Statistically $\epsilon(n)$-**binding**. We say the scheme $\{(Q_0(n), Q_1(n))\}_n$ is statistically $\epsilon(n)$-binding if the fidelity $F(\rho_0(n), \rho_1(n)) < \epsilon(n)$. For cryptographic applications, we usually require $\epsilon(n)$ be negligible, or even exponentially small [5].

Several remarks about our formalization are in order.

1. Here we only consider information-theoretic binding [6], which is defined by requiring the fidelity $F(\rho_0, \rho_1)$ close to 0. According to the relation between fidelity and trace distance as described in inequalities (16), the binding condition can also be expressed in terms of the trace distance $\|\rho_0 - \rho_1\|_1 /2$ being close to 1. We further remark that this definition implies the widely accepted definition of quantum binding [6] such that $p_0 + p_1 < 1 + \epsilon(n)$, where p_0

[5] Actually, what $\epsilon(n)$ really is does not make much difference, because some standard amplification procedures, as described in Appendix G, can decrease $\epsilon(n)$ in exponential speed.

[6] Because we only consider proof system in this paper.

and p_1 are probability that sender can open the bit commitment as 0 and 1, respectively. See Appendix C for detail.

2. We argue that the commit and the open procedures of all constructions of non-interactive quantum bit commitment scheme in standard model (even those of anther flavor, e.g. [6, 15, 16]) can be recast in our formalization. To see it, note that the open procedure in our formalization is actually a verification, via reverse computation, that sender performs honestly in the commit stage. This is in the same spirit as the canonical open procedure in the classical setting, where sender sends random coins he/she used in the commit stage, and receiver checks that such random coins are consistent with the generated transcript. (see Goldreich's textbook [7, page 225]).

3. We stress that here we restrict our attention to the *non-interactive* **QBC**. The reasons for our choice are three-fold. First, in this paper, indeed we can construct such stronger (no need of interaction) notion of **QBC**. Second, almost all previous constructions of **QBC** (including another flavor), e.g. [1, 6, 15, 16], are non-interactive. Third, as we show later, we can actually construct non-interactive **QBC** from **QZK** proof. Therefore, evidences indicate that **QBC** perhaps does not really need interaction; restricting to non-interactive **QBC** does not lose generality. This is in sharp contrast to most of classical constructions of **BC** that are interactive.

From now on, when we say **QBC**, we refer to the formalization given above rather than any specific constructions.

4 A construction of statistically-binding QBC

In this section, we consider how to construct non-interactive statistically-binding **QBC** from quantum one-way function (**QOWF**); previously, we only know how to do this assuming quantum one-way permutation (**QOWP**) [1]. The idea of our construction is inspired by our formalization of **QBC**: it suffices for us to generate in polynomial time an ensemble of a pair of quantum states $\{(\rho_0(n), \rho_1(n))\}_n$ such that $\{\rho_0(n)\}_n$ and $\{\rho_1(n)\}_n$ are computationally indistinguishable but statistically distinguishable. To this end, we use idea of Naor's [20]: let $\rho_0(n)$ be the density operator corresponding to a pseudorandom distribution, while $\rho_1(n)$ corresponding to a truly random (i.e. uniform) distribution. The commit and the open procedures follow the ones in our formalization (Definition 5).

In more detail, assume $G : \{0,1\}^n \to \{0,1\}^{3n}$ is a classical pseudorandom generator secure against any quantum polynomial-time distinguisher. Then we let quantum circuit Q_0 output quantum state

$$\rho_0 = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} |G(x)\rangle\langle G(x)|. \tag{1}$$

We point out that given G, the construction of quantum circuit Q_0 which simulates G in a reversible way is standard. The construction of quantum circuit Q_1 which outputs quantum state

$$\rho_1 = \frac{1}{2^{3n}} \sum_{x \in \{0,1\}^{3n}} |x\rangle\langle x| \tag{2}$$

is easy. Details of the construction and its security proof are referred to Appendix D.

Common input: a directed graph G with n vertices.

Private input to prover: a Hamiltonian cycle of G.

Protocol:

- Prover (P1): Select a random permutation π of $\{1, 2, \ldots, n\}$, and commit to each bit of the string encoding the adjacency matrix of $\pi(G)$ independently. Send these bit commitments to verifier.
- Verifier (V1): Select a challenge bit $b \in \{0, 1\}$ randomly and uniformly, and send it to prover.
- Prover (P2): When $b = 0$, prover sends to verifier permutation π, as well as information used to open all bit commitments as the adjacency matrix of $\pi(G)$. When $b = 1$, prover sends to verifier the information about the position where the Hamiltonian cycle locates, i.e. n out of n^2 entries in the adjacency matrix of $\pi(G)$, as well as information used to open bit commitments at these n positions as all 1's.
- Verifier (V2): When $b = 0$, verifier checks that all bit commitments are opened as the adjacency matrix of $\pi(G)$ successfully. When $b = 1$, verifier checks that bit commitments at the n specified positions are all opened as 1's successfully and the corresponding edges form a Hamiltonian cycle.

Figure 3: GMW-type zero-knowledge protocol for Hamiltonian Cycle

We remark that the exact complexity assumption we are using here is (classical) pseudorandom generator against quantum distinguisher; but if [11] can be generalized to the quantum setting, which is widely believed, then our construction can in turn be based on **QOWF**.

5 QZK from QBC

We intend to plug **QBC**, as formalized in Definition 5, into GMW-type zero-knowledge protocol to obtain **QZK**. For its security proof, we mentioned that compared with Watrous [31], we encounter new difficulty in the soundness analysis; briefly, this is because malicious prover may deploy a superposition attack.

Soundness analysis: a geometric approach

To overcome the new difficulty, we take a geometric approach: we consider verifier's accepting subspaces corresponding to each of his/her challenge. In the following, we give a soundness proof of GMW-type protocol for Hamiltonian Cycle problem (described in Figure 3). We remark that our approach is generic; it presumably can be applied to any GMW-type protocols, including the one for Graph 3-Coloring (refer to Appendix F for a sketched proof).

