Quantum Cryptography from Meta-Complexity

Taiga Hiroka[1] and Tomoyuki Morimae[1]

[1]Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto, Japan
{taiga.hiroka,tomoyuki.morimae}@yukawa.kyoto-u.ac.jp

Abstract

In classical cryptography, one-way functions (OWFs) are the minimal assumption, while recent active studies have demonstrated that OWFs are not necessarily the minimum assumption in quantum cryptography. Several new primitives have been introduced such as pseudorandom unitaries (PRUs), pseudorandom function-like state generators (PRFSGs), pseudorandom state generators (PRSGs), one-way state generators (OWSGs), one-way puzzles (OWPuzzs), and EFI pairs. They are believed to be weaker than OWFs, but they still imply many useful applications such as private-key quantum money schemes, secret-key encryption, message authentication codes, digital signatures, commitments, and multiparty computations. Now that the possibility of quantum cryptography without OWFs has opened up, the most important goal in the field is to provide them with concrete instantiations. For example, in classical cryptography, there are many instantiations of OWFs based on concrete hardness assumptions, such as the hardness of discrete logarithms or learning with errors. The study of generic primitives is justified by the existence of concrete instantiations. On the other hand, in quantum cryptography, all known constructions of those primitives are only from OWFs. We therefore have the following important open problem: *Do they have instantiations based on some concrete hardness assumptions that will not imply OWFs?* Ideally, the assumptions should be the ones that are studied in other contexts than cryptography. In this paper, we give a candidate answer to the question by showing that quantum-average-hardness of GapK problem implies the existence of OWPuzzs. A GapK problem is a promise problem to decide whether a given bit string has a small Kolmogorov complexity or not. Its quantum-average-hardness means that an instance is sampled from a quantum-polynomial-time-samplable distribution, and no quantum-polynomial-time algorithm can solve the problem with high probability. As far as we know, this is the first time that a "Microcrypt" primitive is constructed based on concrete hardness assumptions that do not seem to imply OWFs. Moreover, the assumptions are studied in other contexts than cryptography, especially in the field of meta-complexity. (Note: During the preparation of this manuscript, Khurana and Tomer [KT24b] uploaded a concurrent work.)

1 Introduction

In classical cryptography, the existence of one-way functions (OWFs) is the minimal assumption [IL89], because they are existentially equivalent to many primitives, such as pseudorandom generators (PRGs), pseudorandom functions (PRFs), secret-key encryption (SKE), message authentication code (MAC), digital signatures, and commitments. Moreover, almost all primitives (including public-key encryption and multiparty computations) imply OWFs.

On the other hand, in the quantum cryptography, OWFs are not necessarily the minimum assumption [Kre21, MY22, AQY22]. Several new primitives have been introduced such as pseudorandom unitaries (PRUs) [JLS18], pseudorandom function-like state generators (PRFSGs) [AQY22, AGQY22], pseudorandom state generators (PRSGs) [JLS18], one-way state generators (OWSGs) [MY22], one-way puzzles (OWPuzzs) [KT24a], and EFI pairs [BCQ23]. Although they are believed to be weaker than OWFs [Kre21, KQST23, LMW24], they still imply many useful applications such as private-key quantum money schemes [JLS18], SKE [AQY22], MAC [AQY22], digital signatures [MY22], commitments [MY22, AQY22], and multiparty computations [MY22, AQY22].

Now that the possibility of a quantum cryptographic world without OWFs has opened up, the most important goal in the field is to provide these primitives with concrete instantiations. For example, in classical cryptography, there are many instantiations of OWFs based on some concrete hardness assumptions, such as the hardness of discrete logarithms or learning with errors. The study of generic primitives is justified by the existence of concrete instantiations. On the other hand, in quantum cryptography, all known constructions of those primitives are only from OWFs [JLS18, HM24]. We therefore have the following important open problem:

Do those primitives have instantiations based on some concrete hardness assumptions that will not imply OWFs?

Ideally, the assumptions should be the ones that are studied in other contexts than cryptography.

In this paper, we give a candidate answer to the open problem. We show the following:

Theorem 1.1 (Informal). *If GapK problem is quantum-average-hard, then OWPuzzs exist.*

OWPuzzs [KT24a] are a quantum analogue of OWFs, and one of the most fundamental primitives in quantum cryptography. A OWPuzz is a pair $(\mathsf{Samp}, \mathsf{Ver})$ of two algorithms. Samp is a quantum polynomial-time (QPT) algorithm that, on input the security parameter 1^λ, outputs two classical bit strings, ans and puzz. Ver is an unbounded algorithm that, on input $(\mathsf{puzz}, \mathsf{ans}')$, outputs $\top/\bot$. Correctness requires that Ver accepts $(\mathsf{puzz}, \mathsf{ans}) \leftarrow \mathsf{Samp}(1^\lambda)$ with high probability. Security requires that no QPT adversary that receives puzz can outputs ans' such that $(\mathsf{puzz}, \mathsf{ans}')$ is accepted by Ver with high probability. OWPuzzs are implied by almost all primitives including PRUs, PRFSGs, PRSGs, OWSGs, SKE, MAC, private-key quantum money schemes, etc. [MY24, MY22, KT24a]. OWPuzzs imply EFI pairs, commitments, multiparty computations, and quantum advantage [KT24a, GLSV21, BCKM21, MSY24].

A GapK problem [IRS21] is a promise problem to decide whether a given classical bit string x has a small Kolmogorov complexity or not. Roughly speaking, a Kolmogorov complexity of a bit string x is the length of the shortest program that outputs x. (For more details, see for example [LV19].) Its quantum-average-hardness means that an instance x is sampled from a QPT samplable distribution D, and no QPT algorithm can decide whether x has a small Kolmogorov complexity or not with high probability. If D is PPT samplable, we call it classical-average-hardness. Classical-average-hardness of several problems related to Kolmogorov complexity has been well studied in classical complexity theory and classical cryptography [LP20, IRS21, LP22]. We consider its quantum version, namely, *quantum*-average-hardness where the instance sampling is in QPT. Because PPT is a special case of QPT, our assumption is more general than the classical one.

We believe that our assumption will not imply OWFs, because of the following argument.[1] In the classical case, classical-average-hardness of GapK problem is equivalent to the existence of OWFs [IRS21]. With a similar proof, we can show that quantum-average-hardness of GapK problem is implied by the existence of (quantumly-secure) *quantum OWFs* (QOWFs), which are OWFs with *quantum* evaluations.[2][3] If our assumption implies OWFs, then QOWFs imply OWFs. However, it seems unlikely that QOWFs imply OWFs.

