Complete Problem for Perfect Zero-Knowledge Quantum Proof

Jun Yan*

School of Computer Science and Technology
University of Science and Technology of China
Hefei, Anhui 230027, China
and
State Key Laboratory of Computer Science
Institute of Software, Chinese Academy of Sciences
Beijing 100190, China
junyan@ios.ac.cn

Abstract. The main purpose of this paper is to prove that (promise) problem Quantum State Identicalness (abbreviated QSI) is *essentially* complete for perfect zero-knowledge quantum interactive proof (**QPZK**). Loosely speaking, problem QSI is to decide whether two efficiently preparable quantum states (captured by quantum circuit of polynomial size) are identical or far apart (in trace distance). It is worthy noting that our result does not have classical counterpart yet; natural complete problem for perfect zero-knowledge interactive proof (**PZK**) is still unknown. Our proof generalizes Watrous' completeness proof for statistical zero-knowledge quantum interactive proof (**QSZK**), with an extra idea inspired by Malka to deal with completeness error. With complete problem at our disposal, we can immediately prove (and reprove) several interesting facts about **QPZK**.

Keywords: Quantum zero-knowledge proof, perfect zero-knowledge, complete problem, quantum complexity, quantum cryptography.

1 Introduction

Zero-knowledge proof has been a hot topic and played an important role in complexity and cryptography research since it was introduced by Goldwasser, Micali, and Rackoff in [11]. Zero-knowledge proof is an intriguing notion, from which verifier "learns" nothing but the truth of the assertion. Recall that in canonical proof system represented by complexity class **NP**, prover just sends witness as the proof for the verifier to check. Intuitively, a canonical proof system cannot be zero-knowledge, for it also reveals the witness to the verifier other than the truth of the assertion. To construct zero-knowledge proof system, we have to generalize the notion of canonical proof. Such generalization turns out to be of

* This work is supported by the National Natural Science Foundation of China (Grant No. 60833001).

M. Bieliková et al. (Eds.): SOFSEM 2012, LNCS 7147, pp. 419–430, 2012.

two folds: First, we allow the proof to be *probabilistic*, with a slight of *completeness and soundness errors*. Second, we allow the proof to be *interactive*, in the sense that prover and verifier can exchange messages. The resulting proof system is known as *interactive proof system*. An alternative way which preserves non-interactiveness of the canonical proof is to let prover and verifier share a random string a prior, resulting in a proof system known as *non-interactive proof system*. There is a *protocol* associated with each interactive and non-interactive proof system, describing (honest) prover's and (honest) verifier's strategies. The formulation of the zero-knowledge property of a proof system follows *simulation paradigm*; loosely speaking, we says verifier "learns nothing" from a proof if the proof itself (a probability distribution) can be approximately generated without prover. According to the "quality" of approximation, we have *perfect*, *statistical*, and *computational* zero-knowledge proofs (denoted by **PZK**, **SZK**, and **ZK** in the interactive model, and **NIPZK**, **NISZK**, and **NIZK** in the non-interactive model, respectively). The formal definition and more details about zero-knowledge proof can be found in standard textbooks such as [8, Chapter 9], [7, Chapter 4].

Quantum proof system is a generalization of classical proof system in the quantum world. In the past decade, a variety of computational models of quantum proof system (see [23,1,12,17,15,4]) were proposed and studied. Since quantumness is a phenomenan, for good or bad, that exists in nature, we cannot help considering the possibility of zero-knowledge quantum proof[1], which may play an important role in quantum cryptography (like its classical counterpart in classical cryptography). As a natural generalization of classical zero-knowledge proof, we can define **QPZK**, **QSZK**, and **QZK** in the interactive model, and **NIQPZK**, **NIQSZK**, and **NIQZK** in the non-interactive model, respectively (see [24,27,15,4]).

Two Generic Approaches

To study properties of zero-knowledge proof, there are two generic approaches. The first one is via (black-box) transformation. That is, given a zero-knowledge proof system, we construct a new one for which prover's and verifier's strategies are constructed using original prover's strategy, original verifier's strategy, plus original simulator, as black-boxes. For example, one can transform an honest-verifier statistical zero-knowledge interactive proof system with completeness error into another one with perfect completeness [6].

