General Properties of Quantum Zero-Knowledge Proofs

Hirotada Kobayashi

Principles of Informatics Research Division, National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan
hirotada@nii.ac.jp

Abstract. This paper studies general properties of quantum zero-knowledge proof systems. Among others, the following properties are proved on quantum computational zero-knowledge proofs:

- *Honest-verifier* quantum zero-knowledge equals general quantum zero-knowledge.
- *Public-coin* quantum zero-knowledge equals general quantum zero-knowledge.
- Quantum zero-knowledge with *perfect completeness* equals general quantum zero-knowledge with imperfect completeness.
- Any quantum zero-knowledge proof system can be transformed into a *three-message public-coin* quantum zero-knowledge proof system of perfect completeness with polynomially small error in soundness (hence with arbitrarily small constant error in soundness).

All the results proved in this paper are unconditional, i.e., they do not rely any computational assumptions. The proofs for all the statements are direct and do not use complete promise problems, and thus, essentially the same method works well even for quantum statistical and perfect zero-knowledge proofs. In particular, all the four properties above hold also for the statistical zero-knowledge case (the first two were shown previously by Watrous), and the first two properties hold even for the perfect zero-knowledge case. It is also proved that allowing a simulator to output "FAIL" does not change the power of quantum perfect zero-knowledge proofs. The corresponding properties are not known to hold in the classical perfect zero-knowledge case.

1 Introduction

Background Zero-knowledge proof systems were introduced by Goldwasser, Micali, and Rackoff [13], and have played a central role in modern cryptography since then. Intuitively, an interactive proof system is zero-knowledge if *any* verifier who communicates with the *honest* prover learns nothing except for the validity of the statement being proved in that system. By "learns nothing" we mean that there exists a polynomial-time *simulator* whose output is indistinguishable from the output of the verifier after communicating with the honest prover. Depending on the strength of this indistinguishability, several variants of zero-knowledge proofs have been investigated: *perfect* zero-knowledge in which the output of the simulator is identical to that of the verifier, *statistical* zero-knowledge in which the output of the simulator is statistically close to that of the verifier, and *computational* zero-knowledge in which the output of the simulator is indistinguishable from that of the verifier in polynomial time. The most striking result on zero-knowledge proofs would be that every problem in NP has a computational zero-knowledge proof system under certain intractability assumptions [10]. It is also known that some problems have perfect or statistical zero-knowledge proof systems. Among others, the Graph Isomorphism problem has a perfect zero-knowledge proof system [10], and some lattice problems have statistical zero-knowledge proof systems [9].

Another direction of studies on zero-knowledge proofs has been to prove their general properties. Sahai and Vadhan [22] were the first who took an approach of characterizing zero-knowledge proofs by complete promise problems. They showed that the Statistical Difference problem is complete for the class HVSZK of problems having *honest-verifier* statistical zero-knowledge proof systems. Here, the honest-verifier zero-knowledge is a weaker notion of zero-knowledge in which now zero-knowledge property holds only against the *honest* verifier who follows the specified protocol. Using this complete promise problem, they proved a number of general properties of HVSZK and simplified the proofs of several previously known results, including that HVSZK is in AM [6, 2], that HVSZK is closed under complement [21], and that any problem in HVSZK has a public-coin honest-verifier statistical zero-knowledge proof system [21]. Goldreich and Vadhan [12] presented another complete promise problem for HVSZK, called the Entropy Difference problem, and obtained further properties of HVSZK. Since Goldreich, Sahai, and Vadhan [11] proved that HVSZK = SZK, where SZK denotes the class of problems having statistical zero-knowledge proof systems, all the properties proved for HVSZK are inherited to SZK (except for those related to round complexity). More recently, Vadhan [24] gave two characterizations, the Indistinguishability characterization and the Conditional Pseudo-Entropy characterization, for the class ZK of problems having computational zero-knowledge proof systems. These are not complete promise problems, but more or less analogous to complete promise problems and play essentially same roles as complete promise problems in his proofs. Using these characterizations, he proved a number of general properties of ZK unconditionally (i.e., not assuming any intractability assumptions), such as that honest-verifier computational zero-knowledge equals general computational zero-knowledge, that public-coin computational zero-knowledge equals general computational zero-knowledge, and that computational zero-knowledge with perfect completeness equals that with imperfect completeness.

Quantum zero-knowledge proofs were first studied by Watrous [25] in a restricted situation of *honest-verifier* quantum statistical zero-knowledge proofs. He gave an analogous characterization to the classical case due to Sahai and Vadhan [22] by showing that the Quantum State Distinguishability problem is complete for the class HVQSZK of problems having honest-verifier quantum statistical zero-knowledge proof systems. Using this, he proved a number of general properties of HVQSZK, such as that HVQSZK is closed under complement, that any problem in HVQSZK has a public-coin honest-verifier quantum statistical zero-knowledge proof system, and that HVQSZK is in PSPACE. Very recently, Ben-Aroya and Ta-Shma [3] presented another complete promise problem for HVQSZK, called the Quantum Entropy Difference problem, which is a quantum analogue of the result by Goldreich and Vadhan [12]. It has been a wide open problem if there are nontrivial problems that have quantum zero-knowledge proofs secure even against any dishonest quantum verifiers, because of the difficulties arising from the "rewinding" technique [14], which is commonly used in classical zero-knowledge proofs. Damgård, Fehr, and Salvail [4] studied zero-knowledge proofs against dishonest quantum verifier, but they assumed the restricted setting of the common-reference-string model to avoid this rewinding problem. Very recently, Watrous [27] settled this affirmatively. He established a quantum "rewinding" technique by using a method that was originally developed in Ref. [19] for the purpose of amplifying the success probability of QMA, a quantum version of NP, without increasing quantum witness sizes. With this quantum rewinding technique, he proved that the classical proof system for the Graph Isomorphism problem in Ref. [10] has a perfect zero-knowledge property even against any dishonest *quantum* verifiers, and under some reasonable intractability assumption, the classical proof system for NP in Ref. [10] has a computational zero-knowledge property even against any dishonest *quantum* verifiers. He also proved that HVQSZK = QSZK, where QSZK denotes the class of problems having quantum statistical zero-knowledge proof systems. Together with his proof construction, this implies that all the properties proved for HVQSZK in Ref. [25] are inherited to QSZK (except for those related to round complexity), in particular, that any problem in QSZK has a public-coin quantum statistical zero-knowledge proof system.

Our contribution This paper proves a number of general properties on quantum zero-knowledge proofs, not restricted to the statistical zero-knowledge case. Specifically, for quantum computational zero-knowledge proofs, letting QZK and HVQZK denote the classes of problems having quantum computational zero-knowledge proof systems and *honest-verifier* quantum computational zero-knowledge proof systems, respectively, the following are proved among others:

Theorem 1. HVQZK = QZK.

Theorem 2. *Any problem in* QZK *has a public-coin quantum computational zero-knowledge proof system.*

Theorem 3. *Any problem in* QZK *has a quantum computational zero-knowledge proof system of perfect completeness.*

Theorem 4. *Any problem in* QZK *has a three-message public-coin quantum computational zero-knowledge proof system of perfect completeness with soundness error at most* $\frac{1}{p}$ *for any polynomially bounded function* $p\colon \mathbb{Z}^+ \to \mathbb{N}$.

