On One-way Functions and Kolmogorov Complexity

Yanyi Liu
Cornell University
yl2866@cornell.edu

Rafael Pass
Cornell Tech
rafael@cs.cornell.edu

Abstract—We prove that the equivalence of two fundamental problems in the theory of computing. For every polynomial $t(n) \geq (1 + \varepsilon)n$, $\varepsilon > 0$, the following are equivalent:

- One-way functions exist (which in turn is equivalent to the existence of secure private-key encryption schemes, digital signatures, pseudorandom generators, pseudorandom functions, commitment schemes, and more);
- $t$-time bounded Kolmogorov Complexity, $K^t_x$, is mildly hard-on-average (i.e., there exists a polynomial $p(n) > 0$ such that no FPT algorithm can compute $K^t_x$, for more than a $1 - \frac{1}{n}$ fraction of $n$-bit strings).

In doing so, we present the first natural, and well-studied, computational problem characterizing the feasibility of the central private-key primitives and protocols in Cryptography.

I. INTRODUCTION

We prove the equivalence of two fundamental problems in the theory of computing: (a) the existence of one-way functions, and (b) mild average-case hardness of the time-bounded Kolmogorov Complexity problem.

Existence of One-way Functions: A one-way function [13] (OWF) is a function $f$ that can be efficiently computed (in polynomial time), yet no probabilistic polynomial-time (PPT) algorithm can invert $f$ with inverse polynomial probability for infinitely many input lengths $n$. Whether one-way functions exist is unequivocally the most important open problem in Cryptography (and arguably the most importantly open problem in the theory of computation, see e.g., [35]): OWFs are both necessary [31] and sufficient for many of the most central cryptographic primitives and protocols (e.g., pseudorandom generators [8], [26], pseudorandom functions [17], private-key encryption [20], digital signatures [43], commitment schemes [39], identification protocols [15], coin-flipping protocols [10], and more). These primitives and protocols are often referred to as private-key primitives, or “Minicrypt” primitives [29] as they exclude the notable task of public-key encryption [13], [42]. Additionally, as observed by Impagliazzo [22], [29], the existence of a OWF is equivalent to the existence of polynomial-time method for sampling hard solved instances for an NP language (i.e., hard instances together with their witnesses).

While many candidate constructions of OWFs are known—most notably based on factoring [42], the discrete logarithm problem [13], or the hardness of lattice problems [1]—the question of whether there exists some natural average-case hard problem that characterizes the hardness of OWFs (and thus the feasibility of the above central cryptographic primitives) has been a long-standing open problem:

Does there exists some natural average-case hard computational problem (i.e., both the computational problem and the distribution over instances is “natural”), which characterizes the existence of one-way functions?

This problem is particularly pressing given recent advances in quantum computing [7] and the fact that many classic OWF candidates (e.g., based on factoring and discrete log) can be broken by a quantum computer [45].

Average-case Hardness of $K^{poly}$-Complexity: What makes the string 121212121212121 less random than 60484850668340357492? The notion of Kolmogorov complexity ($K$-complexity), introduced by Solomonoff [48], Kolmogorov [34] and Chaitin [12], provides an elegant method for measuring the amount of “randomness” in individual strings: The $K$-complexity of a string is the length of the shortest program (to be run on some fixed universal Turing machine $U$) that outputs the string $x$. From a computational point of view, however, this notion is unappealing as there is no efficiency requirement on the program. The notion of $t(\cdot)$-time-bounded Kolmogorov Complexity ($K^t$-complexity) overcomes this issue: $K^t_x(x)$ is defined as the length of the shortest program that outputs the string $x$ within time $t(|x|)$. As surveyed by Trakhtenbrot [49], the problem of efficiently determining the $K^t$-complexity for $t(n) = \text{poly}(n)$ predates the theory of NP-completeness and was studied in the Soviet Union since the 60s as a candidate for a problem that requires “brute-force search” (see Task 5 on page 392 in [49]). The modern complexity-theoretic

1Note that Levin [36] presents an ingenious construction of a universal one-way function—a function that is one-way if one-way functions exists. But his construction (which relies on an enumeration argument) is artificial. Levin [35] takes a step towards making it less artificial by constructing a universal one-way function based on a new specially-tailored Tiling Expansion problem.
study of this problem goes back to Sipser [46], Ko [33] and Hartmanis [25].

Intriguingly, Trakhtenbrot also notes that a “frequentential” version of this problem was considered in the Soviet Union in the 60s: the problem of finding an algorithm that succeeds for a “high” fraction of strings \( x \)—in more modern terms from the theory of average-case complexity [37], whether \( K^t \) can be computed by a heuristic algorithm with inverse polynomial error, over random inputs \( x \). We say that \( K^t \) is mildly hard-on-average (mildly HoA) if there exists some polynomial \( p(\cdot) > 0 \) such that every PPT fails in computing \( K^t(\cdot) \) for at least a \( \frac{1}{p(x)} \) fraction of \( n \)-bit strings \( x \) for every sufficiently large \( n \), and that \( K^{poly} \) is mildly HoA if there exists some polynomial \( t(n) > 0 \) such that \( K^t \) is mildly HoA. Our main result shows that the existence of OWFs is equivalent to mild average-case hardness of \( K^{poly} \). In doing so, we resolve the above-mentioned open problem, and present the first natural (and well-studied) computational problem, characterizing the feasibility of the central private-key primitve in Cryptography.

**Theorem 1.** The following are equivalent:
- One-way functions exist;
- \( K^{poly} \) is mildly hard-on-average.

In other words,

Secure private-key encryption, digital signatures, pseudorandom generators, pseudorandom functions, commitment schemes, etc., are possible iff \( K^{poly} \)-complexity is mildly hard-on-average.

In fact, our main theorem is stronger than stated: we show that for every polynomial \( t(n) \geq (1 + \varepsilon)n \), where \( \varepsilon > 0 \) is a constant, mild average-case hardness of \( K^t \) is equivalent to the existence of one-way functions.

**On the Hardness of Approximating \( K^{poly} \)-complexity:**

Our connection between OWFs and \( K^t \)-complexity has direct implications to the theory of \( K^t \)-complexity. Trakhtenbrot [49] also discusses average-case hardness of the approximate \( K^t \)-complexity problem: the problem of, given a random \( x \), outputting an “approximation” \( y \) that is \( \beta(|x|) \)-close to \( K^t(x) \) (i.e., \( |K^t(x) - y| \leq \beta(|x|)) \). He observes that there is a trivial heuristic approximation algorithm that succeeds with probability approaching 1 (for large enough \( n \)): Given \( x \), simply output \( |x| \). In fact, this trivial algorithm produces a \( (d \log n) \)-approximation with probability \( \geq 1 - \frac{1}{n^c} \) over random \( n \)-bits strings.\(^2\) We note that our proof that OWFs imply mild average-case hardness of \( K^{poly} \) actually directly extends to show that \( K^{poly} \) is mildly-HoA also to \( (d \log n) \)-approximate. We thus directly get:

\(^2\)At most \( 2^n - d \log n \) out of \( 2^n \) strings have \( K^t \)-complexity that is smaller than \( n - d \log n \).

**Theorem 2.** If \( K^{poly} \) is mildly hard-on-average, then for every constant \( d \), \( K^{poly} \) is mildly hard-on-average to \( (d \log n) \)-approximate.

In other words, any efficient algorithm that only slightly beats the success probability of the “trivial” approximation algorithm, can be used to break OWFs.