[1] See also Section 1.2.

[2] For a OWF f, $f(x)$ is computed in classical deterministic polynomial time. For a QOWF f, $f(x)$ is computed in quantum almost-deterministic polynomial time.

[3] In the classical case, OWFs are constructed from classical-average-hardness of GapK problem, but we do not know how to apply the proof technique to the quantum case.

As far as we know, this is the first time that a "Microcrypt" primitive (i.e., OWPuzzss) is instanciated with concrete hardness assumptions that do not seem to imply OWFs. Moreover, the assumptions are studied in other contexts than cryptography, especially in the field of meta-complexity.

Finally, we note that during the preparation of this manuscript, Khurana and Tomer uploaded a concurrent work [KT24b]. See Section 1.3.

1.1 Technical Overview

Our main result, Theorem 1.1, is the construction of QWPuzzs from quantum-average-hardness of GapK problem. In this subsection, we provide a high-level overview of the proof.

A GapK problem $\mathsf{GapK}[s_1, s_2]$ is the following promise problem: Given a bit string x, decide $K(x) \leq s_1$ or $K(x) \geq s_2$, where $K(x)$ is the Kolmogorov complexity of x, i.e., the length of the shortest program that a universal Turing machine outputs x. Its average-hardness means that an instance x is sampled from a certain distribution, and no QPT algorithm can decide whether $K(x) \leq s_1$ or $K(x) \geq s_2$ with sufficiently large probability. More precisely, we require that there exist an integer $k > 0$ and a family $\mathcal{D} := \{\mathcal{D}_n\}_{n\in\mathbb{N}}$ of distributions such that, for any QPT algorithm $\mathcal{A}$,

$$\Pr_{x\leftarrow\mathcal{D}_n}[\mathsf{no} \leftarrow \mathcal{A}(x) \wedge x \in \mathcal{L}_{\mathsf{Yes}}] + \Pr_{x\leftarrow\mathcal{D}_n}[\mathsf{yes} \leftarrow \mathcal{A}(x) \wedge x \in \mathcal{L}_{\mathsf{No}}] \geq \frac{1}{n^k} \tag{1}$$

for all sufficiently large $n \in \mathbb{N}$, where $\mathcal{L}_{\mathsf{Yes}}$ (resp. $\mathcal{L}_{\mathsf{No}}$) is the set of yes (resp. no) instances of the GapK problem.

If $\mathcal{D}$ is QPT (resp. PPT) samplable, which means that there exists a QPT (resp. PPT) algorithm $\mathcal{Q}$ such that $\mathcal{Q}(1^n)$ exactly samples from $\mathcal{D}_n$ for each $n \in \mathbb{N}$, we say that the above hardness is quantum-(resp. classical-)average-hardness.

We do not directly show the existence of OWPuzzs from quantum-average-hardness of GapK problem. We further introduce another assumption, and show that quantum-average-hardness of GapK problem implies the assumption, and that the assumption implies OWPuzzs. The assumption is quantum-average-hardness of probability estimation problem. A probability estimation problem is the following one: Let D be a distribution. The goal is, for a given bit string x, to compute a value η such that η is a good approximation of $\Pr[x \leftarrow D]$. Its average-hardness means that x is sampled from D, and no QPT algorithm that gets x as input can output a good approximation of $\Pr[x \leftarrow D]$ with sufficiently high probability. Quantum-(resp. classical-)average-hardness means that D is QPT (PPT) samplable. More precisely, we require that there exist a real $c > 1$, an integer $q > 0$, and a QPT samplable distribution family $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbb{N}}$ such that, for any QPT algorithm $\mathsf{Estimate}$,

$$\Pr_{x\leftarrow\mathcal{D}_n}\left[\frac{1}{c}\Pr[x \leftarrow \mathcal{D}_n] \leq \mathsf{Estimate}(x) \leq c\Pr[x \leftarrow \mathcal{D}_n]\right] \leq 1 - \frac{1}{n^q} \tag{2}$$

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

We first explain how OWPuzzs are constructed from quantum-average-hardness of probability estimation problem. [CGG24] showed the equivalence between OWPuzzs and distributional OWPuzzs. Hence if OWPuzzs do not exist, then distributional OWPuzzs do not as well. Then, there exists a QPT algorithm Invert that, given a marginal distribution $(x_1, ..., x_{i-1}) \leftarrow \mathcal{D}_n$, can sample x_i, such that the statistical distance between $(x_1, ..., x_i)_{(x_1,...,x_i)\leftarrow\mathcal{D}_n}$ and $(x_1, ..., x_{i-1}, \mathsf{Invert}(x_1, ..., x_{i-1}))_{(x_1,...,x_{i-1})\leftarrow\mathcal{D}_n}$ is small. Then, by repeatedly running Invert, we can compute an approximation of $\Pr[(x_1, ..., x_n) \leftarrow \mathcal{D}_n]$. This means that quantum-average-hardness of probability estimation problem does not hold.

Next, let us explain how quantum-average-hardness of probability estimation problem is derived from quantum-average-hardness of GapK problem.[4] Assume that quantum-average-hardness of probability estimation problem does not hold. Then, there is a QPT algorithm $\mathsf{Estimate}$ that can estimate output probability of any QPT distribution. We construct an algorithm $\mathcal{A}$ that solves GapK problem as follows: given $x \leftarrow \mathcal{D}_n$, run $\mathsf{Estimate}(x)$ and output yes if the approximation of $\Pr[x \leftarrow \mathcal{D}_n]$ is larger than a certain threshold. Intuitively, $K(x)$ being small (resp. large) if $\Pr[x \leftarrow \mathcal{D}_n]$ is large (resp. small)[5], and therefore $\mathcal{A}$ can correctly decide whether $K(x)$ is small or large.

[4] This was essentially shown in [IRS21], but we slightly modified the proof for our purpose.

[5] If $\Pr[x \leftarrow \mathcal{D}_n]$ is large, x can be taken from the support of $\mathcal{D}_n$, which allows a shorter program to output x.

