Electronic Colloquium on Computational Complexity, Report No. 221 (2025)

A Meta-Complexity Characterization of Minimal Quantum Cryptography

Bruno Cavalar[*], Boyang Chen[†], Andrea Coladangelo[‡], Matthew Gray[*], Zihan Hu[§], Zhengfeng Ji[†], Xingjian Li[†]

November 13, 2025

Abstract

We give a meta-complexity characterization of EFI pairs, which are considered the "minimal" primitive in quantum cryptography (and are equivalent to quantum commitments). More precisely, we show that the existence of EFI pairs is equivalent to the following: there exists a non-uniformly samplable distribution over pure states such that the problem of estimating a certain Kolmogorov-like complexity measure is hard given a *single copy*.

A key technical step in our proof, which may be of independent interest, is to show that the existence of EFI pairs is equivalent to the existence of *non-uniform* single-copy secure pseudorandom state generators (nu 1-PRS). As a corollary, we get an alternative, arguably simpler, construction of a universal EFI pair.

Contents

1 Introduction **2**
1.1 Our contributions . . . 5
1.2 Connections . . . 6
1.3 Open problems . . . 7

2 Technical overview **8**
2.1 Equivalence of EFI pairs and (non-uniform) 1PRS . . . 8
2.2 From a (non-uniform) 1PRS to a "universal" EFI pair. . . . 9
2.3 A meta-complexity characterization of EFI pairs . . . 10
2.4 A unifying viewpoint on various notions of Kolmogorov complexity of states . 11

3 Preliminaries **12**
3.1 Quantum information . . . 12
3.2 Quantum cryptographic primitives . . . 15
3.3 Quantum extractors . . . 16
3.4 Kolmogorov complexity . . . 19

[*] University of Oxford
[†] Tsinghua University
[‡] University of Washington
[§] EPFL

ISSN 1433-8092

4 Entropic EFI and pseudo-mixed states 23
4.1 Entropic EFI from EFI . . . 23
4.2 Non-uniform pseudo-mixed states from entropic EFI . . . 24

5 Single-copy pseudorandom states from pseudo-mixed states 26

6 A natural universal EFI 29

7 Equivalence with GapH hardness 29
7.1 Quantum algorithmic information . . . 30
7.2 Extraction . . . 32
7.3 Putting the pieces together . . . 32

8 Equivalence with GapU hardness 36

9 Equivalence with the hardness of identifying the "span of easy states" 38
9.1 Characterization of EFI from the hardness of identifying the "span of easy states" 38
9.2 Relating algorithmic entropy with the "*robust* span of easy states" . . . 39

10 Equivalence with hardness of state complexity over unkeyed state families 42

A Quantum Kolmogorov complexities - Invariance and Equivalence 50
A.1 $\mathsf{K}_{\mathsf{net}}$ Invariance . . . 51
A.2 $\underline{\mathsf{H}}$ Invariance . . . 51
A.3 Equivalence of $\underline{\mathsf{H}}$ notions . . . 52

1 Introduction

What is the minimum complexity assumption that implies cryptography? This question has proved extremely fruitful in the classical world and has sparked recent works in the new worlds of quantum complexity and cryptography [CGGH25, HM25, KT25]. In the classical world, the central cryptographic primitive of study is the one-way function (OWF). One-way functions (functions which are efficiently computable, but hard to invert) are natural, their existence is implied by the security of almost all cryptographic primitives and schemes[1], and their existence is equivalent to the existence of the wide variety of cryptographic primitives and schemes found in the crypto-complexity class "Minicrypt" [HILL99, ILL89, Imp95, Gol90]. Since an NP oracle can invert one-way functions, it is clear that $\mathsf{P} \neq \mathsf{NP}$ is implied by non trivial cryptography. But it is much less clear whether it in turn implies anything non-trivial. Proving this converse statement (that $\mathsf{P} \neq \mathsf{NP}$ implies one-way functions) remains the "holy grail" [LP23] of complexity-theoretic cryptography, and would result in the elimination of Heuristica and Pessiland, two of Impagliazzo's "five worlds" [Imp95].

There have been three main approaches to this question. The first has been to find concrete problems that are believed to be hard and to build one-way functions from them. These problems include factoring [RSA78], discrete logarithm [DH76], and learning with errors [Reg05]. This approach has enabled our current world of widespread practical cryptography, but is unlikely to ultimately answer our question. While the hardness of these problems does imply

[1] With the exceptions of indistinguishability obfuscation and information theoretic primitives like secret sharing.

the existence of one-way functions, their hardness is not thought to be implied by the existence of OWF, and they do not seem to capture anything fundamental about computation or complexity. Consequently they are very unlikely to prove to be minimal.

The second approach is due to Levin, who showed that there exists a specific universal OWF U that is one-way so long as any OWF exists at all [Lev87]. This does, to some extent, provide an answer to our question. The hardness of this (or any other) universal one-way functions is exactly equivalent to the existence of one-way functions and so "characterizes" their existence. However these universal one-way functions are quite unnatural, their hardness has not been of much independent interest, and they are only "weakly" one-way. Moreover they are difficult to study, and researchers have not been able to directly connect them to more fundamental complexity questions.

Both of these approaches then seem unlikely to satisfactorily answer our question, or bring us closer to a holy grail style result. However, over the last six years, there has been surprising progress coming from a new approach, meta-complexity.

Meta-complexity. Meta-complexity refers to the study of problems such as the Minimum Circuit Size Problem (MCSP) and Kolmogorov complexity estimation, which are themselves concerned with the complexity of other problems. Some of these problems (such as estimating time-unbounded Kolmogorov complexity) are undecidable in the worst case, but most (such as time-bounded Kolmogorov complexity and MCSP) are known to be in NP, but are not known to be NP-complete. These problems are widely applicable in areas including learning [HN23], hardness magnification [CHO+20], and sampling complexity [Aar10], and have been studied in their own right for decades [Tra84]. One of those applications, and one of the key motivations for their initial introduction, is that they can be used to measure the amount of randomness in specific objects. In particular this means that, in general, the meta-complexity of random and pseudo-random objects diverges significantly.

Using the hardness of meta-complexity for cryptography is relatively new, but has developed quickly since Santhanam's result showing that (under a conjecture) we can base the existence of pseudorandomness on the hardness of MCSP [San19]. Since then, a number of papers have shown that a wide variety of meta-complexity problems can be used to characterize one-way functions. These include the hardness of time-bounded Kolmogorov complexity on the universal distribution [LP20], the hardness of gap Kolmogorov complexity on any samplable distribution [IRS21], and "breakdown of symmetry of information" for probabilistic time-bounded Kolmogorov complexity [HIL+23].

Unlike the problems studied in the first approach, the hardness of these problems is equivalent to OWF. Unlike the universal functions studied in the second approach these problems are of significant independent interest, have closely related problems which have been shown to be NP-complete [Ila20], and seem more amenable to the kind of worst-case results that are required to achieve the holy grail [LP25]. Since these results also tell us that these problems are easy in a world without one-way functions, they have re-contextualized Pessiland from the worst of all worlds into a "wonderland for learning" [HN23].

However in one important sense none of these approaches have actually answered our question. Our question was "what is the minimal complexity assumption that implies cryptography?" The rational for studying OWF was that they have long been thought to be the minimal cryptographic assumption. However the recent explosion of work on quantum cryptographic primitives has weakened OWF position as minimal. This has raised the possibility of cryptography from weaker assumptions, including assumptions that do not even imply

$\mathsf{P} \neq \mathsf{NP}$.

Quantum Cryptography Following the introduction of pseudorandom states by Ji, Liu, and Song [JLS18] a wide variety of works have investigated a new world of quantum cryptographic primitives. To date more than thirty such primitives have been introduced and investigated. Their study is significantly motivated by the results of Kretschmer, which showed that there are oracles relative to which these primitives exist even when $\mathsf{BQP} = \mathsf{QMA}$ [Kre21] or $\mathsf{P} = \mathsf{NP}$ [KQST22] (a world in which one-way functions do not exist). This world of primitives has been named "Microcrypt" — a world of computational cryptography weaker than one-way functions.

As these primitives have been investigated, the picture that has emerged is very different from the relatively clean world of classical cryptography. The vast majority of classical cryptographic primitives are equivalent to OWF, and those that are not mostly fall into an orderly ladder-like hierarchy of strictly more powerful primitives. In contrast the current map of quantum primitives appears much more complicated (and much less is known).

In a recent work [GMMY24] Goldin et al. split these primitives into three sub-worlds defined by the classical oracle that can be used to break them. Their first world is "QuantuMania", and includes primitives such as quantum-computable post-quantum one-way functions, and efficiently verifiable one-way puzzles. The security of these primitives is defined in terms of a classical-input, classical-output problem in QCMA which is quantumly hard, meaning that these primitives can be broken by QCMA oracles.

Their second world is "CountCrypt" and includes primitives such as pseudo-random states, one-way state generators, and one-way puzzles. The security of these primitives is typically defined in terms a quantum-input, classical output which is hard given many copies of the quantum input. Since many copies of the input are available, these problems all reduce, via shadow tomography, to one-way puzzles, which can be broken with a PP oracle [CGG$^+$25]. Consequently, all CountCrypt primitives can be broken by PP oracles. Recent works [CGGH25, HM25] showed a meta-complexity characterization for one-way puzzles, and left open the question of whether meta-complexity characterizations could be extended to cryptographic primitives below one-way puzzles. Moreover, separation between primitives in CountCrypt have been recently shown [CCS25, AGL24, BCN25], which illustrates the depth of CountCrypt.

Our work focuses on their final world, "NanoCrypt" which contains primitives whose security is defined in terms of hardness of a single-copy quantum input, classical output problem. These primitives are not known to be breakable by any classical oracle, and there exists an oracle under which these primitives are secure against a single query to any classical oracle [LMW24]. Moreover, formal black-box separations exist between NanoCrypt and CountCrypt [BCN25], giving NanoCrypt the title of "minimal" world of quantum cryptography. Within NanoCrypt, EFI pairs, first proposed by Brakerski, Canetti, and Qian [BCQ22], are the primitive of interest if one wishes to characterize minimal quantum cryptography, and thus answer the opening question.

EFI pairs were first proposed by Brakerski, Canetti, and Qian [BCQ22]. An EFI pair consists of a pair of mixed state families which are efficient (E) to sample, are statistically far (F), and are computationally indistinguishable (I). They have been shown to be implied by all quantum cryptographic primitives, and to be equivalent to quantum bit commitments and quantum multiparty computation, while being simple and natural. In the handful of years since their introduction they have quickly become the consensus choice for the minimal quantum cryptographic primitive. Thus, in this work, we focus on the following question:

Can we find a meta-complexity problem whose hardness is equivalent to the existence of the minimal primitive in quantum cryptography, namely EFI *pairs?*

1.1 Our contributions

Meta-complexity characterizations are made up of a pair of implications. First, that the existence of a cryptographic primitive implies that some meta-complexity problem is hard; second, that the meta-complexity problem being hard implies the existence of that primitive. The first kind of implication is typically proven by taking advantage of meta-complexity as a measure of randomness. In a paradigmatic example of this, Ilango et al. [IRS21] achieve a meta-complexity characterization of OWF in terms of a Kolmogorov complexity estimation problem. The key is to show that a Kolmogorov complexity estimation algorithm can distinguish the outputs of a PRG from uniformly random strings [IRS21]. Since PRGs are equivalent to OWF by the well-known work of Håstad et al. [HILL99], breaking a PRG is sufficient to break OWFs. In the previous quantum characterizations of meta-complexity [CGGH25, HM25], the latter step is achieved by showing that a quantum Kolmogorov complexity estimation algorithm can distinguish between the outputs of a pseudo-entropy generator (which can be built from one-way puzzles), and the fully entropic distribution it should be indistinguishable from.

So if we are following this roadmap, our first step should be to build some kind of pseudo-entropy generator from EFI pairs (which we will refer to as EFI from here on, for short). Before our work, it was known that single-copy secure pseudorandom state generators (1PRS) imply EFI, and that they are a NanoCrypt primitive. But showing that EFI imply any kind of pseudo-entropy has been an open problem. We spend the first section of this paper showing our first main result: while EFI may not imply 1PRS, they do imply a (only slightly) non-uniform version.

Theorem 1.1. EFI *exist if and only if non-uniform* 1PRS *with advice size $O(\log \lambda)$ exist.*

Our first result immediately implies that, for any notion of "complexity" of states that distinguishes between "pseudorandom states" and Haar-random states, estimating this notion given a single copy of a state must be hard on non-uniform state families if EFIs exist. Between 2000 and 2004, four quantum generalizations of Kolmogorov complexity [Vit00, Gác01, MB04, BvDL00] were introduced, each of which extrapolated one of the equivalent ways of thinking about Kolmogorov complexity. All four notions are such that the Kolmogorov complexity is much higher for random states than for pseudorandom states. So, assuming EFI exist, all of these notions must be hard to estimate given just a single copy.

However, to prove a meta-complexity characterization, we need to prove the converse direction: if EFI do not exist, then we can efficiently estimate one of these complexity notions given just a single copy. None of the above notions turn out to have all of the necessary properties for a proof of this direction. However, Gács' notion (which he called "quantum algorithmic entropy", and of the four notions above most closely resembles a measure of entropy) has several of them, and we show that a smoothed version of his notion, which we will refer to as H-complexity in this introduction, turns out to have all of them. Overall, letting GapH denote the problem of estimating this notion of quantum Kolmogorov complexity (given some promise gap), we obtain the following meta-complexity characterization of EFI.

Theorem 1.2 (Informal)**.** EFI *exist if and only if there exists a non-uniform family of efficiently samplable states $\{|\psi_k\rangle\}$ such that* GapH *is hard on average.*

In conjunction, we provide a second characterization of EFI pairs in terms of the hardness of estimating a different, but related, notion of Kolmogorov complexity. We refer to the associated problem as GapU. The formal definitions of these notions and the corresponding estimation problems can be found in Sections 3.4.

From the characterizations above, we get several corollaries. First, because of the structure of our proof, one of the distributions that serves as half of our EFI pair is also a 1PRS. This means that if our initial hard-on-average GapH instance was uniformly sampled this results in a uniform 1PRS. Conversely, since 1PRS are, almost by definition, hard-on-average GapH instances, this gives us a meta-complexity characterization of 1PRS as well.

Corollary 1.1. 1PRS *exist if and only if there exists a uniform family of efficiently samplable states* $\{|\psi_k\rangle\}$ *such that, for some uniformly computable gap, the problem* GapH *is hard on average.*

Second, one direction of Theorem 1.2 does not rely on the fact that the state family $\{|\psi_k\rangle\}$ is efficiently samplable. In Section 10, we obtain characterizations of EFI from the hardness of GapH over single-copy samplable state families (i.e., state families for which one can only efficiently sample a single copy of a state).

Third, as a corollary of Theorem 1.1, we get a concrete construction of a "universal" EFI pair. That is, a concrete candidate that is an EFI pair if and only if an EFI pair exists at all. This construction is arguably simpler than the universal construction from [HKNY24], which requires the use of a "combiner".

As a final contribution, we provide a potentially unifying viewpoint on our meta-complexity characterizations of EFI pairs. A bit more precisely, let Π_r denote the span of states with $\mathsf{K}_{\mathsf{net}}$-complexity of size at most r (where informally, $\mathsf{K}_{\mathsf{net}}$-complexity is a notion introduced by Mora and Briegel [MB04] that captures the minimum-length of a program that can output the state). We refer to the latter as the "span of easy states". Then, we show the following characterization.

Theorem 1.3 (Informal)**.** EFI *exist if and only if there exists an efficiently computable* r *and a non-uniform family of efficiently samplable states* $\{|\psi_k\rangle\}$ *such that it is hard on average to decide whether a state from the family is in* Π_r*, or has small overlap with* $\Pi_{r+\omega(\log n)}$*, given a single copy.*

The notion of "span of easy states" is unifying in the following sense. There exists an appropriate "robust" version of the latter such that the H-complexity of a state is tightly related to its overlap onto this robust span. Roughly speaking, a state has low H-complexity if and only if it has a large overlap onto the "robust span of easy states". We refer the reader to Subsection 2.4 in the technical overview and Subsection 9.2 in the main text for more details.

1.2 Connections

OWPuzz ⇒ EFI. Combining this result with the meta-complexity characterizations of OWPuzz gives an alternate proof that OWPuzz imply EFI. All the notions of meta-complexity considered here reduce to (resource-unbounded) Kolmogorov complexity when restricted to classical strings. In [CGGH25, HM25] they show that OWPuzz exists if and only if there exists a distribution D samplable in quantum polynomial-time such that GapK is weakly hard. To show this they first show that that OWPuzz exists if and only if there exists a distribution D samplable in non-uniform quantum polynomial-time such that GapK is hard [CGGH25, Thm

5.1], then they combine over the choice of advice. By interpreting this non-uniform distribution as a mixed state, we obtain that all the notions discussed in this paper must also be non-uniformly hard on average over that mixed state, which in turn implies that EFI exists.

Unitary Synthesis and Quantum Complexity. A recent work shows that there exists an oracle relative to which there exists an EFI secure against a single query to any classical oracle [LMW24]. This has been interpreted (for instance by [CGGH25]) as a weak but general barrier to showing any complexity-theoretic consequences of the existence of EFI. This work in no way breaks the arguments of Lombardi et al. but it does show that the existence of EFI implies that these specific complexity theoretic problems must be hard on some distribution.

This further motivates the study of a complexity theory focused on inherently quantum tasks. This inherently or "properly" quantum complexity theory should help us better understand the relationships between tasks with either quantum inputs, outputs, or both.

1.3 Open problems

This work leaves open several problems.

1. **Uniform 1PRS.** We are able to show that EFI are equivalent to non-uniform single copy pseudo-random states. However, the amount of non-uniformity is quite small and corresponds to the amount of entropy of some efficiently preparable mixed state. So, in addition to being quite small, this advice is also (inefficiently) computable, contrasting with the more fundamentally non-uniform advice used for instance to show that unary halting is in P/poly. Proving that EFI implies 1PRS would significantly clean up NanoCrypt, resulting in a broad equivalence that more closely resembles Minicrypt. The most obvious route to showing this would be to create a robust combiner for single-copy PRS; however, this seems challenging, and it is unclear which other approaches might work.
2. **Other characterizations of EFI.** OWFs have been shown to be equivalent to the hardness of a wide variety of distinct meta-complexity problems. It seems very possible that EFI may have more equivalences than just those shown in this paper. Unlike OWPuzz, for which Kretschmer's oracle separations provide a barrier to showing an equivalence with time-bounded Kolmogorov complexity or MCSP, there does not seem to be any such barriers for EFI.
3. **Applications of the non-existence of EFI.** Using meta-complexity, Hirahara and Nanashima have shown that the non-existence of OWFs has powerful applications for learning [HN23]. Are there similar applications for the non-existence of EFI for quantum circuit learning, state synthesis, or other problems?
4. **A uniform characterization.** The non-uniformity which remains in our final theorem statement is somewhat unsatisfying and does not feel fundamental. Even if an equivalence with 1PRS stays out of reach, it is possible that we could prove that the existence of EFI is equivalent to some form of hardness of some meta-complexity notion on a uniformly samplable distribution.
5. **Characterizing one-way state generators.** One-way state generators still do not have a meta-complexity characterization. Previous work has mentioned this as an open problem [CGGH25]. Either giving a characterization or providing a formal barrier to doing so would be valuable. In [BJ24], it is shown that one-way state generators with inefficient verifiers are equivalent to EFI, so the meta-complexity characterization we build up in this paper is also a characterization of one-way state generators with inefficient verifiers. But one-way

state generators with efficient verifiers are plausibly stronger primitives [BCN25, BMM$^+$25], and it's unclear whether we have a meta-complexity characterization of efficiently-verifiable one-way state generators.

2 Technical overview

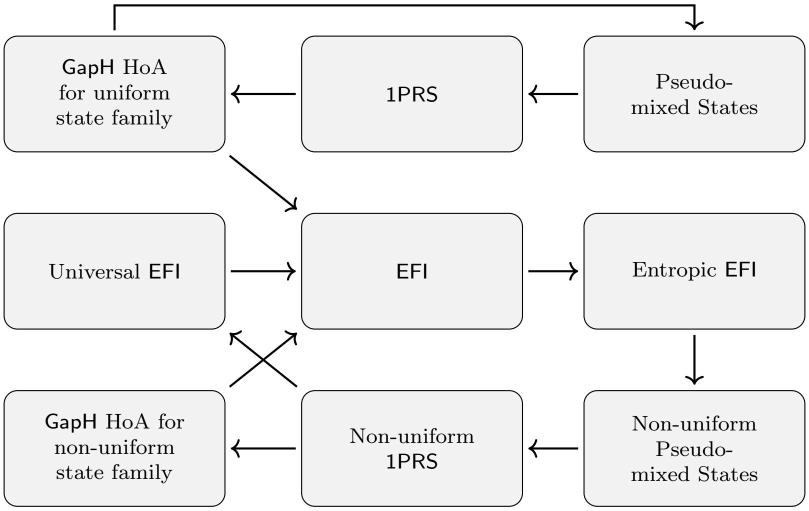
GapH HoA for uniform state family
1PRS
Pseudo-mixed States
Universal EFI
EFI
Entropic EFI
GapH HoA for non-uniform state family
Non-uniform 1PRS
Non-uniform Pseudo-mixed States

Figure 1: Outline of reductions. "HoA" stands for hard on average. The six problems at the bottom are all equivalent, as the reductions form cycles. The top three are also equivalent and imply the bottom six.

In this section, we give a high-level overview of how we prove our results. The starting point for our results is to establish a novel equivalence between EFI pairs and (non-uniform) single-copy pseudorandom states (1PRS). We then leverage this equivalence to obtain concrete characterizations of EFI pairs. Recall that a 1PRS is a family of efficiently generatable quantum states $\{|\psi_k\rangle\}$ that is "stretching" (i.e., the key size is smaller than the number of qubits), and computationally indistinguishable, but statistically far, from a uniformly (Haar) random state given a *single copy* of the state.[2]

2.1 Equivalence of EFI pairs and (non-uniform) 1PRS

One direction of this equivalence is easy. It is well-known that a 1PRS implies an EFI pair, where $\rho_0 = \mathbb{E}_k |\psi_k\rangle\langle\psi_k|$ (where here $\{|\psi_k\rangle\}$ is the family of pseudorandom states) and $\rho_1 = \frac{I}{2^n}$, where n is the number of qubits.

The converse is the crux. Consider an arbitrary EFI pair (ρ_0, ρ_1). At a high level, there are two obstacles to turning this into a 1PRS: the first is that ρ_1 may not equal $\frac{I}{2^n}$ for EFI pairs. The second is that instead of a mixed state ρ_0, we require a family of *pure* states $\{|\psi_k\rangle\}$ such that $\mathbb{E}_k |\psi_k\rangle\langle\psi_k|$ is computationally indistinguishable from $\frac{I}{2^n}$. So the question becomes: can an arbitrary EFI pair (where ρ_1 may not be maximally mixed) always be "massaged" into one where ρ_1 is maximally mixed?

[2] The expert reader will already know that the "multi-copy" variant of a PRS is qualitatively stronger than EFI pairs (formally, a black-box separation is known), so there is no hope of proving an equivalence.

Our approach takes inspiration from Goldreich's construction of a PRG from an EFID pair (the classical analogue of an EFI pair) [Gol90], but requires some uniquely quantum insights[3]. The high-level outline is the following:

- First, show that, starting from (ρ_0, ρ_1), one can construct a new EFI pair (σ_0, σ_1) where σ_0 and σ_1 have *noticeably different* von Neumann entropies. The key insight is that, if ρ_0 and ρ_1 are statistically far (and hence approximately orthogonal), then the states $\sigma_0 = \frac{1}{2}\left|0\right\rangle\left\langle 0\right| \otimes \rho_0 + \frac{1}{2}\left|1\right\rangle\left\langle 1\right| \otimes \rho_1$ and $\sigma_1 = \frac{I}{2} \otimes (\frac{1}{2}\rho_0 + \frac{1}{2}\rho_1)$ have von Neumann entropies that differ approximately by one bit! It is also not too difficult to show that σ_0 and σ_1 remain computationally indistinguishable. We refer to (σ_0, σ_1) as a "pseudo-entropy" pair, or more formally as an entropic EFI pair.
- Second, "upgrade" the pseudo-entropy pair to one where the second state is maximally mixed. This is possible via a combination of parallel repetition (to amplify the entropy gap), and the use of a "strong quantum randomness extractor", such as the one from [Dup10].
- Finally, given an EFI pair (σ_0, σ_1), where σ_0 has noticeably less than full entropy, and $\sigma_1 = \frac{I}{2^n}$, the idea to obtain a $\mathsf{1PRS}$ is the following. Since σ_0 is efficiently generatable, there exists an efficiently generatable purification $\left|\psi_0\right\rangle_{\mathsf{AB}}$ such that $\mathrm{tr}_{\mathsf{A}}[\left|\psi_0\right\rangle] = \sigma_0$. One should then choose an appropriate family of "twirling" unitaries U_k on A with the property that $\mathbb{E}_k (U_k \otimes I)\left|\psi_0\right\rangle\left\langle\psi_0\right|(U_k^\dagger \otimes I) \approx \frac{I}{|\mathsf{A}|} \otimes \sigma_0$. Why is this useful? This is because, by hypothesis, the latter state is computationally indistinguishable from $\frac{I}{|\mathsf{A}|} \otimes \frac{I}{|\mathsf{B}|}$. Thus, defining the $\mathsf{1PRS}$ to be $\left|\psi_k\right\rangle = U_k\left|\psi_0\right\rangle$ would yield the desired guarantee. Now, such a family of efficiently implementable twirling unitaries always exists, but, to obtain a $\mathsf{1PRS}$, we crucially need the length of the seed k to be smaller than the number of qubits of the output state. This is possible to achieve thanks to the fact that the von Neumann entropy of σ_0 (and hence the entanglement entropy of $\left|\psi_0\right\rangle$) is less than full (one can again leverage a strong quantum randomness extractor [Dup10]).