**Existential vs. Constructive \( K^t \)-complexity:**

Trakhtenbrot [49] considers also “constructive” variant of the \( K^t \)-complexity problem, where the task of the solver is to, not only determine the \( K^t \)-complexity of a string \( x \), but to also output a minimal-length program \( P \) that generates \( x \). We remark that for our proof that mild average-case hardness of \( K^{poly} \) implies OWFs, it actually suffices to assume mild average-case hardness of the “constructive” \( K^{poly} \) problem, and thus we obtain an equivalence between the “existential” and “constructive” versions of the problem in the average-case regime.

**On Decisional Time-Bounded Kolmogorov Complexity Problems:**

We finally note that our results also show an equivalence between one-way functions and mild average-case hardness of a decisional \( K^{poly} \) problem: Let \( MINK^t[s] \) denote the set of strings \( x \) such that \( K^t(|x|)(x) \leq s(|x|) \). Our proof directly shows that there exists some constant \( c \) such that for every constant \( \varepsilon > 0 \), every \( t(n) \geq (1 + \varepsilon)n \), and letting \( s(n) = n - c \log n \), mild average-case hardness of the language \( MINK^t[s] \) (with respect to the uniform distribution over instances) is equivalent the existence of one-way functions.

A. Related Work

We refer the reader to Goldreich’s textbook [16] for more context and applications of OWFs (and complexity-based cryptography in general); we highly recommend Barak’s survey on candidate constructions of one-way functions [9]. We refer the reader to the textbook of Li and Vitanyi [38] for more context and applications of Kolmogorov complexity; we highly recommend Allender’s surveys on the history, and recent applications, of notions of time-bounded Kolmogorov complexity [2]–[4].

**On Connections between \( K^{poly} \)-complexity and OWFs:**

We note that some (partial) connections between \( K^t \)-complexity and OWFs already existed in the literature:

- Results by Kabanets and Cai [32] and Allender et al [5] show that the existence of OWFs implies that \( K^{poly} \) must be worst-case hard to compute; their results will be the starting point for our result that OWFs also imply average-case hardness of \( K^{poly} \).
- Allender and Das [6] show that every problem in \( SZK \) (the class of promise problems having statistical zero-knowledge proofs [21]) can be solved in probabilistic polynomial-time using a
A very recent elegant work by Santhanam [44] is also explicitly motivated by the above-mentioned open problem, and presents an intriguing connection between one-way functions and error-less average-case hardness of the circuit minimization problem (MCSP) [32]—i.e., the problem of, given a truth table of a boolean function, determining the size of the smallest circuit that computes the function; the MCSP problem is closely related to the time-bounded Kolmogorov complexity problem [5], [49]. Santhanam proves equivalence between OWFs and errorless average-case hardness of MCSP under a new (and somewhat complicated) conjecture that he introduces. We emphasize that, in contrast, our equivalence is unconditional.

On Worst-case to Average-case Reductions for $K^{\text{poly}}$: We highlight a very elegant recent result by Hirahara [27] that presents a worst-case (approximation) to average-case reduction for $K^{\text{poly}}$-complexity. Unfortunately, his result only gives average-case hardness w.r.t. errorless heuristics—namely, heuristics that always provide either the correct answer or output ⊥ (and additionally only output ⊥ with small probability). For our construction of a OWF, however, we require average-case hardness of $K^t$ also with respect to heuristics that may err (with small probability). Santhanam [44], independently, obtains a similar result for a related problem.

Hirahara notes that it is an open problem to obtain a worst-case to average-case reduction for $K^{\text{poly}}$ w.r.t. heuristics that may err. Let us emphasize that average-case hardness w.r.t. errorless heuristics is a much weaker property that just “plain” average-case hardness (with respect to heuristics that may err): Consider a random 3SAT formula on $n$ variables with 1000$n$ clauses. It is well-known that, with high probability, the formula is not satisfiable. Thus, there is a trivial heuristic algorithm for solving 3SAT on such random instances by simply outputting “No”. Yet, the question of whether there exists an efficient errorless heuristic for this problem is still open, and non-existence of such an algorithm is implied by Feige’s Random 3SAT conjecture [14].

On Universal Extrapolation: Impagliazzo and Levin [30] consider a problem of universal extrapolation: Roughly speaking, extrapolation with respect to some polynomial-time Turing machine $M$ requires, given some prefix string $x_{\text{pre}}$, sampling a random continuation $x_{\text{post}}$ such that $M$ (on input a random tape) generates $x_{\text{pre}} || x_{\text{post}}$. Universal extrapolation is said to be possible if all polynomial-time Turing machines can be extrapolated. Impagliazzo and Levin demonstrate the equivalence of one-way functions and the infeasibility of universal extrapolation.

As suggested by an anonymous FOCS reviewer, universal extrapolation seems related to time-bounded Kolmogorov complexity: Extrapolation with respect to a universal Turing machine should, intuitively, be equivalent to approximating $K^{\text{poly}}$ (for random string $x$) by counting the number of possible continuations $x_{\text{post}}$ to a prefix $x_{\text{pre}}$ of $x$. Strings with small $K^{\text{poly}}$-complexity should have many possible continuation, while strings with large $K^{\text{poly}}$-complexity should have few.

While this method may perhaps be used to obtain an alternative proof of one direction (existence of one-way function from hardness of $K^{\text{poly}}$ of our main theorem, as far as we can tell, the actual proof is non-trivial and would result in a significantly weaker conclusion than what we obtain: It would only show that average-case hardness of approximating $K^{\text{poly}}$ implies infeasibility of universal extrapolation and thus one-way functions, whereas we show that even average-case hardness of exactly computing $K^{\text{poly}}$ implies the existence of one-way functions.

For the converse direction, the infeasibility of universal extrapolation only means that there exists some polynomial-time Turing machine $M$ that is hard to extrapolate, and this $M$ is not necessarily a universal Turing machine. It is not a-priori clear whether infeasibility of extrapolation w.r.t. some $M$ implies infeasibility of extrapolation w.r.t. a universal Turing machine.

A direct corollary of our main theorem is a formal connection between universal extrapolation and average-case hardness of $K^{\text{poly}}$: Infeasibility of universal extrapolation is equivalent to mild average-case hardness of $K^{\text{poly}}$ (since by [30], infeasibility of universal extrapolation is equivalent to the existence of one-way functions).

B. Proof outline

We provide an outline for the proof of Theorem 1.

**OWFs from Avg-case $K^{\text{poly}}$-Hardness:** We show that if $K^t$ is mildly average-case hard for some polynomial $t(n) > 0$, then a weak one-way function exists\(^3\); the existence of (strong) one-way functions then follows by Yao’s hardness amplification theorem [50]. Let $c$ be a constant such that every string $x$ can be output by a program of length $|x| + c$ (running on the fixed Universal Turing machine $U$). Consider the function $f(\ell || \Pi')$, where $\ell$ is a bitstring of length $\log(n+c)$ and $\Pi'$ is a bitstring of length $n+c$, that lets $\Pi$ be the first $\ell$ bits.

