Electronic Colloquium on Computational Complexity, Report No. 156 (2024)

A Meta-Complexity Characterization of Quantum Cryptography

Bruno P. Cavalar* University of Oxford

Eli Goldin† New York University

Matthew Gray‡ University of Oxford

Peter Hall§ New York University

Abstract

We prove the first meta-complexity characterization of a quantum cryptographic primitive. We show that one-way puzzles exist if and only if there is some quantum samplable distribution of binary strings over which it is hard to approximate Kolmogorov complexity. Therefore, we characterize one-way puzzles by the average-case hardness of a *uncomputable* problem. This brings to the quantum setting a recent line of work that characterizes classical cryptography with the average-case hardness of a meta-complexity problem, initiated by Liu and Pass. Moreover, since the average-case hardness of Kolmogorov complexity over *classically* polynomial-time samplable distributions characterizes one-way functions, this result poses one-way puzzles as a natural generalization of one-way functions to the quantum setting. Furthermore, our equivalence goes through probability estimation, giving us the additional equivalence that one-way puzzles exist if and only if there is a quantum samplable distribution over which probability estimation is hard. We also observe that the oracle worlds of defined by Kretschmer et. al. rule out any relativizing characterization of one-way puzzles by the hardness of a problem in NP or QMA, which means that it may not be possible with current techniques to characterize one-way puzzles with another meta-complexity problem.

Contents

1 Introduction **2**
1.1 A Characterization of One-way Puzzles . . . 4
1.2 Related Work . . . 5
1.3 Technical Overview . . . 6
1.4 Open Problems . . . 8

2 Definitions and Preliminaries **9**
2.1 Probability . . . 9
2.2 Cryptography and one-way Puzzles . . . 10
2.3 Kolmogorov Complexity . . . 11
2.4 Probability estimation . . . 11
2.5 Average-case complexity . . . 11

*Email: bruno.cavalar@cs.ox.ac.uk
†Email: eli.goldin@nyu.edu
‡Email: matthew.gray@magd.ox.ac.uk
§Email: pf2184@nyu.edu

ISSN 1433-8092

3 Probability Estimation from the Nonexistence of One-way Puzzles 12
3.1 Proofs of claims 14
3.1.1 Proof of Theorem 3.4 14
3.1.2 Proofs of Theorems 3.5 and 3.6 16

4 Computing GapK with Probability Estimation 18
4.1 Coding Theorem for Quantum Samplable Distributions 18
4.2 Low Complexity, High Probability Strings are Uncommon 19

5 Breaking One-Way Puzzles with a GapK oracle 20

1 Introduction

What is the minimal complexity-theoretic assumption required for *quantum* cryptography? This is a fundamental question which even in the classical case began to be understood only recently. *One-way functions (OWFs)* are a basic, minimal primitive in classical cryptography, being necessary for a wide variety of cryptographic tasks, as well as being equivalent to many others [HILL99, IL89, GGM84, Imp95]. It is easy to observe that if one-way functions exist then $\mathsf{P} \neq \mathsf{NP}$ (the most fundamental complexity-theoretic conjecture). Furthermore, there is a long tradition of building cryptographic primitives from the computational hardness of *specific* problems, e.g. factoring, Learning-with-Errors, etc. [RSA78, BFKL94]. However, these implications only go in a single direction.

The "holy grail" result of this form [Pas23] would be to show that one-way functions exist if and only if $\mathsf{P} \neq \mathsf{NP}$. Note that one-way functions are the "central" classic cryptographic primitive. As remarked above, one way functions are minimal — almost all classical modern cryptography implies the existence of OWFs, mostly through trivial reductions. Moreover, one way functions are useful — they can be used to build everything in the "crypto-complexity" class Minicrypt [Imp95] including commitments, pseudorandom generators, and secret key cryptography. Similarly, $\mathsf{P} \neq \mathsf{NP}$ is the central conjecture in complexity theory. If it is shown to be false, much of complexity theory becomes trivial. Thus, if the holy grail result is true, then it implies the more general claim that "classical cryptography is possible if and only if complexity theory is interesting."

For many years, researchers have tried and failed to achieve this holy grail [BT03, AGGM10] [BB15]. However, some progress has come in recent years from a surprising front: meta-complexity.

Meta-complexity characterizations of cryptography. Meta-complexity refers to computational problems which are themselves about computational complexity. The foremost example of a meta-complexity problem is the task of computing the Kolmogorov complexity $\mathsf{K}(x)$ of a string x, which is defined as the length of the shortest Turing machine outputting x. The theory of meta-complexity is known to have numerous applications [LV19], including some recent discoveries in learning algorithms, hardness magnification, pseudorandomness and worst-case to average-case reductions [CIKK16, Hir21, San20, CHO$^+$20].

In a recent breakthrough, Liu and Pass [LP20] have shown that OWFs exist if and only the if problem of computing K^t (i.e., the length of the shortest program that outputs x in $t(|x|)$ steps) is *weakly hard on average* over the uniform distribution for some polynomial t. Later works have shown similar characterizations of OWFs from the hardness of various other meta-complexity problems

[LP23, LP21, San20, IRS21, Hir23, HIL+23]. These results reveal both a deep connection between cryptography and meta-complexity, and OWFs role as a central node equating many different meta-complexity tasks and properties.

Of particular interest to this work is [IRS21], which shows that one-way functions exist if and only if there exists a *samplable distribution* on which Kolmogorov complexity is hard to approximate. This result has the advantage of applying not only to the uniform distribution but to any distribution that is samplable by a polynomial-time algorithm, a more natural setting from the perspective of the theory of average-case complexity [BT06].

The complications of the quantum setting. The above focus on OWFs as the minimal assumption for computational cryptography has been complicated by recent work in quantum cryptography. Starting with Ji, Liu, and Song's introduction of pseudorandom states (PRS) [JLS18], recent works [MY24, MY22a, AQY22] have defined a new suite of quantum cryptographic primitives, most of which appeared to be less powerful than OWFs. Kretschmer formalized this by introducing an oracle world in which PRSs (and the many primitives which they imply) exist, but $\mathsf{BQP} = \mathsf{QCMA}$ [Kre21] meaning that no post-quantum OWFs are possible[1].

Thus, in the quantum setting, the classical holy grail result is no longer relevant. It is possible that $\mathsf{P} = \mathsf{NP}$, but useful cryptography exists. This brings up the question

What is the minimal natural complexity assumption required for quantum cryptography?

To answer this question, it would be worthwhile to look at the minimal primitive for quantum cryptography. However, even this is not clear in the quantum setting. Though one-way functions play this role in classical cryptography, and indeed all the cryptographic primitives of Minicrypt are known to be equivalent to it [Imp95], the cryptographic primitives that follow from PRSs (the collection of which some have called *Microcrypt* [Mor23]) are not known to be equivalent to each other, nor is there an unequivocably minimal primitive underlying all others.

Currently the two weakest candidate primitives are quantum bit commitments (EFI) [BCQ22, Yan22] which seem to be minimal for settings with quantum communication, and one way puzzles (OWPuzz) which seem to be minimal in the quantum-computation classical-communication (QCCC) [KT24a, CGG24] setting. One-way puzzles can also be constructed from a number of important quantum output primitives, such as pseudorandom states and one-way state generators [KT24a, CGG+23]. Notably, the existence of OWPuzz implies that $\mathsf{BQP} \neq \mathsf{PP}$ [CGG+23]. On the other hand, there are barriers to showing that the existence of EFI implies any conjectures in complexity theory [LMW24].

In this work, we will characterize one-way puzzles with the average-case hardness of estimating Kolmogorov complexity. Our results will naturally generalize the characterizations of [IRS21], corroborating the centrality of one-way puzzles in quantum cryptography, and providing the first complexity-theoretic characterization of a quantum cryptographic primitive. Furthermore, we will argue that this is in some sense the only possible characterization of one-way puzzles based on the hardness of a meta-complexity problem.

[1] Post-quantum OWFs are OWFs secure against quantum adversaries. The paper [KQST23] similarly shows a classical oracle under which PRSs exist but $\mathsf{P} = \mathsf{NP}$.

1.1 A Characterization of One-way Puzzles

Our main result is an equivalence between the existence of one-way puzzles and the average-case hardness of estimating Kolmorogov complexity over quantum samplable distributions. An interesting aspect of this result is that, though Kolmogorov complexity is known to be *uncomputable* [LV19], it nevertheless characterizes cryptography in the average-case setting.

Let $\mathsf{GapK}[s,t]$ be the promise problem of distinguishing between binary strings of Kolmogorov complexity at most s and those of Kolmogorov complexity at least t. A problem is said to be *weakly average-case hard* on a distribution $\mathcal{D}$ if, for all sufficiently large n, every quantum polynomial-time algorithm gives the wrong answer with probability at least $n^{-O(1)}$.

We now recall the definition of one-way puzzles [KT24a]. A one-way puzzle is defined by a quantum sampler algorithm, which samples a puzzle and a corresponding key, as well as an inefficient verification algorithm. The puzzle and key for a OWPuzz must be classical strings. The puzzle should be easy to sample, but hard to solve. That is, the sampled key-and-puzzle pairs should pass verification, but given just the puzzle it should be hard to find a key which passes the test. We show that, just like with OWFs, one-way puzzles can be characterized by the average-case hardness of computing GapK.