Note one important point here: in order to pick the appropriate family $\{U_k\}$ (i.e., the extractor), one needs to know the von Neumann entropy of σ_0. It is not yet clear how this can be circumvented, and this is why this approach only shows that an EFI pair implies a *non-uniform* $\mathsf{1PRS}$, where the advice is of logarithmic size (since the entropy is at most n).

2.2 From a (non-uniform) 1PRS to a "universal" EFI pair.

Leveraging the above equivalence, we can obtain a concrete construction of a "universal" EFI pair, reminiscent of Levin's universal OWF construction. This is a concrete EFI pair construction that is secure if and only if an EFI pair exists at all. We note that our construction will differ from the universal EFI construction of [HKNY24] in that we do not need combiners.

Informally, the outline is the following. Assume a non-uniform $\mathsf{1PRS}$ (with logarithmic-length advice) exists. Denote the seed length by λ, and the length of the output state by $n(\lambda)$. Then, if the advice is logarithmic size, for each 1PRS state $\left|\psi_k\right\rangle$, there exists a Turing machine with description length $r = \lambda + O(\log \lambda) + C$, where C is a universal constant, that there exists a Turing machine of size C, takes in 1^λ and k as input, in some polynomial time $T(\lambda)$, outputs a quantum circuit whose output (when run on the all zero state) is $\left|\psi_k\right\rangle$. Then, we argue that

[3] As pointed out also by Brakerski, Canetti, and Qian [BCQ22], Goldreich's proof relies crucially on the fact that for a BPP algorithm it is possible to separate the randomness from the rest of the computation. Such techniques cannot work for quantum algorithms, as observed also in the work of Aaronson, Ingram, and Kretschmer comparing BPP and BQP [AIK21].

the following concrete universal construction must be an EFI pair. Consider the pair of state families $\left(\{\rho_{r,T}\}, \{\frac{I}{2^n}\}\right)$, implicitly indexed by λ, where $\rho_{r,T} = \frac{1}{2^r}\sum_{|P|\leq r} |\psi_P^T\rangle\langle\psi_P^T|$, and $|\psi_P^T\rangle$ is the n-qubit state obtained by running Turing machine P for time T to get a quantum circuit Q with an n-qubit state output, and then running Q on the all-zero state. The key point is that the states $\rho_{r,T}$ and $\frac{1}{2^n}I$ are statistically far because the rank of $\rho_{r,T}$ is far from being full (since $n = r + \omega(\log\lambda)$). At the same time, any computational distinguisher has at least an inverse-polynomial failure probability due to the fact that an inverse-polynomial fraction of the programs P outputs a state from the 1PRS family. This kind of "weak" EFI pair can be upgraded to a standard EFI pair, based on known results.

2.3 A meta-complexity characterization of EFI pairs

While the construction above is a desirable step forward, as it gives a valid and concrete characterization of minimal quantum cryptography, it is still not as "natural" as one could hope for. Finding characterizations that are of independent interest, with natural connections to other well-studied problems in complexity theory is an important step towards relating (or decoupling) the existence of quantum cryptography to (or from) other complexity-theoretic statements. Here, we describe how we obtain a characterization of EFI pairs in terms of the hardness of a natural meta-complexity problem.

Recall that the Kolmogorov complexity of a string x captures the description length of the *shortest* program (to be run on some fixed universal Turing machine U) that outputs x. In the quantum setting, different variants of Kolmogorov complexity of *states* have been proposed (differing mainly in how they account for the program outputting an approximation of the state) [Gác01, MBK06]. Let $\underline{\mathsf{H}}$ denote a suitable such notion (which will describe in more detail below). Informally, here is the problem we propose to consider: let $\{|\psi_k\rangle\}$ be an efficiently sampleable family of states with the promise that each state either has $\underline{\mathsf{H}}$-complexity above some threshold $r(n)$ or below $r(n) - \omega(\log n)$; given a *single copy* of a state from the family, decide if it has low or high $\underline{\mathsf{H}}$-complexity. Due to the fact that the equivalence we can prove is between EFI and *non-uniform* 1PRS, our approach eventually leads to a version of the latter problem with respect to a *non-uniform* family of states. A bit informally, the notion of $\underline{\mathsf{H}}$-complexity that we are looking for should satisfy the following properties:

- It should be such that pseudorandom states have low complexity, while a uniformly random string has high complexity with overwhelming probability. If this is the case, then we can build on the previous equivalence: assuming an EFI pair exists, a (non-uniform) 1PRS also exists, and thus we can consider the following family of states. Sample a state from the 1PRS family with probability $\frac{1}{2}$, and sample a uniformly random standard basis state with probability $\frac{1}{2}$. Thus, assuming an EFI pair exists, this would be a (non-uniform) family of states for which the problem of estimating $\underline{\mathsf{H}}$-complexity is hard.
- It should be such that low complexity states have low von Neumann entropy while high complexity states have high von Neumann (or min-)entropy. This would allow us to argue the converse direction: if there exists a family $\{|\psi_k\rangle\}$ on which the problem of estimating $\underline{\mathsf{H}}$-complexity is hard, then an EFI pair exists. The EFI pair would be $(\rho, \frac{I}{2^n})$, where ρ is the state obtained by applying a suitable strong quantum randomness extractor [Dup10] to the state $\mathbb{E}_k |\psi_k\rangle\langle\psi_k|$. The point is that ρ is efficiently preparable, and, if the appropriate parameters are chosen for the extractor, it is far from the maximally mixed state since half of the states in $\{|\psi_k\rangle\}$ have low von Neumann entropy.

We show that a notion of $\underline{\mathsf{H}}$-complexity that satisfies the two properties above is a "smooth" version of (a variant of) Gács' complexity [Gác01] (defined precisely in Definition 3.12, and 3.13 for its smoothed version). We denote the smooth version by $\underline{\mathsf{H}}^{\varepsilon}$ for $\varepsilon \in [0,1]$. Ultimately, a bit more precisely, the promise problem that we arrive at is: let $\{|\psi_k\rangle\}$ be a non-uniform family of states with the promise that, for almost all states, either $\underline{\mathsf{H}}^{1-\varepsilon} < r(n) - \omega(\log n)$ or $\underline{\mathsf{H}}^{0} > r(n)$, given a *single copy* of a state from the family, decide which is the case. The hardness of this problem for some family of states is equivalent to the existence of EFI pairs. Just like for our 1PRS construction from an EFI pair, the length of the advice needed to efficiently sample the family of states is logarithmic.

We note that our proof of the equivalence above does not actually rely on the fact that $\{|\psi_k\rangle\}$ is a keyed family. In fact, it also works for any single-copy samplable state family, i.e., a family such that there exists a QPT algorithm that can sample *a single copy* of a state from the family. Thus as a result, we can also show an equivalence between the existence of EFI and hardness of $\underline{\mathsf{H}}$-complexity estimation over single-copy samplable state families.

2.4 A unifying viewpoint on various notions of Kolmogorov complexity of states

While so far we have primarily focused on $\underline{\mathsf{H}}$, we also consider other complexity notions (e.g., U) and their robust versions, and prove characterizations of EFI from the hardness of estimating these complexity notions. As a final contribution, we provide a potentially unifying viewpoint on several of these notions in terms of the following problem.

Let Π_r be the span of all the states with $\mathsf{K}_{\mathsf{net}}$-complexity at most r (where informally, $\mathsf{K}_{\mathsf{net}}$-complexity is a notion introduced by Mora and Briegel [MB04] that captures the minimum-length of a program that can output the state). Let $\{|\psi_k\rangle\}$ be an efficiently samplable family of states with the promise that each state either lies (almost) entirely in Π_r or it is (almost) orthogonal to $\Pi_{r+\omega(\log n)}$; given a single copy of the state, decide which is the case.

Note that deciding whether the state is in the "span of easy states" or not is the best that one can hope for given only a single copy. One cannot distinguish the easy states from the (potentially hard) states in the span of the easy states given a single copy since their density matrices might be statistically very close. In Theorem 9.1, we prove that the existence of EFI is equivalent to the existence of a non-uniform family of states on which the above problem is hard.

An important remark is that the "span of easy states" is a notion that is not robust against the choice of the universal gate set used to define $\mathsf{K}_{\mathsf{net}}$-complexity. Although, from Solovay-Kitaev, any two universal gate sets can approximate each other to arbitrary precision, the span of easy states can be very different even if we only perturb the easy states a little bit: for example, the span of $\{|0\rangle, \sqrt{1-2^{-200}}\,|0\rangle + 2^{-100}\,|1\rangle\}$ is exactly $\mathsf{span}\{|0\rangle, |1\rangle\}$, while the span of $\{|0\rangle, \sqrt{1-2^{-200}}\,|0\rangle + 2^{-100}\,|2\rangle\}$ is exactly $\mathsf{span}\{|0\rangle, |2\rangle\}$. Two almost identical state families might have very different spans.

In order to relate other notions of complexity to the "overlap" on the span of easy states, we need to introduce a notion of "robust" span, which characterizes the significant components of the state family. A bit more formally, the "robust" span of a state family $\{|\psi_k\rangle\}$ is the subspace spanned by all the significant eigenvalues of $\mathbb{E}_k\,|\psi_k\rangle\!\langle\psi_k|$, where the expectation is taken over uniformly random k. This subspace is much more robust against perturbations, and, in Subsection 9.2, we are able to tightly relate $\underline{\mathsf{H}}$ to the "robust" span: a state has low H-complexity if and only if it has a large overlap onto the robust span of easy states. This relation allows us to give an alternative proof of the characterization of EFI from the hardness of GapH. With this relation in hand, we can summarize the proof of the latter characterization as follows:

- If EFI exist, then a non-uniform state family with a $\underline{\mathsf{H}}$-complexity gap exists (as our Theorem 1.1 says that EFI implies non-uniform $\mathsf{1PRS}$).
- For the converse direction, our proof goes through the following steps: we show that a state family with a $\underline{\mathsf{H}}$-complexity gap also has a gap in overlap with the "robust span of easy states"; the latter gap implies a gap in von Neumann entropy; finally, if EFI do not exist, such an entropy gap can be detected using quantum randomness extractors.

3 Preliminaries

In this section, we introduce the fundamentals of quantum information, quantum extractors, quantum cryptography, and the necessary tools.

3.1 Quantum information

Our notation for quantum information mainly follows [NC02]. We refer the reader to [NC02] for a more detailed discussion. For a given Hilbert space $\mathcal{H}$, we use $\mathrm{L}(\mathcal{H})$ and $\mathrm{P}(\mathcal{H})$ to denote the set of linear operators and positive semi-definite operators on $\mathcal{H}$. For $A, B \in \mathrm{L}(\mathcal{H})$, we write $A \geq B$ or $B \leq A$ if $A - B \in \mathrm{P}(\mathcal{H})$. The Schatten 1-norm of a linear operator A is defined as

$$\|A\|_1 = \mathrm{Tr}(\sqrt{A^\dagger A}). \tag{1}$$

A pure quantum state is a unit vector in a Hilbert space $\mathcal{H}$. A mixed quantum state is a density matrix ρ in $\mathrm{P}(\mathcal{H})$ with unit trace. We use $\mathrm{D}(\mathcal{H})$ to denote the set of density matrices on a Hilbert space $\mathcal{H}$. When considering multiple quantum systems, we use labels such as A and B to refer to different systems and use $\mathcal{H}_A$ and $\mathcal{H}_B$ to denote the corresponding Hilbert spaces. For example, $\rho_{AB} \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is a density matrix describing a mixed state on the joint AB system. We also consider sub-normalized states ρ where $\rho \in \mathrm{P}(\mathcal{H})$ and $\mathrm{Tr}(\rho) \leq 1$. In this case, the matrix ρ is called a semi-density matrix. We use $\mathrm{D}_{\leq}(\mathcal{H})$ to denote the set of semi-density matrices. Every density matrix $\rho_A \in \mathrm{D}(\mathcal{H})$ has a purification $|\psi\rangle_{AB}$ such that $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|_{AB})$, where Tr_B is the partial trace over B.

Various distance measures between two quantum states are needed. For density matrices ρ and σ, we use $D(\rho, \sigma)$ to denote their trace distance:

$$D(\rho, \sigma) = \frac{1}{2} \|\rho - \sigma\|_1 .$$

The trace distance generalizes the total variation distance between probability distributions. For pure states $|\psi\rangle$ and $|\phi\rangle$, the trace distance can be computed as $\sqrt{1 - |\langle\psi|\phi\rangle|^2}$.

Another commonly used quantity measuring the closeness of two quantum states is the fidelity:

$$F(\rho, \sigma) = \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1 .$$

For pure states $|\psi\rangle, |\phi\rangle \in \mathcal{H}$, we have $F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|$. Fidelity can be seen as a quantum generalization of the Bhattacharyya coefficient for two probability distributions, $\mathrm{BC}(p, q) = \sum_i \sqrt{p_i q_i}$. Uhlmann's theorem characterizes the fidelity of two mixed states $\rho, \sigma \in \mathrm{D}(\mathcal{H}_A)$ as the maximum overlap of their purifications: $F(\rho, \sigma) = \max_{|\psi\rangle, |\phi\rangle} |\langle\psi|\phi\rangle|$, where $|\psi\rangle, |\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ are purifications of ρ and σ, respectively, and system B is a copy of system A with the same dimension.

Lemma 3.1 (Fuchs-van de Graaf inequalities, cf., for example, Theorem 3.33 of [Wat18]). *For any mixed states ρ and σ, we have*

$$D(\rho, \sigma) \geq 1 - F(\rho, \sigma).$$

Lemma 3.2. *Let $\{\rho_k\}$ be a family of quantum states. If for all k, there is a state ρ'_k such that $D(\rho_k, \rho'_k) \leq \delta$, we have $D(\mathbb{E}_k\, \rho_k, \mathbb{E}_k\, \rho'_k) \leq \delta$.*

Proof. This follows directly from the joint convexity of the trace distance. □

The trace distance and fidelity can be generalized to sub-normalized states [TCR10]. For two semi-density matrices $\rho, \sigma \in \mathrm{D}_{\leq}(\mathcal{H})$,

$$D(\rho, \sigma) = \frac{1}{2}\left\|\rho - \sigma\right\|_1 + \frac{1}{2}\left|\mathrm{Tr}(\rho) - \mathrm{Tr}(\sigma)\right|,$$
$$F(\rho, \sigma) = \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1 + \sqrt{1 - \mathrm{Tr}(\rho)}\sqrt{1 - \mathrm{Tr}(\sigma)}.$$

These generalizations are obtained by extending the system and considering the normalized states $\rho \oplus (1 - \mathrm{Tr}(\rho))$ and $\sigma \oplus (1 - \mathrm{Tr}(\sigma))$, so many properties of the trace distance and fidelity carry over to the generalized versions.

For two semi-density matrices $\rho, \sigma \in \mathrm{D}_{\leq}(\mathcal{H})$, the purified distance [TCR10, Tom12] is defined as

$$P(\rho, \sigma) = \sqrt{1 - F^2(\rho, \sigma)}.$$

It is known that P is a metric on $\mathrm{D}_{\leq}(\mathcal{H})$ and that $P(\rho, \sigma) \geq D(\rho, \sigma)$. The purified distance is used to define the smoothed versions of min-entropy considered below.

For our purposes, we require the following definitions of quantum entropies. The von Neumann entropy of a state $\rho \in \mathrm{D}(\mathcal{H})$ is defined as $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$. If $\rho \in \mathrm{D}(\mathcal{H}_A)$ is a density matrix of system A, we may also write $S(A)_\rho$ to denote the von Neumann entropy, and may omit the subscript ρ and simply write $S(A)$ when no confusion arises. The quantum conditional entropy is defined as $S(A|B)_\rho = S(AB)_\rho - S(B)_\rho$. Unlike the classical case, the quantum conditional entropy can be negative. The relative entropy of ρ with respect to σ is $S(\rho\|\sigma) = \mathrm{Tr}(\rho \log \rho - \rho \log \sigma)$.

The quantum min-entropy of a sub-normalized quantum state $\rho \in \mathrm{D}_{\leq}(\mathcal{H})$ is $H_{\min}(\rho) = \sup\{\lambda \in \mathbb{R} \mid \rho \leq 2^{-\lambda} I\}$. The ε-smooth min-entropy of a sub-normalized quantum state $\rho \in \mathrm{D}_{\leq}(\mathcal{H})$ is

$$H^{\varepsilon}_{\min}(\rho) = \sup_{\rho' \in \mathrm{D}_{\leq}(\mathcal{H}), P(\rho, \rho') \leq \varepsilon} H_{\min}(\rho').$$

The quantum conditional min-entropy of a semi-density matrix $\rho_{AB} \in \mathrm{D}_{\leq}(\mathcal{H}_{AB})$ is defined as

$$H_{\min}(A|B)_\rho = \sup_{\sigma_B \in \mathrm{D}(\mathcal{H}_B)} \sup\{\lambda \in \mathbb{R} \mid \rho \leq 2^{-\lambda} I_A \otimes \sigma_B\}.$$

Its smoothed version is given by

$$H^{\varepsilon}_{\min}(A|B)_\rho = \sup_{\rho'_{AB} \in \mathrm{D}_{\leq}(\mathcal{H}_{AB}), P(\rho, \rho') \leq \varepsilon} H_{\min}(A|B)_{\rho'}.$$

The quantum max-entropy, according to [Ren08], is defined as[4]

$$H_{\max}(\rho) = \log(\mathrm{rank}(\rho)).$$

[4] The quantum max-entropy has definitions by Renner and Tomamichel. Ref [Ren08] defines the max-entropy as the Rényi entropy of order 0, while [Tom12] defines the max-entropy as the Rényi entropy of order 1/2. We adopt the definition from [Ren08] as it has a better operational meaning.

Its smoothed version is given by

$$H_{\max}^{\varepsilon}(\rho) = \inf_{\rho' \in \mathrm{D}_{\leq}(\mathcal{H}), P(\rho,\rho') \leq \varepsilon} H_{\max}(\rho').$$

The following inequality between smoothed min-entropy and von Neumann entropy is implicit in [Tom12].

Lemma 3.3 (Result 5 and Corollary 6.5 of [Tom12])**.** *Let ρ be an arbitrary quantum state on systems A and B and let R be the quantum system of its purification. Let n be the number of qubits of system A. For $g(\varepsilon) = -\log(1-\sqrt{1-\varepsilon^2})$, $0 < \varepsilon < 1$, and $m \geq \frac{8}{5} g(\varepsilon)$, we have*

$$\frac{1}{m} H_{\min}^{\varepsilon}(A^m|B^m)_{\rho^{\otimes m}} \geq S(A|B)_\rho - \frac{2(n+4)\sqrt{g(\varepsilon)}}{\sqrt{m}},$$
$$\frac{1}{m} H_{\max}^{\varepsilon}(A^m|B^m)_{\rho^{\otimes m}} \leq S(A|B)_\rho + \frac{2(n+4)\sqrt{g(\varepsilon)}}{\sqrt{m}}.$$

Corollary 3.1. *Let ρ be an arbitrary quantum systems on systems A and B. Let n be the number of qubits of system A. For any $m \geq 5 \log \frac{1}{\varepsilon}$, $\varepsilon < 1/2$ and $n > 10$, we have*

$$\frac{1}{m} H_{\min}^{\varepsilon}(A^m|B^m)_{\rho^{\otimes m}} \geq S(A|B)_\rho - 6n\sqrt{\frac{\log(1/\varepsilon)}{m}},$$
$$\frac{1}{m} H_{\max}^{\varepsilon}(A^m|B^m)_{\rho^{\otimes m}} \leq S(A|B)_\rho + 6n\sqrt{\frac{\log(1/\varepsilon)}{m}}.$$

Proof. This is just a direct application of Lemma 3.3 and the observation that $g(\varepsilon) = -\log(1-\sqrt{1-\varepsilon^2}) \leq 3 \log \frac{1}{\varepsilon}$. □

Remark. When we take B as the trivial system in Lemma 3.3 and Corollary 3.1, then we get the bound of $H_{\min}^{\varepsilon}(\rho^{\otimes m})$ and $H_{\max}^{\varepsilon}(\rho^{\otimes m})$ with $S(\rho)$.

The following helper lemma will be useful in entropy estimation.

Definition 3.1 (Almost Orthogonality)**.** We call two n-qubit quantum mixed states ρ, σ are almost orthogonal if there exists a projector Π such that $\mathrm{Tr}((I-\Pi)\rho) \leq \mathrm{negl}(n)$, and $\mathrm{Tr}(\Pi\sigma) \leq \mathrm{negl}(n)$.

Lemma 3.4. *If two n-qubit states ρ, σ have trace distance $D(\rho,\sigma) \geq 1 - \mathrm{negl}(n)$, ρ and σ are almost orthogonal.*

Proof. The proof of the lemma follows from the operational meaning of trace distance via setting the projector Π as the pretty good measurement. □

Lemma 3.5. *For two almost orthogonal n-qubit states ρ, σ,*

$$\left| S\Big(\frac{\rho+\sigma}{2}\Big) - \frac{S(\rho)+S(\sigma)}{2} - 1 \right| \leq \mathrm{negl}(n).$$

Proof. By Definition 3.1, there exists a projector Π such that $\mathrm{Tr}((I-\Pi)\rho) \leq \mathrm{negl}(n)$, and $\mathrm{Tr}(\Pi\sigma) \leq \mathrm{negl}(n)$. We denote $\tilde{\rho} = \frac{\Pi\rho\Pi}{\mathrm{Tr}(\Pi\rho\Pi)}$ and $\tilde{\sigma} = \frac{(I-\Pi)\sigma(I-\Pi)}{\mathrm{Tr}((I-\Pi)\sigma(I-\Pi))}$.

By the gentle measurement lemma [Win99], we have that $D(\rho,\tilde{\rho}) \leq \mathrm{negl}(n)$ and $D(\sigma,\tilde{\sigma}) \leq \mathrm{negl}(n)$, and thus $D((\rho+\sigma)/2, (\tilde{\rho}+\tilde{\sigma})/2) \leq \mathrm{negl}(n)$. By Fannes inequality [Fan73], we have that $|S(\tilde{\rho}) - S(\rho)|$, $|S(\tilde{\sigma}) - S(\sigma)|$, and $|S((\rho+\sigma)/2) - S((\tilde{\rho}+\tilde{\sigma})/2)|$ are negligible. Since $\tilde{\rho}$ and $\tilde{\sigma}$ are orthogonal, we have that

$$S\left(\frac{\tilde{\rho}+\tilde{\sigma}}{2}\right) = \frac{S(\tilde{\rho}) + S(\tilde{\sigma})}{2} + 1.$$

The lemma follows from a triangle inequality. □

Definition 3.2. Let $n(\cdot)$ be a polynomial function. We say that $\{|\psi_k\rangle\}_{k\in\{0,1\}^{n(\lambda)},\lambda\in\mathbb{N}}$ is an *efficiently samplable distribution of keyed states* if there exists a QPT quantum algorithm G such that, for all k of length $n(\lambda)$, we have $G(1^\lambda, k) = |\psi_k\rangle$. We say that $\{|\psi_k\rangle\}_{k\in\{0,1\}^{n(\lambda)},\lambda\in\mathbb{N}}$ is a *non-uniform* efficiently samplable distribution of keyed states if there exists a *non-uniform* quantum polynomial-time algorithm G such that, for all k of length $n(\lambda)$, $G(1^\lambda, k) = |\psi_k\rangle$. We sometimes denote the advice string as a, and refer to the length of a as the advice size of the family.

Definition 3.3. We say that $\{|\psi_k\rangle\}_{k\in\{0,1\}^*}$ together with a family distribution $\{\mathcal{D}_n\}_{n\in\mathbb{N}}$ is a single-copy samplable family if $\mathcal{D}_n$ is a distribution on $|\psi_k\rangle$ with $k \in \{0,1\}^n$ and there exists a QPT algorithm $\mathcal{A}$ that takes in 1^n as input and outputs a pair $(k, |\psi_k\rangle)$ according to the distribution $\mathcal{D}_n$.

3.2 Quantum cryptographic primitives

We recall several existing quantum cryptographic primitives used in this paper. EFI pairs were first proposed by Brakerski, Canetti, and Qian [BCQ22].

Definition 3.4 (EFI)**.** We call two families of mixed states $\{\rho_{0,\lambda}\}_\lambda$ and $\{\rho_{1,\lambda}\}_\lambda$ an EFI pair if the following conditions hold:

Efficient Generation: There exists a QPT algorithm G that takes input $(1^\lambda, b)$ for integer λ and $b \in \{0,1\}$, and outputs the mixed state $\rho_{b,\lambda}$.

Statistically Far: $D(\rho_{0,\lambda}, \rho_{1,\lambda}) \geq 1 - \mathrm{negl}(\lambda)$.

Computational Indistinguishability: For any QPT adversary $\mathcal{A}$, we have

$$\left|\Pr[\mathcal{A}(1^\lambda, \rho_{0,\lambda}) = 1] - \Pr[\mathcal{A}(1^\lambda, \rho_{1,\lambda}) = 1]\right| \leq \mathrm{negl}(\lambda).$$

Remark. In the original definition of EFI in [BCQ22], they only required $1/\mathrm{poly}(\lambda)$ statistical gap. It is easy to show the equivalence between their definition and the current definition by considering polynomial copies of their states (say, by [BQSY24]).

We can relax the definition of EFI to allow other gaps in the statistical distance and computational indistinguishability.

Definition 3.5 (Weak EFI)**.** For any functions $\varepsilon(\cdot)$ and $\delta(\cdot)$, we call two families of mixed states $\{\rho_{0,\lambda}\}_\lambda, \{\rho_{1,\lambda}\}_\lambda$ an (ε, δ)-weak EFI pair if the following conditions hold:

Efficient Generation: There exists a QPT algorithm G that takes input $(1^\lambda, b)$ for integer λ and $b \in \{0,1\}$, and outputs the mixed state $\rho_{b,\lambda}$.

Statistically $(1-\varepsilon)$*-Far:* $D(\rho_{0,\lambda}, \rho_{1,\lambda}) \geq 1 - \varepsilon(\lambda)$.