\(^3\)Recall that an efficiently computable function $f$ is a weak OWF if there exists some polynomial $q > 0$ such that $f$ cannot be efficiently inverted with probability better than $1 - 1/q(n)$ for sufficiently large $n$. 


of Π′, and outputs ℓ||y where y is the output generated by running the program Π′ for t(n) steps.\(^{5}\)

We aim to show that if f can be inverted with high probability—significantly higher than \(1 - 1/n\)—then \(K^t\)-complexity of random strings \(z \in \{0, 1\}^n\) can be computed with high probability. Our heuristic \(\mathcal{H}\), given a string \(z\), simply tries to invert \(f\) on \(\ell||z\) for all \(\ell \in [n + c]\), and outputs the smallest \(\ell\) for which inversion succeeds.\(^{6}\) First, note that since every length \(\ell \in [n + c]\) is selected with probability \(1/(n + c)\), the inverter must still succeed with high probability even if we condition the output of the one-way function on any particular length \(\ell\) (as we assume that the one-way function inverter fails with probability significantly smaller than \(1/\ell\)). This, however, does not suffice to prove that the heuristic works with high probability, as the string \(y\) output by the one-way function is not uniformly distributed (whereas we need to compute the \(K^t\)-complexity for uniformly chosen strings). But, we show using a simple counting argument that \(y\) is not too “far” from uniform in relative distance. The key idea is that for every string \(z\) with \(K^t\)-complexity \(w\), there exists some program \(\Pi_z\) of length \(w\) that outputs it; furthermore, by our assumption on \(c\), \(w \leq n + c\). We thus have that \(f(\mathcal{U}_{n+c+\log(n+c)})\) will output \(w||z\) with probability at least \(\frac{1}{n+c}.2^{-w} \geq \frac{1}{n+c}.2^{-(n+c)} = \frac{2^{-w}}{\mathcal{O}(n)}\) (we need to pick the right length, and next the right program). So, if the heuristic fails with probability \(\delta\), then the one-way function inverter must fail with probability at least \(\frac{\delta}{\mathcal{O}(n)}\), which leads to the conclusion that \(\delta\) must be small (as we assumed the inverter fails with probability significantly smaller than \(1/\ell\)).

**Avg-case \(K^t\)-Hardness from EP-PRGs:** To show the converse direction, our starting point is the earlier result by Kabanets and Cai [32] and Allender et al [5] which shows that the existence of OWFs implies that \(K^t\)-complexity, for every sufficiently large polynomial \(t(\cdot)\), must be worst-case hard to compute. In more detail, they show that if \(K^t\)-complexity can be computed in polynomial-time for every input \(x\), then pseudo-random generators (PRGs) cannot exist (and PRGs are implied by OWF by [26]). This follows from the observations that (1) random strings have high \(K^t\)-complexity with overwhelming probability, and (2) outputs of a PRG always have small \(K^t\)-complexity as long as \(t(n)\) is sufficiently greater than the running time of the PRG (as the seed plus the constant-sized description of the PRG suffice to compute the output). Thus, using an algorithm that computes \(K^t\), we can easily distinguish outputs of the PRG from random strings—simply output 1 if the \(K^t\)-complexity is high, and 0 otherwise. This method, however, relies on the algorithm working for every input. If we only have access to a heuristic \(\mathcal{H}\) for \(K^t\), we have no guarantees that \(\mathcal{H}\) will output a correct value when we feed it a pseudorandom string, as those strings are sparse in the universe of all strings.\(^{7}\)

To overcome this issue, we introduce the concept of an entropy-preserving PRG (EP-PRG). This is a PRG that expands the seed by \(O(\log n)\) bits, while ensuring that the output of the PRG loses at most \(O(\log n)\) bits of Shannon entropy—it will be important for the sequel that we rely on Shannon entropy as opposed to min-entropy. In essence, the PRG preserves (up to an additive term of \(O(\log n)\)) the entropy in the seed \(s\). We next show that any good heuristic \(\mathcal{H}\) for \(K^t\) can break such an EP-PRG. The key point is that since the output of the PRG is entropy preserving, by an averaging argument, there exists a \(1/n\) fraction of “good” seeds \(S\) such that, conditioned on the seed belonging to \(S\), the output of the PRG on input seeds of length \(n\) has min-entropy \(n - O(\log n)\). This means that the probability that \(\mathcal{H}\) fails to compute \(K^t\) on output of the PRG, conditioned on picking a “good” seed, can increase at most by a factor \(\mathcal{O}(n)\). We conclude that \(\mathcal{H}\) can be used to determine (with sufficiently high probability) the \(K^t\)-complexity for both random strings and for outputs of the PRG.

**EP-PRGs from Regular OWFs:** We start by noting that the standard Blum-Micali-Goldreich-Levin [11], [19] PRG construction from one-way permutations is entropy preserving. To see this, recall the construction:

\[
G_f(s, h_{GL}) = f(s)||h_{GL}||h_{GL}(s)
\]

where \(f\) is a one-way permutation and \(h_{GL}\) is a hardcore function for \(f\)—by [19], we can select a random hardcore function \(h_{GL}\) that output \(O(\log n)\) bits. Since \(f\) is a permutation, the output of the PRG fully determines the input and thus there is actually no entropy loss. We next show that the PRG construction of [16], [18], [26], [51] from regular OWFs also is an EP-PRG. We

---

\(^{5}\)Formally, the program/description \(\Pi\) is an encoding of a pair \((M, w)\) where \(M\) is a Turing machine and \(w\) is some input, and we evaluate \(M(w)\) on the Universal Turing machine \(U\).

\(^{6}\)We remark that although our construction of the function \(f\) is somewhat reminiscent of Levin’s construction of a universal OWF, the actual function (and even more so the analysis) is actually quite different. Levin’s function \(f\), roughly speaking, parses the input into a Turing machine \(M\) of length \(\log n\) and an input \(x\) of length \(n\), and next outputs \(M(x)\). As he argues, if a OWF \(f^*\) exists, then with probability \(\frac{1}{n}\), \(f\) will compute output \(f^*(x)\) for a randomly selected \(x\), and is thus hard to invert. In contrast, in our candidate OWF construction, the key idea is to vary the length of a “fully specified” program \(\Pi\) (including an input).

\(^{7}\)We note that, although it was not explicitly pointed out, their argument actually also extends to show that \(K^t\) does not have an errorless heuristic assuming the existence of PRGs. The point is that even on outputs of the PRG, an errorless heuristic must output either a small value or \(\bot\) (and perhaps always just output \(\bot\)). But for random strings, the heuristic can only output \(\bot\) with small probability. Dealing with heuristics that may err will be more complicated.
refer to a function $f$ as being $r$-regular if for every $x \in \{0,1\}^*$, $f(x)$ has between $2^{r(|x|)-1}$ and $2^{r(|x|)}$ many preimages. Roughly speaking, the construction applies pairwise independent hash functions (that act as strong extractors) $h_1, h_2$ to both the input and output of the OWF (parametrized to match the regularity $r$) to “squeeze” out randomness from both the input and the output, and finally also applies a hardcore function that outputs $O(\log n)$ bits:

$$G'_f(s || h_1 || h_2)_{GL} = h_{GL}(s) || h_1 || h_2 || h_1(s)_{r-O(\log n)} || h_2(f(s))_{n-r-O(\log n)} || h_{GL}(s), \quad (1)$$

where $[a]_j$ means $a$ truncated to $j$ bits. As already shown in [16] (see also [51]), the output of the function excluding the hardcore bits is actually $1/\text{poly}(n)$ -close to uniform in statistical distance (this follows directly from the Leftover Hash Lemma [26]), and this implies (using an averaging argument) that the Shannon entropy of the output is at least $n - O(\log n)$, thus the construction is an EP-PRG. We finally note that this construction remains both secure and entropy preserving, even if the input domain of the function $f$ is not $\{0,1\}^n$, but rather any set $S$ of size $2^n/n$; this will be useful to us shortly.

**Cond EP-PRGs from Any OWFs:** Unfortunately, constructions of PRGs from OWFs [23], [24], [26], [28] are not entropy preserving as far as we can tell. We, however, remark that to prove that $K^t$ is mildly HoA, we do not actually need a “full-fledged” EP-PRG: Rather, it suffices to have what we refer to as a conditionally-secure EP-PRG $G$: a conditionally-secure EP-PRG (cond EP-PRG) is an efficiently computable function $G$ having the property that there exists some event $E$ such that:

1. $G(U_n || E)$ has Shannon entropy $n' - O(\log n')$;
2. $G(U_n || E)$ is indistinguishable from $U_m$ for some $m \geq n' + O(\log n')$.