Adopting notations used in Figure 3, we introduce projectors

$$P_0 = \sum_{\pi} |\pi\rangle\langle\pi| \otimes Q_{\pi(G)}|0\rangle\langle 0|Q^*_{\pi(G)}, \tag{3}$$

$$P_1 = \sum_{c} |c\rangle\langle c| \otimes Q_c|0\rangle\langle 0|Q^*_c, \tag{4}$$

denoting accepting subspaces corresponding to challenge bit 0 and 1, respectively. The expressions of P_0, P_1 are explained as below. We assume **QBC** is represented in terms of quantum circuits (Q_0, Q_1). For the expression of P_0, π denotes a permutation, which is a part of prover's response. Projector $Q_{\pi(G)}|0\rangle\langle 0|Q^*_{\pi(G)}$ operates on all n^2 (quantum) bit commitments, where $Q_{\pi(G)}$ is the quantum circuit to commit graph $\pi(G)$. In more detail, suppose the adjacency matrix of $\pi(G)$ can be represented by binary string $b_1 b_1 \cdots b_{n^2}$. Then $Q_{\pi(G)} = Q_{b_1} \otimes Q_{b_2} \otimes \cdots \otimes Q_{b_{n^2}}$. For the expression of P_1, c denotes the location of Hamiltonian cycle. Projector $Q_c|0\rangle\langle 0|Q^*_c$ operates on n (out of n^2) bit commitments at positions specified by c, where Q_c $(= Q_1^{\otimes n})$ is quantum circuit to commit n 1's.

At a high level, to prove soundness, it becomes to show that whatever quantum state prover prepares as commitment, its projections on subspaces P_0 and P_1 cannot be too long simultaneously. To this end, we need a technical lemma stated as below (its proof is delayed to Appendix E), which implies that for contradiction, it then suffices to show that subspaces P_0 and P_1 are almost orthogonal. The intuition of the lemma is referred to the remark immediately after it.

Lemma 6 *Let $\mathcal{X}, \mathcal{Y}$ be two complex Euclidean spaces, and $P_1, \ldots, P_m$ be projectors on $\mathcal{X} \otimes \mathcal{Y}$. If there exists a vector $|\psi\rangle \in \mathcal{X} \otimes \mathcal{Y}$ and unitary transformations $U_1, \ldots, U_m \in U(\mathcal{Y})$ such that $\sum_i \|P_i U_i|\psi\rangle\|^2 / m \geq 1-\delta$ for some $0 \leq \delta \leq 1$, then there exists unitary transformations $U'_1, \ldots, U'_m \in U(\mathcal{Y})$ satisfying $\|P_1 U'_1 \cdots P_m U'_m|\psi\rangle\| \geq 1 - m\sqrt{\delta}$.*

Remark. In a special case where subspace $\mathcal{Y}$ is trivial (then there are no U_i's and U'_i's), then the lemma above gives two equivalent characterizations of a bunch of subspaces having almost non-trivial intersection. In more detail, expression $\sum_i \|P_i|\psi\rangle\|^2 / m \geq 1 - \delta$ says there exists a vector whose projections on all subspaces P_i's are almost one, while expression $\|P_1 \cdots P_m|\psi\rangle\| \geq 1 - m\sqrt{\delta}$ says there exists a vector such that after a sequence of projections P_i's, the resulting vector almost has length one.

For our purpose, the general case where subspace $\mathcal{Y}$ is non-trivial corresponds to prover preparing response adaptively (according to verifier's challenge); subspace $\mathcal{X}$ is induced by the commitment, which is out of prover's reach at the moment preparing his response.

Putting things together

We next show how our technical lemma magically reduce quantum soundness analysis to classical soundness analysis.

Proof of soundness: Suppose graph G does not have Hamiltonian cycle. Moreover, without loss of generality, suppose **QBC** represented by (Q_0, Q_1) satisfies binding condition $F(\rho_0, \rho_1) < 2^{-n^2}$. For contradiction, assume verifier will accept with probability at least, say, 0.8. That is, there exists a quantum state vector $|\psi\rangle$ such that

$$\sum_{i=0,1} \|P_i U_i|\psi\rangle\|^2 / 2 \geq 0.8,$$

where P_0, P_1 are described in expressions (3), (4), respectively; vector $|\psi\rangle$ is the quantum state prover prepares before seeing verifier's challenge (part of it is sent to verifier in the first message as commitment), and unitary transformations U_0, U_1 can be viewed as prover's strategy after seeing challenge but before sending response. By Lemma 6, there exists unitary transformation U'_0, U'_1, which operate on prover's response, such that

$$\left\|P_0 U'_0 P_1 U'_1|\psi\rangle\right\| \geq 1 - 2\sqrt{0.2} = \Omega(1).$$

Thus, to derive contradiction, we suffice to show that for any U_0', U_1', operating only on prover's response, the operator norm $\|P_0U_0'P_1'U_1\|$ is negligible.

By our assumption of (Q_0, Q_1), we have

$$\begin{aligned}\left\|P_0U_0'P_1U_1'\right\| &= \left\|\sum_{\pi}|\pi\rangle\langle\pi|\otimes Q_{\pi(G)}|0\rangle\langle 0|Q^*_{\pi(G)}U_0'\sum_{c}|c\rangle\langle c|\otimes Q_c|0\rangle\langle 0|Q_c^*U_1'\right\| \\ &\leq \sum_{\pi,c}\left\||\pi\rangle\langle\pi|\otimes Q_{\pi(G)}|0\rangle\langle 0|Q^*_{\pi(G)}\cdot U_0'\cdot|c\rangle\langle c|\otimes Q_c|0\rangle\langle 0|Q_c^*\cdot U_1'\right\| \\ &\leq \sum_{\pi,c}F(\rho_{\pi(G)|_c},\rho_1^{\otimes n}),\end{aligned}$$

where $\rho_{\pi(G)|_c}$ denote the quantum state corresponding to the commitment of string $\pi(G)|_c$, i.e. string $\pi(G)$ restricting to position specified by c. The last "$\leq$" holds because $|\langle\pi|\langle 0|Q^*_{\pi(G)}\cdot U_0'\cdot|c\rangle Q_c|0\rangle|$ is upperbounded by $F(\rho_{\pi(G)|_c},\rho_1^{\otimes n})$, according to Uhmann's Theorem (Fact 11).