Theorem 1.1. *The following are equivalent:*

1. *One way puzzles exist.*
2. *There exists a quantum samplable distribution $\mathcal{D}$ on which probability estimation (Theorem 2.7) is weakly hard on average.*
3. *For some $s = n^{\Omega(1)}$ and $\Delta = \omega(\log n)$, there exists a quantum samplable distribution $\mathcal{D}$ such that $\mathsf{GapK}[s, s+\Delta]$ is quantum weakly average-case hard on $\mathcal{D}$.*

Interestingly, the only difference between our hard problem and the hard problem of [IRS21] characterizing OWFs is that our hardness is over quantum samplable distributions, whereas theirs is over classically samplable distributions. Indeed, one of their main results state that replacing every reference to *quantum* by *probabilistic* in Items 2 and 3 of our Theorem 1.1 yields a characterization of OWFs. Consequently, our result gives an exact characterization of Microcrypt from meta-complexity: we live in Microcrypt if and only if 1) all classical distributions are easy to estimate Kolmogorov complexity on, and 2) there are quantum distributions over which estimating Kolmogorov complexity is hard.

On the central importance of one-way puzzles. One way puzzles were introduced by Khurana and Tomer [KT24a] as an intermediate primitive between Morimae and Yamakawa's one way state generator (OWSG) [MY22b] and EFI pairs, and were studied as an object of independent interest by Chung, Goldin, and Gray [CGG24]. They fall near the base of the current hierarchy of quantum cryptographic primitives (only EFI is believed to be a weaker primitive) and have several properties desirable for a cryptographic primitive including combiners, a universal construction, and hardness amplification.

Prior work shows that a large number of quantum primitives (pseudorandom states, one-way state generators, and all of QCCC cryptography) can be used to build one-way puzzles [KT24a, CGG24]. Furthermore, one-way puzzles can be used to build EFI pairs, as well as everything else equivalent to them, such as multi-party computation and quantum bit commitments [KT24a].

However, we do not yet know of any efficient cryptographic primitive that can be built using one-way puzzles that cannot also be built using EFI pairs[2]. In fact, there are barriers to using one-way puzzles to build a number of primitives other than EFI pairs [CGG24]. Thus, the place of one-way puzzles in quantum cryptography is not yet well-understood.

One way to view our result is as giving more evidence that one-way puzzles are valuable to study as an independent primitive. Indeed, since Theorem 1.1 is the natural quantum generalization of a characterization of one-way functions, our result can be interpreted as showing that one-way puzzles are the natural quantum generalization of one-way functions. Furthermore, given the central role that the hardness of meta-complexity plays in classical cryptography, one can read this result as saying that one-way puzzles embody some fundamental aspect of quantum cryptographic hardness.

Other meta-complexity characterizations are difficult. Recall that there exists an oracle relative to which OWPuzz exist but $\mathsf{BQP} = \mathsf{QMA}$. This means that any characterization of OWPuzz by a problem in QMA must by necessity be non-relativizing. However, most meta-complexity characterizations of OWFs are based on problems in NP *do* relativize.

In particular, other meta-complexity problems known to characterize OWFs can easily be seen to be in NP or QMA. Examples include the (classical or quantum) minimum circuit size problem as well as time-bounded Kolmogorov complexity [LP20, CCZZ22]. Thus, the paper of Kretschmer [Kre21] provides a concrete barrier to showing that variants of these problems characterize one-way puzzles. Concretely, any such characterization must avoid the relativizing techniques usually employed in meta-complexity, or use one of the handful of problems (such as K^{exp} or Kt) which do not have efficiently checkable witnesses.

An observation about the hardness of estimating Kolmogorov complexity with an NP oracle. Finally, since our results do relativize, and since there exists an oracle relative to which $\mathsf{P} = \mathsf{NP}$ but OWPuzz exist, our results also provide a barrier to showing that estimating Kolmogorov complexity on average (on non polynomial time samplable distributions) can be solved using an NP oracle. This is not surprising, since computing Kolmogorov complexity exactly is undecidable [LV19], but this is not an observation we are aware of existing elsewhere.

1.2 Related Work

Other Meta-Complexity Characterizations. Almost all the meta-complexity characterizations of cryptography have shown equivalences between OWFs and the hardness of a specific meta-complexity problem on some kind of distribution. Two results however fall outside this paradigm and are of particular interest.

First is the work of Hirahara et al [HIL+23] which showed that the existence of OWFs is equivalent to the failure of symmetry of information to hold on average for a probabilistic time-bounded notion of Kolmogorov complexity.

Second is the work of Ball, Liu, Mazor, and Pass [BLMP23], which first extended this program outside Minicrypt. In their work they characterize the existence of key-agreement (generally considered the domain of "Cryptomania") by showing that the existence of key-agreement (KA)

[2] Concurrent work shows that one-way puzzles can be used to build inefficiently-verifiable proofs of quantumness, an inefficient yet important primitive [MSY24]

protocols is equivalent to the worst case hardness of an interactive promise notion of Kolmogorov complexity.

Quantum Meta-Complexity. In the aftermath of Bernstein and Vazirani's robust definition of quantum Turing machines [BV97] and their popularization amongst complexity theorists by Fortnow [For00], four main definitions Kq [Vit00], QC [BvDL01], H [Gac01], and $\mathsf{K}^{\epsilon}_{net}$ [MB04] were proposed as extensions of Kolmogorov complexity that could measure the complexity of quantum states. Pseudorandom states can be seen to trivially imply the hardness of estimating any of those measures on the quantum samplable distribution consisting of either many copies of a Haar random state, or many copies of a PRS output. But, besides this trivial implication, there have been no results connecting them to quantum cryptography. When restricted to classical strings all four definitions are equivalent to classical Kolmogorov complexity. Consequently our result immediately gives corollary versions of our main theorem by replacing GapK with GapKq, GapQC, GapH, or $\mathsf{GapK}^{\epsilon}_{net}$, and specifying that the distribution $\mathcal{D}$ is over classical states.

Recently Chia, Chou, Zhang, and Zhang gave three extensions of the minimum circuit size problem (MCSP) to the quantum setting [CCZZ22]: MQCSP which measures the quantum circuit complexity of classical strings, UMCSP which measures the complexity of implementing a unitary, and SMCSP which measures the complexity of generating a quantum state. They show that several implications between cryptography and the hardness of MCSP generalize to the quantum setting. In particular they generalize the result of Allender and Das that $\mathsf{SZK} \subseteq \mathsf{BPP}^{\mathsf{MCSP}}$ to $\mathsf{SZK} \subseteq \mathsf{BPP}^{\mathsf{MQCSP}}$ [AD17], and the observation (which can be found in [IRS21]) that OWFs imply GapMCSP is hard to post-quantum OWFs imply GapMQCSP is hard. They show the interesting implication that quantum-secure $i\mathcal{O}$ plus $\mathsf{MQCSP} \in \mathsf{BQP}$ imply that $\mathsf{NP} \subseteq \mathsf{coRQP}$, and make the observation that the existence of PRS implies that computing SMCSP, just like estimating the quantum Kolmogorov measures above, is hard.

Concurrent work. A concurrent work by Khurana and Tomer independently proves that the existence of one-way puzzles is equivalent to the hardness of probability estimation on quantum samplable distributions [KT24b], i.e. the first part of our Theorem 1.1. The reason they needed this lemma was for a different purpose than ours. While we use this to show that one-way puzzles are characterized by hardness of a meta-complexity problem, they are interested in building one-way puzzles from sampling assumptions. In addition, they use this lemma to show that one-way puzzles are equivalent to state puzzles, one-way puzzles where the key is quantum.

Another concurrent work by Hiroka and Morimae independently shows one direction of our result, namely that the hardness of GapK implies the existence of one-way puzzles. Their proof also goes through probability estimation [HM24].

1.3 Technical Overview

We go over the main technical insights in proving the equivalence of (1) the existence of one way puzzles, (2) the hardness of probability estimation, and (3) the hardness of GapK estimagtion (as in Theorem 1.1). We first prove that $\neg(1) \Rightarrow \neg(2)$, i.e., the nonexistence of one way puzzles implies that probability estimation is easy on all quantum distributions. We then prove $\neg(2) \Rightarrow \neg(3)$, i.e., that probability estimation being easy implies that GapK is easy on all distributions. Finally, we prove that $\neg(3) \Rightarrow \neg(1)$, i.e., that GapK being easy on all distributions is sufficient for breaking OWPuzz. Concluding the loop and showing that the three statements in our theorem are equivalent.

Nonexistence of One-way Puzzles $\implies$ Probability Estimation. The task in this section is to estimate $p_y = \Pr[y \sim \mathcal{D}]$ using one-way puzzle inverters. In the works of Ilango, Ren, and Santhanam [IRS21] and Impagliazzo and Luby [IL89], the parallel step of estimating p_x using one-way function inverters is done by treating a classical distribution $\mathcal{D}$ as a function f mapping random inputs r to samples $y = f(r)$. They then use Valiant and Vazirani [VV85] style hashing tricks which intuitively work as follows.

Instead of only inverting f, they invert the function $f'(r, h) = f(r), h, h(r)$, where h is the description of a hash function. By extending the length of the hash's output and fixing the bits of $z = h(r)$ at random (i.e., sampling h, z and giving $f(r), h, z$ as input to our inverter), the space of valid preimages can be cut in half again and again until eventually only one valid preimage remains. At this point, the only preimage of $f'(r, h)$ will be r itself, so further increases to the length will with high probability leave no valid preimages. If we try each possible output length, then, we will be able to approximately identify this point with very high probability allowing us to estimate p_y.