In other words, there exists some event $E$ such that conditioned on the event $E$, $G$ behaves like an EP-PRG. We next show how to adapt the above construction to yield a cond EP-PRG from any OWF $f$. Consider $G(i||s || h_1, h_2, h_{GL}) = G'_f(s,h_1, h_2, h_{GL})$ where $|s| = n$, $|i| = \log n$, and $G'_f$ is the PRG construction defined in equation 1. We remark that for any function $f$, there exists some regularity $i^*$ such that at least a fraction $1/n$ of inputs $x$ have regularity $i^*$. Let $S_{i^*}$ denote the set of these $x$'s. Clearly, $|S_{i^*}| \geq 2^n/n$; thus, by the above argument, $G'_f(U_n || |S_{i^*}|)$ is both pseudorandom and has entropy $n' - O(\log n')$. Finally, consider the event $E$ that $i = i^*$ and $s \in S_{i^*}$. By definition, $G(U_{\log n} || U_n || U_m || E)$ is identically distributed to $G'_f(U_{\log n} || S_{i^*} || E)$, and thus $G$ is a cond EP-PRG from any OWF. For clarity, let us provide the full expanded description of the cond EP-PRG $G$:

$$G(i || s || h_1, h_2 || h_{GL}) = h_{GL}(s) || h_1 || h_2 || h_1(s)_{r-O(\log n)} || h_2(f(s))_{n-r-O(\log n)} || h_{GL}(s).$$

Note that this $G$ is not a PRG: if the input $i \neq i^*$ (which happens with probability $1 - \frac{n}{n}$), the output of $G$ may not be pseudorandom! But, recall that the notion of a cond EP-PRG only requires the output of $G$ to be pseudorandom conditioned on some event $E$ (while also being entropy preserving conditioned on the same event $E$).

Finally, the above outline only shows that $K^t$ is mildly HoA if $t(\cdot)$ is larger than running time of the cond EP-PRG that we constructed; that is, so far, we have only shown that OWFs imply that $K^t$ is mildly HoA for some polynomial $t$. To prove that this holds for every $t(n) \geq (1+\epsilon)n$, $\epsilon > 0$, we remark that using a padding trick, we can also construct a cond EP-PRG that can be computed in time $n + O(n')$, where $\alpha < 1$—we refer to this as a rate-$1$ efficient PRG. Using such a rate-1 efficient cond EP-PRG, we can show that $K^t$ is mildly HoA for every $t(n) \geq (1+\epsilon)n$, $\epsilon > 0$.

**II. PRELIMINARIES**

We assume familiarity with basic concepts such as Turing machines, polynomial-time algorithms and probabilistic-polynomial-time algorithms (PPT). A function $\mu$ is said to be negligible if for every polynomial $p(\cdot)$ there exists some $n_0$ such that for all $n > n_0$, $\mu(n) \leq \frac{1}{p(n)}$. A probability ensemble is a sequence of random variables $A = \{A_n\}_{n \in \mathbb{N}}$. We let $U_n$ the uniform distribution over $\{0,1\}^n$.

**A. One-way Functions**

We recall the definition of one-way functions [13]. Roughly speaking, a function $f$ is one-way if it is polynomial-time computable, but hard to invert for PPT attackers.

**Definition 3.** Let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be a polynomial-time computable function. $f$ is said to be a one-way function (OWF) if for every PPT algorithm $A$, there exists a negligible function $\mu$ such that for all $n \in \mathbb{N}$, $\Pr[x \leftarrow \{0,1\}^n; y = f(x) : A(1^n, y) \in f^{-1}(f(x)) \leq \mu(n)]$.

We may also consider a weaker notion of a weak one-way function [50], where we only require all PPT attackers to fail with probability noticeably bounded away from 1:

**Definition 4.** Let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be a polynomial-time computable function. $f$ is said to be a $\alpha$-weak one-way function ($\alpha$-weak OWF) if for every PPT algorithm $A$, for all sufficiently large $n \in \mathbb{N}$, $\Pr[x \leftarrow \{0,1\}^n; y = f(x) : A(1^n, y) \in f^{-1}(f(x)) \leq 1-\alpha(n)]$.

We say that $f$ is simply a weak one-way function (weak OWF) if there exists some polynomial $q > 0$ such that $f$ is a $\frac{1}{q(\cdot)}$ weak OWF.
Yao’s hardness amplification theorem [50] shows that any weak OWF can be turned into a (strong) OWF.

**Theorem 5** ([50]). Assume there exists a weak one-way function. Then there exists a one-way function.

**B. Time-bounded Kolmogorov Complexity**

Let $U$ be some fixed Universal Turing machine that can emulate any Turing machine $M$ with polynomial overhead. Given a description $\Pi \in \{0, 1\}^*$ which encodes a pair $(M, w)$ where $M$ is a (single-tape) Turing machine and $w \in \{0, 1\}^*$ is an input, let $U(\Pi, 1^t)$ denote the output of $M(w)$ when evaluated on $U$ for $t$ steps. Note that (by assumption that $U$ only has polynomial overhead) $U(\Pi, 1^t)$ can be computed in time $\text{poly}(d, t)$.

The $t$-time bounded Kolmogorov Complexity, $K^t(x)$, of a string $x$ [33], [34], [46], [49] is defined as the length of the shortest description $\Pi$ such that $U(\Pi, 1^t) = x$:

$$K^t(x) = \min_{\Pi \in \{0, 1\}^*} \{|\Pi| : U(\Pi, 1^{|x|}) = x\}.$$

A central fact about $K^t$-complexity is that the length of a string $x$ essentially (up to an additive constant) bounds the $K^t$-complexity of the string for every $t(n) > 0$ [12], [34], [48] (see e.g., [47] for simple treatment). This follows by considering $\Pi = (M, x)$ where $M$ is a constant-length Turing machine that directly halts; consequently, $M$ simply outputs its input and thus $M(x) = x$.

**Fact 1.** There exists a constant $c$ such that for every function $t(n) > 0$ and every $x \in \{0, 1\}^*$ it holds that $K^t(x) \leq |x| + c$.

**C. Average-case Hard Functions**

We turn to defining what it means for a function to be average-case hard (for PPT algorithms).

**Definition 6.** We say that a function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is $\alpha$-hard-on-average ($\alpha$-HoA) if for all PPT heuristic $\mathcal{H}$, for all sufficiently large $n \in \mathbb{N}$,

$$\Pr[x \leftarrow \{0, 1\}^n : \mathcal{H}(x) = f(x)] < 1 - \alpha(n).$$

In other words, there does not exist a PPT “heuristic” $\mathcal{H}$ that computes $f$ with probability $1 - \alpha(n)$ for infinitely many $n \in \mathbb{N}$. We also consider what it means for a function to be average-case hard to approximate.

**Definition 7.** We say that a function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is $\alpha$ hard-on-average ($\alpha$-HoA) to $\beta$-approximate if for all PPT heuristic $\mathcal{H}$, for all sufficiently large $n \in \mathbb{N}$,

$$\Pr[x \leftarrow \{0, 1\}^n : |\mathcal{H}(x) - f(x)| \leq \beta(|x|)] < 1 - \alpha(n).$$

Finally, we refer to a function $f$ as being mildly HoA (resp HoA to approximate) if there exists a polynomial $p(\cdot) > 0$ such that $f$ is $\frac{1}{p(\cdot)}$-HoA (resp. HoA to approximate).

**D. Computational Indistinguishability**

We recall the definition of (computational) indistinguishability [20].

