Quantum-Proof Extractors: Optimal up to Constant Factors

Kai-Min Chung* Gil Cohen† Thomas Vidick‡ Xiaodi Wu§

Abstract

We give the first construction of a family of quantum-proof extractors that has optimal seed length dependence $O(\log(n/\epsilon))$ on the input length n and error ϵ. Our extractors support any min-entropy $k = \Omega(\log n + \log^{1+\alpha}(1/\epsilon))$ and extract $m = (1-\alpha)k$ bits that are ϵ-close to uniform, for any desired constant $\alpha > 0$. Previous constructions had a quadratically worse seed length or were restricted to very large input min-entropy or very few output bits.

Our result is based on a generic reduction showing that any strong classical condenser is automatically quantum-proof, with comparable parameters. The existence of such a reduction for extractors is a long-standing open question; here we give an affirmative answer for condensers. Once this reduction is established, to obtain our quantum-proof extractors one only needs to consider high entropy sources. We construct quantum-proof extractors with the desired parameters for such sources by extending a classical approach to extractor construction, based on the use of block-sources and sampling, to the quantum setting.

Our extractors can be used to obtain improved protocols for device-independent randomness expansion and for privacy amplification.

1 Introduction

A randomness extractor is a deterministic procedure that extracts almost uniform random bits from a weak source of randomness using a *seed*, a short uniform random string, as a catalyst. Originally introduced as tools for derandomization [36], extractors have found uses and surprising connections in many areas such as pseudorandomness [35, 50], complexity theory [17, 45, 31], cryptography [5, 14], and combinatorics [1, 8, 7] to name a few.

We say that an n-bit random variable X is an (n,k)-source if the min-entropy $H_{\min}(X) \geq k$. For two random variables X, Y we write $X \approx_\epsilon Y$ to mean that the statistical distance between X and Y is at most ϵ. We use U_m to denote a random variable uniformly distributed over m-bit strings. With these definitions in place we can define our main object of study.[1]

Definition 1.1 (Extractor) *A function* $\mathrm{Ext}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is called a* (k,ϵ) extractor *if for any* (n,k)*-source* X, $\mathrm{Ext}(X,S) \approx_\epsilon U_m$, *where* S *is uniformly distributed over* d*-bit strings and independent of* X. Ext *is said to be* strong *if* $(\mathrm{Ext}(X,S),S) \approx_\epsilon (U_m,S)$.

---

[*] Institute of Information Science, Academia Sinica, Taiwan. kmchung@iis.sinica.edu.tw

[†] Computing and Mathematical Sciences Department, Caltech. Supported by a Walter S. Baer and Jeri Weiss CMI Postdoctoral Fellowship. Email: `coheng@caltech.edu`

[‡] Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, USA. vidick@cms.caltech.edu

[§] Department of Computer and Information Science, University of Oregon, Eugene, OR 97403, USA. xiaodiwu@cs.uoregon.edu.

[1] We refer to the preliminaries for more formal definitions.

Depending on the application, different regimes of parameters for extractors are of interest. The general goal is to construct, given any desired integers n, k and $\epsilon > 0$, an extractor with the shortest possible seed length d and longest output length m. Computational aspects aside, one can prove the existence of extractors for any n, k and $\epsilon > 0$ such that $k \geq 2\log(1/\epsilon) + O(1)$ with $m = k - 2\log(1/\epsilon) - O(1)$ output bits and seed length $d = \log(n-k) + 2\log(1/\epsilon) + O(1)$. Further, this is known to be tight [37]. Significant work in the area of pseudorandomness (see e.g. [42, 52]) has led to efficient constructions that come very close to matching the optimal existential parameters. In particular, Guruswami *et. al.* [18] gave a construction for any n, k and $\epsilon > 0$ with seed length $d = O(\log(n/\epsilon))$ and output length $m = 0.99k$.

Applications of extractors to cryptography motivate a slightly different perspective on the definition. Consider the task of privacy amplification [5, 29, 3]. Two parties, Alice and Bob, are assumed to share an initial secret that is "somewhat random" from the point of view of a computationally unbounded adversary Eve. Alice and Bob can communicate over a public channel on which Eve may (passively) eavesdrop. Their goal is to agree on an m-bit string R that is ϵ-close to uniform even conditioned on all information available to Eve. It is not hard to see that this can be solved by using a strong randomness extractor: Alice chooses a random seed, communicates it to Bob, and they both evaluate the extractor on their initial shared secret. The protocol will achieve the desired task *provided* both the input and output conditions for the extractor are measured conditioned on the adversary's side information E: it is required that, for any X (the initial secret) such that $H_{\min}(X|E) \geq k$, the output condition $(\mathrm{Ext}(X,S), S, E) \approx_\epsilon (U_m, S, E)$ holds.

1.1 Quantum-proof extractors

The ubiquitous use of privacy amplification in quantum (as well as post-quantum) cryptography prompts the question of constructing extractors in the presence of quantum adversaries, who may possess quantum side information E about the source. The fundamental problem thus becomes the following.

Problem 1. Construct a quantum-proof extractor with parameters comparable to known constructions of extractors in the classical setting.

The existential arguments, based on the probabilistic method, used to delineate optimal parameter regimes for classical extractors are not known to extend to the quantum setting. Nevertheless, taking an optimistic stance, a very direct approach to solving Problem 1 would be to establish that any classical extractor is automatically quantum-proof with comparable parameters.

Problem 2. Is any classical extractor also quantum-proof (up to some parameter loss)?

Aside from being a natural question in extractor theory, Problem 2 reaches deep into what is perhaps the most fundamental problem in quantum information theory — *what is the information content of a quantum state?* From Holevo's theorem [20] to bounds on quantum random access codes [33] through a host of measures of quantum conditional entropy [32], the question is continuously being probed from different angles, and we believe that extractors can provide one of the most fruitful approaches to the problem.

Both problems outlined above have been extensively studied in the literature. Regarding Problem 2, the work of [25] proves that any (k, ϵ) classical strong extractor with one-bit output is also a $(k + \log(1/\epsilon), O(\sqrt{\epsilon}))$ strong quantum-proof extractor. Combining this result with the quantum version of the XOR lemma [21] it is possible to show that any (k, ϵ) classical strong extractor is a $(k + \log(1/\epsilon), O(2^m \sqrt{\epsilon}))$ strong quantum-proof extractor. Using a connection with operator space theory, the recent work of [6] further shows that any (k, ϵ) classical strong extractor is a $(k + \log(2/\epsilon), O(2^{m/2}\sqrt{\epsilon}))$, as well as a $(k + 1, O(2^{n-k}\epsilon))$ strong quantum-proof extractor. Obtaining results without the exponential blow-up in the output length or input entropy deficit, however, has proven challenging; preventing such loss is crucial for applications to tasks such as privacy amplification.

The single counter-example known to a direct reduction is due to Gavinsky *et. al.* [16] and implies that some loss in parameters is unavoidable. The implied loss, however, lies in a range of parameters that is not the most relevant for typical applications, so that a partial solution to Problem 2 remains possible.

Regarding Problem 1, current results are limited to several specific constructions of extractors, such as two-universal hashing [48] or Trevisan's extractor [12], which can be shown quantum-proof with little loss in parameters compared to the classical setting. In particular, for general min-entropy k and $\epsilon > 0$, explicit quantum-proof extractors with seed length $d = O(\frac{\log^2(n/\epsilon)}{\log k})$ and $m = k^{0.99}$ output bits are known.[2] These constructions remain far from optimal; while a quadratic loss in the seed length may be tolerable in many applications, for others, such as exponential randomness amplification, it can lead to much more stringent limitations.

1.2 Our contribution

In this work we make progress on both problems. First, we consider the analog of Problem 1 for *condensers.*

Definition 1.2 (Condenser) *A function* Cond: $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is called a* (k, k', ϵ) condenser *if for any* (n, k)*-source* X*,* $\mathrm{Cond}(X, S) \approx_\epsilon Z$ *where* $H_{\min}(Z) \geq k'$*.* Cond *is said to be* strong *if* $(\mathrm{Cond}(X, S), S) \approx_\epsilon (Z, S)$ *where* $H_{\min}(Z|S) \geq k'$*.*

Note that for an m-bit random variable Z, $H_{\min}(Z) = m$ if and only if $Z = U_m$, thus a (k, m, ϵ) condenser is a (k, ϵ) extractor. A condenser is a weakening of an extractor where the output is only required to be close to a high-entropy random variable. As indicated by their name, interesting condensers are typically ones for which the output has higher min-entropy rate (entropy divided by length) than the input: $k'/m \gg k/n$. As a weaker object, condensers are central building blocks in the construction of extractors. In fact, they are key to all best constructions of known extractors [18, 15, 47]. Beyond their use as a building block, condensers have found many further applications [26, 27, 28, 9].

Our first contribution is an affirmative answer to Problem 2 in the setting of condensers. As for the setting of extractors, we term a condenser *quantum-proof* if both the input and output min-entropy conditions are measured conditional on an arbitrary quantum system E. Informally, we show that any classical condenser is also quantum-proof, with only a factor-$1/2$ loss in the output entropy rate.

Theorem 1.3 *Let* Cond *be a strong* (k, k', ϵ) *condenser. Then* Cond *is also a strong* $(k, k'/2 - O(\log(1/\epsilon)), O(\epsilon))$ *quantum-proof condenser.*

---

[2] It is also possible to extract essentially all the input min-entropy, but the seed length becomes $O(\log^2(n/\epsilon)\log m)$ [12, Corollary 5.3].

We remark that any (k, k', ϵ) condenser with seed length d is automatically a *strong* $(k, k' - d - O(\log(1/\epsilon)), O(\epsilon))$ condenser [10], and so the assumption of Theorem 1.3 that Cond is strong can be removed without a significant effect. By applying Theorem 1.3 to a construction from [18] we obtain the following construction of a strong quantum-proof condenser, which is geared towards optimizing the output min-entropy rate.

Corollary 1.4 *For any constant $\delta \in (0,1)$, any integers $k \leq n$, and any $\epsilon > 0$, there is an explicit strong $(k, k/2 - \log(4/\epsilon), \epsilon)$ quantum-proof condenser* Cond: $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with seed length $d = (1+\delta) \cdot \log(nk/\epsilon^4) + O(1)$ and $m \leq (1+\delta^{-1})k + 2d$.*

To the best of our knowledge this is the first non-trivial construction of a quantum-proof condenser — and it reaches almost-optimal parameters!