Now comes classical soundness argument: since G does not have Hamiltonian cycle, neither does $\pi(G)$. It follows that among the n terms in the tensor product in the expression of $\rho_{\pi(G)|_c}$, at least one must be ρ_0. Since $F(\rho_0,\rho_1)<2^{-n^2}$ by quantum binding condition,

$$\left\|P_0U_0'P_1U_1'\right\|<\sum_{\pi,c}2^{-n^2}<n!\cdot(n-1)!\cdot 2^{-n^2}=o(1). \tag{5}$$

We arrive at the contradiction. This completes the soundness proof.

■

Remark.

1. Here we require quantum binding hold as strong as $F(\rho_0,\rho_1)<2^{-n^2}$ for technical reason (inequality (5)). But this does not matter because we can strengthen the quantum binding condition by taking multiple (polynomial bounded) copies of the original scheme.

2. Here we can only prove that when graph G does not have Hamiltonian cycle, then verifier's acceptance probability is at most 0.8. In comparison, in classical setting, we can actually show that this probability is ≈ 0.5. But such difference does not matter either, as long as there is a non-negligible probability gap from one.

Combing with Watrous' quantum rewinding technique [31] to show quantum (computational) zero-knowledge property, which is omitted here since the proof is almost the same, we arrive at our main theorem.

RESTATEMENT OF **Theorem 1**: *All **NP** languages have quantum computational zero-knowledge proof given access to non-interactive statistically-binding quantum bit commitment scheme.*

6 An equivalence between QBC and QZK

In the same spirit as [24], we investigate whether **QBC** and **QZK** are equivalent. To this end, like [24], we first need to generalize the definition of **QBC** to the instance-dependent one.

Definition 7 We say a (promise) problem A has *instance-dependent* **QBC** if on input $x\in A_{\text{YES}}\cup A_{\text{NO}}$, we can construct in polynomial time a quantum bit commitment scheme such that

- When $x \in A_{\text{YES}}$, then the scheme is hiding;
- When $x \in A_{\text{NO}}$, then the scheme is binding.

The hiding and binding conditions can be defined in a similar way as in Definition 5.

Remark. Instance-dependent **QBC** can be simultaneously statistically-hiding and statistically-binding.

Now we can prove a theorem which is a precise restatement of Theorem 3.

Theorem 8 *For every language $A \in$ **NP**, A has quantum statistical (resp. computational) zero-knowledge proof if and only if A has an instance-dependent quantum bit commitment scheme that is statistically (resp. computationally) hiding on* YES *instances and statistically binding on* NO *instances.*

PROOF SKETCH: From **QZK** to **QBC**, the basic idea is to use Watrous' construction of **QSZK**-complete problem, together with some amplification procedures; detail is referred to appendix G.

On the other hand, from **QBC** to **QZK**, the proof is almost the same as what we have given in the last section, except that now we use instance-dependent **QBC** instead. A key observation is that quantum zero-knowledge property only relies on quantum hiding, while soundness on quantum binding.

■

7 Consequences

As an immediate corollary of our equivalence theorem (Theorem 8), we can prove several interesting properties about quantum zero-knowledge proof for **NP** languages. We remark that all these properties are proved *unconditionally*, not relying on any complexity assumptions. Compared with Kobayashi's results [13], we highlight here (honest) prover can be implemented in polynomial time.

Corollary 9 *For every language $A \in$ **NP**:*

1. *$A \in$ **HVQSZK** (resp. **HVQZK**) with efficient prover if and only if $A \in$ **QSZK** (resp. **QZK**) with efficient prover;*
2. *If $A \in$ **QSZK** (resp. **QZK**), then A has a three-round quantum statistical (resp. computational) zero-knowledge proof with perfect completeness, constant soundness error, and verifier's message being just a single random bit. Moreover, prover can be implemented in quantum polynomial time given a witness.*

Second, combining Theorem 1 and **QBC** we constructed in section 4, we have the following theorem.

Theorem 10 *If (classical) pseudorandom generator against quantum attack exists, then all languages in **NP** have quantum computational zero-knowledge proof.*

Due to different bit commitment schemes used, Theorem 10 relies on conceivably a much weaker complexity assumption than Watrous [31]; and one less message than [10] based on the same assumption, but at the cost of requiring quantum computation and quantum communication. Though widely believed, we have not yet seen a formal proof that the same construction of pseudorandom generator as in [11] remains secure against quantum attack if we assume **QOWF**. If this is true, then we can relax the assumption of Theorem 10 to the existence of **QOWF**.

8 Conclusion

A summary of our results. In this paper, we show that one can construct quantum zero-knowledge proof for all **NP** languages given access to non-interactive statistically-binding quantum bit commitment scheme. As for the security proof, compared with Watrous [31], the novel part of ours lies in the soundness analysis. We take a geometric approach to solve this problem, proving a technical lemma that reduces quantum soundness analysis to classical soundness analysis.

On the other hand, we show that non-interactive statistically-binding quantum bit commitment scheme is also necessary for quantum zero-knowledge proof. We carry out an unconditional study of quantum zero-knowledge proof mimicking its classical counterpart [27].

QBC as cryptographic primitive. Observing from previous study of **QBC** [6, 1, 15, 16], as well as its applications in quantum oblivious transfer (**QOT**) [5, 14] and quantum zero-knowledge in this paper, we propose to study **QBC** as cryptographic primitive in the future study of quantum cryptography. We have two reasons for this:

1. Seeing from its constructions, both two flavors (i.e. statistically-binding and statistically-hiding) of **QBC** have non-interactive commit stage. Moreover, in this paper we show that the non-interactivity of **QBC** seems *not* a too strong requirement; it is necessary for **QZK**. Thus, compared with classical **BC** for which interactivity in the commit stage seems inherent, **QBC** has greater advantage regarding round complexity. Maybe we can construct much more round-efficient (compared with classical setting) quantum cryptographic protocols using **QBC** as a building block.

