Non-Interactive Quantum Statistical and Perfect 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

27 July 2002

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 class of languages having one-sided bounded error non-interactive quantum perfect zero-knowledge proof systems has a natural complete problem. Non-triviality of such a proof system is based on the fact proved in this paper that the Graph Non-Automorphism problem, which is not known in BQP, can be reduced to our complete problem. Our results may be the first non-trivial quantum zero-knowledge proofs secure even against dishonest quantum verifiers, since our protocols are non-interactive, and thus the zero-knowledge property does not depend on whether the verifier in the protocol is honest or not. A restricted version of our complete problem derives a natural complete problem for BQP.

1 Introduction

Zero-knowledge proof systems were introduced by Goldwasser, Micali, and Rackoff [12] 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, 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 only considers the case with an *honest verifier*. The reason why he only considers the case with an honest verifier 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 cheating verifiers by extending classical definitions of zero-knowledge in the most straightforward ways. See [13] 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 restricted 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.

Classical version of non-interactive zero-knowledge proof systems was introduced by Blum, Feldman, and Micali [3], and was later studied by a number of works [5, 6, 2, 9, 16, 4, 11, 20]. Such non-interactive proof systems put an assumption that a verifier and a prover share some random string, and it is known that sharing randomness is necessary for non-trivial protocols (i.e. protocols for languages beyond BPP) of non-interactive quantum zero-knowledge proofs [9]. As for non-interactive statistical zero-knowledge proof systems, De Santis, Di Crescenzo, Persiano, and Yung showed an existence of a complete promise problem for the class NISZK of languages having non-interactive statistical zero-knowledge proof systems. Goldreich, Sahai, and Vadhan [11] showed another two complete promise problems for NISZK, namely 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]. First, similar to the classical cases, it is shown that sharing randomness or entanglement is necessary for non-trivial protocols (i.e. protocols for languages beyond BQP) of non-interactive quantum perfect and statistical zero-knowledge. Next, it is shown that, with sharing EPR pairs a priori, the class of languages having one-sided bounded error non-interactive quantum perfect zero-knowledge proof systems has a natural complete promise problem, which we call the *Quantum State Closeness to Identity (QSCI)* problem, informally described as follows: given a description of a quantum circuit Q, is the output qubits of Q is maximally entangled to the non-output part or is it far from that? Note that our QSCI problem may be viewed as a quantum variant of the SDU problem, which is shown NISZK-complete by Goldreich, Sahai, and Vadhan [11]. However, our proof for the completeness of the QSCI problem is quite different from their proof for the classical case at least in the following two senses: (i) the completeness of the QSCI problem is shown in a direct manner, while that of the classical SDU problem was shown by using other complete problems such as the EA problem, and (ii) our proof for the completeness result 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) has a non-interactive quantum perfect zero-knowledge proof system of perfect completeness. Since the GNA problem is not know in BQP, this gives an evidence of non-triviality of our proof systems. One of the merits of considering non-interactive models is that the zero-knowledge property in non-interactive 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. It is also shown that a restricted version of our complete problem derives a natural complete problem for BQP.

The remainder of this paper is organized as follows. In Section 2 we give formal definitions of non-interactive quantum statistical and perfect zero-knowledge proof systems, and introduce the Quantum State Closeness to Identity problem. In Section 3 we show the necessity of sharing randomness or entanglement for non-trivial protocols of non-interactive quantum zero-knowledge. In Section 4 we show our main result of completeness and its applications. Finally, we conclude with Section 5, which mentions our conjectures on non-interactive quantum zero-knowledge proofs. Familiarity with the basics of quantum computation and information theory as well as classical zero-knowledge proof systems is assumed throughout this paper. See [14, 17] for the basics of quantum computation and information theory and [7, 8] for those of classical zero-knowledge proof systems.

2 Definitions

2.1 Quantum Circuits and Polynomial-Time Preparable Sets of Quantum States

A family $\{Q_x\}$ of quantum circuits is said to be *polynomial-time uniformly generated* if there exists a classical deterministic procedure that, on each input x, outputs a description of Q_x and runs in time polynomial in $n = |x|$. For simplicity, we assume that all input strings are over the alphabet

$\Sigma = \{0,1\}$. It is assumed that the quantum circuits in such a family are composed of gates in some reasonable, universal, finite set of quantum gates such as the Shor basis. Furthermore, it is assumed that the number of gates in any circuit is not more than the length of the description of that circuit, therefore Q_x must have size polynomial in n. For convenience, in the subsequent sections, we often identify a circuit Q_x with the unitary operator it induces.