In this paper, we are more interested in the second approach to study zero-knowledge proof, namely, via complete problem. This approach is in the same spirit as we study complexity class **NP** via various **NP**-complete problems. Sahai and Vadhan [19] initialized this approach. In particular, they found problems Statistical Difference (SD) and its complement $\overline{\mathsf{SD}}$ are complete for statistical zero-knowledge interactive proof (**SZK**). Follow-up works include [10], [21], [9],

[1] Some researchers may use term "quantum zero-knowledge proof", but we choose to follow Watrous [26].

among others. Using complete problems, many interesting facts about statistical zero-knowledge (interactive and non-interactive) proof are proved *unconditionally* (in contrast to those proved based on complexity assumption such as existence of one-way function). Refer to [22] for a survey on the study of statistical zero-knowledge proof via complete problem.

In quantum case, we can also study zero-knowledge quantum proof via both transformation and complete problem. Interested readers are referred to [12], [17], [14], et al., for the first approach. With respect to complete problem, Watrous [24] was the first to extend the idea of [19] to study statistical zero-knowledge quantum interactive proof (**QSZK**). Specifically, in [24] two promise problems, Quantum State Distinguishability (QSD) and its complement Quantum State Closeness (QSC), were shown to be **QSZK**-complete, where problem QSD can be viewed as the quantum analog of **SZK**-complete problem SD. Later, in the same spirit, Kobayashi [15] (implicitly) found a problem named Quantum State Closeness to Identity (QSCI) that is complete for statistical zero-knowledge quantum non-interactive proof (**NIQSZK**). More recently, using quantum extractor, complete problems for **QSZK** and **NIQSZK** about (von Neumann) entropy difference were found; see [3,4]. Thus far, almost all complete problems for statistical zero-knowledge (classical) proof find their quantum counterparts.

Motivation and Related Work

Note that in either classical or quantum cases, only complete problems for statistical zero-knowledge proof are found. Naturally we shall ask, what about complete problems for perfect and computational zero-knowledge proof, in classical and quantum cases, respectively? In this paper, we shall focus on perfect zero-knowledge proof.

Let us first review some prior related works. In his thesis [22, section 4.7], Vadhan fully discussed the extension of **SZK** completeness proof to **PZK**. In particular, he found that the straightforward adaption of his proof only gives hard problems for a restriction of **PZK**. Since then, there have been no progress towards complete problems for perfect zero-knowledge proof until recently, when Malka [16] constructed a (comparably natural) complete problem for perfect zero-knowledge non-interactive proof (**NIPZK**) and a hard problem for public-coin **PZK**. The genesis of Malka's construction is a way to deal with completeness error.

In quantum case, up until now, nearly nothing is known about the complete problem for **QPZK**. Instead, Kobayashi [14] proved several impressing properties about **QPZK** via transformations, while remarking that the finding of natural complete problem for **QPZK** are definitely helpful. As for non-interactive model, Kobayashi [15] constructed a complete problem for $\mathbf{NIQPZK}_1$ (**NIQPZK** with perfect completeness).

In this paper, we try to answer the following question: can we apply Malka's [16] idea in classical case to construct complete problem for perfect zero-knowledge quantum proof?

Our Contribution

The main result of this paper is to give a (comparably) natural (promise) problem that is complete for **QPZK**. To our knowledge, this is the first time that some natural (not involving computation of universal model of computation) complete problem is found for general perfect zero-knowledge interactive proof (in both classical and quantum case). We can also carry the same study in non-interactive model, obtaining a **NIQPZK**-complete problem.

To get a taste of our **QPZK**-complete problem, it would be beneficial to first recall the **QSZK**-complete problem QSC. Loosely speaking, instances of problem QSC consist of a pair of efficiently preparable quantum states (captured by quantum circuit of polynomial size; see section 3 for detail), where for yes instance these two states are close (in trace distance), while for no instance they are far apart. Our **QPZK**-complete problem is *essentially* (not exactly) a special case of problem QSC as follows: the no instance is the same as problem QSC, whereas the yes instance now is restricted to a pair of efficiently preparable quantum states that are *identical*; we call this special problem Quantum State Identicalness (QSI). Roughly, our actual **QPZK**-complete problem adds a **BQP** instance to each instance of problem QSI; the formal definition is referred to Definition 2.

