Non-interactive Quantum Perfect and Statistical Zero-Knowledge

Hirotada Kobayashi

Quantum Computation and Information Project,
Exploratory Research for Advanced Technology,
Japan Science and Technology Corporation,
5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan
hirotada@qci.jst.go.jp

Abstract. This paper introduces quantum analogues of non-interactive perfect and statistical zero-knowledge proof systems. Similar to the classical cases, it is shown that sharing randomness or entanglement is necessary for non-trivial protocols of non-interactive quantum perfect and statistical zero-knowledge. It is also shown that, with sharing EPR pairs a priori, the complexity class resulting from non-interactive quantum perfect zero-knowledge proof systems of perfect completeness has a natural complete promise problem. Using our complete promise problem, the Graph Non-Automorphism problem is shown to have a non-interactive quantum perfect zero-knowledge proof system.

1 Introduction

Zero-knowledge proof systems were introduced by Goldwasser, Micali, and Rackoff [10] and have been studied extensively from both complexity theoretical and cryptographic viewpoints. Because of their wide applicability in the domain of classical communication and cryptography, the quantum analogue of zero-knowledge proof systems is expected to play very important roles in the domain of quantum communication and cryptography.

Very recently Watrous [21] proposed a formal model of quantum statistical zero-knowledge proof systems. To our knowledge, his model is the only one for a formal model of quantum zero-knowledge proofs, although he considered only the case with an *honest verifier*. The reason why he put such a restriction seems to be that even his model may not give a cryptographically satisfying definition for quantum statistical zero-knowledge when the honest verifier assumption is absent. Indeed, generally speaking, difficulties arise when we try to define the notion of quantum zero-knowledge against dishonest verifiers by extending classical definitions of zero-knowledge in the most straightforward ways. See [11] for a discussion of such difficulties in security of quantum protocols. Nevertheless, the model of quantum statistical zero-knowledge proofs by Watrous is natural and reasonable at least in some restricted situations. One of such situations is the case with an honest verifier, which was discussed by Watrous himself. Another situation is the case of *non-interactive* protocols, which this paper treats.

T. Ibaraki, N. Katoh, and H. Ono (Eds.): ISAAC 2003, LNCS 2906, pp. 178–188, 2003.

Classical version of non-interactive zero-knowledge proof systems was introduced by Blum, Feldman, and Micali [2], and was later studied by a number of works [4,5,1,7,14,3,9,19]. Such non-interactive proof systems put an assumption that a verifier and a prover share some random string, and this shared randomness is necessary for non-trivial protocols (i.e., protocols for problems beyond BPP) of non-interactive quantum zero-knowledge proofs [7]. As for non-interactive statistical zero-knowledge proof systems, De Santis, Di Crescenzo, Persiano, and Yung [3] showed that the resulting complexity class NISZK has a complete promise problem, namely the Image Density (ID) problem. Goldreich, Sahai, and Vadhan [9] showed another two complete promise problems for NISZK, the Entropy Approximation (EA) problem and the Statistical Difference from Uniform (SDU) problem, from which they derived a number of properties of NISZK such as evidence of non-triviality of the class NISZK.

This paper focuses on quantum analogues of non-interactive perfect and statistical zero-knowledge proof systems. The notion of quantum zero-knowledge used in this paper is along the lines defined by Watrous [21]. Similar to the classical cases, it is shown that shared randomness or entanglement is necessary for non-trivial protocols (i.e., protocols for problems beyond BQP) of non-interactive quantum perfect and statistical zero-knowledge. It is proved that, with sharing EPR pairs a priori, the complexity class resulting from non-interactive quantum perfect zero-knowledge proof systems of perfect completeness has a natural complete promise problem, which we call the *Quantum State Closeness to Maximally Mixed (QSCMM)* problem, informally described as follows: given a description of a quantum circuit Q, is the output quantum state of Q close to the maximally mixed state or is it far from that? Note that our QSCMM problem may be viewed as a quantum variant of the SDU problem, which was shown NISZK-complete by Goldreich, Sahai, and Vadhan [9]. However, our proof for the completeness of the QSCMM problem is quite different from their proof for the classical case at least in the following two senses: (i) the completeness of the QSCMM problem is shown in a direct manner, while that of the classical SDU problem was shown by using other complete problems such as the ID problem and the EA problem, and (ii) our proof is rather quantum information theoretical. Using our complete problem, it is straightforward to show that the Graph Non-Automorphism (GNA) problem (or sometimes called the Rigid Graphs problem), which is not known in BQP, has a non-interactive quantum perfect zero-knowledge proof system of perfect completeness. Classically, the GNA problem can be reduced to the EA problem [19], and thus it is in NISZK. However, the protocol for the EA problem [9] makes use of hash functions, and is quite complicated. In contrast, both our reduction from a GNA instance to a QSCMM instance and our protocol for the QSCMM problem are remarkably simple.