1.2 Discussion

In this paper, we construct OWPuzzs from the assumption, quantum-average-hardness of GapK problem. The assumption requires the existence of a QPT samplable distribution family $\mathcal{D}$ whose outputs are hard instances on average, but the assumption itself holds even if $\mathcal{D}$ is *PPT* samplable, because PPT is a special case of QPT. However, in that case, the assumption implies OWFs as well, which is not interesting in the present context. Hence if we require the assumption to be "OWFs-free", we need an additional condition that the distribution family $\mathcal{D}$ that satisfies the assumption should not be PPT samplable. In other words, we need the existence of quantum advantage to construct (OWFs-free) OWPuzzs.[6] It is then an interesting open problem whether we can construct "Microcrypt" primitives solely from quantum advantage.[7] Because quantum advantage restricts only classical power and does not say anything about the upper bound of quantum power, quantumly-secure crypto primitives solely from quantum advantage seem to be unlikely, but as far as we know, there is no proof that prohibits it.

1.3 Concurrent Work

During the preparation of this manuscript, Khurana and Tomer uploaded [KT24b]. They introduce two hardness assumptions, Assumption 1 and Assumption 2. Assumption 1 is a well-studied assumption in the field of quantum advantage, because Assumption 1 implies the existence of sampling-based quantum advantage. They show that Assumption 1 plus a mild complexity assumption, $\mathbf{P}^{\sharp\mathsf{P}} \not\subseteq (io)\mathbf{BQP}/\mathbf{qpoly}$, imply Assumption 2. They then show that Assumption 2 is equivalent to the existence of OWPuzzs.

Their Assumption 2 is similar to our assumption, Assumption 3.2, from which we construct OWPuzzs. Moreover, their proof of "Assumption 2 $\Rightarrow$ OWPuzzs" looks similar to our proof of "Assumption 3.2 $\Rightarrow$ OWPuzzs". However, there are the following two different points: They show that the existence of OWPuzzs implies Assumption 2, but we do not show that direction. On the other hand, we derive Assumption 3.2 from the quantum-average-hardness of GapK problem.

In addition, their Assumption 2 allows quantum advice for adversaries. In this paper we do not explicitly consider quantum advice, but we believe that our proofs can be straightforwardly extended to the case with quantum advice.

2 Preliminaries

Basic notations. We use the standard notations of cryptography and quantum information. λ is the security parameter. negl is a negligible function. $[n]$ denotes the set $\{1, 2, ..., n\}$. QPT stands for quantum polynomial time. For an algorithm (or a Turing machine) $\mathcal{A}$, $y \leftarrow \mathcal{A}(x)$ means that $\mathcal{A}$ runs on input x and outputs y. $\mathsf{TD}(\rho, \sigma)$ is the trace distance between two quantum states ρ and σ. The maximum probability to distinguish ρ and σ is $\frac{1}{2} + \frac{1}{2}\mathsf{TD}(\rho, \sigma)$. $\mathsf{SD}(D, E)$ is the statistical distance between two distributions D and E.

QPT samplability. In this paper, we use the notion of QPT samplability defined as follows.

Definition 2.1 (QPT Samplable Distribution Family). *We say that a family $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbb{N}}$ of distributions is a QPT samplable distribution family if there exists a uniform QPT algorithm $\mathcal{Q}$ such that $\mathcal{Q}(1^n)$ can exactly sample from $\mathcal{D}_n$ for each $n \in \mathbb{N}$.*

One-way puzzles. We also review the definition of OWPuzzs.

Definition 2.2 (One-Way Puzzles (OWPuzzs) [KT24a]). *A one-way puzzle is a pair $(\mathsf{Samp}, \mathsf{Ver})$ of algorithms with the following syntax:*

- $\mathsf{Samp}(1^\lambda) \to (\mathsf{ans}, \mathsf{puzz})$*: It is a QPT algorithm that, on input 1^λ, outputs two classical bit strings $(\mathsf{ans}, \mathsf{puzz})$.*

[6] This observation was also given in [KT24b], and can also be obtained from the equivalence between inefficient-verifier proofs of quantumness (IV-PoQ) and classically-secure OWPuzzs [MSY24].

[7] [KT24b] constructed OWPuzzs not from quantum advantage but from assumptions that imply quantum advantage. [MSY24] constructed a crypto primitive from quantum advantage, but the primitive is only classically-secure.

- $\mathsf{Ver}(\mathsf{ans}', \mathsf{puzz}) \to \top/\bot$*: It is an unbounded algorithm that, on input* $(\mathsf{ans}', \mathsf{puzz})$*, outputs* $\top/\bot$*.*

We require the following correctness and security.

Correctness:

$$\Pr_{(\mathsf{ans},\mathsf{puzz})\leftarrow\mathsf{Samp}(1^\lambda)}[\top \leftarrow \mathsf{Ver}(\mathsf{ans}, \mathsf{puzz})] \geq 1 - \mathsf{negl}(\lambda). \tag{3}$$

Security: *For any* ***uniform*** *QPT adversary* $\mathcal{A}$*,*

$$\Pr_{(\mathsf{ans},\mathsf{puzz})\leftarrow\mathsf{Samp}(1^\lambda)}[\top \leftarrow \mathsf{Ver}(\mathcal{A}(1^\lambda, \mathsf{puzz}), \mathsf{puzz})] \leq \mathsf{negl}(\lambda). \tag{4}$$

[CGG24] introduced distributional OWPuzzs, and show their equivalence to OWPuzzs. The following lemma comes from the equivalence. We will use the lemma later.

Lemma 2.3 ([CGG24]). *Suppose that (resp. infinitely-often) OWPuzzs do not exist. Then, for any QPT samplable distribution family* $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbb{N}}$*, where* $\mathcal{D}_n$ *is a distribution over* $\{0,1\}^n$*, and for any constant* $t > 0$*, there exists a uniform QPT algorithm* Invert *that outputs a single bit such that*

$$\mathsf{SD}\left((y_1, ..., y_i)_{(y_1,...,y_i)\leftarrow\mathcal{D}_n}, (y_1, ..., y_{i-1}, \mathsf{Invert}(i, y_1, ..., y_{i-1}))_{(y_1,...,y_{i-1})\leftarrow\mathcal{D}_n}\right) \leq \frac{1}{n^t} \tag{5}$$

for all $i \in [n]$ *and infinitely many* $n \in \mathbb{N}$ *(resp. all sufficiently large* $n \in \mathbb{N}$*). Here* y_j *is the* i*th bit of* $y \in \{0,1\}^n$*, and* $(y_1, ..., y_i) \leftarrow \mathcal{D}_n$ *is the marginal distribution over the first* i *bits of the output of* $\mathcal{D}_n$*.*

Kolmogorov complexity. We also review some basics of Kolmogorov complexity. For details, see for example [LV19].