With complete problems at our disposal, we can immediately prove (and reprove) several interesting facts about perfect zero-knowledge quantum (interactive and non-interactive) proof as follows.

1. Every problem possessing perfect zero-knowledge quantum interactive proof has a two-message honest-verifier perfect zero-knowledge quantum interactive proof, with exponentially small completeness and soundness error; it also has a three-message public-coin honest-verifier perfect zero-knowledge quantum interactive proof, in which verifier's message consists of a single coin flip.
2. **HVQPZK** = **QPZK**. That is, from complexity view, the restriction to honest verifier *does not* change the class of problems possessing perfect zero-knowledge quantum interactive proof.
3. $\mathbf{QPZK} \subseteq \mathbf{BQP}^{\mathbf{QPZK}_1}$, $\mathbf{NIQPZK} \subseteq \mathbf{BQP}^{\mathbf{NIQPZK}_1}$, where the subscript "1" stands for with perfect completeness. This implies that allowing completeness error essentially *does not* increase the complexity of perfect zero-knowledge quantum proof.
4. $\mathbf{NIQPZK}_{\mathrm{h}} = \mathbf{QPZK} = \mathbf{QPZK}_{\mathrm{h}}$, where subscript "h" indicates the help model [4] (a model lying between standard interactive and non-interactive models).
5. $\mathbf{QPZK}_1$ is closed under monotone boolean formula. This result can be viewed as quantum analog of results in [20] and [5], where boolean closure property for some special cases of **PZK** is established.

We remark that among the facts listed above, only the second part of item 1 and item 2 are previously known, which were proved by Kobayashi [14] through a series of transformations. In comparison, our proof via complete problem is almost straightforward.

Main Idea

The main idea of our construction of **QPZK**-complete problem is from Watrous [24] and Malka [16]: we almost follow [24] to do simulator analysis, with only one difference that is similar to [16] to deal with completeness error. Roughly speaking, the difference is that now we no longer move the completeness error into the simulation. This difference will result in the instance of our complete problem having an extra quantum circuit (compared with **QSZK**-complete problem QSC) to encode the acceptance probability of simulator. More detail is referred to section 4. We remark that due to the quantum nature, our construction of **QPZK**-complete problem is different from [16]; indeed, it is simpler and more straightforward.

Our **NIQPZK**-complete problem is obtained by the same idea, except that now the simulator analysis follows Kobayashi [15].

Comparing with Results in Classical Case

Problem QSI can be viewed as the quantum analog of problem $\overline{\mathsf{SD}^{1/2,0}}$ introduced in [22, section 4.7], whose instances consist of a pair of efficiently samplable probability distributions, where for yes instance these two distributions are close (in statistical difference), while for no instance they are far apart. As a special case of **SZK**-complete problem $\overline{\mathsf{SD}}$, it is tempting to prove that problem $\overline{\mathsf{SD}^{1/2,0}}$ is **PZK**-complete. But whether this is true is still open: we only know that this problem is hard for public-coin **PZK** with respect to honest verifier and with perfect completeness. Malka [16] modified problem $\overline{\mathsf{SD}^{1/2,0}}$ to get a hard problem for public-coin **PZK** with respect to honest verifier, removing perfect completeness restriction. In comparison, our quantum result is much stronger: it does not suffer any restrictions, giving a complete problem for general **QPZK**.

Organization

In this extended abstract, we shall highlight the specification of our **QPZK**-complete problem and the idea of its construction. The technical detail of the proof, as well as the completeness theorem in non-interactive model, and applications of complete problems, are all referred to the full version of this paper [28].

The remainder of this paper is organized as follows. In section 2 we review some background materials. Section 3 is devoted to the formal definition of our complete problems. Section 4 contains the sketch of the proof of completeness theorem for **QPZK**. We conclude with section 5.

2 Preliminaries

We assume readers are familiar with basic quantum computation and information (see [18,13]), as well as basic notion of zero-knowledge (classical) interactive proof system (see [2,7,8]).

2.1 Quantum Circuit Model

In this paper, we shall restrict our attention to *unitary* quantum circuit model, where the choice of universal gate set could be arbitrary[2]. In particular, one can choose *Shor basis*: Toffoli gate, Hadamard gate, and Phase-shift gate. Measurement of a qubit is with respect to computational basis $\{|0\rangle, |1\rangle\}$, described by $\{\Pi_0, \Pi_1\}$.