δ*-Computational Indistinguishability:* For any QPT adversary $\mathcal{A}$, we have

$$\left|\Pr[\mathcal{A}(1^\lambda, \rho_{0,\lambda}) = 1] - \Pr[\mathcal{A}(1^\lambda, \rho_{1,\lambda}) = 1]\right| \leq \delta(\lambda) + \mathrm{negl}(\lambda).$$

In certain parameter regime, weak EFI pairs imply standard EFI pairs. The following theorem is implicit in [BQSY24].

Theorem 3.1 (Weak EFI implies EFI)**.** *The existence of an (ε,δ)-weak* EFI *pair family in any of the following parameter range implies a standard* EFI

- $\varepsilon = \mathrm{negl}(\lambda), \delta = 1 - \frac{1}{\mathrm{poly}(\lambda)}$.
- $\varepsilon = 1 - \frac{1}{\mathrm{poly}(\lambda)}, \delta = \mathrm{negl}(\lambda)$.
- $(1-\varepsilon)^2 - \sqrt{\delta} \geq C$ *for some universal constant C independent of λ.*

implies the existence of a standard EFI pair family.

Definition 3.6 (Single-copy Pseudorandom State (1PRS))**.** A state family $\{|\phi_k\rangle\}$ of $n(\lambda)$ qubits and key length $\ell(\lambda)$ is called single-copy pseudorandom if the following conditions hold:

Efficient Preparation: There is a QPT algorithm G that on input $(1^\lambda, k)$ prepares the state $|\phi_k\rangle$.

Single-copy Pseudorandom Property: For any QPT adversary $\mathcal{A}$, there exists a negligible function $\mathrm{negl}(\cdot)$ such that for all $\lambda \in \mathbb{N}$ and $n = n(\lambda)$,

$$\left| \Pr_k[\mathcal{A}(1^\lambda, |\phi_k\rangle) = 1] - \Pr_{|\phi\rangle \leftarrow \mu_n}[\mathcal{A}(1^\lambda, |\phi\rangle) = 1] \right| = \mathrm{negl}(\lambda), \tag{2}$$

where μ_n is the Haar measure on $n(\lambda)$-qubit states.

Stretch Property: The length $\ell(\lambda)$ of the key k is strictly less than the number of qubits $n(\lambda)$.

3.3 Quantum extractors

As a natural generalization of classical extractors, there are also studies of quantum extractors in the context of quantum information [BFW14, DBWR14]. We rephrase their definition and results to show their similarity with classical extractors.

Definition 3.7 ((k,ε,δ)-Quantum Strong Extractor)**.** Let $\ell \in \mathbb{N}$ and $A = A_1A_2$ be a quantum system with A_1 and A_2 as subsystems, where the subsystem A_1 consists of ℓ qubits. A collection of quantum unitaries $\{U_j\}_{j\in L}$ acting on system A is called a (k,ε,δ)-quantum strong extractor that extracts ℓ qubits if for any quantum state $\rho_{AE} \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_E)$ with $H^\delta_{\min}(A|E)_\rho \geq k$,

$$D\left(\frac{1}{|L|} \sum_{j\in L} |j\rangle\langle j| \otimes \mathrm{Tr}_{A_2}(U_j \rho_{AE} U_j^\dagger), \frac{I_L}{|L|} \otimes \frac{I_{A_1}}{|A_1|} \otimes \rho_E \right) \leq \varepsilon.$$

To construct quantum extractors, we need the unitary t-design.

Definition 3.8. An ensemble of quantum unitaries $\{U_r\}_{r\in R}$ is called a unitary t-design if for all $M \in \mathrm{L}(A)$:

$$\frac{1}{|R|} \sum_{r\in R} U_r^{\otimes t} M U_r^{\dagger^{\otimes t}} = \int U^{\otimes t} M U^{\dagger^{\otimes t}} \mathrm{d}\eta(U),$$

where η is the Haar measure over $U(A)$.

Unitary t-designs can be viewed as the quantum analog of classical t-wise independent hash functions.

We use the Choi-Jamiołkowski isomorphism.

Definition 3.9. The Choi-Jamiołkowski map J takes maps $\mathcal{T}_{A\to B} : \mathrm{L}(\mathcal{H}_A) \to \mathrm{L}(\mathcal{H}_B)$ to operators $J(\mathcal{T}_{A\to B})$ in $\mathrm{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$. It is defined as

$$J(\mathcal{T}_{A\to B}) = (\mathcal{I}_A \otimes \mathcal{T}_{A'\to B})(|\phi\rangle\langle\phi|_{AA'}),$$

where $|\phi\rangle_{AA'} = \frac{1}{\sqrt{|A|}} \sum_i |i\rangle_A \otimes |i\rangle_{A'}$.

Remark. It is well known that this map is in fact an isomorphism: The Choi-Jamiołkowski map J bijectively maps the set of completely positive maps from $\mathcal{H}_A$ to $\mathcal{H}_B$ to the set $\mathrm{P}(\mathcal{H}_A\otimes\mathcal{H}_B)$, and its inverse maps any $\gamma_{AB} \in \mathrm{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ to

$$\mathcal{T}_{A\to B} : M_A \mapsto |A|\mathrm{Tr}_A \left[\gamma_{AB} M_A^T\right]$$

Using this, $J(\mathcal{T}_{A\to B})$ is called the Choi-Jamiołkowski representation of $\mathcal{T}_{A\to B}$.

We recall the decoupling theorem proved in [DBWR14, Theorem 3.1].

Theorem 3.2 (Decoupling Theorem)**.** *Let $\mathcal{T}_{A\to B}$ be a completely-positive map with Choi-Jamiołkowski representation $\tau_{AB} = J(\mathcal{T})$ such that $\mathrm{Tr}(\tau_{AB}) \leq 1$. Let E be a quantum system for the environment. Then, for $\varepsilon > 0$, $\rho_{AE} \in \mathrm{D}(\mathcal{H}_A\otimes\mathcal{H}_E)$, and any unitary 2-design $\{U_j\}_{j\in L}$ on A, we have*

$$\frac{1}{|L|}\sum_{j\in L} \left\|\mathcal{T}(U_j\rho_{AE}U_j^\dagger), \tau_B \otimes \rho_E\right\|_1 \leq 2^{-\frac{1}{2}H^\varepsilon_{\min}(A|E)_\rho - \frac{1}{2}H^\varepsilon_{\min}(A|B)_\tau} + 12\varepsilon.$$

Lemma 3.6. *Let $k \in [-n, n]$ and $\varepsilon \in (0, 1)$. Let E be a quantum system for the environment and $A = A_1A_2$ be an n-qubit quantum system with A_1 and A_2 as subsystems, where the subsystem A_1 consists of at most $\frac{n+k}{2} - \log(1/\varepsilon)$ qubits. Let $\rho_{AE} \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_E)$ be a density matrix on systems A and E having smoothed conditional min-entropy $H^{\varepsilon/12}_{\min}(A|E) \geq k$. Then, for any unitary 2-design $\{U_j\}_{j\in L}$ on A,*

$$\frac{1}{2|L|}\sum_{j\in L}\left\|\mathrm{Tr}_{A_2}\left(U_j\rho_{AE}U_j^\dagger\right) - \frac{I_{A_1}}{|A_1|}\otimes\rho_E\right\|_1 \leq \varepsilon.$$

Proof of Lemma 3.6. We apply Theorem 3.2 to prove the statement and choose B to be the subsystem A_1, and $\mathcal{T}$ to be the partial trace over subsystem A_2.

By definition, we compute the Choi-Jamiołkowski state

$$\tau_{AB} = \frac{1}{|A_1|}\sum_{x,y} |x\rangle\langle y|_{A_1} \otimes \frac{I_{A_2}}{|A_2|} \otimes |x\rangle\langle y|_B\,.$$

Its reduced density matrix $\tau_B = \frac{I_B}{|B|}$ is maximally mixed. The conditional min-entropy $H_{\min}(A|B)_\tau$ of τ_{AB} can be computed as

$$\begin{aligned} H_{\min}(A|B)_\tau &= \log|A_2| + H_{\min}(A_1|B) \\ &= \log|A_2| - \log|A_1| \\ &= n - 2\log|A_1| \\ &\geq 2\log(1/\varepsilon) - k, \end{aligned}$$

where the last step follows from the condition on the number of qubits in system A_1. Hence, we can bound

$$H_{\min}^{\varepsilon/12}(A|E)_\rho + H_{\min}^{\varepsilon/12}(A|B)_\tau \geq H_{\min}^{\varepsilon/12}(A|E)_\rho + H_{\min}(A|B)_\tau \geq 2\log(1/\varepsilon), \tag{3}$$

where the first inequality follows from the definition of smoothed min-entropy taking the maximum over close states.

The conditions of Theorem 3.2 are all met and we have

$$\frac{1}{|L|}\sum_{j\in L}\left\|\mathrm{Tr}_{A_2}\left(U_j\rho_{AE}U_j^\dagger\right) - \frac{I_{A_1}}{|A_1|}\otimes\rho_E\right\|_1 \leq 2^{-\frac{1}{2}H_{\min}^{\varepsilon/12}(A|E)_\rho - \frac{1}{2}H_{\min}^{\varepsilon/12}(A|B)_\tau} + \varepsilon \leq 2\varepsilon,$$

where the last step follows from Eq. (3). □

Theorem 3.3. *Let $n, \ell \in \mathbb{N}$, $k \in [-n, n]$, and $\varepsilon \in (0,1)$ such that $\ell \leq \frac{n+k}{2} - \log(1/\varepsilon)$. Then any unitary 2-design on n-qubit system is a $(k, \varepsilon, \varepsilon/12)$-quantum strong extractor that extracts ℓ qubits.*

Proof. By Definition 3.7, the condition for the unitary 2-design $\{U_j\}_{j\in L}$ on n-qubit system A to be such a quantum strong extractor is that for every state ρ on systems A and E having smoothed conditional min entropy $H_{\min}^{\varepsilon/12}(A|E)_\rho \geq k$,

$$D\left(\frac{1}{|L|}\sum_{j\in L}|j\rangle\langle j|\otimes \mathrm{Tr}_{A_2}(U_j\rho_{AE}U_j^\dagger), \frac{I_L}{|L|}\otimes\frac{I_{A_1}}{|A_1|}\otimes\rho_E\right) \leq \varepsilon,$$

where A_1 consists of ℓ qubits, and A_2 consists of the other $n-\ell$ qubits. The left hand side is the trace distance of two block diagonal matrices indexed by j and can hence be simplified to

$$\frac{1}{|L|}\sum_{j\in L} D\left(\mathrm{Tr}_{A_2}\left(U_j\rho_{AE}U_j^\dagger\right), \frac{I_{A_1}}{|A_1|}\otimes\rho_E\right).$$

The statement then follows from Lemma 3.6. □

For a given unitary 2-design $\{U_j\}_{j\in L}$ on an n-qubit quantum system $A = A_1A_2$, we introduce the notation $\mathsf{Ext}_\ell^{A\to A_1}(\cdot)$, or simply $\mathsf{Ext}_\ell^{A}(\cdot)$, to denote the extractor that extracts ℓ qubits (on A_1) from the input system A. That is,

$$\mathsf{Ext}_\ell^{A\to A_1}(\rho_{AE}) = \frac{1}{|L|}\sum_{j\in L}|j\rangle\langle j|\otimes\mathrm{Tr}_{A_2}(U_j\rho_{AE}U_j^\dagger).$$

The claim in the above theorem can be written as

$$D\left(\mathsf{Ext}_\ell^{A}(\rho_{AE}), \frac{I_L}{|L|}\otimes\frac{I_{A_1}}{|A_1|}\otimes\rho_E\right) \leq \varepsilon,$$

for $\ell \leq (n + H_{\min}^{\varepsilon/12}(A|E))/2 - \log(1/\varepsilon)$.

3.4 Kolmogorov complexity

In this paper we will use several notions of Kolmogorov complexity. The most well-known of these is the standard prefix-free classical Kolmogorov complexity of binary strings, which we denote by $\mathsf{K}(x)$.

Definition 3.10. Let U be a universal prefix-free Turing machine. For strings $x \in \{0,1\}^*$, the Kolmogorov complexity $\mathsf{K}_U(x)$ of x is the length of the shortest program p such that $U(p)$ will halt and output x after a finite number of steps.

We clarify that, here and in the rest of the paper, by "length of a program p" we mean the length of the string corresponding to p when viewed as an input to the universal Turing machine U (we do not mean the size of the program p in terms of some set of gates).

Because for any two universal Turing machines U and V there exists some constant c such that for all x, $|\mathsf{K}_U(x) - \mathsf{K}_V(x)| < c$, the choice of universal Turing machine is unimportant to us. So, we choose to fix some universal Turing machine U, and simply write $\mathsf{K}(x)$, dropping the subscript.

In this work we are interested in the complexity of quantum states, and we will use several generalizations of Kolmogorov complexity that allow us to measure their complexity. The first of these was introduced by Mora and Briegel [MB04, MBK06] and can be thought of as measuring the amount of classical information required to generate a good approximation of the state of interest. It is defined relative to some choice of a universal classical Turing machine U and a universal quantum gate set B. It measures the length of the shortest program on which the universal classical Turing machine outputs a description of a quantum circuit C that, when given $|0\cdots 0\rangle$ as input, outputs a state which is ε-close to the state of interest.

Definition 3.11 ($\mathsf{K}_{\mathsf{net}}$-*complexity* [MB04, MBK06])**.** Let U be a universal Turing machine, B a universal set of quantum gates, and $\mathcal{C}^B$ be the set of circuits composed of gates from B. Let $\varepsilon \in [0,1]$. For a pure state $|\psi\rangle$, we define its $\mathsf{K}_{\mathsf{net}}$-*complexity* as:

$$\mathsf{K}_{\mathsf{net}}^{U,B,\varepsilon}(|\psi\rangle) = \min_p \{|p| : C = U(p) \in \mathcal{C}^B \text{ and } |\langle\psi| C |0^m\rangle|^2 \geq 1 - \varepsilon\},$$

where the minimum is taken over program descriptions p, and $\mathcal{C}^B$ is the set of quantum circuits of finite size consisting of gates from B (here, m denotes the size of inputs to C, which can depend on C).

Since B and U are universal, this definition changes only by a just barely superconstant factor when we change our choice of U or B (see Appendix A.1 for details). So, going forward, we will simply fix a choice of U and B and write $\mathsf{K}_{\mathsf{net}}^{\varepsilon}(|\psi\rangle)$, dropping the superscripts.

The second notion that we will use was introduced by Gács [Gác01] and generalizes the definition of the classical Kolmogorov complexity $\mathsf{K}(x)$ when viewed as the negative logarithm of the probability of x being output by the "universal distribution". When U is prefix-free, the (classical) universal semi-distribution[5] D_U is defined as follows: sample a uniformly random program p, run $U(p)$, and return its output. Defining $\mathsf{K}(x) = -\log(\Pr[x \sim D_U])$ results in a notion equivalent to the one from Definition 3.10 up to an additive constant.

[5] A semi-distribution is a distribution where the total probability adds up to some value less than one, which here corresponds to the probability that we sample a program which halts. This is possible because U is prefix-free.

We can generalize D_U to the universal *semi-density matrix*[6] $\boldsymbol{\mu}$ in one of several equivalent ways. Gács chooses to take the outputs of $U(p)$ and interpret them as vectors of complex numbers describing the amplitudes of a state. He then takes $\boldsymbol{\mu}$ to be the resulting semi-density matrix from picking state $|\psi\rangle$ with the probability that D_U would output the vector corresponding to $|\psi\rangle$. We can take an approach closer to that of Mora and Briegel and equivalently define $\boldsymbol{\mu}_n$ to be the semi-density matrix resulting from picking state $|\psi\rangle$ over n qubits with the probability that D_U outputs a classical description of a quantum circuit C such that $C|0\rangle = |\psi\rangle$ (so we only consider circuits outputting n-qubit states). Towards this, we fix some finite universal set of quantum gates, and consider circuits consisting of gates from this set. Given this notion of universal semi-density matrix, Gács' notion of state complexity is the following.

Definition 3.12 ("$\underline{\mathsf{H}}$-complexity" [Gác01])**.** Let U be a universal Turing machine, and B a universal set of quantum gates. For a pure state $|\psi\rangle$ over n qubits, we define its $\underline{\mathsf{H}}$-complexity as

$$\underline{\mathsf{H}}^{U,B}(|\psi\rangle) = -\log \langle\psi|\boldsymbol{\mu}_n|\psi\rangle\,,$$

where $\boldsymbol{\mu}_n$ is the universal semi-density matrix defined with respect to U and B.

Since this variant of the notion is new, we include proofs of its invariance with respect to U and B and its equivalence with the notion introduced by Gács in Appendix A.1. Given its invariance we will fix a choice of U and B and write $\underline{\mathsf{H}}(|\psi\rangle)$, dropping the superscripts. Furthermore, whenever n is clear from context we will omit it and simply write $\boldsymbol{\mu}$. While the notion described here is equivalent to the notion defined by Gács, our notion is more natural in a setting like ours where we are interested in quantum algorithms.

We also introduce a robust version of Gács' complexity $\underline{\mathsf{H}}$.

Definition 3.13. For any $\varepsilon \in [0,1]$, we define

$$\underline{\mathsf{H}}^{\varepsilon}(|\psi\rangle) = \max_{|\phi\rangle : D(|\psi\rangle,|\phi\rangle)\leq\varepsilon} \underline{\mathsf{H}}(|\phi\rangle).$$

Remark. The definition of $\underline{\mathsf{H}}^{\varepsilon}$ takes the maximum of $\underline{\mathsf{H}}$ in the ε-neighborhood of $|\psi\rangle$, analogous to ε-smoothed min-entropies, since the purified distance becomes the trace distance for pure states. For a state to have small $\underline{\mathsf{H}}^{\varepsilon}$, all nearby states must have small $\underline{\mathsf{H}}$. We note that only taking the maximum is meaningful here, as $\underline{\mathsf{H}}$ is always small when taking the minimum in the following sense: any state is negligibly close to a state with $\underline{\mathsf{H}}$ less than $O(\log^2 n)$. Specifically, for any n-qubit state $|\psi\rangle$, it is $2^{-\log^2 n}$-close in purified distance to a state of the form $|\psi'\rangle = ae^{i\theta}|0^n\rangle + \sqrt{1-a^2}\,|\phi\rangle$, where $\langle 0^n|\phi\rangle = 0$ and $a \geq 2^{-\log^2 n}$. According to the definition of $\boldsymbol{\mu}$, we have $\frac{1}{cn}|0^n\rangle\langle 0^n| \leq \boldsymbol{\mu}$ for some constant c; thus,

$$\langle\psi'|\boldsymbol{\mu}|\psi'\rangle \geq \frac{1}{cn}\left|\langle\psi'|0^n\rangle\right|^2 \geq 2^{-2\log^2 n - \log(cn)},$$

which implies $\underline{\mathsf{H}}(|\psi'\rangle) \leq 2\log^2 n + \log(cn)$.

Gács' also considered a dual state complexity measure $\overline{\mathsf{H}}(|\psi\rangle) = -\langle\psi|\log\boldsymbol{\mu}|\psi\rangle$ which we do not use. What we will instead use is a new complexity measure U, which is overlooked by Gács' work. As we will see, this notion is closely related to the measures $\underline{\mathsf{H}}$ and $\overline{\mathsf{H}}$. Moreover, we find that this new measure is a much better dual of $\underline{\mathsf{H}}$ as their properties demonstrate.

[6] Similar to a semi-distribution, a semi-density matrix is defined as some $\sum_i c_i |\phi_i\rangle\langle\phi_i|$ where the c_i's add up to less than or equal to 1.

Consider the relative min-entropy, which is defined as

$$D_\infty(\rho\|\sigma) = \min\{\lambda \mid \rho \leq 2^\lambda \sigma\}.$$

The new measure $\mathsf{U}(|\psi\rangle)$ is the relative min-entropy of $|\psi\rangle$ with respect to the universal density matrix $\boldsymbol{\mu}$:

$$\mathsf{U}(|\psi\rangle) = D_\infty(\rho\|\boldsymbol{\mu}).$$

We can define the smoothed version of it as:

$$\mathsf{U}^\varepsilon(|\psi\rangle) = \min_{D(|\psi\rangle,|\phi\rangle)\leq\varepsilon} \mathsf{U}(|\phi\rangle).$$

We prove some simple properties of U.

Lemma 3.7. $\mathsf{U}(|\psi\rangle) = \log\langle\psi|\boldsymbol{\mu}^{-1}|\psi\rangle$.

Proof. $|\psi\rangle\langle\psi| \leq 2^r\boldsymbol{\mu}$ is equivalent to $\boldsymbol{\mu}^{-1/2}|\psi\rangle\langle\psi|\boldsymbol{\mu}^{-1/2} \leq 2^r I$. (note that $\boldsymbol{\mu}$ is invertible as $\boldsymbol{\mu}$ is a full-rank Hermitian matrix). Then, the inequality holds if and only if $\|\boldsymbol{\mu}^{-1/2}|\psi\rangle\|^2 \leq 2^r$, which can be reformulated as $\langle\psi|\boldsymbol{\mu}^{-1}|\psi\rangle \leq 2^r$, so we are done. □

Lemma 3.8. *For any quantum pure state $|\psi\rangle$ satisfying $\boldsymbol{\mu} \geq 2^{-\kappa}|\psi\rangle\langle\psi|$, we have $\mathsf{U}(|\psi\rangle) \leq \kappa$.*

Proof. Write $\boldsymbol{\mu} = 2^{-\kappa}|\psi\rangle\langle\psi| + \boldsymbol{\nu}$. We can assume without loss of generality that $\boldsymbol{\nu}$ is strictly positive; otherwise, we can consider a small perturbation of it. Using the Sherman-Morrison formula

$$\left(A + uv^\dagger\right)^{-1} = A^{-1} - \frac{A^{-1}uv^\dagger A^{-1}}{1 + v^\dagger A^{-1}u}$$

with $A = \boldsymbol{\nu}$, $u = v = 2^{-\kappa/2}|\psi\rangle$, we obtain

$$\boldsymbol{\mu}^{-1} = \boldsymbol{\nu}^{-1} - \frac{2^{-\kappa}\boldsymbol{\nu}^{-1}|\psi\rangle\langle\psi|\boldsymbol{\nu}^{-1}}{1 + 2^{-\kappa}\langle\psi|\boldsymbol{\nu}^{-1}|\psi\rangle}.$$

Define $w = \langle\psi|\boldsymbol{\nu}^{-1}|\psi\rangle$ and take the expectation value of $|\psi\rangle$ on both sides:

$$\begin{aligned}\langle\psi|\boldsymbol{\mu}^{-1}|\psi\rangle &= w - \frac{2^{-\kappa}w^2}{1 + 2^{-\kappa}w} \\ &= \frac{w}{1 + 2^{-\kappa}w} \\ &\leq 2^\kappa.\end{aligned}$$

This completes the proof. □

Lemma 3.9. *For any pure quantum state $|\psi\rangle$, we have*

$$\mathsf{U}(|\psi\rangle) \leq \mathsf{K}_{\mathsf{net}}(|\psi\rangle).$$

Proof. By the definition of $\boldsymbol{\mu}$, we have

$$\boldsymbol{\mu} = 2^{-\mathsf{K}_{\mathsf{net}}(|\psi\rangle)}|\psi\rangle\langle\psi| + \boldsymbol{\nu}$$

for some positive semi-definite $\boldsymbol{\nu}$. Lemma 3.8 then completes the proof. □

Lemma 3.10. *For all pure quantum states $|\psi\rangle$ and $\varepsilon \in (0,1]$, the following two bounds hold:*

$$\mathsf{U}^{1-\varepsilon}(|\psi\rangle) \geq \underline{\mathsf{H}}(|\psi\rangle) + \log \varepsilon,$$
$$\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \leq \mathsf{U}(|\psi\rangle) - \log \varepsilon.$$

Proof. By definition, $\mathsf{U}^{1-\varepsilon}(|\psi\rangle) = \min_{|\phi\rangle : D(|\psi\rangle, |\phi\rangle) \leq 1-\varepsilon} \mathsf{U}(|\phi\rangle)$. From the condition of the minimization, we have

$$D(|\psi\rangle, |\phi\rangle) = \sqrt{1 - |\langle\psi|\phi\rangle|^2} \leq 1 - \varepsilon,$$

and

$$|\langle\psi|\phi\rangle|^2 \geq 1 - (1-\varepsilon)^2 = 2\varepsilon - \varepsilon^2 \geq \varepsilon.$$

Using the Cauchy-Schwarz inequality, we have

$$\langle\psi|\boldsymbol{\mu}|\psi\rangle \langle\phi|\boldsymbol{\mu}^{-1}|\phi\rangle \geq |\langle\psi|\phi\rangle|^2 \geq \varepsilon.$$

Taking the logarithm on both sides completes the proof. The other inequality follows from a similar reasoning. □

Definition 3.14 (The GapH problem)**.** Let $r, \Delta, n \in \mathbb{N}$. Let $\varepsilon \in [0,1]$. We define $\mathsf{GapH}^{\varepsilon}(r, r+\Delta)$ as the following (promise) problem: given a *single* copy of a state $|\psi\rangle$ on some number n of qubits, decide whether

- $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \leq r$, or
- $\underline{\mathsf{H}}(|\psi\rangle) \geq r + \Delta$.

Definition 3.15 (Hardness of GapH over a "promise" family)**.** Let $r, \Delta, n \in \mathbb{N}$ be functions of λ. Let $\varepsilon \in [0,1]$. We say that $\mathsf{GapH}^{\varepsilon}(r, r+\Delta)$ is hard over a family of states $\{|\psi_k\rangle : k \in \{0,1\}^{n(\lambda)}\}_{\lambda\in\mathbb{N}}$ if the following hold:

- (*promise*) There exists a negligible function negl such that, for all $\lambda \in \mathbb{N}$, $\Pr_k[\underline{\mathsf{H}}^{1-\varepsilon}(|\psi_k\rangle) \leq r] \geq \frac{1}{2} - \mathrm{negl}(\lambda)$ and $\Pr_k[\underline{\mathsf{H}}(|\psi_k\rangle) \geq r + \Delta] \geq \frac{1}{2} - \mathrm{negl}(\lambda)$.
- (*hardness of distinguishing*) For any QPT adversary $\mathcal{A}$, there exists a negligible function negl' such that, for all $\lambda \in \mathbb{N}$,

$$\left| \Pr_k[\mathcal{A}(1^\lambda, |\psi_k\rangle) = 0 | C_{\text{high}}] - \Pr_k[\mathcal{A}(1^\lambda, |\psi_k\rangle) = 0 | C_{\text{low}}] \right| \leq \mathrm{negl}(\lambda),$$

  where C_{high} and C_{low} are events standing for $\underline{\mathsf{H}}(|\psi_k\rangle) \geq r + \Delta$ and $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi_k\rangle) \leq r$, respectively.