As mentioned earlier, condensers form one of the main building blocks in many of the best constructions of extractors known. Our second main result consists in showing that a classical approach to extractor constructions due to [36, 41, 57], based on the use of block-sources and sampling, can also be made quantum-proof. By combining the result (see Theorem 4.6 in Section 4) with our Theorem 1.3 we obtain the first explicit construction of a family of quantum-proof extractors that is optimal, up to constant factors, both in terms of seed length and output length.

Theorem 1.5 *For any constant $0 < \alpha < 1$, integers n, k and $\epsilon > 0$ such that $k = \Omega(\log n + \log^{1+\alpha}(1/\epsilon))$ there exists an explicit (k, ϵ) quantum-proof strong extractor* Ext : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with seed length $d = O(\log(n/\epsilon))$ and output length $m = (1-\alpha)k$.*

Theorem 1.5 is proved in Section 4.3. The theorem significantly improves upon previous work on quantum-proof extractors. A substantial line of prior works establish quantum-proof security of several classical extractors [22, 39, 40, 25, 46, 13, 12, 2], but none of them reach the optimal parameters up to constant factors. In particular, $O(\log(n/\epsilon))$ seed length has only been shown achievable either for extractors with short (shorter than the seed) output [25, 6], or for extractors that only work for high input min-entropy rate or high error. For instance, as mentioned earlier Trevisan's extractor has seed length $d = O(\frac{\log^2(n/\epsilon)}{\log k})$ (with output length $m = k^{0.99}$ in this case). Thus, it has seed length $O(\log(n/\epsilon))$ only for $k \geq n^{\Omega(1)}$ and $\epsilon \geq 1/\mathrm{poly}(n)$, and has a quadratic loss in general. A different instantiation of Trevisan's extractor due to Ben-Aroya and Ta-Shma [2] can achieve seed length $O(\log(n/\epsilon))$ for the same range of ϵ as our Theorem 1.5, but is restricted to large min-entropy rates, $k > (1/2 + \gamma)n$ for $\gamma > 0$.

1.3 Applications

Aside from their intimate connection to fundamental questions on the information content of quantum states, quantum-proof extractors have found significant applications in quantum cryptography, in particular to the task of privacy amplification in quantum key distribution (QKD) [4, 3] and to device-independent randomness expansion [53, 30]. For the former, by replacing Trevisan's extractor [12] with ours leads to improved protocols in terms of communication complexity and entropy loss. The significance of the improvement depends on the assumption one is willing to make on the availability of trusted randomness to the honest parties; here the practical bottlenecks are admittedly often more tied to the computational effort than to the generation of random bits.

The relevance of the extractor's seed length is most striking when one considers the task of randomness expansion. Protocols for this task typically follow a two-step procedure. In the first step, part of the initial seed randomness is used to make partially random input choices to the devices, which are used repeatedly to eventually produce a long string of output bits with guaranteed min-entropy rate (we refer to e.g. [11] for a more complete description of this step). In the second step the remainder of the random seed is used as seed for an extractor applied to the bits produced in the first step, eventually yielding an as-large-as-possible number of (close to) uniformly random bits. It was previously shown [30] that the first step could be be achieved with exponential expansion, expanding a d-bit seed into $N = 2^{d^{0.99}}$ bits that have constant min-entropy rate. Prior to our work the best extractor constructions required $\Omega(d^2)$ bits to extract from such a source, meaning that almost all the seed was in fact consumed in the second step of the scheme, resulting in an overall expansion of $\overline{d} \mapsto 2^{\overline{d}^{0.49}}$ bits only. In contrast, our results allow a more even splitting of the seed between the two steps and yield a super-polynomial improvement in the final expansion, $\overline{d} \mapsto 2^{\overline{d}^{0.99}}$ uniformly random bits.

1.4 Techniques

Interestingly, the proof of Theorem 1.3 is quite short and fairly simple. We use the operational interpretation of the output min-entropy of the condenser as the maximum probability with which a (quantum) adversary may successfully guess the output string. In the first step of the proof we establish a general reduction showing that for any such quantum adversary there must exist another adversary whose measurement operators take a particularly simple form (derived from the pretty-good-measurement (PGM) [19]), and still succeeds with at most a quadratic loss in the guessing probability. In the second step we observe that, due to the simplified form of its guessing measurement, this new adversary could equivalently have measured its quantum side information *before* the application of the condenser to obtain *classical* side information about the source, from which it would later (after having been revealed the seed) classically infer a successful guess for the condenser's output, contradicting the classical condenser guarantee.

Combining both steps gives our generic reduction from quantum-proof security to classical security. (See Section 3 for more details.) We note that the proof is made slightly more involved technically by the need to handle ϵ approximations; for this it is crucial that the condition on the output min-entropy of the condenser be measured according to the ϵ-smooth conditional min-entropy.

Once Theorem 1.3 has been proven, to prove Theorem 1.5 it only remains to construct quantum-proof extractors for min-entropy rate, say, 1/3. Unfortunately, even for such high min-entropy, existing results are not able to extract a constant fraction of the min-entropy using logarithmic seeds. To obtain such extractors we make use of the "block-sampling-and-extraction" framework developed in [36, 41, 57]. We observe that all key ingredients used in this construction have been shown to be quantum-proof with comparable parameters:

- A strong extractor based on almost pairwise independent hashing. This was proved quantum-proof by Tomamichel *et. al.* [49] with essentially the same parameters as classically.

- A randomness-efficient sampler to sample blocks from the source while preserving the min-entropy rate. Such a procedure was analyzed in the presence of quantum side information by König and Renner [23]. Unfortunately the results of [23] induce a loss in the entropy rate, which we discuss in more detail in Section 4.1.[3]

---

[3] It is worthwhile mentioning that we cannot adopt the later improvement of [23] by Wullschleger [56] because the latter does not apply to randomness-efficient samplers.

- A chain rule for the conditional min-entropy. A sufficient relation for our purposes was shown by König and Terhal [25] in the quantum setting.

Combining these ingredients and making appropriate adjustments to the analysis of [36, 41, 57], we obtain an extractor for min-entropy rate 1/3 sources (and, in fact, for any constant min-entropy rate) that extracts a constant fraction of the min-entropy using logarithmic seeds (see Theorem 4.6 for a precise statement). We observe that the output length can be increased to $(1-\alpha)k$ for any constant $\alpha > 0$ using standard techniques, that can also be shown to be quantum-proof.

Open questions. Our construction achieves optimal seed length, up to constant factors, even for very low input min-entropy. Nevertheless, gaps remain in our understanding of quantum-proof extractors. For example, several classical works achieved even more stringent demands, such as seed length $d = (1+\alpha)\log n$ [43], or sub-linear entropy loss (i.e., $m = k - o(k)$) [15, 47]. We do not know whether quantum-proof extractors with such parameters exist, even non-constructively. Another intriguing question is whether the generic error reduction technique of [38] could be made quantum-proof.

We leave open the question of whether the 1/2-loss of entropy in our reduction from quantum-proof condensers to classical condensers is inherent or rather only an artifact of our proof technique. Proving that such a reduction holds with no loss will in particular resolve Problem 2 to the affirmative. We remark that if the loss can be reduced to a small enough constant $\lambda \ll 1/2$, one would be able to construct quantum-proof extractors with even better parameters than those stated in Theorem 1.5, and using a somewhat simpler construction.

2 Preliminaries

We summarize necessary background about quantum information and our terminology in Section 2.1. (We refer to the books [34, 55] for additional background on quantum computing and quantum information theory respectively.) In subsequent sections, we survey relevant results on three topics: quantum min-entropy sources (Section 2.2), condensers & extractors (Section 2.3), and samplers (Section 2.4).

2.1 Quantum information

Quantum states. The state space $\mathcal{A}$ of m-qubit is the complex Euclidean space $\mathbb{C}^{2^m}$. An m-qubit quantum state is represented by a density operator ρ, i.e., a positive semidefinite operator over $\mathcal{A}$ with trace 1. The set of all quantum states in $\mathcal{A}$ is denoted by $\mathcal{S}_=(\mathcal{A}) := \{\rho \geq 0 : \mathrm{tr}(\rho) = 1\}$. We sometimes consider a larger set of states on $\mathcal{A}$, the sub-normalized states $\mathcal{S}_\leq(\mathcal{A}) := \{\rho \geq 0 : \mathrm{tr}(\rho) \leq 1\}$.

Let $\mathrm{L}(\mathcal{A})$ denote the set of all linear operators on space $\mathcal{A}$. The Hilbert-Schmidt inner product on $\mathrm{L}(\mathcal{A})$ is defined by $\langle X, Y\rangle = \mathrm{tr}(X^*Y)$, for all $X, Y \in \mathrm{L}(\mathcal{A})$, where X^* is the adjoint conjugate of X. Let $\mathsf{id}_{\mathcal{X}}$ denote the identity operator over $\mathcal{X}$.

For a multi-partite state, e.g. $\rho_{ABC} \in \mathcal{S}_=(\mathcal{A}\otimes\mathcal{B}\otimes\mathcal{C})$, its reduced state on some subsystem(s) is represented by the same state with the corresponding subscript(s). For example, the reduced state on $\mathcal{A}$ system of ρ_{ABC} is $\rho_A = \mathrm{tr}_{\mathcal{BC}}(\rho_{ABC})$, and $\rho_{AB} = \mathrm{tr}_{\mathcal{C}}(\rho_{ABC})$. When all subscript letters are omitted, the notation represents the original state (e.g., $\rho = \rho_{ABE}$).

A *classical-quantum-*, or cq-state $\rho \in \mathcal{S}_=(\mathcal{A}\otimes\mathcal{B})$ indicates that the $\mathcal{A}$ subsystem is classical and $\mathcal{B}$ is quantum. Likewise for ccq-, etc., states. We use *lower case* letters to denote specific values assignment to the classical part of a state. For example, any cq-state $\rho_{AB} = \sum_a p_a |a\rangle\langle a| \otimes \rho_B^a$ in which $p_a = \mathbf{Pr}[A = a]$ and ρ_B^a is a normalized state.