This technique fails to naively transfer to the quantum setting because quantum distributions cannot be purified in the way that classically random ones can. That is, classically samplable distributions can have the randomness removed from the sampling process and isolated as an input to the sampler, but quantum distributions cannot have their "quantum randomness" removed in this way. However, two facts give us some hope.

First, the proof of the equivalence between one-way functions and the hardness of probability estimation laid out above uses the exact same techniques as is used to prove one-way functions are equivalent to distributional one-way functions, a similar primitive where now only distributional inversion is hard. Consequently breaking a distributional one-way function requires a stronger inverter which can not only find a single valid preimages but can sample from the distribution of preimages.

Second, the recent work of [CGG24] showed that we can get the quantum version of this result showing that one-way puzzles exists if and only if *distributional one-way puzzles* (whose security guarantee) do. Meaning that the non existence of OWPuzz gives us the powerful tool of distribution inverters. Using these, and hashing over the outputs instead of the now inaccessible random inputs we are able to complete our task as follows.

Given a quantum distribution $\mathcal{D}$, we define a distributional one-way puzzle treating y as a key and $h, h(y)$ as the puzzle. Using similar intuition as above we can think of each bit $h(y)_i$ as cutting the distribution of other valid outputs $x \neq y$ in half. When $t = 0$ every output is a valid inversion. When $t = 1$ then we would expect only a subset of outputs with overall probability of one half are likely to be considered valid. And when $t = -\log(\Pr_D[y])$ we'd expect only a 2^{-t} fraction be considered valid. This intuition holds as long as a noticeable fraction of outputs occur with probability 2^{-t}.

By analyzing the distribution over the probability mass of the valid outputs, we are able to show that distributionally inverting such puzzles allows you to reliably estimate the probability of an output up to a polynomial multiplicative factor. This is somewhat weaker than what can be obtained in the classical setting (i.e. a constant estimation factor). However this is sufficient to distinguish between elements with a probability gap of $\omega(\log(n))$ as needed in the next section.

Probability Estimation $\implies$ Computing GapK. The reduction is from GapK to probability estimation is simple: We assume that strings with probability above the midpoint in the gap (x s.t. $\Pr[x] > 2^{-m}$) have "low" Kolmogorov complexity, and that strings with probability below the midpoint $\Pr[x] < 2^{-m}$ have "high" Kolmogorov complexity. For this reduction to be valid, we need to prove that this procedure makes few mistakes in each direction.

First, we show that strings output from a quantum distribution with high probability but high Kolmogorov complexity do not exist. To do this, we prove a quantum generalization of the coding theorem which shows how to create a short description of any high probability string. This proof is based on the observation that a time unbounded machine (like those considered in Kolmogorov complexity) can simulate the running of a quantum machine. Next we show that we make few errors caused by strings with low probability and low Kolmogorov complexity. We argue that such strings must be sampled by the distribution with only negligible probability. This is because there are few strings with low Kolmogorov complexity, and by definition they individually have low probability of being sampled.

Computing GapK $\implies$ Nonexistence of One-way Puzzles. This section diverges the farthest from the classical equivalent [IRS21], as they use the fact that OWFs imply PRGs with arbitrary stretch [HILL99, VZ12]. The outputs of such PRGs have very low Kolmogorov complexity (and K^t complexity) and so can be distinguished straightforwardly from random in the PRG security game. Therefore GapK being easy implies that there are no PRGs and therefore no OWFs. However a quantum equivalent to [HILL99] is not known, and neither OWPuzz nor even OWSG are known to imply a quantum pseudo-random sampler.

Instead, we will use GapK to break what one could call a *non-uniform pseudorandom low-entropy distribution*, an intermediary construction used to build EFI pairs from OWPuzz in a recent work by Chung, Goldin, and Gray [CGG24]. They are created by taking the machinery for building PRGs from OWFs [HILL99, VZ12] and applying them to OWPuzzs resulting in something as close to a PRG as we can currently get from OWPuzzs. The resulting primitive takes some small ($\log n$ bit) piece of non-uniform advice (which corresponds to the total next-bit pseudoentropy of the OWPuzz's sampler) and then samples from a distribution which is indistinguishable from uniform while having less than $n - n^{\Omega(1)}$ bits of true entropy.

Unfortunately, this distribution is non-uniform and our argument only gives us GapK estimation on uniform distributions from the non-existence of one-way puzzles. However, because the advice strings needed are only $\log n$ bits long, a uniform distribution which samples an advice string uniformly at random will include a $1/\mathsf{poly}(n)$ fraction of the distribution that corresponds to the correct advice we want to do well on. We are guaranteed to be able to estimate GapK on this distribution and therefore on the sub-distribution of interest. If GapK is easy on that sub-distribution then we can invert the underlying OWPuzz.

1.4 Open Problems

We conclude with a few interesting open problems left by our work.

1. **Other Characterizations and Implications for OWPuzz.** The Kretschmer's black-box barrier for quantum cryptography [Kre21] rules out any (relativizing) characterization of one-way puzzles by a meta complexity property which can be computed by QMA or NP algorithms. Specifically, that barrier rules out a relativizing proof that one-way puzzles imply the hardness of MCSP, MQCSP, $\mathsf{K}^{\mathsf{poly}}$, or KT, as each of these problems have efficiently checkable witnesses. Can we nonetheless still show an implication in the other direction by building one-way puzzles from their average-case hardness over quantum distributions?

Moreover, it remains possible that OWPuzz can be characterized by the hardness of meta-complexity measures which allow for descriptions that take super-polynomial time to output the string in question such as Kt.

2. **Characterizing OWSGs.** One-way state generators (OWSGs) are a classical-input quantum-output generalization of one way functions. Can their existence be characterized by the hardness of some *quantum* meta-complexity notion? Such a characterization would have to overcome several barriers, such as likely needing to show an equivalence between OWSGs and distributional OWSGs (generalizing a result of Cao and Xue [CX22] which is limited to their symmetric setting).

3. **Meta-complexity and EFIs.** EFIs are pairs of computationally indistinguishable and statistically far mixed states which are equivalent to quantum bit commitments. This work implies that the average-case hardness of GapK on quantum distributions implies EFIs. However, it is unclear whether the existence of EFIs has any direct meta-complexity implications. In fact, there exist weak barriers to showing that the existence of EFIs has any complexity theory implications at all [LMW24]. Nevertheless, perhaps meta-complexity (or quantum meta-complexity) holds the key to bypassing this barrier.

4. **Strong average-case hardness of Kolmogorov complexity.** One of the strengths of the results of [IRS21] compared to previous ones is that their characterization of one-way functions not only holds with respect to the *weak* average-case hardness of computing GapK, but also with respect to *strong* average-case hardness. Moreover, their result is robust with regards to any choice of parameters $s = n^{\varepsilon}$ and $\Delta = n - s - \omega(\log n)$. Essential to that weak-to-strong derivation and robustness is the equivalence between pseudorandom generators and one-way functions [HILL99]. Unfortunately, because it is currently only known that one-way puzzles imply quantum samplable distributions with linear pseudoentropy, we are only able to prove an equivalence in the weak average-case setting. Can our results be extended to the strong average-case setting, and can there be more latitude in the choice of parameters?

2 Definitions and Preliminaries

Throughout this paper we assume Δ and s are polynomial time computable functions from $\mathbb{N} \to \mathbb{N}$. By $\mathsf{negl}(n)$ we denote a negligible function vanished by all polynomials: $\mathsf{negl}(n) = 1/n^{\omega(1)}$. We will write QPT as a shorthand for "quantum polynomial time".

2.1 Probability

Given two distributions X, Y, we denote their statistical distance as $\mathsf{SD}(X;Y)$ or $\mathsf{SD}(X,Y)$ which is equal to $\frac{1}{2}\sum_{z \in X \cup Y}(|\Pr[X \to z] - \Pr[Y \to z]|))$. We denote by $\mathcal{U}_n$ the uniform distribution over $\{0,1\}^n$. Given a distribution $\mathcal{D}$, we denote by $\{\mathcal{D} \to x\}$ the event that a sample of $\mathcal{D}$ is equal to x. We will also write $x \overset{\$}{\leftarrow} \mathcal{D}$ to denote that x is sampled from $\mathcal{D}$. We denote by $H(\mathcal{D})$ the entropy of a probability distribution $\mathcal{D}$, which is defined as $H(\mathcal{D}) := \mathbb{E}_{x \overset{\$}{\leftarrow} \mathcal{D}}[-\log(\Pr[\mathcal{D} \to x])]$.

2.2 Cryptography and one-way Puzzles

We say that a distribution $\mathcal{D}$ supported on $\{0,1\}^m$ is computationally indistinguishable from the uniform distribution if, for every $c \geq 1$ and every QPT algorithm $\mathcal{A}$, we have

$$|\mathcal{A}(\mathcal{D}) - \mathcal{A}(\mathcal{U}_m)| < n^{-c},$$

for every large enough n.