All the properties proved in this paper on quantum computational zero-knowledge proofs hold unconditionally, meaning that they hold without any computational assumptions such as the existence of quantum one-way functions or permutations. Some of these properties may be regarded as quantum versions of the results by Vadhan [24]. It is stressed, however, that our approach to prove these properties is completely different from those the existing studies took to prove general properties of classical or quantum zero-knowledge proofs. No complete promise problems nor characterizations are used in our proofs. Instead, we *directly* prove these properties.

The idea is remarkably simple. We start from any proof system of *honest-verifier* quantum zero-knowledge, and apply several transformations so that we finally obtain another proof system of honest-verifier quantum zero-knowledge that possesses a number of desirable properties. For instance, to prove that $\mathrm{HVQZK} = \mathrm{QZK}$, we show that any proof system of honest-verifier quantum computational zero-knowledge can be transformed into another proof system of honest-verifier quantum computational zero-knowledge (with some smaller gap between completeness and soundness accepting probabilities) such that (i) the proof system consists of three messages and (ii) the proof system is public-coin in which the message from the honest verifier consists of a single bit that is an outcome of a classical fair coin-flipping. This can be done by first achieving negligible completeness error by sequential repetition, then applying the parallelization method for usual quantum interactive proofs due to Kitaev and Watrous [16] to obtain a *three-message* honest-verifier quantum zero-knowledge proof system, and finally applying the Marriott-Watrous construction for usual quantum interactive proofs [19] to obtain a three-message *public-coin* honest-verifier quantum zero-knowledge proof system. It is proved that the Kitaev-Watrous parallelization method preserves the honest-verifier zero-knowledge property if completeness error is negligible, and that the Marriott-Watrous construction also preserves the honest-verifier zero-knowledge property. Now, by applying the quantum rewinding technique due to Watrous [27], this three-message public-coin proof system is proved to be zero-knowledge even against any *dishonest* quantum verifiers. The final piece is the sequential repetition, which makes completeness and soundness errors arbitrarily small. This simultaneously shows the equivalence of public-coin quantum computational zero-knowledge and general quantum computational zero-knowledge. To show that any quantum computational zero-knowledge proofs can be made perfectly complete, now we have only to show that any *honest-verifier* quantum computational zero-knowledge proofs can be made perfectly complete. Again we can use another construction for usual quantum interactive proofs due to Kitaev and Watrous [16], but now we need to carefully and explicitly design a protocol for the honest prover in their construction so that the honest-verifier zero-knowledge property is preserved. Using this construction as a preprocessing, the previous argument shows the equivalence of quantum computational zero-knowledge with perfect completeness and that with imperfect completeness. Combining all the desirable properties of honest-verifier quantum computational zero-knowledge proofs shown in this paper with a careful application of the quantum rewinding technique, we can show that any problem in QZK has a three-message public-coin quantum computational zero-knowledge proof system of perfect completeness with soundness error at most $\frac{1}{p}$ for any polynomially bounded function p.

In fact, our approach above is very general and basically works well even for quantum statistical and perfect zero-knowledge proofs. In the quantum statistical zero-knowledge case, all the properties shown for the quantum computational zero-knowledge case also hold. This gives alternative proofs of the facts that HVQSZK = QSZK and that public-coin quantum statistical zero-knowledge equals general quantum statistical zero-knowledge, which were originally shown by Watrous [27] using his previous results [25], and also shows the following new properties of quantum statistical zero-knowledge proofs:

Theorem 5. *Any problem in* QSZK *has a quantum statistical zero-knowledge proof system of perfect completeness.*

Theorem 6. *Any problem in* QSZK *has a three-message public-coin quantum statistical zero-knowledge proof system of perfect completeness with soundness error at most* $\frac{1}{p}$ *for any polynomially bounded function* $p\colon \mathbb{Z}^+ \to \mathbb{N}$.

In the quantum perfect zero-knowledge case, however, not all the properties above can be shown to hold, because very subtle points easily lose the *perfect* zero-knowledge property. In particular, our method of making proof systems perfectly complete no longer works well for quantum perfect zero-knowledge case. Also, we need a careful modification of the protocol when parallelizing to three messages. Still, we can show the following properties for the classes QPZK and HVQPZK of problems having quantum perfect zero-knowledge proof systems and *honest-verifier* quantum perfect zero-knowledge proof systems, respectively:

Theorem 7. HVQPZK = QPZK.

Theorem 8. *Any problem in* QPZK *has a public-coin quantum perfect zero-knowledge proof system.*

Note that no such general properties are known for the classical perfect zero-knowledge case. As a bonus property, it is also proved that quantum perfect zero-knowledge with a worst-case polynomial-time simulator that is not allowed to output "FAIL" is equivalent to the one in which a simulator is allowed to output "FAIL" with small probability. Again, such equivalence is not known in the classical case.

Due to space limitations, most of the technical proofs are relegated to the full version of this paper [18].

2 Preliminaries

We assume the reader is familiar with classical zero-knowledge proof systems and quantum interactive proof systems. Detailed discussions of classical zero-knowledge proof systems can be found in Refs. [7, 8], for instance, while quantum interactive proof systems are discussed in Refs. [26, 16, 19]. We also assume familiarity with the quantum formalism, including the quantum circuit model and definitions of mixed quantum states, admissible transformations (completely-positive trace-preserving mappings), trace norm, diamond norm, and fidelity (all of which are discussed in detail in Refs. [20, 15], for instance). Some of the notions and notations that are used in this paper are summarized in this section.

Throughout this paper, let $\mathbb{N}$ and $\mathbb{Z}^+$ denote the sets of positive and nonnegative integers, respectively. Let poly denote the set of all functions $p\colon \mathbb{Z}^+ \to \mathbb{N}$ such that there exists a polynomial-time deterministic Turing machine that outputs $1^{p(n)}$ on input 1^n. For every $d \in \mathbb{N}$, let I_d denote the identity operator of dimension d. Also, for any Hilbert space $\mathcal{H}$, let $I_{\mathcal{H}}$ denote the identity operator over $\mathcal{H}$. In this paper, all Hilbert spaces are of dimension power of two.

For any Hilbert space $\mathcal{H}$, let $|0_{\mathcal{H}}\rangle$ denote the quantum state in $\mathcal{H}$ of which all the qubits are in state $|0\rangle$, and let $\mathbf{D}(\mathcal{H})$ and $\mathbf{U}(\mathcal{H})$ denote the sets of density and unitary operators over $\mathcal{H}$, respectively. For any Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, let $\mathbf{T}(\mathcal{H}, \mathcal{K})$ be the set of admissible transformations from $\mathbf{D}(\mathcal{H})$ to $\mathbf{D}(\mathcal{K})$. An admissible transformation $\Phi \in \mathbf{T}(\mathcal{H}, \mathcal{K})$ is *q_{in}-in q_{out}-out* if $\mathcal{H}$ and $\mathcal{K}$ consist of q_{in} and q_{out} qubits, respectively. Let $\mathcal{N}$, $\mathcal{X}$, and $\mathcal{Y}$ be Hilbert spaces such that $\mathcal{H} \otimes \mathcal{X} = \mathcal{K} \otimes \mathcal{Y} = \mathcal{N}$. A unitary transformation $U_\Phi \in \mathbf{U}(\mathcal{N})$ is a *unitary realization* of Φ if $\mathrm{tr}_{\mathcal{Y}} U_\Phi \bigl(\rho \otimes |0_{\mathcal{X}}\rangle\langle 0_{\mathcal{X}}|\bigr) U_\Phi^\dagger = \Phi(\rho)$ for any $\rho \in \mathbf{D}(\mathcal{H})$.