Quantum measurements. Let Σ be a finite nonempty set of *measurement outcomes*. A *positive-operator valued measure (POVM)* on the state space $\mathcal{A}$ with outcomes in Σ is a collection of positive semidefinite operators $\{P_a : a \in \Sigma\}$ such that $\sum_{a\in\Sigma} P_a = \mathsf{id}_{\mathcal{A}}$. If instead of equality, $\sum_{a\in\Sigma} P_a \le \mathsf{id}_{\mathcal{A}}$, the collection is a *sub-normalized* POVM. When this POVM is applied to a quantum state ρ, the probability of each outcome $a \in \Sigma$ is $\langle \rho, P_a\rangle$. When outcome a is observed, the quantum state ρ becomes the state $\sqrt{P_a}\rho\sqrt{P_a}/\langle \rho, P_a\rangle$.

Distance measures. For any $X \in \mathrm{L}(\mathcal{A})$ with singular values $\sigma_1, \cdots, \sigma_d$, where $d = \dim(\mathcal{A})$, the trace norm of $\mathcal{A}$ is $\|X\|_1 = \sum_{i=1}^d \sigma_i$. The *trace distance* between $\rho_0, \rho_1 \in \mathcal{S}_\le(\mathcal{A})$ is defined to be

$$\|\rho_0 - \rho_1\|_{\mathrm{tr}} \overset{\mathrm{def}}{=} \frac{1}{2}\|\rho_0 - \rho_1\|_1 + \frac{1}{2}\big|\mathrm{Tr}(\rho_0 - \rho_1)\big|.$$

Quantum operations. Let $\mathcal{X}$ and $\mathcal{Y}$ be state spaces. A *super-operator* from $\mathcal{X}$ to $\mathcal{Y}$ is a linear map

$$\Psi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y}).$$

Physically realizable *quantum operations* are represented by *admissible* super-operators, which are completely positive and trace-preserving. Thus any classical operation (such as extractors) can be viewed as an admissible super-operator.

Fact 2.1 (Monotonicity of trace distance) *For any admissible super-operator* $\Psi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ *and* $\rho_0, \rho_1 \in \mathcal{S}_=(\mathcal{X})$*, we have*

$$\|\Psi(\rho_0) - \Psi(\rho_1)\|_{\mathrm{tr}} \le \|\rho_0 - \rho_1\|_{\mathrm{tr}}. \tag{2.1}$$

2.2 Quantum min-entropy sources

Min-entropy. Before we introduce the quantum min-entropy, let us recall the min-entropy definition of classical sources.

Definition 2.2 (Classical Sources) *The* min-entropy *of a random variable* X *is given by*

$$H_{\min}(X) = \min_{x\in\mathcal{X}} \log_2(1/\mathbf{Pr}[X = x]).$$

For $X \in \{0,1\}^n$*, we call* X *an* $(n, H_{\min}(X))$*-source (or* $H_{\min}(X)$*-source) with* entropy rate $R_{\min}(X) = H_{\min}(X)/n$.

In the regime of quantum extractors, it is necessary to consider the existence of adversaries who are furthermore given quantum computational power. In the seeded extractor setting, it suffices to model the adversary as *quantum side information* which is stored in the system $\mathcal{E}$ as follows. For a cq state $\rho_{XE} \in \mathcal{S}_\le(\mathcal{X} \otimes \mathcal{E})$, the amount of *extractable* randomness (from X against E) is characterized by its conditional min-entropy.

Definition 2.3 *Let* $\rho_{XE} \in \mathcal{S}_\le(\mathcal{X} \otimes \mathcal{E})$*. The* min-entropy *of* X *conditioned on* E *is defined as*

$$H_{\min}(X|E)_\rho \overset{def}{=} \max\{\lambda \ge 0 : \exists \sigma_E \in \mathcal{S}_\le(\mathcal{E}), \text{s.t. } 2^{-\lambda}\mathsf{id}_X \otimes \sigma_E \ge \rho_{XE}\}.$$

This definition has a simple operational interpretation shown in [24] that

$$H_{\min}(X|E)_\rho = -\log(p_{\text{guess}}(X|E)_\rho),$$

where $p_{\text{guess}}(X|E)_\rho$ is the maximum probability of guessing X by making arbitrary measurements on E system.

We also consider the *smooth* min-entropy that consists in maximizing the min-entropy over all sub-normalized states that are ϵ-close to the actual state ρ_{XE} in trace distance[4]. Note that allowing an extra error ϵ can significantly increase the min-entropy of certain states.

Definition 2.4 *Let $\epsilon \geq 0$ and $\rho_{XE} \in \mathcal{S}_=(\mathcal{X} \otimes \mathcal{E})$, then the* ϵ-smooth min-entropy *of X conditioned on E is defined as*

$$H^{\epsilon}_{\min}(X|E)_\rho \overset{def}{=} \max_{\|\sigma_{XE},\rho_{XE}\|_{\text{tr}} \leq \epsilon} H_{\min}(X|E)_\sigma,$$

Definition 2.5 (Quantum Sources) *We call ρ_{XE} an (n,k)-cq source (or k-cq source) if $X \in \{0,1\}^n$ and $H_{\min}(X|E)_\rho \geq k$. The min-entropy rate of ρ_{XE}, denoted $R_{\min}(X|E)$, is defined by*

$$R_{\min}(X|E)_\rho \overset{def}{=} \frac{H_{\min}(X|E)_\rho}{H_0(X)_\rho},$$

where $H_0(X)_\rho = \log(|\mathcal{X}|)$. Similarly, we could define all these terms with smooth errors.

Definition 2.6 (Quantum Block-source) *A cq state $\rho_{X_1 \cdots X_C E} \in \mathcal{S}_=(X_1 \otimes \cdots \otimes X_C \otimes \mathcal{E})$ is called a quantum $(k_1, k_2, \cdots, k_C)$ block-source if for any $i \in [C]$ and any $x_1 \in \mathcal{X}_1, \cdots, x_{i-1} \in \mathcal{X}_{i-1}$ it holds that $H_{\min}(X_i|X_1 = x_1, \cdots, X_{i-1} = x_{i-1}, E) \geq k_i$. If $k_1 = k_2 = \cdots = k_C = k$, then X is called a quantum k block-source.*

If the weaker conditions $H^{\gamma_i}_{\min}(X_i|X_1 = x_1, \cdots, X_{i-1} = x_{i-1}, E) \geq k_i$, for $i = 1, \ldots, C$ and $\gamma_1, \ldots, \gamma_C > 0$, hold, then X is called a smooth quantum $(k_1, \ldots, k_C)$ block-source with smooth error $(\gamma_1, \ldots, \gamma_C)$. If $\gamma_1 = \cdots = \gamma_C = \gamma$ and $k_1 = \cdots k_C = k$ it is called a smooth quantum k block-source with smooth error γ.

Properties of Quantum Min-entropy Similar to the classical min-entropy, the quantum conditional entropy also satisfies the following property.

Lemma 2.7 ([25]) *Given any ccq state ρ_{XWE} in which $W \leftrightarrow X \leftrightarrow E$* [5]*, we have*

$$\Pr_{w \sim W}\left[H_{\min}(X|W = w, E) \geq H_{\min}(X|E) - \log\dim(\mathcal{W}) - \log(1/\epsilon)\right] \geq 1 - \epsilon$$

---

[4] We note that alternative measures, such as the purified distance, are often used in the definition of the smooth min-entropy. Ultimately all reasonable distance measures lead to essentially equivalent definitions, and we choose the trace distance for technical convenience.

[5] Namely, we have $\rho_{XWE} = \sum_{x,w} \mathbf{Pr}[X = x, W = w] \, |x,w\rangle\langle x,w| \otimes \rho^x_E$.

2.3 Seeded extractors: classical & quantum

Classical Seeded Extractors: are deterministic functions that convert any classical min-entropy source to a marginally uniform output with the help of short uniform seed. Precisely,

Definition 2.8 (Strong Seeded Extractor) *A function* Ext : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a classical* (k, ϵ)-strong seeded (randomness) extractor*, if for any min-entropy* $\geq k$ *source* $X \in \{0,1\}^n$*, and for a uniform seed* $Y \in \{0,1\}^d$ *independent of* X*, we have*

$$\|(\mathrm{Ext}(X, Y), Y) - (\mathcal{U}_m, Y)\|_{\mathrm{tr}} \leq \epsilon. \tag{2.2}$$

One of the best known classical extractors is as follows.

Theorem 2.9 ([18]) *For every constant* $\alpha > 0$*, and all positive integers* n, k *and* $\epsilon > 0$*, there is an explicit construction of a strong* (k, ϵ) *extractor* Ext : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with* $d = O(\log n + \log(1/\epsilon))$ *and* $m \geq (1 - \alpha)k$*.*

Quantum Seeded Extractors. We also review quantum seeded randomness extractors, which turn a quantum min-entropy source to a quantum-secure uniform output, with the help of a short seed. Since now the system involves a quantum adversary, we refer this as the *quantum* security.

Definition 2.10 (Quantum Strong Seeded Extractor) *A function* Ext : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a* quantum-secure *(or simply quantum)* (k, ϵ)-strong seeded (randomness) extractor*, if for all cq states* ρ_{XE} *with* $H_{\min}(X|E) \geq k$*, and for a uniform seed* Y *independent of* ρ_{XE}*, we have*

$$\left\|\rho_{\mathrm{Ext}(X,Y)YE} - \mathcal{U}_m \otimes \rho_Y \otimes \rho_E\right\|_{\mathrm{tr}} \leq \epsilon. \tag{2.3}$$

We state the following quantum strong seeded extractor that is useful to instantiate our construction in the paper.

Theorem 2.11 (Theorem 10, [49]) *There exists a family of hash functions from* $\{0,1\}^n$ *to* $\{0,1\}^m$ *with seed length* $d = 2(m + \log(n/m) + \log(1/\epsilon^2) - 1)$ *and* $e \leq 3\epsilon + \frac{1}{2}\sqrt{2^{m - H^{\epsilon}_{\min}(X|E)_{\rho} + \log(2/\epsilon^2 + 1)}}$ *for any* $\epsilon > 0$*.*

A concrete instantiation of the above theorem is as follows.

Corollary 2.12 *There exists an explicit extractor* Ext : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *that is quantum* (k, ϵ) *strong, where* $d = O(\log(n/\epsilon))$*,* $m = 0.01d$ *and* $k = 0.02d$*.*

The following simple lemma will be useful to obtain extractor constructions that extract almost all the input min-entropy (see e.g. [25, Theorem 2] for a proof).