**Definition 8.** Two ensembles $\{A_n\}_{n \in \mathbb{N}}$ and $\{B_n\}_{n \in \mathbb{N}}$ are said to be $\mu(\cdot)$-indistinguishable, if for every probabilistic machine $D$ (the “distinguisher”) whose running time is polynomial in the length of its first input, there exists some $n_0 \in \mathbb{N}$ so that for every $n \geq n_0$:

$$|\Pr[D(1^n, A_n) = 1] - \Pr[D(1^n, B_n) = 1]| < \mu(n)$$

We say that are $\{A_n\}_{n \in \mathbb{N}}$ and $\{B_n\}_{n \in \mathbb{N}}$ simply indistinguishable if they are $1/\text{poly}(\cdot)$-indistinguishable for every polynomial $p(\cdot)$.

**E. Statistical Distance and Entropy**

For any two random variables $X$ and $Y$ defined over some set $\mathcal{V}$, we let $SD(X, Y) = \frac{1}{2} \sum_{v \in \mathcal{V}} |\Pr[X = v] - \Pr[Y = v]|$ denote the statistical distance between $X$ and $Y$. For a random variable $X$, let $H(X) = \mathbb{E}[\log \frac{1}{\Pr[X = x]}]$ denote the (Shannon) entropy of $X$, and let $H_\infty(X) = \min_{x \in \text{supp}(X)} \log \frac{1}{\Pr[X = x]}$ denote the min-entropy of $X$.

We next demonstrate a simple lemma showing that any distribution that is statistically close to random, has very high Shannon entropy.

**Lemma 2.** For every $n \geq 4$, the following holds. Let $X$ be a random variable over $\{0, 1\}^n$ such that $SD(X, U_n) \leq \frac{1}{n^2}$. Then $H(X) \geq n - 2$.

**Proof:** Let $S = \{x \in \{0, 1\}^n : \Pr[X = x] \leq 2^{-n-1}\}$. Note that for every $x \notin S$, $x$ will contribute at least

$$\frac{1}{2} \left( \Pr[X = x] - \frac{\Pr[U = x]}{2} \right) = \frac{\Pr[X = x]}{4}$$

to $SD(X, U_n)$. Thus,

$$\Pr[X \notin S] \leq 4 \cdot \frac{1}{n^2}.$$

Since for every $x \in S$, $\log \frac{1}{\Pr[X = x]} \geq n - 1$ and the probability that $X \in S$ is at least $1 - 4/n^2$, it follows that

$$H(X) \geq \Pr[X \in S](n-1) + (1 - \frac{4}{n^2})(n-1) \geq n - \frac{4}{n} - 1 \geq n - 2.$$

$\blacksquare$
III. The Main Theorem

Theorem 9. The following are equivalent:

(a) The existence of one-way functions.
(b) The existence of a polynomial $t(n) > 0$ such that $K^t$ is mildly hard-on-average.
(c) For all constants $d > 0, \varepsilon > 0$, and every polynomial $t(n) \geq (1+\varepsilon)n$, $K^t$ is mildly hard-on-average to $(d \log n)$-approximate.

We prove Theorem 9 by showing that (b) implies (a) (in Section IV) and next that (a) implies (c) (in Section V). Finally, (c) trivially implies (b).

Note that a consequence of 9 is that for every polynomial $t(n) \geq (1+\varepsilon)n$, where $\varepsilon > 0$ is a constant $t(n)$, mild average-case hardness of $K^t$ is equivalent to the existence of one-way functions.

IV. OWFs from Mild AVG-case K$^t$-Hardness

In this section, we state our main theorem.

Theorem 10. Assume there exist polynomials $t(n) > 0, p(n) > 0$ such that $K^t$ is $1/n^c$-HoA. Then there exists a weak OWF $f$ (and thus also a OWF).

Proof: Let $c$ be the constant from Fact 1. Consider the function $f : \{0,1\}^{\log(n+c)} \to \{0,1\}^*$, which given an input $\Pi' \in \Pi'$, where $|\Pi'| = |\log(n+c)|$ and $|\Pi'| = n+c$, outputs $\Pi / \Pi'$ where $\Pi$ is the $\ell$-bit prefix of $\Pi'$. This function is only defined over some input lengths, but by an easy padding trick, it can be transformed into a function $f'$ defined over all input lengths, such that if $f$ is (weakly) one-way (over the restricted input lengths), then $f'$ will be (weakly) one-way (over all input lengths): $f'(x')$ simply truncates its input $x'$ (as little as possible) so that the (truncated) input $x$ now becomes of length $m = n + c + \lceil \log(n+c) \rceil$ for some $n$ and outputs $f(x)$.

We now show if $K^t$ is $1/n^c$-HoA, then $f$ is a $1/q(n)$-weak OWF, where $q(n) = 2^{2c+2n^p(n)}$, which concludes the proof of the theorem. Assume for contradiction that $f$ is not a $1/q(n)$-weak OWF. That is, there exists some PPT attacker $A$ that inverts $f$ with probability at least $1 - \frac{1}{q(n)} = 1 - \frac{1}{q(m)}$ for infinitely many $m = n + c + \lceil \log(n+c) \rceil$. Fix some such $m, n > 2$.

By an averaging argument, except for a fraction $\frac{1}{2p(n)}$ of random tapes $r$ for $A$, the deterministic machine $A_r$ (i.e., machine $A$ with randomness fixed to $r$) fails to invert $f$ with probability at most $\frac{2p(n)}{q(n)}$. Fix some such “good” randomness $r$ for which $A_r$ succeeds to invert $f$ with probability $1 - \frac{1}{2p(n)q(n)}$.

We next show how to use $A_r$ to compute $K^t$ with high probability over random inputs $z \in \{0,1\}^n$. Our heuristic $H_r(z)$ runs $A_r(i|x)$ for all $i \in [n+c]$ where $i$ is represented as a $\lceil \log(n+c) \rceil$ bit string, and outputs the length of the smallest program $\Pi$ output by $A_r$ that produces the string $z$ within $t(n)$ steps. Let $S$ be the set of strings $z \in \{0,1\}^n$ for which $H_r(z)$ fails to compute $K^t(z)$. Note that $H_r$ thus fails with probability

$$f_{\text{fail}} = \frac{|S|}{2^n}.$$

Consider any string $z \in S$ and let $w = K^t(z)$ be its $K^t$-complexity. By Fact 1, we have that $w \leq n + c$. Since $H_r(z)$ fails to compute $K^t(z)$, $A_r$ must fail to invert $(w||z)$. But, since $w \leq n + c$, the output $(w||z)$ is sampled with probability

$$\frac{1}{n+c} \cdot \frac{1}{2w} \geq \frac{1}{(n+c)} \cdot \frac{1}{2n+c} \geq \frac{1}{n^2c+1} \cdot \frac{1}{2^n}$$

in the one-way function experiment, so $A_r$ must fail with probability at least

$$\frac{|S|}{n^2c+1} \cdot \frac{1}{2^n} = \frac{f_{\text{fail}}}{n^2c+1},$$

which by assumption (that $A_r$ is a good inverter) is at most that $\frac{2p(n)}{q(n)}$. We thus conclude that

$$f_{\text{fail}} \leq \frac{2^{2c+2np(n)}}{q(n)}.$$

Finally, by a union bound, we have that $H$ (using a uniform random tape $r$) fails in computing $K^t$ with probability at most

$$\frac{1}{2p(n)} + \frac{2^{2c+2np(n)}}{q(n)} = \frac{1}{2p(n)} + \frac{2^{2c+2np(n)}}{2c+3np(n)^2} = \frac{1}{2p(n)}.$$

Thus, $H$ computes $K^t$ with probability $1 - \frac{1}{2p(n)}$ for infinitely many $n \in \mathbb{N}$, which contradicts the assumption that $K^t$ is $1/n^c$-HoA.

