Cryptographic Characterization of Quantum Advantage

Tomoyuki Morimae
Kyoto University
Kyoto, Japan
tomoyuki.morimae@yukawa.kyoto-u.ac.jp

Yuki Shirakawa
Kyoto University
Kyoto, Japan
yuki.shirakawa@yukawa.kyoto-u.ac.jp

Takashi Yamakawa
NTT Social Informatics Laboratories
Tokyo, Japan
Kyoto University
Kyoto, Japan
takashi.yamakawa@ntt.com

Abstract

Quantum computational advantage refers to an existence of computational tasks that are easy for quantum computing but hard classically. Unconditionally showing quantum advantage is beyond our current understanding of complexity theory, and therefore some computational assumptions are needed. Which complexity assumption is necessary and sufficient for quantum advantage? In this paper, we show that inefficient-verifier proofs of quantumness (IV-PoQ) exist if and only if classically-secure one-way puzzles (OWPuzzs) exist. As far as we know, this is the first time that a complete cryptographic characterization of quantum advantage is obtained. IV-PoQ are a generalization of proofs of quantumness (PoQ) where the verifier is efficient during the interaction but may use unbounded time afterward. IV-PoQ capture various types of quantum advantage previously studied, such as sampling and search based quantum advantage. Previous work [Morimae and Yamakawa, Crypto 2024] showed that IV-PoQ can be constructed from OWFs, but a construction of IV-PoQ from weaker assumptions was left open. Our result solves the open problem, because OWPuzzs are believed to be weaker than OWFs. OWPuzzs are one of the most fundamental quantum cryptographic primitives implied by many quantum cryptographic primitives weaker than one-way functions (OWFs), such as pseudorandom unitaries (PRUs), pseudorandom state generators (PRSGs), and one-way state generators (OWSGs). The equivalence between IV-PoQ and classically-secure OWPuzzs therefore highlights that if there is no quantum advantage, then these fundamental cryptographic primitives do not exist. The equivalence also means that quantum advantage is an example of the applications of OWPuzzs. Except for commitments, no application of OWPuzzs was known before. Our result shows that quantum advantage is another application of OWPuzzs, which solves the open question of [Chung, Goldin, and Gray, Crypto 2024]. Moreover, it is the first quantum-computation-classical-communication (QCCC) application of OWPuzzs. To show the main result, we introduce several new concepts and show some results that will be of independent interest. In particular, we introduce an interactive (and average-case) version of sampling problems where the task is to sample the transcript obtained by a classical interaction between two quantum polynomial-time algorithms. We show that quantum advantage in interactive sampling problems is equivalent to the existence of IV-PoQ, which is considered as an interactive (and average-case) version of Aaronson's result [Aaronson, TCS 2014], **SampBQP ≠ SampBPP ⇔ FBQP ≠ FBPP**. Finally, we also introduce zero-knowledge IV-PoQ and study sufficient and necessary conditions for their existence.

CCS Concepts

• **Theory of computation** → **Quantum complexity theory**.

Keywords

Quantum advantage, Quantum cryptography, Proofs of quantumness, One-way puzzles

ACM Reference Format:
Tomoyuki Morimae, Yuki Shirakawa, and Takashi Yamakawa. 2025. Cryptographic Characterization of Quantum Advantage. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing (STOC '25), June 23–27, 2025, Prague, Czechia.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3717823.3718133

1 Introduction

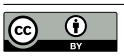
Quantum computational advantage refers to the existence of computational tasks that are easy for quantum computing but hard classically. Unconditionally showing quantum advantage is extremely hard, and is beyond our current understanding of complexity theory.[1] Some computational assumptions are therefore required. Which complexity assumption is necessary and sufficient for quantum advantage? As far as we know, no complete characterization of quantum advantage has been achieved before.

In this paper, we identify a cryptographic assumption that is necessary and sufficient for quantum advantage. Our main result is the following one:[2,3]

Theorem 1.1. *Inefficient-verifier proofs of quantumness (IV-PoQ) exist if and only if classically-secure one-way puzzles (OWPuzzs) exist.*

As far as we know, this is the first time that a complete cryptographic characterization of quantum advantage is obtained.

[1] There are several interesting results (such as [17]) that show unconditional quantum advantage by restricting classical computing. In this paper, we consider any polynomial-time classical computing.
[2] In this paper, all classically-secure OWPuzzs are ones with $(1-\mathrm{negl}(\lambda))$-correctness and $(1-1/\mathrm{poly}(\lambda))$-security. Unlike quantumly-secure OWPuzzs, we do not know how to amplify the gap for classically-secure OWPuzzs.
[3] In this paper, we consider the uniform adversarial model (i.e., adversaries are modeled as Turing machines), and some steps of the proofs of Theorem 1.1 crucially rely on the uniformity of the adversary. We leave it open to prove (or disprove) the non-uniform variant of Theorem 1.1.



STOC '25, Prague, Czechia

ACM ISBN 979-8-4007-1510-5/25/06
https://doi.org/10.1145/3717823.3718133

What are IV-PoQ? IV-PoQ are a generalization of proofs of quantumness (PoQ) [16]. A PoQ is an interactive protocol between a prover and a classical probabilistic polynomial-time (PPT) verifier over a classical channel. There exists a quantum polynomial-time (QPT) prover such that the verifier accepts with high probability (*completeness*), but for any PPT prover the verifier rejects with high probability (*soundness*). PoQ can be constructed from several cryptographic assumptions, such as (noisy) trapdoor claw-free functions with the adaptive-hardcore-bit property [16], trapdoor 2-to-1 collision-resistant hash functions [31], (full-domain) trapdoor permutations [43], quantum homomorphic encryptions [32], or knowledge assumptions [8]. Non-interactive PoQ are possible based on the hardness of factoring [47] or random oracles [50].

IV-PoQ [44] are the same as PoQ except that the verifier's final computation to make the decision can be unbounded. IV-PoQ are a generalization of PoQ, and as we will explain later, IV-PoQ capture various types of quantum advantage studied so far, such as sampling and search based quantum advantage.

Identifying a necessary and sufficient assumption for the existence of (IV-)PoQ remained open. In particular, in [44], IV-PoQ were constructed from classically-secure OWFs, but the problem of constructing IV-PoQ from weaker assumptions was left open in that paper. Our main result Theorem 1.1 solves the open problem, because as we will explain later, OWPuzzs are believed to be weaker than OWFs [33, 35, 42]. Moreover, a known necessary condition for the existence of IV-PoQ was only the almost trivial one: $\mathbf{BPP} \neq \mathbf{PP}$[4] [44]. Our main result Theorem 1.1 improves this to a highly non-trivial necessary condition, namely, the existence of classically-secure OWPuzzs.[5]

What are OWPuzzs? In classical cryptography, the existence of OWFs is the minimum assumption [29], because many primitives exist if and only if OWFs exist, such as pseudorandom generators (PRGs), pseudorandom functions (PRFs), zero-knowledge, commitments, digital signatures, and secret-key encryptions (SKE), and almost all primitives imply OWFs. On the other hand, recent active studies have revealed that in quantum cryptography OWFs are not necessarily the minimum assumption. Many fundamental primitives have been introduced, such as pseudorandom unitaries (PRUs) [30], pseudorandom function-like state generators (PRFSGs) [7], unpredictable state generators (UPSGs) [41], pseudorandom state generators (PRSGs) [30], one-way state generators (OWSGs) [42], EFI pairs [15], and one-way puzzles (OWPuzzs) [33]. These could exist even if OWFs do not exist [35, 36, 38], but still imply several useful applications such as message authentication codes [7], commitments [7, 42], multi-party computations [7, 11, 25, 42], secret-key encryptions [7], private-key quantum money [30], digital signatures [42], etc.

In particular, one-way puzzles (OWPuzzs) are one of the most fundamental primitives in this "cryptographic world below OWFs". A OWPuzz is a pair $(\mathsf{Samp}, \mathsf{Ver})$ of two algorithms. Samp is a QPT algorithm that takes 1^λ as input and outputs two classical bit strings puzz and ans. Ver is an unbounded algorithm that takes puzz and ans$'$ as input, and outputs $\top$ or $\bot$. We require two properties, correctness and security. Correctness requires that Ver accepts $(\mathsf{puzz}, \mathsf{ans})$ sampled by Samp with large probability. Security requires that for any QPT algorithm $\mathcal{A}$ that takes puzz as input and outputs ans$'$, Ver accepts $(\mathsf{puzz}, \mathsf{ans}')$ with only small probability. In particular, when the security is required only for all PPT adversaries, we say that a OWPuzz is classically-secure. (Note that the Samp algorithm of classically-secure OWPuzzs is QPT, not PPT, even when we consider classical security.)

OWPuzzs (and therefore classically-secure OWPuzzs) are implied by many primitives such as

- PRUs, PRFSGs, UPSGs, PRSGs, (pure) OWSGs,
- (pure) private-key quantum money, secret-key encryption schemes, digital signatures,
- many quantum-computation-classical-communication (QCCC) primitives[6] [21, 24, 33],
- quantum EFID pairs [21].

Our Theorem 1.1 therefore highlights that if there is no quantum advantage, then all of these quantum cryptographic primitives do not exist.

On the other hand, although many primitives imply OWPuzzs, no application of OWPuzzs is known except for commitments [33]. Finding more applications of OWPuzzs is one of the most important goals in this field. Our result Theorem 1.1 shows that OWPuzzs imply quantum advantage, which demonstrates that quantum advantage is another application of OWPuzzs. Moreover, we emphasize that this is the first application of OWPuzzs in the QCCC setting: IV-PoQ are a QCCC primitive because the communication between the verifier and the prover is classical, while commitments [33] constructed from OWPuzzs are those over quantum channels. The question of the existence of QCCC applications of OWPuzzs was raised in [21]. We solve the open problem.

Why IV-PoQ? In addition to (IV-)PoQ, there are mainly two other approaches to demonstrate quantum advantage, namely sampling and search based quantum advantage. Here we argue that IV-PoQ capture both of them, and therefore identifying a necessary and sufficient assumption for the existence of IV-PoQ is significant.

A sampling problem is a task of sampling from some distribution. There are several distributions that are easy to sample with QPT algorithms but hard with PPT algorithms, such as output distributions of random quantum circuits [14], Boson Sampling circuits [3], constant-depth circuits [48], IQP circuits [18, 19], and one-clean-qubit circuits [23, 39]. Several assumptions are known to be sufficient for quantum advantage in sampling problems, but these assumptions are newly-introduced assumptions that were not studied before such as an average-case #**P**-hardness of approximating some functions. Moreover, quantum advantage in sampling problems is in general not known to be verifiable (even inefficiently). On the other hand, one advantage of sampling-based quantum advantage (and others relying on newly-introduced assumptions) is that experimental realizations with NISQ machines seem to be

[4]The output probability distribution of any QPT algorithm can be computed by a classical polynomial-time deterministic algorithm that queries the **PP** oracle [22]. Therefore, if $\mathbf{BPP} = \mathbf{PP}$, a PPT prover can cheat the verifier.