Lemma 2.13 *Suppose* Ext : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a quantum* (k, ϵ) *strong seeded extractor, and* $\mathrm{Ext}' : \{0,1\}^n \times \{0,1\}^{d'} \to \{0,1\}^{m'}$ *is a quantum* (k', ϵ') *strong seeded extractor for* $k' = k - m$*. Then* $\mathrm{Ext}'' : \{0,1\}^n \times \{0,1\}^{d+d'} \to \{0,1\}^{m+m'}$ *defined as* $\mathrm{Ext}'(X, Y_1 \circ Y_2) = \mathrm{Ext}(X, Y_1) \circ \mathrm{Ext}(X, Y_2)$ *is a quantum* $(k, \epsilon + \epsilon')$ *strong seeded extractor.*

Proof. By definition provided $H_{\min}(X|E) \geq k$ it holds that $\|\rho_{\mathrm{Ext}(X,Y_1)Y_1E} - \mathcal{U}_m \otimes \rho_{Y_1} \otimes \rho_E\|_{tr} \leq \epsilon$. Let $E' = \mathrm{Ext}(X,Y_1)Y_1E$. Using that Y_1 is independent from X,

$$\begin{aligned} H_{\min}(X|E') &= H_{\min}(X|\mathrm{Ext}(X,Y_1)E) \\ &\geq H_{\min}(X|E) - \log\dim \mathrm{Ext}(X,Y_1) \\ &\geq k - m, \end{aligned}$$

where the second line is by [48, Lemma 6.8]. Thus $\|\rho_{\mathrm{Ext}'(X,Y_2)Y_2E'} - \mathcal{U}_{m'} \otimes \rho_{Y_2} \otimes \rho_{E'}\|_{tr} \leq \epsilon'$. Using the triangle inequality for the trace distance proves the lemma. ■

We will also make use of the following lemma from Widgerson and Zuckerman [54], which states that we can increase the output length of an extractor at the cost of increasing the seed length and error proportionally. This is done by using independent seeds to extract from the source multiple times. The lemma holds for the quantum-proof setting with the same proof.

Lemma 2.14 *For every constant $\alpha, \gamma \in (0,1)$, for every n, k, d, m, ϵ with $m = \gamma k$ and $\epsilon \geq 2^{-k/2}$, if there exists a (k,ϵ)-strong quantum-proof extractor* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, *then there exists a $(k' = 2k/\alpha, \epsilon')$-strong quantum-proof extractor* $\mathrm{Ext}' : \{0,1\}^n \times \{0,1\}^{d'} \to \{0,1\}^{m'}$ *with output length $m' = (1-\alpha)k'$, seed length $d' = O(d/\alpha\gamma)$, and error $\epsilon' = O(\epsilon/\alpha\gamma)$.*

Classical & Quantum Condensers. A relevant but weaker notion is called *condenser* which converts any min-entropy source to a min-entropy source of higher min-entropy rate.

Definition 2.15 *A function* $\mathrm{Cond} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a (k,k',ϵ)* condenser *if for every k-source X in $\{0,1\}^n$,* $\mathrm{Cond}(X,Y)$ *is ϵ-close to some k'-source, where Y is uniformly distributed and independent of X.* Cond *is* strong *if $H^{\epsilon}_{\infty}(\mathrm{Cond}(X,Y)|Y) \geq k'$, and is* lossless *if $k' = k + d$.*

We say that Cond *is a* quantum-proof *strong condenser if both min-entropies can be taken conditional on an additional quantum system E, correlated with X but independent from Y.*

We will make use of the following classical construction of a condenser.

Theorem 2.16 ([18]) *For any constant $\tau > 0$ (τ can be taken to be larger than 1), all integers n, k such that $k \leq n$, and for any $\epsilon > 0$, there exists an efficiently-computable $(k, k+t, \epsilon)$ condenser* $\mathsf{Cond}\colon \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ *having seed length $t = (1+1/\tau)\log(nk/\epsilon) + O(1)$ and $m = (1+\tau)k + 2t$ output bits.*

2.4 Samplers on quantum sources

Sampling is a fundamental step in the construction of extractors in Nisan and Zuckerman [36], which says that if one samples a random subset of bits from a weak random source, the min-entropy rate of the source is (nearly) preserved. However, directly choosing a random subset S is too expensive in the seed length. Instead, we refer to a more randomness-efficient notion known as *averaging* (or *oblivious*) *samplers*, which have been studied extensively (e.g., [57, 51]). Precisely, let n be the size of the universe to sample and $[n]$ denote the set $\{1, \cdots, n\}$, we define the (one-sided) averaging sampler as follows.

Definition 2.17 (Averaging Samplers) *A* function Samp : $\{0,1\}^r \to [n]^t$ *is a* (μ, β, γ) *averaging sampler* if for every function $f : [n] \to [0,1]$ *with* average value $\frac{1}{n}\sum_i f(i) \geq \mu$*, it holds that*

$$\mathbf{Pr}_{(i_1,\cdots,i_t)\sim\mathrm{Samp}(U_r)}\left[\frac{1}{t}\sum_{j=1}^{t} f(i_j) < (1-\beta)\mu\right] \leq \gamma.$$

Note the one-sided formulation, which only requires an upper bound on the probability of a lower average than expected. Moreover, the above definition of the sampler has a multiplicative error rather than an additive error, which allows us to get better sample complexity dependence on the error.

We use the following sampler from k-wise independent hashing, implicitly analyzed in [36, 41, 57]. We state the lemma in a convenient form for our purpose.

Lemma 2.18 *For every constant $\alpha, \beta \in (0,1)$, there exist a constant $c > 0$ such that the following holds. For sufficiently large $n \in \mathbb{N}$, $\mu, \gamma \in (0,1)$ with $\gamma \geq 2^{-c\mu n^{1-\alpha}}$, there is a (μ, β, γ) averaging sampler* Samp : $\{0,1\}^r \to [n]^t$ *such that*

- Samp *uses $r = O((1/\alpha)\cdot\log(n/\gamma)) = O(\log(n/\gamma))$ random bits.*
- Samp *produces t samples, for any desired $t = \Omega((n^\alpha \log(1/\gamma))/(\alpha\beta^2\mu))$.*

Quantum Source Sampling. Since we are interested in sampling on quantum sources, we define quantum source samplers as follows.

Definition 2.19 (Quantum Source Samplers) *A* function Samp : $\{0,1\}^r \to [n]^t$ *is a (μ, β, γ) quantum sampler* if for every cq source ρ_{XE} *over $\{0,1\}^n$ with quantum conditional min-entropy $k \geq \mu n$, it holds that $H_{\min}^{\gamma}(X_{\mathrm{Samp}(U_r)}|U_r = a, E) \geq (1-\beta)\mu t$, for every $a \in \{0,1\}^r$.*

The following result from [23] that states one can use any averaging sampler to sample over quantum sources with worse parameters, i.e., the additional κ term in the entropy rate loss. Let X_S denote the restriction of X to those coordinates in the set S.

Theorem 2.20 (Corollary 6.19, [23]) *Let ρ_{X^nE} be a quantum state where $X^n = (X_1, \cdots, X_n)$ on $\mathcal{X}^n$ is classical with smooth min-entropy rate $R_{\min}^{\tau}(X|E)_\rho \geq \mu$. Let* Samp *be a $(\mu_{\mathrm{Samp}}, \beta_{\mathrm{Samp}}, \gamma_{\mathrm{Samp}})$ averaging sampler and S be the sampled subset. Assume that $\kappa = \frac{n}{|S|\log(|\mathcal{X}|)} < 0.15$. Then*

$$\begin{aligned} R_{\min}^{\epsilon'+\tau}(X_S|SE)_\rho &\geq R_{\min}^{\tau}(X^n|E)_\rho - 3\beta_{\mathrm{Samp}}\mu_{\mathrm{Samp}} - 2\kappa\log 1/\kappa \ \textit{with} \\ \epsilon' &= 2\cdot 2^{-\beta_{\mathrm{Samp}}\mu_{\mathrm{Samp}}n\log|\mathcal{X}|} + 3\gamma_{\mathrm{Samp}}^{1/4}. \end{aligned}$$

for all $\tau \geq 0$.

In order to make use of Theorem 2.20, we need to combine groups of X_i into big chunks and then sample over these chunks. We will formulate this idea in Section 4.

3 Classical condensers are quantum-proof

This section is devoted to the proof of our first main result, which establishes a general reduction showing that any strong condenser is automatically quantum-proof, with a small loss in parameters. Precisely, we show the following.

Theorem 3.1 *Let* Cond *be a classical* (k, k', ϵ) *strong condenser. Then* Cond *is also a* $(k, (k' - \log(1/(2\epsilon)))/2, \epsilon)$ *strong condenser against quantum adversaries.*

Before giving the proof of the theorem we state a couple interesting corollaries which follow by plugging in know constructions of strong classical condensers. Using a condenser due to Guruswami-Umans-Vadhan, with parameters stated in Theorem 2.16 (take $\delta = 1/\tau$), we obtain the following, which is a slightly stronger statement of Corollary 1.4.

Corollary 3.2 *For all* $\delta > 0$ *and integers* n, k *such that* $k \leq n$*, for any* $\epsilon > 0$*, there exists an efficiently-computable quantum-proof* $(k, k/2 - \log(4/\epsilon), \epsilon)$ *strong condenser* $\mathrm{Cond}_{\mathrm{GUV}}\colon \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ *having seed length* $t = (1+\delta)\log(nk/\epsilon^2) + O(1)$ *and* $m = (1 + 1/\delta)k + 2t$ *output bits.*

Proof. Choosing $\tau = 1/\delta$ in Theorem 2.16 gives an efficiently-computable $(k, k+t, \epsilon)$ condenser $\mathrm{Cond}_{\mathrm{GUV}}\colon \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^m$ with seed length $t = (1+\delta)\log(nk/\epsilon) + O(1)$ and $m = (1+1/\delta)k + 2t$ output bits. By [10, Lemma 4.8] the same is automatically a $(k, k - \log(2/\sqrt{\epsilon}), 3\sqrt{\epsilon})$ strong condenser. Applying Theorem 3.1 we deduce that $\mathrm{Cond}_{\mathrm{GUV}}$ is a quantum-proof $(k, (k - \log(4/\epsilon)/2, 3\sqrt{\epsilon})$ strong condenser. Renaming $\epsilon \leftarrow 3\sqrt{\epsilon}$ and updating parameters accordingly completes the proof. ■

We note that in case one is interested in fully optimizing the seed length, a different application of the results of [18] gives us the following corollary.