One of the merits of considering non-interactive models is that the zero-knowledge property in such protocols does not depend on whether the verifier in the protocol is honest or not. Thus, our results may be the first non-trivial quantum zero-knowledge proofs secure even against dishonest quantum verifiers.

Familiarity with the basics of quantum computation and information theory is assumed throughout this paper. See [12,16,15], for instance.

2 Definitions

We start with a notion of polynomial-time preparable sets of quantum states introduced by Watrous [21]. Throughout this paper we assume that all input strings are over the alphabet $\Sigma = \{0, 1\}$, and $\mathbb{N}$ and $\mathbb{Z}^+$ denote the sets of natural numbers and nonnegative integers, respectively. We also use the notation $\mathbf{D}(\mathcal{H})$ for the set of mixed states in $\mathcal{H}$.

A collection $\{\rho_x\}$ of mixed states is *polynomial-time preparable* if there exists a polynomial-time uniformly generated family $\{Q_x\}$ of quantum circuits such that, for every x of length n, (i) Q_x is a quantum circuit over $q(n)$ qubits for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$, and (ii) for the pure state $Q_x|0^{q(n)}\rangle$, the first $q_{\mathrm{out}}(n)$ qubits of it is in the mixed state ρ_x when tracing out the rest $q(n) - q_{\mathrm{out}}(n)$ qubits, where $q_{\mathrm{out}}\colon \mathbb{Z}^+ \to \mathbb{N}$ is a polynomially bounded function satisfying $q_{\mathrm{out}} \leq q$. In this context, the collection of the first $q_{\mathrm{out}}(n)$ qubits may be regarded as an output, and thus we also say that such a family $\{Q_x\}$ of quantum circuits is *q-in q_{out}-out*.

Now we give a definition of non-interactive quantum perfect and statistical zero-knowledge proof systems in terms of quantum circuits.

For each input x of length n, the entire system of our quantum circuit consists of $q(n) = q_{\mathcal{V}}(n) + q_{\mathcal{M}}(n) + q_{\mathcal{P}}(n)$ qubits, where $q_{\mathcal{V}}(n)$ is the number of qubits that are private to a verifier V, $q_{\mathcal{P}}(n)$ is the number of qubits that are private to a prover P, and $q_{\mathcal{M}}(n)$ is the number of message qubits sent from P to V. Furthermore, it is assumed that the verifier V and the prover P share EPR pairs a priori among their private qubits. Let $q_{\mathcal{S}}(n)$ be the number of the EPR pairs shared by V and P. It is also assumed that $q_{\mathcal{V}}$, $q_{\mathcal{M}}$, and $q_{\mathcal{S}}$ are polynomially bounded functions. Let $q_{\mathcal{V}_{\overline{\mathcal{S}}}} = q_{\mathcal{V}} - q_{\mathcal{S}}$ and $q_{\mathcal{P}_{\overline{\mathcal{S}}}} = q_{\mathcal{P}} - q_{\mathcal{S}}$.

A *$(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier* V is a polynomial-time computable mapping of the form $V\colon \Sigma^* \to \Sigma^*$. V receives a message of at most $q_{\mathcal{M}}(n)$ qubits from the prover, and uses at most $q_{\mathcal{V}}(n)$ qubits for his private space, including qubits of shared EPR pairs. For every x, $V(x)$ is interpreted as a description of a polynomial-time uniformly generated quantum circuit acting on $q_{\mathcal{V}}(n) + q_{\mathcal{M}}(n)$ qubits. One of the private qubits of V is designated as the output qubit.

A *$(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum prover* P is a mapping of the form $P\colon \Sigma^* \to \Sigma^*$. P uses at most $q_{\mathcal{P}}(n)$ qubits for his private space, including qubits of shared EPR pairs, and sends a message of at most $q_{\mathcal{M}}(n)$ qubits to the verifier. For every x, $P(x)$ is interpreted as a description of a quantum circuit acting on $q_{\mathcal{M}}(n) + q_{\mathcal{P}}(n)$ qubits. No restrictions are placed on the complexity of the mapping P (i.e., $P(x)$ can be an arbitrary unitary transformation).

A *$(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted non-interactive quantum proof system* consists of a $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier V and a $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum prover P. Let $\mathcal{V} = l_2(\Sigma^{q_{\mathcal{V}}})$, $\mathcal{M} = l_2(\Sigma^{q_{\mathcal{M}}})$, and $\mathcal{P} = l_2(\Sigma^{q_{\mathcal{P}}})$ denote the Hilbert spaces corresponding to the private qubits of the verifier, the message qubits between