Quantum circuits It is assumed that any quantum circuit Q in this paper is unitary and is composed of gates in some reasonable, universal, finite set of unitary quantum gates. For convenience, we may identify a circuit Q with the unitary operator it induces. Since non-unitary and unitary quantum circuits are equivalent in computational power [1], it is sufficient to treat only unitary quantum circuits, which justifies the above assumption. For avoiding unnecessary complication, however, the descriptions of procedures often include non-unitary operations in the subsequent sections. Even in such cases, it is always possible to construct unitary quantum circuits that essentially achieve the same procedures described. When proving statements concerning quantum perfect zero-knowledge proofs or proofs having perfect completeness, we assume that the Hadamard transformation and any classical reversible transformations are exactly implementable in our gate set. This condition may not hold with an arbitrary universal gate set, but is satisfied by most of the standard gate sets including the Shor basis [23], and thus, the author believes that it is not restrictive. These subtle issues regarding choices of the universal gate set is discussed in the full version of this paper [18]. It is stressed, however, that all of our statements not concerning quantum perfect zero-knowledge proofs nor proofs having perfect completeness do hold with an arbitrary choice of the universal gate set (the completeness and soundness conditions may become worse by negligible amounts in some of the claims, which does not matter for the final main statements).

A quantum circuit Q is *q_{in}-in q_{out}-out* if it exactly implements a unitary realization U_Φ of some q_{in}-in q_{out}-out admissible transformation Φ. For convenience, we may identify a circuit Q with Φ in such a case. As a special case of this, a quantum circuit Q is a *generating circuit* of a quantum state ρ of q qubits if it exactly implements a unitary realization of a zero-in q-out admissible transformation that always outputs ρ. A family $\{Q_x\}$ of quantum circuits is *polynomial-time uniformly generated* if there exists a deterministic procedure that, on every input x, outputs a description of Q_x and runs in time polynomial in $|x|$. It is assumed that the number of gates in any circuit is not more than the length of the description of that circuit, which assures that Q_x has size polynomial in $|x|$. An ensemble $\{\rho_x\}$ of quantum states is *polynomial-time preparable* if there exists a polynomial-time uniformly generated family $\{Q_x\}$ of quantum circuits such that each Q_x is a generating circuit of ρ_x. In what follows, we may use the notation $\{\rho(x)\}$ instead of $\{\rho_x\}$ for ensembles of quantum states simply for descriptional convenience.

Quantum computational indistinguishability We use the notions of quantum computational indistinguishability introduced by Watrous [27]: polynomially quantum indistinguishable ensembles of quantum states and polynomially quantum indistinguishable ensembles of admissible transformations.

Definition 9. *Let $S \subseteq \{0,1\}^*$ be an infinite set and let $m \in \mathrm{poly}$. For each $x \in S$, let ρ_x and σ_x be mixed states of $m(|x|)$ qubits. The ensembles $\{\rho_x \colon x \in S\}$ and $\{\sigma_x \colon x \in S\}$ are* polynomially quantum indistinguishable *if it holds for all but finitely many $x \in S$ that, for every choice of $k, p, s \in \mathrm{poly}$, an ensemble $\{\xi_x \colon x \in S\}$ where ξ_x is a mixed state of $k(|x|)$ qubits, and an $(m(|x|) + k(|x|))$-in one-out quantum circuit Q of size at most $s(|x|)$,*

$$|\langle 1|Q(\rho_x \otimes \xi_x)|1\rangle - \langle 1|Q(\sigma_x \otimes \xi_x)|1\rangle| < \frac{1}{p(|x|)}.$$

Definition 10. *Let $S \subseteq \{0,1\}^*$ be an infinite set and let $l, m \in \mathrm{poly}$. For each $x \in S$, let Φ_x and Ψ_x be $l(|x|)$-in $m(|x|)$-out admissible transformations. The ensembles $\{\Phi_x \colon x \in S\}$ and $\{\Psi_x \colon x \in S\}$ are* polynomially quantum indistinguishable *if it holds for all but finitely many $x \in S$ that, for every choice of $k, p, s \in \mathrm{poly}$, an ensemble $\{\xi_x \colon x \in S\}$ where ξ_x is a mixed state of $l(|x|) + k(|x|)$ qubits, and an $(m(|x|) + k(|x|))$-in one-out quantum circuit Q of size at most $s(|x|)$,*

$$\left|\langle 1|Q\big((\Phi_x \otimes I_{2^{k(|x|)}})(\xi_x)\big)|1\rangle - \langle 1|Q\big((\Psi_x \otimes I_{2^{k(|x|)}})(\xi_x)\big)|1\rangle\right| < \frac{1}{p(|x|)}.$$

In what follows, we will often use the term "computationally indistinguishable" instead of "polynomially quantum indistinguishable" for simplicity. Also, we will often informally say that mixed states ρ_x and σ_x or admissible transformations Φ_x and Ψ_x are computationally indistinguishable when $x \in S$ to mean that the ensembles $\{\rho_x \colon x \in S\}$ and $\{\sigma_x \colon x \in S\}$ or $\{\Phi_x \colon x \in S\}$ and $\{\Psi_x \colon x \in S\}$ are polynomially quantum indistinguishable.

Quantum zero-knowledge proofs For readability, in what follows, the arguments x and $|x|$ are often dropped in various functions. It is assumed that operators acting on subsystems of a given system are extended to the entire system by tensoring with the identity, as it will be clear from the context upon what part of a system a given operator acts. Although all the statements in this paper can be proved only in terms of languages without using promise problems [5], in what follows we define models and prove statements in terms of promise problems, for generality and for the compatibility with some other studies on quantum zero-knowledge proofs [25, 17, 27, 3]. This paper follows a manner in Ref. [25] when defining various honest-verifier quantum zero-knowledge proofs, and that in Ref. [27] when defining various general quantum zero-knowledge proofs.

We start with formally defining quantum verifiers and quantum provers. An *m-message* quantum verifier V is a mapping of the form $V\colon \{0,1\}^* \to \{0,1\}^*$. For every input $x \in \{0,1\}^*$, the string $V(x)$ is interpreted as a $\lceil (m(|x|)+1)/2 \rceil$-tuple $(V(x)_1, \ldots, V(x)_{\lceil (m(|x|)+1)/2 \rceil})$, with each $V(x)_j$ a description of a polynomial-size quantum circuit acting over the qubits in the verifier's private space and message qubits. A quantum verifier V is *uniform* if the corresponding mapping V is polynomial-time computable, and is *non-uniform* if no restrictions are placed on the complexity of the mapping V (but each circuit $V(x)_j$ must have size polynomial in $|x|$). Similarly, an *m-message* quantum prover P is a mapping of the form $P\colon \{0,1\}^* \to \{0,1\}^*$. For every input $x \in \{0,1\}^*$, the string $P(x)$ is interpreted as a $\lceil m(|x|)/2 \rceil$-tuple $(P(x)_1, \ldots, P(x)_{\lceil m(|x|)/2 \rceil})$, with each $P(x)_j$ a description of a quantum circuit acting over the qubits in the prover's private space and message qubits. No restrictions are placed on the complexity of the mapping P, and each $P(x)_j$ can be an arbitrary unitary transformation.