Definition 2.1 (OWPuzz). *An (α, β) one way puzzle (OWPuzz) is a pair of a sampling algorithm and a verification function $(\mathsf{Samp}, \mathsf{Ver})$ with the following syntax:*

1. $\mathsf{Samp}(1^\lambda) \to (k, s)$ *is a uniform QPT algorithm which outputs a pair of classical strings (k, s). We refer to s as the puzzle and k as the key. Without loss of generality, we can assume $k \in \{0,1\}^\lambda$.*

2. $\mathsf{Ver}(k, s) \to b$ *is some (possibly uncomputable) function which takes in a key and puzzle and outputs a bit $b \in \{0,1\}$.*

satisfying the following properties:

1. *Correctness: For all sufficiently large λ, outputs of the sampler pass verification with overwhelming probability*
$$\Pr_{\mathsf{Samp}(1^\lambda) \to (k,s)}[\mathsf{Ver}(k, s) \to 1] \geq 1 - \alpha$$

2. *Security: Given a puzzle s, it is computationally infeasible to find a key s which verifies. That is, for all non-uniform QPT algorithms $\mathcal{A}$, for all sufficiently large λ,*
$$\Pr_{\mathsf{Samp}(1^\lambda) \to (k,s)}[\mathsf{Ver}(\mathcal{A}(s), s) \to 1] \leq \beta$$

If for all c, $(\mathsf{Samp}, \mathsf{Ver})$ is a $(\lambda^{-c}, \lambda^{-c})$ one way puzzle, then we say that $(\mathsf{Samp}, \mathsf{Ver})$ is a strong OWPuzz and omit the constants. When unambigious, we will simply say that such a $(\mathsf{Samp}, \mathsf{Ver})$ is a OWPuzz.

Definition 2.2 (distOWPuzz). *Let Samp be a QPT algorithm such that $\mathsf{Samp}(1^\lambda) \to (k, s)$ is a pair of classical strings referred to as the key and the puzzle, respectively. We say that the sampling algorithm Samp is a γ-*secure distributional one-way puzzle *if, for every QPT algorithm $\mathcal{A}$, we have*

$$\mathsf{SD}((k, s)\ ;(\mathcal{A}(s), s)) > \gamma,$$

where (k, s) is sampled from $\mathsf{Samp}(1^\lambda)$.

Theorem 2.3 ([CGG24, Theorem 33]). *If there exists a n^{-c}-secure distributional one-way puzzle for some $c \geq 1$, then there exists a one-way puzzle.*

2.3 Kolmogorov Complexity

This section introduces Kolmogorov complexity and a computational problem about estimating its value. We refer the reader to [LV19] for properties about Kolmogorov complexity.

Definition 2.4. *Let U be a universal Turing machine. For strings $x \in \{0,1\}^*$, the Kolmogorov complexity $\mathsf{K}_U(x)$ of x is the length of the shortest program ρ such that $U(\rho)$ will halt and output x after a finite number of steps.*

Our results hold for every universal Turing Machine U, so we will omit U and simply write K_U as K.

Definition 2.5. *For two functions $s_1(n), s_2(n) : \mathbb{N} \to \mathbb{N}$ satisfying, $0 < s_1(n) < s_2(n) < n$, we denote by $\mathsf{GapK}[s_1, s_2]$ the promise problem where YES instances are strings with $\mathsf{K}(x) \leq s_1(n)$ and NO instances are strings with $\mathsf{K}(x) \geq s_2$.*

Lemma 2.6. *The number of strings $x \in \{0,1\}^n$ such that $\mathsf{K}(x) \leq t$ is at most $2^{t+1} - 1$.*

2.4 Probability estimation

We say that a quantum algorithm $\mathcal{D}$ is a *family of quantum samplable distributions* if $\mathcal{D}$ is a QPT algorithm such that $\mathcal{D}(1^n) \in \{0,1\}^n$. We will use the shorthand $\mathcal{D}_n := \mathcal{D}(1^n)$.

We now define the task of probability estimation formally.

Definition 2.7. *Let $\mathcal{D} = \{\mathcal{D}_n\}_{n \in \mathbb{N}}$ be a family of quantum samplable distribution. For $x \in \{0,1\}^n$, let p_x be the probability that x is sampled from $\mathcal{D}_n$. We say that an algorithm $\mathcal{A}$ performs* probability estimation on $\mathcal{D}$ infinitely often with error at most ε and precision δ *if, for infinitely many $n \in \mathbb{N}$, we have*

$$\Pr_{\substack{x \xleftarrow{\$} \mathcal{D}_n \\ \mathcal{A}}} [\delta \cdot p_x \leq \mathcal{A}(x) \leq p_x] \geq 1 - \varepsilon.$$

We say that probability estimation *on a distribution $\mathcal{D}$ is* weakly hard on average *if there exists a constant $q \geq 1$ such that no QPT algorithm can perform probability estimation on $\mathcal{D}$ infinitely often with error at most n^{-q} and precision at least $n^{-O(q)}$.*

2.5 Average-case complexity

A decision or promise problem is said to be *weakly average-case hard for quantum algorithms on a distribution* $\mathcal{D}$ if there exists a constant $q \geq 1$ such that every quantum polynomial-time algorithm gives the wrong answer with probability at least n^{-q} on inputs sampled from $\mathcal{D}$, for all sufficiently large n. The problem is simply said to be *weakly hard on average for quantum algorithms* if it's hard on some quantum samplable distribution.

An algorithm is said to *solve* a problem *with error at most ε on a distribution* $\mathcal{D}$ if it gives the right answer with probability at least $1 - \varepsilon$ on inputs sampled from $\mathcal{D}$. A problem is said to be *weakly easy on average* for quantum algorithms on a distribution $\mathcal{D}$ if, for every constant $q \geq 1$, there exists a QPT algorithm that solves it on $\mathcal{D}$ with error at most n^{-q} on infinitely many input lengths.

3 Probability Estimation from the Nonexistence of One-way Puzzles

In this section we prove that the non-existence of one-way puzzles implies algorithms for probability estimation on all quantum samplable distributions.

Theorem 3.1 (Item 2 $\implies$ Item 1)**.** *If one-way puzzles do not exist, then, for any family of quantum samplable distributions $\mathcal{D}$, probability estimation on the distribution $\mathcal{D}$ is not weakly hard on average.*

The result will follow from the following lemma.

Lemma 3.2. *Let $c > 0$. If there do not exist n^{-c}-secure distributional one-way puzzles, then, for any family of quantum samplable distributions $\mathcal{D}$, there is a QPT algorithm $\mathcal{A}$ which multiplicatively estimates $p_x \coloneqq \Pr[\mathcal{D}_n \to x]$ infinitely often. In other words, we have*

$$\Pr_{\substack{x \xleftarrow{\$} \mathcal{D}_n \\ \mathcal{A}}} [p_x \leq \mathcal{A}(x) \leq 4n^{2c} p_x] \geq 1 - n^{1-c/2}$$

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

Indeed, Theorem 2.3 states that, if one-way puzzles do not exist, then n^{-c}-secure distributional one-way puzzles do not exist for every $c > 0$. In particular, setting $c = 2(d+1)$ in Theorem 3.2, Theorem 3.1 follows. We now prove the lemma.

Proof of Theorem 3.2. Let

$$S = \left\{ x \in \{0,1\}^n : \Pr_{x' \xleftarrow{\$} \mathcal{D}} [p_{x'} \leq p_x] \leq n^{-c} \right\}.$$

We observe that we rarely sample elements from S, so we only need to succeed in the probability estimation of p_x for $x \notin S$.

Claim 3.3. *We have $\Pr_{x \xleftarrow{\$} \mathcal{D}}[x \in S] \leq n^{-c}$.*

Proof. Note that, if $x \in S$ and $p_{x'} \leq p_x$, then $x' \in S$. This implies that $x \in S$ iff $p_x \leq \theta$, where $\theta = \max\{p_x : x \in S\}$. Therefore, we have $\Pr[x \in S] = \Pr[p_x \leq \theta] \leq n^{-c}$. □

Let $\mathcal{H}_n^k$ be a family of 3-wise independent hash functions with input $\{0,1\}^n$ and output $\{0,1\}^k$. On input 1^n, define a distributional one-way puzzle candidate Samp as follows:

Algorithm 1 One-way puzzle candidate Samp

```
Input: Number $n \in \mathbb{N}$ in unary ($1^n$).
Sample $k \xleftarrow{\$} [2n]$.
Sample $h \xleftarrow{\$} \mathcal{H}_n^k$.
Sample $x \xleftarrow{\$} \mathcal{D}_n$.
Output $(k, h, h(x))$ as the puzzle and $x$ as the key.
```

Since n^{-c}-distributional one-way puzzles do not exist, there exists an algorithm $\mathcal{O}$ which distributionally inverts Samp infinitely often. In particular, for infinitely many n, the distributions

$$\begin{aligned} P_n &\coloneqq (k, h, h(x), x), \text{ and} \\ \widetilde{P}_n &\coloneqq (k, h, h(x), \mathcal{O}(k, h, h(x))) \end{aligned}$$

satisfy

$$\Delta(P_n, \widetilde{P}_n) \leq n^{-c}.$$

From now on, fix $n \in \mathbb{N}$ such that the distributional inverter $\mathcal{O}$ satisfies the above inequality. We now define the distribution $P_{k,x}$ as follows:

1. Sample $h : \{0,1\}^n \to \{0,1\}^k$ a random 3-wise independent hash function from $\mathcal{H}_n^k$.
2. Sample $x' \xleftarrow{\$} \mathcal{D}_n$ conditioned on $h(x') = h(x)$.
3. Output x'.

We first observe that, if k is large, then the probability that $P_{k,x}$ outputs x is large. Moreover, if k is small, the probability that $P_{k,x}$ outputs x is smaller.

Lemma 3.4. *Let m be such that $p_x \leq 2^{-m}$ and $x \notin S$.*
If $k \leq m - 2c \log n - 2$, then

$$\Pr[P_{k,x} \to x] \leq 17n^{-c}$$

If $k \geq m$, then

$$\Pr[P_{k,x} \to x] \geq \frac{9}{10}$$

We define another distribution $\widetilde{P}_{k,x}$ as follows:

1. Sample $h : \{0,1\}^n \to \{0,1\}^k$ a random 3-wise independent hash function from $\mathcal{H}_n^k$.
2. Output $\mathcal{O}(k, h, h(x))$.