[5]This is an improvement, because if classically-secure OWPuzzs exist then $\mathbf{BPP} \neq \mathbf{PP}$.

[6]Here, QCCC primitives are primitives with local quantum computation and classical communication. For example, in QCCC commitments, sender and receiver are QPT, while the message exchanged between them are classical.

easier.[7] As we will explain later, we introduce an average-case version of **SampBQP** ≠ **SampBPP**[8], and show that it is equivalent to the existence of non-interactive IV-PoQ. IV-PoQ therefore capture sampling-based quantum advantage.

A search problem is a task of finding an element z that satisfies a relation $R(z) = 1$. Several search problems have been shown to be easy for QPT algorithms but hard for PPT algorithms. Their classical hardness, however, relies on newly-introduced assumptions that were not studied before, such as QUATH [5] and XQUATH [6], or relies on random oracles [1, 9]. One advantage of searching-based quantum advantage over sampling-based one is that quantum advantage can be verified at least inefficiently when R is computable. (We can check $R(z) = 1$ or not by computing $R(z)$.) Because such inefficiently-verifiable searching-based quantum advantage is equivalent to the existence of non-interactive IV-PoQ, IV-PoQ capture inefficiently-verifiable searching-based quantum advantage. There are some search problems that are efficiently verifiable such as Factoring [47] and the Yamakawa-Zhandry problem [50] but the former is based on the hardness of a specific problem, and the latter relies on the random oracle model. Quantum advantage in efficiently-verifiable search problems is captured by non-interactive PoQ, and therefore by IV-PoQ.

Summary. In summary, we have shown that IV-PoQ are existentially equivalent to classically-secure OWPuzzs. We believe that this result is significant mainly because of the following five reasons.

(1) As far as we know, this is the first time that a complete cryptographic characterization of quantum advantage is achieved.
(2) IV-PoQ capture various types of quantum advantage studied so far including sampling and search based quantum advantage.
(3) The previous result [44] constructed IV-PoQ from classically-secure OWFs, but the problem of constructing IV-PoQ from weaker assumptions was left open. We solve the open problem.
(4) OWPuzzs are implied by many important primitives, such as PRUs, PRSGs, and OWSGs. Therefore, our main result shows that if there is no quantum advantage, then these quantum cryptographic primitives do not exist.
(5) No application of OWPuzzs was known before except for commitments (and therefore multiparty computations). We show that quantum advantage is another application of OWPuzzs. Moreover, it is the first QCCC application of OWPuzzs. This solves the open problem of [21].

1.1 Additional Results

In addition to the main result, Theorem 1.1, we obtain several important results. In the following, we explain them.

Relations to the sampling complexity. In the field of quantum advantage, one of the more studied notion of sampling-based quantum advantage is **SampBQP** ≠ **SampBPP**. We can show the following relation between IV-PoQ and **SampBQP** ≠ **SampBPP**:[9]

Theorem 1.2. *If IV-PoQ exist, then quantumly-secure OWFs exist or* **SampBPP** ≠ **SampBQP**.

Because the existence of quantumly-secure OWFs implies **NP** ⊈ **BQP**, Theorem 1.2 also means that if IV-PoQ exist, then **NP** ⊈ **BQP** or **SampBPP** ≠ **SampBQP**. This characterizes a lower bound of IV-PoQ in terms of worst-case complexity class assumptions. Note that this lower bound improves the previous known bound, **BPP** ≠ **PP**, of [44].[10]

Quantum advantage samplers (QASs). To show the main result, we introduce a new concept, which we call quantum advantage samplers (QASs). The existence of QASs is an average-case version of **SampBQP** ≠ **SampBPP**.

Let $\mathcal{A}$ be a QPT algorithm that takes 1^λ as input and outputs classical bit strings. $\mathcal{A}$ is a quantum advantage sampler (QAS) if there exists a polynomial p such that for any PPT algorithm $\mathcal{B}$,

$$\mathrm{SD}(\mathcal{A}(1^\lambda), \mathcal{B}(1^\lambda)) > \frac{1}{p(\lambda)} \tag{1}$$

holds for all sufficiently large $\lambda \in \mathbb{N}$, where SD is the statistical distance, and $\mathcal{A}(1^\lambda)$ (resp. $\mathcal{B}(1^\lambda)$) is the output probability distribution of $\mathcal{A}$ (resp. $\mathcal{B}$) on input 1^λ.

Intuitively, Equation (1) means that the output distribution of the QPT algorithm $\mathcal{A}$ cannot be classically efficiently sampled. How is this different from the more studied notion, **SampBPP** ≠ **SampBQP**? The existence of QASs can be considered as an average-case version of **SampBPP** ≠ **SampBQP**.[11] In fact, the existence of QASs implies **SampBPP** ≠ **SampBQP** (Lemma 3.4), but the inverse does not seem to hold. In order to show our main result, the worst-case notion of **SampBPP** ≠ **SampBQP** is not enough for our cryptographic (and therefore average-case) argument, and therefore we introduce QASs. We believe that the new concept, QASs, will be useful for other future studies of quantum sampling advantage in the context of quantum cryptography.

We show the following result.

Theorem 1.3. *QASs exist if and only if non-interactive IV-PoQ exist.*

Because the existence of QASs is an average-case version of **SampBQP** ≠ **SampBPP** while the existence of non-interactive IV-PoQ is an average-case version of **FBQP** ≠ **FBPP**, Theorem 1.3 can

[7] Although NISQ experimental realizations of quantum advantage are very important goals, in this paper, we focus on theoretical upper and lower bounds by assuming that any polynomial-time quantum computing is possible.
[8] For the definitions of **SampBQP** and **SampBPP**, see Definitions 2.17 and 2.18.

[9] Note that "quantumly-secure" in the theorem is not a typo. The reason why we can get quantumly-secure OWFs from classically-secure OWPuzzs is, roughly speaking, that if **SampBPP** = **SampBQP**, then classically-secure OWFs means quantumly-secure OWFs.
[10] First, **NP** ⊈ **BQP** implies **BPP** ≠ **PP**, because if **BPP** = **PP**, then **NP** ⊆ **PP** = **BPP** ⊆ **BQP**. Second, **SampBPP** ≠ **SampBQP** implies **BPP** ≠ **PP**, because a classical deterministic polynomial-time algorithm that queries the **PP** oracle can compute the output distribution of any QPT algorithm [22].
[11] **SampBPP** and **SampBQP** are worst-case complexity classes, and therefore $\{\mathcal{A}(1^\lambda)\}_\lambda \notin$ **SampBPP** means that there is at least one $\lambda \in \mathbb{N}$ such that $\mathcal{A}(1^\lambda)$ cannot be classically efficiently sampled, while the definition of QASs requires that $\{\mathcal{A}(1^\lambda)\}_\lambda$ cannot be classically efficiently sampled for all sufficiently large $\lambda \in \mathbb{N}$. In addition, there is a subtle technical difference: $\{\mathcal{A}_\lambda\}_\lambda \notin$ **SampBPP** means that $\mathcal{A}(1^\lambda)$ cannot be classically efficiently sampled for a precision ϵ, but this ϵ could be $\mathrm{negl}(\lambda)$, while QASs requires that the precision is $1/\mathrm{poly}(\lambda)$. For more details, see Section 3.

be considered as an average-case version of [2]'s result **SampBPP** ≠ **SampBQP** ⇔ **FBPP** ≠ **FBQP**.

In previous works on sampling-based quantum advantage [3, 14, 19, 39], **SampBQP** ≠ **SampBPP** was derived based on three assumptions. First is the complexity assumption of $\mathbf{P}^{\#\mathbf{P}} \not\subseteq \mathbf{BPP}^{\mathbf{NP}}$, which especially means that the polynomial-time hierarchy will not collapse to the third level. Second is the assumption that computing some functions (such as matrix permanents and Ising partition functions) within a certain multiplicative error is #**P**-hard on average. The third is called the anti-concentration assumption, which roughly means that the output probability of the quantum algorithm is not so concentrating.[12] For simplicity, we call the combination of the last two assumptions just the quantum advantage assumption.

The quantum advantage assumption has been traditionally studied in the field of quantum advantage to show sampling-based quantum advantage (in terms of **SampBQP** ≠ **SampBPP**) of several "non-universal" models such as random quantum circuits [14], Boson Sampling circuits [3], IQP circuits [19], and one-clean-qubit circuits [39]. We can show that the quantum advantage assumption also implies the existence of QASs.[13]

Theorem 1.4. *If the quantum advantage assumption holds and* $\mathbf{P}^{\#\mathbf{P}} \not\subseteq \mathbf{ioBPP}^{\mathbf{NP}}$*, then QASs exist.*

As we have explained above, QASs are cryptographically a more natural notion of sampling-based quantum advantage, and the existence of QASs seems to be stronger than **SampBQP** ≠ **SampBPP**. Therefore this theorem reveals that the quantum advantage assumption traditionally studied in the field actually implies a stronger form of quantum advantage (modulo the difference between **BPP** and **ioBPP**).

Interactive quantum advantage samplers (Int-QASs). We also introduce an interactive version of QASs, which we call interactive QASs (Int-QASs). Int-QASs are a generalization of QASs to interactive settings. An Int-QAS is a pair $(\mathcal{A}, C)$ of two interactive QPT algorithms $\mathcal{A}$ and C that communicate over a classical channel. Its security roughly says that no PPT algorithm $\mathcal{B}$ that interacts with C can sample the transcript of $(\mathcal{A}, C)$. (Here, the transcript is the sequence of all classical messages exchanged between $\mathcal{A}$ and C.) More precisely, $(\mathcal{A}, C)$ is an Int-QAS if there exists a polynomial p such that for any PPT algorithm $\mathcal{B}$ that interacts with C,

$$\mathrm{SD}(\langle \mathcal{A}, C\rangle(1^\lambda), \langle \mathcal{B}, C\rangle(1^\lambda)) > \frac{1}{p(\lambda)} \tag{2}$$

holds for all sufficiently large $\lambda \in \mathbb{N}$, where SD is the statistical distance, and $\langle \mathcal{A}, C\rangle(1^\lambda)$ (resp. $\langle \mathcal{B}, C\rangle(1^\lambda)$) is the probability distribution over the transcript of the interaction between $\mathcal{A}$ (resp. $\mathcal{B}$) and C on input 1^λ.

It is easy to see that IV-PoQ imply Int-QASs: for any IV-PoQ $(\mathcal{P}, \mathcal{V}_1, \mathcal{V}_2)$, where $\mathcal{P}$ is the prover, $\mathcal{V}_1$ is the efficient verifier, and $\mathcal{V}_2$ is the inefficient verifier, we have only to take $(\mathcal{A}, C) = (\mathcal{P}, \mathcal{V}_1)$. However, the opposite direction is not immediately clear. We show that the opposite direction can be also shown. We hence have the following result.

[12] For several models, such as the IQP model [19] and the one-clean-qubit model [39], the anti-concentration property can be shown.

[13] This result was not included in the previous version of this manuscript. We obtained this result after reading [34].