It should be mentioned that to permit non-unitary quantum circuits, in particular, to permit measurements at any timing in the computation does not change the computational power of the model of quantum circuits in view of time complexity. See [1] for a detailed description of the equivalence of the unitary and non-unitary quantum circuit models.

Given a collection $\{\rho_x\}$ of mixed states, let us say that the collection 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 the above description, 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*.

2.2 Non-Interactive Quantum Statistical Zero-Knowledge with Shared EPR-Pairs

Here we give a definition of non-interactive quantum statistical (and perfect) zero-knowledge proof systems in which the verifier and the prover share EPR-pairs prior to the protocol.

Similar to quantum statistical zero-knowledge proof systems [21], we define non-interactive quantum statistical zero-knowledge proof systems in terms of quantum circuits.

For each input $x \in \Sigma^*$ of length $n = |x|$, the entire system of a non-interactive quantum statistical zero-knowledge proof 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 shares 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 $V\colon \Sigma^* \to \Sigma^*$, where $\Sigma = \{0,1\}$ is the alphabet set. 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 each input $x \in \Sigma^*$ of length $n = |x|$, $V(x)$ 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 the verifier 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 each input $x \in \Sigma^*$, $|x| = n$, $P(x)$ 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., each $P(x)$ 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. We say that 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 input 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 $|0\rangle$-states.

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 the (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 $|\psi_{\text{init}}\rangle$.

In what follows, the circuits $P(x)$ and $V(x)$ of prover and verifier may be simply denoted by P and V, respectively, if it is not confusing. We also use the notation $\mathbf{D}(\mathcal{H})$ for the set of mixed states in $\mathcal{H}$.

First we define the class NIQSZK$(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}}, q_{\mathcal{S}}, a, b)$ of languages having $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted $q_{\mathcal{S}}$-shared-EPR-pairs non-interactive quantum statistical zero-knowledge proof systems with error probabilities a and b in completeness and soundness sides, respectively.

Definition 1 *Given polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{S}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and a function $q_{\mathcal{P}} \colon \mathbb{Z}^+ \to \mathbb{N}$, and functions $a, b \colon \mathbb{Z}^+ \to [0, 1]$, let* NIQSZK$(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}}, q_{\mathcal{S}}, a, b)$ *denote the class of languages L for which there exists 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 exists a $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum prover P such that (P, V) accepts x with probability at least $a(n)$,

(ii) Soundness:
if $x \notin L$, for any $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum prover P', (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 $x \in L$,

$$\|\sigma_x - \mathrm{tr}_{\mathcal{P}}(P|\psi_{\text{init}}\rangle\langle\psi_{\text{init}}|P^\dagger)\|_{\text{tr}} \leq \delta(n)$$

for an honest prover P and some negligible function δ (i.e., $\delta(n) < 1/p(n)$ for sufficiently large n for all polynomials p).

We say that a language L is in NIQSZK(a, b) in short if there exist some polynomially bounded functions $q_{\mathcal{V}}$, $q_{\mathcal{M}}$, and $q_{\mathcal{S}}$ such that L is in NIQSZK$(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}}, q_{\mathcal{S}}, a, b)$ for any function $q_{\mathcal{P}}$.

Similarly, we define the class NIQPZK$(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}}, q_{\mathcal{S}}, a, b)$ of languages having $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted $q_{\mathcal{S}}$-shared-EPR-pairs non-interactive quantum perfect zero-knowledge proof systems with error probabilities a and b in completeness and soundness sides, respectively.

Definition 2 *Given polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{S}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and a function $q_{\mathcal{P}} \colon \mathbb{Z}^+ \to \mathbb{N}$, and functions $a, b \colon \mathbb{Z}^+ \to [0, 1]$, let* NIQPZK$(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}}, q_{\mathcal{S}}, a, b)$ *denote the class of languages L for which there exists 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 exists a $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum prover P such that (P, V) accepts x with probability at least $a(n)$,

(ii) Soundness:
if $x \notin L$, for any $(q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted quantum prover P', (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 $x \in L$, σ_x exactly coincides with $\mathrm{tr}_{\mathcal{P}}(P|\psi_{\text{init}}\rangle\langle\psi_{\text{init}}|P^\dagger)$.