First we define the notions of various *honest-verifier* quantum zero-knowledge proofs. Given a quantum verifier V and a quantum prover P, let $\mathrm{view}_{V,P}(x,j)$ be the quantum state that V possesses immediately after the jth transformation of P during an execution of the protocol between V and P. Now we define the classes $\mathrm{HVQPZK}(m,c,s)$, $\mathrm{HVQSZK}(m,c,s)$, and $\mathrm{HVQZK}(m,c,s)$ of problems having m-message honest-verifier quantum perfect, statistical, and computational zero-knowledge proof systems, respectively, with completeness at least c and soundness at most s.

Definition 11. *Given functions $m \in \mathrm{poly}$ and $c, s\colon \mathbb{Z}^+ \to [0,1]$, a problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ is in $\mathrm{HVQPZK}(m,c,s)$ ($\mathrm{HVQSZK}(m,c,s)$) [$\mathrm{HVQZK}(m,c,s)$] iff there exist an m-message uniform honest quantum verifier V and an m-message honest quantum prover P such that*

(Completeness and Soundness) *(V,P) forms an m-message quantum interactive proof system with completeness at least c and soundness at most s,*

(Honest-Verifier Zero-Knowledge) *there exists a polynomial-time preparable ensemble $\{S_V(x,j)\}$ of quantum states such that $S_V(x,j) = \mathrm{view}_{V,P}(x,j)$ for every $x \in A_{\mathrm{yes}}$ and $j \in T$ ($\|S_V(x,j) - \mathrm{view}_{V,P}(x,j)\|_{\mathrm{tr}}$ is negligible with respect to $|x|$ for all but finitely many $(x,j) \in A_{\mathrm{yes}} \times T$) [the ensembles $\{S_V(x,j)\colon (x,j) \in A_{\mathrm{yes}} \times T\}$ and $\{\mathrm{view}_{V,P}(x,j)\colon (x,j) \in A_{\mathrm{yes}} \times T\}$ are polynomially quantum indistinguishable], where $T = \bigl\{1, \ldots, \lceil \frac{m(|x|)}{2} \rceil\bigr\}$.*

Using these, we define the classes HVQPZK, HVQSZK, and HVQZK of problems having honest-verifier quantum perfect, statistical, and computational zero-knowledge proof systems, respectively.

Definition 12. *A problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ is in* HVQPZK *(*HVQSZK*) [*HVQZK*] if there exists a function $m \in \mathrm{poly}$ such that A is in* $\mathrm{HVQPZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$ *(*$\mathrm{HVQSZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$*) [*$\mathrm{HVQZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$*].*

Note that it is easy to see that we can amplify the success probability of honest-verifier quantum perfect/statistical/computational zero-knowledge proof systems by sequential repetition, which justifies Definition 12.

Next we define the notions of various quantum zero-knowledge proofs. Let V be an arbitrary non-uniform quantum verifier. Suppose that V possesses some auxiliary quantum state in $\mathbf{D}(\mathcal{A})$ at the beginning and possesses some quantum state in $\mathbf{D}(\mathcal{Z})$ after having received the last message from the prover, for some Hilbert spaces $\mathcal{A}$ and $\mathcal{Z}$. For such V, for any quantum prover P, and for every $x \in \{0,1\}^*$, let $\langle V, P\rangle(x)$ denote the admissible transformation in $\mathbf{T}(\mathcal{A}, \mathcal{Z})$ induced by the interaction between V and P on input x. Note that the last transformation of V is *not* considered as a part of the interaction, since we want to focus on the state V would possess immediately after having received the last message from P. We call this $\langle V, P\rangle(x)$ the *induced admissible transformation* from V, P, and x. We define the classes $\mathrm{QPZK}(m, c, s)$, $\mathrm{QSZK}(m, c, s)$, and $\mathrm{QZK}(m, c, s)$ of problems having m-message quantum perfect, statistical, and computational zero-knowledge proof systems, respectively, with completeness at least c and soundness at most s, as follows.

Definition 13. *Given functions $m \in \mathrm{poly}$ and $c, s \colon \mathbb{Z}^+ \to [0,1]$, a problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ is in* $\mathrm{QPZK}(m, c, s)$ *(*$\mathrm{QSZK}(m, c, s)$*) [*$\mathrm{QZK}(m, c, s)$*] iff there exist an m-message uniform honest quantum verifier V and an m-message honest quantum prover P such that*

(Completeness and Soundness) *(V, P) forms an m-message quantum interactive proof system with completeness at least c and soundness at most s,*

(Zero-Knowledge) *there exists a polynomial-time uniformly generated family $\{Q_{x,y}\}$ of quantum circuits such that, for any m-message non-uniform quantum verifier V', the circuit $Q_{x,V'(x)}$ exactly implements an admissible transformation $S_{V'}(x)$ such that $S_{V'}(x) = \langle V', P\rangle(x)$ for every $x \in A_{\mathrm{yes}}$ ($\|S_{V'}(x) - \langle V', P\rangle(x)\|_{\diamond}$ is negligible with respect to $|x|$ for all but finitely many $x \in A_{\mathrm{yes}}$) [the ensembles $\{S_{V'}(x) \colon x \in A_{\mathrm{yes}}\}$ and $\{\langle V', P\rangle(x) \colon x \in A_{\mathrm{yes}}\}$ are polynomially quantum indistinguishable], where $\langle V', P\rangle(x)$ is the induced admissible transformation from V', P, and x.*

Using these, we define the classes QPZK, QSZK, and QZK of problems having quantum perfect, statistical, and computational zero-knowledge proof systems, respectively.

Definition 14. *A problem $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ is in* QPZK *(*QSZK*) [*QZK*] if there exists a function $m \in \mathrm{poly}$ such that A is in* $\mathrm{QPZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$ *(*$\mathrm{QSZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$*) [*$\mathrm{QZK}\left(m, \frac{2}{3}, \frac{1}{3}\right)$*].*

Again note that it is not hard to see that we can amplify the success probability of quantum perfect/statistical/computational zero-knowledge proof systems by sequential repetition, which justifies Definition 14.

In the classical case, the most common definition of perfect zero-knowledge proofs would be the one that allows the simulator to output "FAIL" with small probability, say, with probability at most $\frac{1}{2}$ [7, 22]. Adopting this convention leads to alternative definitions of honest-verifier and general quantum perfect zero-knowledge proof systems. At a glance, the two types of definitions seem likely to form different complexity classes of quantum perfect zero-knowledge proofs. Fortunately, it is proved in Section 6 that the two types of definitions result in the same complexity class of quantum perfect zero-knowledge proofs. Such equivalence is not known in the classical case.