We formalize efficient quantum algorithm Q in terms of *polynomial-time uniformly generated* family of quantum circuits $\{Q_x\}$, where by "polynomial-time uniformly generated" we mean there is a (classical) Turing machine which on input x, outputs a description of quantum circuits Q_x in time polynomial of $|x|$.

2.2 Efficiently Preparable Quantum State

An *efficiently preparable quantum state* is encoded by a quantum circuit Q of polynomial size in the following way: apply Q on quantum registers denoted by (O, G) that are initialized in state $|0\rangle$, where registers O and G correspond to the *output* and *non-output* (garbage) qubits, respectively. That is, quantum state encoded by quantum circuit Q, which we denote by ρ^Q, is $\mathrm{Tr}_{\mathcal{G}}\big(Q|0\rangle\langle 0|Q^*\big)$, where *partial trace* $\mathrm{Tr}_{\mathcal{G}}(\cdot)$ is tracing out qubits corresponding to register G.

Efficiently preparable quantum state can be viewed as quantum analog of efficiently samplable probability distribution [22, Definition 3.1.1].

2.3 Perfect Zero-Knowledge Quantum Interactive Proof

Quantum interactive proof system [12] generalizes classical interactive proof system by allowing prover, verifier, as well as communication channel, to use quantumness. To formally define perfect zero-knowledge property of quantum interactive proof system, we need first to introduce the notion of verifier's view.

Suppose (P,V) is an m-message quantum interactive proof system. Following [24], we define *verifier's view* immediately after the i-th message is sent, denoted by $\mathrm{view}_{\mathrm{P,V}}(x, i)$, as the joint quantum state of all qubits other than those at prover's hand at that moment. For our convenience, we also define $\mathrm{view}_{\mathrm{P,V}}(x, 0)$ and $\mathrm{view}_{\mathrm{P,V}}(x, m+1)$ as the *initial* (before the running) and *final* (after the running) views of verifier, respectively.

Following [24], we say quantum interactive proof system (P,V) has *perfect zero-knowledge* property with respect to *honest verifier* if there exists a collection of efficiently preparable quantum states $\{\sigma_{x,i}\}$ such that for each input $x \in A_{\mathrm{yes}}$, and for each $i \in \{0, 1, \ldots, m+1\}$,

$$\mathrm{view}_{\mathrm{P,V}}(x, i) = \sigma_{x,i}. \tag{1}$$

[2] We remark that our complete theorems are insensible to the choice of universal unitary quantum gate set. However, to prove **HVQPZK** = **QPZK**, we need *reversible computation* and *phase-flip* be implemented without error (this is required in *quantum rewinding lemma* [24] that will be applied).

In other words, there is a *simulator* which on input $x \in A_{\text{yes}}$, runs in polynomial time and outputs $\text{view}_{\text{P,V}}(x, i)$ for each i.

We shall denote by **HVQPZK** the class of promise problems possessing honest-verifier perfect zero-knowledge quantum interactive proof. Though perfect zero-knowledge property only with respect to honest-verifier seems a little bit weak in practice, class **HVQPZK** is nevertheless suitable for complexity study. In this paper, we actually prove completeness theorem for **HVQPZK**; it turns out that with our **HVQPZK**-complete problem, we immediately have **HVQPZK** = **QPZK** by calling quantum rewinding lemma [27]. The equivalence of **HVQPZK** and **QPZK** in turn justifies that our focus on **HVQPZK** does not lose any generality. Thus, here we even choose not to give formal definition of **QPZK**, which requires more setup that is not relevant to the focus of this paper; the formal definition of **QPZK** can be found in [27,14].

As a remark about the definition of perfect zero-knowledge quantum interactive proof, note that the generally accepted definition for perfect zero-knowledge (classical) proof allows simulator to fail with some probability. In spite of this, it turns out that such relaxation does not change the corresponding complexity classes induced by perfect zero-knowledge proof, either in classical or quantum cases (see [16] and [14], respectively). These facts once again illustrate the robustness of complexity classes **PZK** and **QPZK**.