If the hardness is against *non-uniform* quantum polynomial-time adversaries, then we say that $\mathsf{GapH}^{\varepsilon}(r, r+\Delta)$ is non-uniformly hard over the family of states.

Definition 3.16 (The GapU problem)**.** Let $r, \Delta, n \in \mathbb{N}$. Let $\varepsilon \in [0,1]$. We define $\mathsf{GapU}^{\varepsilon}(r, r+\Delta)$ as the following (promise) problem: given a *single* copy of a state $|\psi\rangle$ on some number n of qubits, decide whether

- $\mathsf{U}(|\psi\rangle) \leq r$, or
- $\mathsf{U}^{1-\varepsilon}(|\psi\rangle) \geq r + \Delta$.

We then define the hardness of GapU similarly as we did for GapH in Definition 3.15.

4 Entropic EFI and pseudo-mixed states

In this section, we introduce two variants of the EFI primitive called entropic EFI and (non-uniform) pseudo-mixed states. As the main results of this section, we show that EFI implies both of these variants.

4.1 Entropic EFI from EFI

Entropic EFI uses the entropy difference as a measure of distance between the state pair, rather than the trace distance. The more formal definition is given in Definition 4.1.

Definition 4.1 (Entropic EFI)**.** We call two families of mixed states $\{\sigma_{0,\lambda}\}_\lambda$, $\{\sigma_{1,\lambda}\}_\lambda$ an entropic EFI pair, if the following condition holds:

Efficient Generation: There exists a QPT algorithm G that takes input $(1^\lambda, b)$ for security parameter λ and $b \in \{0,1\}$, and outputs the mixed state $\sigma_{b,\lambda}$.

Entropy Gap: $S(\sigma_{1,\lambda}) > S(\sigma_{0,\lambda}) + 1/\mathrm{poly}(\lambda)$.

Computational Indistinguishability: For any QPT adversary algorithm $\mathcal{A}$, we have that

$$\left|\Pr[\mathcal{A}(1^\lambda, \sigma_{0,\lambda}) = 1] - \Pr[\mathcal{A}(1^\lambda, \sigma_{1,\lambda}) = 1]\right| \leq \mathrm{negl}(\lambda).$$

We remark that by Fannes' inequality, every entropic EFI is automatically an EFI, as for any two states $\sigma_{0,\lambda}$ and $\sigma_{1,\lambda}$ satisfying $S(\sigma_{1,\lambda}) > S(\sigma_{0,\lambda}) + 1/\mathrm{poly}(\lambda)$, we have $D(\sigma_{1,\lambda}, \sigma_{0,\lambda}) \geq 1/\mathrm{poly}(\lambda)$. An EFI is not necessarily an entropic EFI, as there are states with large trace distance but no entropy difference. However, we can show that the existence of an EFI implies that of an entropic EFI by slightly modifying the state generation procedure.

Theorem 4.1. *The existence of* EFI *implies the existence of entropic* EFI.

Proof. Let $\{\rho_{0,\lambda}\}_\lambda$ and $\{\rho_{1,\lambda}\}_\lambda$ be an EFI pair that can be generated by a QPT algorithm G^*. We consider the quantum states

$$\begin{aligned} \sigma_{0,\lambda} &= \frac{1}{2}\,|0\rangle\langle 0| \otimes \rho_{0,\lambda} + \frac{1}{2}\,|1\rangle\langle 1| \otimes \rho_{1,\lambda}, \\ \sigma_{1,\lambda} &= \frac{I}{2} \otimes \frac{\rho_{0,\lambda} + \rho_{1,\lambda}}{2}. \end{aligned}$$

We claim that $\{\sigma_{0,\lambda}\}_\lambda$ and $\{\sigma_{1,\lambda}\}_\lambda$ form an entropic EFI family.

Efficient Generation It is not difficult to see that the following QPT algorithm G in Algorithm 1 outputs the mixed state $\sigma_{b,\lambda}$ on input $(1^\lambda, b)$.

Algorithm 1 Construction of the entropic EFI state generation algorithm G

```
Require: Inputs $1^\lambda$ and a state generation algorithm $G^*$ for EFI
If $b = 0$, initialize the registers $A$ and $B$ as the mixed state $\frac{|00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB}}{2}$.
If $b = 1$, initialize the registers $A$ and $B$ as the mixed state $\frac{I_A}{2} \otimes \frac{I_B}{2}$.
Run $G^*(1^\lambda, \cdot)$ on the register $B$ and store the obtained state in register $C$.
Output registers $A$ and $C$.
```

Entropy Gap We can directly calculate the entropy of $\sigma_{0,\lambda}$, since it can be block diagonalized:

$$S(\sigma_{0,\lambda}) = \frac{S(\rho_{0,\lambda}) + S(\rho_{1,\lambda})}{2} + 1.$$

Note that by Definition 3.4, $D(\rho_{0,\lambda}, \rho_{1,\lambda}) \geq 1 - \mathrm{negl}(\lambda)$. Thus by Lemmas 3.4 and 3.5, we have that

$$\begin{aligned} S(\sigma_{1,\lambda}) &= 1 + S\left(\frac{\rho_{0,\lambda} + \rho_{1,\lambda}}{2}\right) \\ &\geq 2 + \frac{S(\rho_{0,\lambda}) + S(\rho_{1,\lambda})}{2} - \mathrm{negl}(\lambda). \end{aligned}$$

This implies an $1 - \mathrm{negl}(\lambda)$ entropy gap between $\sigma_{0,\lambda}$ and $\sigma_{1,\lambda}$.

Computational Indistinguishability By Definition 3.4, $\rho_{0,\lambda}$ and $\rho_{1,\lambda}$ are computationally indistinguishable. A standard hybrid argument shows that $\sigma_{0,\lambda} \approx_c \frac{I}{2} \otimes \rho_{0,\lambda} \approx_c \sigma_{1,\lambda}$, which concludes the proof of Theorem 4.1.

□

4.2 Non-uniform pseudo-mixed states from entropic EFI

Next, we study a variant of EFI pair called pseudo-mixed states. Informally, a pseudo-mixed state is an efficiently preparable state ρ that, together with the maximally mixed state, forms an EFI. That is, ρ is far from $I/2^n$, yet no QPT algorithm can distinguish them with non-negligible advantage. We require a non-uniform version of PMS for which the generation algorithm uses a classical advice string. The formal definition of (non-uniform) PMS is given in Definition 4.2.

Algorithm 2 Construction of non-uniform PMS from entropic EFI

```
Require: Inputs $1^\lambda$, a classical advice $a(\lambda) \in [\lambda^2 n^2(\lambda) p^2(\lambda)]$, and a state generation algorithm $G$ for the entropic EFI.
Let $\rho_{0,\lambda}$, $\rho_{1,\lambda}$ be the $n(\lambda)$-qubit entropic EFI family pair with entropy gap $1/p(\lambda)$ for polynomial $p$, namely $S(\rho_{1,\lambda}) - S(\rho_{0,\lambda}) \geq 1/p(\lambda)$.
Let $m(\lambda) = \lambda^2 n^2(\lambda) p^2(\lambda)$, and $\rho'_{0,\lambda} = \rho_{0,\lambda}^{\otimes m}, \rho'_{1,\lambda} = \rho_{1,\lambda}^{\otimes m}$.
Let $\varepsilon(\lambda) = 2^{-\lambda} k(\lambda) = a(\lambda) - \lambda^2 n^2(\lambda) p(\lambda)/2$ and $\ell(\lambda) = (n(\lambda)m(\lambda) + k(\lambda))/2 - \log(1/\varepsilon)$.
Let $\{C_j\}_{j \in L}$ be the Clifford family over $n(\lambda)m(\lambda)$ qubits. By Theorem 3.3, it's a $(k, \varepsilon, \varepsilon/12)$ quantum strong extractor $\mathsf{Ext}_\ell^{A \to A_1}$ that extracts $\ell$ qubits. Let $A = A_1 A_2$ where subsystem $A_1$ consists of the first $\ell$ qubits of system $A$ and subsystem $A_2$ consists of the last $n(\lambda)m(\lambda) - \ell(\lambda)$ qubits.
Output state
    $$\tau_{0,\lambda} = \mathsf{Ext}_\ell^{A \to A_1}(\rho'_{0,\lambda}), \quad \tau_{1,\lambda} = \mathsf{Ext}_\ell^{A \to A_1}(\rho'_{1,\lambda}).$$
```

Definition 4.2 (Pseudo-mixed States). A family of mixed states $\{\rho_\lambda\}_\lambda$ of $n(\lambda)$ qubits is called a pseudo-mixed state family if the following conditions hold:

Efficient Generation: There exists a QPT algorithm G that, on input 1^λ for integer λ, outputs the mixed state ρ_λ.

Entropy Gap: $S(\rho_\lambda) < n(\lambda) - 1/\mathrm{poly}(\lambda)$.

Computational Indistinguishability: For any QPT adversary $\mathcal{A}$,

$$\left|\Pr[\mathcal{A}(1^\lambda, \rho_\lambda) = 1] - \Pr[\mathcal{A}(1^\lambda, I/2^{n(\lambda)}) = 1]\right| \leq \mathrm{negl}(\lambda).$$

Definition 4.3 (Non-uniform pseudo-mixed states)**.** A family of mixed states $\{\rho_{\lambda,a}\}_\lambda$ of $n(\lambda)$ qubits is a non-uniform pseudo-mixed state family if it satisfies the condition of Definition 4.2 with the only change that the state generation algorithm G takes an additional advice string a as input. The length of the string a is called the advice size of the pseudo-mixed state.

Our main theorem concerning pseudo-mixed states is the following:

Theorem 4.2. *The existence of* EFI *implies the existence of non-uniform pseudo-mixed states with advice size $O(\log \lambda)$.*

As established by Theorem 4.1, EFI implies entropic EFI, so it suffices to prove Theorem 4.3.

Theorem 4.3. *The construction in Algorithm 2 is a secure non-uniform* PMS *with advice size $O(\log \lambda)$.*

Proof of Theorem 4.3. We will show that the construction in Algorithm 2 is a secure PMS in case that $a(\lambda)$ is a $1/m(\lambda)$ of $S(\rho_{1,\lambda})$, i.e., $(a(\lambda)-1)/m(\lambda) < S(\rho_{1,\lambda}) \leq a(\lambda)/m(\lambda)$

We consider a large number of copies of the state both to amplify the entropy gap and to better approximate the min-entropy with von Neumann entropy. According to Corollary 3.1, we have that

$$S(\rho'_{0,\lambda}) = m(\lambda)S(\rho_{0,\lambda}) \leq S(\rho'_{1,\lambda}) - \lambda^2 n^2(\lambda)p(\lambda).$$

From Corollary 3.1, we have that

$$\begin{aligned} H_{\min}^{\varepsilon/12}(\rho'_{1,\lambda}) &\geq S(\rho'_{1,\lambda}) - O\left(n(\lambda)\sqrt{\log(1/\varepsilon)m(\lambda)}\right) \\ &= S(\rho'_{1,\lambda}) - O\left(\lambda^{1.5}n^2(\lambda)p(\lambda)\right). \end{aligned}$$

We proceed to show that $\tau_{0,\lambda}$ forms a pseudo-mixed state of $\log|L| + \ell$ qubits.

Efficient Generation Since we can prepare $m(\lambda)$ copies of $\rho_{0,\lambda}$ and apply the unitary U_r in polynomial time, $\tau_{0,\lambda}$ can be prepared efficiently.

Entropy Gap Define states $\rho^{(j)} = U_j \rho'_{0,\lambda} U_j^\dagger$. By the subadditivity of von Neumann entropy, we have

$$\begin{aligned} S(A_1)_{\rho^{(j)}} &\leq S(A)_{\rho^{(j)}} + S(A_2)_{\rho^{(j)}} \\ &\leq S(\rho'_{0,\lambda}) + \log|A_2| \\ &\leq S(\rho'_{1,\lambda}) - \lambda^2 n^2(\lambda)p(\lambda) + (n'(\lambda) - \ell(\lambda)) \\ &\leq a(\lambda) - \lambda^2 n^2(\lambda)p(\lambda) + (n'(\lambda) - \ell(\lambda)). \end{aligned}$$

Together with the definition of ℓ, this proves that for all j

$$S(A_1)_{\rho^{(j)}} \leq \ell(\lambda) - \Omega(\lambda^2 n^2(\lambda)p(\lambda)).$$

We can compute the entropy of $\tau_{0,\lambda}$ as

$$\begin{aligned} S(\tau_{0,\lambda}) &= \log|L| + \frac{1}{|L|}\sum_{j\in L} S\left(\mathrm{Tr}_{A_2}\left[U_j\rho'_{0,\lambda}U_j^\dagger\right]\right) \\ &\leq \log|L| + \frac{1}{|L|}\sum_{j} S(A_1)_{\rho^{(j)}} \\ &\leq \log|L| + \ell(\lambda) - \Omega(\lambda^2 n^2(\lambda)p(\lambda)), \end{aligned}$$

which has a non-negligible gap with the entropy of the $(\log|L|+\ell)$-qubit maximally mixed state.

Computational Indistinguishability Notice that the smoothed min entropy of $\rho'_{1,\lambda}$ satisfies

$$H_{\min}^{\varepsilon/12}(\rho'_{1,\lambda}) \geq S(\rho'_{1,\lambda}) - O\left(\lambda^{1.5}n^2(\lambda)p(\lambda)\right) \geq k(\lambda).$$

By the definition of $(k,\varepsilon,\varepsilon/12)$-strong extractor, we have $D\left(\tau_{1,\lambda}, \frac{I_L}{|L|}\otimes\frac{I_{A_1}}{|A_1|}\right) \leq \varepsilon$, where $\log|A_1| = \ell$. By our parameter choice $\varepsilon = 2^{-\lambda}$, it follows that $\tau_{1,\lambda}$ and $\frac{I_L}{|L|}\otimes\frac{I_{A_1}}{|A_1|}$ are statistically indistinguishable.

By Definition 3.4, $\rho_{0,\lambda}$ and $\rho_{1,\lambda}$ are computationally indistinguishable. A standard hybrid argument shows that $\rho'_{0,\lambda} \approx_c \rho'_{1,\lambda}$ and thus $\tau_{0,\lambda} \approx_c \tau_{1,\lambda}$. Therefore, $\tau_{0,\lambda} \approx_c \frac{I_L}{|L|}\otimes\frac{I_{A_1}}{|A_1|}$, yielding our pseudo-mixed state.

Our construction relies on knowing an estimate $a(\lambda)/m(\lambda)$ of the von Neumann entropy of our entropic EFI state $\rho_{1,\lambda}$. To address this, we introduce non-uniformity and take $a(\lambda)$ as advice, which can be represented by a bit string of length $O(\log\lambda)$. □

Remark. Actually, we have constructed a special type of imbalanced EFI defined in [KT24]. We can show that if $\log|A_1| \leq \frac{n+H_{\min}^{\varepsilon/12}(\rho'_{1,\lambda})}{2} - \lambda$, the state $\tau_{0,\lambda}$ should be computationally indistinguishable from $\frac{I_L}{|L|}\otimes\frac{I_{A_1}}{|A_1|}$; while if $\log|A_1| \geq \frac{n+S(\rho'_{0,\lambda})}{2} + 1/\mathrm{poly}(\lambda)$, we can show that $S(\tau_\lambda) \leq \log|L| + \log|A_1| - 1/\mathrm{poly}(\lambda)$.

5 Single-copy pseudorandom states from pseudo-mixed states

In this section, we show how to construct 1PRS from a pseudo-mixed state. If the pseudo-mixed state is non-uniform, then so is the resulting 1PRS.

Assume $\{\rho_\lambda\}_\lambda$ is a family of pseudo-mixed states on system A. By applying the tensoring method to amplify the gap if necessary, we can assume without loss of generality that ρ_λ is an $n(\lambda)$-qubit state with entropy $S(\rho_\lambda) < n(\lambda) - 1$.

To construct single-copy pseudorandom states that are pure, a natural approach is to consider the purification $|\Psi_\lambda\rangle_{AB}$ of the state ρ_λ, such that $\mathrm{Tr}_B(|\Psi_\lambda\rangle\langle\Psi_\lambda|) = \rho_\lambda$. Assume without loss of generality that system B consists of $n'(\lambda) \geq n(\lambda)$ qubits. Then the state $|\Psi_\lambda\rangle_{AB}$ is computationally indistinguishable from the maximally mixed state on system A, but there is no guarantee regarding system B.

To make the system B also indistinguishable from the maximally mixed state, we apply the quantum extractor to the system $B = B_1B_2$, treating the system A as the environment. We use the Clifford group, a unitary 2-design, as the quantum extractor, and use a quantum one-time pad on the subsystem B_2 to effectively trace out B_2 when the keys are sampled uniformly at random:

$$|\phi_k\rangle = \Big(I_A \otimes ((I_{B_1} \otimes (X^{\alpha} Z^{\beta})_{B_2}) C_B)\, |\Psi_\lambda\rangle_{AB}\Big) \otimes |C\rangle_L$$

where the key $k = C \parallel \alpha \parallel \beta$, C ranges over all Clifford gates on B, B_1 consists of ℓ qubits, and $\alpha, \beta \in \{0,1\}^{n'-\ell}$ are the quantum one-time pad keys on the $n' - \ell$ qubits of B_2 for some ℓ to be chosen later.

The goal is to show that our extractor makes the subsystem B indistinguishable from the maximally mixed state while using a short key. However, notice that the quantum strong extractor works on states with low min-entropy, but a pseudo-mixed state only has a low von Neumann entropy, rather than a low min-entropy. Thus, we must consider a sufficiently large number m of copies of ρ_λ so that the min-entropy and von Neumann entropy are close asymptotically. The complete construction is provided in Algorithm 3.

Algorithm 3 Construction of 1PRS from pseudo-mixed states

```
Require: Inputs $1^\lambda$, $k \in \{0,1\}^{r(\lambda)}$.
Let $G$ be the generation algorithm for a pseudo-mixed states family $\{\rho_\lambda\}_\lambda$ of entropy gap at least 1.
Obtain from $G$ a circuit $V_\lambda$ that prepares a purification $|\Psi_\lambda\rangle_{AB}$ of $\rho_\lambda$. Let the number of qubits of $A$ be $n$ and the number of qubits of $B$ be $n'$. Without loss of generality, we assume that $n' \geq n$.
Pick $m = 50(n')^2\lambda$, $\ell = (n' - n)m/2 + 1$.
Parse $k$ as $C \parallel \alpha \parallel \beta$ where $C$ is a Clifford gate over $B^m$, and $\alpha, \beta \in \{0,1\}^{n'm-\ell}$.
Let $B^m = B_1 B_2$ where $B_1$ consists of the first $\ell$ qubits of $B^m$.
Output state
    $$|\phi_k\rangle = \Big(I_{A^m} \otimes ((I_{B_1} \otimes (X^{\alpha} Z^{\beta})_{B_2}) C_{B^m})(V_\lambda |0^{n+n'}\rangle_{AB})^{\otimes m}\Big) \otimes |C\rangle_L .$$
```

Theorem 5.1. *Assuming that pseudo-mixed states family exists, then* 1PRS *exists.*

Proof. We prove that the procedure in Algorithm 3 constructs 1PRS.

We first establish that the construction in Algorithm 3 possesses a non-trivial stretch property. Let L denote the set of Clifford gates over B^m of mn' qubits. The key k has length $r = 2(n'm - \ell) + \log|L|$. The state $|\phi_k\rangle$ consists of $(n + n')m + \log|L|$ qubits. Therefore, the stretch is

$$(n - n')m + 2\ell = 2.$$

Next, we show that $\mathbb{E}_k\left[|\phi_k\rangle\langle\phi_k|\right]$ is computationally indistinguishable from the maximally mixed state on the system $A^m B^m L$. By the properties of the quantum one-time pad, we have

$$\underset{k}{\mathbb{E}}\left[|\phi_k\rangle\langle\phi_k|\right] = \underset{C}{\mathbb{E}}\left[|C\rangle\langle C|_L \otimes \mathrm{Tr}_{B_2}\Big(C_{B^m} |\Psi_\lambda\rangle\langle\Psi_\lambda|^{\otimes m} C^{\dagger}_{B^m}\Big)\right] \otimes \frac{I_{B_2}}{|B_2|}.$$

It therefore suffices to prove that

$$\underset{C}{\mathbb{E}}\left[|C\rangle\langle C|_L \otimes \mathrm{Tr}_{B_2}\Big(C_{B^m} |\Psi_\lambda\rangle\langle\Psi_\lambda|^{\otimes m} C^{\dagger}_{B^m}\Big)\right] \tag{4}$$

is computationally indistinguishable from the maximally mixed state on LA^mB_1.

Define $\sigma = |\Psi_\lambda\rangle\langle\Psi_\lambda|^{\otimes m}$. Equation (4) can be written as $\mathsf{Ext}_\ell^{B^m}(\sigma)$.

Recall that $\mathrm{Tr}_{B^m}(\sigma) = \left(\rho_\lambda^{\otimes m}\right)_{A^m}$, which, by standard hybrid argument, is computationally indistinguishable with the maximally mixed state on A^m. By Theorem 3.3, we have that

$$\mathsf{Ext}_\ell^{B^m}(\sigma) \approx_s \frac{I_L}{|L|} \otimes \frac{I_{B_1}}{|B_1|} \otimes (\rho_\lambda^{\otimes m})_{A^m} \approx_c \frac{I_L}{|L|} \otimes \frac{I_{B_1}}{|B_1|} \otimes \frac{I_{A^m}}{|A^m|},$$

as long as there exists $\varepsilon = \mathrm{negl}(\lambda)$ such that

$$\ell \leq \frac{mn' + H_{\min}^{\varepsilon/12}(B^m|A^m)_\sigma}{2} - \log(1/\varepsilon). \tag{5}$$

It remains to prove inequality 5.

Let $\varepsilon = 2^{-\lambda}$. We apply Corollary 3.1 to bound the smoothed conditional min entropy of the state σ. Since $m \geq 5 \log \frac{1}{\varepsilon}$, we have that

$$\begin{aligned} H_{\min}^{\varepsilon/12}(B^m|A^m)_\sigma &\geq mS(B|A)_{|\Psi_\lambda\rangle} - 6n'\sqrt{(\lambda+4)m} \\ &= -\, mS(\rho_\lambda) - 6n'\sqrt{(\lambda+4)m} \\ &\geq m(1-n) - 6n'\sqrt{(\lambda+4)m}. \end{aligned}$$

A direct calculation shows that

$$\begin{aligned} &\frac{mn' + H_{\min}^{\varepsilon/12}(B^m|A^m)_\sigma}{2} - \log(1/\varepsilon) \\ \geq\, &\frac{m(n'-n)}{2} + \frac{m - 6n'\sqrt{(\lambda+4)m} - 2\lambda}{2} \\ \geq\, &\ell \end{aligned}$$

for large λ, which concludes the proof. □

Theorem 5.2. *Assuming that non-uniform pseudo-mixed states family with advice size $s(\lambda)$ exists, then non-uniform* 1PRS *with advice size $s(\lambda)$ exists.*

Proof. In the non-uniform setting, we provide Algorithm 3 with the same advice as that of the non-uniform pseudo-mixed states family. Using this advice, the algorithm can generate the corresponding circuits for producing the pseudo-mixed states. The rest of the proof then follows without modification. □

Theorem 5.3. *Assuming that* EFI *exists, then non-uniform* 1PRS *with advice size $O(\log \lambda)$ exists.*

Proof. Assuming that EFI exists, by Theorem 4.2, there exist non-uniform pseudo-mixed states with advice size $O(\log \lambda)$. Then by Theorem 5.2, there exists non-uniform 1PRS with advice size $O(\log \lambda)$. □

Corollary 5.1. *Assuming the existence of* EFI*, there exists non-uniform* 1PRS *of $n(\lambda)$ qubits with advice size $O(\log \lambda)$ such that the stretch is at least $\sqrt{n(\lambda)}$.*

Proof. Assuming the existence of EFI, by Theorem 5.3, there exists non-uniform $\mathsf{1PRS}$ $\{|\phi_k\rangle\}$ with advice size $O(\log\lambda)$. Denote the number of qubits as $n'(\lambda)$.

We can construct another non-uniform $\mathsf{1PRS}$ with the same advice size by parallel repetition: $|\Phi_K\rangle = |\phi_{k_1}\rangle\,|\phi_{k_2}\rangle \cdots |\phi_{k_{n'(\lambda)}}\rangle$, where $K = k_1 \parallel k_2 \parallel \cdots \parallel k_{n'(\lambda)}$. Let $n(\lambda) = n'^2(\lambda)$. It is clear that $\{|\Phi_K\rangle\}$ is a n-qubit state that can be generated with an advice of size $O(\log\lambda)$ and that it is a non-uniform $\mathsf{1PRS}$ of $n(\lambda)$ qubits whose stretch is at least $\sqrt{n(\lambda)}$, which concludes the proof. □

6 A natural universal EFI

In cryptography, it is sometimes possible to have universal constructions of a cryptographic primitive, meaning that it is secure as long as such primitives exist. For example, a universal one-way function is known to exist as an early result in the field [Lev87]. Such universal constructions are of theoretical importance and often reveal the essential reason and understanding of the corresponding primitive. In this section, we prove the existence of a weak form of universal EFI as an interesting corollary of the construction of non-uniform $\mathsf{1PRS}$ from EFI proved in the previous section.