3 Computational Zero-Knowledge Case

We start with showing that any *honest-verifier* quantum computational zero-knowledge proof system with two-sided bounded error can be transformed into one with perfect completeness (if the completeness error in the original proof system is negligible, which may be assumed without loss of generality since the success probability can be amplified by sequential repetition). This can be basically proved by using a method for usual quantum interactive proofs due to Kitaev and Watrous (Theorem 2 of Ref. [16]), but now it is necessary for the honest-verifier zero-knowledge property to carefully and explicitly construct a protocol for the honest prover. The proof is found in the full version of this paper [18].

Lemma 15. *Let $m \in \mathrm{poly}$, let $\varepsilon \colon \mathbb{Z}^+ \to [0,1]$ be any negligible function such that there exists a polynomial-time uniformly generated family $\{Q_x\}$ of quantum circuits such that Q_{1^n} exactly performs the unitary transformation $U_{\varepsilon(n)} = \begin{pmatrix} \sqrt{\varepsilon(n)} & \sqrt{1-\varepsilon(n)} \\ \sqrt{1-\varepsilon(n)} & -\sqrt{\varepsilon(n)} \end{pmatrix}$, and let $\delta \colon \mathbb{Z}^+ \to [0,1]$ be any function that satisfies $\delta > \varepsilon$. Then,* $\mathrm{HVQZK}(m, 1-\varepsilon, 1-\delta) \subseteq \mathrm{HVQZK}(m+2, 1, 1-(\delta-\varepsilon)^2)$.

Next we show that any honest-verifier quantum computational zero-knowledge proof system that involves polynomially many messages can be parallelized to one that involves only three messages. This can be achieved again by applying a method in usual quantum interactive proofs due to Kitaev and Watrous (Theorem 4 of Ref. [16]). The main idea in their parallelization protocol is that the verifier receives each snapshot state of the underlying proof system as the first message, and then checks if the following three properties are satisfied: (i) the first snapshot state is a legal state in the underlying proof system after the first message, (ii) the last snapshot state can make the original verifier accept, and (iii) any two consecutive snapshot states are indeed transformable with each other by one round of communication. The verifier first checks if the conditions (i) and (ii) really hold for the received snapshot states. He then randomly chooses a consecutive pair of the snapshot states and challenges the prover to show the transformability from one to the other. It is straightforward to show that their construction preserves the honest-verifier zero-knowledge property.

Lemma 16. *Let* $m \in \mathrm{poly}$ *and let* $\delta \colon \mathbb{Z}^+ \to [0,1]$ *be any function. Then,* $\mathrm{HVQZK}(m,1,1-\delta) \subseteq \mathrm{HVQZK}\bigl(3,1,1-\frac{\delta^2}{4m^2}\bigr)$.

Finally we show that any three-message honest-verifier quantum computational zero-knowledge proof system can be transformed into a three-message public-coin one in which the message from the verifier consists of only one classical bit. Marriott and Watrous (Theorem 5.4 of Ref. [19]) showed such a transformation in the case of usual quantum interactive proofs. In their construction, the verifier first receives a state that is supposed to be the reduced state in the verifier's private space after the second message in the original proof system, and then challenges the prover to recover either the state the original verifier would have after the first message or that after the third message, depending on the outcome of the public coin-flip. It is easy to show that their construction preserves the honest-verifier zero-knowledge property.

Lemma 17. *Let* $c, s \colon \mathbb{Z}^+ \to [0,1]$ *be any functions that satisfy* $c^2 > s$. *Then, any problem in* $\mathrm{HVQZK}(3,c,s)$ *has a three-message public-coin honest-verifier quantum computational zero-knowledge proof system with completeness at least* $\frac{1+c}{2}$ *and soundness at most* $\frac{1+\sqrt{s}}{2}$ *in which the message from the verifier consists of only one classical bit.*

Now we can use the quantum rewinding technique due to Watrous [27] to show that any three-message public-coin honest-verifier quantum computational zero-knowledge proof system in which the message from the verifier consists of only one classical bit is computational zero-knowledge even against any dishonest non-uniform quantum verifier.

Lemma 18. *Any three-message public-coin honest-verifier quantum computational zero-knowledge proof system such that the message from the verifier consists of only one classical bit is computational zero-knowledge against any non-uniform quantum verifier.*

Proof. Let $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ be a problem having a three-message public-coin honest-verifier quantum computational zero-knowledge proof system such that the message from the verifier consists of only one classical bit. Let V and P be the corresponding honest quantum verifier and honest quantum prover, respectively. Let M and N be the quantum registers sent to V at the first message and at the third message, respectively, and let R and S be the single-qubit registers that are used to store the classical information representing the outcome b of a public coin flipped by V, where R is inside the private space of V and S is sent to P.

Simulator for General Verifier $\boldsymbol{W}$

1. Store the auxiliary quantum state ρ in the quantum register X. Prepare the quantum registers S, W, M, N, R, and A, and further prepare a single-qubit quantum register F. Initialize all the qubits in F, S, W, M, N, R, and A to state $|0\rangle$.
2. Apply the generating circuit Q of the quantum state $S_V(x, 2)$ to the qubits in $(\mathsf{M}, \mathsf{N}, \mathsf{R}, \mathsf{A})$.
3. Apply W_1 to the qubits in $(\mathsf{S}, \mathsf{W}, \mathsf{X}, \mathsf{M})$, where W_1 is the first transformation of the simulated verifier W.
4. Compute the exclusive-or of the contents of R and S and write the result in F.
5. Measure the qubit in F in the $\{|0\rangle, |1\rangle\}$ basis. If this results in $|0\rangle$, output the qubits in $(\mathsf{W}, \mathsf{X}, \mathsf{M}, \mathsf{N}, \mathsf{R})$, otherwise apply $W_1^\dagger$ to the qubits in $(\mathsf{S}, \mathsf{W}, \mathsf{X}, \mathsf{M})$ and then apply $Q^\dagger$ to the qubits in $(\mathsf{M}, \mathsf{N}, \mathsf{R}, \mathsf{A})$.
6. Apply the phase-flip if all the qubits in F, S, W, M, N, R, and A are in state $|0\rangle$, apply Q to the qubits in $(\mathsf{M}, \mathsf{N}, \mathsf{R}, \mathsf{A})$, and apply W_1 to the qubits in $(\mathsf{S}, \mathsf{W}, \mathsf{X}, \mathsf{M})$. Output the qubits in $(\mathsf{W}, \mathsf{X}, \mathsf{M}, \mathsf{N}, \mathsf{R})$.

Fig. 1. Simulator for a general verifier W.

Let S_V be the simulator for V such that, if x is in A_{yes}, the states $S_V(x, 1)$ and $\mathrm{view}_{V,P}(x, 1)$ consisting of qubits in M are computationally indistinguishable and the states $S_V(x, 2)$ and $\mathrm{view}_{V,P}(x, 2)$ consisting of qubits in $(\mathsf{M}, \mathsf{N}, \mathsf{R})$ are also computationally indistinguishable.