2.4 Perfect Zero-Knowledge Quantum Non-interactive Proof

Recall that in classical case, non-interactive proof consists of only one message which is sent from prover to verifier; moreover, prover and verifier share a prior a uniformly distributed random string known as *common reference string* [7]. In quantum case, Kobayashi [15] suggested replacing the random string with *EPR pairs* such that prover and verifier keep one qubit of each EPR pair privately before the execution of the protocol.

3 Complete Problems

In this section, we shall introduce several promise problems concerning about efficiently preparable quantum state. Before giving formal definition, we need first introduce the notion of trace distance between two quantum states. Specifically, the *trace distance* between two quantum states ρ and ξ, which we denote by $\delta(\rho, \xi)$, is equal to $\|\rho - \xi\|_1 / 2$, where $\|\cdot\|_1$ is the *trace norm*, or 1-norm (see [25]). The trace distance can be viewed as the quantum analog of statistical difference between two probability distributions.

The first problem we are to introduce is problem Quantum State Identicalness (abbreviated QSI).

Definition 1. *The specification of problem* QSI *is as follows.*

Input: description of a pair of quantum circuits (Q_0, Q_1), which encode two quantum states, respectively.

Promise: Circuits Q_0 and Q_1 act on, and output, the same number of qubits. Moreover, either of the following two conditions hold:
(1) $\delta(\rho^{Q_0}, \rho^{Q_1}) = 0$,
(2) $\delta(\rho^{Q_0}, \rho^{Q_1}) \geq 2/3$.
Output: Accept in case (1) and reject in case (2).

We point out that problem QSI can be viewed as a special case problem QSC, in which the yes instance is relaxed to be $\delta(\rho^{Q_0}, \rho^{Q_1}) \leq 1/3$. We are interested in problem QSI because later in this paper we shall show its $\mathbf{QPZK}_1$-completeness (**QPZK** with perfect completeness); moreover, our **QPZK**-complete problem is just a slight variant of problem QSI, as described below.

Definition 2. *The specification of problem* QSI′ *is as follows.*

Input: description of a triple of quantum circuits (Q_0, Q_1, Q_2), which encode three quantum states, respectively.
Promise: Circuits Q_0 and Q_1 act on, and output, the same number of qubits; circuit Q_2 outputs one qubit. Moreover, either of the following two conditions hold:
(1) $\delta(\rho^{Q_0}, \rho^{Q_1}) = 0$ and $Tr(\Pi_1 \rho^{Q_2}) \geq 2/3$;
(2) $\delta(\rho^{Q_0}, \rho^{Q_1}) \geq 1/2$ or $Tr(\Pi_1 \rho^{Q_2}) \leq 1/3$.
Output: Accept in case (1) and reject in case (2).

Compared with problem QSI, the instance of problem QSI′ has an extra quantum circuit Q_2, which induces a **BQP** instance; the motivation of its construction is referred to section 4.

We remark that the choice of constants in the definitions above is arbitrary, due to a straightforward polarization lemma.

Next, we are going to introduce two additional problems concerning about efficiently preparable quantum state. Actually, these two problems can be viewed as special cases of the two problems defined above respectively: if we fix quantum circuit Q_0 to encode *maximally mixed state* (represented by density operator $\mathbb{1}/2^k$, where integer k is the number of qubits designated as output) in the definitions of problem QSI and QSI′, then we obtain problems that we shall denote by QSII (Quantum State Identicalness to Identity) and QSII′, respectively. Kobayashi [15] proved that problem QSII is $\mathbf{NIQPZK}_1$-complete; we can extend this result to show that problem QSII′ is **NIQPZK**-complete.

4 The Completeness Theorem

In this section, we shall sketch the completeness proof for **HVQPZK**, with the focus on the idea of the construction of our complete problem QSI′. The proof itself is adapted from Watrous' completeness proof for **HVQSZK** [24], with a new idea inspired by Malka [16] to deal with completeness error. We shall also give the statement of complete theorem for **NIQPZK** without proof.

Theorem 1. *Problem* QSI' *is* **HVQPZK***-complete.*

Proof. We only sketch the proof here, highlighting the main idea.