Theorem 6.1. *The following are equivalent:*

1. EFI *exists.*
2. *There exist (efficiently computable) functions* $T(\lambda) = \mathrm{poly}(\lambda)$, $n(\lambda) = \mathrm{poly}(\lambda)$, $r(\lambda) = n - \omega(\log n)$, $\varepsilon = \mathrm{negl}(\lambda)$, $\delta = 1 - \Omega(\frac{1}{\lambda})$ *such that the pair* $\left(\{\rho_r^T\}, \{\frac{1}{2^n}I\}\right)$ *is an* (ε,δ)*-weak* EFI*, where* $\rho_r^T = \frac{1}{2^r}\sum_{|P|\le r} |\psi_P^T\rangle\langle\psi_P^T|$*, and* $|\psi_P^T\rangle$ *is the* n*-qubit state output by program* P *in time at most* T *(if the number of output qubits exceeds* n*, abort; if the output state* $|\psi_P\rangle$ *has* $k < n$ *qubits, replace it with* $|\psi_P\rangle\,|0^{n-k}\rangle$*).*[7]

Proof. Suppose there exists r, T, ε, and δ as in 2 such that ρ_r^T and $\frac{1}{2^n}I$ is an (ε,δ)-weak EFI pair, then, by Theorem 3.1, an EFI pair also exists.

Assume that EFI exist, then, by Theorem 5.3, there exists a non-uniform $\mathsf{1PRS}$ with $\log(n)$-size advice, say m-to-n Gen_λ where $\lambda \in [n]$ is the advice. For any $k \in \{0,1\}^m$ and $\lambda \in [n]$, $\mathsf{Gen}_\lambda\,|k\rangle$ can be generated by a Turing machine with size $m + \log n + C$, where C is a constant. Thus for $r = m + \log n + C$, and T be the running time of Gen, we can view ρ_r^T as sampling a state from the non-uniform $\mathsf{1PRS}$ with probability $\Omega(\frac{1}{n})$, and sampling from some other state with the remaining probability. Thus, any adversary can distinguish ρ_r^T from $\frac{1}{2^n}I$ with advantage at most $1 - \Omega(\frac{1}{n}) + \mathrm{negl}$, and they are $(1 - 2^{r-n})$-statistically far (since the entropy of ρ_r^T is bounded by r, while the entropy of $\frac{1}{2^n}I$ is n). Thus, the pair $\left(\{\rho_r^T\}, \{\frac{1}{2^n}I\}\right)$ is an (ε,δ)-weak EFI pair, for $\varepsilon = \mathrm{negl}(n)$, and $\delta = 1 - \Omega(\frac{1}{n})$. □

7 Equivalence with GapH hardness

In this section, we characterize EFI with the hardness of estimating the robust Gács' complexity. The proof goes in three steps. In Subsection 7.1, we show the entropy gap for the

[7] Some care needs to be taken to ensure that this output is an n-qubit pure state. If a program, outputs a state that is longer than n qubits we can output some canonical state such as $|0\rangle^{\otimes n}$. If a program outputs a state that may be mixed, there are ways to check if the output is far from pure, for instance by doing two runs of the program, and performing a swap test on their outputs. If a program output a state that is noticeably mixed, we can again output a canonical state. Finally, programs that output fewer than n qubits can be padded with $|0\rangle$'s.

mixture of high and low complexity states. In Subsection 7.2, we show how to extract randomness from the mixture of high complexity states. And then in Subsection 7.3, we put pieces together and propose an algorithm for estimating the non-uniform GapH problem.

7.1 Quantum algorithmic information

Lemma 7.1 (Mixtures over low-complexity states are approximately low-entropy)**.** *For any family of states $\{|\psi_k\rangle\}$ such that for all k, $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi_k\rangle) \leq r$, the mixed state $\mathbb{E}_k |\psi_k\rangle\langle\psi_k|$ is $\sqrt{2\varepsilon}$-close to a state with von Neumann entropy at most r.*

Proof. Let $\boldsymbol{\mu} = \sum_i \mu_i |\phi_i\rangle\langle\phi_i|$ be the spectral decomposition of the universal density matrix $\boldsymbol{\mu}$. Define Π_{low} to be the projection onto the span of low complexity eigenstates $|\phi_i\rangle$ of $\boldsymbol{\mu}$ with eigenvalue μ_i at least 2^{-r}, and Π_{high} to be the projection onto the span of high complexity eigenstates, i.e. those with eigenvalue less than 2^{-r}. Since $\boldsymbol{\mu}$ has trace at most 1, the number of μ_i's at least 2^{-r} is at most 2^r, and therefore the low-complexity space defined by Π_{low} has dimension at most 2^r.

For any state $|\psi\rangle$, define $|\psi_{\text{high}}\rangle = \Pi_{\text{high}} |\psi\rangle / \|\Pi_{\text{high}} |\psi\rangle\|$ and $|\psi_{\text{low}}\rangle = \Pi_{\text{low}} |\psi\rangle / \|\Pi_{\text{low}} |\psi\rangle\|$.

We first show that for any state $|\psi\rangle$ satisfying $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \leq r$, the trace distance between $|\psi\rangle$ and $|\psi_{\text{low}}\rangle$ is at most $\sqrt{2\varepsilon}$. To establish this, observe that

$$D(|\psi\rangle, |\psi_{\text{high}}\rangle) = \sqrt{1 - |\langle\psi|\psi_{\text{high}}\rangle|^2} = \|\Pi_{\text{low}} |\psi\rangle\|.$$

If $\|\Pi_{\text{low}} |\psi\rangle\| \leq 1-\varepsilon$, then by the definition of $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle)$, we would have

$$\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \geq \underline{\mathsf{H}}(|\psi_{\text{high}}\rangle) > r,$$

since $|\psi_{\text{high}}\rangle$ is $(1-\varepsilon)$-close to $|\psi\rangle$ and has $\underline{\mathsf{H}}$-complexity greater than r. This contradicts the assumption that $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \leq r$.

Therefore, it must be that $\|\Pi_{\text{low}} |\psi\rangle\| > 1-\varepsilon$. Consequently,

$$D(|\psi\rangle, |\psi_{\text{low}}\rangle) = \sqrt{1 - \|\Pi_{\text{low}} |\psi\rangle\|^2} < \sqrt{1-(1-\varepsilon)^2} < \sqrt{2\varepsilon}.$$

Next, we apply the result from the first step to $|\psi_k\rangle$, since it holds that $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi_k\rangle) \leq r$. This implies that, for all k, $D(|\psi_k\rangle, |\psi_{k,\text{low}}\rangle) < \sqrt{2\varepsilon}$. By Lemma 3.2, $\mathbb{E}_k |\psi_k\rangle\langle\psi_k|$ is $\sqrt{2\varepsilon}$-close to $\mathbb{E}_k |\psi_{k,\text{low}}\rangle\langle\psi_{k,\text{low}}|$. Since $\mathbb{E}_k |\psi_{k,\text{low}}\rangle\langle\psi_{k,\text{low}}|$ is supported on the low-complexity subspace Π_{low}, a linear subspace of dimension at most 2^r, its von Neumann entropy is at most r. □

Lemma 7.2. *Let $\rho = \sum \alpha_i |\varphi_i\rangle\langle\varphi_i|$ be a density matrix with its eigenvalue decomposition. Let $\tilde{\Pi}_{\text{low}}$ be the projector of subspace spanned by $|\varphi_i\rangle$ with $\alpha_i \geq 2^{-s}$. If $\mathrm{Tr}(\tilde{\Pi}_{\text{low}}\rho) \leq \varepsilon$, then we have $H^{2\varepsilon}_{\min}(\rho) \geq s + \log(1-\varepsilon)$.*

Proof. Let $p := \mathrm{Tr}(\tilde{\Pi}_{\text{low}}\rho) \leq \varepsilon$, and $\tilde{\rho} := (I - \tilde{\Pi}_{\text{low}})\rho(I - \tilde{\Pi}_{\text{low}}), \hat{\rho} := \frac{\tilde{\rho}}{1-p}$, then we have

$$\|\hat{\rho}\| \leq \frac{2^{-s}}{1-p} \leq \frac{2^{-s}}{1-\varepsilon},$$

so

$$H_{\min}(\hat{\rho}) \geq s + \log(1-\varepsilon)$$

Also

$$\|\rho - \hat{\rho}\| \leq \|\rho - \tilde{\rho}\| + \|\tilde{\rho} - \hat{\rho}\| = p + p = 2p \leq 2\varepsilon,$$

so $\hat{\rho}$ lies within trace distance 2ε of ρ, so we have $H^{2\varepsilon}_{\min}(\rho) \geq s + \log(1-\varepsilon)$ □

Lemma 7.3 (Mixtures over high complexity states are approximately high min-entropy)**.** *For any (not necessarily efficiently) samplable state family* $|\psi_k\rangle$ *such that* $\forall k : \underline{\mathsf{H}}^0(|\psi_k\rangle) \geq s$*, there exists a constant* C *such that for any* $\Gamma > \log n + C$*, the mixed state* $\rho = \mathbb{E}_k |\psi_k\rangle\langle\psi_k|$ *is* $2^{-\Gamma+\log n+C}$*-close to a state with min-entropy at least* $s - \Gamma$*.*

Proof. Let $\rho = \sum_i \beta_i |\varphi_i\rangle\langle\varphi_i|$ be the spectral decomposition of ρ. We prove the lemma by showing that removing the large eigenvalues does not significantly change the state. Let $\tilde{\Pi}_{\text{low}}$ be the projection onto the subspace spanned by $|\varphi_i\rangle$ with $\beta_i \geq 2^{\Gamma-s-1}$. Each of these eigenvectors of ρ has a short program of length at most $s-\Gamma+\log n+c$ for some constant c. That is, for all such $|\varphi_i\rangle$, $\mathsf{K}_{\mathsf{net}}(\varphi_i) \leq s - \Gamma + \log n + c$. Thus, we can write $\boldsymbol{\mu} = \sum_i 2^{-\mathsf{K}_{\mathsf{net}}(|\varphi_i\rangle)} |\varphi_i\rangle\langle\varphi_i| + \boldsymbol{\mu}'$, where $\boldsymbol{\mu}'$ is a semi-density matrix representing the remaining part of $\boldsymbol{\mu}$, and the sum is only over the eigenvectors of ρ corresponding to $\tilde{\Pi}_{\text{low}}$. Then, we have

$$\begin{aligned}\boldsymbol{\mu} &= \sum_i 2^{-\mathsf{K}_{\mathsf{net}}(|\varphi_i\rangle)} |\varphi_i\rangle\langle\varphi_i| + \boldsymbol{\mu}' \\ &\geq \sum_i 2^{-\mathsf{K}_{\mathsf{net}}(|\varphi_i\rangle)} |\varphi_i\rangle\langle\varphi_i| \\ &\geq 2^{-(s-\Gamma+\log n+c)} \sum_i |\varphi_i\rangle\langle\varphi_i| \\ &= 2^{-(s-\Gamma+\log n+c)}\, \tilde{\Pi}_{\text{low}}\,. \end{aligned} \tag{6}$$

Now, for any state $|\psi\rangle$ with $\underline{\mathsf{H}}^0(|\psi\rangle) \geq s$, we have $\langle\psi|\boldsymbol{\mu}|\psi\rangle \leq 2^{-s}$. So, it follows from Eq. (6) that

$$\langle\psi|\tilde{\Pi}_{\text{low}}|\psi\rangle \leq 2^{s-\Gamma+\log n+c} \langle\psi|\boldsymbol{\mu}|\psi\rangle \leq 2^{-\Gamma+\log n+c},$$

and, as a result,

$$\mathrm{Tr}(\tilde{\Pi}_{\text{low}}\rho) = \mathop{\mathbb{E}}_k \langle\psi_k|\tilde{\Pi}_{\text{low}}|\psi_k\rangle \leq 2^{-\Gamma+\log n+c}. \tag{7}$$

According to Lemma 7.2, set $\varepsilon = 2^{-\Gamma+\log n+c}$, we have

$$H_{\min}^{2\varepsilon}(\rho) \geq s - \Gamma + 1 - \log(1-\varepsilon) \geq s - \Gamma$$

As long as $\varepsilon \leq 1/2$ (this is the case in case that $\Gamma > \log n + C$). Choose $C = c + 1$ to be the constant in the lemma statement, then we have $H_{\min}^{2^{-\Gamma+\log n+C}}(\rho) \geq s - \Gamma$. □

Lemma 7.4. *For any state* $|\psi\rangle$ *and* $\varepsilon \in [0,1)$*, we have* $H^{1-\varepsilon}(|\psi\rangle) \leq \mathsf{K}_{\mathsf{net}}(|\psi\rangle) + \log\frac{1}{\varepsilon}$*.*

Proof. By the definition of $\boldsymbol{\mu}$ we know that for all $|\psi\rangle$,

$$\boldsymbol{\mu} = 2^{-\mathsf{K}_{\mathsf{net}}(|\psi\rangle)} |\psi\rangle\langle\psi| + \boldsymbol{\mu}' \geq 2^{-\mathsf{K}_{\mathsf{net}}(|\psi\rangle)} |\psi\rangle \langle\psi|\,,$$

where $\boldsymbol{\mu}'$ is the residual part of the universal density matrix.

Recall that $\underline{\mathsf{H}}^0$ is defined as $\underline{\mathsf{H}}^0(|\psi'\rangle) = \langle\psi'|\boldsymbol{\mu}|\psi'\rangle$. So in case that $|\langle\psi|\psi'\rangle|^2 \geq \varepsilon$ then we have

$$\langle\psi'|\boldsymbol{\mu}|\psi'\rangle \geq \varepsilon \langle\psi|\boldsymbol{\mu}|\psi\rangle \geq \varepsilon 2^{\mathsf{K}_{\mathsf{net}}(|\psi\rangle)},$$

and $\underline{\mathsf{H}}^0(|\psi'\rangle) \leq -\log(\varepsilon 2^{\mathsf{K}_{\mathsf{net}}(|\psi\rangle)}) = \mathsf{K}_{\mathsf{net}}(|\psi\rangle) + \log 1/\varepsilon$. □

7.2 Extraction

Lemma 7.5. *Let ρ be a mixed state over an n-qubit system A. Let A_1 be a subsystem of A with ℓ qubits, and let A_2 be the remaining $n-l$ qubits. Let $\mathsf{Ext}_\ell^{A\to A_1}$ be an extractor on A mapping states on A to A_1 by applying a unitary 2-design $\{U_j\}_{j\in L}$. Define $\rho' = \mathsf{Ext}_\ell^{A\to A_1}(\rho)\otimes \frac{I_{A_2}}{|A_2|}$. Then for any Δ, the following holds:*

- *If $S(\rho)\le 2\ell - n - \Delta$, then $S(\rho')\le n+\log|L|-\Delta$.*
- *If $H_{\min}(\rho)\ge 2\ell-n+\Delta$, then ρ' is $2^{-\Delta/2}$-close to $\frac{I_A}{|A|}\otimes\frac{I_L}{|L|}$.*

Proof. For the first statement, we write

$$\begin{aligned}\rho' &= \mathsf{Ext}_\ell^{A\to A_1}(\rho)\otimes\frac{I_{A_2}}{|A_2|}\\ &= \frac{1}{L}\sum_{j\in L}|j\rangle\langle j|_L\otimes \mathrm{Tr}_{A_2}(U_j\rho U_j^\dagger)\otimes\frac{I_{A_2}}{|A_2|}.\end{aligned}$$

Define $\rho_A^{(j)} = U_j\rho U_j^\dagger$. Noticing that ρ' is a cq-state, we have

$$S(\rho')\le \log|L| + n - \ell + \max_j S(\rho_{A_1}^{(j)}), \tag{8}$$

where $\rho_{A_1}^{(j)} = \mathrm{Tr}_{A_2}\,\rho_A^{(j)}$ is the reduced density matrix of $\rho_A^{(j)}$ on A_1. Using subadditivity of the von Neumann entropy, $S(A_1)\le S(A_2)+S(A)$, we have for all j

$$\begin{aligned}S(\rho_{A_1}^{(j)}) &\le S(\rho_{A_2}^{(j)}) + S(\rho_A^{(j)})\\ &\le (n-\ell) + (2\ell - n - \Delta)\\ &= \ell - \Delta.\end{aligned}$$

Together with the bound in Eq. (8), this proves the first statement.

The second statement is a direct application of Theorem 3.3 by taking $\varepsilon = 2^{-\Delta/2}$. Since $H_{\min}^{\varepsilon/12}(\rho)\ge H_{\min}(\rho)\ge 2\ell-n+\Delta$, the theorem guarantees that the number of qubits that one can extract is at least

$$\frac{n+(2\ell-n+\Delta)}{2} - \log(1/\varepsilon) = \ell.$$

Thus, by Theorem 3.3, we have

$$\begin{aligned}D\left(\rho',\frac{I_A}{|A|}\otimes\frac{I_L}{|L|}\right) &= D\left(\mathsf{Ext}_\ell^A(\rho)\otimes\frac{I_{A_2}}{|A_2|},\frac{I_A}{|A|}\otimes\frac{I_L}{|L|}\right)\\ &\le \varepsilon = 2^{-\Delta/2}.\end{aligned}$$

□

7.3 Putting the pieces together

Theorem 7.1. *The following two statements are equivalent:*

- *EFI exists.*
- *There exists a non-uniform family of efficiently samplable states $\{|\psi_k\rangle\}$, efficiently computable functions $r\in[n(\lambda)], \Delta=\omega(\log\lambda)$, and a universal constant $\varepsilon<\frac{1}{100}$, such that $\mathsf{GapH}^\varepsilon(r,r+\Delta)$ is non-uniformly hard on average over $\{|\psi_k\rangle\}$.*

Algorithm 4 Algorithm for solving $\mathsf{GapH}[r, r+\Delta]$

```
Require: A single-copy input state $|\psi_k\rangle \in \mathcal{H}_A$.
Let $\rho = \mathbb{E}_k |\psi_k\rangle\langle\psi_k|$, and let $\ell = (n + r + \Delta/2)/2$.
Let $\Pi$ be the projector that distinguishes $\mathsf{Ext}_\ell^{A\to A_1}(\rho)$ from the maximally mixed state,
    where $A_1$ is the first $\ell$ qubits of system $A$.
Test the projector $\Pi$ on $\mathsf{Ext}_\ell^{A\to A_1}(|\psi_k\rangle\langle\psi_k|)$.
If the test passes report low, otherwise report high.
```

Proof. First, assuming EFI exists, we prove that the GapH problem for some non-uniform state family is hard on average. By the existence of EFI and Corollary 5.1, there exists a non-uniform $n(\lambda)$-qubit 1PRS family $\{|\phi_{k'}\rangle\}$ where the advice a has size $O(\log\lambda)$ and the stretch is at least $\sqrt{n(\lambda)}$ (i.e. the seed is of length at most $n(\lambda) - \sqrt{n(\lambda)}$)

Define $k = b \parallel k' \parallel j$ with $j \in \{0,1\}^n$ and $b \in \{0,1\}$. Consider the non-uniform state family $|\psi_k\rangle$ defined as

$$|\psi_k\rangle = \begin{cases} |\phi_{k'}\rangle & \text{if } \ b = 0, \\ |j\rangle & \text{otherwise.} \end{cases} \tag{9}$$

We will show that this state family is a hard instance of GapH.

When $b = 0$, the state $|\psi_k\rangle$ is $|\phi_{k'}\rangle$, and thus it can be described by a program of size at most $n(\lambda) - \sqrt{n(\lambda)} + O(\log\lambda) + C$ for some constant C, i.e. $\mathsf{K}^0_{\mathsf{net}}(|\psi_k\rangle) \le n(\lambda) - \sqrt{n(\lambda)} + O(\log\lambda) + C$. Hence, by Lemma 7.4, the state has low $\underline{\mathsf{H}}^{1-\epsilon}$ complexity: $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi_k\rangle) \le \mathsf{K}^0_{\mathsf{net}}(|\psi_k\rangle) + \log(1/\varepsilon) \le n(\lambda) - \sqrt{n(\lambda)} + O(\log\lambda) + C + \log(1/\varepsilon)$. On the other hand, when $b = 1$, the state $|\psi_k\rangle$ is $|j\rangle$ for a uniformly random $j \in \{0,1\}^n$. Since $\sum_j \langle j|\boldsymbol{\mu}|j\rangle \le \mathrm{Tr}(\boldsymbol{\mu}) \le 1$, we have for all $\delta > 0$

$$\Pr_{j\in\{0,1\}^n}[\langle j|\boldsymbol{\mu}|j\rangle \ge 2^{-n(\lambda)+\delta}] \le 2^{-\delta}.$$

Taking, for example, $\delta = \sqrt{n(\lambda)}/2$, the state has high $\underline{\mathsf{H}}$ complexity with high probability:

$$\Pr_{j\in\{0,1\}^n}[\underline{\mathsf{H}}(|j\rangle) > n(\lambda) - \delta] \ge 1 - 2^{-\delta} = 1 - \mathrm{negl}(\lambda). \tag{10}$$

Choose $r = n(\lambda) - \sqrt{n(\lambda)} + O(\log\lambda) + C + \log(1/\varepsilon)$ and $r + \Delta = n(\lambda) - \delta$. We have $\Delta = \sqrt{n(\lambda)}/2 - O(\log\lambda) - C - \log(1/\varepsilon) = \omega(\log\lambda)$. We claim that if there is an adversary $\mathcal{A}$ that solves the GapH for this non-uniform family, the same adversary breaks the 1PRS $\{|\phi_{k'}\rangle\}$.

Define events C_{low} and C_{high} $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi_k\rangle) \le r$ and $\underline{\mathsf{H}}(|\psi_k\rangle) \ge r + \Delta$ over the random key k, representing the complexity of the state being low and high respectively. Define events A_{low} and A_{high} for $\mathcal{A}$ outputting 0 and 1 on input $|\psi_{k,a}\rangle$. The discussion above indicates that $\Pr[C_{\text{low}}|b = 0] = 1$ and $\Pr[C_{\text{high}}|b = 0] > 1 - \mathrm{negl}(\lambda)$. Under these two condition, we can easily show that for all possible events A,

$$|\Pr[A \wedge b = 0] - \Pr[A \wedge C_{\text{low}}]| \le \mathrm{negl}(\lambda),$$
$$|\Pr[A \wedge b = 1] - \Pr[A \wedge C_{\text{high}}]| \le \mathrm{negl}(\lambda).$$

By the linearity of quantum operations,

$$\begin{aligned}\Pr[\mathcal{A}(1^\lambda, \mathbb{E}_{k'} |\phi_{k'}\rangle\langle\phi_{k'}|) = 0] &= \Pr_{k'}[\mathcal{A}(1^\lambda, |\phi_{k'}\rangle\langle\phi_{k'}|) = 0] \\ &= \Pr_{k:b=0}[\mathcal{A}(1^\lambda, |\phi_k\rangle\langle\phi_k|) = 0] \\ &= \Pr_k[A_{\text{low}}|b = 0] \\ &= 1 - \Pr_k[A_{\text{high}}|b = 0] \\ &= 1 - 2\Pr_k[A_{\text{high}} \wedge b = 0]\end{aligned}$$

On the other hand,

$$\begin{aligned}\Pr\left[\mathcal{A}\Big(1^\lambda, \frac{I}{2^n}\Big) = 0\right] &= \Pr_{k:b=1}[\mathcal{A}(1^\lambda, |\phi_k\rangle\langle\phi_k|) = 0] \\ &= \Pr_k[A_{\text{low}}|b = 1] \\ &= 2\Pr_k[A_{\text{low}} \wedge b = 1]\end{aligned}$$

So when the failure probability of $\mathcal{A}$ for the GapH problem is at most $\frac{1}{2} - \frac{1}{\lambda^c}$ for some constant c, the advantage of $\mathcal{A}$ for the $\mathsf{1PRS}$ is bounded by

$$\begin{aligned}&\left|1 - 2\Big(\Pr_k[A_{\text{low}} \wedge b = 1] + \Pr_k[A_{\text{high}} \wedge b = 0]\Big)\right| \\ \geq\ &\left|1 - 2\Big(\Pr_k[A_{\text{low}} \wedge C_{\text{high}}] + \Pr_k[A_{\text{high}} \wedge C_{\text{low}}]\Big)\right| - \text{negl}(\lambda) \\ \geq\ &\frac{2}{\lambda^c} - \text{negl}(\lambda).\end{aligned}$$

That is, $\mathcal{A}$ breaks $\mathsf{1PRS}$ and therefore also EFI. This completes the proof for the direction that EFI implies the average hardness of GapH.

Next, we establish the converse direction by demonstrating that if no EFI exists, then non-uniform GapH can be solved efficiently. Define the subsets K_{high} and K_{low} of keys k as follows:

$$\begin{aligned}K_{\text{high}} &= \{k : \underline{\mathsf{H}}(|\psi_k\rangle) \geq r + \Delta\}, \\ K_{\text{low}} &= \{k : \underline{\mathsf{H}}^{1-\varepsilon}(|\psi_k\rangle) \leq r\}.\end{aligned}$$

Define the states

$$\begin{aligned}\rho_{\text{high}} &= \mathop{\mathbb{E}}_{k \in K_{\text{high}}} |\psi_k\rangle\langle\psi_k|\,, \\ \rho_{\text{low}} &= \mathop{\mathbb{E}}_{k \in K_{\text{low}}} |\psi_k\rangle\langle\psi_k|\,, \\ \rho_{\text{mid}} &= \mathop{\mathbb{E}}_{k \notin K_{\text{low}} \cup K_{\text{high}}} |\psi_k\rangle\langle\psi_k|\,.\end{aligned}$$

Then we can express

$$\rho = p_{\text{low}}\rho_{\text{low}} + p_{\text{mid}}\rho_{\text{mid}} + p_{\text{high}}\rho_{\text{high}}\,,$$

where p_{low}, p_{mid}, and p_{high} are the respective probabilities. We begin by examining a few simple cases. First, if

$$\Pr_k[\underline{\mathsf{H}}(|\psi_k\rangle) \geq r + \Delta] \leq \frac{1}{2} - \text{non-negl}(\lambda)$$

where non-negl(λ) is some non-negligible function, then one can always guess that the state has low complexity and obtain a non-negligible advantage. Thus, we assume without loss of generality that

$$p_{\mathrm{high}} = \Pr_k[\underline{\mathsf{H}}(|\psi_k\rangle) \geq r + \Delta] \geq \frac{1}{2} - \mathrm{negl}(\lambda). \tag{11}$$

Similarly, we may also assume

$$p_{\mathrm{low}} = \Pr_k[\underline{\mathsf{H}}^{1-\varepsilon}(|\psi_k\rangle) \leq r] \geq \frac{1}{2} - \mathrm{negl}(\lambda). \tag{12}$$

A direct consequence is that $p_{\mathrm{mid}} = \mathrm{negl}(\lambda)$.