2. As we have discussed, party (prover in this paper) who plays the role of sender in quantum commitment scheme may carry out a superposition attack, and classical security analysis will fail. In spite of this, previous work on **QOT** [5] and our work on **QZK** shows that **QBC** also suffices for some serious cryptographic applications; maybe more are waiting for discovery.

Acknowledgements We thank Yi Deng for helpful discussion during the progress of this work. Thanks also go to Dominique Unruh and anonymous referee of QIP 2014 for their invaluable insights on the subject of this paper.

References

[1] Mark Adcock and Richard Cleve. A quantum Goldreich-Levin theorem with cryptographic applications. In *STACS 2002*, pages 323–334. Springer, 2002. 2, 5, 8, 13

[2] 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. 2, 4

[3] André Chailloux and Iordanis Kerenidis. Optimal bounds for quantum bit commitment. In *FOCS*, pages 354–362, 2011. 3

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

[5] 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. 5, 13

[6] Paul Dumais, Dominic Mayers, and Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *EUROCRYPT*, pages 300–315, 2000. 2, 7, 8, 13, 17

[7] Oded Goldreich. *Foundations of Cryptography, Basic Tools*, volume I. Cambridge University Press, 2001. 2, 6, 8, 18, 19

[8] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991. 2, 4

[9] 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

[10] Sean Hallgren, Adam Smith, and Fang Song. Classical cryptographic protocols in a quantum world. In *CRYPTO*, pages 411–428, 2011. 5, 12

[11] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999. 9, 12

[12] Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation, volume 47 of Graduate Studies in Mathematics*. American Mathematical Society, 2002. 19

[13] Hirotada Kobayashi. General properties of quantum zero-knowledge proofs. *Available as arXiv.org e-Print 0705.1129*, 2007. Preliminary version appears in TCC 2008. 5, 12

[14] Takeshi Koshiba. Quantum oblivious transfer and quantum one-way functions. In *Japan-Singapore Workshop on Multi-user Quantum Networks*, 2012. 13

[15] Takeshi Koshiba and Takanori Odaira. Statistically-hiding quantum bit commitment from approximable-preimage-size quantum one-way function. In *TCQ*, pages 33–46, 2009. 2, 8, 13

[16] Takeshi Koshiba and Takanori Odaira. Non-interactive statistically-hiding quantum bit commitment from any quantum one-way function. *arXiv preprint arXiv:1102.3441*, 2011. 2, 8, 13

[17] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, 1997. 2

[18] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414–3417, 1997. 2

[19] Daniele Micciancio and Salil P. Vadhan. Statistical zero-knowledge proofs with efficient provers: Lattice problems and more. In *CRYPTO*, pages 282–298, 2003. 4

[20] Moni Naor. Bit commitment using pseudorandomness. *J. Cryptology*, 4(2):151–158, 1991. 5, 8

[21] Ashwin Nayak and Peter Shor. Bit-commitment-based quantum coin flipping. *Physical Review A*, 67(1):012304, 2003. 17

[22] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and Quantum Informatioin*. Cambridge University Press, 2000. 6

[23] Shien Jin Ong and Salil P. Vadhan. Zero knowledge and soundness are symmetric. In *EUROCRYPT*, pages 187–209, 2007. 4

[24] Shien Jin Ong and Salil P. Vadhan. An equivalence between zero knowledge and commitments. In *TCC*, pages 482–500, 2008. 4, 5, 11

[25] Amit Sahai and Salil P. Vadhan. A complete problem for statistical zero knowledge. *J. ACM*, 50(2):196–249, 2003. Preliminary version appears in FOCS 1997. 23

[26] Dominique Unruh. Quantum proofs of knowledge. In *EUROCRYPT*, pages 135–152, 2012. 3, 5

[27] Salil P. Vadhan. An unconditional study of computational zero knowledge. *SIAM J. Comput.*, 36(4):1160–1214, 2006. 4, 13

[28] Jeroen van de Graaf. *Towards a formal definition of security for quantum protocols*. PhD thesis, Université de Montréal, 1997. 2, 3

[29] John Watrous. *Theory of Quantum Information*. Online Lecture Notes: `https://cs.uwaterloo.ca/~watrous/CS766/`. 6, 16, 17

[30] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *FOCS*, pages 459–468, 2002. 4, 5, 6, 17, 22

[31] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. Preliminary version appears in STOC 2006. 3, 4, 6, 9, 11, 12, 13, 17, 23

A Quantum information

Here we just give a quick review of some basics of quantum information, most of which are adopted from Watrous' lecture notes [29].

According to axioms of quantum mechanics, every quantum system mathematically induces a Hilbert space, which we denote by, e.g., $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$. The state of a quantum system could be either *pure* or *mixed*, depending on whether this quantum system is isolated or entangled with other quantum systems (or environment). A pure quantum state is mathematically represented by a vector in the Hilbert space induced by the quantum system; we write, e.g., u, v, or $|\psi\rangle$, to denote state vector, with their conjugates u^*, v^*, or $\langle\psi|$, respectively. A mixed quantum state can be mathematically described by an *density operator*, which contains all the statistical properties of the quantum system. Formally, a density operator is a positive semi-definite operator with trace one; we usually write, e.g., ρ, ξ, to denote density operator, and write $\mathrm{D}(\mathcal{X})$ to denote the set of all density operators in Hilbert space $\mathcal{X}$.

Measurements of the distance (or closeness) between two quantum states are important in quantum information. There are two commonly used measurements for our purpose. The first one is *trace distance*. Specifically, for two density operator $\rho, \xi \in \mathrm{D}(\mathcal{X})$, their trace distance is given by $\|\rho - \xi\|_1 / 2$, where the 1-norm $\|\cdot\|_1$ is equal to the sum of the absolute value of all eigenvalues. Another measurement is called *fidelity*, as explained as below.