As is the statistical zero-knowledge case, we say that a language L is in NIQPZK(a, b) in short if there exist some polynomially bounded functions $q_{\mathcal{V}}$, $q_{\mathcal{M}}$, and $q_{\mathcal{S}}$ such that L is in NIQPZK$(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}}, q_{\mathcal{S}}, a, b)$ for any function $q_{\mathcal{P}}$.

Note that, similar to the QMA case, parallel repetition of non-interactive quantum statistical (or perfect) zero-knowledge proof systems can reduce completeness and soundness errors to be exponentially small while preserving the zero-knowledge property.

2.3 Variants of Quantum State Distinguishability Problem

This paper focuses on the following promise problems, all of which are parameterized by constants α and β satisfying $0 \leq \alpha < \beta \leq 1$.

First we review the (α, β)-Quantum State Distinguishability ((α, β)-QSD) problem, which was introduced and shown to be HVQSZK-complete (for any $0 \leq \alpha < \beta^2 \leq 1$) by Watrous [21]. Note that this problem can be regarded as a quantum analogue of the Statistical Difference problem [18], which is HVSZK-complete (and thus SZK-complete from the result HVSZK = SZK [10] shown later).

(α, β)-Quantum State Distinguishability ((α, β)-QSD)

Input: Descriptions of quantum circuits Q_0 and Q_1, each 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: Letting $\rho_i = \text{tr}_{\mathcal{H}_{\overline{\text{out}}}}(Q_i|0^{q_{\text{in}}}\rangle\langle 0^{q_{\text{in}}}|Q_i^\dagger)$ for $i = 0, 1$, we have either one of the following two:

(a) $\|\rho_0 - \rho_1\|_{\text{tr}} \leq \alpha$,

(b) $\|\rho_0 - \rho_1\|_{\text{tr}} \geq \beta$.

Output: Accept if $\|\rho_0 - \rho_1\|_{\text{tr}} \geq \beta$, and reject if $\|\rho_0 - \rho_1\|_{\text{tr}} \leq \alpha$.

Note that the complement of (α, β)-QSD, which we call (α, β)-*Quantum State Closeness (*(α, β)-*QSC)* problem, is also HVQSZK-complete, as shown by Watrous [21].

Next we introduce (α, β)-*Quantum State Closeness to Identity (*(α, β)-*QSCI)* problem, which is a restricted version of the (α, β)-QSC problem. Later $(0, \beta)$-QSCI problem will be shown to be NIQPZK$(1, b)$-complete for any $0 < \beta < 1$ and any bounded error probability b. Note that this problem can be regarded as a quantum analogue of the Statistical Difference from Uniform Distribution (SDU) problem [11], which is NISZK-complete.

(α, β)-Quantum State Closeness to Identity ((α, β)-QSCI)

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: Letting $\rho = \text{tr}_{\mathcal{H}_{\overline{\text{out}}}}(Q|0^{q_{\text{in}}}\rangle\langle 0^{q_{\text{in}}}|Q^\dagger)$, we have either one of the following two:

(a) $\|\rho - I/2^{q_{\text{out}}}\|_{\text{tr}} \leq \alpha$,

(b) $\|\rho - I/2^{q_{\text{out}}}\|_{\text{tr}} \geq \beta$.

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

Putting restrictions on the number of output qubits of the quantum circuits given as input yields the following two promise problems, both of which will be shown to be BQP-complete.

(α, β)-One Qubit Quantum State Distinguishability ((α, β)-1QSD)

Input: Descriptions of quantum circuits Q_0 and Q_1, each acting over the Hilbert space $\mathcal{H}_{\rm in} = \mathcal{H}_{\rm out} \otimes \mathcal{H}_{\overline{\rm out}}$, where $\mathcal{H}_{\rm in}$ consists of $q_{\rm in}$ qubits and $\mathcal{H}_{\rm out}$ consists of a single qubit.

Promise: Letting $\rho_i = {\rm tr}_{\mathcal{H}_{\overline{\rm out}}}(Q_i|0^{q_{\rm in}}\rangle\langle 0^{q_{\rm in}}|Q_i^\dagger)$ for $i = 0, 1$, we have either one of the following two:

(a) $\|\rho_0 - \rho_1\|_{\rm tr} \leq \alpha$,

(b) $\|\rho_0 - \rho_1\|_{\rm tr} \geq \beta$.