Throughout this paper, we consider a fixed deterministic universal Turing machine U.

Definition 2.4 (Kolmogorov Complexity). *The Kolmogorov complexity* $\mathrm{K}(x)$ *for a string* x *is defined as*

$$\mathrm{K}(x) := \min_{d\in\{0,1\}^*}\{|d| : x \leftarrow U(d)\}. \tag{6}$$

Definition 2.5 (GapK**).** *Let* $s_1 : \mathbb{N} \to \mathbb{N}$ *and* $s_2 : \mathbb{N} \to \mathbb{N}$ *be functions.* $\mathsf{GapK}[s_1, s_2] := (L_{\mathsf{Yes}}, L_{\mathsf{No}}) \subseteq \{0,1\}^*$ *is a promise problem whose yes instances are strings* x *such that* $K(x) \leq s_1(|x|)$ *and no instances are strings* x *such that* $K(x) \geq s_2(|x|)$*.*

3 OWPuzzs from quantum-average-hardness of GapK

In this section, we introduce two assumptions, and show our main result, Theorem 1.1.

3.1 Assumptions

Here we introduce two assumptions.

Assumption 3.1 (Quantum-Average-Hardness of GapK). Let $\Delta : \mathbb{N} \to \mathbb{N}$ be a polynomial-time-computable function such that $\Delta(n) = w(\log(n))$. There exist an integer $k > 0$, a polynomial-time-computable function $s : \mathbb{N} \to \mathbb{N}$, and a QPT samplable distribution family $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbb{N}}$ such that for any QPT algorithm $\mathcal{A}$,

$$\Pr_{x\leftarrow\mathcal{D}_n}[\mathsf{no} \leftarrow \mathcal{A}(x) \wedge x \in \mathcal{L}_{\mathsf{Yes}}] + \Pr_{x\leftarrow\mathcal{D}_n}[\mathsf{yes} \leftarrow \mathcal{A}(x) \wedge x \in \mathcal{L}_{\mathsf{No}}] \geq \frac{1}{n^k} \tag{7}$$

for all sufficiently large $n \in \mathbb{N}$, where $\mathcal{L}_{\mathsf{Yes}}$ (resp. $\mathcal{L}_{\mathsf{No}}$) is the set of yes (resp. no) instances of $\mathsf{GapK}[s - \Delta, s]$.

Assumption 3.2 (Quantum-Average-Hardness of Quantum Probability Estimation). There exists a real $c > 1$ and an integer $q > 0$ and a QPT samplable distribution family $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbb{N}}$ such that, for any QPT algorithm $\mathsf{Estimate}$, we have

$$\Pr_{x\leftarrow\mathcal{D}_n}\left[\frac{1}{c}\Pr[x\leftarrow\mathcal{D}_n] \le \mathsf{Estimate}(x) \le c\Pr[x\leftarrow\mathcal{D}_n]\right] \le 1-\frac{1}{n^q} \tag{8}$$

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

3.2 Theorems

We can show the following two theorems.[8] By combining them, we obtain our main result, Theorem 1.1.

Theorem 3.3. *Assumption 3.1 implies Assumption 3.2.*

Theorem 3.4. *Assumption 3.2 implies the existence of OWPuzzs.*

In the following two subsections, we show these theorems.

3.3 Proof of Theorem 3.3

In this subsection, we show Theorem 3.3. The proof was essentially given in [IRS21], but here we re-provide a proof with slightly different parameters, because it is convenient to show Theorem 3.4 (and also for the convenience of readers).

Proof of Theorem 3.3. In the following, for the notational simplicity, we often omit $|y|$ of $s(|y|)$ and $\Delta(|y|)$, and just write s and Δ, respectively. For contradiction, we assume that Assumption 3.2 does not follow, and construct a QPT algorithm $\mathcal{A}$ that breaks Assumption 3.1. For an arbitrary constant $k > 0$, there exists a constant $q > 0$ such that

$$\frac{1}{n^q} + 2^{-\Delta/3} \le \frac{1}{n^k} \tag{9}$$

for all sufficiently large $n \in \mathbb{N}$. Because we assume that Assumption 3.2 does not hold, for any $q > 0$ and for any QPT samplable distribution family $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbb{N}}$ there exists a QPT algorithm $\mathsf{Estimate}$ such that

$$\Pr_{y\leftarrow\mathcal{D}_n}\left[\frac{99}{100}\Pr[y\leftarrow\mathcal{D}_n] \le \mathsf{Estimate}(y) \le \frac{100}{99}\Pr[y\leftarrow\mathcal{D}_n]\right] > 1-\frac{1}{n^q} \tag{10}$$

for infinitely many $n \in \mathbb{N}$.

Our QPT algorithm $\mathcal{A}$ that solves $\mathsf{GapK}[s-\Delta, s]$ is constructed as follows: It receives an instance $y \leftarrow \mathcal{D}_n$ and runs $\mathsf{Estimate}(y)$. $\mathcal{A}$ outputs yes indicating $y \in \mathcal{L}_{\mathsf{yes}}$ if $\mathsf{Estimate}(y) \ge 2^{-s+\Delta/2}$, and outputs no otherwise indicating $y \in \mathcal{L}_{\mathsf{no}}$.

We use the following Claims 3.5 and 3.6, which we will prove later.

Claim 3.5. For all sufficiently large $n \in \mathbb{N}$,

$$\Pr_{y\leftarrow\mathcal{D}_n}\left[\Pr[y\leftarrow\mathcal{D}_n] < \frac{100}{99}\cdot 2^{-s+\Delta/2} \wedge K(y) \le s-\Delta\right] \le 2^{-\Delta/3}. \tag{11}$$

Claim 3.6. We have

$$\Pr_{y\leftarrow\mathcal{D}_n}\left[\Pr[y\leftarrow\mathcal{D}_n] \ge \frac{99}{100}\cdot 2^{-s+\Delta/2} \wedge K(y) \ge s\right] = 0 \tag{12}$$

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

[8] Theorem 3.3 was essentially shown in [IRS21]. Here, we show it with slightly different parameters for our purpose.