We claim that this distribution approximates $P_{k,x}$ with large probability.

Lemma 3.5. *Let $d \leq \frac{c-1}{2}$. With probability at least $1 - n^{-d}$ over x, for all $k \in [2n]$,*

$$\Delta(P_{k,x}, \widetilde{P_{k,x}}) \leq n^{-d}.$$

Crucially, the claim shows that, with large probability over $x \xleftarrow{\$} \mathcal{D}$, the distributions $P_{k,x}$ and $\widetilde{P_{k,x}}$ have small statistical distance *for all* k. Moreover, note that $P_{k,x}$ is not samplable, while $\widetilde{P}_{k,x}$ is. Together with Theorem 3.4, this means we can approximate p_x by sampling $\widetilde{P}_{k,x}$ over many values of k and estimating its probability. We formalize this idea in the following algorithm to approximate p_x. Let $t = \mathsf{poly}(n)$ be a large enough polynomial.

Algorithm 2 Probability estimation algorithm $\mathcal{A}$

```
for $k \in [2n]$ do
    for $j \in [t]$ do
        Sample $h \xleftarrow{\$} \mathcal{H}_n^k$
        Let $x'_{k,j} \leftarrow \mathcal{O}(k, h, h(x))$
    end for
    Let $c(k) \leftarrow$ the number of $j$ such that $x'_{k,j} = x$
end for
Let $k^*$ be the smallest $k$ such that $c(k) \geq \frac{3}{8}t$. If none exists, set $k^* = 2n$.
Output $2^{-(k^*-1)}$.
```

We claim that the algorithm correctly estimates p_x when $x \notin S$ and x is such that $P_{k,x}$ and $\widetilde{P_{k,x}}$ are statistically close. Henceforth, let $d = \frac{c-1}{2}$.

Lemma 3.6. *Let x be such that $\Delta(P_{k,x}, \widetilde{P}_{k,x}) \leq n^{-d}$ for all k and such that $x \notin S$. We claim that*

$$\Pr[p_x \leq \mathcal{A}(x) \leq 4n^{2c}p_x] \geq 1 - n^{-c}$$

infinitely often.

We are now ready to conclude the proof. By Theorem 3.5, we have $\Pr_{x \xleftarrow{\$} \mathcal{D}_n}[\Delta(P_{k,x}, \widetilde{P}_{k,x}) \geq n^{-d}] \leq n^{-d}$. Putting this all together, we get by Theorem 3.6 and the Claim that

$$\Pr_{x \xleftarrow{\$} \mathcal{D}_n}[p_x \leq \mathcal{A}(x) \leq 2n^{2c}p_x] \geq 1 - 2n^{-c} - n^{-d} \geq 1 - 3n^{-d} \geq 1 - n^{1-c/2}.$$

□

3.1 Proofs of claims

3.1.1 Proof of Theorem 3.4

We first prove Theorem 3.4. We will need the following lemmas.

Lemma 3.7. *Let $m = \lceil -\log p_x \rceil$ and $\Pr_{\mathcal{D} \to x'}[p_{x'} \leq 2^{-m}] \geq n^{-c}$. Let $k \leq m - 2\log n^c$. Then*

$$\Pr_h[\Pr_{\mathcal{D}' \to x}[h(x') = h(x) \text{ and } x' \neq x] \leq 2^{-k-2}n^{-c}] \leq 16n^{-c}$$

where h is drawn from a 3-wise independent hash family $\{0,1\}^n \to \{0,1\}^k$.

Proof. Note that if $\frac{1}{2^m} > n^{-c}/2$, then $k < 0$ so this trivially holds.

Define $\varepsilon = \Pr_{\mathcal{D} \to x'}[p_{x'} \leq 2^{-m} \text{ and } x' \neq x] \geq n^{-c} - \frac{1}{2^m} \geq n^{-c}/2$. Define $\gamma = \Pr_{\mathcal{D} \to x'}[h(x') = h(x) \text{ and } x' \neq x \text{ and } p_{x'} \leq 2^{-m}]$, a random variable in h. Define $R_{x'} = p_{x'}\mathbb{1}[h(x') = h(x)]$. We have

$$\gamma = \sum_{x' \neq x : p_{x'} \leq 2^{-m}} R_{x'}.$$

Note that $\mathbb{E}[R_{x'}] = p_{x'} \cdot \Pr[h(x') = h(x)] \leq p_{x'} \cdot 2^{-k}$. Furthermore, $\mathbb{E}[R_{x'}^2] = p_{x'}^2 \cdot \Pr_h[h(x') = h(x)] = p_{x'}^2 \cdot 2^{-k}$. And so

$$\mathbb{E}[\gamma] = \sum_{x' \neq x : p_{x'} \leq 2^{-m}} p_{x'} \cdot \Pr_h[h(x') = h(x)] = 2^{-k} \cdot \Pr_{\mathcal{D} \to x'}[p_{x'} \leq 2^{-m}] = 2^{-k} \cdot \varepsilon.$$

By 3-wise independence of h, the $R_{x'}$'s are pairwise independent, so

$$\mathrm{Var}(\gamma) = \sum_{x' \neq x : p_{x'} \leq 2^{-m}} p_{x'}^2 \cdot 2^{-k} \leq \sum_{x' \neq x : p_{x'} \leq 2^{-m}} p_{x'} \cdot 2^{-(m+k)} = 2^{-(m+k)} \cdot \varepsilon.$$

Chebyshev inequality then says that

$$\begin{aligned} \Pr\left[\gamma \leq 2^{-k}\varepsilon - 2^{-k}\varepsilon/2\right] &\leq \frac{\mathrm{Var}(\gamma)}{(2^{-k}\varepsilon/2)^2} \\ &= \frac{4}{\varepsilon} 2^{-m+k}. \end{aligned}$$

And so plugging in $k = m - 2c \log n$ and $\varepsilon \geq n^{-c}$, we get

$$\Pr\left[\gamma \leq 2^{-k-2} n^{-c}\right] \leq 16 n^c \cdot 2^{-2c \log n} \leq 16 n^{-c}.$$

Since $\Pr_{\mathcal{D}' \to x}[h(x') = h(x) \text{ and } x' \neq x] \geq \gamma$, the lemma follows. □

Lemma 3.8. *Let $m = \lceil -\log p_x \rceil$. Then*

$$\Pr_h[\Pr_{\mathcal{D}' \to x}[h(x') = h(x) \textit{ and } x' \neq x] \geq t \cdot 2^{-k}] \leq t^{-1},$$

where h is drawn from a 3-wise independent hash family $\{0,1\}^n \to \{0,1\}^k$.

Proof. Let $\alpha = \Pr_{\mathcal{D}' \to x}[h(x') = h(x) \text{ and } x' \neq x]$. A simple calculation of expectation gives us

$$\begin{aligned} \mathbb{E}_h[\alpha] &= \sum_{x' \neq x} p_{x'} \cdot 2^{-k} \\ &\leq 2^{-k}, \end{aligned}$$

and so Markov bound says

$$\Pr[\alpha \geq t \cdot 2^{-k}] \leq t^{-1},$$

and we are done. □

We are now ready to prove Theorem 3.4.

Proof of Theorem 3.4. Define $\alpha = \Pr_{\mathcal{D}' \to x}[h(x') = h(x) \text{ and } x' \neq x]$ a random variable in h.

Let us first consider $k \leq m - 2c \log n - 2$. Theorem 3.7 gives us

$$\Pr[\alpha \leq n^{-c} \cdot 2^{-k-2}] \leq 16 n^{-c}.$$

Let us define $P_{k,h,x}$ to be $P_{k,x}$ conditioned on the hash function being h. Note that if $\alpha \geq n^{-c} \cdot 2^{-k-2}$, then

$$\begin{aligned}
\Pr[P_{k,h,x} \to x] &= \frac{p_x}{\alpha + p_x} \\
&\leq \frac{p_x}{n^{-c} \cdot 2^{-k-2} + p_x} \\
&\leq \frac{p_x}{n^{c} \cdot 2^{-m} + p_x} \\
&\leq \frac{p_x}{n^{c} \cdot p_x + p_x} \leq \frac{1}{n^c + 1} \\
&\leq n^{-c}.
\end{aligned}$$

And so we get that

$$\Pr[P_{k,x} \to x] \leq \Pr[\alpha \leq n^{-c} \cdot 2^{-k-2}] + n^{-c} = 17 n^{-c}.$$

We now consider the case where $k \geq m + 11$. By Theorem 3.8

$$\Pr_h[\alpha \geq t \cdot 2^{-k}] \leq t^{-1}.$$

Furthermore, if $\alpha \leq t \cdot 2^{-k}$, then

$$\begin{aligned}
\Pr[P_{k,h,x} \to x] &= \frac{p_x}{\alpha + p_x} \\
&\geq \frac{p_x}{t \cdot 2^{-k} + p_x} \\
&\geq \frac{p_x}{t \cdot 2^{-10} p_x + p_x} \\
&\geq \frac{1}{t \cdot 2^{-10} + 1} \geq \frac{1}{t/1000 + 1}.
\end{aligned}$$

Picking $t = 100$, we get

$$\begin{aligned}
\Pr\left[P_{k,x} \to x] \geq \Pr[P_{k,h,x} \to x | \Pr_{\mathcal{D}' \to x}[\alpha \leq t \cdot 2^{-k}]\right] \Pr_{\mathcal{D}' \to x}[\alpha \leq t \cdot 2^{-k}] \\
\geq \frac{99}{100} \frac{1}{1/10 + 1} \geq \frac{99}{100} \frac{10}{11} = \frac{9}{10}.
\end{aligned}$$

□

3.1.2 Proofs of Theorems 3.5 and 3.6

Proof of Theorem 3.5. To ease notation, let $P = P_{k,x}$ and $\widetilde{P} = \widetilde{P_{k,x}}$. First, we will observe an equivalent sampling procedure for P.