Output: Accept if $\|\rho_0 - \rho_1\|_{\rm tr} \geq \beta$, and reject if $\|\rho_0 - \rho_1\|_{\rm tr} \leq \alpha$.

(α, β)-One Qubit Quantum State Closeness to Identity ((α, β)-1QSCI)

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

Promise: Letting $\rho = {\rm tr}_{\mathcal{H}_{\overline{\rm out}}}(Q|0^{q_{\rm in}}\rangle\langle 0^{q_{\rm in}}|Q^\dagger)$, we have either one of the following two:

(a) $\|\rho - I/2\|_{\rm tr} \leq \alpha$,

(b) $\|\rho - I/2\|_{\rm tr} \geq \beta$.

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

3 Necessity of Shared Randomness or Shared Entanglement

First, similar to the classical cases [9], it is shown that sharing randomness or entanglement is necessary for non-trivial protocols of non-interactive quantum perfect and statistical zero-knowledge.

Theorem 3 *Without shared randomness nor shared entanglement, any language having non-interactive quantum perfect or statistical zero-knowledge proofs is necessarily in* BQP.

Proof. It is sufficient to show that, without shared randomness nor shared entanglement, NIQSZK$(3/4, 1/4)$ is in BQP.

Let L be a language having an NIQSZK$(3/4, 1/4)$ protocol without shared randomness nor shared entanglement. Let V be the corresponding honest quantum verifier and $\{\sigma_x\}$ be the corresponding polynomial-time preparable set of mixed states. For every input x, consider the following polynomial-time quantum algorithm:

1. Prepare σ_x in a quantum register $\mathbf{R}$.
2. Apply $V(x)$ to $\mathbf{R}$ to have a state $V(x)\sigma_x V(x)^\dagger$.
3. Accept iff the contents of $\mathbf{R}$ correspond to ones that make the original verifier V accept.

(i) In the case x is in L:
From the zero-knowledge property of the original protocol, the difference between σ_x and the state received from the honest prover is negligible. Thus, the input x is accepted by the algorithm above with probability more than $2/3$.

(ii) In the case x is not in L:
From the soundness property of the original protocol, whatever state the honest verifier V receives from the prover, V accepts the input x with probability at most 1/4. In particular, if the honest verifier V receives σ_x from the prover, V accepts the input x with probability at most 1/4. Thus, the input x is accepted by the algorithm above with probability at most 1/4 (less than 1/3).

□

4 Completeness Results and their Applications

4.1 NIQPZK(1, 1/2)-Completeness of $(0, \beta)$-QSCI

Here we show that the $(0, \beta)$-QSCI problem is NIQPZK(1, 1/2)-complete, that is, complete for the class of languages having non-interactive quantum perfect zero-knowledge proof systems of perfect completeness. While our result is closely related to the classical result by Goldreich, Sahai, and Vadhan [11], the proofs adopted in this paper are rather quantum information theoretical.

The proof of Lemma 5 below uses the following well-known property in quantum information theory.

Theorem 4 ([19, 15]) *Let $|\phi\rangle, |\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ satisfy $\mathrm{tr}_{\mathcal{H}_2}|\phi\rangle\langle\phi| = \mathrm{tr}_{\mathcal{H}_2}|\psi\rangle\langle\psi|$. Then there is a unitary transformation U over $\mathcal{H}_2$ such that $(I_{\mathcal{H}_1} \otimes U)|\phi\rangle = |\psi\rangle$, where $I_{\mathcal{H}_1}$ is the identity operator over $\mathcal{H}_1$.*

Lemma 5 *$(0, \beta)$-QSCI is in* NIQPZK(1, 1/2) *for any $0 < \beta < 1$.*

Proof. Let Q be a quantum circuit of the $(0, \beta)$-QSCI, 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 and ξ is either $I/2^{q'_{\mathrm{out}}}$ or the one such that $\|\xi - I/2^{q_{\mathrm{out}}}\|_{\mathrm{tr}}$ is arbitrary close to 1, say $\|\xi - I/2^{q_{\mathrm{out}}}\|_{\mathrm{tr}} > 1 - 2^{-n}$.