Theorem 1.5. *Int-QASs exist if and only if IV-PoQ exist.*

This theorem is considered as an interactive (and average-case) version of **SampBPP** ≠ **SampBQP** ⇔ **FBPP** ≠ **FBQP**, because the existence of Int-QASs is an interactive (and average-case) version of **SampBQP** ≠ **SampBPP** while the existence of IV-PoQ is an interactive (and average-case) version of **FBQP** ≠ **FBPP**.

QAS/OWF condition. In addition to QASs and Int-QASs, we also introduce another new concept, the QAS/OWF condition, which is inspired by the SZK/OWF condition [49]. As we will explain later, the QAS/OWF condition plays a pivotal role to show our main result. Roughly speaking, the QAS/OWF condition is satisfied if there is a pair of candidates of a QAS and a classically-secure OWF such that for all sufficiently large security parameters, either of them is secure.[14] If a QAS exists or a classically-secure OWF exists, then the QAS/OWF is satisfied, but the converse is unlikely. For example, if there are (candidates of) a QAS that is secure for all odd security parameters and a OWF that is secure for all even security parameters, then the QAS/OWF is satisfied, but it does not necessarily imply either of a QAS or a OWF.

We show that the QAS/OWF condition is equivalent to both the existence of IV-PoQ and the existence of classically-secure OWPuzzs:

Theorem 1.6. *IV-PoQ exist if and only if the QAS/OWF condition holds.*

Theorem 1.7. *Classically-secure OWPuzzs exist if and only if the QAS/OWF condition holds.*

By combining these two results, we obtain our main result, Theorem 1.1.

Variants of IV-PoQ.. Recall that the verifier of IV-PoQ must be PPT during the interaction. We consider the following two variants of IV-PoQ, *public-coin IV-PoQ*, where all the verifier's messages must be uniformly random strings, and *quantum-verifier IV-PoQ*, where the verifier is allowed to be QPT instead of PPT during the interaction. Clearly, public-coin IV-PoQ is a special case of IV-PoQ (since uniformly random strings can be sampled in PPT), and IV-PoQ is a special case of quantum-verifier IV-PoQ (since PPT computations can be simulated in QPT). We show implications in the other direction, making them equivalent in terms of existence.

Theorem 1.8. *The existence of public-coin IV-PoQ, IV-PoQ, and quantum-verifier IV-PoQ are equivalent.*

This theorem suggests that the power of IV-PoQ is robust to the choice of the computational power of the verifier during the interaction.

Zero-knowledge IV-PoQ.. We define the zero-knowledge property for IV-PoQ, which roughly requires that the verifier's view can be simulated by a PPT simulator. Intuitively, this ensures that the verifier learns nothing from the prover beyond what could have been computed in PPT. We say that an IV-PoQ satisfies statistical (resp. computational) zero-knowledge if for any PPT malicious verifier, there is a PPT simulator that statistically (resp. computationally) simulates the verifier's view. We say that an IV-PoQ

[14] See Definition 4.1 for the precise definition.

satisfies honest-verifier statistical zero-knowledge if there is a PPT simulator that statistically simulates the honest verifier's view. We prove the following results.

Theorem 1.9. *If honest-verifier statistical zero-knowledge IV-PoQ exist, then classically-secure OWFs exist.*

Theorem 1.10. *If classically-secure OWFs exist, then computational zero-knowledge IV-PoQ exist.*

The above theorems establish a loose equivalence between zero-knowledge IV-PoQ and classically-secure OWFs. However, there is still a gap between them, and filling it is left as an open problem.

1.2 Technical Overview

Our main result is Theorem 1.1, which shows that IV-PoQ exist if and only if classically-secure OWPuzzs exist. In this technical overview, we provide intuitive explanations for the result. To show it, the QAS/OWF condition plays a pivotal role. For ease of presentation, we think of the QAS/OWF condition as just the condition that "a QAS exists or a classically-secure OWF exists" in this overview. Though this is stronger than the actual definition, this rough description is enough for understanding our ideas.

We first show IV-PoQ $\Leftrightarrow$ QAS/OWF condition. We next show classically-secure OWPuzzs $\Leftrightarrow$ QAS/OWF condition. By combining them, we finally obtain the main result. In the following, we explain each step.

Step 1: IV-PoQ $\Rightarrow$ QAS/OWF condition. Our proof is inspired by [45]. However, we emphasize that our proof is not a trivial application of [45]. As we will explain later, the same proof of [45] does not work in our setting, and therefore we had to overcome several technical challenges to show the result.

Let $(\mathcal{P}, \mathcal{V}_1, \mathcal{V}_2)$ be an ℓ-round IV-PoQ, where $\mathcal{P}$ is the prover, $\mathcal{V}_1$ is the efficient verifier, and $\mathcal{V}_2$ is the inefficient verifier. (We count two messages as a single round.) Without loss of generality, we can assume that $\mathcal{V}_1$ first sends a message. Let $(c_1, a_1, ..., c_\ell, a_\ell)$ be the transcript (i.e., the sequence of all messages exchanged) of the interaction between $\mathcal{P}$ and $\mathcal{V}_1$, where c_i is $\mathcal{V}_1$'s i-th message and a_i is $\mathcal{P}$'s i-th message. Our goal is, by assuming that the QAS/OWF condition is not satisfied, to construct a classical PPT adversary $\mathcal{P}^*$ that breaks the soundness of the IV-PoQ.

If the QAS/OWF condition is not satisfied, then, roughly speaking, both of the following two conditions are satisfied:

(a) QASs do not exist. In other words, the output probability distribution of any QPT algorithm can be approximately sampled with a PPT algorithm.
(b) Classically-secure OWFs do not exist.

From (a), the distribution of the transcript generated by the interaction between $\mathcal{P}$ and $\mathcal{V}_1$ can be approximately sampled with a PPT algorithm $\mathcal{S}$. One might think that if a malicious PPT prover of the IV-PoQ just runs $\mathcal{S}$, the soundness of the IV-PoQ is broken. However, this is not correct: The ability to classically efficiently sample from the distribution $\langle \mathcal{P}, \mathcal{V}_1 \rangle (1^\lambda)$ is not enough to break the soundness of the IV-PoQ, because what the PPT adversary $\mathcal{P}^*$ has to do is not to sample $(c_1, a_1, ..., c_\ell, a_\ell)$ but to sample "correct" a_k given the transcript $(c_1, a_1, ..., c_{k-1}, a_{k-1}, c_k)$ obtained so far for every $k \in [\ell]$.

We use (b) to solve it. From $\mathcal{S}$, we define a function f as follows.

(1) Get an input (k, r).
(2) Run $(c_1, a_1, ..., c_\ell, a_\ell) = \mathcal{S}(1^\lambda; r)$.[15]
(3) Output $(k, c_1, a_1, ..., c_{k-1}, a_{k-1}, c_k)$.

From (b), OWFs do not exist. Then, distributional OWFs do not exist as well [29].[16] This means that there exists a PPT algorithm $\mathcal{R}$ such that the statistical distance between $(x, f(x))$ and $(\mathcal{R}(f(x)), f(x))$ is small for random x. Therefore, for each $k \in [\ell]$, the following PPT adversary $\mathcal{P}^*$ can return "correct" a_k given $(c_1, a_1, ..., c_{k-1}, a_{k-1}, c_k)$.

(1) Take $(c_1, a_1, ..., c_{k-1}, a_{k-1}, c_k)$ as input.
(2) Run $(k', r') \leftarrow \mathcal{R}(k, c_1, a_1, ..., c_{k-1}, a_{k-1}, c_k)$.
(3) Run $(c'_1, a'_1, ..., c'_\ell, a'_\ell) = \mathcal{S}(1^\lambda; r')$.
(4) Output $a'_{k'}$.

In this way, we can break the soundness of the IV-PoQ. Hence we have shown that IV-PoQ $\Rightarrow$ the QAS/OWF condition.

The idea underlying this proof is similar to that of [45]. In [45], it was shown that if SZK is average hard then OWFs exist. To show it, [45] used the zero-knowledge property to guarantee the existence of a PPT simulator that can sample the transcript between the verifier and the prover. From that simulator, [45] constructed a OWF. Very roughly speaking, our $\mathcal{S}$ that comes from (a) corresponds to the zero-knowledge simulator of [45]: the transcript of [45] can be PPT sampled because of the zero-knowledge property while our transcript can be PPT sampled because QASs do not exist. However, there are several crucial differences between our setting and [45]'s. In particular, in the setting of [45] the constructed OWF can depend on the simulator. On the other hand, in our setting, we finally want to construct a OWF that is independent of $\mathcal{S}$.[17] In order to solve the issue, we use the universal construction of OWFs [27, 37]. We first construct a OWF $f_{\mathcal{S}}$ from each $\mathcal{S}$ as we have explained above, and next construct a OWF g that is independent of $\mathcal{S}$ by using the universal construction. In addition to this issue, there are several other points where the direct application of [45] does not work, but for details, see the full version of this paper [40].

Note that in the actual proof, we do not directly show IV-PoQ $\Rightarrow$ the QAS/OWF condition. We first show IV-PoQ $\Rightarrow$ Int-QAS, and then show Int-QAS $\Rightarrow$ the QAS/OWF condition in order to obtain stronger results and to avoid repeating similar proofs twice. However, the proof of Int-QAS $\Rightarrow$ the QAS/OWF condition is essentially the same as that explained above.

Step 2: Classically-secure OWPuzzs $\Rightarrow$ QAS/OWF condition. Its proof is similar to that of step 1. Let (Samp, Ver) be a classically-secure OWPuzz. Assume that the QAS/OWF condition is not satisfied. This roughly means that both of the following two conditions are satisfied.

(a) QASs do not exist.
(b) Classically-secure OWFs do not exist.

[15] For a PPT algorithm $\mathcal{A}$, $y = \mathcal{A}(x; r)$ means that $\mathcal{A}$'s output is y when the input is x and the random seed is r.
[16] An efficiently-computable function $f : \{0,1\}^* \to \{0,1\}^*$ is called a classically-secure (resp. quantumly-secure) distributional OWF if for any PPT (resp. QPT) adversary $\mathcal{A}$, the statistical distance between $(x, f(x))$ and $(\mathcal{A}(f(x)), f(x))$ is large for random x.
[17] In the precise definition of QAS/OWF condition, the OWFs should be independent of $\mathcal{S}$. Otherwise, we do not know how to show the other direction, namely, the QAS/OWF condition $\Rightarrow$ IV-PoQ.

From (a), there exists a PPT algorithm $\mathcal{S}$ such that the output probability distribution of $\mathcal{S}(1^\lambda)$ is close to that of $\mathsf{Samp}(1^\lambda)$ in the statistical distance. From such $\mathcal{S}$, we construct a function f as follows.

(1) Get a bit string r as input.
(2) Compute $(\mathsf{puzz}, \mathsf{ans}) = \mathcal{S}(1^\lambda; r)$.
(3) Output puzz.