1. Sample $k \xleftarrow{\$} [2n]$.

2. Sample $h \xleftarrow{\$} \mathcal{H}_n^k$.

3. Sample $x \overset{\$}{\leftarrow} \mathcal{D}_n$.
4. Sample $x' \overset{\$}{\leftarrow} \mathcal{D}_n$ conditioned on $h(x') = h(x)$.
5. Output $(k, h, h(x), x')$.

We obtain

$$\begin{aligned}
\Delta(P, \widetilde{P}) &= \frac{1}{2} \sum_{k,h,y,x'} \left| \Pr[P \to (k,h,y,x')] - \Pr[\widetilde{P} \to (k,h,y,x')] \right| \\
&= \frac{1}{n} \sum_{k} \left(\frac{1}{2} \sum_{h,y,x'} \left| \begin{array}{l} \frac{1}{2^{|h|}} \Pr_{x \overset{\$}{\leftarrow} \mathcal{D}}[h(x) = y] \Pr_{x \overset{\$}{\leftarrow} \mathcal{D}}[x = x' | h(x) = y] \\ -\frac{1}{2^{|h|}} \Pr_{x \overset{\$}{\leftarrow} \mathcal{D}}[h(x) = y] \Pr[\mathcal{O}(k,h,y) = x'] \end{array} \right| \right) \\
&= \mathbb{E}_{k} \left[\sum_{h,y} \left(\Pr_{x \overset{\$}{\leftarrow} \mathcal{D}}[h(x) = y] \frac{1}{2} \sum_{x'} \left| \frac{1}{2^{|h|}} \Pr_{x \overset{\$}{\leftarrow} \mathcal{D}}[x = x' | h(x) = y] - \frac{1}{2^{|h|}} \Pr[\mathcal{O}(k,h,y) = x'] \right| \right) \right] \\
&= \mathbb{E}_{k} \left[\sum_{h} \mathbb{E}_{y \overset{\$}{\leftarrow} h(\mathcal{D})} \left[\frac{1}{2} \sum_{x'} \left| \frac{1}{2^{|h|}} \Pr_{x \overset{\$}{\leftarrow} \mathcal{D}}[x = x' | h(x) = y] - \frac{1}{2^{|h|}} \Pr[\mathcal{O}(k,h,y) = x'] \right| \right] \right].
\end{aligned}$$

We briefly explain each of the equalities above. The first follows the definitions of P and $\widetilde{P}$, using also the fact that k is sampled uniformly in both distributions, and from the fact that h is also sampled uniformly from a pairwise independent hash family. The second equality simply used the linearity of expectation and the definition of expectation. The third equality again uses the definition of expectation. We now continue to manipulate the expression above as follows:

$$\begin{aligned}
\Delta(P, \widetilde{P}) &= \mathbb{E}_{k} \left[\sum_{h} \mathbb{E}_{x \overset{\$}{\leftarrow} \mathcal{D}} \left[\frac{1}{2} \sum_{x'} \left| \frac{1}{2^{|h|}} \Pr_{x'' \overset{\$}{\leftarrow} \mathcal{D}}[x'' = x' | h(x'') = h(x)] - \frac{1}{2^{|h|}} \Pr[\mathcal{O}(k,h,h(x)) = x'] \right| \right] \right] \\
&\geq \mathbb{E}_{k} \left[\mathbb{E}_{x \overset{\$}{\leftarrow} \mathcal{D}} \left[\frac{1}{2} \sum_{x'} \left| \sum_{h} \left(\frac{1}{2^{|h|}} \Pr_{x'' \overset{\$}{\leftarrow} \mathcal{D}}[x'' = x' | h(x'') = h(x)] - \frac{1}{2^{|h|}} \Pr[\mathcal{O}(k,h,h(x)) = x'] \right) \right| \right] \right] \\
&= \mathbb{E}_{k} \left[\mathbb{E}_{x \overset{\$}{\leftarrow} \mathcal{D}} \left[\frac{1}{2} \sum_{x'} \left| \Pr_{h, x'' \overset{\$}{\leftarrow} \mathcal{D}}[x'' = x' | h(x'') = h(x)] - \Pr_{h}[\mathcal{O}(k,h,h(x)) = x'] \right| \right] \right] \\
&= \mathbb{E}_{k, x \overset{\$}{\leftarrow} \mathcal{D}} \left[\Delta(P_{k,x}, \widetilde{P}_{k,x}) \right].
\end{aligned}$$

We again briefly explain each of the equalities above. The first equality simply rewrites the previous one. The second line (and only inequality) uses the triangle inequality. The third and fourth equations use the definition of expectation.

Since $\Delta(P, \widetilde{P}) \leq n^{-c}$, the inquality above implies $\mathbb{E}_{k,x}[\Delta(P_{k,x}, \widetilde{P}_{k,x})] \leq n^{-c}$. We can then show that, with probability $1 - n^{-d}$ over x, it holds that $\Delta(P_{k,x}, \widetilde{P}_{k,x}) \leq n^{-d}$ for all k. Indeed, suppose not: then with probability n^{-d} over x, there exists a k such that $\Delta(P_{k,x}, \widetilde{P}_{k,x}) > n^{-d}$. Thus, with probability $n^{-d} \cdot n^{-1}$ over x and k, we obtain $\Delta(P_{i,x}, \widetilde{P}_{i,x}) > n^{-d}$. But then $\mathbb{E}_{k,x}[\Delta(P_{i,x}, \widetilde{P}_{i,x})] > n^{-2d-1} \geq n^{-c}$, and we reach a contradiction. □

Proof of Theorem 3.6. Let $m = -\log p_x$. We first show that $\mathcal{A}(x) \geq p_x$ with probability at least $1 - n^{-c}/2$. Note that if the test (Line 8 of Algorithm 2 stating that $c(k) \geq \frac{3}{8}$) passes for some $k \leq \lceil m \rceil$, then $\mathcal{A}(x) \geq 2^{-k} \geq 2^{-(\lceil m \rceil - 1)} = 2^{\lfloor \log p_x \rfloor + 1} \geq 2^{\log p_x} = p_x$. Thus,

$$\Pr_{x \xleftarrow{\$} \mathcal{D}_n}[\mathcal{A}(x) \geq p_x] \geq \Pr_{x \xleftarrow{\$} \mathcal{D}_n}[\text{test passes for } k = \lceil m \rceil].$$

But we know that, for infinitely many n, the probability that $\mathcal{O}(k, h, h(x)) = x$ for $k = \lceil m \rceil$ is at least $\frac{9}{10} - n^{-d} \geq 0.98$ by Theorem 3.4 and the assumption, supposing n is sufficiently large. Thus, by the Chernoff bound, we have

$$\Pr_{x \xleftarrow{\$} \mathcal{D}_n}[\mathcal{A}(x) \geq p_x] \geq 1 - \exp\left(-O(t)\right) \geq 1 - n^{-c}/2,$$

for infinitely many n, since $t = \mathsf{poly}(n)$.

We now show that $\mathcal{A}(x) \leq 2n^{2c} p_x$ with probability at least $1 - n^{-c}/2$. Note that, as long as the test fails for all $k \leq m - 2c \log n - 2$, then $\mathcal{A}(x) \leq 4n^{2c} p_x$. Since $n^{-d} \leq \frac{1}{16}$ for large enough n, by the Chernoff bound, Claim 3.4 and the assumption, the probability that the test passes for any given $k \leq m - 2c \log n - 2$ is at most $\exp(-\Omega(t))$. Therefore, by the union bound, we have that

$$\Pr[\mathcal{A}(x) \geq 4n^{2c} p_x] \leq 2n \cdot \exp\left(-\Omega(n)\right) \leq n^{-c}/2,$$

for infinitely many n, using also the fact that $t = \mathsf{poly}(n)$ is a large enough polynomial. □

4 Computing GapK with Probability Estimation

In this section, we prove the following theorem.

Theorem 4.1 (Item 3 $\implies$ Item 2)**.** *Suppose that probability estimation is not weakly hard on average on a quantum samplable distribution $\mathcal{D}$. Then, for every $s : \mathbb{N} \to \mathbb{N}$ and $\Delta = \omega(\log n)$, the promise problem $\mathsf{GapK}[s, s + \Delta]$ is not weakly hard on average for quantum algorithms on $\mathcal{D}$.*

4.1 Coding Theorem for Quantum Samplable Distributions

First we need to show that probability estimation upper bounds Kolmogorov complexity. To do this we need to generalize the coding theorem to cover quantum samplable distributions. This can be done because Kolmogorov complexity is a time-unbounded notion and quantum algorithms can be simulated by a time-unbounded classical machine.