Now, we use Algorithm 4 and prove that it will provide a non-negligible advantage in solving non-uniform GapH assuming EFI's do not exist. Note that all the parameters in Algorithm 4 is efficiently computable: $\ell = (n + r + \Delta/2)/2$ is efficiently computable as $r(\lambda)$ and $\Delta(\lambda)$ are effiiently computable functions. (Algorithm 4 is a uniform GapH estimator, but it can be also used for a non-uniform GapH estimation by replacing the EFI distinguisher with the non-uniform distinguisher) Define $\ell = (n + r + \Delta/2)/2$ as in the algorithm. Applying the extractor Ext_ℓ to ρ, we have

$$\mathsf{Ext}_\ell(\rho) = p_{\mathrm{low}}\mathsf{Ext}_\ell(\rho_{\mathrm{low}}) + p_{\mathrm{mid}}\mathsf{Ext}_\ell(\rho_{\mathrm{mid}}) + p_{\mathrm{high}}\mathsf{Ext}_\ell(\rho_{\mathrm{high}}).$$

By Lemma 7.1, we know that ρ_{low} is $\sqrt{2\varepsilon}$-close to a state of von Neumann entropy at most $r = 2\ell - n - \Delta/2$. We denote this state by ρ'_{low}. By the first part of Lemma 7.5, we have $S(\mathsf{Ext}_\ell(\rho'_{\mathrm{low}})) \leq n + \log|L| - \Delta/2$. This implies that

$$D(\mathsf{Ext}_\ell(\rho'_{\mathrm{low}}), \pi) \geq 1 - 2^{-\Delta/2}.$$

By the triangle inequality, it follows that

$$D(\mathsf{Ext}_\ell(\rho_{\mathrm{low}}), \pi) \geq 1 - 2^{-\Delta/2} - \sqrt{2\varepsilon},$$

where $\pi = \frac{I_L}{|L|} \otimes \frac{I_{A_1}}{|A_1|}$ is the maximally mixed state.

Taking $\Gamma = \Delta/4$ in Lemma 7.3, we have that ρ_{high} is $2^{-\Delta/4+\log n+C}$-close to a state with min-entropy at least $r+\Delta-\Gamma = r+3\Delta/4$. Let this state be ρ'_{high}. By Lemma 7.5, $\mathsf{Ext}_\ell(\rho'_{\mathrm{high}})$ is $2^{-\Delta/8}$-close to the maximally mixed state π. By the triangle inequality, we have

$$D(\mathsf{Ext}_\ell(\rho_{\mathrm{high}}), \pi) \leq 2^{-\Delta/4+\log n+C} + 2^{-\Delta/8} = \mathrm{negl}(\lambda). \tag{13}$$

So, we can conclude that

$$D(\mathsf{Ext}_\ell(\rho), \pi) > 1/2 - \sqrt{2\varepsilon} - \mathrm{negl}(\lambda) > 1/4$$

when $\varepsilon < 1/100$. As a result, the two states $\mathsf{Ext}_\ell(\rho)$ and π are statistically far and efficiently samplable pairs. According to the non-existence of EFI, there exists a projector Π that can distinguish these two with non-negligible probability. In more detail,

$$\mathrm{Tr}(\Pi\,\mathsf{Ext}_\ell(\rho)) - \mathrm{Tr}(\Pi\,\pi) = p(\lambda)$$

for some non-negligible probability $p(\lambda)$. From Eq. (13), it follows that

$$\mathrm{Tr}(\Pi\,\mathsf{Ext}_\ell(\rho)) - \mathrm{Tr}(\Pi\,\mathsf{Ext}_\ell(\rho_{\mathrm{high}})) \geq p(\lambda) - \mathrm{negl}(\lambda). \tag{14}$$

By Eqs. (11) and (12), we have

$$D\Big(\mathsf{Ext}_\ell(\rho), \frac{1}{2}\mathsf{Ext}_\ell(\rho_{\text{low}}) + \frac{1}{2}\mathsf{Ext}_\ell(\rho_{\text{high}})\Big) \le \operatorname{negl}(\lambda).$$

Using this in Eq. (14), we have

$$\operatorname{Tr}(\Pi\, \mathsf{Ext}_\ell(\rho_{\text{low}})) - \operatorname{Tr}(\Pi\, \mathsf{Ext}_\ell(\rho_{\text{high}})) \ge 2p(\lambda) - \operatorname{negl}(\lambda),$$

which is also non-negligible. Thus Π provides non-negligible advantage in estimating GapH given only a single copy of $|\psi_k\rangle$. □

In the previous theorem we build the equivalence of non-uniform hardness of GapH. The uniform harness of GapH in turn is a characterization of $\mathsf{1PRS}$.

Corollary 7.1. *The following two statements are equivalent:*

- $\mathsf{1PRS}$ *exists.*
- *There exists a uniform family of efficiently samplable states $\{|\psi_k\rangle\}$, a universal constant $\varepsilon < 1/100$, and $\Delta = \omega(\log \lambda)$ such that* GapH *is hard over $\{|\psi_k\rangle\}$.*

Proof. In case that $\mathsf{1PRS}$ exist, then define the same state family as in Theorem 7.1. Then we can define a uniform state family on which $\mathsf{GapH}^\varepsilon[r, r+\Delta]$ for some function r and $\Delta = \omega(\log n)$.

On the other hand, in case that $\mathsf{1PRS}$ do not exist, then as the proof of Theorem 5.3 implicitly shows that pseudo-mixed states are equivalent to $\mathsf{1PRS}$, we can conclude that pseudo-mixed states do not exist. Then we can apply Algorithm 4 (as pseudo-mixed states do not exist, we can distinguish mixed states from the maximally mixed state efficiently), which provides a non-negligible advantage for estimating GapH. □

8 Equivalence with GapU hardness

In this section, we obtain a characterization of EFI analogous to that of Section 7, but using U instead of $\underline{\mathsf{H}}$. In particular, we build up equivalence of EFI with the hardness of GapU (Definition 3.16). The proof goes in the same way as Section 7: first we show that the complexity gap implies the entropy gap. Then we extract the entropy from the state with quantum extractors and apply Algorithm 4 to estimate the complexity.

Lemma 8.1 (Mixture over low-complexity states is approximately low-entropy for U)**.** *For any family of states $\{|\psi_k\rangle\}$ such that for all k, $\mathsf{U}(|\psi_k\rangle) \le r$, the mixed state $\mathbb{E}_k\, |\psi_k\rangle\langle\psi_k|$ is $2^{-\Gamma/2}$-close to a state with von Neumann entropy at most $r + \Gamma$.*

Proof. Consider the spectral decomposition $\boldsymbol{\mu} = \sum_i \mu_i\, |\phi_i\rangle\langle\phi_i|$ of $\boldsymbol{\mu}$. Let Π_{low} be the projection onto the subspace spanned by the low-complexity eigenvectors $|\phi_i\rangle$ with eigenvalues $\mu_i \ge 2^{-r-\Gamma}$ and let $\Pi_{\text{high}} = I - \Pi_{\text{low}}$. For any state $|\psi\rangle$ satisfying $\mathsf{U}(|\psi\rangle) \le r$, we write

$$|\psi\rangle = \Pi_{\text{low}}\, |\psi\rangle + \Pi_{\text{high}}\, |\psi\rangle\,.$$

By the condition $\mathsf{U}(|\psi\rangle) \le r$, we have $\langle\psi|\boldsymbol{\mu}^{-1}|\psi\rangle \le 2^r$. Using $\langle\psi|\Pi_{\text{low}}\boldsymbol{\mu}^{-1}\Pi_{\text{high}}|\psi\rangle = 0$ and $\langle\psi|\Pi_{\text{high}}\boldsymbol{\mu}^{-1}\Pi_{\text{low}}|\psi\rangle = 0$, we obtain

$$\begin{aligned}
2^{r+\Gamma}\, \langle\psi|\Pi_{\text{high}}|\psi\rangle &\le \langle\psi|\Pi_{\text{high}}\boldsymbol{\mu}^{-1}\Pi_{\text{high}}|\psi\rangle \\
&\le \langle\psi|\Pi_{\text{low}}\boldsymbol{\mu}^{-1}\Pi_{\text{low}}|\psi\rangle + \langle\psi|\Pi_{\text{high}}\boldsymbol{\mu}^{-1}\Pi_{\text{high}}|\psi\rangle \\
&= \langle\psi|\boldsymbol{\mu}^{-1}|\psi\rangle \\
&\le 2^r.
\end{aligned}$$

Thus, for all k, $\langle\psi_k|\Pi_{\mathrm{high}}|\psi_k\rangle \le 2^{-\Gamma}$. Define $|\psi_{k,\mathrm{low}}\rangle = \Pi_{\mathrm{low}}|\psi_k\rangle / \|\Pi_{\mathrm{low}}|\psi_k\rangle\|$, we have

$$D(|\psi_k\rangle, |\psi_{k,\mathrm{low}}\rangle) \le \|\Pi_{\mathrm{high}}|\psi_k\rangle\| \le 2^{-\Gamma/2}.$$

It follows from Lemma 3.2 that

$$D\Big(\mathop{\mathbb{E}}_{k} |\psi_k\rangle\langle\psi_k|, \mathop{\mathbb{E}}_{k} |\psi_{k,\mathrm{low}}\rangle\langle\psi_{k,\mathrm{low}}|\Big) \le 2^{-\Gamma/2},$$

which completes the proof by noting that $\mathbb{E}_k |\psi_{k,\mathrm{low}}\rangle\langle\psi_{k,\mathrm{low}}|$ is supported on Π_{low} of dimension $2^{r+\Gamma}$ and has entropy at most $r+\Gamma$. □

Lemma 8.2 (Mixture over high complexity states is approximately high min-entropy for U)**.** *For any (not necessarily efficiently) samplable state family $|\psi_k\rangle$ such that $\forall k: \mathsf{U}^{1-\varepsilon}(|\psi_k\rangle) > s$, then there is constant C such that the mixed state $\rho = \mathbb{E}_k |\psi_k\rangle\langle\psi_k|$ is 2ε-close to a state with min-entropy at least $s - \log n - C$.*

Proof. Consider the spectral decomposition of $\rho = \sum_i \beta_i |\varphi_i\rangle\langle\varphi_i|$. Let c be the length of the program describing the sampling algorithm for $|\psi_k\rangle$. Let $\tilde{\Pi}_{\mathrm{low}}$ be the projection onto the span of eigenvectors $|\varphi_i\rangle$ with corresponding eigenvalue $\beta_i \ge 2^{-(s-\log n - c)}$. All such vectors can be indexed by programs of length at most $(s-\log n - c) + \log n + c = s$ and therefore have $\mathsf{K}_{\mathsf{net}}(|\varphi_i\rangle) \le s$. Thus, we can write $\boldsymbol{\mu} = \sum_i 2^{-\mathsf{K}_{\mathsf{net}}(|\varphi_i\rangle)} |\varphi_i\rangle\langle\varphi_i| + \boldsymbol{\mu}'$ for some positive semi-definite $\boldsymbol{\mu}'$. From this, we have $\boldsymbol{\mu} \ge 2^{-s}\tilde{\Pi}_{\mathrm{low}}$ and, by Lemma 3.8, for any state $|\psi\rangle$ in the space that Π_{good} projects onto, $\mathsf{U}(|\psi\rangle) \le s$.

For any state $|\psi\rangle$, define $|\psi_{\mathrm{low}}\rangle = \tilde{\Pi}_{\mathrm{low}}|\psi\rangle / \left\|\tilde{\Pi}_{\mathrm{low}}|\psi\rangle\right\|$. When $\left\|\tilde{\Pi}_{\mathrm{low}}|\psi\rangle\right\| \le 1-\varepsilon$, we have $D(|\psi\rangle, |\psi_{\mathrm{low}}\rangle) = \left\|\tilde{\Pi}_{\mathrm{low}}|\psi\rangle\right\| \le 1-\varepsilon$. So we have $\mathsf{U}^{1-\varepsilon}(|\psi\rangle) \le s$ as $|\psi_{\mathrm{low}}\rangle$ is in the space $\tilde{\Pi}_{\mathrm{low}}$ projects onto. Thus for any $\mathsf{U}^{1-\varepsilon}(|\psi\rangle) > s$, we have $\left\|\tilde{\Pi}_{\mathrm{low}}|\psi\rangle\right\| > 1-\varepsilon$ and consequently

$$\langle\psi|\tilde{\Pi}_{\mathrm{low}}|\psi\rangle < 1-(1-\varepsilon)^2 \le 2\varepsilon.$$

Using the condition $\mathsf{U}^{1-\varepsilon}(|\psi_k\rangle) > s$ for all k, we have $\mathrm{Tr}(\Pi_{\mathrm{good}}\, \mathbb{E}_k |\psi_k\rangle\langle\psi_k|) < 2\varepsilon$.

Define projection $\tilde{\Pi}_{\mathrm{high}} = I - \tilde{\Pi}_{\mathrm{low}}$ and state $\rho' = \frac{\tilde{\Pi}_{\mathrm{high}}\rho\tilde{\Pi}_{\mathrm{high}}}{\mathrm{Tr}(\tilde{\Pi}_{\mathrm{high}}\rho\tilde{\Pi}_{\mathrm{high}})}$. We have $D(\rho,\rho') = \mathrm{Tr}(\tilde{\Pi}_{\mathrm{low}}\rho) < 2\varepsilon$. Any eigenvalue of ρ' is bounded above by $2^{-s+\log n+c}/(1-2^{-s+\log n+c}) \le 2^{-s+\log n+c+1}$. Taking $C = c+1$ completes the proof. □

We are now ready to prove that the average-case hardness of estimating U is equivalent to the existence of EFI.

Theorem 8.1. *The following two statements are equivalent:*

- EFI *exists.*
- *There exists a non-uniform family of states $\{|\psi_k\rangle\}$ such that* $\mathsf{GapU}[r, r+\Delta]$ *is hard on average.*

Proof. The proof is similar to that of Theorem 7.1 and we only outline the differences.

We first prove that the existence of EFI implies the hardness of GapU for a non-uniform family of states. We use the same construction in Eq. (9). Now define events C_{low} and C_{high} to be $\mathsf{U}(|\psi_k\rangle) \le r$ and $\mathsf{U}^{1-\varepsilon}(|\psi_k\rangle) \ge r+\Delta$ over the random keys. Define events A_{low} and A_{high} be the events that the algorithm $\mathcal{A}$ for GapU outputs 0 and 1 respectively. As in the proof of Theorem 7.1, we prove that $\Pr[C_{\mathrm{low}}|b=0] = 1$. That is, when the state is sampled from the 1PRS family $\{|\phi_{k'}\rangle\}$, we have by Lemma 3.9, $\mathsf{U}(|\psi_k\rangle) \leq \mathsf{K}_{\mathsf{net}}(|\psi_k\rangle) \leq n(\lambda) - \sqrt{n(\lambda)} + O(\log \lambda) + C$. Similarly, we can prove $\Pr[C_{\text{high}} | b = 1] = 1 - \text{negl}(\lambda)$. When $b = 1$, the state is a random computational basis state $|j\rangle$ of n qubits, and by Eq. (10) and Lemma 3.10, we have

$$\Pr_{j\in\{0,1\}^n}[\mathsf{U}^{1-\varepsilon}(|j\rangle) \geq n(\lambda) - \delta + \log \varepsilon] \geq \Pr_{j\in\{0,1\}^n}[\underline{\mathsf{H}}(|j\rangle) \geq n(\lambda) - \delta] \geq 1 - 2^{-\delta}.$$

Choosing $r = n(\lambda) - \sqrt{n(\lambda)} + O(\log \lambda) + C$ and $r + \Delta = n(\lambda) - \delta + \log \varepsilon$, a similar argument as in the rest of the proof of Theorem 7.1 shows that $\mathcal{A}$ also breaks EFI.

Next, assume that EFI does not exist. We can prove, for any state family $\{|\psi_k\rangle\}$, there exists an algorithm that solves $\mathsf{GapU}(r, r + \Delta)$ efficiently. The proof is essentially the same as that for $\mathsf{U}^{1-\varepsilon}$ and U^0 in place of $\underline{\mathsf{H}}^0$ and $\underline{\mathsf{H}}^{1-\varepsilon}$, respectively, and using Lemmas 8.1 and 8.2 in place of Lemmas 7.1 and 7.3. We omit the details. □

9 Equivalence with the hardness of identifying the "span of easy states"

We now give a different characterization of EFIs, showing that they are equivalent to the hardness of deciding if a state is in the span of states of low $\mathsf{K}_{\mathsf{net}}$ complexity. We then introduce a notion of "robust span" of states, and briefly sketch how this can give a unified perspective into the proofs of Sections 7 and 8.

9.1 Characterization of EFI from the hardness of identifying the "span of easy states"

In this section, we characterize EFI with the hardness of learning whether a state in the span of easy states or not. We will denote Π_r as the span of states with $\mathsf{K}_{\mathsf{net}}$ at most r.

Remark. The definition of Π_r is not robust over choice of the universal gate set: different choice of the gate set would correspond to different sets of easy states, and different sets of easy states (even with a very little deviation) have different spans. According to Solovay-Kitaev, universal gate set can simulate any state up to arbitrary precision, but the span of two states might differ significantly even if two state families are very close to each other. For example, span of $\{|0\rangle, |0\rangle\}$ is one-dimensional, and span of $\{|0\rangle, \sqrt{1 - 2^{-2n}}\, |0\rangle + 2^{-n}\, |1\rangle\}$ is two-dimensional, albeit these two states are almost identical. But we will see that the non-robustness does not matter a lot for our arguments.

We'll need lemma on the entropy bound related to Π_r.

Lemma 9.1. *For any family of states $\{|\psi_k\rangle\}$ such that $|\psi_k\rangle$ lies in Π_r for all k, the mixed state $\mathbb{E}_k\, |\psi_k\rangle\langle\psi_k|$ has von Neumann entropy at most $r + 1$.*

Proof. As Π_r is spanned by states with $\mathsf{K}_{\mathsf{net}}$ at most r, and there are at most $2^{r+1} - 1$ such states, the dimension of Π_r is at most $2^{r+1} - 1$. Since $\mathbb{E}_k\, |\psi_k\rangle\langle\psi_k|$ is a state supported in Π_r, its entropy is at most $\log(2^{r+1} - 1) < r + 1$. □

Lemma 9.2. *For any efficiently family of states $\{|\psi_k\rangle\}$ such that $\langle\psi_k|\Pi_s|\psi_k\rangle \leq \varepsilon$ for all k, the mixed state $\mathbb{E}_k\, |\psi_k\rangle\langle\psi_k|$ is 2ε-close to a state with min-entropy at least $s - \Gamma$ for any $\Gamma = \omega(\log n)$.*

Proof. According to the same argument as in Lemma 7.3, we can define $\tilde{\Pi}_{\text{low}}$ as the eigenstates $|\varphi_i\rangle$ of $\rho = \mathbb{E}_k |\psi_k\rangle\langle\psi_k|$ with eigenvalues $\beta_i \geq 2^{\Gamma-s-1}$. Then all such states can be encoded with the index of eigenstates in the decreasing order of eigenvalues, so $\mathsf{K}_{\mathsf{net}}(|\varphi_i\rangle) \leq s - \Gamma + 1 + O(\log n) < s$, and thus $\tilde{\Pi}_{\text{low}}$ is a subspace contained in Π_s. As a result, we have $\langle\psi_k|\tilde{\Pi}_{\text{low}}|\psi_k\rangle \leq \langle\psi_k|\Pi_s|\psi_k\rangle \leq \varepsilon$ for all k, so $\text{Tr}(\tilde{\Pi}_{\text{low}}\rho) = \mathbb{E}_k \langle\psi_k|\tilde{\Pi}_{\text{low}}|\psi_k\rangle \leq \varepsilon$. Now, according to Lemma 7.2, we have

$$H_{\min}^{2\varepsilon}(\rho) \geq s - \Gamma + 1 + \log(1-\varepsilon) \geq s - \Gamma.$$

So we can conclude that ρ is 2ε-close to a state with min-entropy at least $s - \Gamma$. □

Theorem 9.1. EFI *exists if and only if there exists a non-uniform family of efficiently samplable states* $\{|\psi_k\rangle\}$*, efficiently computable functions* $r \in [n(\lambda)], \Delta = \omega(\log \lambda)$*, and* $\varepsilon < 1/100$ *such that it is non-uniformly hard to distinguish the following two cases given a single copy of a state from the family (sampled uniformly at random over* k*):*

- *The states lies in* Π_r
- *The overlap of the state with* $\Pi_{r+\Delta}$ *is at most* ε*.*

Proof. First, assuming EFI exists, we consider the same state family as in Theorem 7.1. When $b = 0$, the state can be described by a program of size at most $n(\lambda) - \sqrt{n(\lambda)} + O(\log \lambda) + C$ for some constant C, i.e.. $\mathsf{K}_{\mathsf{net}}(|\psi_k\rangle) \leq n(\lambda) - \sqrt{n(\lambda)} + O(\log \lambda) + C$. Hence, the state has low $\mathsf{K}_{\mathsf{net}}$ complexity and lies in $\Pi_{n-\Delta}$ for $r = n - \sqrt{n} + O(\log n) + C$. On the other hand, when $b = 1$, the state $|\psi_k\rangle$ is $|j\rangle$ for a uniformly random $j \in \{0,1\}^n$. Let $\Delta = n - \sqrt{n}/2 - r$, then $r + \Delta = n - \sqrt{n}/2$. Since $\sum_j \langle j|\Pi_{n-\sqrt{n}/2}|j\rangle = \text{Tr}\,\Pi_{n-2\sqrt{n}/3} \leq 2^{n-2\sqrt{n}/3}$, we obtain from Markov's inequality:

$$\Pr_{j\in\{0,1\}^n}[\langle j|\Pi|j\rangle \geq 2^{-\sqrt{n}/3}] \leq 2^{-\sqrt{n}/3} = \text{negl}(\lambda).$$

This means that the state has little overlap with $\Pi_{r+\Delta} = \Pi_{n-2\sqrt{n}/3}$ with high probability. Thus, with the same argument in Theorem 7.1, we conclude that $|\psi_k\rangle$ is a non-uniformly hard instance to decide whether it's in the span or not.

Second, assuming EFI does not exist, we can apply the algorithm as in Theorem 7.1. Note that the same randomness extractor works as we have the entropy bound from Lemma 9.2 and Lemma 9.1. □

Remark. If we replace the non-uniform family of states with a uniform family, we will build up a characterization of 1PRS. The argument goes in the same way as Corollary 7.1.

Remark. Here we adapt the strong version of promise: we require that the state lies exactly in Π_r. We can also adapt the robust version, modifying the requirement to be so that the state almost lies in the span of states.

9.2 Relating algorithmic entropy with the "*robust* span of easy states"

The definitions of $\underline{\mathsf{H}}$ and its robust version $\underline{\mathsf{H}}^{\varepsilon}$ are presented in Subsection 3.4, but arguably the intuition behind the definition of $\underline{\mathsf{H}}^{\varepsilon}$ is still vague. In this section, we relate $\underline{\mathsf{H}}$ with the robust span (we'll give the definition of the robust span later) of the easy states: if $\underline{\mathsf{H}}$ is low, then the state almost lies in the robust span of easy states; if $\underline{\mathsf{H}}$ is high, then the state almost lies in the complement of the robust span of easy states.

Definition 9.1. Let $\{|\psi_k\rangle\}_{k\in[L]}$ be a family of quantum sates. Then the *ε-robust span* of $\{|\psi_k\rangle\}$ is defined as the subspace spanned by eigenstates of $\frac{1}{L}\sum_{k\in[L]}|\psi_k\rangle\!\langle\psi_k|$ whose corresponding eigenvalues are at least $\frac{\varepsilon}{L}$.

Theorem 9.2 (High $\underline{\mathsf{H}}$ complexity implies low overlap with robust span of easy states)**.** *If a state $|\psi\rangle$ satisfies $\underline{\mathsf{H}}^0(|\psi\rangle) \geq r$ with $r \leq n$, and $\Pi_{r,\gamma}$ is the projector on the γ-robust span of states with $\mathsf{K}_{\mathsf{net}}$ at most $r-\Delta$, then we have $\langle\psi|\Pi_{r,\gamma}|\psi\rangle \leq \mathrm{poly}(n)\gamma^{-1}2^{-\Delta}$.*

Proof. We can bound r by the number of qubits of $|\psi\rangle$: as there is a universal upper bound on $\underline{\mathsf{H}}$ for any states: $\underline{\mathsf{H}}(|\psi\rangle) \leq n + O(\log n)$ for any n-qubit state $|\psi\rangle$, it follows that $r \leq n + O(\log n)$.

First, from the condition $\underline{\mathsf{H}}^0(|\psi\rangle) \geq r$ and the definition of $\underline{\mathsf{H}}$, we have $\underline{\mathsf{H}}^0(|\psi\rangle) = \underline{\mathsf{H}}(|\psi\rangle) = -\log\langle\psi|\boldsymbol{\mu}|\psi\rangle \geq r$, which implies $\langle\psi|\boldsymbol{\mu}|\psi\rangle \leq 2^{-r}$.

