# 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

## 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 Background

Zero-knowledge proof systems were introduced by Goldwasser, Micali, and Rackoff [8] 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 [13] 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 [9] 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 [2], and was later studied by a number of works [4, 5, 1, 6, 10, 3, 7, 12]. 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 [6]. As for non-interactive statistical zero-knowledge proof systems, De Santis, Di Crescenzo, Persiano, and Yung [3] 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 [7] 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.

## 2 Our Results

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 [13].

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 with the non-output part or is it far from that? More formally, we consider the following promise problem which is parameterized by constants $\alpha$ and $\beta$ satisfying $0 \leq \alpha < \beta \leq 1$:

$(\alpha, \beta)$-Quantum State Closeness to Identity

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

**Promise:** Letting $\rho = \mathrm{tr}_{\mathcal{H}_{\overline{\mathrm{out}}}}(Q|0^{q_{\mathrm{in}}}\rangle\langle 0^{q_{\mathrm{in}}}|Q^{\dagger})$, we have either one of the following two:
(a) $\|\rho - I/2^{q_{\mathrm{out}}}\|_{\mathrm{tr}} \leq \alpha$,
(b) $\|\rho - I/2^{q_{\mathrm{out}}}\|_{\mathrm{tr}} \geq \beta$.

**Output:** Accept iff $\|\rho - I/2^{q_{\mathrm{out}}}\|_{\mathrm{tr}} \leq \alpha$.

It is proved that $(0, \beta)$-QSCI is complete for the class of languages having one-sided bounded error non-interactive quantum perfect zero-knowledge proof systems for any constant $0 < \beta < 1$. 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 [7]. 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 the following restricted version of our complete problem is complete for BQP for any fixed constants $0 < \alpha < \beta < 1$:

$(\alpha, \beta)$-One Qubit Quantum State Closeness to Identity

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

**Promise:** Letting $\rho = \mathrm{tr}_{\mathcal{H}_{\overline{\mathrm{out}}}}(Q|0^{q_{\mathrm{in}}}\rangle\langle 0^{q_{\mathrm{in}}}|Q^{\dagger})$, we have either one of the following two:
(a) $\|\rho - I/2\|_{\mathrm{tr}} \leq \alpha$,
(b) $\|\rho - I/2\|_{\mathrm{tr}} \geq \beta$.

**Output:** Accept iff $\|\rho - I/2\|_{\mathrm{tr}} \leq \alpha$.

See [11] for formal definitions and detailed discussions.

# References

[1] M. Blum, A. De Santis, S. Micali, and G. Persiano. *SIAM Journal on Computing*, 20(6), 1991.

[2] M. Blum, P. Feldman, and S. Mical. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, 1988.

[3] A. De Santis, G. Di Crescenzo, G. Persiano, and M. Yung. In *Proceedings of the 25th International Colloquium on Automata, Languages and Programming*, 1998.

[4] A. De Santis, S. Micali, and G. Persiano. In *Advances in Cryptology – CRYPTO '87*, 1987.

[5] A. De Santis, S. Micali, and G. Persiano. In *Advances in Cryptology – CRYPTO '88*, 1988.

[6] O. Goldreich and Y. Oren. *Journal of Cryptology*, 7(1), 1994.

[7] O. Goldreich, A. Sahai, and S. P. Vadhan. In *Advances in Cryptology – CRYPTO '99*, 1999.

[8] S. Goldwasser, S. Micali, and C. Rackoff. *SIAM Journal on Computing*, 18(1), 1989.

[9] J. van de Graaf. PhD thesis, Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, December 1997.

[10] J. Kilian and E. Petrank. *Journal of Cryptology*, 11(1), 1998.

[11] H. Kobayashi. quant-ph/0207158, 2002.

[12] S. P. Vadhan. PhD thesis, Department of Mathematics, Massachusetts Institute of Technology, August 1999.

[13] J. H. Watrous. In *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science*, 2002. To appear.