the verifier and the prover, and the private qubits of the prover, respectively. A $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted non-interactive quantum proof system is *$q_{\mathcal{S}}$-shared-EPR-pairs* if, for every x of length n, there are $q_{\mathcal{S}}(n)$ copies of the EPR pair $(|00\rangle + |11\rangle)/\sqrt{2}$ that are initially shared by the verifier and the prover. Let $\mathcal{V}_{\mathcal{S}} = l_2(\Sigma^{q_{\mathcal{S}}})$ and $\mathcal{P}_{\mathcal{S}} = l_2(\Sigma^{q_{\mathcal{S}}})$ denote the Hilbert spaces corresponding to the verifier and the prover parts of these shared EPR pairs, respectively, and write $\mathcal{V} = \mathcal{V}_{\overline{\mathcal{S}}} \otimes \mathcal{V}_{\mathcal{S}}$ and $\mathcal{P} = \mathcal{P}_{\overline{\mathcal{S}}} \otimes \mathcal{P}_{\mathcal{S}}$. It is assumed that all the qubits in $\mathcal{V}_{\overline{\mathcal{S}}}$, $\mathcal{M}$, and $\mathcal{P}_{\overline{\mathcal{S}}}$ are initialized to the $|0\rangle$-state.

Given a verifier V, a prover P, and an input x of length n, define a circuit $(P(x), V(x))$ acting on $q(n)$ qubits to be the one applying $P(x)$ to $\mathcal{M} \otimes \mathcal{P}$ and $V(x)$ to $\mathcal{V} \otimes \mathcal{M}$ in sequence. The probability that (P, V) accepts x is defined to be the probability that an observation of the output qubit in the basis of $\{|0\rangle, |1\rangle\}$ yields $|1\rangle$, after the circuit $(P(x), V(x))$ is applied to the initial state.

In what follows, the circuits $P(x)$ and $V(x)$ may be simply denoted by P and V, respectively, if it is not confusing. Furthermore it is assumed that operators acting on subsystems of a given system are extended to the entire system by tensoring with the identity, when it is clear from context upon what part of a system a given operator acts.

The classes NIQPZK(a, b) and NIQSZK(a, b) of languages having non-interactive quantum perfect and statistical zero-knowledge proof systems with error probabilities a and b in completeness and soundness sides, respectively, are defined as follows.

Definition 1. *Given functions $a, b\colon \mathbb{Z}^+ \to [0, 1]$, a language L is in* NIQPZK(a, b) *(resp.* NIQSZK(a, b)*) if there exist polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{S}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and a $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier V such that, for every input x of length n,*

(i) Completeness:
if $x \in L$, there exist a function $q_{\mathcal{P}}\colon \mathbb{Z}^+ \to \mathbb{N}$ and a $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum prover P, where P and V share $q_{\mathcal{S}}(n)$ EPR-pairs a priori, such that (P, V) accepts x with probability at least $a(n)$,

(ii) Soundness:
if $x \notin L$, for any function $q_{\mathcal{P}'}\colon \mathbb{Z}^+ \to \mathbb{N}$ and any $(q_{\mathcal{M}}, q_{\mathcal{P}'})$-restricted quantum prover P', where P' and V share $q_{\mathcal{S}}(n)$ EPR-pairs a priori, (P', V) accepts x with probability at most $b(n)$,

(iii) Zero-Knowledge:
there exists a polynomial-time preparable set $\{\sigma_x\}$ of mixed states of $q_{\mathcal{V}}(n) + q_{\mathcal{M}}(n)$ qubits such that, if $x \in L$, $\sigma_x = \mathrm{tr}_{\mathcal{P}}(P|\psi_{\mathrm{init}}\rangle\langle\psi_{\mathrm{init}}|P^\dagger)$ (resp. $\|\sigma_x - \mathrm{tr}_{\mathcal{P}}(P|\psi_{\mathrm{init}}\rangle\langle\psi_{\mathrm{init}}|P^\dagger)\|_{\mathrm{tr}}$ is negligible in n) for the honest prover P, where $|\psi_{\mathrm{init}}\rangle$ is the initial state in which all the qubits except for the $q_{\mathcal{S}}(n)$ shared EPR-pairs are in the $|0\rangle$-state.

A few notes are in order regarding our definitions of non-interactive quantum perfect and statistical zero-knowledge. First, note that the state $\mathrm{tr}_{\mathcal{P}}(P|\psi_{\mathrm{init}}\rangle\langle\psi_{\mathrm{init}}|P^\dagger)$ in Definition 1 corresponds to the "verifier's view". Second, Definition 1 requires the set $\{\sigma_x\}$ to be prepared in *worst-case* polynomial

time *without fail*. This is in contrast to the common definitions of various classical zero-knowledge proofs in which the simulator is an *expected* polynomial-time machine or a worst-case polynomial-time machine *that may fail*. Third, similar to the QMA case [20,15], parallel repetition of non-interactive quantum perfect and statistical zero-knowledge proof systems can reduce completeness and soundness errors to be exponentially small while preserving the zero-knowledge property. Fourth, the classes NIQSZK and NIQPZK above, which are defined in terms of languages, can be naturally rephrased to those in terms of promise problems. Throughout this paper, we allow a little abuse of complexity classes and common complexity classes such as BPP and BQP are also considered to be those naturally rephrased in terms of promise problems. See [6] for detailed description on promise problems.