V. Mild AVG-case K$^t$-Hardness from OWFs

We introduce the notion of a (conditionally-secure) entropy-preserving pseudo-random generator (EP-PRG) and next show (1) the existence of a condEP-PRG implies that $K^t$ is hard-on-average (even to approximate), and (2) OWFs imply condEP-PRGs.

A. Entropy-preserving PRGs

We start by defining the notion of a conditionally-secure entropy-preserving PRG.

Definition 11. An efficiently computable function $G : \{0,1\}^n \to \{0,1\}^{n+\gamma \log n}$ is a $\mu$-conditionally secure entropy-preserving pseudorandom generator ($\mu$-condEP-PRG) if there exist a sequence of events $\{E_n\}_{n \in \mathbb{N}}$ and a constant $\alpha$ (referred to as the entropy-loss constant) such that the following conditions hold:

- (pseudorandomness): $\{G(U_n | E_n)\}_{n \in \mathbb{N}}$ and $\{U_{n+\gamma \log n}\}_{n \in \mathbb{N}}$ are $\mu(n)$-indistinguishable;
- (entropy-preserving): For all sufficiently large $n \in \mathbb{N}$, $H(G(U_n | E_n)) \geq n - \alpha \log n$. 

1249
If all \( n, E_n = \{0, 1\}^n \) (i.e., there is no conditioning), we say that \( G \) is an \( \mu \)-secure entropy-preserving pseudorandom generator (\( \mu \)-EP-PRG).

We say that \( G \) has rate-1 efficiency if its running time on inputs of length \( n \) is bounded by \( n + \Theta(n^\varepsilon) \) for some constant \( \varepsilon < 1 \).

B. Avg-case \( K^t \)-Hardness from Cond EP-PRGs

**Theorem 12.** Assume that for every \( \gamma > 1 \), there exists a rate-1 efficient \( \mu \)-condEP-PRG \( G : \{0, 1\}^n \rightarrow \{0, 1\}^{n+\gamma \log n} \) where \( \mu(n) = 1/n^2 \). Then, for every constant \( d > 0, \varepsilon > 0 \), for every polynomial \( t(n) \geq (1+\varepsilon)n \), \( K^t \) is mildly hard-on-average to \( (d \log n) \)-approximate.

**Proof:** Let \( \gamma \geq \max(8, 8d) \), and let \( G' : \{0, 1\}^n \rightarrow \{0, 1\}^{m(n)} \) where \( m(n) = n + \gamma \log n \) be a rate-1 efficient \( \mu \)-condEP-PRG, where \( \mu = 1/n^2 \). For any constant \( c \), let \( G''(x) \) be a function that computes \( G'(x) \) and truncates the last \( c \) bits. It directly follows that \( G'' \) is also a rate-1 efficient \( \mu \)-condEP-PRG (since \( G'' \) is so). Consider any \( \varepsilon > 0 \) and any polynomial \( t(n) \geq (1+\varepsilon)n \) and let \( p(n) = 2n^{2(\varepsilon+1)} \).

Assume for contradiction that there exists some PPT \( \mathcal{H} \) that \( \beta \)-approximates \( K^t \) with probability \( 1 - 1/p(m) \) for infinitely many \( m \in \mathbb{N} \), where \( \beta(n) = \gamma/8 \log n \geq d \log n \). Since \( m(n+1) - m(n) \leq \gamma + 1 \), there must exist some constant \( c \leq \gamma + 1 \) such that \( \mathcal{H} \) succeeds to \( \beta \)-approximate \( K^t \) with probability \( 1 - 1/p(m) \) for infinitely many of the form \( m = m(n) = n + \gamma \log n - c \). Let \( G(x) = G''(x) \); recall that \( G \) is a rate-1 efficient \( \mu \)-condEP-PRG (trivially, since \( G'' \) is so), and let \( \alpha \), \( \{E_n\} \), respectively, be the entropy loss constant and sequence of events, associated with it.

We next show that \( \mathcal{H} \) can be used to break the condEP-PRG \( G \). Towards this, recall that a random string has high \( K^t \)-complexity with high probability: for \( m = m(n) \), we have,

\[
\Pr_{x \in \{0, 1\}^m} [K^t(x) \geq m - \gamma/4 \log n] \\
\geq 2^{-m - \gamma/2 \log n} = 1 - \frac{1}{n^{\gamma/4}},
\]

since the total number of Turing machines with length smaller than \( m - \gamma/2 \log n \) is only \( 2^{m - \gamma/2 \log n} \). However, any string output by the EP-PRG, must have “low” \( K^t \) complexity: For every sufficiently large \( n, m = m(n) \), we have that,

\[
\Pr_{s \in \{0, 1\}^n} [K^t(G(s)) \geq m - \gamma/2 \log n] = 0,
\]

since \( G(s) \) can be represented by combining a seed \( s \) of length \( n \) with the code of \( G \) (of constant length), and the running time of \( G(s) \) is bounded by \( t(|s|) = t(n) \leq t(m) \) for all sufficiently large \( n \), so \( K^t(G(s)) = n + \Theta(1) = (m - \gamma/2 \log n - c) + \Theta(1) \approx m - \gamma/2 \log n \) for sufficiently large \( n \).

Based on these observations, we now construct a PPT distinguisher \( \mathcal{A} \) breaking \( G \). On input \( 1^n, x \), where \( x \in \{0, 1\}^m \), \( \mathcal{A}(1^n, x) \) lets \( w \leftarrow \mathcal{H}(x) \) and outputs 1 if \( w \geq m(n) - \gamma/2 \log n \) and 0 otherwise. Fix some \( n \) and \( m = m(n) \) for which \( \mathcal{H} \) succeeds with probability \( 1/p(m) \). The following two claims conclude that \( \mathcal{A} \) distinguishes \( U_{m(n)} \) and \( G(U_n | E_n) \) with probability at least \( 1/n \).

**Claim 1.** \( \mathcal{A}(1^n, U_n) \) outputs 1 with probability at least \( 1 - 2/n^{\gamma/4} \).

**Proof:** Note that \( \mathcal{A}(1^n, x) \) will output 1 if \( x \) is a string with \( K^t \)-complexity larger than \( m - \gamma/4 \log n \) and \( \mathcal{H} \) outputs a \( \gamma/8 \log n \)-approximation to \( K^t(x) \). Thus,

\[
\Pr[\mathcal{A}(1^n, x) = 1] \\
\geq \Pr[K^t(x) \geq m - \gamma/4 \log n \wedge \mathcal{H} \text{ succeeds on } x] \\
\geq 1 - \Pr[K^t(x) < m - \gamma/4 \log n] - \Pr[\mathcal{H} \text{ fails on } x] \\
\geq 1 - \frac{1}{n^{\gamma/4}} - \frac{1}{p(n)} \\
\geq 1 - \frac{2}{n^{\gamma/4}}.
\]

where the probability is over a random \( x \leftarrow U_n \) and the randomness of \( \mathcal{A} \) and \( \mathcal{H} \).

**Claim 2.** \( \mathcal{A}(1^n, G(U_n | E_n)) \) outputs 1 with probability at most \( 1 - \frac{1}{n} + \frac{1}{n^{\gamma/4}} \).