From (b), OWFs do not exist. This means that distributional OWFs do not exist as well. Therefore, there exists a PPT algorithm $\mathcal{R}$ such that the statistical distance between $(x, f(x))$ and $(\mathcal{R}(f(x)), f(x))$ is small for random x. From $\mathcal{S}$ and $\mathcal{R}$, we can construct a PPT adversary $\mathcal{A}$ that breaks the security of the OWPuzz as follows:

(1) Take puzz as input.
(2) Run $r \leftarrow \mathcal{R}(\mathsf{puzz})$.
(3) Run $(\mathsf{puzz}', \mathsf{ans}') \leftarrow \mathcal{S}(1^\lambda; r)$.
(4) Output ans'.

As in step 1, we actually need a OWF that is independent of $\mathcal{S}$, and therefore we have to use the universal construction [27, 37].

Step 3: QAS/OWF condition ⇒ IV-PoQ.. Assume that the QAS/OWF condition is satisfied. Then, roughly speaking, a QAS Q exists or a classically-secure OWF f exists. From f, we can construct an IV-PoQ by using the result of [44]. The non-trivial part is to construct an IV-PoQ from Q. For that goal, we use the idea of [2]. However, as we will explain later, a direct application of [2] does not work for our goal, and some new technical contributions were needed.

We construct a non-interactive IV-PoQ from Q as follows:

(1) The QPT prover runs $Q(1^\lambda)$ N times, where N is a certain polynomial, and sends the result $(y_1, ..., y_N)$ to the verifier, where y_i is the output of the i-th run of $Q(1^\lambda)$.
(2) The unbounded verifier computes the Kolmogorov complexity $K(y_1, ..., y_N)$[18], and accepts if it is larger than

$$\log \frac{1}{\Pr[(y_1, ..., y_N) \leftarrow Q(1^\lambda)^{\otimes N}]}.$$

We can show that thus constructed non-interactive IV-PoQ satisfies completeness and soundness. For completeness, we use Markov's inequality to show that $K(y_1, ..., y_N)$, where $y_i \leftarrow Q(1^\lambda)$ for each $i \in [N]$, is large with high probability and therefore the verifier accepts. To evaluate the bound of Markov's inequality, we use Kraft's inequality for the prefix Kolmogorov complexity, which says that $\sum_x 2^{-K(x)} \leq 1$. For soundness, assume that there exists a PPT adversary $\mathcal{P}^*$ that outputs $(y'_1, ..., y'_N)$ that is accepted by the verifier with high probability, which means that $\log \frac{1}{\Pr[(y'_1,...,y'_N)\leftarrow Q(1^\lambda)^{\otimes N}]} \lesssim K(y'_1, ..., y'_N)$. Because of the property of K, we have $K(y'_1, ..., y'_N) \lesssim \log \frac{1}{\Pr[(y'_1,...,y'_N)\leftarrow \mathcal{P}^*(1^\lambda)]}$. By combining them, we have

$$\log \frac{\Pr[(y'_1.., y'_N) \leftarrow \mathcal{P}^*(1^\lambda)]}{\Pr[(y'_1, ..., y'_N) \leftarrow Q(1^\lambda)^{\otimes N}]} \approx 0,$$

which roughly means that the output probability distribution of $Q(1^\lambda)^{\otimes N}$ is close to that of $\mathcal{P}^*(1^\lambda)$.

[18] More precisely, this is time-bounded prefix Kolmogorov complexity $K^T_U(y_1, ..., y_N)$ with time bound $T(n) = 2^{2^n}$ and the universal self-delimiting machine U.

From such $\mathcal{P}^*$, we can construct a PPT algorithm whose output probability distribution is close to that of $Q(1^\lambda)$ in the statistical distance as follows:

(1) Run $(y'_1, ..., y'_N) \leftarrow \mathcal{P}^*(1^\lambda)$.
(2) Choose a random $i \in [N]$, and output y'_i.

However, this means that Q is not a QAS, which contradicts the assumption. In this way, we can show the QAS/OWF condition ⇒ IV-PoQ.

The idea underlying this proof is similar to that of [2]. In fact, the completeness part is exactly the same. However, for the soundness part, the direct application of [2] does not work, because of several reasons. Here we explain main two issues. First, the search problem constructed in [2] was not necessarily verifiable even in unbounded time since Kolmogorov complexity is uncomputable in general. This is problematic for our goal, because what we want to construct is a non-interactive IV-PoQ where the prover's message should be verified *at least inefficiently*. [2] slightly mentioned an extension of the result to the time-bounded case, but there was no proof. Second, [2] constructed a search advantage from **SampBQP** ≠ **SampBPP**, which is a worst-case notion. However, what we need is a search advantage from the existence of QASs, namely, the *average-case version* of sampling advantage. Hence the proof of [2] cannot be directly used in our setting.

Step 4: QAS/OWF condition ⇒ classically-secure OWPuzzs. The proof uses a similar technique as used in step 3. If the QAS/OWF condition is satisfied, then, roughly speaking, a classically-secure OWF f exists or a QAS Q exists. From the OWF f, we can construct a classically-secure OWPuzz easily as follows:

- $\mathsf{Samp}(1^\lambda) \to (\mathsf{puzz}, \mathsf{ans})$: Choose $x \leftarrow \{0,1\}^\lambda$, and output $\mathsf{puzz} \coloneqq f(x)$ and $\mathsf{ans} \coloneqq x$.
- $\mathsf{Ver}(\mathsf{puzz}, \mathsf{ans}') \to \top/\bot$: Accept if and only if $f(\mathsf{ans}') = \mathsf{puzz}$.

From Q, we can construct a non-interactive IV-PoQ as in step 3. From such a non-interactive IV-PoQ, we can easily construct a classically-secure OWPuzz as follows.

- $\mathsf{Samp}(1^\lambda) \to (\mathsf{puzz}, \mathsf{ans})$: Run $\tau \leftarrow \mathcal{P}(1^\lambda)$, and output $\mathsf{puzz} \coloneqq 1^\lambda$ and $\mathsf{ans} \coloneqq \tau$.
- $\mathsf{Ver}(\mathsf{puzz}, \mathsf{ans}') \to \top/\bot$: Accept if and only if $\top \leftarrow \mathcal{V}_2(1^\lambda, \mathsf{ans}')$.

Full paper. We omit complete proofs of our results due to space constraints but all proofs can be found in the full version of this paper [40].

1.3 Related Work

Khurana and Tomer [34] have recently shown that *quantumly-secure* OWPuzzs can be constructed from some assumptions that imply sampling-based quantum advantage (if a mild complexity assumption, $\mathbf{P}^{\#\mathbf{P}} \not\subseteq (io)\mathbf{BQP}/\mathbf{qpoly}$, is additionally introduced). There is no technical overlap between their paper and the present paper. However, we here clarify relations and differences, because in a broad perspective, their paper and the present paper share several important motivations, including the goal of connecting quantum advantage and "Microcrypt" primitives.

Firstly, what they actually show is not that quantum advantage implies OWPuzzs, but that some assumptions that imply quantum advantage also imply OWPuzzs if the additional assumption, $\mathbf{P}^{\#\mathbf{P}} \not\subseteq (io)\mathbf{BQP}/\mathbf{qpoly}$, is introduced. On the other hand, we show that quantum advantage (in the sense of the existence of IV-PoQ) implies OWPuzzs. Secondly, they construct quantumly-secure OWPuzzs, while we construct only classically-secure ones.

These differences comes from the difference of main goals. Their goal is to construct quantum cryptographic primitives from some well-founded assumptions that will not imply OWFs. Therefore, the constructed primitives should be quantumly-secure. However, in that case, as they also mention in their paper, some additional assumptions that limit quantum power should be introduced, because quantum advantage limits only classical power. On the other hand, the goal of the present paper is to characterize quantum advantage from cryptographic assumptions, and therefore we have to consider quantum advantage itself, not assumptions that imply quantum advantage. Moreover, we want to avoid introducing any additional assumptions that are not related to quantum advantage. In that case, it is likely that we have to be satisfied with classically-secure OWPuzzs.

It is an interesting open problem whether several notions of quantum advantage studied in this paper imply quantumly-secure OWPuzzs (possibly introducing some additional assumptions that limit quantum power).

2 Preliminaries

2.1 Basic Notations

$\log x$ means $\log_2 x$ and $\ln x$ means $\log_e x$. We use standard notations of quantum computing and cryptography. For a bit string x, $|x|$ is its length. $\mathbb{N}$ is the set of natural numbers. We use λ as the security parameter. $[n]$ means the set $\{1, 2, ..., n\}$. For a finite set S, $x \leftarrow S$ means that an element x is sampled uniformly at random from the set S. negl is a negligible function, and poly is a polynomial. All polynomials appear in this paper are positive, but for simplicity we do not explicitly mention it. PPT stands for (classical) probabilistic polynomial-time and QPT stands for quantum polynomial-time. For an algorithm $\mathcal{A}$, $y \leftarrow \mathcal{A}(x)$ means that the algorithm $\mathcal{A}$ outputs y on input x. If $\mathcal{A}$ is a classical probabilistic or quantum algorithm that takes x as input and outputs bit strings, we often mean $\mathcal{A}(x)$ by the output probability distribution of $\mathcal{A}$ on input x. When $\mathcal{A}$ is a classical probabilistic algorithm, $y = \mathcal{A}(x; r)$ means that the output of $\mathcal{A}$ is y if it runs on input x and with the random seed r. For two interactive algorithms $\mathcal{A}$ and $\mathcal{B}$ that interact over a classical channel, $\tau \leftarrow \langle \mathcal{A}(x), \mathcal{B}(y) \rangle$ means that the transcript τ (i.e., the sequence of all messages exchanged) is generated by the interactive protocol between $\mathcal{A}$ and $\mathcal{B}$ where $\mathcal{A}$ takes x as input and $\mathcal{B}$ takes y as input. If both $\mathcal{A}$ and $\mathcal{B}$ take the same input x, we also write it as $\tau \leftarrow \langle \mathcal{A}, \mathcal{B} \rangle(x)$. For two quantum states ρ and σ, $\mathsf{TD}(\rho, \sigma) \coloneqq \frac{1}{2}\|\rho - \sigma\|_1$ means their trace distance, where $\|X\|_1 \coloneqq \mathrm{Tr}\sqrt{X^\dagger X}$ is the trace norm. For two probability distributions $P \coloneqq \{p_i\}_i$ and $Q \coloneqq \{q_i\}_i$, $\mathsf{SD}(Q, P) \coloneqq \frac{1}{2}\sum_i |p_i - q_i|$ is their statistical distance. If $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$ and $\sigma = \sum_i q_i |\phi_i\rangle\langle\phi_i|$ for some orthonormal basis $\{|\phi_i\rangle\}_i$, we have $\mathsf{TD}(\rho, \sigma) = \mathsf{SD}(\{p_i\}_i, \{q_i\}_i)$.

2.2 One-Way Functions

We first review the definition of one-way functions (OWFs).