Now, we have

$$\Pr_{y\leftarrow\mathcal{D}_n}[\mathsf{no}\leftarrow\mathcal{A}(y)\wedge y\in\mathcal{L}_{\mathsf{Yes}}]+\Pr_{y\leftarrow\mathcal{D}_n}[\mathsf{yes}\leftarrow\mathcal{A}(y)\wedge y\in\mathcal{L}_{\mathsf{No}}] \tag{13}$$

$$=\Pr_{y\leftarrow\mathcal{D}_n}[\mathsf{Estimate}(y)<2^{-s+\Delta/2}\wedge K(y)\leq s-\Delta]+\Pr_{y\leftarrow\mathcal{D}_n}[\mathsf{Estimate}(y)\geq 2^{-s+\Delta/2}\wedge K(y)\geq s] \tag{14}$$

$$<\frac{1}{n^q}+\Pr_{y\leftarrow\mathcal{D}_n}\left[\Pr[y\leftarrow\mathcal{D}_n]<\frac{100}{99}\cdot 2^{-s+\Delta/2}\wedge K(y)\leq s-\Delta\right]+\Pr_{y\leftarrow\mathcal{D}_n}\left[\Pr[y\leftarrow\mathcal{D}_n]\geq\frac{99}{100}\cdot 2^{-s+\Delta/2}\wedge K(y)\geq s\right] \tag{15}$$

$$\leq\frac{1}{n^q}+2^{-\Delta/3} \tag{16}$$

$$\leq\frac{1}{n^k}, \tag{17}$$

for infinitely many $n\in\mathbb{N}$, where, in the first inequality, we have used Equation (10), that is, $\frac{99}{100}\Pr[y\leftarrow\mathcal{D}_n]\leq\mathsf{Estimate}(y)\leq\frac{100}{99}\Pr[y\leftarrow\mathcal{D}_n]$ with probability at least $1-\frac{1}{n^q}$ and, in the second inequality, we have used Claims 3.5 and 3.6.

Proof of Claim 3.5. Let

$$\mathsf{Low}:=\left\{y\in\{0,1\}^n:K(y)\leq s-\Delta\text{ and }\Pr[y\leftarrow\mathcal{D}_n]<\frac{100}{99}2^{-s+\Delta/2}\right\}. \tag{18}$$

Because the number of string $y\in\{0,1\}^n$ such that $K(y)\leq s-\Delta$ is at most $2^{s-\Delta+1}$, we have

$$|\mathsf{Low}|\leq 2^{s-\Delta+1}. \tag{19}$$

Therefore, we have

$$\Pr_{y\leftarrow\mathcal{D}_n}[y\in\mathsf{Low}]=\sum_{y\in\mathsf{Low}}\Pr[y\leftarrow\mathcal{D}_n] \tag{20}$$

$$\leq\sum_{y\in\mathsf{Low}}\frac{100}{99}2^{-s+\Delta/2} \tag{21}$$

$$\leq 2^{s-\Delta+1}\cdot\frac{100}{99}2^{-s+\Delta/2} \tag{22}$$

$$\leq 2^{-\Delta/3} \tag{23}$$

for all sufficiently large $n\in\mathbb{N}$, which shows the claim. □

Proof of Claim 3.6. Let

$$\mathsf{High}:=\left\{y\in\{0,1\}^n:\Pr[y\leftarrow\mathcal{D}_n]\geq\frac{99}{100}2^{-s+\Delta/2}\right\}. \tag{24}$$

Then, we have $|\mathsf{High}|\leq\frac{100}{99}2^{s-\Delta/2}$. Let $\mathcal{Q}$ be a QPT algorithm such that $\mathcal{Q}(1^n)$ exactly samples from $\mathcal{D}_n$. There exists a Turing machine $\mathcal{M}$ that generates any $y\in\mathsf{High}$ by specifying the code of $\mathcal{Q}$, n, $\frac{99}{100}2^{-s+\Delta/2}$ and the index i of $y\in\mathsf{High}$[9]. The code of $\mathcal{Q}$ and $\mathcal{M}$ are described by constant bits, n and $\frac{100}{99}2^{-s+\Delta/2}$ are described by $O(\log(n))$ bits, and the index i of $y\in\mathsf{High}$ is described by $(s-\Delta/2+1)$-bits. Therefore, the Kolmogorov complexity of $y\in\mathsf{High}$ is at most

$$O(1)+O(\log(n))+s-\Delta/2+1\leq s-w(\log(n)) \tag{25}$$

for all sufficiently large $n\in\mathbb{N}$. Hence Equation (12) is obtained for all sufficiently large $n\in\mathbb{N}$. □

□

[9] An inefficient Turing machine $y\leftarrow\mathcal{M}\left(\mathcal{Q},n,\frac{99}{100}2^{-s+\Delta/2},i\right)$ works as follows: For all $y\in\{0,1\}^n$, $\mathcal{M}$ computes $\Pr[y\leftarrow\mathcal{Q}(1^n)]$ and adds $y\in\mathsf{High}$ if $\Pr[y\leftarrow\mathcal{Q}(1^n)]\geq\frac{99}{100}2^{-s+\Delta/2}$. $\mathcal{M}$ outputs the i-th string that belongs to High.

3.4 Proof of Theorem 3.4

In this section, we prove Theorem 3.4. For proving this, we show Lemma 3.7, which is the contraposition of Theorem 3.4.

Lemma 3.7 (Restatement of Theorem 3.4). *Assume that OWPuzzs do not exist. Let $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbb{N}}$ be an arbitrary QPT samplable distribution family, and let $c > 1$ and $q > 0$ be two arbitrary constants. Then, there exists a QPT algorithm* Estimate *such that for infinitely many $n \in \mathbb{N}$,*

$$\Pr_{y\leftarrow\mathcal{D}_n}\left[\frac{1}{c}\Pr[y \leftarrow \mathcal{D}_n] \le \mathsf{Estimate}(y) \le c\Pr[y \leftarrow \mathcal{D}_n]\right] \ge 1 - \frac{1}{n^q}. \tag{26}$$

Proof of Lemma 3.7. Let $\mathcal{D} = \{\mathcal{D}_n\}_{n\in\mathbb{N}}$ be an arbitrary QPT samplable distribution family, and let $q > 0$ be an arbitrary constant. Let $\mathcal{Q}$ be a QPT algorithm such that $\mathcal{Q}(1^n)$ exactly samples from $\mathcal{D}_n$. (In the following, we often omit 1^n of $\mathcal{Q}(1^n)$.) Assume that OWPuzzs do not exist. Then, from Lemma 2.3, there exists a QPT algorithm Invert such that

$$\mathsf{SD}\left((y_1,...,y_i)_{(y_1,...,y_i)\leftarrow\mathcal{Q}}, (y_1...,y_{i-1},\mathsf{Invert}(i,y_1,...,y_{i-1}))_{(y_1,...,y_{i-1})\leftarrow\mathcal{Q}}\right) \le \frac{1}{n^{-50q}} \tag{27}$$

for all $i \in [n]$ and infinitely many $n \in \mathbb{N}$.