Then we relate $\boldsymbol{\mu}$ with the robust span $\Pi_{r,\gamma}$. By the definition of the universal semi-density matrix $\boldsymbol{\mu}$, we have that $\boldsymbol{\mu} \geq \sum_{|\phi\rangle} 2^{-\mathsf{K}_{\mathsf{net}}(|\phi\rangle)}|\phi\rangle\!\langle\phi| \geq 2^{-r+\Delta}\sum_{\mathsf{K}_{\mathsf{net}}(|\phi\rangle)\leq r-\Delta}|\phi\rangle\!\langle\phi|$. Although this appears to sum over uncountably many quantum states, it is actually a sum over a countable family: there are only countably many quantum states with finite $\mathsf{K}_{\mathsf{net}}$.

Let $\rho = \mathbb{E}_{\mathsf{K}_{\mathsf{net}}(|\phi\rangle)\leq r-\Delta}|\phi\rangle\!\langle\phi|$, where the expectation is taken uniformly at random over all the quantum states $|\phi\rangle$ with $\mathsf{K}_{\mathsf{net}}$ at most $r-\Delta$. Let L be the number of states with $\mathsf{K}_{\mathsf{net}}$ at most $r-\Delta$. Note that we have a lower bound of L: any states $|k\|0^{n-r+\Delta+O(\log n)}\rangle_{k\in\{0,1\}^{r-\Delta-O(\log n)}}$ can be encoded by a prefix-free Turing machine that outputs n and k (note that $r \leq n + O(\log n)$ so the argument holds), so there are at least $2^{r-\Delta-O(\log n)}$ different states with $\mathsf{K}_{\mathsf{net}}$ at most $r-\Delta$. As a result, we have

$$\boldsymbol{\mu} \geq 2^{-r+\Delta}\sum_{\mathsf{K}_{\mathsf{net}}(|\phi\rangle)\leq r-\Delta}|\phi\rangle\!\langle\phi| \geq 2^{-O(\log n)}\frac{1}{L}\sum_{\mathsf{K}_{\mathsf{net}}(|\phi\rangle)\leq r-\Delta}|\phi\rangle\!\langle\phi| = \frac{1}{\mathrm{poly}(n)}\rho.$$

Thus we can conclude that $\langle\psi|\rho|\psi\rangle \leq \mathrm{poly}(n)\langle\psi|\boldsymbol{\mu}|\psi\rangle \leq \mathrm{poly}(n)\cdot 2^{-r}$.

Let $\sum_i \lambda_i|\psi_i\rangle\!\langle\psi_i|$ be the eigendecomposition of ρ. The γ-robust span of ρ can be expressed as $\Pi_{r,\gamma} = \sum_{\lambda_i\geq\gamma/L}|\psi_i\rangle\!\langle\psi_i|$. Thus $\frac{\gamma}{L}\Pi_{r,\gamma} \leq \rho$, and we have $\langle\psi|\Pi_{r,\gamma}|\psi\rangle \leq \frac{L}{\gamma}\langle\psi|\rho|\psi\rangle \leq \frac{L}{\gamma}\mathrm{poly}(n)2^{-r} = \mathrm{poly}(n)\gamma^{-1}2^{-\Delta}$. □

Theorem 9.3 (Low $\underline{\mathsf{H}}$ complexity implies high overlap with robust span of easy states)**.** *If an n-qubit state $|\psi\rangle$ satisfies $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \leq r$, and $\Pi_{r,\gamma}$ is the projector of the γ-robust span of states with $\mathsf{K}_{\mathsf{net}}$ at least $r + O(\log n)$, then we have $\langle\psi|\Pi_{r,\gamma}|\psi\rangle \geq 1 - \sqrt{2\varepsilon} - \gamma\mathrm{poly}(n)$.*

Proof. Let $\sum_i \mu_i|\phi_i\rangle\!\langle\phi_i| = \boldsymbol{\mu}$ be the spectral decomposition of the universal density matrix $\boldsymbol{\mu}$. Define Π_{low} to be the projection onto the span of eigenstates $|\phi_i\rangle$ of $\boldsymbol{\mu}$ with eigenvalue $\mu_i \geq 2^{-r}$, and Π_{high} to be the projection onto the span of high complexity eigenstates, i.e. those with eigenvalue less than 2^{-r}. Since $\boldsymbol{\mu}$ has trace at most 1, the number of μ_i's at least 2^{-r} is at most 2^r, and therefore the low-complexity space defined by Π_{low} has dimension at most 2^r.

For any state $|\psi\rangle$, define $|\psi_{\mathrm{high}}\rangle = \Pi_{\mathrm{high}}|\psi\rangle/\|\Pi_{\mathrm{high}}|\psi\rangle\|$ and $|\psi_{\mathrm{low}}\rangle = \Pi_{\mathrm{low}}|\psi\rangle/\|\Pi_{\mathrm{low}}|\psi\rangle\|$.

We first show that for any state $|\psi\rangle$ satisfying $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \leq r$, the trace distance between $|\psi\rangle$ and $|\psi_{\mathrm{low}}\rangle$ is at most $\sqrt{2\varepsilon}$. To establish this, observe that

$$D(|\psi\rangle, |\psi_{\mathrm{high}}\rangle) = \sqrt{1 - |\langle\psi|\psi_{\mathrm{high}}\rangle|^2} = \|\Pi_{\mathrm{low}}|\psi\rangle\|.$$

If $\|\Pi_{\mathrm{low}}|\psi\rangle\| \leq 1-\varepsilon$, then by the definition of $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle)$, we would have

$$\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \geq \underline{\mathsf{H}}(|\psi_{\mathrm{high}}\rangle) > r,$$

since $|\psi_{\text{high}}\rangle$ is $(1-\varepsilon)$-close to $|\psi\rangle$ and has $\underline{\mathsf{H}}$-complexity greater than r. This contradicts the assumption that $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \leq r$.

Therefore, it must be that $\|\Pi_{\text{low}}\,|\psi\rangle\| > 1-\varepsilon$. Consequently,

$$D(|\psi\rangle\,, |\psi_{\text{low}}\rangle) = \sqrt{1 - \|\Pi_{\text{low}}\,|\psi\rangle\|^2} < \sqrt{1-(1-\varepsilon)^2} < \sqrt{2\varepsilon}.$$

Thus, $|\psi\rangle$ is $\sqrt{2\varepsilon}$-close to a state $|\psi_{\text{low}}\rangle$ lies in the projector Π_{low} where Π_{low} is the projector onto eigenstates of μ whose corresponding eigenvalues are at least 2^{-r}. These states can be encoded with Turing machine of size $r + O(\log n)$.[8]

Let $\rho = \mathbb{E}_{\mathsf{K}_{\text{net}}(|\phi\rangle)\leq r+O(\log n)} |\phi\rangle\langle\phi|$ be the uniform mixture of states with K_{net} at most $r + O(\log n)$. Then as all the eigenstates of Π_{low} have K_{net} at most $r+O(\log n)$, we can conclude that $\rho \geq \frac{1}{\text{poly}(n)} 2^{-r}\Pi_{\text{low}} \geq \frac{1}{\text{poly}(n)} 2^{-r}\, |\psi_{\text{low}}\rangle\langle\psi_{\text{low}}|$.

Let $\rho = \sum_i \lambda_i\, |\psi_i\rangle\langle\psi_i|$ be the eigendecomposition of ρ, and L be the number of states with K_{net} at most $r + O(\log n)$. Then the γ-robust span of ρ can be expressed as $\Pi_{r,\gamma} = \sum_{\lambda_i \geq \gamma/L} |\psi_i\rangle\langle\psi_i|$. Let $|\tilde{\psi}_{\text{low}}\rangle = \frac{(I-\Pi)|\psi_{\text{low}}\rangle}{\|(I-\Pi)|\psi_{\text{low}}\rangle\|}$, then as $|\tilde{\psi}_{\text{low}}\rangle$ lies in the subspace with spectrum bounded by $\frac{\gamma}{L}$, so $\langle\tilde{\psi}_{\text{low}}|\rho|\tilde{\psi}_{\text{low}}\rangle \leq \gamma/L$. But on the other hand, we have $\langle\tilde{\psi}_{\text{low}}|\rho|\tilde{\psi}_{\text{low}}\rangle \geq \frac{1}{\text{poly}(n)} 2^{-r} |\langle\tilde{\psi}_{\text{low}}|\psi_{\text{low}}\rangle\,|^2$, thus we can deduce that $|\langle\tilde{\psi}_{\text{low}}|\psi_{\text{low}}\rangle\,|^2 \leq \frac{\gamma}{L}\text{poly}(n)2^r \leq \gamma\text{poly}(n)$, where the last line follows from the fact that $L = 2^{r+O(\log n)}$.

So we have $\langle\psi_{\text{low}}|\Pi_{r,\gamma}|\psi_{\text{low}}\rangle = 1 - |(I-\Pi_{r,\gamma})\,|\psi_{\text{low}}\rangle\,|^2 = 1 - |\langle\psi_{\text{low}}|\tilde{\psi}_{\text{low}}\rangle\,|^2 \geq 1 - \gamma\text{poly}(n)$. Combined with $D(|\psi\rangle\langle\psi|\,, |\psi_{\text{low}}\rangle\langle\psi_{\text{low}}|) \leq \sqrt{2\varepsilon}$, we get that $\langle\psi|\Pi_{r,\gamma}|\psi\rangle \geq 1 - \gamma\text{poly}(n) - \sqrt{2\varepsilon}$. □

Theorem 9.4. *For any family of states $\{|\psi_k\rangle\}$ such that $\langle\psi_k|\Pi_{r,\gamma}|\psi_k\rangle \geq 1-\varepsilon$ for all k, where $\Pi_{r,\gamma}$ is the γ-robust span of the states with K_{net} at most r, then the mixed state $\mathbb{E}_k\,|\psi_k\rangle\langle\psi_k|$ is $\sqrt{\varepsilon}$-close to a state with von Neumann entropy at most r.*

Proof. We first show that any state $|\psi\rangle$ satisfying $\langle\psi|\Pi_{r,\gamma}|\psi\rangle \geq 1-\varepsilon$ is $\sqrt{\varepsilon}$-close to a pure state $|\tilde{\psi}\rangle$ which lies in the support of $\Pi_{r,\gamma}$. Indeed, let $|\tilde{\psi}\rangle = \frac{\Pi_{r,\gamma}|\psi\rangle}{\|\Pi_{r,\gamma}|\psi\rangle\|}$, then $\langle\psi|\tilde{\psi}\rangle = \frac{\|\Pi_{r,\gamma}|\psi\rangle^2\|}{\|\Pi_{r,\gamma}|\psi\rangle\|} = \sqrt{\langle\psi|\Pi_{r,\gamma}|\psi\rangle} \geq \sqrt{1-\varepsilon}$, and thus

$$\|\,|\psi\rangle\langle\psi| - |\tilde{\psi}\rangle\langle\tilde{\psi}|\,\| = \sqrt{1 - |\langle\psi|\tilde{\psi}\rangle\,|^2} \leq \sqrt{\varepsilon}.$$

Thus $\mathbb{E}_k\,|\psi_k\rangle\langle\psi_k|$ is $\sqrt{\varepsilon}$-close to $\mathbb{E}_k\,|\tilde{\psi}_k\rangle\langle\tilde{\psi}_k|$ with $|\tilde{\psi}_k\rangle$ lies in the support of $\Pi_{r,\gamma}$. But we know that $\Pi_{r,\gamma}$ is of dimension at most 2^r (because the rank of $\mathbb{E}_{\mathsf{K}_{\text{net}}(|\psi\rangle)\leq r}\,|\psi\rangle\langle\psi|$ is bounded by 2^r), so $\mathbb{E}_k\,|\tilde{\psi}_k\rangle\langle\tilde{\psi}_k|$ is of von Neumann entropy at most r. □

Theorem 9.5. *For any samplable family of states $\{|\psi_k\rangle\}$ such that $\langle\psi_k|\Pi_{r,\gamma}|\psi_k\rangle \leq \varepsilon$ where $\Pi_{r,\gamma}$ is the γ-robust span of the states with K_{net} at most s, the mixed state $\mathbb{E}_k\,|\psi_k\rangle\langle\psi_k|$ is ε-close to a state with min-entropy at least $s-\Gamma$ for some $\Gamma = \omega(\log n)$.*

Proof. Let $\rho = \sum_i \beta_i\,|\varphi_i\rangle\langle\varphi_i|$ be the spectral decomposition of ρ. We prove the lemma by showing that removing the large eigenvalues does not significantly change the state. Let $\tilde{\Pi}_{\text{low}}$ be the projection onto the subspace spanned by $|\varphi_i\rangle$ with $\beta_i \geq 2^{\Gamma-s-1}$. Each of these

[8] More precisely, we can encode the eigenstates of Π_{low} with a Turing machine of size $r+O(\log n)$ that can output a circuit that is 2^{-2^n}-close to the eigenstate. Such encoding can be implemented as, for example, the number of qubits and the index of the eigenstates. The double exponential error does not affect our result so we will ignore the error afterwards.

eigenvectors of ρ has a short program of length at most $s - \Gamma + O(\log n)$. That is, for all such $|\varphi_i\rangle$, we have $\mathsf{K}_{\mathsf{net}}(|\varphi_i\rangle) \leq s - \Gamma + O(\log n)$.

Now, for any state $|\psi\rangle$ with $\langle\psi|\Pi_{r,\gamma}|\psi\rangle \leq \varepsilon$, note that $\frac{1}{L}\tilde{\Pi}_{\text{low}} \leq \frac{1}{L}\sum_{\mathsf{K}_{\mathsf{net}}(|\psi\rangle)\leq s} |\psi\rangle\langle\psi| := \rho$, where L is the number of states with $\mathsf{K}_{\mathsf{net}}$ at most s. So

$$\begin{aligned}\langle\psi|\tilde{\Pi}_{\text{low}}|\psi\rangle &= \langle\psi|(I - \Pi_{r,\gamma})\tilde{\Pi}_{\text{low}}(I - \Pi_{r.\gamma})|\psi\rangle + \langle\psi|(I - \Pi_{r,\gamma})\tilde{\Pi}_{\text{low}}\Pi_{r.\gamma}|\psi\rangle \\ &\quad + \langle\psi|\Pi_{r,\gamma}\tilde{\Pi}_{\text{low}}(I - \Pi_{r.\gamma})|\psi\rangle + \langle\psi|\Pi_{r,\gamma}\tilde{\Pi}_{\text{low}}\Pi_{r.\gamma}|\psi\rangle \\ &\leq 3\sqrt{\varepsilon} + \langle\psi|(I - \Pi_{r,\gamma})\tilde{\Pi}_{\text{low}}(I - \Pi_{r,\gamma})|\psi\rangle \\ &= 3\sqrt{\varepsilon} + L\,\langle\psi|(I - \Pi_{r,\gamma})\rho(I - \Pi_{r.\gamma})|\psi\rangle \\ &\leq 3\sqrt{\varepsilon} + \gamma,\end{aligned}$$

where the second line is from the fact that $\|\Pi_{r,\gamma}\,|\psi\rangle\,\| \leq \sqrt{\varepsilon}$, and the last inequality is from the fact that $\|(I - \Pi_{r,\gamma})\rho(I - \Pi_{r,\gamma})\| \leq \gamma/L$. So as a result,

$$\mathrm{Tr}(\tilde{\Pi}_{\text{low}}\rho) = \mathop{\mathbb{E}}_{k}\langle\psi_k|\tilde{\Pi}_{\text{low}}|\psi_k\rangle \leq 3\sqrt{\varepsilon} + \gamma.$$

According to Lemma 7.2, we can conclude that $H_{\min}^{6\sqrt{\varepsilon}+2\gamma}(\rho) \geq s + \log(1 - 3\sqrt{\varepsilon} - \gamma) - \Gamma + 1 \geq s - \Gamma$. □

So one can write a new proof for Lemma 7.1 and Lemma 7.3 (probably with different bounds, but the bound will be negligible as long as the gap is $\omega(\log n)$): any state family with high $\underline{\mathsf{H}}$ will almost lies in the robust span according to Theorem 9.2, whose mixture has a high smoothed min-entropy according to Theorem 9.5. On the other hand, any state family with low $\underline{\mathsf{H}}^{1-\varepsilon}$ almost lies in the robust span according to Theorem 9.3, whose mixture have low robust von Neumann entropy according to Theorem 9.4.

10 Equivalence with hardness of state complexity over unkeyed state families

In Sections 7 and 8, the state families considered in the GapH and GapU problems are keyed-samplable, meaning that it is possible to output the state $|\psi_k\rangle$ given the key k as input. In this section, we show similar characterizations of EFI using the hardness of Kolmogorov complexity for single-copy samplable state families. As defined in Definition 3.3, a single-copy samplable state family is a family of key-state pairs $\{(k, |\psi_k\rangle)\}$ and a distribution on it which can be sampled by running a generation unitary G on two systems A and B and measuring A in the computational basis. System A holds the key k, and B holds the quantum state. This is more general than a keyed state family, as it is not guaranteed that the state $|\psi_k\rangle$ can be reproduced even given the key k. Such unkeyed state families are relevant in quantum cryptography for quantum money and quantum lightning. Our main result in this section is the following Theorem 10.1.

We need a variant of the GapH problem where in the high complexity case, the measure is also smoothed.

Definition 10.1 (The Double-GapH problem)**.** Let r, Δ, n be functions of λ. We define $\mathsf{Double\text{-}GapH}^{\varepsilon}(r, r + \Delta)$ as the following (promise) problem: given a *single* copy of a state $|\psi\rangle$ on some number n of qubits, decide whether

- $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \leq r$, or

- $\underline{\mathsf{H}}^{\varepsilon}(|\psi\rangle) \geq r + \Delta$.

Theorem 10.1. *The following two statements are equivalent:*

- EFI *exists.*
- *There exists a single-copy samplable family of states* $(\{|\psi_k\rangle\}, \{\mathcal{D}_n\})$ *(namely there exists a QPT algorithm that can sample* $|\psi_k\rangle$ *according to the distribution* $\mathcal{D}_n$*), an (inefficiently computable) function* $r(n) \in [n]$*, and efficient function* $\Delta(n) = \omega(\log(n))$ *such that* $\mathsf{Double\text{-}GapH}(r, r+\Delta)$ *is hard on average over* $\mathcal{D}_n$*.*

Remark. Note that in contrast to all other quantities the function r here is not necessarily efficiently computable. In our upcoming proof, the r will be the entropy of EFI, which does not necessarily have an efficient QPT algorithm. So this is also a non-uniform characterization of EFI.

Before proving the theorem, we first establish several useful lemmas.

Lemma 10.1. *For any (not necessarily efficiently) sampleable family of mixed states* $\{\rho_n\}$*, where* ρ_n *is an* n*-qubit mixed state, and for any pure state* $|\psi\rangle$ *in the support of* ρ_n *(namely there exists* $\varepsilon > 0$ *such that* $\varepsilon |\psi\rangle\langle\psi| \leq \rho_n$*), we have* $\mathsf{U}(|\psi\rangle) \leq H_{\max}(\rho_n) + \log n + C$ *for some constant* C*.*

Proof. Let r be the max-entropy of ρ_n, and let $\rho_n = \sum \lambda_i |\psi_i\rangle\langle\psi_i|$ be a spectral decomposition. As the max-entropy of ρ_n is r, there are at most 2^r different $|\psi_i\rangle$, so we can encode all these eigenstates with a program of size $r + \log n + C$ for some constant C dependent on the state generation algorithm. We can therefore bound the $\mathsf{K}^0_{\mathsf{net}}$ of all the eigenstates of ρ_n: $\mathsf{K}^0_{\mathsf{net}}(|\psi_i\rangle) \leq r + \log n + C$. So the projector $\Pi = \sum_i |\psi_i\rangle\langle\psi_i|$ spanned by the support of ρ_n can be bounded as $2^{-(r+\log n+C)}\Pi \leq \boldsymbol{\mu}$. As a result, any state $|\psi\rangle$ in the support of ρ_n also satisfies $2^{-(r+\log n+C)}|\psi\rangle\langle\psi| \leq 2^{-(r+\log n+C)}\Pi \leq \boldsymbol{\mu}$. By Lemma 3.8, we have $\mathsf{U}(\psi) \leq r + \log n + C$. □

Lemma 10.2. *For any (not necessarily efficiently) sampleable family of mixed states* $\{\rho_n\}$*, where* ρ_n *is an* n*-qubit mixed state, and for any pure state* $|\psi\rangle$ *in the support of* ρ_n *(namely there exists* $\delta > 0$ *such that* $\delta |\psi\rangle\langle\psi| \leq \rho_n$*), we have* $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi\rangle) \leq H_{\max}(\rho_n) + \log n + \log\frac{1}{\varepsilon} + C$ *for some constant* C*.*

Proof. It follows from Lemmas 3.10 and 10.1. □

Corollary 10.1. *For any (not necessarily efficiently) samplable family of mixed states* $\{\rho_n\}$*, where* ρ_n *is an* n*-qubit state, and for* $m \geq 36n^2\log^2 n$ *and any decomposition of* $\rho^{\otimes m} = \sum p_k |\psi_k\rangle\langle\psi_k|$ *we have that except with probability at most* $2^{-O(\log^2 n)}$ *over* $|\psi_k\rangle$ *with probability* p_k*,* $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi_k\rangle) \leq m(S(\rho)+1) + \log n + \log\frac{1}{2\varepsilon} + C$*.*

Proof. Using Corollary 3.1 with $\xi = 2^{-\log^2 n}$, we deduce that

$$H^{\xi}_{\max}(\rho^{\otimes m}) \leq m\Big(S(\rho) + 6n\sqrt{\frac{\log 1/\xi}{m}}\Big) < m(S(\rho)+1).$$

Thus, $\rho^{\otimes m}$ is ξ-close to a semi-density matrix ρ' with max-entropy at most $m(S(\rho)+1)$. Let Π be the projector onto the span of ρ'. Then we have

$$\begin{aligned}\frac{\Pi\rho^{\otimes m}\Pi}{\mathrm{Tr}(\Pi\rho^{\otimes m})} &= \frac{1}{\mathrm{Tr}(\Pi\rho^{\otimes m})}\sum_k p_k \Pi|\psi_k\rangle\langle\psi_k|\Pi \\ &= \sum_k p_k \frac{\|\Pi|\psi_k\rangle\|^2}{\mathrm{Tr}(\Pi\rho^{\otimes m})}\frac{\Pi|\psi_k\rangle}{\|\Pi|\psi_k\rangle\|}\frac{\langle\psi_k|\Pi}{\|\Pi|\psi_k\rangle\|}.\end{aligned} \tag{15}$$

This gives a decomposition of $\Pi\rho^{\otimes m}\Pi$ composed of states $\frac{\Pi|\psi_k\rangle}{\|\Pi|\psi_k\rangle\|}$. Therefore, by Lemma 10.2, we have $\underline{\mathsf{H}}^{1-2\varepsilon}\left(\frac{\Pi|\psi_k\rangle}{\|\Pi|\psi_k\rangle\|}\right) \leq r + \log n + C + \log\frac{1}{2\varepsilon}$ for any $|\psi_k\rangle$.

And we know that $\operatorname{Tr}\Pi\rho = \sum p_k \langle\psi_k|\Pi|\psi_k\rangle \geq 1 - D(\rho,\rho') = 1 - 2^{-\log^2 n}$, so except for negligible probability, we have that $\|\Pi|\psi_k\rangle\|^2 \geq 1-\varepsilon^2$ and

$$D\Big(|\psi_k\rangle, \frac{\Pi|\psi_k\rangle}{\|\Pi|\psi_k\rangle\|}\Big) = \sqrt{1-\|\Pi|\psi_k\rangle\|^2} \leq \varepsilon.$$

Therefore, except for negligible probability, $\underline{\mathsf{H}}^{1-\varepsilon}(|\psi_k\rangle) \leq m(S(\rho)+1) + \log n + \log\frac{1}{2\varepsilon} + C$. □

Lemma 10.3. *For any $\delta > 0$, any state ensemble $\{(p_k, |\psi_k\rangle)\}$ of n-qubit states, and $\rho = \sum_k p_k |\psi_k\rangle\!\langle\psi_k|$, we have $\underline{\mathsf{H}}^0(|\psi_k\rangle) \geq H_{\min}(\rho) - \delta$ with probability at least $2^{-\delta}$ over $|\psi_k\rangle$.*

Proof. Let $H_{\min}(\rho) = r$; then we have $\rho \leq 2^{-r} I$. Consequently,

$$\sum p_k \langle\psi_k|\boldsymbol{\mu}|\psi_k\rangle = \operatorname{Tr}(\boldsymbol{\mu}\rho) \leq 2^{-r}\operatorname{Tr}(\boldsymbol{\mu}) \leq 2^{-r}.$$

Thus, by Markov's inequality, with probability at least $1-2^{-\delta}$ over the choice of $|\psi_k\rangle$, $\langle\psi_k|\boldsymbol{\mu}|\psi_k\rangle \leq 2^{-r+\delta}$. In other words, $\underline{\mathsf{H}}^0(|\psi_k\rangle) \geq r - \delta$ with probability at least $1-2^{-\delta}$. □

Corollary 10.2. *For any n-qubit state ρ and any $m \geq 36n^2 \log\frac{1}{\varepsilon}$ and any decomposition $\rho^{\otimes m} = \sum p_k |\psi_k\rangle\langle\psi_k|$, except with probability $2^{-\log^2 n} + 2^{-\delta}$ we have $\underline{\mathsf{H}}^{\varepsilon}(|\psi_k\rangle) \geq m(S(\rho)-1)-\delta$.*

Proof. According to Corollary 3.1, setting $\xi = 2^{-\log^2 n}$, we have

$$H^{\xi}_{\min}(\rho^{\otimes m}) \geq m\Big(S(\rho) - 6n\sqrt{\frac{\log 1/\xi}{m}}\Big) > m(S(\rho)-1).$$

Thus $\rho^{\otimes m}$ is ξ-close to a state ρ' with min-entropy at least $m(S(\rho)-1)$. Thus we can find a projector Π spanned by eigenstates of ρ such that $\operatorname{Tr}\Pi\rho \geq 1-\xi$ and $\frac{\Pi\rho\Pi}{\operatorname{Tr}\Pi\rho}$ has min-entropy at least $m(S(\rho)-1)$. Then, by the expansion in Eq. (15), we have a decomposition of $\frac{\Pi\rho\Pi}{\operatorname{Tr}\Pi\rho}$ composed of $\frac{\Pi|\psi_k\rangle}{\|\Pi|\psi_k\rangle\|}$. Thus according to Lemma 10.3, we have that except with probability $2^{-\delta}$, $\underline{\mathsf{H}}^0(\frac{\Pi|\psi_k\rangle}{\|\Pi|\psi_k\rangle\|}) \geq m(S(\rho)-1)-\delta$. The distance $D(|\psi_k\rangle, \frac{\Pi|\psi_k\rangle}{\|\Pi|\psi_k\rangle\|}) = \sqrt{1-\|\Pi|\psi_k\rangle\|^2}$, thus by Markov's inequality,

$$\Pr\Big[D\Big(|\psi_k\rangle, \frac{\Pi|\psi_k\rangle}{\|\Pi|\psi_k\rangle\|}\Big) \leq \varepsilon\Big] = \Pr[\|\Pi|\psi_k\rangle\|^2 \geq 1-\varepsilon^2] \geq 1 - \frac{\xi}{\varepsilon^2}.$$

That is, except for negligible probability, $\underline{\mathsf{H}}^{\varepsilon}(|\psi_k\rangle) \geq m(S(\rho)-1)-\delta$ holds for any $\delta = \omega(\log n)$. □

Proof of Theorem 10.1. In the case where EFI exists, there exists an entropic EFI pair ρ_0 and ρ_1 such that $S(\rho_1) - S(\rho_0) \geq \sqrt{n}$ (if we have an entropy gap of at least 1, we can generally boost it to $\sqrt{n}$ by taking multiple independent copies). We can prepare the purification of the state and measure the purification registers in the computational basis. This results in a distribution of pair $(k, |\psi_k\rangle)$, where k is the measurement outcome and $|\psi_k\rangle$ is the post-measurement state in the EFI registers. Name the distribution as $\mathcal{D}_n$.