Let $\rho \in \mathrm{D}(\mathcal{X})$ be a density operator. A *purification* of ρ in space $\mathcal{X} \otimes \mathcal{Y}$ is a vector $u \in \mathcal{X} \otimes \mathcal{Y}$ such that $\mathrm{Tr}_{\mathcal{Y}}(uu^*) = \rho$, where $\otimes$ is the *tensor product* and $\mathrm{Tr}_{\mathcal{Y}}(\cdot)$ is the *partial trace*. Purifications of a (mixed) quantum state are generally not unique and exist if $\dim(\mathcal{Y}) \geq \text{rank } (\rho)$. Then the fidelity between two quantum states $\rho, \xi \in \mathrm{D}(\mathcal{X})$ can be viewed as defined via the following fact.

Fact 11 (Uhlmann) *Let $\mathcal{X}$ and $\mathcal{Y}$ be two Hilbert spaces. Let $\rho, \xi \in D(\mathcal{X})$ be density operators, both having rank at most $\dim(\mathcal{Y})$, and let $u \in \mathcal{X} \otimes \mathcal{Y}$ be any purification of ρ. Then*

$$F(\rho, \xi) = \max \{|u^* v| : v \in \mathcal{X} \otimes \mathcal{Y} \text{ is a purification of } \xi\}.$$

Proof: See [29, Lecture 4]. ■

There are several simple facts about fidelity that we shall use in this paper.

Fact 12 *Let $u \in \mathcal{X}$ be a unit vector and let $\rho \in D(\mathcal{X})$ be density operator. Then*

$$F(uu^*, \rho) = \sqrt{u^* \ \rho \ u}.$$

Proof: See [29, Lecture 4]. ■

Fact 13 *Let $\rho, \xi \in D(\mathcal{X} \otimes \mathcal{Z})$ be density operators. Then*

$$F(\rho, \xi) \leq F(Tr_{\mathcal{Z}}(\rho), Tr_{\mathcal{Z}}(\xi)).$$

Proof: Purifications of density operators ρ and ξ are also purifications of $\mathrm{Tr}_{\mathcal{Z}}(\rho)$ and $\mathrm{Tr}_{\mathcal{Z}}(\xi)$, respectively. Then Uhlmann Theorem (Fact 11) implies $F(\rho, \xi) \leq F(\mathrm{Tr}_{\mathcal{Z}}(\rho), \mathrm{Tr}_{\mathcal{Z}}(\xi))$. ■

Fact 14 *Let density operators $\rho_1, \xi_1 \in D(\mathcal{X})$ and $\rho_2, \xi_2 \in D(\mathcal{Y})$. Then*

$$F(\rho_1 \otimes \rho_2, \xi_1 \otimes \xi_2) = F(\rho_1, \xi_1)\, F(\rho_2, \xi_2).$$

Fact 15 *For any $\rho, \xi, \sigma \in D(\mathcal{X})$, we have*

$$\max_{\sigma} \left(F(\rho, \sigma)^2 + F(\sigma, \xi)^2 \right) = 1 + F(\rho, \xi).$$

Proof: See [30, 21].

■

The two measurements of distance (or closeness) between two quantum states, trace distance and fidelity, are related through the following inequalities.

Fact 16 (Fuchs-van de Graaf inequality) *Let $\mathcal{X}$ be a complex Euclidean space and assume that $\rho, \xi \in D(\mathcal{X})$ are density operators over space $\mathcal{X}$. Then*

$$1 - F(\rho, \xi) \leq \frac{1}{2} \|\rho - \xi\|_1 \leq \sqrt{1 - F(\rho, \xi)^2}.$$

Proof: See [29, Lecture 4].

■

B Quantum Indistinguishability

Following Watrous [31], we introduce the notion of *quantum measurement circuit* as the quantum circuit followed by a measurement of all its output qubits with respect to the computational basis. In particular, *quantum distinguisher* is a quantum measurement circuit which has exactly one bit output. Then quantum indistinguishability is defined as below.

Definition 17 (Quantum Indistinguishable) Let $\{\rho_n\}$ and $\{\xi_n\}$ be two ensembles of mixed states of poly(n) qubits. We say ensembles $\{\rho_n\}$ and $\{\xi_n\}$ are *statistically (resp., computationally) indistinguishable* if for any mixed state σ_n of poly(n) qubits, and any unbounded-size (resp., poly(n)-size) quantum distinguisher D_n, we have

$$|\Pr[D_n(\rho_n \otimes \sigma_n) = 1] - \Pr[D_n(\xi_n \otimes \sigma_n) = 1]| < \epsilon(n),$$

where $\epsilon(\cdot)$ is some negligible function.

Remark. Quantum statistically indistinguishable can be equivalently characterized by the trace distance $\|\rho_n - \xi_n\|_1 / 2$ being negligible.

C A note on quantum statistically-binding

A widely accepted definition of quantum binding [6] is $p_0 + P_1 < 1 + \epsilon$, where p_0 and p_1 are probability that sender can open the bit commitment as 0 and 1, respectively; ϵ is some negligible function. We next show that our definition of quantum statistically-binding in Definition 5 implies this widely accepted definition.

As a preparation, let us first prove a fact which gives a characterization of p_0 and p_1; this fact was also implicit in the proof of [30, Theorem 11].