We construct a $(q'_{\mathrm{out}}, q' - q'_{\mathrm{out}}, q_{\mathcal{P}})$-restricted non-interactive quantum perfect zero-knowledge proof system of q'_{out}-shared-EPR-pairs. Consider the $(q'_{\mathrm{out}}, q' - q'_{\mathrm{out}})$-restricted quantum verifier V. Let the quantum registers $\mathbf{M}$ and $\mathbf{S}$ consist of the message qubits and qubits in the verifier part of the shared EPR pairs, respectively. The verification procedure of the verifier 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 $0^{q'}$, otherwise reject.

For the completeness, suppose that $\xi = I/2^{q'_{\mathrm{out}}}$. 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 4, there exists a unitary transformation P over $\mathcal{M} \otimes \mathcal{P}$ such that

$$(I \otimes P)|\psi_{\mathrm{init}}\rangle = |\phi\rangle.$$

Therefore,

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

Thus V accepts the input with certainty.

For the soundness, suppose that $\|\xi - I/2^{q'_{\rm out}}\|_{\rm tr} > 1 - 2^{-n}$. Then, for any unitary transformation P' over $\mathcal{M} \otimes \mathcal{P}$, letting $|\psi\rangle = (I \otimes P')|\psi_{\rm init}\rangle$, we have

$$\|{\rm tr}_{\mathcal{P}}|\phi\rangle\langle\phi| - {\rm tr}_{\mathcal{P}}|\psi\rangle\langle\psi|\|_{\rm tr} > 1 - 2^{-n},$$

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

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

Thus the probability that V accepts the input is negligible.

Finally, the zero-knowledge property is obvious, because $R|0^{q'}\rangle\langle 0^{q'}|R^{\dagger} = {\rm tr}_{\mathcal{P}}((I\otimes P)|\psi_{\rm init}\rangle\langle\psi_{\rm init}|(I\otimes P^{\dagger}))$ is polynomial-time preparable. □

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

Proof. Let L be in NIQPZK$(1, 1/2)$. Then from the fact that parallel repetition works well for non-interactive quantum perfect zero-knowledge proof systems, for any function $q_{\mathcal{P}}\colon \mathbb{Z}^+ \to \mathbb{N}$, L has a $(q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{P}})$-restricted $q_{\mathcal{S}}$-shared-EPR-pairs non-interactive quantum perfect zero-knowledge proof system of perfect completeness for some polynomially bounded functions $q_{\mathcal{V}}, q_{\mathcal{M}}, q_{\mathcal{S}}\colon \mathbb{Z}^+ \to \mathbb{N}$, whose soundness error is smaller than 2^{-n} for inputs of length n.

Let V and P be the honest verifier and the honest prover of this proof system, and let $V(x)$ and $P(x)$ be the unitary transformations of V and 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 L,

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

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 input x of length n, the first $q_{\mathcal{M}}(n)$ qubits of σ_x correspond to the message qubits of the original proof system, the last $q_{\mathcal{V}}(n) - q_{\mathcal{S}}(n)$ 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.

Let $\mathbf{M}$, $\mathbf{S}$, and $\mathbf{V}$ be quantum registers, each of which consists of $q_{\mathcal{M}}(n)$ qubits, $q_{\mathcal{S}}(n)$ qubits, and $q_{\mathcal{V}}(n) - q_{\mathcal{S}}(n)$ qubits respectively. For every input 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 $|0^{q_{\mathcal{S}}(n)}\rangle\langle 0^{q_{\mathcal{S}}(n)}|$.
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 $I/2^{q_{\mathcal{S}}(n)}$ if the last qubit in $\mathbf{V}$ contains 1, otherwise, output $|0^{q_{\mathcal{S}}(n)}\rangle\langle 0^{q_{\mathcal{S}}(n)}|$.

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

Now suppose that x is not in L. We claim that the output mixed state ρ of Q_x satisfies $\|\rho - I/2^{q_{\mathcal{S}}(n)}\|_{\rm tr} > c$ for some positive constant $c \leq 1$. Without loss of generality, we assume that σ_x is of

the form $\sigma'_x \otimes |0^{q_{\mathcal{V}}(n)}\rangle\langle 0^{q_{\mathcal{V}}(n)}|$, since the step 2 reduces σ_x to the state of this form or outputs the state farthest away from $I/2^{q_{\mathcal{S}}(n)}$.