Finally, similar to the classical cases [7], shared randomness or entanglement is necessary for non-trivial protocols of non-interactive quantum perfect or statistical zero-knowledge. The proof is straightforward and thus omitted.

Theorem 2. *Without shared randomness or shared entanglement, any problem having non-interactive quantum perfect or statistical zero-knowledge proofs is necessarily in* BQP.

3 Complete Promise Problem for NIQPZK(1, 1/2)

This paper considers the promise problem called (α, β)-*Quantum State Closeness to Maximally Mixed (*(α, β)-*QSCMM)* problem, which is parameterized by constants α and β satisfying $0 \leq \alpha < \beta \leq 1$. Our promise problem is a variant of the (α, β)-Quantum State Distinguishability ((α, β)-QSD) problem and its complement, the (α, β)-Quantum State Closeness ((α, β)-QSC) problem, both of which were introduced and shown to be HVQSZK-complete (for any $0 \leq \alpha < \beta^2 \leq 1$) by Watrous [21]. As the (α, β)-QSD problem is a quantum analogue of the Statistical Difference (SD) problem [17], which is HVSZK-complete (and thus SZK-complete from the consecutive result HVSZK = SZK [8]), so the (α, β)-QSCMM problem is a quantum analogue of the Statistical Difference from Uniform Distribution (SDU) problem [9], which is NISZK-complete.

(α, β)-Quantum State Closeness to Maximally Mixed ((α, β)-QSCMM)

Input: A description of a quantum circuit Q acting over the Hilbert space $\mathcal{H}_{\text{in}} = \mathcal{H}_{\text{out}} \otimes \mathcal{H}_{\overline{\text{out}}}$, where $\mathcal{H}_{\text{in}}$ consists of q_{in} qubits and $\mathcal{H}_{\text{out}}$ consists of $q_{\text{out}} \leq q_{\text{in}}$ qubits.

Promise: For $\rho = \text{tr}_{\mathcal{H}_{\overline{\text{out}}}}(Q|0^{q_{\text{in}}}\rangle\langle 0^{q_{\text{in}}}|Q^\dagger)$, we have either $\|\rho - I/2^{q_{\text{out}}}\|_{\text{tr}} \leq \alpha$ or $\|\rho - I/2^{q_{\text{out}}}\|_{\text{tr}} \geq \beta$.

Output: Accept if $\|\rho - I/2^{q_{\text{out}}}\|_{\text{tr}} \leq \alpha$, and reject if $\|\rho - I/2^{q_{\text{out}}}\|_{\text{tr}} \geq \beta$.

Now we show that the $(0, \beta)$-QSCMM problem is NIQPZK$(1, 1/2)$-complete for any $0 < \beta < 1$. Since parallel repetition works well for non-interactive quan-

tum perfect zero-knowledge proofs, this implies the NIQPZK$(1, b)$-completeness for any bounded error probability b.

First we show that $(0, \beta)$-QSCMM is in NIQPZK$(1, 1/2)$. The proof uses the following well-known property in quantum information theory.

Theorem 3 ([18,13]). *For any pure states $|\phi\rangle, |\psi\rangle \in \mathcal{H} \otimes \mathcal{K}$ satisfying $\mathrm{tr}_{\mathcal{K}}|\phi\rangle\langle\phi| = \mathrm{tr}_{\mathcal{K}}|\psi\rangle\langle\psi|$, there exists a unitary transformation U over $\mathcal{K}$ such that $(I_{\mathcal{H}} \otimes U)|\phi\rangle = |\psi\rangle$, where $I_{\mathcal{H}}$ is the identity operator over $\mathcal{H}$.*

Lemma 4. *$(0, \beta)$-QSCMM is in* NIQPZK$(1, 1/2)$ *for any $0 < \beta < 1$.*

Proof. Let Q be a quantum circuit of the $(0, \beta)$-QSCMM, which is q-in q_{out}-out. Running $O(n)$ copies of Q in parallel for n exceeding the length of the input Q constructs a quantum circuit R of q'-in q'_{out}-out that outputs the associated mixed state ξ of q'_{out} qubits such that ξ either is $I/2^{q'_{\mathrm{out}}}$ or satisfies $\|\xi - I/2^{q'_{\mathrm{out}}}\|_{\mathrm{tr}} > 1 - 2^{-n}$.

We construct a $(q'_{\mathrm{out}}, q' - q'_{\mathrm{out}})$-restricted quantum verifier V of a non-interactive quantum perfect zero-knowledge proof system of q'_{out}-shared-EPR-pairs (i.e., all the private qubits of V are particles of the shared EPR-pairs). Let the quantum registers $\mathbf{M}$ and $\mathbf{S}$ consist of the message qubits and the qubits in the verifier part of the shared EPR pairs, respectively. The verification procedure of V is as follows:

1. Receive a message in $\mathbf{M}$ from the prover.
2. Apply $R^{\dagger}$ on the pair of quantum registers $(\mathbf{M}, \mathbf{S})$.
3. Accept if $(\mathbf{M}, \mathbf{S})$ contains $0^{q'}$, and reject otherwise.