A **HVQPZK** protocol for problem QSI' is as follows. On input (Q_0, Q_1, Q_2), we let verifier first run a procedure resembling **BQP** error reduction: apply many copies of Q_2 on qubits in state $|0\rangle$, and then measure the output qubits of all these copies: reject immediately if less than a half of outcomes are one. Then conditioned on verifier does not reject, we let prover and verifier execute either of two *identicalness tests*, which are adapted from closeness tests given in [24], on input (Q_0, Q_1). This will establish that problem QSI' belongs to **HVQPZK**.

Next, we give a reduction from an arbitrary problem $A \in$ **HVQPZK** to problem QSI'.

Suppose (P,V) is an m-message honest-verifier perfect zero-knowledge quantum interactive proof system for problem A. Following [12] and [24], we can formalize the running of (P,V) on input $x \in A_{\text{yes}} \cup A_{\text{no}}$ in terms of quantum circuits. Specifically, the workspace of (P,V) is divided into three parts of quantum registers P, M and V, corresponding to prover's private workspace, communication channel, and verifier's private workspace, respectively. At the beginning, all qubits of the workspace are initialized to be in state $|0\rangle$. Then prover and verifier take in turns to apply their operations (represented by quantum circuits) on quantum register (P, M) and (M, V), respectively. Since in this paper we restrict to unitary quantum circuit model, all these operations are unitary. One qubit, say the first qubit of register V, is designated as the *output* of the whole proof system.

We introduce some notations that are consistent with [24]. Let $n = |x|$. Without loss of generality, assume m is even (thus, verifier sends the first message); let $k = m/2 + 1$. Suppose prover's and verifier's operations are $P_1, \ldots, P_{k-1}$ and $V_1, \ldots, V_k$, respectively. Suppose the simulator for (P,V) outputs a collection of quantum states, $\{\rho_j\}$ and $\{\xi_j\}$, to approximate verifier's views. The case for $m = 4$ is illustrated in Figure 1.

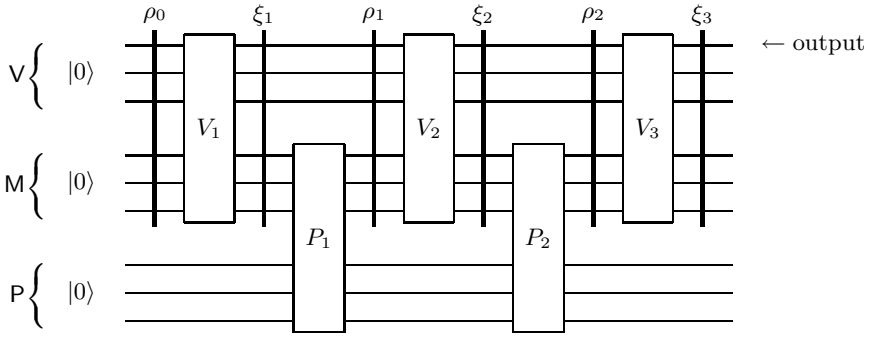

Fig. 1. A 4-message perfect zero-knowledge quantum interactive proof system

Without loss of generality, we can assume that the collection of quantum states $\{\rho_j\}$ and $\{\xi_j\}$ satisfy (whether $x \in A_{\text{yes}}$ or $x \in A_{\text{no}}$) the following properties:

1. $\rho_0 = |0\rangle\langle 0|$;
2. $V_j \rho_{j-1} V_j^* = \xi_j$, for $j = 1, \ldots, k$.

These can be achieved by a simple modification of the simulator as [24].

It turns out that whether $x \in A_{\text{yes}}$ or $x \in A_{\text{no}}$ can be based on the simulator analysis as below:

1. If input $x \in A_{\text{yes}}$, then by completeness and honest-verifier perfect zero-knowledge property of the protocol, we have $\text{Tr}_{\mathcal{M}}(\xi_j) = \text{Tr}_{\mathcal{M}}(\rho_j)$, $j = 1, \ldots, k-1$, and $\text{Tr}\big(\Pi_1 \xi_k\big) \geq 1 - 2^n$.
2. If input $x \in A_{\text{no}}$, then by soundness of the protocol, either for some j, $\delta(\text{Tr}_{\mathcal{M}}(\xi_j), \text{Tr}_{\mathcal{M}}(\rho_j))$ is "noticeable", or $\text{Tr}\big(\Pi_1 \xi_k\big)$ is "negligible". For otherwise, prover can use a simulator-based strategy to cheat verifier to accept with a noticeable amount of probability.