Fact 18 *Let $Q_0, Q_1, \rho_0, \rho_1, p_0, p_1$ and Hilbert spaces $\mathcal{O}, \mathcal{G}$ be the same as introduced in Definition 5. Let $\sigma \in D(\mathcal{O})$ be the quantum state of Sender's message in the commit stage. Then*

$$p_0 = F(\rho_0, \sigma)^2, \quad p_1 = F(\rho_1, \sigma)^2.$$

PROOF: Denote $\gamma_0 \in \mathrm{D}(\mathcal{O} \otimes \mathcal{G})$ the quantum state of all qubits at receiver's hands when he/she has received message in the reveal stage and the bit to open is 0. Seeing from the canonical procedures of commit and reveal stages in our formalization of **QBC**, we know that $\mathrm{Tr}_{\mathcal{G}}(\gamma_0) = \sigma$. Then

$$\begin{aligned} p_0 &= \langle 0|Q_0^* \, \gamma_0 \, Q_0|0\rangle \\ &= F(Q_0|0\rangle, \gamma_0)^2 \qquad \text{(Fact 12)} \\ &\leq F(\rho_0, \sigma)^2. \qquad \text{(Fact 13)} \end{aligned}$$

We highlight that the equality in the last "$\leq$" above can be achieved, if sender prepares $\gamma_0 = \mathrm{Tr}_{\mathcal{A}}(uu^*)$, where $\mathcal{A}$ denote the Hilbert space corresponding to ancilla qubits used by (malicious) sender, and vector $u \in \mathcal{O} \otimes \mathcal{G} \otimes \mathcal{A}$ (guaranteed by Uhlmann Theorem, Fact 11) could be any purification of quantum state σ whose inner product with $Q_0|0\rangle \otimes |0\rangle_{\mathcal{A}}$ is equal to $F(\rho_0, \sigma)$.

Similarly, we can show that $p_1 = F(\rho_1, \sigma)^2$.

■

With the expressions for p_0 and p_1 given in Fact 18, applying 15, we get

$$\begin{aligned} p_0 + p_1 &= \max_{\sigma} \left(F(\rho_0, \sigma)^2 + F(\rho_1, \sigma)^2 \right) \\ &= 1 + F(\rho_0, \rho_1) \\ &< 1 + \epsilon(n). \end{aligned}$$

D A construction of statistically-binding QBC

We first give a formal definition for of *pseudorandom generator* against quantum attack. This definition is adapted from [7].

Definition 19 (Pseudorandom Generator Against Quantum Attack) A **pseudorandom generator** against quantum attack is a (classical) deterministic polynomial-time algorithm G satisfying the following two conditions:

1. *Expansion*: There exists a function $\ell : \mathbb{N} \to \mathbb{N}$ such that $\ell(n) > n$ for all $n \in \mathbb{N}$, and $|G(s)| = \ell|s|$ for all $s \in \{0,1\}^*$.

2. *Pseudorandomness* (against quantum attack): for any quantum state vector $|\phi\rangle \in (\mathbb{C}^2)^{\otimes \mathrm{poly}(n)}$ (i.e., quantum state of polynomial qubits), and any polynomial-size quantum measurement circuit family $\{D_n\}_{n\in\mathbb{N}}$,

$$\left| \Pr_{x \in_R \{0,1\}^n}[D_n(|G(x)\rangle|\phi\rangle) = 1] - \Pr_{y \in_R \{0,1\}^{\ell(n)}}[D_n(|y\rangle|\phi\rangle) = 1] \right| < \epsilon,$$

or equivalently (in the form of density operator, removing randomness),

$$\begin{aligned} \Big| \Pr\Big[D_n\Big(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} |G(x)\rangle\langle G(x)| \otimes |\phi\rangle\langle\phi|\Big) = 1\Big] - \\ \Pr\Big[D_n\Big(\frac{1}{2^{\ell(n)}} \sum_{y\in\{0,1\}^{\ell(n)}} |y\rangle\langle y| \otimes |\phi\rangle\langle\phi|\Big) = 1\Big] \Big| < \epsilon, \end{aligned}$$

Security parameter: n.

Construction: Assume $G : \{0,1\}^n \to \{0,1\}^{3n}$ is a classical pseudorandom generator against quantum attack (any quantum polynomial-time distinguisher). We construct quantum bit commitment scheme represented by a pair of quantum circuits (Q_0, Q_1) as below, both treating the first $3n$ qubits as the output.

- Quantum circuit Q_0:
  1. Apply Hadamard gate on each of the first n qubits;
  2. For $i = 1, \ldots, n$, apply CNOT gate on the i-th and the $(i+n)$-th qubits, with the former as the control.
  3. Simulate G in a standard reversible way, treating the first n qubits as the random bits used by G, and treating qubits from the $(2n+1)$-th one as ancillas that might be used in the simulation, while keeping the $(n+1)$-th to the $2n$-th qubits intact.
  4. Rearrange qubits so that the first $3n$ qubits correspond to the output of G.
- Quantum circuit Q_1:
  1. Apply Hadamard gate on each of the first $3n$ qubits;
  2. For $i = 1, \ldots, 3n$, apply CNOT gate on the i-th and the $(i+3n)$-th qubits, with the former as the control.

Figure 4: Statistically-binding **QBC** based on pseudorandom generator against quantum attack

where $\epsilon(\cdot)$ is some negligible function.

Remark. We point out that the classical construction to increase the expansion factor (refer to [7, section 3.3.2]) generalizes in a straightforward way to the quantum setting. It then follows that extension factor $\ell(n)$ in the definition above could be an arbitrary polynomial of n.

With pseudorandom generator at disposal, our construction of **QBC** is described in Figure 4, where by "simulate G in a standard reversible way" we mean given the description of G, i.e., a classical circuit, the computation of G can be simulated by a classical reversible circuit, which in turn can be simulated by a unitary quantum circuit; detail is referred to, e.g., [12, section 7].

The correctness of our construction is proved in the following lemma.

Lemma 20 *If there exists a classical pseudorandom generator against quantum attack, then the construction described in Figure 4 gives a (computationally hiding) statistically binding quantum bit commitment scheme.*

PROOF: To show that this quantum bit commitment scheme satisfies both hiding and binding conditions, let us write out the expressions for ρ_0 and ρ_1, the quantum states defined by quantum circuits Q_0 and Q_1, respectively.