Definition 2.1 (One-Way Functions (OWFs)). A function $f : \{0,1\}^* \to \{0,1\}^*$ that is computable in classical deterministic polynomial-time is a classically-secure (resp. quantumly-secure) one-way function (OWF) if for any PPT (resp. QPT) adversary $\mathcal{A}$ and any polynomial p,

$$\Pr[f(x') = f(x) : x \leftarrow \{0,1\}^\lambda, x' \leftarrow \mathcal{A}(1^\lambda, f(x))] \leq \frac{1}{p(\lambda)} \quad (3)$$

holds for all sufficiently large $\lambda \in \mathbb{N}$.

We define a variant of OWFs, which we call OWFs on a subset $\Sigma \subseteq \mathbb{N}$. The difference from the standard OWFs is that security holds only when the security parameter belongs to the subset Σ of $\mathbb{N}$.

Definition 2.2 (OWFs on Σ). Let $\Sigma \subseteq \mathbb{N}$ be a set. A function $f : \{0,1\}^* \to \{0,1\}^*$ that is computable in classical deterministic polynomial-time is a classically-secure (resp. quantumly-secure) OWF on Σ if there exists an efficiently-computable polynomial n such that for any PPT (resp. QPT) adversary $\mathcal{A}$ and any polynomial p there exists $\lambda^* \in \mathbb{N}$ such that

$$\Pr[f(x') = f(x) : x \leftarrow \{0,1\}^{n(\lambda)}, x' \leftarrow \mathcal{A}(1^{n(\lambda)}, f(x))] \leq \frac{1}{p(\lambda)} \quad (4)$$

holds for all $\lambda \geq \lambda^*$ in Σ.

Remark 2.3. In the definition of OWFs (Definition 2.1) the input length is treated as the security parameter, but in OWFs on Σ (Definition 2.2), we allow the input length to be an arbitrary polynomial in the security parameter.

Remark 2.4. For any finite Σ, OWFs on Σ always exist because the definition is trivially satisfied. (We have only to take $\lambda^* = \lambda_{max} + 1$, where λ_{max} is the largest element of Σ.) However, we include the case when Σ is finite in the definition for convenience.

The existence of OWFs on $\mathbb{N} \setminus \Sigma$ for a finite subset Σ is actually equivalent to that of the standard OWFs.

Lemma 2.5. *Let $\Sigma \subseteq \mathbb{N}$ be a finite set. Classically-secure (resp. quantumly-secure) OWFs exist if and only if classically-secure (resp. quantumly-secure) OWFs on $\mathbb{N} \setminus \Sigma$ exist.*

2.3 One-Way Puzzles

We also define one-way puzzles (OWPuzzs) on a subset $\Sigma \subseteq \mathbb{N}$, which are a generalization of OWPuzzs defined in [33]. If $\Sigma = \mathbb{N}$, the definition becomes the standard one [33], and in that case we call them just OWPuzzs.

Definition 2.6 (One-Way Puzzles (OWPuzzs) on Σ). Let $\Sigma \subseteq \mathbb{N}$ be a set. A one-way puzzle (OWPuzz) on Σ is a pair $(\mathsf{Samp}, \mathsf{Ver})$ of algorithms such that

- $\mathsf{Samp}(1^\lambda) \to (\mathrm{puzz}, \mathrm{ans})$: It is a QPT algorithm that, on input the security parameter λ, outputs a pair $(\mathrm{puzz}, \mathrm{ans})$ of classical strings.
- $\mathsf{Ver}(\mathrm{puzz}, \mathrm{ans}') \to \top/\bot$: It is an unbounded algorithm that, on input $(\mathrm{puzz}, \mathrm{ans}')$, outputs either $\top/\bot$.

They satisfy the following properties for some functions c and s such that $c(\lambda) - s(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$.

- c-**correctness:** There exists $\lambda^* \in \mathbb{N}$ such that

$$\Pr[\top \leftarrow \mathsf{Ver}(\mathsf{puzz}, \mathsf{ans}) : (\mathsf{puzz}, \mathsf{ans}) \leftarrow \mathsf{Samp}(1^\lambda)] \geq c(\lambda) \quad (5)$$

  holds for all $\lambda \geq \lambda^*$.
- s-**security on** Σ**:** For any QPT adversary $\mathcal{A}$ there exists $\lambda^{**} \in \mathbb{N}$ such that

$$\Pr[\top \leftarrow \mathsf{Ver}(\mathsf{puzz}, \mathcal{A}(1^\lambda, \mathsf{puzz})) : (\mathsf{puzz}, \mathsf{ans}) \leftarrow \mathsf{Samp}(1^\lambda)] \leq s(\lambda) \quad (6)$$

  holds for all $\lambda \geq \lambda^{**}$ in Σ.

Definition 2.7 (Classically-Secure OWPuzzs on Σ). A OWPuzz on Σ is called a classically-secure OWPuzz on Σ if the security is required against PPT adversaries.

Remark 2.8. Again, if Σ is a finite set, OWPuzzs on Σ trivially exist, but we include such a case in the definition for the convenience.

Remark 2.9. All classically-secure OWPuzzs appearing in this paper are ones with $(1 - \mathsf{negl}(\lambda))$-correctness and $(1 - 1/\mathrm{poly}(\lambda))$-security.

Remark 2.10. It is known that c-correct and s-secure OWPuzzs with $c(\lambda) - s(\lambda) \geq 1/\mathrm{poly}(\lambda)$ can be amplified to $(1 - \mathsf{negl}(\lambda))$-correct and $\mathsf{negl}(\lambda)$-secure OWPuzzs [21]. On the other hand, we do not know how to amplify the gap of classically-secure OWPuzzs.

OWPuzzs can be constructed from OWFs. We can show that this is also the case for the variants on Σ.

Lemma 2.11. *Let $\Sigma \subseteq \mathbb{N}$ be a subset. If classically-secure OWFs on Σ exist, then classically-secure OWPuzzs on Σ with* 1*-correctness and* negl*-security exist.*

2.4 Inefficient-Verifier Proofs of Quantumness

In this subsection, we define inefficient-verifier proofs of quantumness (IV-PoQ) on a subset $\Sigma \subseteq \mathbb{N}$. IV-PoQ defined in [44] are special cases when $\Sigma = \mathbb{N}$.

Definition 2.12 (Inefficient-Verifier Proofs of Quantumness (IV-PoQ) on Σ). Let $\Sigma \subseteq \mathbb{N}$ be a set. An IV-PoQ on Σ is a tuple $(\mathcal{P}, \mathcal{V}_1, \mathcal{V}_2)$ of interactive algorithms. $\mathcal{P}$ (prover) is QPT, $\mathcal{V}_1$ (first verifier) is PPT, and $\mathcal{V}_2$ (second verifier) is unbounded. The protocol is divided into two phases. In the first phase, $\mathcal{P}$ and $\mathcal{V}_1$ take the security parameter 1^λ as input and interact with each other over a classical channel. Let τ be the transcript, i.e., the sequence of all classical messages exchanged between $\mathcal{P}$ and $\mathcal{V}_1$. In the second phase, $\mathcal{V}_2$ takes 1^λ and τ as input and outputs $\top$ (accept) or $\bot$ (reject). We require the following two properties for some functions c and s such that $c(\lambda) - s(\lambda) \geq 1/\mathrm{poly}(\lambda)$.

- c-**completeness:** There exists $\lambda^* \in \mathbb{N}$ such that

$$\Pr[\top \leftarrow \mathcal{V}_2(1^\lambda, \tau) : \tau \leftarrow \langle \mathcal{P}, \mathcal{V}_1 \rangle(1^\lambda)] \geq c(\lambda) \quad (7)$$

  holds for all $\lambda \geq \lambda^*$.
- s-**soundness on** Σ**:** For any PPT prover $\mathcal{P}^*$ there exists $\lambda^{**} \in \mathbb{N}$ such that

$$\Pr[\top \leftarrow \mathcal{V}_2(1^\lambda, \tau) : \tau \leftarrow \langle \mathcal{P}^*, \mathcal{V}_1 \rangle(1^\lambda)] \leq s(\lambda) \quad (8)$$

  holds for all $\lambda \geq \lambda^{**}$ in Σ.

Moreover, if all the messages sent from $\mathcal{V}_1$ are uniformly random strings, we say that the IV-PoQ is public-coin.

Remark 2.13. IV-PoQ on Σ always exist for any finite set Σ, but we include the case in the definition for the convenience.

Remark 2.14. In the previous definition of IV-PoQ [44], $\mathcal{V}_2$ does not take 1^λ as input. However, this does not change the definition for interactive IV-PoQ, because 1^λ can be added to the first $\mathcal{V}_1$'s message. We explicitly include 1^λ in the input of $\mathcal{V}_2$ since we also consider non-interactive IV-PoQ in this paper.

[44] showed that classically-secure OWFs imply IV-PoQ by constructing IV-PoQ from statistically-hiding and computationally-binding commitment schemes that are implied by OWFs [26]. By inspecting its proof, one can see that the proof gives a "security-parameter-wise" reduction, i.e., for any efficiently computable polynomial n, we can construct IV-PoQ from classically-secure OWFs such that that if the base OWF is secure on inputs of length $n(\lambda)$, then the resulting IV-PoQ is sound on the security parameter λ.[19] Thus, we have the following lemma.

Lemma 2.15 (Based on [26, 44]). *Let $\Sigma \subseteq \mathbb{N}$ be a set. If classically-secure OWFs on Σ exist, then IV-PoQ on Σ exist. Moreover, the constructed IV-PoQ is public-coin and satisfies* $(1 - \mathsf{negl})$*-completeness and* negl*-soundness on Σ.*

Remark 2.16. In [44], they do not explicitly state that the protocol is public-coin. To see that it is indeed public-coin, observe that the verifier's messages of the IV-PoQ of [44] consist of the receiver's messages of a statistically hiding commitment scheme of [26], descriptions of pairwise independent hash functions, and uniformly random strings from the verifier of [31]. As mentioned in [26, Section 8], their commitment scheme is public-coin. Moreover, we can assume that a description of a pairwise independent hash function is public-coin without loss of generality since we can treat the randomness for choosing the function as its description. Thus, the IV-PoQ of [44] is public-coin.

2.5 Sampling Complexity

Definition 2.17 (Sampling Problems [2, 4]). A (polynomially-bounded) sampling problem S is a collection of probability distributions $\{D_x\}_{x \in \{0,1\}^*}$, where D_x is a distribution over $\{0,1\}^{p(|x|)}$, for some fixed polynomial p.