Corollary 3.3 *For all integers* $k \leq n$ *and* $\epsilon > 0$ *there exists an explicit quantum-proof* $(k, k/2 - \log(2/\epsilon), \epsilon)$*-strong condenser* $\mathrm{Cond}\colon \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with* $d = \log(nk/\epsilon) + 1$ *and* $m = d(k+2)$.

We now give the proof of Theorem 3.1.

Proof. [Theorem 3.1] We first set some notation. Let X be a random variable in $\{0,1\}^n$, taking value x with probability p_x. Let ρ_x be the state of E conditioned on $X = x$, unnormalized (ie $\mathrm{Tr}(\rho_x) = p_x$). The state of the system before applying the condenser is $\sum_x |x\rangle\langle x| \otimes \rho_x$. Afterwards, it is

$$\rho := \rho_{ZYE} = 2^{-t} \sum_{z,y} |z\rangle\langle z| \otimes |y\rangle\langle y| \otimes \rho_z^y,$$

where $\rho_z^y = \sum_{x:C(x,y)=z} \rho_x$.

We now define a possible classical adversary to the condenser. The classical adversary measures ρ_x using the measurement (known as the *pretty good measurement*) with POVM elements

$$M_x := \rho_E^{-1/2} \rho_x \rho_E^{-1/2},$$

where $\rho_E = \sum_x \rho_x$ (note that ρ_E is a density matrix). This classical adversary obtains outcome x' with probability

$$q(x', x) := \langle M_{x'}, \rho_x \rangle = \mathrm{Tr}(\rho_E^{-1/2} \rho_{x'} \rho_E^{-1/2} \rho_x).$$

Upon receiving y, she guesses $z' = C(x', y)$ for the value of z. Let

$$\sigma_x := \sum_{x'} p(x'|x)\,|x'\rangle\langle x'|$$

describe the side information of the classical adversary. Clearly $H_\infty(X|E) \geq k \implies H_\infty(X|X') \geq k$. Since C is assumed to be a (k, k', ϵ) strong condenser, it must be that $H^\epsilon_\infty(C(X,Y)|YE') \geq k'$. In particular, if we define a set $B \subseteq \{0,1\}^m$ of "heavy hitters" by

$$B = \Big\{ z \in \{0,1\}^m \,:\, 2^{-t} \sum_y \mathrm{Tr}\big(\rho^{-1/2}\rho^y_z\rho^{-1/2}\rho^y_z\big) > 2^{-k'+log(2\epsilon)}p(z) \Big\},$$

where $p(z) = 2^{-t}\sum_y \mathrm{Tr}(\rho^y_z)$ is the marginal output distribution on Z, applying Lemma 3.4 below it must be that

$$\sum_{z\in B} p(z) \,<\, \epsilon. \tag{3.1}$$

We are ready to prove the theorem. Reason by contradiction: suppose

$$H^\epsilon_{\min}(C(X,Y)|YE) \,<\, \frac{k' - \log(1/(2\epsilon))}{2}. \tag{3.2}$$

Consider the (sub-normalized) state

$$\tilde\rho_{ZYE} \,=\, \sum_{z\notin B} 2^{-t} \sum_y |z\rangle\langle z| \otimes |y\rangle\langle y| \otimes \rho^y_z.$$

By (3.1) it holds that $\|\rho_{ZYE} - \tilde\rho_{ZYE}\|_1 \leq \epsilon$. Hence there exists an attack for the adversary: a family of POVM $\{M^z_y\}_z$ indexed by y such that

$$\sum_{z\notin B} 2^{-t} \sum_y \mathrm{Tr}\big(M^z_y\rho^y_z\big) > 2^{(-k'+\log(2\epsilon))/2}. \tag{3.3}$$

We repeat the steps showing near-optimality of the pretty-good-measurement, up to a square root:

$$\begin{aligned}
2^{(-k'+\log(2\epsilon))/2} &< \sum_{z\notin B} 2^{-t} \sum_y \mathrm{Tr}\Big(M^z_y\rho^{1/4}\rho^{-1/4}\rho^y_z\rho^{-1/4}\rho^{1/4}\Big)\\
&\leq \Big(\sum_{z\notin B} 2^{-t}\sum_y \mathrm{Tr}\big(M^z_y\rho^{1/2}M^z_y\rho^{1/2}\big)\Big)^{1/2}\Big(\sum_{z\notin B} 2^{-t}\sum_y \mathrm{Tr}\big(\rho^{-1/2}\rho^y_z\rho^{-1/2}\rho^y_z\big)\Big)^{1/2}\\
&\leq \Big(\sum_{z\notin B} 2^{-t}\sum_y \mathrm{Tr}\big(\rho^{-1/2}\rho^y_z\rho^{-1/2}\rho^y_z\big)\Big)^{1/2},
\end{aligned}$$

where the second line is by Cauchy-Schwartz and the third uses $0 \leq M^y_z \leq \mathrm{Id}$ for all y, z. Using the definition of B, it follows that

$$2^{-k'}/(2\epsilon) < \sum_{z\notin B} 2^{-k'}/(2\epsilon)p(z) \leq 2^{-k'}/(2\epsilon),$$

a contradiction. ∎

Lemma 3.4 *Let Z, Z' be two random variables with joint distribution p such that $H_{\min}^{\epsilon}(Z|Z')_p \geq k$ for some $\epsilon, k > 0$. Let $B = \{z' : p(z', z') > 2^{-k'+\log(2\epsilon)} p(z')\}$. Then $\sum_{z' \in B} p(z') < \epsilon$.*

Proof. By definition, for any distribution q,

$$2^{-H_{\min}(Z|Z')_q} = \mathrm{E}_{z' \sim q} 2^{-H_{\min}(Z|Z'=z')_q} \geq \mathrm{E}_{z' \sim q} q(z'|z').$$

Therefore the assumption of the lemma implies that there exists a q such that $\|p - q\|_{\mathrm{tr}} \leq \epsilon$ and $\mathrm{E}_{z'} q(z'|z') \leq 2^{-k}$. By Markov's inequality, for any $\eta > 0$, $\Pr_{z' \sim q}(q(z'|z') > 2^{-k'}/\eta) < \eta$, and this can be equivalently rewritten as

$$\sum_{z' : q(z', z') > 2^{-k'} q(z')/\eta} q(z') < \eta.$$

Choose $\eta = 2\epsilon$. Using $\|p - q\|_{\mathrm{tr}} \leq \epsilon$ it must be that also

$$\sum_{z' : p(z', z') > 2^{-k'} p(z')/(2\epsilon)} p(z') < 2\epsilon - \epsilon,$$

as claimed. ■

4 The block sampling and extraction paradigm

Zuckerman's extractor construction [57] is composed of two fundamental tools. The first is a generic converter from any min-entropy source to a block-source via sampling. We explain this construction and its extension to quantum side information in Section 4.1. The second is a randomness-efficient extraction procedure from block-sources. We extend this procedure to quantum side information in Section 4.2. Finally in Section 4.3 we combine these two components and prove that Zuckerman's construction can be made quantum-proof, with essentially the same parameters as in the classical setting.

4.1 Conversion to block-sources

The conversion of a min-entropy source to a more structured block-source from [57] is based on the use of samplers. In the presence of quantum side information the only available tool for quantifying the effectiveness of the sampling procedure is the main result from [23], which as stated in Theorem 2.20 only provides a meaningful bound when the source is thought of as a sequence of symbols taken from a large enough alphabet. This constraint forces us to sample joint "chunks" of bits from the source. We proceed with the details.

Quantum sampler over chunks. Combining Lemma 2.18 and Theorem 2.20 yields the following.

Lemma 4.1 *For every constants $\alpha, \beta, \delta \in (0, 1)$ such that $2\delta < \alpha$ there exists a constant $c > 0$ such that the following holds. For every sufficiently large $n \in \mathbb{N}$, $\mu, \gamma \in (0, 1)$ with $\mu > n^{-1/2+\delta}$ and $\gamma \geq 2^{-c\mu^2 n^{1-\alpha}/\log(1/\mu)}$, and $t \leq n$ such that $t = \Omega(\sqrt{(n^{1+\alpha} \log(1/\gamma))/\mu^2})$, there is a (μ, β, γ) quantum source sampler* Samp : $\{0, 1\}^r \to [n]^t$ *that uses $r = O(\log(n/\gamma))$ random bits and returns t distinct coordinates.*

Proof. Let ρ_{X^nE} be an (n,k) quantum source with min-entropy rate $\mu = R_{\min}(X|E)_\rho = k/n$, ℓ a chunk size parameter to be determined later, and write $X^n = Y^{n'} = (Y_1 \circ \cdots \circ Y_{n'})$ for $n' = n/\ell$ (assume $\ell | n$ for simplicity). Let $S' \subseteq [n']$, and let $S \subseteq [n]$ be associated with S' in the straightforward way.

Let $\mu_{\text{Samp}} = \mu$, $\beta_{\text{Samp}} = \beta/6$, $\gamma_{\text{Samp}} = (\gamma/2)^4/3$. The averaging $(\mu_{\text{Samp}}, \beta_{\text{Samp}}, \gamma_{\text{Samp}})$ sampler from Lemma 2.18 yields a set S' of samples over $Y^{n'}$ of cardinality

$$|S'| = t_{\text{Samp}} = \Omega\Big(\frac{n^\alpha \log(1/\gamma)}{\alpha\beta^2\mu}\Big).$$

Now set $\ell = O(\sqrt{(n/t_{\text{Samp}}) \cdot (\log(1/\beta\mu)/\beta\mu)})$, with an implied constant large enough so that the parameter κ from Theorem 2.20,

$$\kappa = \frac{n}{|S'| \times \ell^2} = O\Big(\frac{\beta\mu}{\log(1/\beta\mu)}\Big),$$

satisfies the constraint $\kappa < 0.15$. The resulting sampler, obtained by splitting the sampled chunks into bits again, has output length

$$t = |S| = |S'|\ell = \Omega\Big(\sqrt{\frac{n^{1+\alpha}\log(1/\gamma)}{\alpha\beta^3\mu^2}}\Big)$$

and makes use of $r = O((1/\alpha) \cdot \log(1/\gamma)) = O(\log(1/\gamma))$ random bits. The obvious constraint that $t \le n$ imposes the conditions $\mu > n^{-1/2+\delta}$ and $\gamma \ge 2^{-c\mu^2 n^{1-\alpha}/\log(1/\mu)}$ stated in the lemma. Assuming these constraints satisfied, our choice of parameters is such that by Theorem 2.20 the sampled state $\rho_{X_{\text{Samp}(U_r)}U_rE}$ is γ-close in trace distance from a $\mu(1-\beta)t$-source, conditioned on U_r and E. ■

Block-sources from sampling. We show that any min-entropy source can be converted to a block-source by sampling. We use the same procedure, called a *converter* in [44], as introduced in [36]. The procedure is described in Fig. 1 (the parameters $(\mu_i, \beta_i, \gamma_i)_{i=1,\dots,t}$ will be chosen later). The analysis is also essentially the same, but we repeat it here as the parameters of the sampler are not identical.