We construct Estimate by using the Invert as follows.

Construction of Estimate**:**

1. Receive $(y_1, ..., y_n)$ as input.
2. For each $i \in [n]$, run as follows:
   - Run $b \leftarrow \mathsf{Invert}(i, y_1 \cdots y_{i-1})$ for $n^{100}n^{100q}$ times. Let $\mathsf{Count}_{y_1\cdots y_{i-1}}(b)$ be the number of times that $\mathsf{Invert}(i, y_1 \cdots y_{i-1})$ outputs b.
   - Set
   $$\widetilde{p}[y_i] := \frac{\mathsf{Count}_{y_1\cdots y_{i-1}}(y_i)}{n^{100}n^{100q}}. \tag{28}$$
3. Output the value of $\prod_{i=1}^n \widetilde{p}[y_i]$.

In the following, we prove that

$$\frac{1}{c}\Pr[y \leftarrow \mathcal{Q}] \le \prod_{i=1}^{n}\widetilde{p}[y_i] \le c\cdot\Pr[y \leftarrow \mathcal{Q}] \tag{29}$$

with high probability over $y \leftarrow \mathcal{D}_n$.

For showing Lemma 3.7, we use the following Claims 3.8 to 3.10, which we prove later. Here, $\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}] = 1$ if $i = 1$.

Claim 3.8. For any real $a > 0$, we have

$$\Pr_{y\leftarrow\mathcal{Q}}\left[\frac{1}{2a} \le \frac{\Pr[(y_1,...,y_{i-1}y_i)\leftarrow\mathcal{Q}]}{\Pr[(y_1,...,y_{i-1})\leftarrow\mathcal{Q}]} \text{ for all } i\in[n]\right] \ge 1 - \frac{n}{a} \tag{30}$$

for all $n \in \mathbb{N}$.

Claim 3.9. For any real $b > 0$, we have

$$\Pr_{y\leftarrow\mathcal{Q}}\left[\left|\Pr[y_i \leftarrow \mathsf{Invert}(i,y_1,...,y_{i-1})] - \frac{\Pr[(y_1,...,y_{i-1}y_i)\leftarrow\mathcal{Q}]}{\Pr[(y_1,...,y_{i-1})\leftarrow\mathcal{Q}]}\right| \le bn^{-50q} \text{ for all } i\in[n]\right] \ge 1 - \frac{n}{b} \tag{31}$$

for infinitely many $n \in \mathbb{N}$.

Claim 3.10. For any real $d > 0$, we have

$$\Pr\left[|\widetilde{p}[y_i] - \Pr[y_i \leftarrow \mathsf{Invert}(i, y_1, ..., y_{i-1})]| \leq \frac{1}{d} \text{ for all } i \in [n]\right] \geq 1 - 2n \exp\left\{\frac{-2n^{100+100q}}{d^2}\right\} \tag{32}$$

for all $n \in \mathbb{N}$, where the probability is taken over $\mathsf{Estimate}(y)$ for computing $\widetilde{p}[y_i]$.

We use the claims above by setting $a = n^{q+2}$, $b = n^{q+4}$ and $d = n^{q+4}$. From Claims 3.9 and 3.10, with probability at least $1 - 2n^{-q-3}$, we have

$$\left|\widetilde{p}[y_i] - \frac{\Pr[(y_1, ..., y_{i-1}y_i) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]}\right| \leq 1/d + bn^{-50q} \leq 2n^{-q-4} \tag{33}$$

for all $i \in [n]$. This implies that

$$\widetilde{p}[y_i] \leq \frac{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]}\left(1 + 2n^{-q-4}\frac{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]}\right) \tag{34}$$

with probability at least $1 - 2n^{-q-3}$. Furthermore, from Claim 3.8, with probability at least $1 - n^{-q-1}$, we have

$$\frac{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}y_i) \leftarrow \mathcal{Q}]} \leq 2a = 2n^{q+2} \tag{35}$$

for all $i \in [n]$. Therefore, with probability at least $1 - 3n^{-q-1}$, we have

$$\widetilde{p}[y_i] \leq \frac{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]}\left(1 + \frac{4}{n^2}\right). \tag{36}$$

Therefore, with probability at least $1 - 3n^{-q-1}$, we have

$$\prod_{i\in[n]} \widetilde{p}[y_i] \leq \prod_{i\in[n]}\left(\frac{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]}\left(1 + \frac{4}{n^2}\right)\right) \tag{37}$$

$$= \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}]\left(1 + \frac{4}{n^2}\right)^n \tag{38}$$

for infinitely many $n \in \mathbb{N}$.[10] For any constant $c > 1$, there exists an $n_0 \in \mathbb{N}$ such that

$$\left(1 + \frac{4}{n^2}\right)^n \leq c \tag{39}$$

for all $n \geq n_0$. Therefore, we have

$$\prod_{i\in[n]} \widetilde{p}[y_i] \leq c \cdot \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}] \tag{40}$$

for infinitely many $n \in \mathbb{N}$.

In the same way, we can prove that, with probability at least $1 - 3n^{-q-1}$,

$$\frac{1}{c}\Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}] \leq \prod_{i\in[n]} \widetilde{p}[y_i] \tag{41}$$

for infinitely many $n \in \mathbb{N}$ as follows. From Claims 3.9 and 3.10, with probability at least $1 - 2n^{-q-3}$, we have

$$\frac{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]}\left(1 - 2n^{-q-4}\frac{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]}\right) \leq \widetilde{p}[y_i] \tag{42}$$

[10] Remember that Claim 3.9 satisfied only for infinitely many $n \in \mathbb{N}$.

for infinitely many $n \in \mathbb{N}$ and for all $i \in [n]$. Furthermore, from Claim 3.8, with probability at least $1 - n^{-q-1}$, we have

$$-2n^{q+2} = -2a \leq -\frac{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]}{\Pr[(y_1 \cdots y_{i-1} y_i) \leftarrow \mathcal{Q}]}. \tag{43}$$