*Definition 2.18 (***SampBPP** *and* **SampBQP** *[2, 4]).* **SampBPP** is the class of (polynomially-bounded) sampling problems $S = \{D_x\}_{x \in \{0,1\}^*}$ for which there exists a PPT algorithm $\mathcal{B}$ such that for all x and all $\epsilon > 0$, $\mathrm{SD}(\mathcal{B}(x, 1^{\lfloor 1/\epsilon \rfloor}), D_x) \leq \epsilon$, where $\mathcal{B}(x, 1^{\lfloor 1/\epsilon \rfloor})$ is

[19] More precisely, for any efficiently computable function $f : \{0,1\}^* \to \{0,1\}^*$ and efficiently computable polynomial n, there is an IV-PoQ $(\mathcal{P}, \mathcal{V}_1, \mathcal{V}_2)$ such that for any PPT algorithm $\mathcal{P}^*$ and any polynomial p, there are a PPT algorithm $\mathcal{A}$ and a polynomial q such that for any $\lambda \in \mathbb{N}$, if

$$\Pr[\top \leftarrow \mathcal{V}_2(1^\lambda, \tau) : \tau \leftarrow \langle \mathcal{P}^*, \mathcal{V}_1 \rangle(1^\lambda)] > \frac{1}{p(\lambda)}, \quad (9)$$

then

$$\Pr[f(x') = f(x) : x \leftarrow \{0,1\}^{n(\lambda)}, x' \leftarrow \mathcal{A}(1^{n(\lambda)}, f(x))] > \frac{1}{q(\lambda)}. \quad (10)$$

the output probability distribution of $\mathcal{B}$ on input $(x, 1^{\lfloor 1/\epsilon \rfloor})$. **SampBQP** is defined the same way, except that $\mathcal{B}$ is a QPT algorithm rather than a PPT one.

3 QASs and Int-QASs

In this section, we introduce two new concepts, quantum advantage samplers (QASs) and interactive quantum advantage samplers (Int-QASs). We also show some results on them.

3.1 Definitions of QASs and Int-QASs

We first define QASs on a set $\Sigma \subseteq \mathbb{N}$. If $\Sigma = \mathbb{N}$, we call them just QASs.

Definition 3.1 (Quantum Advantage Samplers (QASs) on Σ). Let $\Sigma \subseteq \mathbb{N}$ be a set. Let $\mathcal{A}$ be a QPT algorithm that takes 1^λ as input and outputs a classical string. $\mathcal{A}$ is a quantum advantage sampler (QAS) on Σ if the following is satisfied: There exists a polynomial p such that for any PPT algorithm $\mathcal{B}$ (that takes 1^λ as input and outputs a classical string) there exists $\lambda^* \in \mathbb{N}$ such that

$$\mathrm{SD}(\mathcal{A}(1^\lambda), \mathcal{B}(1^\lambda)) > \frac{1}{p(\lambda)} \tag{11}$$

holds for all $\lambda \geq \lambda^*$ in Σ.

Remark 3.2. For any finite set Σ, QASs on Σ always exist, but we include the case in the definition for the convenience.

We also define interactive versions of QASs, which we call Int-QASs, as follows.

Definition 3.3 (Interactive Quantum Advantage Samplers (Int-QASs)). Let $(\mathcal{A}, C)$ be a tuple of two interactive QPT algorithms $\mathcal{A}$ and C that communicate over a classical channel. $(\mathcal{A}, C)$ is an interactive quantum advantage sampler (Int-QAS) if the following is satisfied: There exists a polynomial p such that for any PPT algorithm $\mathcal{B}$ that interacts with C,

$$\mathrm{SD}(\langle \mathcal{A}, C\rangle(1^\lambda), \langle \mathcal{B}, C\rangle(1^\lambda)) > \frac{1}{p(\lambda)} \tag{12}$$

holds for all sufficiently large $\lambda \in \mathbb{N}$. Here, $\langle \mathcal{A}, C\rangle(1^\lambda)$ (resp. $\langle \mathcal{B}, C\rangle(1^\lambda)$) is the probability distribution over the transcript of the interaction between $\mathcal{A}$ (resp. $\mathcal{B}$) and C.

3.2 Relation Between QASs and Sampling Complexity Classes

We can show that the existence of QASs implies **SampBPP** $\neq$ **SampBQP**.

Lemma 3.4. *Let $\Sigma \subseteq \mathbb{N}$ be an infinite subset. If QASs on Σ exist, then* **SampBPP** $\neq$ **SampBQP**.

Remark 3.5. Note that the other direction, namely, **SampBPP** $\neq$ **SampBQP** implies the existence of QASs, does not seem to hold, because of the following reason: Assume that **SampBPP** $\neq$ **SampBQP**. Then there exists a sampling problem $\{D_x\}_x$ that is in **SampBQP** but not in **SampBPP**. The fact that $\{D_x\}_x \notin$ **SampBPP** means that for any PPT algorithm $\mathcal{B}$, there exist x and $\epsilon > 0$ such that

$$\mathrm{SD}(D_x, \mathcal{B}(x, 1^{\lfloor 1/\epsilon \rfloor})) > \epsilon. \tag{13}$$

This does not necessarily mean that a QPT algorithm $\mathcal{A}$ that samples $\{D_x\}_x$ is a QAS. For example, ϵ in Equation (13) could be $2^{-|x|}$.

3.3 Equivalence of Non-Interactive IV-PoQ and QASs

We can show the equivalence of non-interactive IV-PoQ and QASs.

Lemma 3.6. *Let $\Sigma \subseteq \mathbb{N}$ be an infinite subset. Non-interactive IV-PoQ on Σ exist if and only if QASs on Σ exist.*

3.4 QASs From Quantum Advantage Assumption

Definition 3.7 (Quantum Advantage Assumption [3, 19, 34]). We say that quantum advantage assumption holds if the following is satisfied.

(1) There exists a family $C = \{C_\lambda\}_{\lambda\in\mathbb{N}}$ of distributions such that for each $\lambda \in \mathbb{N}$, C_λ is a (uniform) QPT sampleable distribution over quantum circuits C that output λ-bit classical bit strings.
(2) There exist polynomials p and γ such that:
   (a) For all sufficiently large $\lambda \in \mathbb{N}$,

$$\Pr_{\substack{C\leftarrow C_\lambda \\ x\leftarrow\{0,1\}^\lambda}}\left[\Pr[x \leftarrow C] \geq \frac{1}{p(\lambda)2^\lambda}\right] \geq \frac{1}{\gamma(\lambda)}. \tag{14}$$

   (b) For any oracle O satisfying that for all sufficiently large $\lambda \in \mathbb{N}$,

$$\Pr_{\substack{C\leftarrow C_\lambda \\ x\leftarrow\{0,1\}^\lambda}}\left[|O(C,x) - \Pr[x \leftarrow C]| \leq \frac{\Pr[x \leftarrow C]}{p(\lambda)}\right] \geq \frac{1}{\gamma(\lambda)} - \frac{1}{p(\lambda)}, \tag{15}$$

we have that $\mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{BPP}^O$.

Remark 3.8. Traditionally, we required $\mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{BPP}^O$, but instead of it, we could consider $\mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{BQP}^O$, for example, because $\mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{BQP}^{\mathbf{NP}}$ is also unlikely.

We show that QASs can be derived from the quantum advantage assumption (Definition 3.7) plus $\mathbf{P}^{\#\mathbf{P}} \not\subseteq \mathbf{ioBPP}^{\mathbf{NP}}$.

Theorem 3.9. *If the quantum advantage assumption (Definition 3.7) holds and $\mathbf{P}^{\#\mathbf{P}} \not\subseteq \mathbf{ioBPP}^{\mathbf{NP}}$, then QASs exist.*

We can directly derive the existence of QASs from the quantum advantage assumption plus $\mathbf{P}^{\#\mathbf{P}} \not\subseteq \mathbf{ioBPP}^{\mathbf{NP}}$. However, we first introduce a useful notion, which we call hardness of quantum probability estimation (QPE), and show the theorem via hardness of QPE.

Definition 3.10 (Hardness of Quantum Probability Estimation (QPE)). We say that hardness of quantum probability estimation (QPE) holds if the following is satisfied.

(1) There exists a family $\mathcal{D} = \{\mathcal{D}_\lambda\}_{\lambda\in\mathbb{N}}$ of distributions such that for each $\lambda \in \mathbb{N}$, $\mathcal{D}_\lambda$ is a (uniform) QPT sampleable distribution over classical bit strings.

(2) There exists a polynomial p such that for any oracle PPT algorithm $\mathcal{A}^{\mathbf{NP}}$ and for all sufficiently large $\lambda \in \mathbb{N}$,

$$\Pr_{x\leftarrow\mathcal{D}_\lambda}\left[|\mathcal{A}^{\mathbf{NP}}(1^\lambda,x)-\Pr[x\leftarrow\mathcal{D}_\lambda]|\le\frac{\Pr[x\leftarrow\mathcal{D}_\lambda]}{p(\lambda)}\right]\le 1-\frac{1}{p(\lambda)}. \tag{16}$$

Remark 3.11. A similar notion was introduced in [20, 28, 34]. The main difference here is that the hardness is for PPT algorithms with **NP** oracle.

Theorem 3.9 is shown by combining the following two lemmas.

Lemma 3.12 (Based on [34]). *If the quantum advantage assumption holds and $\mathbf{P}^{\#\mathbf{P}} \not\subseteq \mathbf{ioBPP}^{\mathbf{NP}}$, then hardness of QPE holds.*

Lemma 3.13. *If hardness of QPE holds, then QASs exist.*

4 The QAS/OWF Condition

We also introduce another new concept, which we call the QAS/OWF condition.

Definition 4.1 (The QAS/OWF Condition). The QAS/OWF condition holds if there exist a polynomial p, a QPT algorithm Q that takes 1^λ as input and outputs a classical string, and a function $f:\{0,1\}^*\to\{0,1\}^*$ that is computable in classical deterministic polynomial-time such that for any PPT algorithm $\mathcal{S}$, the following holds: if we define

$$\Sigma_{\mathcal{S}} := \left\{\lambda\in\mathbb{N}\;\middle|\;\mathrm{SD}(Q(1^\lambda),\mathcal{S}(1^\lambda))\le\frac{1}{p(\lambda)}\right\}, \tag{17}$$

then f is a classically-secure OWF on $\Sigma_{\mathcal{S}}$.

We can show the following result:

Theorem 4.2. *If the QAS/OWF condition is satisfied, then quantumly-secure OWFs exist or* **SampBPP** $\neq$ **SampBQP**.

Theorem 1.2 is obtained by combining this theorem and the equivalence of IV-PoQ and the QAS/OWF condition, which will be shown in Section 5.

5 Equivalence of IV-PoQ and Classically-Secure OWPuzzs

Our main result, Theorem 1.1, that IV-PoQ exist if and only if classically-secure OWPuzzs exist is obtained by combining the following theorems.

Theorem 5.1. *If IV-PoQ exist, then Int-QASs exist.*

Theorem 5.2. *If Int-QASs exist, then the QAS/OWF condition is satisfied.*

Theorem 5.3. *If the QAS/OWF condition is satisfied, then IV-PoQ exist.*

Theorem 5.4. *If the QAS/OWF condition is satisfied, then classically-secure OWPuzzs exist.*

Theorem 5.5. *If classically-secure OWPuzzs exist, then the QAS/OWF condition is satisfied.*

6 Variants of IV-PoQ

In Section 6.1 we show equivalence among variants of IV-PoQ. In Section 6.2, we introduce *zero-knowledge* IV-PoQ and show their relationship with OWFs.