Consider a generating circuit Q of the quantum state $S_V(x, 2)$. Without loss of generality, it is assumed that Q acts over the qubits in $(\mathsf{M}, \mathsf{N}, \mathsf{R}, \mathsf{A})$, where A is the quantum register consisting of $q_{\mathcal{A}}$ qubits for some $q_{\mathcal{A}} \in \mathrm{poly}$. For any non-uniform quantum verifier W and any auxiliary quantum state ρ for W stored in the quantum register X inside the private space of W, we construct an efficiently implementable admissible mapping Φ that corresponds to a simulator T_W for W. Without loss of generality it is assumed that the message from W consists of a single *classical* bit, since the honest prover can easily enforce this constraint by measuring the message from the verifier before responding to it. Let W be the quantum register consisting of all the qubits in the private space of W except for those in X and M after the second message having been sent. We consider the procedure described in Fig. 1, which is the implementation of Φ.

Suppose that the input x is in A_{yes}. We shall show that (i) the gap between $\frac{1}{2}$ and the probability of obtaining $|0\rangle$ as the measurement result in Step 5 must be negligible regardless of the auxiliary quantum state ρ, and (ii) the output state in Step 5 in the construction conditioned on the measurement result being $|0\rangle$ must be computationally indistinguishable from the state W would possess after the third message. With these two properties, the quantum rewinding technique due to Watrous [27] works well, by using the amplification lemma for the case with negligible perturbations, which is also due to Watrous [27]. This ensures the computational zero-knowledge property against W.

For the generating circuit Q' of the quantum state $\mathrm{view}_{V,P}(x,2)$ (here no restrictions are placed on the size of Q'), consider the "ideal" construction of the simulator such that Q' is applied instead of Q in Step 2 of the "real" simulator construction.

We first show the property (i).

Since the state $\mathrm{view}_{V,P}(x,2)$ can be written of the form $\mathrm{view}_{V,P}(x,2) = \frac{1}{2}(\sigma_0 \otimes |0\rangle\langle 0| + \sigma_1 \otimes |1\rangle\langle 1|)$ for some quantum states σ_0 and σ_1 in (M,N), the probability of obtaining $|0\rangle$ as the measurement result in Step 5 in the "ideal" construction is exactly equal to $\frac{1}{2}$ regardless of the auxiliary quantum state ρ, because $\mathrm{tr}_{\mathcal{N}}\sigma_0 = \mathrm{tr}_{\mathcal{N}}\sigma_1$ necessarily holds in this case, where $\mathcal{N}$ is the Hilbert space corresponding to N.

Now, from the honest-verifier computational zero-knowledge property, the states $S_V(x,2)$ and $\mathrm{view}_{V,P}(x,2)$ in $(\mathsf{M},\mathsf{N},\mathsf{R})$ are computationally indistinguishable. Since the circuit implementing W_1 is of size polynomial with respect to $|x|$, it follows that the gap between $\frac{1}{2}$ and the probability of obtaining $|0\rangle$ as the measurement result in Step 5 in the "real" construction must be negligible regardless of the auxiliary quantum state ρ, which proves the property (i).

Now we show the property (ii).

Let $\xi_i = \Pi_i W_1(|0_{\mathcal{S}\otimes\mathcal{W}}\rangle\langle 0_{\mathcal{S}\otimes\mathcal{W}}| \otimes \rho \otimes \sigma_i \otimes |i\rangle\langle i|)W_1^{\dagger}\Pi_i$ be an unnormalized state in $(\mathsf{S},\mathsf{W},\mathsf{X},\mathsf{M},\mathsf{N},\mathsf{R})$ for each $i \in \{0,1\}$, where $\Pi_i = |i\rangle\langle i|$ is the projection operator over the qubit in S, and $\mathcal{S}$ and $\mathcal{W}$ are the Hilbert spaces corresponding to S and W, respectively. Then, in the "ideal" construction, conditioned on the measurement result being $|0\rangle$ in Step 5, the output is the state $\mathrm{tr}_{\mathcal{S}}(\xi_0 + \xi_1)$.

Noticing that $\mathrm{tr}_{\mathcal{S}}\frac{\xi_i}{\mathrm{tr}\xi_i}$ is exactly the state the verifier W would possess after the third message when the second message from W is i and that the probability of the second message from W being i is exactly equal to $\mathrm{tr}\xi_i$ for each $i \in \{0,1\}$, $\mathrm{tr}_{\mathcal{S}}(\xi_0 + \xi_1) = \mathrm{tr}\xi_0 \cdot \mathrm{tr}_{\mathcal{S}}\frac{\xi_0}{\mathrm{tr}\xi_0} + \mathrm{tr}\xi_1 \cdot \mathrm{tr}_{\mathcal{S}}\frac{\xi_1}{\mathrm{tr}\xi_1}$ is exactly the state W would possess after the third message.

Towards a contradiction, suppose that the output state in Step 5 in the "real" construction conditioned on the measurement result being $|0\rangle$ is computationally distinguishable from $\mathrm{tr}_{\mathcal{S}}(\xi_0 + \xi_1)$. Let D be the corresponding distinguisher that uses the auxiliary quantum state ρ'. We construct a distinguisher D' for $S_V(x,2)$ and $\mathrm{view}_{V,P}(x,2)$ from D.

On input quantum state η that is either $S_V(x,2)$ or $\mathrm{view}_{V,P}(x,2)$, D' uses the auxiliary quantum state $\rho \otimes \rho'$, where ρ is the auxiliary quantum state the verifier W would use. D' prepares the quantum registers S, W, M, N, R and another quantum register Y. D' stores ρ in the register X, η in the register $(\mathsf{M},\mathsf{N},\mathsf{R})$, and ρ' in Y. All the qubits in S and W are initialized to state $|0\rangle$. Now D' applies W_1 to the qubits in $(\mathsf{S},\mathsf{W},\mathsf{X},\mathsf{M})$, and then applies D to the qubits in $(\mathsf{W},\mathsf{X},\mathsf{M},\mathsf{N},\mathsf{R},\mathsf{Y})$.

It is obvious from this construction that D' with the auxiliary quantum state $\rho \otimes \rho'$ forms a distinguisher for $S_V(x,2)$ and $\mathrm{view}_{V,P}(x,2)$ if D with the auxiliary quantum state ρ' forms a distinguisher for the output state in Step 5 in the "real" simulator construction conditioned on the measurement result being $|0\rangle$ and the state $\mathrm{tr}_{\mathcal{S}}(\xi_0 + \xi_1)$. This contradicts the computational indistinguishability between $S_V(x, 2)$ and $\mathrm{view}_{V,P}(x, 2)$, and thus the property (ii) follows. □

Now we are ready to show Theorem 1 that states HVQZK = QZK.

Proof (of Theorem 1). It is trivial that HVQZK ⊇ QZK, and we show that HVQZK ⊆ QZK. From Lemma 15, we can start with an m-message honest-verifier quantum computational zero-knowledge proof system of perfect completeness with soundness at most $1 - \delta$ for some $m \in \mathrm{poly}$ and δ such that $1 - \delta$ is polynomially bounded away from one. Now from Lemmas 16 and 17 together with Lemma 18, we have that $\mathrm{HVQZK}(m, 1, 1-\delta) \subseteq \mathrm{HVQZK}(3, 1, 1-\delta') \subseteq \mathrm{QZK}\left(3, 1, \frac{1+\sqrt{1-\delta'}}{2}\right)$, where $\delta' = \frac{\delta^2}{4m^2}$. Finally, the sequential repetition establishes HVQZK ⊆ QZK. □

This simultaneously shows Theorem 2, the equivalence of public-coin and general quantum computational zero-knowledge proofs, and Theorem 3, the equivalence of quantum computational zero-knowledge proofs of perfect completeness and general ones.