Hereafter, it is assumed that the output qubits of R and $R^{\dagger}$ correspond to the qubits in $\mathbf{S}$ in the applications of R and $R^{\dagger}$.

For the completeness, suppose that $\xi = I/2^{q'_{\mathrm{out}}}$. Let $q_{\mathcal{P}} = q'_{\mathrm{out}}$ be the number of private qubits of an honest prover (i.e., all the private qubits of the honest prover are particles of the shared EPR-pairs). Note that the pure state $|\phi\rangle = (R|0^{q'}\rangle) \otimes |0^{q_{\mathcal{P}}}\rangle$ of $q' + q_{\mathcal{P}}$ qubits is a purification of ξ. Since the initial state $|\psi_{\mathrm{init}}\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$ of $q' + q_{\mathcal{P}}$ qubits is a purification of $I/2^{q'_{\mathrm{out}}}$ and $\xi = I/2^{q'_{\mathrm{out}}}$, from Theorem 3, there exists a unitary transformation P over $\mathcal{M} \otimes \mathcal{P}$ such that $(I_{\mathcal{V}} \otimes P)|\psi_{\mathrm{init}}\rangle = |\phi\rangle$, where $I_{\mathcal{V}}$ is the identity operator over $\mathcal{V}$. Therefore,

$$(R^{\dagger} \otimes I_{\mathcal{P}})(I_{\mathcal{V}} \otimes P)|\psi_{\mathrm{init}}\rangle = |0^{q'+q_{\mathcal{P}}}\rangle,$$

where $I_{\mathcal{P}}$ is the identity operator over $\mathcal{P}$. Thus V accepts the input with certainty.

For the soundness, suppose that $\|\xi - I/2^{q'_{\mathrm{out}}}\|_{\mathrm{tr}} > 1 - 2^{-n}$. Then, for arbitrarily large private space $\mathcal{P}'$ of a prover and any unitary transformation P' over $\mathcal{M} \otimes \mathcal{P}'$, letting $|\psi\rangle = (I_{\mathcal{V}} \otimes P')|\psi'_{\mathrm{init}}\rangle$ for the initial state $|\psi'_{\mathrm{init}}\rangle \in \mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}'$, we have

$$\|R|0^{q'}\rangle\langle 0^{q'}|R^{\dagger} - \mathrm{tr}_{\mathcal{P}'}|\psi\rangle\langle\psi|\|_{\mathrm{tr}} > 1 - 2^{-n},$$

since $\mathrm{tr}_{\mathcal{M}}(R|0^{q'}\rangle\langle 0^{q'}|R^\dagger) = \xi$ and $\mathrm{tr}_{\mathcal{M}}(\mathrm{tr}_{\mathcal{P}'}|\psi\rangle\langle\psi|) = I/2^{q'_{\mathrm{out}}}$. Therefore we have

$$\||0^{q'}\rangle\langle 0^{q'}| - R^\dagger(\mathrm{tr}_{\mathcal{P}'}|\psi\rangle\langle\psi|)R\|_{\mathrm{tr}} > 1 - 2^{-n}.$$

Thus, using the relation between the trace norm and fidelity, it follows that the probability that V accepts the input is negligible.

Finally, the fact that $R|0^{q'}\rangle\langle 0^{q'}|R^\dagger = \mathrm{tr}_{\mathcal{P}}((I_{\mathcal{V}} \otimes P)|\psi_{\mathrm{init}}\rangle\langle\psi_{\mathrm{init}}|(I_{\mathcal{V}} \otimes P^\dagger))$ is polynomial-time preparable ensures the perfect zero-knowledge property. □

Next we show the NIQPZK$(1, 1/2)$-hardness of $(0, \beta)$-QSCMM. For this, we state one fundamental property on trace norms without a proof.

Theorem 5. *For a constant α, $0 \le \alpha < 1$, let ρ be a mixed state of n qubits satisfying $\|\rho - I/2^n\|_{\mathrm{tr}} \ge \alpha$. Then for any mixed state σ of n qubits and any constant β satisfying $0 \le \beta \le \alpha$, $\|(1-\beta)\rho + \beta\sigma - I/2^n\|_{\mathrm{tr}} \ge \alpha - \beta$.*

Lemma 6. *For any problem A in* NIQPZK$(1, 1/2)$*, there is a deterministic polynomial-time procedure that reduces A to the $(0, \beta)$-QSCMM problem for $0 < \beta < 1$.*

Proof. Let $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ be in NIQPZK$(1, 1/2)$. Then from the fact that parallel repetition works well for non-interactive quantum perfect zero-knowledge proof systems, there exist polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{S}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and a $(q_{\mathcal{V}}, q_{\mathcal{M}})$-restricted quantum verifier V such that, for every input x of length n, (i) if $x \in A_{\mathrm{yes}}$, there exist a function $q_{\mathcal{P}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and a $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum prover P, who shares $q_{\mathcal{S}}(n)$ EPR-pairs with V a priori, such that (P, V) accepts x with certainty, and (ii) if $x \in A_{\mathrm{no}}$, for any function $q_{\mathcal{P}'} \colon \mathbb{Z}^+ \to \mathbb{N}$ and any $(q_{\mathcal{M}}, q_{\mathcal{P}'})$-restricted quantum prover P', who shares $q_{\mathcal{S}}(n)$ EPR-pairs with V a priori, (P', V) accepts x with probability smaller than 2^{-n}. Without loss of generality, we assume that $q_{\mathcal{S}}(n) \ge n$.