6.1 Equivalence Among Variants of IV-PoQ

We consider the following variant of IV-PoQ.

Definition 6.1 (Quantum-Verifier IV-PoQ). A quantum-verifier IV-PoQ $(\mathcal{P},\mathcal{V}_1,\mathcal{V}_2)$ is defined similarly to IV-PoQ (Definition 2.12) except that $\mathcal{V}_1$ is QPT instead of PPT but still only sends classical messages.

We show that the following equivalence theorem.

Theorem 6.2. *The following are equivalent:*

(1) *Public-coin IV-PoQ exist.*
(2) *IV-PoQ exist.*
(3) *Quantum-verifier IV-PoQ exist.*

6.2 Zero-Knowledge IV-PoQ

We give a definition of zero-knowledge IV-PoQ below.

Definition 6.3 (Zero-Knowledge IV-PoQ). An IV-PoQ $(\mathcal{P},\mathcal{V}_1,\mathcal{V}_2)$ satisfies computational (resp. statistical) zero-knowledge if for any PPT malicious verifier $\mathcal{V}_1^*$, there exists a PPT simulator $\mathcal{S}$ such that for any PPT (resp. unbounded-time) distinguisher $\mathcal{D}$,

$$\left|\Pr[\mathcal{D}(\mathrm{view}\langle\mathcal{P},\mathcal{V}_1^*\rangle(1^\lambda))=1]-\Pr[\mathcal{D}(\mathcal{S}(1^\lambda))=1]\right|\le\mathrm{negl}(\lambda) \tag{18}$$

where $\mathrm{view}\langle\mathcal{P},\mathcal{V}_1^*\rangle(1^\lambda)$ means the view of $\mathcal{V}_1^*$ which consists of the transcript and the random coin of $\mathcal{V}_1^*$.

We say that an IV-PoQ $(\mathcal{P},\mathcal{V}_1,\mathcal{V}_2)$ satisfies honest-verifier computational (resp. statistical) zero-knowledge if the above holds for the case of $\mathcal{V}_1^*=\mathcal{V}_1$.

Remark 6.4. Standard definitions of the zero-knowledge property in the literature usually consider *non-uniform* malicious verifiers and distinguishers. On the other hand, since we treat the uniform model as a default notion in this paper, we define the zero-knowledge property in the uniform-style as above. However, we remark that this choice of model of computation is not essential for the results of this subsection, and all the results of this subsection readily extend to the non-uniform setting with essentially the same proofs.

We show relationships between zero-knowledge IV-PoQ and OWFs. First, we show that honest-verifier statistical zero-knowledge IV-PoQ imply classically-secure OWFs.

Theorem 6.5. *If honest-verifier statistical zero-knowledge IV-PoQ exist, then classically-secure OWFs exist.*

Proof of Theorem 6.5. Let $(\mathcal{P},\mathcal{V}_1,\mathcal{V}_2)$ be an honest-verifier statistical zero-knowledge IV-PoQ. By the proof of Theorem 5.1, $(\mathcal{P},\mathcal{V}_1)$ is an Int-QAS, and thus by the proof of Theorem 5.2, the QAS/OWF condition holds where $Q=\langle\mathcal{P},\mathcal{V}_1\rangle$. That is, there exist a polynomial p, and a function $f:\{0,1\}^*\to\{0,1\}^*$ that is computable in classical deterministic polynomial-time such that for any PPT algorithm $\mathcal{S}$, the following holds: if we define

$$\Sigma_{\mathcal{S}} := \left\{\lambda\in\mathbb{N}\;\middle|\;\mathrm{SD}(\langle\mathcal{P},\mathcal{V}_1\rangle(1^\lambda),\mathcal{S}(1^\lambda))\le\frac{1}{p(\lambda)}\right\}, \tag{19}$$

then f is a classically-secure OWF on $\Sigma_{\mathcal{S}}$. By the honest-verifier statistical zero-knowledge property of $(\mathcal{P},\mathcal{V}_1,\mathcal{V}_2)$, there is a PPT

simulator $\mathcal{S}$ such that $\mathrm{SD}(\langle \mathcal{P}, \mathcal{V}_1\rangle(1^\lambda), \mathcal{S}(1^\lambda)) \leq \mathrm{negl}(\lambda)$.[20] For this $\mathcal{S}$, $\Sigma_{\mathcal{S}}$ consists of all but finite elements of $\mathbb{N}$ by the definition of negligible functions. Since f is a classically-secure OWF on $\Sigma_{\mathcal{S}}$, this implies the existence of classically secure OWFs by Lemma 2.5. □

Next, we show that OWFs imply computational zero-knowledge IV-PoQ.

Theorem 6.6. *If classically-secure OWFs exist, then computational zero-knowledge IV-PoQ exist.*

Zero-knowledge PoQ.. Though our main focus is on IV-PoQ, we briefly discuss zero-knowledge (efficiently-verifiable) PoQ. First, we observe that the conversion in the proof of Theorem 6.6 works in the efficiently-verifiable setting as well if we introduce an additional layer of zero-knowledge proofs where the prover proves that the committed transcript passes the verification. However, the conversion requires the base PoQ to be public-coin while most existing PoQ are not public-coin. Fortunately, we observe that we can relax the public-coin property to the "transcript-independent" property which means that the distribution of verifier's messages does not depend on the transcript and only depends on the verifier's randomness. At first glance, one may think that it is problematic if the verifier uses its private randomness to make a decision in which case the statement that "the committed transcript passes the verification" is not an **NP** statement. However, this issue can be resolved by letting the verifier reveal its randomness after receiving all the commitments from the prover.[21] Since the randomness is revealed after the commitments are sent, a cheating prover can no longer change the committed transcript by the binding property of the extractable commitment, and thus this does not affect the soundness. In summary, we can generically upgrade any PoQ with transcript-independent verifiers into a (computational) zero-knowledge PoQ by additionally assuming the existence of OWFs. To our knowledge, all existing PoQ [8, 16, 31, 32, 43, 50] have transcript-independent verifiers.

Toward equivalence between OWFs and zero-knowledge IV-PoQ.. Theorems 6.5 and 6.6 can be regarded as a loose equivalence between OWFs and zero-knowledge IV-PoQ. However, there is a gap between them as Theorem 6.5 assumes honest-verifier *statistical* zero-knowledge while Theorem 6.6 only gives *computational* zero-knowledge. It is an interesting open question if we can fill the gap.

There are two approaches toward solving that. One is to show that computational zero-knowledge IV-PoQ imply OWFs and the other is to show that OWFs imply honest-verifier statistical zero-knowledge IV-PoQ. For the former approach, the technique of [46, 49], which shows that computational zero-knowledge arguments for average-case-hard languages imply OWFs, might be useful, but it is unclear how to adapt their technique to the setting of IV-PoQ.

We also do not have solution for the latter approach either, but we have the following observation. We observe that we can construct statistical zero-knowledge IV-PoQ (or even efficiently-verifiable PoQ) if we additionally assume the existence of an **NP** search problem that is easy for QPT algorithms but hard for PPT algorithms (or equivalently publicly-verifiable one-round PoQ). To see this, we can consider a protocol where the honest quantum prover solves the **NP** search problem and then proves the knowledge of the solution by using statistical zero-knowledge arguments of knowledge for **NP**, which exists if OWFs exist [26]. Examples of classically-hard and quantumly-easy **NP** search problems are the factoring and discrete-logarithm problems (assuming classical hardness of them) [47]. Another example based on a random oracle was recently found in [50]. Thus, based on the random oracle heuristic [13], we have a candidate construction of statistical zero-knowledge PoQ from hash functions.[22] Though this is far from a construction solely based on OWFs, this can be seen as an evidence that "structured" assumptions are not necessary for statistical zero-knowledge PoQ, let alone for statistical zero-knowledge IV-PoQ.[23]

Acknowledgements. TM is supported by JST CREST JPMJCR23I3, JST Moonshot R&D JPMJMS2061-5-1-1, JST FOREST, MEXT QLEAP, the Grant-in Aid for Transformative Research Areas (A) 21H05183, and the Grant-in-Aid for Scientific Research (A) No.22H00522. YS is supported by JST SPRING, Grant Number JPMJSP2110.

References

[1] Scott Aaronson. 2010. BQP and the polynomial hierarchy. In *42nd ACM STOC*, Leonard J. Schulman (Ed.). ACM Press, 141–150. doi:10.1145/1806689.1806711
[2] Scott Aaronson. 2014. The Equivalence of Sampling and Searching. *Theory of Computing Systems* 55, 2 (01 Aug 2014), 281–298. doi:10.1007/s00224-013-9527-3
[3] Scott Aaronson and Alex Arkhipov. 2011. The computational complexity of linear optics. In *43rd ACM STOC*, Lance Fortnow and Salil P. Vadhan (Eds.). ACM Press, 333–342. doi:10.1145/1993636.1993682
[4] Scott Aaronson, Harry Buhrman, and William Kretschmer. 2024. A Qubit, a Coin, and an Advice String Walk into a Relational Problem. In *15th Innovations in Theoretical Computer Science Conference (ITCS 2024) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 287)*, Venkatesan Guruswami (Ed.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 1:1–1:24. doi:10.4230/LIPIcs.ITCS.2024.1
[5] Scott Aaronson and Lijie Chen. 2017. Complexity-theoretic foundations of quantum supremacy experiments. CCC'17: Proceedings of the 32nd Computational Complexity Conference.
[6] Scott Aaronson and Sam Gunn. 2020. On the Classical Hardness of Spoofing Linear Cross-Entropy Benchmarking. *Theory of Computing* 16, 11 (2020), 1–8. doi:10.4086/toc.2020.v016a011
[7] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. 2022. Cryptography from Pseudorandom Quantum States. In *CRYPTO 2022, Part I (LNCS, Vol. 13507)*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer, Cham, 208–236. doi:10.1007/978-3-031-15802-5_8
[8] Petia Arabadjieva, Alexandru Gheorghiu, Victor Gitton, and Tony Metger. 2025. Single-Round Proofs of Quantumness from Knowledge Assumptions. In *16th Innovations in Theoretical Computer Science Conference (ITCS 2025) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 325)*, Raghu Meka (Ed.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 8:1–8:16. doi:10.4230/LIPIcs.ITCS.2025.8
[9] Atul Singh Arora, Andrea Coladangelo, Matthew Coudron, Alexandru Gheorghiu, Uttam Singh, and Hendrik Waldner. 2023. Quantum Depth in the Random Oracle Model. In *55th ACM STOC*, Barna Saha and Rocco A. Servedio (Eds.). ACM Press, 1111–1124. doi:10.1145/3564246.3585153
[10] Boaz Barak. 2017. *The Complexity of Public-Key Cryptography*. Springer International Publishing, Cham, 45–77. doi:10.1007/978-3-319-57048-8_2

[20] Recall that we write $\langle \mathcal{P}, \mathcal{V}_1\rangle(1^\lambda)$ to mean the machine that outputs a transcript of interaction between $\mathcal{P}$ and $\mathcal{V}_1$. Since the honest-verifier statistical zero-knowledge requires the simulator to simulate both the transcript and the verifier's randomness, it is trivial to simulate only the transcript.
[21] A similar idea is used in [12].
[22] This is *not* a construction in the quantum random oracle model since we use the hash function in a non-black-box manner. Instead, we rely on the assumption that the problem considered in [50] is classically hard when the random oracle is instantiated with a concrete hash function.
[23] "Structure" is a commonly used informal term that refers to problems behind constructions of existing public key encryption such as the hardness of factoring, discrete-logarithm, learning with errors, etc. On the other hand, hash functions are often regarded as "unstructured". See [10] for more context.