Clearly we have

$$\rho_1 = \frac{1}{2^{3n}} \sum_{y \in \{0,1\}^{3n}} |y\rangle\langle y|;$$

that is, ρ_1 is the *maximally mixed state*. We also have

$$\begin{aligned} Q_0|0\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |G(x)\rangle|x\rangle|\psi_x\rangle \\ &= \sum_{y\in \mathrm{Im}(G)} |y\rangle \otimes \frac{1}{\sqrt{2^n}} \sum_{\substack{x\in\{0,1\}^n: \\ G(x)=y}} |x\rangle|\psi_x\rangle, \end{aligned}$$

where $\mathrm{Im}(G)$ denote the image of $G(\cdot)$ and $|\psi_x\rangle$ denote the quantum state of ancilla qubits (beyond the first $3n$ qubits) that we do not care about. Thus,

$$\rho_0 = \sum_{y\in \mathrm{Im}(G)} \alpha_y |y\rangle\langle y|,$$

where $\alpha_y = \Pr_{x\in_R\{0,1\}^n}[G(x) = y]$.

Next we show that our construction is computationally hiding and statistically binding.

Hiding. Note that quantum states ensembles $\{\rho_0\}_n$ and $\{\rho_1\}_n$ are quantum computationally indistinguishable because $G(\cdot)$ is a pseudorandom generator against quantum attack. The scheme is thus computationally hiding.

Binding. We estimate the trace distance between ρ_0 and ρ_1:

$$\begin{aligned} \|\rho_0 - \rho_1\|_1 &= \sum_{y\in \mathrm{Im}(G)} \left| \frac{1}{2^{3n}} - \alpha_y \right| + \sum_{y\in\{0,1\}^{3n}\setminus \mathrm{Im}(G)} \frac{1}{2^{3n}} \\ &\leq 2 - o(1), \end{aligned}$$

by observing that $|\mathrm{Im}(G)| \leq 2^n$. Therefore, $F(rho_0, \rho_) = o(1)$ by Fuchs-van de Graaf inequality (Fact 16); the scheme is thus statistically-binding.

■

E A proof for Lemma 6

We give a proof for our technical Lemma 6 below.

RESTATEMENT OF **Lemma 6**: Let $\mathcal{X}, \mathcal{Y}$ be two complex Euclidean spaces, and $P_1, \ldots, P_m$ be projectors on $\mathcal{X}\otimes\mathcal{Y}$. If there exists a vector $|\psi\rangle \in \mathcal{X}\otimes\mathcal{Y}$ and unitary transformations $U_1, \ldots, U_m \in U(\mathcal{Y})$ such that $\sum_i \|P_i U_i|\psi\rangle\|^2 / m \geq 1 - \delta$ for some $0 \leq \delta \leq 1$, then there exists unitary transformations $U'_1, \ldots, U'_m \in U(\mathcal{Y})$ satisfying $\|P_1 U'_1 \cdots P_m U'_m|\psi\rangle\| \geq 1 - m\sqrt{\delta}$.

PROOF: From the assumption $\sum_i \|P_i U_i|\psi\rangle\|^2 / m \geq 1 - \delta$, we have

$$\frac{1}{m}\sum_i \|P_i U_i|\psi\rangle - U_i|\psi\rangle\|^2 \leq \delta. \tag{6}$$

Common input: a graph G with n vertices.

Private input to prover: a coloring scheme of vertices of G such that each edge of G is bi-colored.

Protocol:

- Prover (P1): Select a random permutation π of three colors $\{1, 2, 3\}$, and for each vertex v of G, commit to $\pi(c_v)$ where c_v is the color of v under the coloring scheme. Then send these bit commitments to verifier.
- Verifier (V1): Select an edge e of G randomly and uniformly, and send it to prover.
- Prover (P2): Open the color of the two vertices adjacent to edge e as specified under the coloring scheme after permutation π.
- Verifier (V2): Check if the colors of the two vertices adjacent to edge e are opened successfully and differently.

Figure 5: GMW-type zero-knowledge protocol for Graph 3-Coloring

Choose $U'_i = U_i U^*_{i+1}$ for $1 \le i \le m-1$, and $U'_m = U_m$. Then,

$$\begin{aligned}
& \left\| P_1 U'_1 \cdots P_{m-1} U'_{m-1} P_m U'_m |\psi\rangle \right\| \\
= \; & \left\| P_1 U'_1 \cdots P_{m-1} U'_{m-1} (U_m|\psi\rangle + (P_m U_m|\psi\rangle - U_m|\psi\rangle)) \right\| \\
\ge \; & \left\| P_1 U'_1 \cdots P_{m-1} U'_{m-1} U_m|\psi\rangle \right\| - \left\| P_1 U'_1 \cdots P_{m-1} U'_{m-1} (P_m U_m|\psi\rangle - U_m|\psi\rangle) \right\| \\
\ge \; & \left\| P_1 U'_1 \cdots P_{m-1} U_{m-1}|\psi\rangle \right\| - \| P_m U_m|\psi\rangle - U_m|\psi\rangle \| \\
\ge \; & \cdots \\
\ge \; & 1 - \sum_{i=1}^{m} \| P_i U_i|\psi\rangle - U_i|\psi\rangle \| \\
\ge \; & 1 - \sqrt{\sum_{i=1}^{m} \| P_i U_i|\psi\rangle - U_i|\psi\rangle \|^2 \cdot m} \quad \text{(Cauchy-Schwartz inequality)} \\
\ge \; & 1 - m\sqrt{\delta}. \qquad \text{(Plug inequality (6))}
\end{aligned}$$

We complete the proof. ∎

F QZK for Graph 3-Coloring

The GMW-type zero-knowledge protocol for Graph 3-Coloring is described in Figure 5.