Let $V(x)$ and $P(x)$ be the unitary transformations of the honest verifier V and the honest prover P, respectively, on a given input x. Let $\{\sigma_x\}$ be a polynomial-time preparable set such that, if the input x of length n is in A_{yes},

$$\sigma_x = \mathrm{tr}_{\mathcal{P}}(P(x)|\psi_{\mathrm{init}}\rangle\langle\psi_{\mathrm{init}}|P(x)^\dagger)$$

for the honest prover P. The existence of such a polynomial-time preparable set is ensured by the perfect zero-knowledge property. For convenience, we assume that, for every x of length n, the first $q_{\mathcal{M}}(n)$ qubits of σ_x correspond to the message qubits, the last $q_{\mathcal{V}_{\overline{S}}}(n) = q_{\mathcal{V}}(n) - q_{\mathcal{S}}(n)$ qubits of σ_x correspond to the private qubits of the verifier (not including the prior-entangled part), and the last qubit corresponds to the output qubit, of the original proof system, respectively.

Let $\mathbf{M}$, $\mathbf{S}$, and $\mathbf{V}$ be quantum registers, each of which consists of $q_{\mathcal{M}}(n)$, $q_{\mathcal{S}}(n)$, and $q_{\mathcal{V}_{\overline{S}}}(n)$ qubits, respectively. For every x, we construct a quantum circuit Q_x that corresponds to the following algorithm:

1. Prepare σ_x in the triplet $(\mathbf{M}, \mathbf{S}, \mathbf{V})$ of the quantum registers.

2. If one of qubits in the quantum register $\mathbf{V}$ contains 1, output $|0^{q_S(n)}\rangle\langle 0^{q_S(n)}|$.
3. Do one of the following two uniformly at random.
   3.1 Output the qubits in the quantum register $\mathbf{S}$.
   3.2 Apply $V(x)$ on the triplet $(\mathbf{M}, \mathbf{S}, \mathbf{V})$ of the quantum registers. Output $I/2^{q_S(n)}$ if the last qubit in $\mathbf{V}$ contains 1, and output $|0^{q_S(n)}\rangle\langle 0^{q_S(n)}|$ otherwise.

Suppose that x is in A_{yes}. Then $\sigma_x = \mathrm{tr}_{\mathcal{P}}(P(x)|\psi_{\text{init}}\rangle\langle\psi_{\text{init}}|P(x)^\dagger)$ is satisfied. Note that $\mathrm{tr}_{\mathcal{V}_{\overline{S}}\otimes\mathcal{M}\otimes\mathcal{P}}(P(x)|\psi_{\text{init}}\rangle\langle\psi_{\text{init}}|P(x)^\dagger) = I/2^{q_S(n)}$. Furthermore, for the state $P(x)|\psi_{\text{init}}\rangle\langle\psi_{\text{init}}|P(x)^\dagger$, the verification procedure of V accepts x with certainty. Hence the circuit Q_x constructed above outputs $I/2^{q_S(n)}$ with certainty.

Now suppose that x is in A_{no}. We claim that the output ρ of Q_x satisfies $\|\rho - I/2^{q_S(n)}\|_{\text{tr}} > c$ for some constant $0 < c < 1$.

First we assume that σ_x is of the form $\sigma'_x \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right|$.

From the soundness property of the original proof system, the verification procedure of V results in acceptance with probability smaller than 2^{-n}, for any mixed state $\xi \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right|$ in $\mathbf{D}(\mathcal{M}\otimes\mathcal{V})$ satisfying $\mathrm{tr}_{\mathcal{M}\otimes\mathcal{V}_{\overline{S}}}(\xi \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right|) = I/2^{q_S(n)}$.

Therefore, if $\left\|\mathrm{tr}_{\mathcal{M}\otimes\mathcal{V}_{\overline{S}}}\left(\sigma'_x \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right|\right) - I/2^{q_S(n)}\right\|_{\text{tr}} < 2/3$, we have $\left\|\sigma'_x \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right| - \xi \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right|\right\|_{\text{tr}} < 2/3$ for some mixed state $\xi \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right|$ in $\mathbf{D}(\mathcal{M}\otimes\mathcal{V})$ satisfying $\mathrm{tr}_{\mathcal{M}\otimes\mathcal{V}_{\overline{S}}}\left(\xi \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right|\right) = I/2^{q_S(n)}$. It follows that the step 3.2 results in rejection and outputs $|0^{q_S(n)}\rangle\langle 0^{q_S(n)}|$ with probability greater than $1/3 - 2^{-n}$. Since $q_{\mathcal{S}}(n) \geq n$, this implies that Q_x outputs the mixed state ρ satisfying $\|\rho - I/2^{q_S(n)}\|_{\text{tr}} > 1/6 - 3 \cdot 2^{-(n+1)}$.