To show Theorem 4, we need another two properties. First, it is trivial that parallel repetition of honest-verifier quantum zero-knowledge proofs preserves the honest-verifier zero-knowledge property. Together with the perfect parallel repetition theorem for three-message quantum interactive proofs due to Kitaev and Watrous (Theorem 6 of Ref. [16]), this implies the following.

Lemma 19. *Let $c, s \colon \mathbb{Z}^+ \to [0, 1]$ be any functions such that $c > s$. Then, for any $k \in \mathrm{poly}$, $\mathrm{HVQZK}(3, c, s) \subseteq \mathrm{HVQZK}(3, c^k, s^k)$.*

Second, it is easy to extend Lemma 18 to the following more general statement.

Lemma 20. *Any three-message public-coin honest-verifier quantum computational zero-knowledge proof system such that the message from the verifier consists of $O(\log n)$ bits for every input of length n is computational zero-knowledge against any non-uniform quantum verifier.*

Now Theorem 4 can be proved as follows.

Proof (of Theorem 4). For any $p \in \mathrm{poly}$, take $q \in \mathrm{poly}$ such that $2^{\frac{q}{2}} \geq \log p + 2$. Then, from Lemmas 15, 16, and 19, we have that $\mathrm{HVQZK} \subseteq \mathrm{HVQZK}(3, 1, 2^{-q})$. With Lemma 17, this further implies that any problem in HVQZK has a three-message public-coin honest-verifier quantum computational zero-knowledge proof system of perfect completeness with soundness at most $\frac{1}{2} + 2^{-\frac{q}{2}-1}$ in which the message from the verifier consists of only one classical bit. For every input of length n, we run this proof system $\lceil \log p(n) \rceil + 2$ times in parallel. From Lemma 19, this results in a three-message public-coin honest-verifier quantum computational zero-knowledge proof system of perfect completeness with soundness at most $\frac{1}{4p(n)}\left(1 + 2^{-\frac{q(n)}{2}}\right)^{\lceil \log p(n) \rceil + 2} \leq \frac{1}{p(n)}$ in which the message from the verifier consists of $\lceil \log p(n) \rceil + 2$ bits. Now Lemma 20 ensures that this proof system is computational zero-knowledge even against any dishonest quantum verifier. □

4 Statistical Zero-Knowledge Case

All the properties shown for the computational zero-knowledge case also hold for the statistical zero-knowledge case. The proofs are essentially same as in the computational zero-knowledge case. This proves Theorems 5 and 6, and also gives alternative proofs of the facts that HVQSZK = QSZK and that public-coin quantum statistical zero-knowledge equals general quantum statistical zero-knowledge, which were first shown by Watrous [27] using his previous results [25].

5 Perfect Zero-Knowledge Case

Now we move to the perfect zero-knowledge case. Although our approach for the computational and statistical zero-knowledge cases basically works well even for the perfect zero-knowledge case, some of our transformations do not preserve the *perfect* zero-knowledge property. In particular, our method of making proof systems perfectly complete no longer works well for quantum perfect zero-knowledge case, and we need to use a slightly modified parallelization method.

As mentioned in Section 3, the verifier in the Kitaev-Watrous parallelization protocol checks if the last snapshot state can make the original verifier accept *before* proceeding to the test for consecutivity. The problem arises here, in the check for the last snapshot state, when parallelizing an honest-verifier quantum perfect zero-knowledge proof system with *imperfect* completeness. Because of imperfect completeness, the verifier's check can fail even if the honest prover prepares every snapshot state honestly, which means that the verifier's check causes a small perturbation to the snapshot states. Now we have difficulty in *perfectly* simulating the behavior of the honest prover with respect to these perturbed states, which spoils the perfect zero-knowledge property.

To avoid this difficulty, we modify the parallelization protocol as follows. Our basic idea is to postpone the verifier's check for the last snapshot state until after the third message. At the final verification of the verifier, with equal probability he either carries out the postponed check for the last snapshot state or just carries out the original final verification procedure. Now the honest-verifier perfect zero-knowledge property becomes straightforward, since there is no perturbation to all the snapshot states until after the last transformation of the verifier. The completeness accepting probability cannot be worse than that in the original protocol. However, the soundness condition now becomes a bit harder to prove, because we can no longer assume that the last snapshot state prepared by a dishonest prover makes the original verifier accept, when analyzing the probability to pass the transformability test for two consecutive snapshot states. Nevertheless, we can show that our modified parallelization protocol above indeed works well, and we have the following lemma. The proof is found in the full version of this paper [18].

Lemma 21. *Let* $m \in \mathrm{poly}$ *be such that* $m \geq 4$ *and let* $\varepsilon, \delta \colon \mathbb{Z}^+ \to [0,1]$ *be any functions such that* $\varepsilon < \frac{\delta^2}{16(m+1)^2}$. *Then,* $\mathrm{HVQPZK}(m, 1-\varepsilon, 1-\delta) \subseteq \mathrm{HVQPZK}\bigl(3, 1-\frac{\varepsilon}{2}, 1-\frac{\delta^2}{32(m+1)^2}\bigr)$.

For Lemmas 17 and 18, exactly the same constructions can be used to show their perfect zero-knowledge versions. Putting things together, we have Theorem 7 that states HVQPZK = QPZK, and Theorem 8, the equivalence of public-coin and general quantum perfect zero-knowledge proofs.

6 Equivalence of Two Definitions of Quantum Perfect Zero-Knowledge

In the classical case, the most common definition of perfect zero-knowledge proofs would be the one that allows the simulator to output "FAIL" with small probability [7, 22]. Adopting this convention leads to the following alternative definitions of honest-verifier and general quantum perfect zero-knowledge proof systems.

Definition 22. *Given functions* $m \in \mathrm{poly}$ *and* $c, s\colon \mathbb{Z}^+ \to [0,1]$*, a problem* $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ *is in* $\mathrm{HVQPZK}'(m, c, s)$ *iff there exist an* m*-message uniform honest quantum verifier* V *and an* m*-message honest quantum prover* P *such that*

(Completeness and Soundness) (V, P) *forms an* m*-message quantum interactive proof system with completeness at least* c *and soundness at most* s*,*

(Honest-Verifier Perfect Zero-Knowledge) *there exists a polynomial-time preparable ensemble* $\{S_V(x, j)\}$ *of quantum states such that* $S_V(x, j) = p_{x,j}|0\rangle\langle 0| \otimes |0_{\mathcal{H}_j}\rangle\langle 0_{\mathcal{H}_j}| + (1 - p_{x,j})|1\rangle\langle 1| \otimes \mathrm{view}_{V,P}(x, j)$ *for some* $0 \leq p_{x,j} \leq \frac{1}{2}$*, for every* $x \in A_{\mathrm{yes}}$ *and for each* $1 \leq j \leq \lceil \frac{m(|x|)}{2} \rceil$*, where* $\mathcal{H}_j$ *is the Hilbert space such that* $\mathrm{view}_{V,P}(x, j)$ *is in* $\mathbf{D}(\mathcal{H}_j)$*.*