Theorem 4.2 *Let the converter* Conv : $\{0,1\}^{r_1} \times \{0,1\}^{r_2} \times \cdots \times \{0,1\}^{r_t} \to (S_1, S_2, \cdots, S_t)$ *be as in Fig. 1. Let* $0 < \tau < 1$, $k_i = k - (\sum_{j<i} t_j) - \log(1/\tau)$ *and* $\mu_i = k_i/n_i$ *for* $i \in \{1, \dots, t\}$ *Then if* $(S_1, \dots, S_t) = \text{Conv}(U_{r_1}, \dots, U_{r_t})$ *and* ρ_{X^nE} *is a quantum* (n,k)*-source, the state* $\rho_{X_{S_1}X_{S_2}\cdots X_{S_t}S_1S_2\cdots S_tE}$ *is* $t\tau$*-close, in trace distance, to a state* $\sigma_{X_{S_1}X_{S_2}\cdots X_{S_t}S_1S_2\cdots S_tE}$ *such that for each* $s_1, \dots, s_t$*, the state* $\sigma_{X_{s_1}\cdots X_{s_t}|S_1=s_1,\dots,S_t=s_tE}$ *is a* $(\tilde{k}_1, \dots, \tilde{k}_t)$ *smooth quantum block-source with smooth error* $(\gamma_1, \dots, \gamma_t)$ *and* $\tilde{k}_i = (1-\beta_i)\mu_i|S_i|$.

Proof. Let $\rho = \rho_{X_{S_1}X_{S_2}\cdots X_{S_t}S_1S_2\cdots S_tE}$. We first apply the chain rule for quantum min-entropy, Lemma 2.7, and the quantum sampling lemma, Lemma 4.1, to each block i to show that the quantum sampler QSamp_i "works" most of time. We then show how to modify ρ to a $t\tau$-close state σ with the desired properties.

For every $s_{<i} = (s_1, \dots, s_{i-1})$, by Lemma 2.7 (applied with $W = X_{s_{<i}}$),

$$\Pr_{x_{s_{<i}} \sim X_{S_{<i}}} \big[H_{\min}(X_{\overline{s_{<i}}}X_{s_{<i}}|X_{s_{<i}} = x_{s_{<i}}, E)_\rho \ge H_{\min}(X|E)_\rho - \log\dim(X_{s_{<i}}) - \log(1/\tau)\big]$$
$$\ge 1 - \tau. \qquad (4.1)$$

Converting min-entropy sources to block-sources

Let ρ_{X^nE} be a quantum (n,k)-source and t a target number of blocks for the block-source.

Let $S_0=\emptyset$, $n_0=n$, and for $i=1,\dots,t$ let $n_i=n_{i-1}-|S_{i-1}|$ and $\mathrm{QSamp}_i:\{0,1\}^{r_i}\to S_i\in[n_i]^{t_i}$ be a (μ_i,β_i,γ_i) quantum source sampler.

The converter is a deterministic function $\mathrm{Conv}:\{0,1\}^{r_1}\times\{0,1\}^{r_2}\times\cdots\times\{0,1\}^{r_t}\to(S_1,S_2,\cdots,S_t)$ such that $S_1,S_2,\cdots,S_t$ are disjoint and constructed as follows.

1. Let $S_1=\mathrm{QSamp}_1(U_{r_1})$.
2. For $i=2,\dots,t$ let $S_i=\mathrm{QSamp}_i(U_{r_i})$ be sampled over the set $[n_i]=[n]-(S_1\cup\cdots\cup S_{i-1})$.

Figure 1: Obtaining a block-source by sampling.

Let us call those $x_{s_{<i}}$ such that the above event holds good. For every $s_{<i}$ and good $x_{s_{<i}}$, we have

$$\begin{aligned}H_{\min}(X_{\overline{s_{<i}}}|X_{s_{<i}}=x_{s_{<i}},S_{<i}=s_{<i},E)_\rho&=H_{\min}(X_{\overline{s_{<i}}}X_{s_{<i}}|X_{s_{<i}}=x_{s_{<i}},E)_\rho\\&\geq k_i:=k-\sum_{j<i}t_j-\log(1/\tau),\end{aligned}$$

namely the min-entropy rate is at least $k_i/n_i=\mu_i$. Thus, for every $s_{<i}$ and good $x_{s_{<i}}$, QSamp_i gives

$$H_{\min}^{\gamma_i}(X_{S_i}|X_{s_{<i}}=x_{s_{<i}},S_{<i}=s_{<i},S_iE)_\rho\geq(1-\beta_i)\mu_i|S_i|=\tilde{k}_i.$$

We are ready to show that $\rho=\rho_{X_{S_1}X_{S_2}\cdots X_{S_t}S_1S_2\cdots S_tE}$ is $t\tau$-close, in trace distance, to a state $\sigma=\sigma_{X_{S_1}X_{S_2}\cdots X_{S_t}S_1S_2\cdots S_tE}$ such that for each $s_1,\dots,s_t$, $\sigma_{X_{s_1}\cdots X_{s_t}|S_1=s_1,\dots,S_t=s_tE}$ is a $(\tilde{k}_1,\dots,\tilde{k}_t)$ smooth quantum block-source with smooth error $(\gamma_1,\dots,\gamma_t)$. We define σ by modifying the state ρ as follows: for every classical value $(s_1,\dots,s_t,x_{s_1},\dots,x_{s_t})$ of ρ, if there exists some prefix $x_{s_{<i}}$ that is not good, then we replace $(x_{s_1},\dots,x_{s_t})$ by an independent uniformly random sample of values. Since for every $s_{<i}$, the probability that a random $x_{\leq t}\sim X_{\leq t}$ has a prefix $x_{<i}$ that is not good is at most τ, by a union bound, the probability that some $x_{s_{<i}}$ that is not good is at most $t\tau$. Therefore, ρ and σ are $t\tau$-close in trace distance.

Now, for every fixed $(s_1,\dots,s_t)$, we show that $\sigma_{X_{s_1}\cdots X_{s_t}|S_1=s_1,\dots,S_t=s_tE}$ is a smooth quantum block-source with the desired parameters. For every fixed $(x_{s_1},\dots,x_{s_{i-1}})$, if some $x_{s_{<j}}$ is not good, then by construction, X_{s_i} is uniform and independent of the side information E, so clearly $H_{\min}^{\gamma_i}(X_{S_i}|X_{s_{<i}}=x_{s_{<i}},S_{<i}=s_{<i},S_iE)_\sigma\geq\tilde{k}_i$. On the other hand, if $x_{s_{<i}}$ is good, then $H_{\min}^{\gamma_i}(X_{S_i}|X_{s_{<i}}=x_{s_{<i}},S_{<i}=s_{<i},S_iE)_\rho\geq\tilde{k}_i$, which implies $H_{\min}^{\gamma_i}(X_{S_i}|X_{s_{<i}}=x_{s_{<i}},S_{<i}=s_{<i},S_iE)_\sigma\geq\tilde{k}_i$.

■

4.2 Extraction from block-sources

We introduce a generic procedure of extraction from (smooth quantum) block-sources. The simple idea, again taken from [36], is to first extract from the last block in the block-source, then treat the newly extracted bits together with the original seed as the new seed to extract from the second to last block of the source, and so on. The complete procedure is described in Figure 2.

Extraction from quantum block-sources

Let $X = (X_1, \cdots, X_t) \in \{0,1\}^{n_1} \times \cdots \{0,1\}^{n_t}$ and $\rho_{X_1 \cdots X_t E}$ a (smooth) quantum $(k_1, k_2, \cdots, k_t)$ block-source with t blocks.

For $i \in \{1, \ldots, t\}$ let $\mathrm{Ext}_i : \{0,1\}^{n_i} \times \{0,1\}^{d_i} \to \{0,1\}^{m_i}$ be quantum strong (k_i, ϵ_i) extractors such that $d_{t-i} \leq d_t + \sum_{j=t-i+1}^{t} m_j$. Let $N = \sum_{i=1}^{t} n_i$ and $M = \sum_{i=1}^{t} m_i$.

Construct $\mathrm{BSExt} : \{0,1\}^N \times \{0,1\}^{d_t} \to \{0,1\}^M$ as follows:

1. Let $Y_t = U_{d_t}$ be the seed. Let $Z_t = \mathrm{Ext}_t(X_t, Y_t)$.
2. For $i = 1, \ldots, t-1$ let Y_{t-i} be the length d_{t-i} prefix of the concatenated string $(Y_t, Z_t, \ldots, Z_{t-i+1}) = (Y_{t-i}, \overline{Y_{t-i}})$. Let $Z_{t-i} = \mathrm{Ext}_{t-i}(X_{t-i}, Y_{t-i})$.
3. Return $Z = (Z_1, Z_2, \cdots, Z_t)$.

Figure 2: Construction of the block-source extractor BSExt.