**Proof:** Recall that by assumption, \( \mathcal{H} \) fails to \( (\gamma/8 \log n) \)-approximate \( K^t(x) \) for a random \( x \in \{0, 1\}^m \) with probability at most \( 1/p(m) \). By an averaging argument, for at least a \( 1 - \frac{1}{n^{\gamma/4}} \) fraction of random tapes \( r \) for \( \mathcal{H} \), the deterministic machine \( \mathcal{H}_r \) fails to approximate \( K^t \) with probability at most \( 1/p(m) \). Fix some “good” randomness \( r \) such that \( \mathcal{H}_r \) approximates \( K^t \) with probability at least \( 1 - \frac{1}{n^{\gamma/4}} \). We next analyze the success probability of \( \mathcal{A}_r \). Assume for contradiction that \( \mathcal{A}_r \) outputs 1 with probability at least \( 1 - \frac{1}{n} + \frac{1}{n^{\gamma/4}} \) on input \( G(U_n | E_n) \). Recall that (1) the entropy of \( G(U_n | E_n) \) is at least \( n - \alpha \log n \) and (2) the quantity \( -\log \Pr[G(U_n | E_n) = y] \) is upper bounded by \( n \) for all \( y \in G(U_n | E_n) \) since \( H_\infty(G(U_n | E_n)) \leq H_\infty(U_n | E_n) = n. \) By an averaging argument, with probability at least \( \frac{1}{n} \), a random \( y \in G(U_n | E_n) \) will satisfy

\[
-\log \Pr[G(U_n | E_n) = y] \geq (n - \alpha \log n) - 1.
\]

We refer to an output \( y \) satisfying the above condition as being “good” and other \( y \’s \) as being “bad”. Let \( S = \{y \in G(U_n | E_n) : \mathcal{A}_r(1^n, y) = 1 \land y \text{ is good}\} \), and let \( S^\prime = \{y \in G(U_n | E_n) : \mathcal{A}_r(1^n, y) = 1 \land y \text{ is bad}\} \).

Since

\[
\Pr[\mathcal{A}_r(1^n, G(U_n | E_n)) = 1] \\
= \Pr[G(U_n | E_n) \in S] + \Pr[G(U_n | E_n) \in S^\prime],
\]

1250
and \( \Pr[G(U_n \mid E_n) \in S] \) is at most the probability that
\( G(U_n) \) is “bad” (which as argued above is at most \( 1 - \frac{1}{n^2} \)),
we have that
\[
\Pr[G(U_n \mid E_n) \in S] \\
\geq \left(1 - \frac{1}{n} + \frac{1}{n^{\alpha + \gamma}}\right) - \left(1 - \frac{1}{n}\right) = \frac{1}{n^{\alpha + \gamma}}.
\]
Furthermore, since for every \( y \in S \), \( \Pr[G(U_n \mid E_n) = y] \leq 2^{-n+a \log n+1} \), we also have,
\[
\Pr[G(U_n \mid E_n) \in S] \leq |S|2^{-n+a \log n+1}
\]
So,
\[
|S| \geq \frac{2^{n-a \log n-1}}{n^{\alpha+\gamma}} = 2^{n-(2\alpha + \gamma) \log n - 1}
\]
However, for any \( y \in G(U_n \mid E_n) \), if \( \mathcal{A}_r(1^n, y) \) outputs 1, then by Equation 3, \( H_r(y) > K^t(y) + \gamma/8 \), so \( H \)
fails to output a good approximation. (This follows, since by Equation 3, \( K^t(y) < n - \gamma/2 \log n \) and \( \mathcal{A}_r(1^n, y) \) outputs 1 only if \( H_r(y) \geq n - \frac{\gamma}{8} \log n \).

Thus, the probability that \( H_r \) fails (to output a good approximation) on a random \( y \in \{0,1\}^m \) is at least
\[
|S|/2^m = \frac{2^{n-(2\alpha + \gamma) \log n - 1}}{2^{\alpha + \gamma} \log n - \alpha} \geq 2^{-2(\alpha + \gamma) \log n - 1} = \frac{1}{2n^2(\alpha + \gamma)}
\]
which contradicts the fact that \( H_r \) fails with approximate
\( K^t \) probability at most \( \frac{n^2}{2\log n} < \frac{1}{2n^2(\alpha + \gamma)} \) (since \( n < m \)).

We conclude that for every good randomness \( r \), \( \mathcal{A}_r \) outputs 1 with probability at most \( 1 - 1/n + 1/n^{\alpha + \gamma} \). Finally, by union bound (and since a random tape is bad with probability \( \leq 1/n^2 \)), we have that the probability that \( \mathcal{A}(G(U_n \mid E_n)) \) outputs 1 is at worst
\[
\frac{1}{n^2} + \left(1 - \frac{1}{n} + \frac{1}{n^{\alpha + \gamma}}\right) \leq 1 - \frac{1}{n} + \frac{2}{n^2},
\]
since \( \gamma \geq 2 \).

We conclude, recalling that \( \gamma \geq 8 \), that \( \mathcal{A} \) distinguishes
\( U_n \) and \( G(U_n \mid E_n) \) with probability of at least
\[
\left(1 - \frac{2}{n^{\gamma/2}}\right) - \left(1 - \frac{1}{n} + \frac{2}{n^2}\right) \\
\geq \left(1 - \frac{2}{n^{\gamma/2}}\right) - \left(1 - \frac{1}{n} + \frac{2}{n^2}\right) = \frac{1}{n} - \frac{4}{n^2} \geq \frac{1}{n^2}
\]
for infinitely many \( n \in \mathbb{N} \).

C. Cond EP-PRGs from OWFs

In this section, we show how to construct a condEP-PRG from any OWF. Towards this, we first recall the
construction of [16], [26], [51] of a PRG from a regular
one-way function [18].

Definition 13. A function \( f : \{0,1\}^* \to \{0,1\}^* \) is called
regular if there exists a function \( r : \mathbb{N} \to \mathbb{N} \) such that for all sufficiently long \( x \in \{0,1\}^* \),
\[
2^{r(|x|)} - 1 \leq |f^{-1}(f(x))| \leq 2^{r(|x|)}.
\]
We refer to \( r \) as the regularity of \( f \).

As mentioned in the introduction, the construction proceeds in the following two steps given a OWF \( f \) with
regularity \( r \).

- We “massage” \( f \) into a different OWF \( \tilde{f} \) having the
property that there exists some \( \ell(n) = n - O(\log n) \) such that \( \tilde{f}(U_n) \) is statistically close to \( U_{\ell(n)} \)—
we will refer to such a OWF as being dense. This is done by applying pairwise-independent hash functions
(acting as strong extractors) to both the input and the output of the OWF (parametrized to match the
regularity \( r \)) to “squeeze” out randomness from both the input and the output.

\[
\tilde{f}(s||s_1||s_2) = \sigma_1||\sigma_2||h_{\sigma_1}(s)||h_{\sigma_2}(\tilde{f}(s))||\sigma_3||\sigma_4
\]
where \( [a]_j \) means a truncated to \( j \) bits.

- We next modify \( \tilde{f} \) to include additional randomness
in the input (which is also revealed in the output) to make sure the function has a hardcore function:
\[
f'(s||s_1||s_2||\sigma_{GL}) = \sigma_{GL}||\tilde{f}(s)||\sigma_1||\sigma_2
\]
We note that the above steps do not actually produce a
“fully secure” PRG as the statistical distance between the
output of \( f(U_n) \) and uniform is only \( \frac{1}{\text{poly}(m)} \) as opposed to being negligible. [16] thus presents a final amplification
step to deal with this issue—for our purposes it will suffice to get a \( \frac{1}{\text{poly}(m)} \) indistinguishability gap so we will
not be concerned about the amplification step.

We remark that nothing in the above steps requires \( f \) to be a one-way function defined on the domain
\( \{0,1\}^m \)— all three steps still work even for one-way functions defined over domains \( S \) that are
different than \( \{0,1\}^n \), as long as a lower bound on the size of the domain is efficiently computable (by a minor
modification of the construction in Step 1 to account
for the size of \( S \)). Let us start by formalizing this fact.