[11] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. 2021. One-Way Functions Imply Secure Computation in a Quantum World. In *CRYPTO 2021, Part I (LNCS, Vol. 12825)*, Tal Malkin and Chris Peikert (Eds.). Springer, Cham, Virtual Event, 467–496. doi:10.1007/978-3-030-84242-0_17

[12] James Bartusek, Yael Tauman Kalai, Alex Lombardi, Fermi Ma, Giulio Malavolta, Vinod Vaikuntanathan, Thomas Vidick, and Lisa Yang. 2022. Succinct Classical Verification of Quantum Computation. In *CRYPTO 2022, Part II (LNCS, Vol. 13508)*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer, Cham, 195–211. doi:10.1007/978-3-031-15979-4_7

[13] Mihir Bellare and Phillip Rogaway. 1993. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *ACM CCS 93*, Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby (Eds.). ACM Press, 62–73. doi:10.1145/168588.168596

[14] Adam Bouland, Bill Fefferman, Chinmay Nirkhe, and Umesh Vazirani. 2019. On the complexity and verification of quantum random circuit sampling. *Nature Physics* 15, 2 (01 Feb 2019), 159–163. doi:10.1038/s41567-018-0318-2

[15] Zvika Brakerski, Ran Canetti, and Luowen Qian. 2023. On the Computational Hardness Needed for Quantum Cryptography. In *14th Innovations in Theoretical Computer Science Conference (ITCS 2023) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 251)*, Yael Tauman Kalai (Ed.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 24:1–24:21. doi:10.4230/LIPIcs.ITCS.2023.24

[16] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. 2021. A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device. *J. ACM* 68, 5, Article 31 (Aug. 2021), 47 pages. doi:10.1145/3441309

[17] Sergey Bravyi, David Gosset, and Robert König. 2018. Quantum advantage with shallow circuits. *Science* 362, 6412 (2018), 308–311. doi:10.1126/science.aar3106

[18] Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd. 2011. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 467 (2011), 459–472.

[19] Michael J. Bremner, Ashley Montanaro, and Dan J. Shepherd. 2016. Average-Case Complexity Versus Approximate Simulation of Commuting Quantum Computations. *Phys. Rev. Lett.* 117 (Aug 2016), 080501. Issue 8. doi:10.1103/PhysRevLett.117.080501

[20] Bruno P. Cavalar, Eli Goldin, Matthew Gray, and Peter Hall. 2024. A Meta-Complexity Characterization of Quantum Cryptography. arXiv:2410.04984 [cs.CR] https://arxiv.org/abs/2410.04984

[21] Kai-Min Chung, Eli Goldin, and Matthew Gray. 2024. On Central Primitives for Quantum Cryptography with Classical Communication. In *CRYPTO 2024, Part VII (LNCS, Vol. 14926)*, Leonid Reyzin and Douglas Stebila (Eds.). Springer, Cham, 215–248. doi:10.1007/978-3-031-68394-7_8

[22] Lance Fortnow and John Rogers. 1999. Complexity Limitations on Quantum Computation. *J. Comput. System Sci.* 59, 2 (1999), 240–252. doi:10.1006/jcss.1999.1651

[23] Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, and Seiichiro Tani. 2018. Impossibility of Classically Simulating One-Clean-Qubit Model with Multiplicative Error. *Phys. Rev. Lett.* 120 (May 2018), 200502. Issue 20. doi:10.1103/PhysRevLett.120.200502

[24] Eli Goldin, Tomoyuki Morimae, Saachi Mutreja, and Takashi Yamakawa. 2024. CountCrypt: Quantum Cryptography between QCMA and PP. Cryptology ePrint Archive, Paper 2024/1707. https://eprint.iacr.org/2024/1707

[25] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. 2021. Oblivious Transfer Is in MiniQCrypt. In *EUROCRYPT 2021, Part II (LNCS, Vol. 12697)*, Anne Canteaut and François-Xavier Standaert (Eds.). Springer, Cham, 531–561. doi:10.1007/978-3-030-77886-6_18

[26] Iftach Haitner, Minh-Huyen Nguyen, Shien Jin Ong, Omer Reingold, and Salil Vadhan. 2009. Statistically Hiding Commitments and Statistical Zero-Knowledge Arguments from Any One-Way Function. *SIAM J. Comput.* 39, 3 (2009), 1153–1218. doi:10.1137/080725404

[27] Danny Harnik, Joe Kilian, Moni Naor, Omer Reingold, and Alon Rosen. 2005. On Robust Combiners for Oblivious Transfer and Other Primitives. In *EUROCRYPT 2005 (LNCS, Vol. 3494)*, Ronald Cramer (Ed.). Springer, Berlin, Heidelberg, 96–113. doi:10.1007/11426639_6

[28] Taiga Hiroka and Tomoyuki Morimae. 2024. Quantum Cryptography from Meta-Complexity. Cryptology ePrint Archive, Paper 2024/1539. https://eprint.iacr.org/2024/1539

[29] Russell Impagliazzo and Michael Luby. 1989. One-way Functions are Essential for Complexity Based Cryptography (Extended Abstract). In *30th FOCS*. IEEE Computer Society Press, 230–235. doi:10.1109/SFCS.1989.63483

[30] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. 2018. Pseudorandom Quantum States. In *CRYPTO 2018, Part III (LNCS, Vol. 10993)*, Hovav Shacham and Alexandra Boldyreva (Eds.). Springer, Cham, 126–152. doi:10.1007/978-3-319-96878-0_5

[31] Gregory D. Kahanamoku-Meyer, Soonwon Choi, Umesh V. Vazirani, and Norman Y. Yao. 2022. Classically verifiable quantum advantage from a computational Bell test. *Nature Physics* 18, 8 (01 Aug 2022), 918–924. doi:10.1038/s41567-022-01643-7

[32] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. 2023. Quantum Advantage from Any Non-local Game. In *55th ACM STOC*, Barna Saha and Rocco A. Servedio (Eds.). ACM Press, 1617–1628. doi:10.1145/3564246.3585164

[33] Dakshita Khurana and Kabir Tomer. 2024. Commitments from Quantum One-Wayness. In *56th ACM STOC*, Bojan Mohar, Igor Shinkar, and Ryan O'Donnell (Eds.). ACM Press, 968–978. doi:10.1145/3618260.3649654

[34] Dakshita Khurana and Kabir Tomer. 2024. Founding Quantum Cryptography on Quantum Advantage, or, Towards Cryptography from #P-Hardness. Cryptology ePrint Archive, Paper 2024/1490. https://eprint.iacr.org/2024/1490

[35] W. Kretschmer. 2021. Quantum pseudorandomness and classical complexity. *TQC 2021* (2021). doi:10.4230/LIPICS.TQC.2021.2

[36] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. 2023. Quantum Cryptography in Algorithmica. In *55th ACM STOC*, Barna Saha and Rocco A. Servedio (Eds.). ACM Press, 1589–1602. doi:10.1145/3564246.3585225

[37] Leonid A. Levin. 1985. One-Way Functions and Pseudorandom Generators. In *17th ACM STOC*. ACM Press, 363–365. doi:10.1145/22145.22185

[38] Alex Lombardi, Fermi Ma, and John Wright. 2024. A One-Query Lower Bound for Unitary Synthesis and Breaking Quantum Cryptography. In *56th ACM STOC*, Bojan Mohar, Igor Shinkar, and Ryan O'Donnell (Eds.). ACM Press, 979–990. doi:10.1145/3618260.3649650

[39] Tomoyuki Morimae. 2017. Hardness of classically sampling the one-clean-qubit model with constant total variation distance error. *Phys. Rev. A* 96 (Oct 2017), 040302. Issue 4. doi:10.1103/PhysRevA.96.040302

[40] Tomoyuki Morimae, Yuki Shirakawa, and Takashi Yamakawa. 2024. Cryptographic Characterization of Quantum Advantage. arXiv:2410.00499 [quant-ph] https://arxiv.org/abs/2410.00499

[41] Tomoyuki Morimae, Shogo Yamada, and Takashi Yamakawa. 2024. Quantum Unpredictability *(LNCS)*. Springer, Singapore, 3–32. doi:10.1007/978-981-96-0947-5_1

[42] Tomoyuki Morimae and Takashi Yamakawa. 2022. Quantum Commitments and Signatures Without One-Way Functions. In *CRYPTO 2022, Part I (LNCS, Vol. 13507)*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer, Cham, 269–295. doi:10.1007/978-3-031-15802-5_10

[43] Tomoyuki Morimae and Takashi Yamakawa. 2023. Proofs of Quantumness from Trapdoor Permutations. In *ITCS 2023*, Yael Tauman Kalai (Ed.), Vol. 251. LIPIcs, 87:1–87:14. doi:10.4230/LIPIcs.ITCS.2023.87

[44] Tomoyuki Morimae and Takashi Yamakawa. 2024. Quantum Advantage from One-Way Functions. In *CRYPTO 2024, Part V (LNCS, Vol. 14924)*, Leonid Reyzin and Douglas Stebila (Eds.). Springer, Cham, 359–392. doi:10.1007/978-3-031-68388-6_13

[45] Rafail Ostrovsky. 1991. One-Way Functions, Hard on Average Problems, and Statistical Zero-Knowledge Proofs. *Computational Complexity Conference* (1991).

[46] Rafail Ostrovsky and Avi Wigderson. 1993. One-Way Fuctions are Essential for Non-Trivial Zero-Knowledge. In *Second Israel Symposium on Theory of Computing Systems, ISTCS 1993, Natanya, Israel, June 7-9, 1993, Proceedings*. IEEE Computer Society, 3–17. doi:10.1109/ISTCS.1993.253489

[47] Peter W. Shor. 1994. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *35th FOCS*. IEEE Computer Society Press, 124–134. doi:10.1109/SFCS.1994.365700

[48] B. M. Terhal and D. P. DiVincenzo. 2004. Adaptive quantum computation, constant-depth circuits and Arthur-Merlin games. *Quant. Inf. Comput.* 4, 2 (2004), 134–145.

[49] Salil P. Vadhan. 2006. An Unconditional Study of Computational Zero Knowledge. *SIAM J. Comput.* (2006).

[50] Takashi Yamakawa and Mark Zhandry. 2024. Verifiable Quantum Advantage without Structure. *J. ACM* 71, 3, Article 20 (jun 2024), 50 pages. doi:10.1145/3658665

Received 2024-11-01; accepted 2025-02-01