Theorem 4.3 *Let $\rho_{X_1 \cdots X_t E}$ be a smooth quantum $(k_1, \ldots, k_t)$ block-source with smooth error $(\gamma_1, \ldots, \gamma_t)$, and $\mathrm{BSExt} : \{0,1\}^N \times \{0,1\}^{d_t} \to \{0,1\}^M$ the procedure described in Figure 2. Then*

$$\left\| \rho_{\mathrm{BSExt}((X_1, \ldots, X_t), Y_t) Y_t E} - U_M \otimes U_{d_t} \otimes \rho_E \right\|_{\mathrm{tr}} \leq \sum_{i=1}^{t} (\epsilon_i + 2\gamma_i).$$

Proof. By assumption, $H_{\min}^{\gamma_t}(X_t | X_{t-1} \cdots X_1 E)_\rho \geq k_t$, thus if $Y_t = U_{d_t}$ is a uniform seed, using e.g. [12, Lemma 3.5] we get

$$\left\| \rho_{Z_t Y_t X_{t-1} \cdots X_1 E} - U_{m_t} \otimes U_{d_t} \otimes \rho_{X_{t-1} \cdots X_1 E} \right\|_{\mathrm{tr}} \leq \epsilon_t + 2\gamma_t.$$

Now rearrange (Y_t, Z_t) as $(Y_{t-1}, \overline{Y_{t-1}})$ and note that again by definition $H_{\min}^{\gamma_{t-1}}(X_{t-1} | X_{t-2} \cdots X_1 E)_\rho \geq k_{t-1}$. Applying Ext_{t-1}, by the triangle inequality and Fact 2.1 we get

$$\left\| \rho_{Z_{t-1} Z_t Y_t X_{t-2} \cdots X_1 E} - U_{m_{t-1}} \otimes U_{m_t} \otimes U_{d_t} \otimes \rho_{X_{t-2} \cdots X_1 E} \right\|_{\mathrm{tr}} \leq (\epsilon_t + 2\gamma_t) + (\epsilon_{t-1} + 2\gamma_{t-1}).$$

Repeating this argument t times proves the theorem. ■

4.3 Zuckerman's extractor is quantum-proof

We combine the tools developed in the previous section to show that Zuckerman's extractor construction is quantum-proof. Let ρ_{XE} be an (n,k) quantum source. For the whole section we assume the source has min-entropy rate $\mu = k/n$ that is a positive constant less than 1.[6] We show how to construct a strong quantum-proof extractor Ext_Z that uses seed length $d = O(\log(n/\epsilon))$ to extract $m = k/2$ bits from X for every $\epsilon \geq \Omega(2^{-O(n^{1-\alpha})})$ for any constant $\alpha > 0$ (see Theorem 4.6 for a complete statement). We do so by iteratively composing extractors using the block-sampling and then block-extraction framework to improve parameters, starting from the almost two-universal hashing $\mathrm{Ext}_{\mathrm{hash}}$ from Corollary 2.12. This is done in two steps, as follows.

---

[6] The construction can be extended to sub-constant rates, but analyzing the constant regime is simpler and will ultimately be sufficient for our purposes.

1. In the first step, we combine the block-sampling and then block-extraction framework described in the previous sections, instantiated with a quantum sampler from Lemma 4.1, with an existing quantum-proof seeded extractor, the almost two-universal hashing $\mathrm{Ext}_{\mathrm{hash}}$ from Corollary 2.12. This yields a quantum-proof extractor with seed length $O(\log(n)\log(n/\epsilon))$ and output length $\Omega(k)$, which we denote by $\mathrm{Ext_Z}^1$. We then use Lemma 2.14 to increase the output lenght to $k/2$; denote the resulting extractor by $\mathrm{Ext_Z}^{1'}$. Note that $\mathrm{Ext_Z}^{1'}$ is already a significant improvement over $\mathrm{Ext}_{\mathrm{hash}}$.
2. In the second step, we repeat a similar procedure as in the first step but in addition to $\mathrm{Ext}_{\mathrm{hash}}$, we use the improved extractor $\mathrm{Ext_Z}^{1'}$ from the first step. This yields a quantum-proof extractor $\mathrm{Ext_Z}^2$ with seed length $O(\log\log(n)\cdot\log(n/\epsilon))$ and output length $\Omega(k)$, which can again be increased to $k/2$ by Lemma 2.14. Iterating $\log^*(n)$ times we obtain a quantum-proof extractor $\mathrm{Ext_Z}^{\log^*(n)'}$ with seed length $O(\log(n/\epsilon))$.

We formalize the above two steps in the following two lemmas.

Lemma 4.4 *For every constants $\alpha, \mu \in (0,1)$, for every n, and $\epsilon_0 > 2^{-O(n^{1-\alpha})}$, there exists an efficient $(k = \mu n, \epsilon)$ strong quantum-proof extractor $\mathrm{Ext_Z}^{1'} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with $\epsilon = O((\log n)\cdot\epsilon_0)$, $d = O((\log n)\cdot\log(n/\epsilon_0))$, and $m = k/2$.*

Proof. We first construct an extractor $\mathrm{Ext_Z}^1$ with the same parameters as $\mathrm{Ext_Z}^{1'}$ but output length $m = \Omega(\mu\cdot k)$, then apply Lemma 2.14 to increase the output length to $m = k/2$ at the cost of increasing the seed length and error by a factor of $\Omega(1/\mu)$.

$\mathrm{Ext_Z}^1$ is obtained by composing a sampling step (Theorem 4.2) and extraction from block-sources (Theorem 4.3) with $\mathrm{Ext}_{\mathrm{hash}}$. In other words, $\mathrm{Ext_Z}^1$ first converts the source into a block source, and then extracts from the block source using $\mathrm{Ext}_{\mathrm{hash}}$. For this we need to set the parameters for the converter (Theorem 4.2) and the block-source extractor (Theorem 4.3). The key requirement is for the size of each block $|S_i|$ to be such that each block has the right amount of entropy to perform block-source extraction. We set the parameters as follows:

- Error parameters τ, γ_i, and ϵ_i, for $i \in [t]$, are all set to ϵ_0. The sampling error parameter β_i is set to $\beta_i = 0.01$ for every $i \in [t]$.
- We set the total "sampling budget" $\sum_j |S_j| \le 0.01k$. This will ensure that $k_i \ge k - \sum_j |S_j| - \log(1/\tau) \ge 0.98k$ for each $i \in [t]$, so $\mu_i = k_i/n_i \ge 0.98\mu$, and the sampled blocks have entropy rate $(1-\beta_i)\mu_i \ge 0.97\mu$.
- Let $d_t = O(\log(n/\epsilon_0)$ be the seed length of $\mathrm{Ext}_{\mathrm{hash}}$, as specified in Corollary 2.12. We set $|S_t| = 0.02d_t/(0.97\mu)$ so that the sampled block X_{S_t} has $0.02d_t$ bits of entropy, and $m_t = 0.01d_t$. Then we set $d_{t-j} = (1.01)^j d_t$, $|S_{t-j}| = (1.01)^j\cdot|S_t|$, and $m_{t-j} = (1.01)^j m_t$. We set t to be the largest possible value such that our requirement $\sum_j |S_j| \le 0.01k$ holds.[7]

This setting of parameters in particular ensures that we can indeed apply $\mathrm{Ext}_{\mathrm{hash}}$ to extract from the sampled block-source. In addition, the number of blocks $t = O(\log n)$, the seed length $d = t\cdot O(\log(n/\epsilon_0)) + d_t = O(\log n\cdot\log(n/\epsilon_0))$, the output length $\sum_j m_j = \Omega(\mu\cdot\sum_j |S_j|) = \Omega(\mu k)$, and the error $\epsilon = O(t\cdot\epsilon_0) = O(\log n\cdot\epsilon_0)$, as claimed. ■

---

[7] In the boundary case where $0.02d_0/(0.97\mu) > 0.01k$, we can directly use $\mathrm{Ext}_{\mathrm{hash}}$ to extract $\Omega(k)$ bits from X.

Lemma 4.5 *For every constants $\mu, \alpha \in (0,1)$, for every integers s and n, and any $\epsilon_0 > 2^{-O(n^{1-\alpha})}$, there exists an efficient $(k = \mu n, \epsilon)$ strong quantum-proof extractor $\mathrm{Ext_Z}^{s'}$ with $\epsilon = O((\log n)^s \cdot \epsilon_0)$, $d = O((\log^{(s)} n) \cdot \log(n/\epsilon_0))$, and $m = k/2$.*

Proof. We prove the lemma by induction on s. Note that the base case $s = 1$ is exactly Lemma 4.4. Assuming the lemma holds for $s-1$, we prove the lemma for s.

As in the proof of Lemma 4.4, we first construct an extractor $\mathrm{Ext_Z}^s$ with the same parameters as $\mathrm{Ext_Z}^{s'}$ but output length $m = \Omega(\mu \cdot k)$, then apply Lemma 2.14 to increase the output length to $m = k/2$ at the cost of increasing the seed length and error by a factor of $\Omega(1/\mu)$. $\mathrm{Ext_Z}^s$ is constructed in the same way as $\mathrm{Ext_Z}^1$ by composing Theorems 4.2 and 4.3, but using $\mathrm{Ext_Z}^{(s-1)'}$ instead of $\mathrm{Ext_{hash}}$ as a starting point.

Recall that in the construction of $\mathrm{Ext_Z}^1$, we need $t = O(\log n)$ blocks to extract $\Omega(\mu k)$ bits of entropy using $\mathrm{Ext_{hash}}$, since $\mathrm{Ext_{hash}}$ requires seed length $\Omega(m)$ to extract m bits. With $\mathrm{Ext_Z}^{(s-1)'}$, we only need to collect $O((\log^{(s-1)} n) \cdot \log(n/\epsilon_0))$ bits of seed from blocks $X_{S_2}, \ldots, X_{S_t}$ using $\mathrm{Ext_{hash}}$, and then use $\mathrm{Ext_Z}^{(s-1)'}$ to extract $\Omega(\mu \cdot k)$ bits from the first block X_{S_1} of length $\Omega(k)$. This reduces the number of blocks to $O(\log^{(s)} n)$ and improves the seed length to $d = O((\log^{(s)} n) \cdot \log(n/\epsilon_0))$. More precisely, we set the parameters as follows.

- We set all the error parameters τ, γ_i, and ϵ_i, for $i \in \{2, \ldots, t\}$, to equal ϵ_0, We set the sampling error parameter $\beta_i = 0.01$ for every $i \in [t]$.
- We instantiate Ext_1 as $\mathrm{Ext_Z}^{(s-1)'}$, so $d_1 = O((\log^{(s-1)} n) \cdot \log(n/\epsilon_0))$ and $\epsilon_1 = O((\log n)^{s-1} \cdot \epsilon_0)$. We keep $\gamma_1 = \epsilon_0$.
- We set the total "sampling budget" to satisfy $\sum_j |S_j| \leq 0.01k$. This implies that $k_i \geq k - \sum_j |S_j| - \log(1/\tau) \geq 0.98k$ for all $i \in [t]$, so $\mu_i = k_i/n_i \geq 0.98\mu$, and the sampled blocks have entropy rate $(1-\beta_i)\mu_i \geq 0.97\mu$.
- Let $d_t = O(\log(n/\epsilon_0)$ be the seed length of $\mathrm{Ext_{hash}}$, as specified in Corollary 2.12. We set $|S_t| = 0.02 d_t/(0.97\mu)$ so that the sampled block X_{S_t} has $0.02d_t$ bits of entropy, and $m_t = 0.01d_t$. Then we set $d_{t-j} = (1.01)^j d_t$, $|S_{t-j}| = (1.01)^j \cdot |S_t|$, and $m_{t-j} = (1.01)^j m_t$ for $j < t-1$. We choose t to be the smallest $t \geq 2$ such that $d_t + \sum_{j=2}^t m_j \geq d_1$, and we set $|S_1| = 0.01k - \sum_{j=2}^t |S_j|$ to use up the "sampling budget".