On the other hand, if $\left\|\mathrm{tr}_{\mathcal{M}\otimes\mathcal{V}_{\overline{S}}}\left(\sigma'_x \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right|\right) - I/2^{q_S(n)}\right\|_{\text{tr}} \geq 2/3$, that is, if $\|\mathrm{tr}_{\mathcal{M}}\sigma'_x - I/2^{q_S(n)}\|_{\text{tr}} \geq 2/3$, from Theorem 5, Q_x outputs the mixed state ρ satisfying $\|\rho - I/2^{q_S(n)}\|_{\text{tr}} \geq 1/6$, since the step 3.1 outputs $\mathrm{tr}_{\mathcal{M}}\sigma'_x$.

Putting things together, the circuit Q_x outputs the mixed state ρ satisfying $\|\rho - I/2^{q_S(n)}\|_{\text{tr}} > 1/7$ (for $n \geq 6$), if σ_x is of the form $\sigma'_x \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right|$.

To deal with general σ_x, notice that the step 2 outputs the state farthest away from $I/2^{q_S(n)}$ with some probability p, or otherwise reduces σ_x to the state of the form $\sigma'_x \otimes \left|0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right\rangle\left\langle 0^{q_{\mathcal{V}_{\overline{S}}}(n)}\right|$. For the latter case, the step 3 outputs the mixed state ρ' satisfying $\|\rho' - I/2^{q_S(n)}\|_{\text{tr}} > 1/7$ (for $n \geq 6$) from the argument above. Thus, if x is in A_{no}, from Theorem 5, the circuit Q_x outputs the mixed state ρ satisfying $\|\rho - I/2^{q_S(n)}\|_{\text{tr}} > \max\{1/7 - p, p - 2^{-n}\} > 1/15$ (for $n \geq 8$).

Now, constructing r copies of Q_x for appropriately chosen r to have a circuit $Q_x^{\otimes r}$ reduces A to the $(0,\beta)$-QSCMM problem for arbitrary $0 < \beta < 1$. □

Thus we have the following theorem.

Theorem 7. *$(0,\beta)$-QSCMM is complete for* NIQPZK$(1, 1/2)$ *for* $0 < \beta < 1$.

4 Graph Non-automorphism is in NIQPZK(1, 1/2)

The *Graph Non-Automorphism (GNA)* problem is a variant of the *graph non-isomorphism (GNI)* problem, and is not known in BQP nor in NP.

Graph Non-Automorphism (GNA)

Input: A description of a graph G of n vertices.

Output: Accept if $\pi(G) \neq G$ for all non-trivial permutations π over n vertices and reject otherwise.

It is easy to show that any instance of GNA is reduced to an instance of $(0, \beta)$-QSCMM, and thus we have the following corollary.

Corollary 8. *GNA has a non-interactive quantum perfect zero-knowledge proof system of perfect completeness.*

Proof. We assume an appropriate ordering of permutations over n vertices so that each permutation can be represented with $q_{\mathcal{P}}(n) = \lceil \log n! \rceil$ qubits. Let π_i be the ith permutation according to this ordering for $0 \leq i \leq n! - 1$.

Let $\mathcal{P}$ be a Hilbert space consisting of $q_{\mathcal{P}}(n)$ qubits and $\mathcal{G}$ be a Hilbert space consisting of $q_{\mathcal{G}}(n) = O(n^2)$ qubits. Given a graph G of n vertices, consider the following quantum circuit Q_G behaving as follows.

1. Prepare the following quantum state in $\mathcal{P} \otimes \mathcal{G}$:

$$\frac{1}{\sqrt{2^{q_{\mathcal{P}}(n)}}} \sum_{i=0}^{n!-1} |i\rangle|0, \pi_i(G)\rangle + \frac{1}{\sqrt{2^{q_{\mathcal{P}}(n)}}} \sum_{i=n!}^{2^{q_{\mathcal{P}}(n)}-1} |i\rangle|1, i\rangle.$$

2. Output the qubits in $\mathcal{P}$.

If a given graph G has no non-trivial automorphism groups, every $\pi_i(G)$ is different from each other, and thus the output of Q_G is the mixed state $I/2^{q_{\mathcal{P}}(n)}$.

On the other hand, if a given graph G has a non-trivial automorphism group, the contents of qubits in $\mathcal{G}$ have at most $2^{q_{\mathcal{P}}(n)} - n!/2 < 3/4 \cdot 2^{q_{\mathcal{P}}(n)}$ variations, and the trace norm between $I/2^{q_{\mathcal{P}}(n)}$ and the output of Q_G is at least $1/4$.