The proof for the soundness of the protocol is similar to Hamiltonian Cycle, which we sketch below. Specifically, suppose verifier selects edge denoted by e as the challenge. Then verifier's action upon receiving prover's response (the third message) can be viewed as a binary measurement $\{P_e, \mathbb{1} - P_e\}$, where projector $P_e = \sum_{c_1 \neq c_2} |c_1 c_2\rangle\langle c_1 c_2| \otimes \Pi_e(c_1, c_2)$; c_1, c_2 denotes two colors; projector $\Pi_e(c_1, c_2)$ corresponds to that commitments of colors at the two vertices adjacent to edge e are opened as color c_1 respective c_2 successfully. In more detail, using our formalization of **QBC**, which

is described by a pair of quantum circuits (Q_0, Q_1), then $\Pi_e(c_1, c_2) = Q_{c_1}|0\rangle_e\langle 0|Q^*_{c_1} \otimes Q_{c_2}|0\rangle_e\langle 0|Q^*_{c_2}$, where suppose color c is described by two bits b_1b_2, then quantum circuit $Q_c = Q_{b_1} \otimes Q_{b_2}$; moreover, projectors $Q_{c_1}|0\rangle_e\langle 0|Q^*_{c_1}$ and $Q_{c_2}|0\rangle_e\langle 0|Q^*_{c_2}$ operate on the bit commitments of colors corresponding to the two vertices adjacent to edge e, respectively.

Then like soundness analysis of Hamiltonian Cycle, it suffices to show that for any unitary transformations $U'_1, \ldots U'_m$ operating on prover's response, the operator norm $\|P_1U'_1 \cdots P_mU'_m\|$ is negligible, where m is the number of edges of G, and $P_1, \ldots, P_m$ are projectors described above corresponding to verifier's different challenges (edges).

We first consider the operator norm of the tensor product of term $\Pi_e(c_1, c_2)$ within P_e for each edge e, where $\Pi_e(c_1, c_2) = Q_{c_1}|0\rangle_e\langle 0|Q^*_{c_1} \otimes Q_{c_2}|0\rangle_e\langle 0|Q^*_{c_2}$ as described above. Since graph G is not 3-colorable, there exist edges e, e' such that their common vertex is colored with different colors in the coloring schemes of e and e'. It follows that the operator norm $\|\bigotimes_e \Pi_e(c_1, c_2)\|$ is upperbounded by $F(\rho_0, \rho_1)$, where ρ_0, ρ_1 are quantum states defined by quantum circuits (Q_0, Q_1) in our formalization of **QBC**. Summing up over all possible pair of colors (c_1, c_2) for each edge, we have the operator norm

$$\|P_1P_2 \cdots P_m\| < 6^m \cdot F(\rho_0, \rho_1) < 6^m \cdot 2^{-n^3} = o(1).$$

Finally, we remark that the same upper bound also applies to $\|P_1U'_1 \cdots P_mU'_m\|$, because $U'_1, \ldots U'_m$ only operate on prover's response; but our upper bound is derived from the subspace corresponding to prover's commitment, which $U'_1, \ldots U'_m$ does not touch.

G QBC from QZK

Our basic construction from **QZK** proof to (statistically binding) instance-dependent **QBC** is borrowed from Watrous [30]. Specifically, suppose problem A has an m-message *honest-verifier* quantum statistical (resp. computational) zero-knowledge proof. By Watrous' construction [30, section 5], given an instance $x \in \mathsf{A}_{\text{YES}} \cup \mathsf{A}_{\text{NO}}$, we can construct a pair of quantum circuits (Q_0, Q_1), which define two quantum states ρ_0, ρ_1, respectively, satisfying the following properties:

- If $x \in \mathsf{A}_{\text{YES}}$, then ρ_0 and ρ_1 are statistically (resp. computationally) indistinguishable.
- If $x \in \mathsf{A}_{\text{NO}}$, then $\|\rho_0 - \rho_1\|_1 / 2 > c/m$, where c is some constant.

We remark that Watrous only proves the properties above for quantum statistically zero-knowledge proof (**QSZK**). Regarding quantum computationally zero-knowledge proof (**QCZK**), the proof for the case $x \in \mathsf{A}_{\text{NO}}$ is the same as Watrous, since the soundness for **QSZK** and **QCZK** are the same (both information-theoretic). After a careful examination, we find the proof for the case $x \in \mathsf{A}_{\text{YES}}$ is also similar to Watrous, except that we replace statistically indistinguishable in Watrous' proof with computationally indistinguishable.

We observe that this pair of quantum circuits naturally gives a weak instance-dependent **QBC**, where by "weak" we mean the trace distance between ρ_0 and ρ_1 is *not* large enough as we need when $x \in \mathsf{A}_{\text{NO}}$. Constructions to amplify the trace distance, though different with respect to quantum statistical and computational zero-knowledge proofs, are standard; we describe them below.

Statistical setting. In this setting, the hiding condition (when $x \in \mathsf{A}_{\text{YES}}$) can be equivalently characterized by the trace distance $\|\rho_0 - \rho_1\|_1 / 2$ being negligible. Thus, what we really need is a procedure to *polarize* the trace distance: we want to increase the trace distance when it is mildly large while decrease it when negligible. Actually, Watrous [30, Theorem 5] also gave such a kind

of polarization procedure, which is adapted from its classical counterpart [25]; we omit the detail here. Anyway, by applying Watrous' polarization procedure to quantum circuits (Q_0, Q_1), we get another pair of quantum circuits denoted by (Q'_0, Q'_1), whose sizes are $O(\mathrm{poly}(|x|))$, defining a pair of quantum states (ρ'_0, ρ'_1) such that

- If $x \in \mathsf{A}_{\mathrm{YES}}$, then ρ'_0 and ρ'_1 are statistically indistinguishable (or precisely, $\|\rho'_0 - \rho'_1\|_1 /2 < 2^{-\mathrm{poly}(|x|)}$).
- If $x \in \mathsf{A}_{\mathrm{NO}}$, then $\|\rho'_0 - \rho'_1\|_1 /2 > 1 - 2^{-\mathrm{poly}(|x|)}$.

As a consequence, quantum circuits (Q'_0, Q'_1) give a desired instance-dependent quantum bit commitment scheme.

Computational setting. In this setting, just taking multiple copies of (Q_0, Q_1) do the job. This is because the property of computationally indistinguishable is preserved when $x \in \mathsf{A}_{\mathrm{YES}}$ (just by a simple hybrid argument; see [31, Proposition 4] for detail), while the trace distance $\|\rho_0 - \rho_1\|_1 /2$ decreases with exponential speed when $x \in \mathsf{A}_{\mathrm{NO}}$.