With this setting of parameters we can indeed use $\mathrm{Ext_{hash}}$ to extract from blocks $t, t-1, \ldots, 2$, and then use $\mathrm{Ext_Z}^{(s-1)'}$ to extract from the first block. In addition, the number of blocks $t = O(\log^{(s)} n)$, the seed length $d = t \cdot O(\log(n/\epsilon_0)) + d_t = O(\log^{(s)} n \cdot \log(n/\epsilon_0))$, the output legnth $\sum_j m_j = \Omega(\mu \cdot \sum_j |S_j|) = \Omega(\mu k)$, and the error $\epsilon = O(t \cdot \epsilon_0) + \epsilon_1 = O(\log^{(s)} n \cdot \epsilon_0)$, as claimed. ■

Theorem 4.6 *For every constants $\alpha, \mu \in (0,1)$, for every n and $\epsilon = 2^{-O(n^{1-\alpha})}$, there exists an efficient $(k = \mu n, \epsilon)$ strong quantum-proof extractor $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with seed length $d = O(\log(n/\epsilon))$ and $m = k/2$.*

Proof. The theorem follows immediately by setting Ext to $\mathrm{Ext_Z}^{s'}$ in Lemma 4.5 with $s = \Theta(\log^* n)$. ■

Combining the above theorem together with Lemma 2.13 to extract (almost) all the entropy using a few independent seeds and then with Corollary 3.2 gives the following construction of an extractor.

Theorem 4.7 *For any constants* $0 < \alpha, \delta < 1$*, integers* n, k *and* $\epsilon > 0$ *such that* $k = \Omega(\log n + \log^{1+\alpha}(1/\epsilon))$ *there exists an efficient quantum-proof strong extractor* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$ *where* $d = (1+\delta)\log n + O(\log(k/\epsilon))$ *and* $m = (1-\delta)k/2$*.*

By applying Lemma 2.13 an additional constant number of times we can extract almost all the entropy from the seed, at the cost of a constant multiplicative blow-up in the seed length. This proves Theorem 1.5.

Acknowledgements

We thank Yanlin Chen, Yi-Hsiu Chen, Anindya De, Andrew Drucker, Robert König, Ashwin Nayak, Salil Vadhan, and Nengkun Yu for helpful discussions. Part of the research was conducted when KC and XW were visiting the Institute for Quantum Computing, University of Waterloo and we thank IQC for its hospitality. Part of the research was conducted while XW was affiliated with the Simons Institute for the Theory of Computing, University of California, Berkeley and with the Center for Theoretical Physics, Massachusetts Institute of Technology. TV was partially supported by NSF CAREER Grant CCF-1553477, an AFOSR YIP award, and the IQIM, an NSF Physics Frontiers Center (NFS Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028).

References

[1] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson. 2-source dispersers for sub-polynomial entropy and Ramsey graphs beating the Frankl-Wilson construction. In *Proceedings of the thirty-eighth annual ACM symposium on Theory of Computing*, pages 671–680. ACM, 2006.

[2] A. Ben-Aroya and A. Ta-Shma. Better short-seed quantum-proof extractors. *Theor. Comput. Sci.*, 419:17–25, 2012.

[3] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[4] C. H. Bennett, G. Brassard, and J. Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, 17(2):210–229, 1988.

[5] C. H. Bennett, G. Brassard, and J. M. Robert. How to reduce your enemy's information. In *Advances in Cryptology (CRYPTO)*, volume 218, pages 468–476. Springer, 1985.

[6] M. Berta, O. Fawzi, and V. B. Scholz. Quantum-proof randomness extractors via operator space theory. *arXiv preprint arXiv:1409.3563*, 2014.

[7] E. Chattopadhyay and D. Zuckerman. Explicit two-source extractors and resilient functions. Technical Report TR15-119, Electronic Colloquium on Computational Complexity, 2015.

[8] G. Cohen. Two-source dispersers for polylogarithmic entropy and improved Ramsey graphs. *arXiv preprint arXiv:1506.04428*, 2015.

[9] G. Cohen. Making the most of advice: New correlation breakers and their applications. Technical Report TR16-052, Electronic Colloquium on Computational Complexity, 2016.

[10] G. Cohen and L. Schulman. Extractors for near logarithmic min-entropy. Technical Report TR16-014, Electronic Colloquium on Computational Complexity, 2016.

[11] M. Coudron, T. Vidick, and H. Yuen. Robust randomness amplifiers: Upper and lower bounds. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 468–483. Springer, 2013.

[12] A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan's extractor in the presence of quantum side information. *SIAM J. Comput.*, 41(4):915–940, 2012.

[13] A. De and T. Vidick. Near-optimal extractors against quantum storage. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 161–170. ACM, 2010.

[14] Y. Dodis and D. Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *Proceedings of the forty-first annual ACM Symposium on Theory of Computing*, pages 601–610. ACM, 2009.

[15] Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. *SIAM J. Comput.*, 42(6):2305–2328, 2013.

[16] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM J. Comput.*, 38(5):1695–1708, 2008.

[17] O. Goldreich and D. Zuckerman. Another proof that BPP $\subseteq$ PH (and more). Technical Report TR97-045, Electronic Colloquium on Computational Complexity, 1997.

[18] V. Guruswami, C. Umans, and S. P. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *J. ACM*, 56(4), 2009.

[19] P. Hausladen and W. K. Wootters. A "pretty good" measurement for distinguishing quantum states. *Journal of Modern Optics*, 41(12):2385–2390, 1994.

[20] A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Transactions on Information Theory*, 44(1):269 –273, 1998.

[21] R. Kasher and J. Kempe. Two-source extractors secure against quantum adversaries. *Theory of Computing*, 8(21):461–486, 2012.

[22] R. König, U. M. Maurer, and R. Renner. On the power of quantum memory. *IEEE Transactions on Information Theory*, 51(7):2391–2401, 2005.

[23] R. König and R. Renner. Sampling of min-entropy relative to quantum knowledge. *IEEE Transactions on Information Theory*, 57(7):4760–4787, 2011.

[24] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9):4337–4347, Sept 2009.

[25] R. König and B. Terhal. The bounded-storage model in the presence of a quantum adversary. *IEEE Transactions on Information Theory*, 54(2):749–762, 2008.

[26] X. Li. Improved constructions of three source extractors. In *2011 IEEE 26th Annual Conference on Computational Complexity (CCC)*, pages 126–136. IEEE, 2011.

[27] X. Li. Design extractors, non-malleable condensers and privacy amplification. In *Proceedings of the forty-fourth annual ACM Symposium on Theory of Computing*, pages 837–854, 2012.

[28] X. Li. Non-malleable condensers for arbitrary min-entropy, and almost optimal protocols for privacy amplification. *arXiv preprint arXiv:1211.0651*, 2012.

[29] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[30] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 417–426. ACM, 2014.

[31] D. Moshkovitz. Parallel repetition from fortification. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 414–423. IEEE, 2014.

[32] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel. On quantum Rényi entropies: A new generalization and some properties. *Journal of Mathematical Physics*, 54(12):122203, 2013.

[33] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Foundations of Computer Science, 1999. 40th Annual Symposium on*, pages 369–376. IEEE, 1999.

[34] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, UK, 2000.

[35] N. Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12(4):449–461, 1992.

[36] N. Nisan and D. Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–52, 1996.

[37] J. Radhakrishnan and A. Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM Journal on Discrete Mathematics*, 13(1):2–24, 2000.

[38] R. Raz, O. Reingold, and S. Vadhan. Extracting all the randomness and reducing the error in Trevisan's extractors. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, pages 149–158, 1999.

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

[40] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, pages 407–425. Springer, 2005.

[41] L. J. Schulman and D. Zuckerman. Asymptotically good codes correcting insertions, deletions and transpositions. *IEEE Transactions on Information Theory*, 45(7):2552–2557, 1999.

[42] R. Shaltiel. An introduction to randomness extractors. In *Automata, languages and programming*, pages 21–41. Springer, 2011.

[43] R. Shaltiel and C. Umans. Simple extractors for all min-entropies and a new pseudorandom generator. *Journal of the ACM*, 52(2):172–216, 2005.

[44] A. Srinivasan and D. Zuckerman. Computing with very weak random sources. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pages 264–275, 1994.

[45] M. Sudan, L. Trevisan, and S. Vadhan. Pseudorandom generators without the XOR lemma. In *Proceedings of the thirty-first annual ACM symposium on Theory of Computing*, pages 537–546. ACM, 1999.

[46] A. Ta-Shma. Short seed extractors against quantum storage. *SIAM J. Comput.*, 40(3):664–677, 2011.

[47] A. Ta-Shma and C. Umans. Better condensers and new extractors from Parvaresh-Vardy codes. In *Proceedings of the 27th Conference on Computational Complexity, CCC 2012, Porto, Portugal, June 26-29, 2012*, pages 309–315, 2012.

[48] M. Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*, volume 5. Springer, 2015.

[49] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, 2011.

[50] L. Trevisan. Extractors and pseudorandom generators. *J. ACM*, 48(4):860–879, 2001.

[51] S. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology*, 17(1):43–77, 2003.

[52] S. Vadhan. Pseudorandomness. *Foundations and Trends in Theoretical Computer Science*, 2011.

[53] U. Vazirani and T. Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 61–76. ACM, 2012.

[54] A. Wigderson and D. Zuckerman. Expanders that beat the eigenvalue bound: Explicit construction and applications. *Combinatorica*, 19(1):125–138, 1999.

[55] M. M. Wilde. *Quantum information theory.* Cambridge University Press, 2013.

[56] J. Wullschleger. Bitwise quantum min-entropy sampling and new lower bounds for random access codes. In *Theory of Quantum Computation, Communication, and Cryptography*, pages 164–173. Springer, 2011.

[57] D. Zuckerman. Randomness-optimal oblivious sampling. *Random Structures and Algorithms*, 11:345–367, 1997.