Theorem 4.2 (Coding Theorem for Quantum Samplable Distributions)**.** *For any quantum samplable distribution $\mathcal{D}$, and any $x \in \{0,1\}^n$, we have*

$$\mathsf{K}(x) \leq -\log(\Pr[\mathcal{D}_n \to x]) + |\mathcal{D}| + O(\log n).$$

Proof. As shown in [FR99, Lemma 3.2], there exists a (classical) algorithm that, given x, computes the probability p_x that $\mathcal{D}_n$ outputs x. Let ρ be the code of this algorithm. Observe that the length of ρ is $|\mathcal{D}_n| + O(1) = |\mathcal{D}| + O(\log n)$. If we sort the strings in $\{0,1\}^n$ in decreasing order of probability, the string x will appear in the first $\lceil 1/p_x \rceil$ elements of the list. Thus, we can specify the index of x in that list with $\log(1/p_x) + O(1)$ bits. Therefore, a universal Turing machine can recover x given $\log(1/p_x) + |\mathcal{D}| + O(\log n)$ bits. □

4.2 Low Complexity, High Probability Strings are Uncommon

Via the same argument given in [IRS21], we can show that, for any quantum samplable distribution, probability estimation on average implies Kolmogorov complexity estimation on average.

From the argument in the previous subsection, we know that high probability outputs have low Kolmogorov complexity, and assuming that low probability outputs have high Kolmogorov complexity can only hurt us in the very low probability instances. More formally, we show that, given oracle access to an algorithm that performs probability estimation on average on a distribution $\mathcal{D}$, we can solve GapK on average on that same distribution. Theorem 4.1 will follow from the lemma below.

Lemma 4.3. *Let $\mathcal{D}$ be a quantum samplable distribution and suppose $\Delta = \omega(\log n)$. Let $\mathcal{O}$ be an oracle, $c \geq 1$ be a constant and $\varepsilon : \mathbb{N} \to (0,1)$ be such that*

$$\Pr_{x \xleftarrow{\$} \mathcal{D}_n} [p_x / n^{-c} \leq \mathcal{O}(x) \leq p_x] \geq 1 - \varepsilon.$$

There exists a QPT algorithm which, given oracle access to $\mathcal{O}$, solves $\mathsf{GapK}[s - \Delta, s]$ on $\mathcal{D}$ with error at most $\varepsilon + 2^{-\Delta/3}$, for any choice of s.

Proof. Let $\alpha := 2^{-s+\Delta/2}$. The algorithm simply queries $\mathcal{O}$ and accepts if $\mathcal{O}(x) \geq \alpha$, and rejects when $\mathcal{O}(x) < \alpha$.

We first show that the error from mischaracterizing high Kolmogorov complexity outputs is zero. From Theorem 4.2 above, we get that, if $p_x \geq \alpha$, then

$$\mathsf{K}(x) \leq s - \Delta/2 + O(\log n) = s - \omega(\log n).$$

Therefore, for large enough n, no string x with Kolmogorov complexity at least s satisfies $p_x \geq \alpha$, and the algorithm never errs when the oracle doesn't.

Furthermore, we show that the error from mischaracterizing low Kolmogorov complexity outputs is small. Supposing the oracle is correct, we only make a mistake on inputs x such that $\mathsf{K}(x) \leq s - \Delta$ and $p_x \leq n^c \alpha$. There are at most $2^{s-\Delta+1}$ strings with Kolmogorov complexity less than $s - \Delta$. Their total probability is at most

$$2^{s-\Delta+1} \cdot n^c \alpha = 2n^c \cdot 2^{s-\Delta-s+\Delta/2} = 2n^c \cdot 2^{-\Delta/2} \leq 2^{-\Delta/3}$$

for sufficiently large n since $\Omega = \omega(\log n)$.

In conclusion, adding up the error of the oracle $\mathcal{O}$, the total error of the algorithm is $\varepsilon + 2^{-\Delta/3}$. □

Theorem 4.1 now follows from Theorem 4.3 since, if probability estimation is easy on average on $\mathcal{D}$, then there exists for every $q \geq 1$ a quantum algorithm that satisfies the assumption of the oracle of the lemma, with error at most n^{-q}. Furthermore, the error $2^{-\Delta/3}$ is negligible because $\Delta = \omega(\log n)$.

5 Breaking One-Way Puzzles with a GapK oracle

In this section we complete the characterization by showing that being able to estimate GapK on any quantum samplable distribution is sufficient for breaking OWPuzz. In [IRS21], this direction is very simple since one way functions are known to imply pseudo-random generators [HILL99], which can be broken by estimating any meta-complexity measure (such as GapK) which distinguishes between random and non-random strings. However, a quantum equivalent to [HILL99] is not known and neither OWPuzz nor even OWSG are known to imply a quantum pseudorandom "generator".

However, we observe that, implicit in the proof of Corollary 14 of [CGG24], is a statement in that direction which is enough for our purposes. They show that, if one-way puzzles exist, then there exists a non-uniform QPT sampling algorithm $\mathcal{D}$ such that, for some advice, the distribution $\mathcal{D}$ is indistinguishable from uniform, and exhibits an entropy gap. Since the entropy of the distribution is small, we can argue that its Kolmogorov complexity is small as well. Moreover, the sampler crucially uses only $O(\log n)$ bits of non-uniformity, which means that we can employ a GapK oracle that works on a uniformly quantum samplable distribution to distinguish the sampler $\mathcal{D}$ from the uniform distribution, thus breaking its security.

Theorem 5.1 ([CGG24, Proof of Corollary 14])**.** *If one way puzzles exist, there exists a polynomial-time quantum algorithm $\mathcal{D}$ with the following properties. The algorithm $\mathcal{D}$ takes in two inputs 1^n and ν, and outputs $m(n) > n$ bits. Moreover, for each sufficiently large n, there exists a binary string $\nu^*(n)$ such that*

1. *$\nu^*(n) \in \{0,1\}^{t(n)}$ and $t(n) = O(\log n)$;*
2. *$\mathcal{D}_n(\nu^*(n))$ is computationally indistinguishable from the uniform distribution on $m(n)$ bits;*
3. *$H(\mathcal{D}_n(\nu^*(n))) \leq m(n) - n$,*

where $\mathcal{D}_n(\nu) := \mathcal{D}(1^n, \nu)$.

Lemma 5.2. *For all c, m and n, we have*

$$\Pr[\mathsf{K}(\mathcal{U}_m) \leq m - c\log n] \leq n^{-c}.$$

Proof. There are $2^{m-c\log n}$ Turing machines of length $\leq m - c\log n$, and so there are at most $2^{m-c\log n}$ strings with $\mathsf{K}(x) \leq m - c\log n$. Therefore,

$$\Pr[\mathsf{K}(\mathcal{U}_m) \leq m - c\log n] \leq \frac{2^{m-c\log n}}{2^m} = n^{-c}.$$

□

Lemma 5.3. *Let $\mathcal{D}$ and $\nu^*(n)$ be as in Theorem 5.1. Then*

$$\Pr[\mathsf{K}(D_n(\nu^*(n))) \leq m(n) - n + O(\log n)] \geq \frac{1}{m}.$$

Proof. In this proof we will write $\mathcal{D}_n$ to denote $\mathcal{D}_n(\nu^*(n))$ for simplicity.

Let $p_x := \Pr[\mathcal{D}_n \to x]$. Observe that $H(\mathcal{D}_n) = \mathbb{E}_{x \xleftarrow{\$} \mathcal{D}_n}[-\log p_x]$. Since $H(\mathcal{D}_n) \leq m - n$, by Markov's bound we get

$$\Pr_{x \xleftarrow{\$} \mathcal{D}_n}[-\log p_x \geq m - n + 1] \leq \frac{m-n}{m-n+1} = 1 - \frac{1}{m-n+1}.$$

But note that $\mathcal{D}_n$ is samplable by a constant size Turing machine on input $n, \nu^*(n)$. Since $|n, \nu^*(n)| = O(\log n)$, by Theorem 4.2 and the previous inequality we obtain

$$\Pr_{x \xleftarrow{\$} \mathcal{D}_n}[\mathsf{K}(x) \leq m - n + O(\log n)] \geq \Pr_{x \xleftarrow{\$} \mathcal{D}_n}[-\log p_x \leq m - n + 1] \geq \frac{1}{m-n+1} \geq \frac{1}{m},$$

and the claim follows. □

Theorem 5.4 (Item 1 $\implies$ Item 3)**.** *If one-way puzzles exist, then there exists* $s = n^{\Omega(1)}$, $\Delta = \omega(\log n)$ *and a quantum samplable distribution* $\mathcal{S}$ *such that* $\mathsf{GapK}[s, s+\Delta]$ *is weakly average-case hard on* $\mathcal{S}$*.*

Proof. Assume one-way puzzles exist. Let $\mathcal{D}, m$ and ν^* be as given by Theorem 5.1. We define the following distribution $\mathcal{S}_n$:

1. Sample $b \xleftarrow{\$} \{0,1\}$
2. If $b = 0$, sample $s \xleftarrow{\$} \{0,1\}^{t(n)}$. Output $\mathcal{D}_n(s)$.
3. If $b = 1$, output $r \xleftarrow{\$} \mathcal{U}_m$.

Suppose for contradiction that, for all samplable distributions, for all $s = n^{\Omega(1)}$ and $\Delta = \omega(\log n)$, the problem $\mathsf{GapK}[s, s+\Delta]$ is not weakly average-case hard. Let c be such that $m, 2^{|\nu^*|} \leq n^c$. Note that, since $m = n^{O(1)}$, we have $n = m^{\Omega(1)} = \omega(\log m)$. Thus, we have $(m - 2c\log n) - (m - n/2) = \omega(\log m)$. Let $\mathcal{O}$ solve $\mathsf{GapK}[m - n/2, m - 2c\log n]$ with success probability $\geq 1 - \frac{1}{4n^{2c}}$ over $\mathcal{S}_n$.