Thus the constructed Q_G is an instance of $(0, 1/4)$-QSCMM. □

5 Conjectures

We conjecture the following.

Conjecture 9. There is a (deterministic) polynomial-time procedure that, on an input $\langle Q, 1^n \rangle$ where Q is a description of a quantum circuit specifying a mixed state ρ of q_1 qubits, outputs a description of a quantum circuit R (having size

polynomial in n and the size of Q) specifying a mixed state ξ of q_2 qubits such that (for α and β satisfying an appropriate condition)

$$\|\rho - I/2^{q_1}\|_{\mathrm{tr}} < \alpha \Rightarrow \|\xi - I/2^{q_2}\|_{\mathrm{tr}} < 2^{-n},$$
$$\|\rho - I/2^{q_1}\|_{\mathrm{tr}} > \beta \Rightarrow \|\xi - I/2^{q_2}\|_{\mathrm{tr}} > 1 - 2^{-n}.$$

Classically, Goldreich, Sahai, and Vadhan [9] implicitly proved a similar property to Conjecture 9. One of the troublesome points in applying a direct modification of their proof to our case is that the joint von Neumann entropy $S(A, B)$ for a composite system with two components A and B can be smaller than $S(A)$ and $S(B)$ (recall that classically the joint Shannon entropy $H(X, Y)$ is never smaller than $H(X)$ and $H(Y)$). Therefore, the classical technique of just discarding some part to reduce the entropy of output distribution no longer works well in the quantum case.

Under the assumption that Conjecture 9 holds, it is easy to modify the proofs of Lemma 4 and Lemma 6 to the statistical zero-knowledge case. Thus the following conjecture is provable if Conjecture 9 holds.

Conjecture 10. (α, β)-QSCMM is complete for NIQSZK for any α and β satisfying an appropriate condition.

References

1. M. Blum, A. De Santis, S. Micali, and G. Persiano. Non-interactive zero-knowledge. *SIAM Journal on Computing*, 20(6):1084–1118, 1991.
2. M. Blum, P. Feldman, and S. Mical. Non-interactive zero-knowledge and its applications (extended abstract). In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 103–112, 1988.
3. A. De Santis, G. Di Crescenzo, G. Persiano, and M. Yung. Image density is complete for non-interactive-SZK (extended abstract). In *Automata, Languages and Programming, 25th International Colloquium, ICALP '98*, volume 1443 of *Lecture Notes in Computer Science*, pages 784–795, 1998.
4. A. De Santis, S. Micali, and G. Persiano. Non-interactive zero-knowledge proof systems. In *Advances in Cryptology – CRYPTO '87, A Conference on the Theory and Applications of Cryptographic Techniques*, volume 293 of *Lecture Notes in Computer Science*, pages 52–72, 1987.
5. A. De Santis, S. Micali, and G. Persiano. Non-interactive zero-knowledge with preprocessing. In *Advances in Cryptology – CRYPTO '88, 8th Annual International Cryptology Conference*, volume 403 of *Lecture Notes in Computer Science*, pages 269–282, 1988.
6. S. Even, A. L. Selman, and Y. Yacobi. The complexity of promise problems with applications to public-key cryptography. *Information and Control*, 61(2):159–173, 1984.
7. O. Goldreich and Y. Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1):1–32, 1994.
8. O. Goldreich, A. Sahai, and S. P. Vadhan. Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 399–408, 1998.

9. O. Goldreich, A. Sahai, and S. P. Vadhan. Can statistical zero knowledge be made non-interactive? or on the relationship of SZK and NISZK. In *Advances in Cryptology – CRYPTO '99, 19th Annual International Cryptology Conference*, volume 1666 of *Lecture Notes in Computer Science*, pages 467–484, 1999.
10. S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.
11. J. van de Graaf. *Towards a formal definition of security for quantum protocols*. PhD thesis, Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, December 1997.
12. J. D. Gruska. *Quantum Computing*. McGraw-Hill, 1999.
13. L. P. Hughston, R. O. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183:14–18, 1993.
14. J. Kilian and E. Petrank. An efficient noninteractive zero-knowledge proof system for NP with general assumptions. *Journal of Cryptology*, 11(1):1–27, 1998.
15. A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.
16. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
17. A. Sahai and S. P. Vadhan. A complete problem for statistical zero knowledge. *Journal of the ACM*, 50(2):196–249, 2003.
18. A. Uhlmann. Parallel transport and "quantum holonomy" along density operators. *Reports on Mathematical Physics*, 24:229–240, 1986.
19. S. P. Vadhan. *A Study of Statistical Zero-Knowledge Proofs*. PhD thesis, Department of Mathematics, Massachusetts Institute of Technology, August 1999.
20. J. H. Watrous. Succinct quantum proofs for properties of finite groups. In *41st Annual Symposium on Foundations of Computer Science*, pages 537–546, 2000.
21. J. H. Watrous. Limits on the power of quantum statistical zero-knowledge. In *43rd Annual Symposium on Foundations of Computer Science*, pages 459–468, 2002.