Then $(|\psi_k\rangle, \mathcal{D}_n)$ is a single-copy samplable state family and $\mathbb{E}_{k\sim\mathcal{D}_n}|\psi_k\rangle\langle\psi_k| = \rho_0$. Thus, we can define a single-copy state family that with probability 1/2 samples according to ρ_0

and with probability 1/2 samples according to ρ_1. According to Corollary 10.2, $\mathcal{D}_n$ is a $\mathsf{Double\text{-}GapH}[r, r + \Delta]$ instance, where $r = mS(\rho)$ and $\Delta = \sqrt{m}$. Thus, according to the security of $\mathsf{1PRS}$, $\mathsf{Double\text{-}GapH}$ is hard over $\mathcal{D}_n$ given a single copy of the state.

Assuming that EFI does not exist, we can apply the algorithm in Theorem 7.1. The argument is exactly the same, as we never rely on the fact that the state family is an efficiently samplable keyed family. □

Remark. The same argument also works well for the GapU characterization of EFI. With similar arguments, we can show that EFI exists if and only if $\mathsf{DoubleGapU}[r, r + \Delta]$ is hard on average over some single-copy samplable state family, where r is an inefficiently computable function.

Acknowledgements. B.C. acknowledges support of Royal Society University Research Fellowship URF\R1\211106 and EPSRC project EP/Z534158/1 on "Integrated Approach to Computational Complexity: Structure, Self-Reference and Lower Bounds".

References

[Aar10] Scott Aaronson. The equivalence of sampling and searching. *Electron. Colloquium Comput. Complex.*, TR10-128, 2010. 1

[AGL24] Prabhanjan Ananth, Aditya Gulati, and Yao-Ting Lin. Cryptography in the common haar state model: feasibility results and separations. In *Theory of Cryptography Conference*, pages 94–125. Springer, 2024. 1

[AIK21] Scott Aaronson, DeVon Ingram, and William Kretschmer. The Acrobatics of BQP. Technical Report 164, 2021. 3

[BCN25] John Bostanci, Boyang Chen, and Barak Nehoran. Oracle separation between quantum commitments and quantum one-wayness. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part VII*, volume 15607 of *Lecture Notes in Computer Science*, pages 3–22. Springer, 2025. 1, 5

[BCQ22] Zvika Brakerski, Ran Canetti, and Luowen Qian. On the computational hardness needed for quantum cryptography, 2022. 1, 3, 3.2, 3.2

[BFW14] Mario Berta, Omar Fawzi, and Stephanie Wehner. Quantum to Classical Randomness Extractors. *IEEE Transactions on Information Theory*, 60(2):1168–1192, February 2014. 3.3

[BJ24] Rishabh Batra and Rahul Jain. Commitments are equivalent to statistically-verifiable one-way state generators. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1178–1192. IEEE, 2024. 5

[BMM$^+$25] Amit Behera, Giulio Malavolta, Tomoyuki Morimae, Tamer Mour, and Takashi Yamakawa. A new world in the depths of microcrypt: Separating owsgs and quantum money from qefid. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 23–52. Springer, 2025. 5

[BQSY24] John Bostanci, Luowen Qian, Nicholas Spooner, and Henry Yuen. An efficient quantum parallel repetition theorem and applications. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1478–1487, 2024. 3.2, 3.2

[BvDL00] André Berthiaume, Wim van Dam, and Sophie Laplante. Quantum kolmogorov complexity. In *Proceedings of the 15th Annual IEEE Conference on Computational Complexity, Florence, Italy, July 4-7, 2000*, pages 240–249. IEEE Computer Society, 2000. 1.1

[CCS25] Boyang Chen, Andrea Coladangelo, and Or Sattath. The power of a single haar random state: constructing and separating quantum pseudorandomness. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 108–137. Springer, 2025. 1

[CGG$^+$25] Bruno Cavalar, Eli Goldin, Matthew Gray, Peter Hall, Yanyi Liu, and Angelos Pelecanos. On the computational hardness of quantum one-wayness. *Quantum*, 9:1679, 2025. 1

[CGGH25] Bruno Pasqualotto Cavalar, Eli Goldin, Matthew Gray, and Peter Hall. A meta-complexity characterization of quantum cryptography. In Serge Fehr and Pierre-Alain Fouque, editors, *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part VII*, volume 15607 of *Lecture Notes in Computer Science*, pages 82–107. Springer, 2025. 1, 1, 1.1, 1.2, 1.2, 5

[CHO$^+$20] Lijie Chen, Shuichi Hirahara, Igor C. Oliveira, Ján Pich, Ninad Rajgopal, and Rahul Santhanam. Beyond natural proofs: Hardness magnification and locality. In Thomas Vidick, editor, *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA*, volume 151 of *LIPIcs*, pages 70:1–70:48. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. 1

[DBWR14] Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner. One-shot decoupling. *Communications in Mathematical Physics*, 328(1):251–284, May 2014. 3.3, 3.3

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6):644–654, 1976. 1

[DN06] Christopher M. Dawson and Michael A. Nielsen. The solovay-kitaev algorithm. *Quantum Inf. Comput.*, 6(1):81–95, 2006. A, A

[Dup10] Frédéric Dupuis. *The Decoupling Approach to Quantum Information Theory*. PhD thesis, Université de Montréal, April 2010. 2.1, 2.3

[Fan73] M. Fannes. A continuity property of the entropy density for spin lattice systems. *Comm. Math. Phys.*, 31:291–294, 1973. 3.1

[Gác01] Peter Gács. Quantum algorithmic entropy. *Journal of Physics A: Mathematical and General*, 34(35):6859, August 2001. 1.1, 2.3, 3.4, 3.12

[GMMY24] Eli Goldin, Tomoyuki Morimae, Saachi Mutreja, and Takashi Yamakawa. Countcrypt: Quantum cryptography between QCMA and PP. *IACR Cryptol. ePrint Arch.*, page 1707, 2024. 1

[Gol90] Oded Goldreich. A note on computational indistinguishability. *Information Processing Letters*, 34(6):277–281, May 1990. 1, 2.1

[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 Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 1039–1050. ACM, 2023. 1

[HILL99] Johan HÅstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A Pseudorandom Generator from any One-way Function. *SIAM Journal on Computing*, 28(4):1364–1396, January 1999. 1, 1.1

[HKNY24] Taiga Hiroka, Fuyuki Kitagawa, Ryo Nishimaki, and Takashi Yamakawa. Robust combiners and universal constructions for quantum cryptography. In *Theory of Cryptography Conference*, pages 126–158. Springer, 2024. 1.1, 2.2

[HM25] Taiga Hiroka and Tomoyuki Morimae. Quantum cryptography and meta-complexity. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part II*, volume 16001 of *Lecture Notes in Computer Science*, pages 545–574. Springer, 2025. 1, 1, 1.1, 1.2

[HN23] Shuichi Hirahara and Mikito Nanashima. Learning in pessiland via inductive inference. In *64th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2023, Santa Cruz, CA, USA, November 6-9, 2023*, pages 447–457. IEEE, 2023. 1, 3

[Ila20] Rahul Ilango. Constant depth formula and partial function versions of MCSP are hard. In Sandy Irani, editor, *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*, pages 424–433. IEEE, 2020. 1

[ILL89] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, STOC '89, pages 12–24, New York, NY, USA, February 1989. Association for Computing Machinery. 1

[Imp95] Russell Impagliazzo. A personal view of average-case complexity. In *Proceedings of the Tenth Annual Structure in Complexity Theory Conference, Minneapolis, Minnesota, USA, June 19-22, 1995*, pages 134–147. IEEE Computer Society, 1995. 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. 1, 1.1

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, volume 10993 of *Lecture Notes in Computer Science*, pages 126–152. Springer, 2018. 1

[KQST22] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. Quantum Cryptography in Algorithmica, December 2022. 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, July 5-8, 2021, Virtual Conference*, volume 197 of *LIPIcs*, pages 2:1–2:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. 1

[KT24] Dakshita Khurana and Kabir Tomer. Commitments from quantum one-wayness. In Bojan Mohar, Igor Shinkar, and Ryan O'Donnell, editors, *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*, pages 968–978. ACM, 2024. 4.2

[KT25] Dakshita Khurana and Kabir Tomer. Founding quantum cryptography on quantum advantage, or, towards cryptography from #p hardness. In Michal Koucký and Nikhil Bansal, editors, *Proceedings of the 57th Annual ACM Symposium on Theory of Computing, STOC 2025, Prague, Czechia, June 23-27, 2025*, pages 178–188. ACM, 2025. 1

[Lev87] Leonid A. Levin. One-way functions and pseudorandom generators. *Comb.*, 7(4):357–363, 1987. 1, 6

[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, *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*, pages 979–990. ACM, 2024. 1, 1.2

[LP20] Yanyi Liu and Rafael Pass. On one-way functions and kolmogorov complexity. In Sandy Irani, editor, *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*, pages 1243–1254. IEEE, 2020. 1

[LP23] Yanyi Liu and Rafael Pass. One-way functions and the hardness of (probabilistic) time-bounded kolmogorov complexity w.r.t. samplable distributions. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part II*, volume 14082 of *Lecture Notes in Computer Science*, pages 645–673. Springer, 2023. 1

[LP25] Yanyi Liu and Rafael Pass. Hardness along the boundary: Towards one-way functions from the worst-case hardness of time-bounded kolmogorov complexity. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology -*

CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part I, volume 16000 of *Lecture Notes in Computer Science*, pages 617–650. Springer, 2025. 1

[LV19] Ming Li and Paul M. B. Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications, 4th Edition.* Texts in Computer Science. Springer, 2019. A.1

[MB04] Caterina E. Mora and Hans J. Briegel. Algorithmic complexity of quantum states. *International Journal of Quantum Information 4.04*, 2004. 1.1, 1.1, 2.4, 3.4, 3.11

[MBK06] C. Mora, H. Briegel, and B. Kraus. Quantum kolmogorov complexity and its applications, 2006. 2.3, 3.4, 3.11

[NC02] Michael A Nielsen and Isaac L. Chuang. *Quantum Information and Quantum Computation.* Cambridge University Press, 2002. 3.1, A

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93. ACM, 2005. 1

[Ren08] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008. 3.1, 4

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978. 1

[San19] Rahul Santhanam. Pseudorandomness and the minimum circuit size problem. *Electron. Colloquium Comput. Complex.*, TR19-155, 2019. 1

[TCR10] Marco Tomamichel, Roger Colbeck, and Renato Renner. Duality between smooth min-and max-entropies. *IEEE Transactions on information theory*, 56(9):4674–4681, 2010. 3.1

[Tom12] Marco Tomamichel. A framework for non-asymptotic quantum information theory. *Ph.D. thesis (Swiss Federal Institute of Technology)*, 2012. 3.1, 4, 3.3

[Tra84] Boris A. Trakhtenbrot. A survey of russian approaches to perebor (brute-force searches) algorithms. *IEEE Ann. Hist. Comput.*, 6(4):384–400, 1984. 1

[Vit00] Paul M. B. Vitányi. Three approaches to the quantitative definition of information in an individual pure quantum state. In *Proceedings of the 15th Annual IEEE Conference on Computational Complexity, Florence, Italy, July 4-7, 2000*, pages 263–270. IEEE Computer Society, 2000. 1.1

[Wat18] John Watrous. *The Theory of Quantum Information.* Cambridge University Press, Cambridge, 2018. 3.1

[Win99] Andreas Winter. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inform. Theory*, 45(7):2481–2485, 1999. 3.1

A Quantum Kolmogorov complexities - Invariance and Equivalence

In Subsection 3.4 we claimed that the definitions of $\mathsf{K}_{\mathsf{net}}$ and $\underline{\mathsf{H}}$ are robust to changes in our choice of universal Turing machine and gate basis. We also claimed that our notion of $\underline{\mathsf{H}}$ is equivalent to the one introduced by Gács. In this appendix we will give proofs for those three claims. Each of these claims is essentially a corollary of the fact that universal gate sets are defined as being "dense" in the space of unitaries. This definition is standard and can be seen for instance in [NC02, sec 4.5] or [DN06, Definition 1].

Definition A.1. A quantum gate set B is universal if for any unitary U and degree of precision ε there exists a B circuit C such that $||U - C|| \leq \varepsilon$ where $||U - C||$ is measuring the operator norm.

In the typical setting where one cares about efficient algorithms, switching between universal gate sets requires using the Solovay-Kitaev theorem [DN06], which morally states that, given a description of a unitary U, a B-circuit of length $O(\log(1/\varepsilon))$ which ε-approximates U can be efficiently found. However, in the time-unbounded setting of Kolmogorov complexity, we do not need the circuits to be short or efficiently findable, we just need them to exist and therefore be findable via brute-force search, which follows almost immediately from the definition.

We will now formalize this intuition in the following lemma. Below, a *"description format"* is any encoding scheme for unitaries that allows for a unitary's entries to be computed to arbitrary precision. Possible formats for encoding a unitary A include algebraic representations of all entries, descriptions of a circuit implementing the unitary, and programs mapping a tuple (i, j, ε) to values $A'_{i,j}$ such that $|A_{i,j} - A'_{i,j}| \leq \varepsilon$. This universality with respect to description format is what allows us to use this lemma to prove all three of our claims.

Lemma A.1. *Let $\mathcal{G}$ be a universal gate set with computable entries, and fix a description format for unitaries allowing each entry to be computable. There exists a fixed length program p such that, given a unitary A in the format and a precision parameter $\varepsilon \in (0, 1)$, the program $U(p, A, \varepsilon)$ outputs a $\mathcal{G}$-circuit C such that $\|C - A\| \leq \varepsilon$.*

Proof. The program p first determines d the dimension of the unitary A, then computes approximations of every entry of A to an approximation factor of $\varepsilon/4d$ resulting in matrix A', then finally iterates through all circuits of each size searching for a circuit C of minimal length such that $||A' - C|| \leq \varepsilon/2$.

If we define $\Delta = A - A'$ we can see that

$$||\Delta|| \leq ||\Delta||_F = \sqrt{\sum_{i,j} ||\Delta_{i,j}||^2} \leq \sqrt{d^2(\varepsilon/4d)^2} = \varepsilon/4.$$

By the universality of $\mathcal{G}$ a circuit C such that $||A - C'|| \leq \varepsilon/4$ must exist. And by the triangle inequality any C such that $||A - C|| \leq \varepsilon/4$ will satisfy $||A' - C|| \leq \varepsilon/2$. Therefore there is guaranteed to exist some circuit satisfying $||A' - C|| \leq \varepsilon/2$ which p will eventually find.

By the triangle inequality $||A - C|| \leq ||A - A'|| + ||A' - C|| \leq \varepsilon/4 + \varepsilon/2 < \varepsilon$. Meaning that any circuit satisfying $||A' - C|| \leq \varepsilon/2$ will also satisfy $||A - C|| \leq \varepsilon$. □

Using this lemma we will now prove our three claims.

A.1 $\mathsf{K}_{\mathsf{net}}$ Invariance

In Subsection 3.4, we claimed that the definition of $\mathsf{K}_{\mathsf{net}}$ only changes by nearly a constant when B and U are universal. Because the definition of $\mathsf{K}_{\mathsf{net}}$ goes through circuits which are represented as strings, we can change our choice of universal Turing machine while only incurring a fixed constant difference. However, because we cannot guarantee that B circuits can exactly simulate all the gates in B', it is possible that there exists states for which $\mathsf{K}_{\mathsf{net}}^{U,B,0}(|\psi\rangle) = \infty$ while $\mathsf{K}_{\mathsf{net}}^{U',B',0}(|\psi\rangle) = c$. Thus, an "ideal" invariance theorem of the following form cannot hold: $\forall U, U', B, B' \exists c : \mathsf{K}_{\mathsf{net}}^{U,B,0}(|\psi\rangle) \leq \mathsf{K}_{\mathsf{net}}^{U',B',0}(|\psi\rangle) + c$. However if we allow for some very small additional error term δ, and a just slightly super constant difference, we are able to show an invariance, as the following lemma states.

Lemma A.2. *For any universal Turing machines U and U', universal quantum gate sets B, and B' with computable amplitudes, and m qubit state $|\psi\rangle$, we get that*

$$\mathsf{K}_{\mathsf{net}}^{U,B,\varepsilon+\delta}(|\psi\rangle) \leq \mathsf{K}_{\mathsf{net}}^{U',B',\varepsilon}(|\psi\rangle) + O(1) + \min_{v>1/\delta}[\mathsf{K}(v|m)].$$

Proof. For convenience we will label $\alpha = \mathsf{K}_{\mathsf{net}}^{U',B',\varepsilon}(|\psi\rangle)$. By the definition of $\mathsf{K}_{\mathsf{net}}$ we know that there exists some B' circuit $C_{B'}$ such that $\mathsf{K}_{U'}(C_{B'}) = \alpha$ and $|\langle\psi|C_{B'}|0^m\rangle|^2 \geq 1 - \varepsilon$. By the invariance of K we know that $\mathsf{K}_U(C_{B'}) \leq \alpha + O(1)$.

By Lemma A.1, for any pair of universal gate sets B, B' with computable amplitudes, there exists a constant length program $p_{B,B'}(\delta, C_{B'})$ which takes in ε and a B'-circuit $C_{B'}$ and outputs a B-circuit C_B approximately computing $C_{B'}$ such that $||C_B - C_{B'}|| \leq \delta$.

Let $\min_{v>1/\delta}[K(v|m)] = l$, then there exists a program with size l that will output a $v > 1/\delta$. If we consider an optimal program which first generates $C_{B'}$, then generates $v \geq 1/\delta$ (this can either be done from no input or taking as input some value that the program has already generated such as the length of the output of the circuit i.e. m), runs $p_{B,B'}(n_0, C_{B'}) \to C_B$, then runs $C_B |0\rangle \to |\psi'\rangle$, the resulting state $|\psi'\rangle$ will satisfy $|\langle\psi'|C_{B'}|0\rangle|^2 \leq 1/v \leq \delta$, and by the triangle inequality $|\langle\psi|C_{B'}|0\rangle|^2 \leq \delta + \varepsilon$. This program will have length at most $\mathsf{K}_U(C_{B'}) \leq \alpha + O(1)$ to generate $C_{B'}$, plus $l + O(1)$ to generate $1/v$ which is smaller than $1/\delta$, plus $O(1)$ to implement $p_{B,B'}$ and apply $p_{B,B'}(1/v, C_{B'})$. □

Note that as observed by Li and Vitanyi [LV19, sec 3.3], the summand $\min_{n>1/\delta}[\mathsf{K}(n)] \leq \min_{n>1/\delta}[\mathsf{K}(n|m)] + O(1)$ goes to infinity more slowly than any unbounded monotonic computable function. Thus, while the final term in the lemma above is not quite constant, it is of the order $o(f(1/\delta))$ for any monotonic unbounded computable function in $1/\delta$, including $\log(\log(\ldots\log(1/\delta)))$ for any number of composed logarithm's. Consequently, even for exceptionally small δ, the complexity $\mathsf{K}_{\mathsf{net}}^{U,B,\varepsilon+\delta}(|\psi\rangle)$ is only ever a just barely super constant amount larger than $\mathsf{K}_{\mathsf{net}}^{U',B',\varepsilon}(|\psi\rangle)$.

A.2 $\underline{\mathsf{H}}$ Invariance

As in our discussion of invariance for $\mathsf{K}_{\mathsf{net}}$, the invariance of $\underline{\mathsf{H}}$'s with respect to the choice of universal Turing machines follows straightforwardly from the invariance of the prefix-free Kolmogorov complexity of the classical string describing a circuit. We can derive the invariance with respect to the choice of gate set B using similar ideas as those in Lemma A.2, but because small errors in recreating the state impact the value of $\underline{\mathsf{H}}$ rather than changing a parameter we can here achieve the ideal version of invariance.

Lemma A.3. *For any universal Turing machines U and U', and universal quantum gate sets B, and B' with computable amplitudes we get that*

$$\underline{\mathsf{H}}^{U,B}(|\psi\rangle) \leq \underline{\mathsf{H}}^{U',B'}(|\psi\rangle) + O(1).$$

Proof. We label the set of prefix free programs as $P \subset \{0,1\}^*$, the circuit given by $U(p)$ as $C_{U,B,p}$, and the state $C_{U',B',p}|0^m\rangle$ as $|\psi_p\rangle$.

For any U, U', there exists some constant length program $p_{U,U'}$ such that $U(p_{U,U'}, p) = U'(p)$. There also exists a constant length program which, if given a quantum circuit, will output the length m of the quantum state it operates on. Moreover, for any two computable gate sets B, B', by Lemma A.1 there exists a constant length program $p_{B,B'}(2^{-2m}, C_{B'}) \to C_B$ such that $\forall |\psi\rangle : |\langle\psi| C_{B'}|0\rangle - \langle\psi| C_B |0\rangle| \leq 2^{-2m}$ and consequently $|\langle\psi| C_{B'}|0\rangle|^2 - |\langle\psi| C_B|0\rangle|^2 \leq 2^{-2m+1}$.

For each U', B' program p' resulting in state $|\psi_{p'}\rangle$, consider the following U, B program p: first run $U(p_{U,U'}, p') = U'(p') = C_{U',B',p'}$, second extract the length of the resulting state m from $C_{U',B',p'}$, third run $p_{B,B'}(2^{-2m}, U(p_{U,U'}, p'))$ and call the resulting B circuit $C_{U,B,p}$, finally compute and output the state $C_{U,B,p}|0\rangle$, which we will call $|\psi_p\rangle$. Since all three steps are computable by constant length programs, there exists some constant c such that, for each p', we have $|p| \leq |p'| + c$.

By the definition of $\underline{\mathsf{H}}$ we know that

$$\begin{aligned}
\underline{\mathsf{H}}^{U,B}(|\psi\rangle) &\geq -\log\left(\sum_{p\in P} 2^{-|p|} |\langle\psi|\psi_p\rangle|^2\right) \\
&\geq -\log\left(\sum_{p'\in P} 2^{-|p'|-c}\left(\left|\langle\psi|\psi_{p'}\rangle\right|^2 - 2^{-2m+1}\right)\right) \\
&\geq -\log\left(-2^{-2m+1} + \sum_{p'\in P} 2^{-|p'|-c}\left(\left|\langle\psi|\psi_{p'}\rangle\right|^2\right)\right) \\
&\geq -\log\left(-2^{-2m+1} + 2^{-c}\sum_{p'\in P} 2^{-|p'|}\left(\left|\langle\psi|\psi_{p'}\rangle\right|^2\right)\right) \\
&\geq -\log\left(2^{-c-1}\sum_{p'\in P} 2^{-|p'|}\left(\left|\langle\psi|\psi_{p'}\rangle\right|^2\right)\right) \\
&= c + 1 + \underline{\mathsf{H}}^{U',B'}(|\psi\rangle).
\end{aligned}$$

The second to last inequality follows from the fact that $\underline{\mathsf{H}}(|\psi\rangle)$ is at most $m + c'$ for some global constant c', meaning $\sum_{p'\in P} 2^{-|p'|}\left(\left|\langle\psi|\psi_{p'}\rangle\right|^2\right) \geq 2^{-m-c'}$, and consequently the right term is at least $2^{-m-c'-c}$ which is more than twice 2^{-2m+1} for any large enough m. □

A.3 Equivalence of $\underline{\mathsf{H}}$ notions

Gács' original version of $\underline{\mathsf{H}}$ is defined by defining the universal semi-mixed state

$$\boldsymbol{\mu} = \sum_{p\in P} 2^{-|p|} |\phi_p\rangle\langle\phi_p|,$$

where $|\phi_p\rangle$ is the state corresponding to reading the output of $U(p)$ as an amplitude vector with each amplitude being read as an algebraic number. The difference between our approaches is to interpret $U(p)$ as quantum circuits.

Given our argument for the previous lemma, to prove the equivalence between our notions it suffices to show that, for any universal gate set B, there exists a constant length classical Turing machine which maps from algebraic amplitude vectors representing $|\phi\rangle$ to quantum circuits C_B such that

$$|\langle\phi| C_B |0^m\rangle| \geq 1 - 2^{-2m}.$$

Since algebraic numbers are computable, we can modify the program described in the proof of Lemma A.1 to halt when it finds a circuit which maps $|0^m\rangle$ to within ε of $|\phi\rangle$ (where ε is 2^{-2m}) and we have a program satisfying the above requirement.