We highlight that compared with the simulator analysis for **HVQSZK** in Watrous' proof, here we have an extra term $\text{Tr}\big(\Pi_1 \xi_k\big)$, which is used to capture the acceptance probability of the final state output by the simulator (probability that the final state will cause verifier to accept). In Watrous' proof, this term is not needed because in case of **HVQSZK**, one can assume, also by a simple modification of simulator, that the resulting simulator always outputs a final state which will cause verifier to accept with certainty. However, this modification moves completeness error into the simulation. Note that this error of simulation is allowable in case of statistical zero-knowledge, which can tolerate exponentially small error. But in case of perfect zero-knowledge, we cannot do this. So in our reduction, we do not do this modification of simulator; instead, we use an extra quantum circuit to capture the acceptance probability of the final state. This will cause the resulting complete problem (QSI') a bit more complex (having an extra quantum circuit to capture $\text{Tr}\big(\Pi_1 \xi_k\big)$) than **HVQSZK**-complete problem QSC. Actually, this is exactly quantum analog of Malka's idea [16] in classical case.

Now we describe the instance of problem QSI' to which input x is reduced:

- Q_0: quantum circuit which encodes quantum state $\text{Tr}_{\mathcal{M}}(\rho_1) \otimes \cdots \otimes \text{Tr}_{\mathcal{M}}(\rho_{k-1})$.
- Q_1: quantum circuit which encodes quantum state $\text{Tr}_{\mathcal{M}}(\xi_1) \otimes \cdots \otimes \text{Tr}_{\mathcal{M}}(\xi_{k-1})$.
- Q_2: quantum circuit which encodes quantum state ξ_k, with the output redesignated as the qubit intended as the approximation of the first qubit of register V.

Clearly, the description of quantum circuits Q_0, Q_1, Q_2 can be computed in polynomial time given the simulator (which runs in polynomial time). □

We observe that for $\mathbf{HVQPZK}_1$, a special case of **HVQPZK** with perfect completeness, quantum circuit Q_2 in our reduction above can be discarded by the same modification of simulator as Watrous [24]. We thus have the following completeness theorem for $\mathbf{HVQPZK}_1$.

Theorem 2. *Problem* QSI *is* $\mathbf{HVQPZK}_1$*-complete.*

We note that complete problems for **HVQPZK** and $\mathbf{HVQPZK}_1$ only differ up to a **BQP** instance. Does $\mathbf{HVQPZK} = \mathbf{HVQPZK}_1$? This is an interesting open problem. It is worthy noting that Kobayashi [14] showed that $\mathbf{HVQSZK} = \mathbf{HVQSZK}_1$ by giving a transformation. However, this transformation cannot be applied directly to perfect zero-knowledge quantum proof, because it will introduce an additional message which may not be perfectly output by simulator (though it can be approximated with exponentially small error).

In non-interactive model, we can also prove a completeness theorem with the same strategy as in interactive model, except that now the proof is adapted from Kobayashi [15].

Theorem 3. *Problem* QSII′ *is* **NIQPZK***-complete.*

5 Conclusion

Combining our results with [24] and [14], we can draw a table as below to summerize all complete problems we known for statistical and perfect zero-knowledge quantum proofs.

Complexity class	**QSZK**	$\mathbf{QPZK}_1$	**QPZK**	**NIQSZK**	$\mathbf{NIQPZK}_1$	**NIQPZK**
Complete problem	QSC	QSI	QSI′	QSCI	QSII	QSII′

We note that all these complete problems can be viewed as derived from problem QSC, comparing them may reveal the relationship among corresponding complexity classes.