Therefore, with probability at least $1 - 3n^{-q-1}$, we have

$$\frac{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]} \left(1 - \frac{4}{n^2}\right) \leq \widetilde{p}[y_i]. \tag{44}$$

Hence, with probability at least $1 - 3n^{-q-1}$, we have

$$\prod_{i \in [n]} \widetilde{p}[y_i] \geq \prod_{i \in [n]} \left(\frac{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]} \left(1 - \frac{4}{n^2}\right)\right) \tag{45}$$

$$= \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}] \left(1 - \frac{4}{n^2}\right)^n \tag{46}$$

for infinitely many $n \in \mathbb{N}$. For any constant $c > 1$, there exists an $n_1 \in \mathbb{N}$ such that

$$\frac{1}{c} \leq \left(1 - \frac{4}{n^2}\right)^n \tag{47}$$

for all $n \geq n_1$. Therefore, we have, with probability at least $1 - 3n^{-q-1}$

$$\frac{1}{c} \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}] \leq \prod_{i \in [n]} \widetilde{p}[y_i] \tag{48}$$

for infinitely many $n \in \mathbb{N}$. By combining Equation (40) and Equation (48), we have that

$$\frac{1}{c} \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}] \leq \prod_{i \in [n]} \widetilde{p}[y_i] \leq c \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}] \tag{49}$$

with probability at least $1 - 6n^{-q-1}$ (which is larger than $1 - \frac{1}{n^q}$ for sufficiently large $n \in \mathbb{N}$) for infinitely many $n \in \mathbb{N}$, which shows the lemma.

Proof of Claim 3.8. This is shown by a standard probabilistic argument. Let

$$\mathsf{Good} := \left\{ y \in \{0,1\}^n : \frac{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]} \geq \frac{1}{2a} \text{ for all } i \in [n] \right\}, \tag{50}$$

and let

$$\mathsf{Bad_i} := \left\{ y \in \{0,1\}^n : \frac{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]} < \frac{1}{2a} \right\}. \tag{51}$$

Because

$$\sum_{y \in \mathsf{Good}} \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}] \geq 1 - \sum_{i \in [n]} \sum_{y \in \mathsf{Bad}_i} \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}], \tag{52}$$

it is sufficient to show

$$\sum_{y \in \mathsf{Bad}_i} \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}] < 1/a \tag{53}$$

for all $i \in [n]$. We have

$$\sum_{y \in \mathsf{Bad}_i} \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}] = \sum_{y \in \mathsf{Bad}_i} \left(\prod_{j \in [n]} \frac{\Pr[(y_1, ..., y_j) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{j-1}) \leftarrow \mathcal{Q}]} \right) \tag{54}$$

$$= \sum_{y \in \mathsf{Bad}_i} \left(\prod_{j \in [n] \setminus i} \frac{\Pr[(y_1, ..., y_j) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{j-1}) \leftarrow \mathcal{Q}]} \right) \cdot \frac{\Pr[(y_1, ..., y_{i-1} y_i) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]} \tag{55}$$

$$< \sum_{y \in \mathsf{Bad}_i} \left(\prod_{j \in [n] \setminus i} \frac{\Pr[(y_1 \cdots y_j) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{j-1}) \leftarrow \mathcal{Q}]} \right) \cdot \frac{1}{2a} \tag{56}$$

$$< \sum_{y \in \{0,1\}^n} \left(\prod_{j \in [n] \setminus i} \frac{\Pr[(y_1, ..., y_j) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{j-1}) \leftarrow \mathcal{Q}]} \right) \cdot \frac{1}{2a} \tag{57}$$

$$= \frac{1}{a}. \tag{58}$$

In the last equation, we have used that

$$\sum_{y_1, ..., y_n \in \{0,1\}^n} \left(\prod_{j \in [n] \setminus i} \frac{\Pr[(y_1, ..., y_j) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{j-1}) \leftarrow \mathcal{Q}]} \right) \tag{59}$$

$$= \sum_{y_1, ..., y_n \in \{0,1\}^n} \frac{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_i) \leftarrow \mathcal{Q}]} \Pr[(y_1, ..., y_n) \leftarrow \mathcal{Q}] \tag{60}$$

$$= \sum_{y_1, ..., y_n \in \{0,1\}^n} \Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}] \Pr[(y_{i+1}, ..., y_n) \leftarrow \mathcal{Q} | (y_1, ..., y_i) \leftarrow \mathcal{Q}] \tag{61}$$

$$= \sum_{y_1, ..., y_i \in \{0,1\}^i} \Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}] \tag{62}$$

$$= \sum_{y_i \in \{0,1\}} 1 \tag{63}$$

$$= 2. \tag{64}$$

□

Proof of Claim 3.9. From the definition of Invert, we have

$$\mathsf{SD}\left((y_1, ..., y_i)_{(y_1, ..., y_i) \leftarrow \mathcal{Q}}, (y_1, ..., y_{i-1}, \mathsf{Invert}(i, y_1, ..., y_{i-1}))_{(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}} \right) \leq \frac{1}{n^{-50q}} \tag{65}$$

for all $i \in [n]$. This implies that

$$\sum_{y_1, ..., y_{i-1} \in \{0,1\}^{i-1}} \left| \Pr[(y_1, ..., y_{i-1}, 1) \leftarrow \mathcal{Q}] - \Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}] \Pr[1 \leftarrow \mathsf{Invert}(i, y_1, ..., y_{i-1})] \right| \tag{66}$$

$$= \sum_{y_1, ..., y_{i-1} \in \{0,1\}^{i-1}} \Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}] \cdot \left| \frac{\Pr[(y_1, ..., y_{i-1}, 1) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]} - \Pr[1 \leftarrow \mathsf{Invert}(i, y_1, ..., y_{i-1})] \right| \tag{67}$$

$$= \mathbb{E}_{(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}} \left[\left| \frac{\Pr[(y_1, ..., y_{i-1}, 1) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]} - \Pr[1 \leftarrow \mathsf{Invert}(i, y_1, ..., y_{i-1})] \right| \right] \leq n^{-50q} \tag{68}$$

for all $i \in [n]$. From Markov inequality, for each $i \in [n]$, we have

$$\Pr_{(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}} \left[\left| \frac{\Pr[(y_1, ..., y_{i-1}, 1) \leftarrow \mathcal{Q}]}{\Pr[(y_1, ..., y_{i-1}) \leftarrow \mathcal{Q}]} - \Pr[1 \leftarrow \mathsf{Invert}(i, y_1, ..., y_{i-1})] \right| \geq b n^{-50q} \right] \leq \frac{1}{b}. \tag{69}$$