Definition 23. *Given functions* $m \in \mathrm{poly}$ *and* $c, s\colon \mathbb{Z}^+ \to [0,1]$*, a problem* $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ *is in* $\mathrm{QPZK}'(m, c, s)$ *iff there exist an* m*-message uniform honest quantum verifier* V *and an* m*-message honest quantum prover* P *such that*

(Completeness and Soundness) (V, P) *forms an* m*-message quantum interactive proof system with completeness at least* c *and soundness at most* s*,*

(Perfect Zero-Knowledge) *there exists a polynomial-time uniformly generated family* $\{Q_{x,y}\}$ *of quantum circuits such that, for any* m*-message non-uniform quantum verifier* V'*, the circuit* $Q_{x,V'(x)}$ *exactly implements an admissible transformation* $S_{V'}(x)$ *such that, for every* $x \in A_{\mathrm{yes}}$*,* $S_{V'}(x) = p_x(\Phi_0 \otimes \Psi_{\mathrm{fail}}) + (1 - p_x)(\Phi_1 \otimes \langle V', P\rangle(x))$ *for some* $0 \leq p_x \leq \frac{1}{2}$*, where* $\langle V', P\rangle(x) \in \mathbf{T}(\mathcal{A}, \mathcal{Z})$ *is the induced admissible transformation from* V'*,* P*, and* x *for some Hilbert spaces* $\mathcal{A}$ *and* $\mathcal{Z}$*,* $\Psi_{\mathrm{fail}} \in \mathbf{T}(\mathcal{A}, \mathcal{Z})$ *is the admissible transformation that always outputs* $|0_{\mathcal{Z}}\rangle\langle 0_{\mathcal{Z}}|$*, and* Φ_b *is the admissible transformation that takes nothing as input and outputs* $|b\rangle\langle b|$*, for each* $b \in \{0, 1\}$*.*

In Definitions 22 and 23, the first qubit of the output of the simulator indicates whether or not the simulation succeeds — $|0\rangle\langle 0|$ is interpreted as failure and $|1\rangle\langle 1|$ as success.

Definition 24. *A problem* $A = \{A_{\mathrm{yes}}, A_{\mathrm{no}}\}$ *is in* HVQPZK' *(*QPZK'*) if there exists a function* $m \in \mathrm{poly}$ *such that* A *is in* $\mathrm{HVQPZK}'\left(m, \frac{2}{3}, \frac{1}{3}\right)$ *(*$\mathrm{QPZK}'\left(m, \frac{2}{3}, \frac{1}{3}\right)$*).*

It is not obvious at a glance that $\mathrm{HVQPZK} = \mathrm{HVQPZK}'$ and $\mathrm{QPZK} = \mathrm{QPZK}'$, i.e., that the definitions of honest-verifier and general quantum perfect zero-knowledge proof systems using Definitions 11 and 13 is equivalent to those using Definitions 22 and 23. Fortunately, with Theorem 7, we can show that $\mathrm{HVQPZK} = \mathrm{HVQPZK}'$ and $\mathrm{QPZK} = \mathrm{QPZK}'$. It is stressed that such equivalence is not known in the classical case.

Theorem 25. $\mathrm{HVQPZK} = \mathrm{HVQPZK}'$ *and* $\mathrm{QPZK} = \mathrm{QPZK}'$*.*

Note that $\mathrm{QPZK} \subseteq \mathrm{QPZK}' \subseteq \mathrm{HVQPZK}'$ is obvious. From Theorem 7, we have $\mathrm{HVQPZK} = \mathrm{QPZK}$. Therefore, to show Theorem 25, it is sufficient to show that $\mathrm{HVQPZK}' \subseteq \mathrm{HVQPZK}$. Now, the idea is to modify the protocol of the honest prover for the HVQPZK' system so that the honest prover "adjusts" his behavior to that of the simulator, i.e., he privately runs the simulator and intentionally fails to return the correct response whenever the simulator fails. The detailed proof is found in the full version of this paper [18].

Acknowledgement. The author is grateful to John Watrous for his helpful comments on the choice of the universal gate set. The author would also like to thank anonymous referees for their helpful suggestions for improving this paper. This work is supported by the Strategic Information and Communications R&D Promotion Programme No. 031303020 of the Ministry of Internal Affairs and Communications of Japan.

References

1. D. Aharonov, A. Yu. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998.
2. W. Aiello and J. Håstad. Statistical zero-knowledge languages can be recognized in two rounds. *Journal of Computer and System Sciences*, 42(3):327–345, 1991.
3. A. Ben-Aroya and A. Ta-Shma. Quantum expanders and the quantum entropy difference problem. arXiv.org e-Print archive, quant-ph/0702129, 2007.
4. I. Damgård, S. Fehr, and L. Salvail. Zero-knowledge proofs and string commitments withstanding quantum attacks. In *Advances in Cryptology – CRYPTO 2004, 24th Annual International Cryptology Conference*, volume 3152 of *Lecture Notes in Computer Science*, pages 254–272, 2004.
5. 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.
6. L. J. Fortnow. The complexity of perfect zero-knowledge. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 327–343. JAI Press, 1989.

7. O. Goldreich. *Foundations of Cryptography – Volume I Basic Tools.* Cambridge University Press, 2001.
8. O. Goldreich. Zero-knowledge twenty years after its invention. Electronic Colloquium on Computational Complexity, Report No. 63, 2002.
9. O. Goldreich and S. Goldwasser. On the limits of nonapproximability of lattice problems. *Journal of Computer and System Sciences*, 60(3):540–463, 2000.
10. O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(3):691–729, 1991.
11. 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.
12. O. Goldreich and S. P. Vadhan. Comparing entropies in statistical zero knowledge with applications to the structure of SZK. In *Fourteenth Annual IEEE Conference on Computational Complexity*, pages 54–73, 1999.
13. S. Goldwasser, S. Micali, and C. W. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.
14. 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.
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. A. Yu. Kitaev and J. H. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 608–617, 2000.
17. H. Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In *Algorithms and Computation, 14th International Symposium, ISAAC 2003*, volume 2906 of *Lecture Notes in Computer Science*, pages 178–188, 2003.
18. H. Kobayashi. General properties of quantum zero-knowledge proofs. arXiv.org e-Print archive, arXiv:0705.1129 [quant-ph], 2007.
19. C. Marriott and J. H. Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.
20. M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.
21. T. Okamoto. On relationships between statistical zero-knowledge proofs. *Journal of Computer and System Sciences*, 60(1):47–108, 2000.
22. A. Sahai and S. P. Vadhan. A complete problem for statistical zero knowledge. *Journal of the ACM*, 50(2):196–249, 2003.
23. P. W. Shor. Fault-tolerant quantum computation. In *37th Annual Symposium on Foundations of Computer Science*, pages 56–65, 1996.
24. S. P. Vadhan. An unconditional study of computational zero-knowledge. *SIAM Journal on Computing*, 36(4):1160–1214, 2006.
25. 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.
26. J. H. Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.
27. J. H. Watrous. Zero-knowledge against quantum attacks. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, pages 296–305, 2006.