We claim that $\mathcal{O}$ breaks the security of the sampler as in Theorem 5.1. Observe that $\mathcal{S}_n$ conditioned on $b = 0$ and $s = \nu^*$ is exactly $\mathcal{D}_n(\nu^*)$. Since this condition holds with probability $\geq \frac{1}{2n^c}$, we have that $\mathcal{O}$ correctly distinguishes Kolmogorov complexity over $\mathcal{D}_n(\nu^*)$ with success probability $\geq 1 - \frac{2n^c}{4n^{2c}} \geq 1 - \frac{1}{2n^c}$. Thus, by Theorem 5.3,

$$\Pr[\mathcal{O}(\mathcal{D}_n(\nu^*)) \to 1] \geq \frac{1}{n^c} - \frac{1}{2n^c} \geq \frac{1}{2n^c}.$$

Similarly, we know that $\mathcal{O}$ correctly distinguishes Kolmogorov complexity over $\mathcal{U}_m$ with success probability $\geq 1 - \frac{2}{4n^{2c}} \geq 1 - \frac{1}{2n^{2c}}$. By Theorem 5.2, we have

$$\Pr[\mathcal{O}(\mathcal{U}_m) \to 1] \leq \frac{1}{n^{2c}} + \frac{1}{2n^{2c}} = \frac{3}{2n^{2c}}.$$

This means that $\mathcal{D}_n(\nu^*)$ is not indistinguishable from uniform, which contradicts the security of the sampler $\mathcal{D}$.

□

Acknowledgements

We thank Yanyi Liu and Angelos Pelecanos for collaborating on an earlier stage of this project. We thank the Simons Institute for the Theory of Computing for hosting the Meta-Complexity program where this collaboration began. B. Cavalar acknowledges support of Royal Society University Research Fellowship URF\R1\211106. Eli Goldin is supported by a NSF Graduate Student Research Fellowship.

References

[AD17] Eric Allender and Bireswar Das. Zero knowledge and circuit minimization. *Information and Computation*, 256:2–8, 2017.

[AGGM10] Adi Akavia, Oded Goldreich, Shafi Goldwasser, and Dana Moshkovitz. Erratum for: on basing one-way functions on NP-hardness. pages 795–796, 2010.

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. Cryptography from pseudorandom quantum states. pages 208–236, 2022.

[BB15] Andrej Bogdanov and Christina Brzuska. On basing size-verifiable one-way functions on NP-hardness. pages 1–6, 2015.

[BCQ22] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography. *arXiv preprint arXiv:2209.04101*, 2022.

[BFKL94] Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. pages 278–291, 1994.

[BLMP23] Marshall Ball, Yanyi Liu, Noam Mazor, and Rafael Pass. Kolmogorov comes to cryptomania: On interactive kolmogorov complexity and key-agreement. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 458–483. IEEE, 2023.

[BT03] Andrej Bogdanov and Luca Trevisan. On worst-case to average-case reductions for NP problems. pages 308–317, 2003.

[BT06] Andrej Bogdanov and Luca Trevisan. Average-case complexity. *Found. Trends Theor. Comput. Sci.*, 2(1), 2006.

[BV97] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[BvDL01] André Berthiaume, Wim van Dam, and Sophie Laplante. Quantum kolmogorov complexity. *Journal of Computer and System Sciences*, 63(2):201–221, 2001.

[CCZZ22] Nai-Hui Chia, Chi-Ning Chou, Jiayu Zhang, and Ruizhe Zhang. Quantum meets the minimum circuit size problem. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 47:1–47:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[CGG$^+$23] Bruno Cavalar, Eli Goldin, Matthew Gray, Peter Hall, Yanyi Liu, and Angelos Pelecanos. On the computational hardness of quantum one-wayness. *ArXiv*, abs/2312.08363, 2023.

[CGG24] Kai-Min Chung, Eli Goldin, and Matthew Gray. On central primitives for quantum cryptography with classical communication. In *Annual International Cryptology Conference*, pages 215–248. Springer, 2024.

[CHO$^+$20] Lijie Chen, Shuichi Hirahara, Igor Carboni Oliveira, Ján Pich, Ninad Rajgopal, and Rahul Santhanam. Beyond natural proofs: Hardness magnification and locality. pages 70:1–70:48, 2020.

[CIKK16] Marco L. Carmosino, Russell Impagliazzo, Valentine Kabanets, and Antonina Kolokolova. Learning algorithms from natural proofs. In Ran Raz, editor, *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, volume 50 of *LIPIcs*, pages 10:1–10:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016.

[CX22] Shujiao Cao and Rui Xue. On constructing one-way quantum state generators, and more. *Cryptology ePrint Archive*, 2022.

[For00] Lance Fortnow. One complexity theorist's view of quantum computing. *Electronic Notes in Theoretical Computer Science*, 31:58–72, 2000.

[FR99] Lance Fortnow and John Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999.

[Gac01] Peter Gacs. Quantum algorithmic entropy. In *Proceedings 16th Annual IEEE Conference on Computational Complexity*, pages 274–283. IEEE, 2001.

[GGM84] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions (extended abstract). pages 464–479, 1984.

[HIL$^+$23] Shuichi Hirahara, Rahul Ilango, Zhenjian Lu, Mikito Nanashima, and Igor C Oliveira. A duality between one-way functions and average-case symmetry of information. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1039–1050, 2023.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. 28(4):1364–1396, 1999.

[Hir21] Shuichi Hirahara. Average-case hardness of NP from exponential worst-case hardness assumptions. pages 292–302, 2021.

[Hir23] Shuichi Hirahara. Capturing one-way functions via np-hardness of meta-complexity. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 1027–1038, 2023.

[HM24] Taiga Hiroka and Tomoyuki Morimae. Quantum cryptography from meta-complexity. Cryptology ePrint Archive, Paper 2024/1539, 2024.

[IL89] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography. In *30th Annual Symposium on Foundations of Computer Science*, pages 230–235. IEEE Computer Society, 1989.

[Imp95] Russell Impagliazzo. A personal view of average-case complexity. In *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*, pages 134–147. IEEE, 1995.

[IRS21] Rahul Ilango, Hanlin Ren, and Rahul Santhanam. Hardness on any samplable distribution suffices: New characterizations of one-way functions by meta-complexity. In *Electron. Colloquium Comput. Complex*, volume 28, page 82, 2021.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*, pages 126–152. Springer, 2018.

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum cryptography in algorithmica, 2023.

[Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

[KT24a] Dakshita Khurana and Kabir Tomer. Commitments from quantum one-wayness. pages 968–978, 2024.

[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.

[LMW24] Alex Lombardi, Fermi Ma, and John Wright. A one-query lower bound for unitary synthesis and breaking quantum cryptography. pages 979–990, 2024.

[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. IEEE, 2020.

[LP21] Yanyi Liu and Rafael Pass. Cryptography from sublinear-time average-case hardness of time-bounded kolmogorov complexity. In Samir Khuller and Virginia Vassilevska Williams, editors, *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 722–735. ACM, 2021.

[LP23] Yanyi Liu and Rafael Pass. One-way functions and the hardness of (probabilistic) time-bounded Kolmogorov complexity w.r.t. samplable distributions. pages 645–673, 2023.

[LV19] Ming Li and Paul M. B. Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications, 4th Edition*. Texts in Computer Science. Springer, 2019.

[MB04] Caterina E. Mora and Hans J. Briegel. Algorithmic complexity of quantum states. *International Journal of Quantum Information 4.04*, 2004.

[Mor23] Tomoyuki Morimae. Introduction to quantum cryptography without one-way functions. https://www.youtube.com/live/PKfYJlKD3z8?t=1048s, 2023.

[MSY24] Tomoyuki Morimae, Yuki Shirakawa, and Takashi Yamakawa. Cryptographic characterization of quantum advantage, 2024.

[MY22a] Tomoyuki Morimae and Takashi Yamakawa. One-wayness in quantum cryptography. Cryptology ePrint Archive, Report 2022/1336, 2022.

[MY22b] Tomoyuki Morimae and Takashi Yamakawa. Quantum commitments and signatures without one-way functions. In *Annual International Cryptology Conference*, pages 269–295. Springer, 2022.

[MY24] Tomoyuki Morimae and Takashi Yamakawa. Quantum advantage from one-way functions. pages 359–392, 2024.

[Pas23] Rafael Pass. Cryptography and Kolmogorov Complexity (Part I). https://www.youtube.com/live/sYtLGewgi7w?si=V4uDMiJFKzDBW7Zy&t=654, 2023.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[San20] Rahul Santhanam. Pseudorandomness and the minimum circuit size problem. *LIPIcs*, 151, 2020.

[Vit00] Paul Vitanyi. Three approaches to the quantitative definition of information in an individual pure quantum state. In *Proceedings 15th Annual IEEE Conference on Computational Complexity*, pages 263–270. IEEE, 2000.

[VV85] Leslie G Valiant and Vijay V Vazirani. Np is as easy as detecting unique solutions. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 458–463, 1985.

[VZ12] Salil P. Vadhan and Colin Jia Zheng. Characterizing pseudoentropy and simplifying pseudorandom generator constructions. In Howard J. Karloff and Toniann Pitassi, editors, *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 817–836. ACM, 2012.

[Yan22] Jun Yan. General properties of quantum bit commitments. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 628–657. Springer, 2022.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il