Therefore,

$$\left|\frac{\Pr[(y_1,..,y_{i-1},1)\leftarrow\mathcal{Q}]}{\Pr[(y_1,...,y_{i-1})\leftarrow\mathcal{Q}]}-\Pr[1\leftarrow\mathsf{Invert}(i,y_1,...,y_{i-1})]\right| \tag{70}$$

$$=\left|\frac{\Pr[y_1,...,y_{i-1},0\leftarrow\mathcal{Q}]}{\Pr[y_1,...,y_{i-1}\leftarrow\mathcal{Q}]}-\Pr[0\leftarrow\mathsf{Invert}(i,y_1,...,y_{i-1})]\right|<bn^{-50q} \tag{71}$$

is satisfied for all $i\in[n]$ with probability at least $1-\frac{n}{b}$. □

Proof of Claim 3.10. From the Hoeffding inequality, for each $i\in[n]$,

$$\Pr_{\widetilde{p}[y_i]\leftarrow\mathsf{Estimate}(y)}\left[|\widetilde{p}[y_i]-\Pr[y_i\leftarrow\mathsf{Invert}(i,y_1,...,y_{i-1})]|>\frac{1}{d}\right]\leq 2\exp\left(\frac{-2n^{100+100q}}{d^2}\right). \tag{72}$$

Union bound implies that

$$\Pr_{\{\widetilde{p}[y_i]\}_{i\in[n]}\leftarrow\mathsf{Estimate}(y)}[|\widetilde{p}[y_i]-\Pr[y_i\leftarrow\mathsf{Invert}(i,y_1,...,y_{i-1})]|>1/d \text{ for some } i\in[n]]\leq 2n\exp\left(\frac{-2n^{100+100q}}{d^2}\right). \tag{73}$$

□

□

Acknowledgements. TH is supported by JSPS research fellowship and by JSPS KAKENHI No. JP22J21864. 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.

References

[AGQY22] Prabhanjan Ananth, Aditya Gulati, Luowen Qian, and Henry Yuen. Pseudorandom (function-like) quantum state generators: New definitions and applications. In Eike Kiltz and Vinod Vaikuntanathan, editors, *TCC 2022, Part I*, volume 13747 of *LNCS*, pages 237–265. Springer, Cham, November 2022. (Cited on page 1.)

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 208–236. Springer, Cham, August 2022. (Cited on page 1.)

[BCKM21] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. One-way functions imply secure computation in a quantum world. In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 467–496, Virtual Event, August 2021. Springer, Cham. (Cited on page 1.)

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. In Yael Tauman Kalai, editor, *14th Innovations in Theoretical Computer Science Conference, ITCS 2023, January 10-13, 2023, MIT, Cambridge, Massachusetts, USA*, volume 251 of *LIPIcs*, pages 24:1–24:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023. (Cited on page 1.)

[CGG24] Kai-Min Chung, Eli Goldin, and Matthew Gray. On central primitives for quantum cryptography with classical communication. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part VII*, volume 14926 of *LNCS*, pages 215–248. Springer, Cham, August 2024. (Cited on page 2, 4.)

[GLSV21] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in MiniQCrypt. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 531–561. Springer, Cham, October 2021. (Cited on page 1.)

[HM24] Hsin-Yuan Huang and Fermi Ma. Talk at simons institute, 2024. (Cited on page 1.)

[IL89] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *30th FOCS*, pages 230–235. IEEE Computer Society Press, October / November 1989. (Cited on page 1.)

[IRS21] Rahul Ilango, Hanlin Ren, and Rahul Santhanam. Hardness on any samplable distribution suffices: New characterizations of one-way functions by meta-complexity. *Electron. Colloquium Comput. Complex.*, TR21-082, 2021. (Cited on page 1, 2, 5.)

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part III*, volume 10993 of *LNCS*, pages 126–152. Springer, Cham, August 2018. (Cited on page 1.)

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica. In Barna Saha and Rocco A. Servedio, editors, *55th ACM STOC*, pages 1589–1602. ACM Press, June 2023. (Cited on page 1.)

[Kre21] William Kretschmer. Quantum Pseudorandomness and Classical Complexity. In Min-Hsiu Hsieh, editor, *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*, volume 197 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:20, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. (Cited on page 1.)

[KT24a] Dakshita Khurana and Kabir Tomer. Commitments from quantum one-wayness. In Bojan Mohar, Igor Shinkar, and Ryan O'Donnell, editors, *56th ACM STOC*, pages 968–978. ACM Press, June 2024. (Cited on page 1, 3.)

[KT24b] Dakshita Khurana and Kabir Tomer. Founding quantum cryptography on quantum advantage, or, towards cryptography from #P-hardness. Cryptology ePrint Archive, Paper 2024/1490, 2024. (Cited on page 1, 2, 3.)

[LMW24] Alex Lombardi, Fermi Ma, and John Wright. A one-query lower bound for unitary synthesis and breaking quantum cryptography. In Bojan Mohar, Igor Shinkar, and Ryan O'Donnell, editors, *56th ACM STOC*, pages 979–990. ACM Press, June 2024. (Cited on page 1.)

[LP20] Yanyi Liu and Rafael Pass. On one-way functions and kolmogorov complexity. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1243–1254, 2020. (Cited on page 1.)

[LP22] Yanyi Liu and Rafael Pass. On one-way functions from NP-complete problems. In *Proceedings of the 37th Computational Complexity Conference*, CCC '22, Dagstuhl, DEU, 2022. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. (Cited on page 1.)

[LV19] Ming Li and Paul Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications*. Texts in Computer Science. Springer Cham, 4th edition, 2019. (Cited on page 1, 4.)

[MSY24] Tomoyuki Morimae, Yuki Shirakawa, and Takashi Yamakawa. Cryptographic characterization of quantum advantage. arXiv:2410.00499, 2024. (Cited on page 1, 3.)

[MY22] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *CRYPTO 2022, Part I*, volume 13507 of *LNCS*, pages 269–295. Springer, Cham, August 2022. (Cited on page 1.)

[MY24] Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. In Frédéric Magniez and Alex Bredariol Grilo, editors, *19th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2024, September 9-13, 2024, Okinawa, Japan*, volume 310 of *LIPIcs*, pages 4:1–4:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024. (Cited on page 1.)