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

Therefore, if $\|\mathrm{tr}_{\mathcal{M}\otimes\mathcal{V}_{\overline{\mathcal{S}}}}(\sigma'_x \otimes |0^{q_{\mathcal{V}}(n)}\rangle\langle 0^{q_{\mathcal{V}}(n)}|) - I/2^{q_{\mathcal{S}}(n)}\|_{\mathrm{tr}} \geq 1/2$, then

$$\|\mathrm{tr}_{\mathcal{M}}(\sigma'_x \otimes |0^{q_{\mathcal{V}}(n)}\rangle\langle 0^{q_{\mathcal{V}}(n)}|) - I/2^{q_{\mathcal{S}}(n)} \otimes |0^{q_{\mathcal{V}}(n)}\rangle\langle 0^{q_{\mathcal{V}}(n)}|\|_{\mathrm{tr}} \geq 1/2,$$

and thus

$$\|\mathrm{tr}_{\mathcal{M}}\sigma'_x - I/2^{q_{\mathcal{S}}(n)}\|_{\mathrm{tr}} \geq 1/2.$$

Hence the step 3.1 outputs the mixed state ρ satisfying $\|\rho - I/2^{q_{\mathcal{S}}(n)}\|_{\mathrm{tr}} \geq 1/2$.

On the other hand, if $\|\mathrm{tr}_{\mathcal{M}\otimes\mathcal{V}_{\overline{\mathcal{S}}}}(\sigma'_x \otimes |0^{q_{\mathcal{V}}(n)}\rangle\langle 0^{q_{\mathcal{V}}(n)}|) - I/2^{q_{\mathcal{S}}(n)}\|_{\mathrm{tr}} \leq 1/2$, we have

$$\|\sigma'_x \otimes |0^{q_{\mathcal{V}}(n)}\rangle\langle 0^{q_{\mathcal{V}}(n)}| - \xi \otimes |0^{q_{\mathcal{V}}(n)}\rangle\langle 0^{q_{\mathcal{V}}(n)}|\|_{\mathrm{tr}} \leq 1/2$$

for some mixed state $\xi \otimes |0^{q_{\mathcal{V}}(n)}\rangle\langle 0^{q_{\mathcal{V}}(n)}|$ in $\mathbf{D}(\mathcal{M}\otimes\mathcal{V})$ satisfying $\mathrm{tr}_{\mathcal{M}\otimes\mathcal{V}_{\overline{\mathcal{S}}}}(\xi \otimes |0^{q_{\mathcal{V}}(n)}\rangle\langle 0^{q_{\mathcal{V}}(n)}|) = I/2^{q_{\mathcal{S}}(n)}$. Therefore, the step 3.2 results in rejection with probability at least $1/2 - 2^{-(n+1)}$, and thus the circuit Q_x outputs $|0^{q_{\mathcal{V}}(n)}\rangle\langle 0^{q_{\mathcal{V}}(n)}|$ with probability at least $1/2 - 2^{-(n+1)}$.

Putting things together, in the case x is not in L, the circuit Q_x outputs the mixed state ρ satisfying $\|\rho - I/2^{q_{\mathcal{S}}(n)}\|_{\mathrm{tr}} > c$ for some constant c greater than, say $1/5$.

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

Thus we have the following theorem.

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

4.2 NIQPZK(1, 1/2)-Protocol for Graph Non-Automorphism

The *Graph Non-Automorphism (GNA)* problem defined below is a special case 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 $(0,\beta)$-QSCI, 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 $q_{\mathcal{L}}(n) = \lceil \log n! \rceil = O(n \log n)$ qubits. Let π_i be the i-th permutation according to this ordering for $0 \leq i \leq n! - 1$.

Let $\mathcal{P}$ be a Hilbert space consisting of $q_{\mathcal{L}}(n)$ qubits and $\mathcal{G}$ be a Hilbert space consisting of $q_{\mathcal{G}}(n) = O(n^2)$ qubits (intuitively, $\mathcal{P}$ is for a representation of a permutation and $\mathcal{G}$ is for a representation of a graph).

Given a graph G of n vertices, consider the following quantum circuit Q_G behaving as follows.

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

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

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 $I/2^{q_{\mathcal{L}}(n)}$.