References

1. Aharonov, D., Naveh, T.: Quantum NP - a survey (2002)
2. Arora, S., Barak, B.: Computational Complexity: A Modern Approach. Cambridge University Press (2009)
3. Ben-Aroya, A., Schwartz, O., Ta-Shma, A.: Quantum expanders: Motivation and construction. Theory of Computing 6(1), 47–79 (2010)
4. Chailloux, A., Ciocan, D.F., Kerenidis, I., Vadhan, S.P.: Interactive and Noninteractive Zero Knowledge are Equivalent in the Help Model. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 501–534. Springer, Heidelberg (2008)
5. Damgård, I.B., Cramer, R.J.: On monotone function closure of perfect and statistical zero-knowledge. Technical report, Amsterdam, The Netherlands (1996)
6. Furer, M., Goldreich, O., Mansour, Y., Sipser, M., Zachos, S.: On completeness and soundness in interactive proof systems. In: Micali, S. (ed.) Randomness and Computation, Greenwich, Connecticut. Advances in Computing Research, vol. 5, pp. 429–442. JAI Press (1996)
7. Goldreich, O.: Foundations of Cryptography, Basic Tools, vol. I. Cambridge University Press (2001)

8. Goldreich, O.: Computational Complexity: A Conceptual Approach. Cambridge University Press (2008)
9. Goldreich, O., Sahai, A., Vadhan, S.P.: Can Statistical Zero Knowledge be Made Non-Interactive? or on the Relationship of SZK and NISZK. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, p. 467. Springer, Heidelberg (1999)
10. Goldreich, O., Vadhan, S.P.: Comparing entropies in statistical zero knowledge with applications to the structure of SZK. In: IEEE Conference on Computational Complexity, pp. 54–73 (1999)
11. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. SIAM J. Comput. 18(1), 186–208 (1989)
12. Kitaev, A.Y., Watrous, J.: Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In: STOC, pp. 608–617 (2000)
13. Kitaev, A.Y., Shen, A.H., Vyalyi, M.N.: Classical and Quantum Computation. In: American Mathematical Society. Graduate Studies in Mathematics, vol. 47. American Mathematical Society (2002)
14. Kobayashi, H.: General Properties of Quantum Zero-Knowledge Proofs. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 107–124. Springer, Heidelberg (2008), arXiv.org e-Print 0705.1129
15. Kobayashi, H.: Non-Interactive Quantum Perfect and Statistical Zero-Knowledge. In: Ibaraki, T., Katoh, N., Ono, H. (eds.) ISAAC 2003. LNCS, vol. 2906, pp. 178–188. Springer, Heidelberg (2003)
16. Malka, L.: How to Achieve Perfect Simulation and A Complete Problem for Non-Interactive Perfect Zero-Knowledge. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 89–106. Springer, Heidelberg (2008)
17. Marriott, C., Watrous, J.: Quantum Arthur-Merlin games. Computational Complexity 14(2), 122–152 (2005)
18. Nielsen, M.A., Chuang, I.L.: Quantum computation and Quantum Informatioin. Cambridge University Press (2000)
19. Sahai, A., Vadhan, S.P.: A complete problem for statistical zero knowledge. J. ACM 50(2), 196–249 (2003)
20. Santis, A.D., Crescenzo, G.D., Persiano, G., Yung, M.: On monotone formula closure of SZK. In: FOCS, pp. 454–465 (1994)
21. De Santis, A., Di Crescenzo, G., Persiano, G., Yung, M.: Image Density is Complete for Non-Interactive-SZK (Extended Abstract). In: Larsen, K.G., Skyum, S., Winskel, G. (eds.) ICALP 1998. LNCS, vol. 1443, pp. 784–795. Springer, Heidelberg (1998)
22. Vadhan, S.: Ph.D Thesis: A Study of Statistical Zero-Knowledge Proofs (1999)
23. Watrous, J.: Succinct quantum proofs for properties of finite groups. In: FOCS, pp. 537–546 (2000)
24. Watrous, J.: Limits on the power of quantum statistical zero-knowledge. In: FOCS, pp. 459–468 (2002)
25. Watrous, J.: Theory of Quantum Information. Online Lecture Notes (2008), http://www.cs.uwaterloo.ca/~watrous/798/
26. Watrous, J.: Quantum computational complexity. In: Encyclopedia of Complexity and Systems Science, pp. 7174–7201 (2009)
27. Watrous, J.: Zero-knowledge against quantum attacks. SIAM J. Comput. 39(1), 25–58 (2009)
28. Yan, J.: Complete problem for perfect zero-knowledge quantum proof. Full version, http://lcs.ios.ac.cn/~junyan/Yan11_qpzk-SOFSEM12-final-full.pdf