Definition 14. Let \( S = \{S_n\} \) be a sequence of sets
such that \( S_n \subseteq \{0,1\}^n \) and let \( f : S_n \to \{0,1\}^* \) be
a polynomial-time computable function. \( f \) is said to be a
one-way function over \( S \) (S-OWF) if for every PPT
algorithm \( \mathcal{A} \), there exists a negligible function \( \mu \) such that
for all \( n \in \mathbb{N} \),
\[
\Pr[x \leftarrow S_n; y = f(x) : \mathcal{A}(1^n, y) \in f^{-1}(f(x))] \leq \mu(n)
\]
We refer to \( f \) as being regular if it satisfies Definition 13
with the exception that we only quantify over all \( n \in \mathbb{N} \)
and all \( x \in S_n \) (as opposed to all \( x \in \{0,1\}^n \)).
We say that a family of functions $\{f_i\}_{i \in I}$ is efficiently computable if there exists a polynomial-time algorithm $M$ such that $M(i, x) = f_i(x)$.

**Lemma 3** (implicit in [16, 51]). Let $S = \{S_n\}$ be a sequence of sets such that $S_n \subseteq \{0, 1\}^n$, let $s$ be an efficiently computable function such that $s(n) \leq \log |S_n|$, and let $f$ be an $S$-OWF with density $r$. Then, there exists a constant $c \geq 1$ such that for every $\alpha, \gamma > 0$, there exists an efficiently computable family of functions $\{f_i\}_{i \in \mathbb{N}}$, and an efficiently computable function $GL$, such that the following holds for $\ell(n) = s(n) + 3n^c - 2\alpha' \log n, \ell'(n) = \ell(n) + \gamma' \log n$:

- **density:** For all sufficiently large $n$, the distributions
  - $\{x \leftarrow S_n, \sigma_1, \sigma_2, \sigma_{GL} \leftarrow \{0, 1\}^{n'} : f'_r(x, \sigma_1, \sigma_2, \sigma_{GL})\}$, and
  - $U_{\ell(n)}$
  are $\frac{3}{n^{\alpha'2}}$-close in statistical distance.

- **pseudorandomness:** The ensembles of distributions,
  - $\{x \leftarrow S_n, \sigma_1, \sigma_2, \sigma_{GL} \leftarrow \{0, 1\}^{n'} : f'_r(x, \sigma_1, \sigma_2, \sigma_{GL}) | GL(x, \sigma_1, \sigma_2, \sigma_{GL})\}$, and
  - $\{U_{\ell'}(n)\}_{n \in \mathbb{N}}$
  are $\frac{4}{n^{\alpha'2}}$-indistinguishable.

**Proof:** Given a $r(\cdot)$-regular $S$-OWF $f$, the construction of $f'$ has the form

$$f'(s | \sigma_1 | \sigma_2 | \sigma_{GL}) = \sigma_{GL} | \sigma_1 | \sigma_2 | [h_{\sigma_1}(s)]_{r-\alpha' \log n} | [h_{\sigma_2}(f(s))]_{s(n) - r-\alpha' \log n}$$

where $|x| = n, |\sigma_1| = |\sigma_2| = |\sigma_{c}| = n^c$, and $GL(x, \sigma_1, \sigma_2, \sigma_{GL})$ is simply the Goldreich-Levin hard-core predicate [19] outputting $\gamma' \log n$ inner products between $x$ and vectors in $\sigma_{GL}$. The function $f'_r$ thus maps $n' = n + 3n^c$ bits to $3n^c + s(n) - 2\alpha' \log n$ bits, and once we add the output of $GL$, the total output length becomes $3n^c + s(n) - 2\alpha' \log n + \gamma' \log n$ as required. The proof in [16, 51] directly works to show that $\{f_i\}, GL$ satisfy the requirements stated in the theorem. ■

We additionally observe that every OWF actually is a regular S-OWFs for a sufficiently large $S$.

**Lemma 4.** Let $f$ be an one way function. There exists an integer function $r(\cdot)$ and a sequence of sets $S = \{S_n\}$ such that $S_n \subseteq \{0, 1\}^n$, $|S_n| \geq 2^n / n$, and $f$ is a $S$-OWF with regularity $r$.

**Proof:** The following simple claim is the crux of the proof:

**Claim 3.** For every $n \in \mathbb{N}$, there exists an integer $r_n \in [n]$ such that

$$\Pr[x \leftarrow \{0, 1\}^n : 2^{r_n-1} \leq |f^{-1}(f(x))| \leq 2^{r_n}] \geq \frac{1}{n}.$$  

We refer the reader to the full version for a detailed proof.

**Proof:** For all $i \in [n]$, let

$$w(i) = \Pr[x \leftarrow \{0, 1\}^n : 2^{i-1} \leq |f^{-1}(f(x))| \leq 2^i].$$

Since for all $x$, the number of pre-images that map to $f(x)$ must be in the range of $[1, 2^n]$, we know that $\sum_{i=1}^n w(i) = 1$. By an averaging argument, there must exist some $r_n$ such that $w(r_n) \geq \frac{1}{n}$.

Let $r(n) = r_n$ for every $n \in N$, $S_n = \{x \in \{0, 1\}^n : 2^{r(n)-1} \leq |f^{-1}(f(x))| \leq 2^{r(n)}\}$; regularity of $f$ when the input domain is restricted to $S$ follows directly. It only remains to show that $f$ is a $S$-OWF; this follows directly from the fact that the set $S_n$ are dense in $\{0, 1\}$. More formally, assume for contradiction that there exists a PPT algorithm $A$ that inverts $f$ with probability $\varepsilon(n)$ when the input is sampled in $S_n$. Since $|S_n| \geq 2^n / n$, it follows that $A$ can invert $f$ with probability at least $\varepsilon(n)/n$ over uniform distribution, which is a contradiction (as $f$ is a OWF).

By combining Lemma 3 and Lemma 4, we can directly get an EP-PRG defined over a subset $S$. We next turn to showing how to instead get a $\mu$-conditionally secure EP-PRG that is defined over $\{0, 1\}^n$. The formal proof appears in the full version and we only give the statement of the theorem as below.

**Theorem 15.** Assume that one way functions exist. Then, there exists a polynomial $t_0(\cdot)$ such that for every $\gamma > 1, \delta > 1$, there exists a $(\frac{\gamma}{\delta})$-cond-EP-PRG $G_{\delta, \gamma} : \{0, 1\}^n \rightarrow \{0, 1\}^{n+\gamma \log n}$ with running time bounded by $(\gamma + \delta)t_0(n)$.

We now use a standard padding trick to obtain a rate-1 efficient $\mu$-cond EP-PRG: we simply output the first $n - \ell$ bits unchanged, and next apply a cond EP-PRG on the last $\ell$ bits. Since we only have a cond EP-PRG that satisfies inverse polynomial (as opposed to negligible) indistinguishability, we need to be a bit careful with the choice of the parameters. The formal proof appears in the full version and we only give the statement of the theorem as below.

**Theorem 16.** Assume that one way functions exist. Then, for every $\gamma > 1$, there exists a rate-1 efficient $\mu$-cond EP-PRG $G_{\gamma} : \{0, 1\}^n \rightarrow \{0, 1\}^{n+\gamma \log n}$, where $\mu(n) = 1/n^2$.

**VI. ACKNOWLEDGEMENTS**

We are very grateful to Eric Allender, Kai-min Chung, Naomi Ephraim, Cody Freitag, Johan Håstad, Yuval Ishai, Ilan Komargodski, Rahul Santhanam, and abhi shelat for extremely helpful comments. We are also very grateful to the anonymous FOCS reviewers.

Supported in part by NSF Award SATC-1704788, NSF Award RI-1703846, AFOSR Award FA9550-18-1-0267, and a JP Morgan Faculty Award. This research is based upon work supported in part by the Office of the
Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via 2019-19-020700006. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation therein.

REFERENCES