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

Thus the constructed quantum circuit Q_G is an instance of $(0, 1/4)$-QSDI, which completes the proof. □

4.3 BQP-Completeness Results

Theorem 9 *(α, β)-1QSCI and (α, β)-1QSD are complete for* BQP *for $0 < \alpha < \beta < 1$.*

Proof. Straightforward and thus omitted. □

5 Conjectures

Conjecture 1 *There is a (deterministic) polynomial-time procedure that, on an input $(Q, 1^n)$ where Q is a description of a quantum circuit specifying a mixed state ρ of q_1 qubits, outputs a description of a quantum circuits R (having size polynomial in n and in the size of Q) specifying a mixed state ξ of q_2 qubits satisfying the following (for α and β satisfying an appropriate condition such as $0 < \alpha < 1/q_1 < 1 - 1/q_1 < \beta < 1$).*

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

Under the assumption that Conjecture 1 holds, the following two conjectures can be shown in similar manners as the proofs of Lemma 5 and Lemma 6.

Conjecture 2 *(α, β)-QSCI is in* NIQSZK *for any α and β satisfying an appropriate condition such as $0 < \alpha < 1/q_1 < 1 - 1/q_1 < \beta < 1$, where q_1 is the number of output qubits of the quantum circuit given as an instance of (α, β)-QSCI.*

Conjecture 3 *For any promise problem $L \in$ NIQSZK, there is a polynomial-time deterministic procedure that reduces L to the (α, β)-QSCI problem for any α and β satisfying an appropriate condition such as $0 < \alpha < 1/q_1 < 1 - 1/q_1 < \beta < 1$, where q_1 is the number of output qubits of the quantum circuit given as an instance of (α, β)-QSCI.*

Thus, under the assumption that Conjecture 1 holds, the following conjecture is provable.

Conjecture 4 *(α, β)-QSCI is complete for* NIQSZK *for any α and β satisfying an appropriate condition such as $0 < \alpha < 1/q_1 < 1 - 1/q_1 < \beta < 1$, where q_1 is the number of output qubits of the quantum circuit given as an instance of (α, β)-QSCI.*

References

[1] Dorit Aharonov, Alexei Yu. Kitaev, and Noam Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998.

[2] Manuel Blum, Alfredo De Santis, Silvio Micali, and Giuseppe Persiano. Non-interactive zero-knowledge. *SIAM Journal on Computing*, 20(6):1084–1118, 1991.

[3] Manuel Blum, Paul Feldman, and Silvio 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.

[4] Alfredo De Santis, Giovanni Di Crescenzo, Giuseppe Persiano, and Moti Yung. Image density is complete for non-interactive-SZK (extended abstract). In *Proceedings of the 25th International Colloquium on Automata, Languages and Programming*, volume 1443 of *Lecture Notes in Computer Science*, pages 784–795, 1998.

[5] Alfredo De Santis, Silvio Micali, and Giuseppe 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.

[6] Alfredo De Santis, Silvio Micali, and Giuseppe 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.

[7] Oded Goldreich. *Modern Cryptography, Probabilistic Proofs and Pseudo-randomness*. Springer, 1999.

[8] Oded Goldreich. *Foundations of Cryptography – Basic Tools*. Cambridge, 2001.

[9] Oded Goldreich and Yair Oren. Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1):1–32, 1994.

[10] Oded Goldreich, Amit Sahai, and Salil 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.

[11] Oded Goldreich, Amit Sahai, and Salil 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.

[12] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.
Preliminary version appeared in *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 291–304, 1985.

[13] Jeroen 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.

[14] Jozef Gruska. *Quantum Computing*. McGraw-Hill, 1999.

[15] Lane P. Hughston, Richard Jozsa, and William K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183:14–18, 1993.

[16] Joe Kilian and Erez Petrank. An efficient noninteractive zero-knowledge proof system for NP with general assumptions. *Journal of Cryptology*, 11(1):1–27, 1998.

[17] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[18] Amit Sahai and Salil P. Vadhan. A complete promise problem for statistical zero-knowledge. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, pages 448–457, 1997.

[19] Armin Uhlmann. Parallel transport and "quantum holonomy" along density operators. *Reports on Mathematical Physics*, 24:229–240, 1986.

[20] Salil P. Vadhan. *A Study of Statistical Zero-Knowledge Proofs*. PhD thesis, Department of Mathematics, Massachusetts Institute of Technology, August 1999.

[21] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science*, 2002. To appear.