Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions

Kai-Min Chung[*] Yaoyun Shi[†] Xiaodi Wu[‡]

Abstract

How can one be certain that the output of an alleged random number generator is indeed random? The mathematical theory of randomness extraction requires two or more *independent* weak randomness sources for ensuring output quality. To circumvent this fundamental yet hard-to-enforce limit, we formulate precisely a model of extracting randomness from non-interacting and untrusted quantum devices, and base security on the validity of physical theories. We further construct the first such extractor that uses a single and arbitrarily weak source and is secure against all-powerful quantum adversaries. Our construction can reach a close-to-optimal error parameter, and is efficient in several configurations. In conjunction with Miller-Shi (arXiv:1402.0489), it can tolerate a constant level of device imperfection, produce an arbitrarily long and near-prefect random output, using just one source of only a constant amount of weak randomness.

Our result also implies a strong "dichotomy" that unless the world is deterministic, we can experimentally create arbitrarily many inherently random events and be confident of their unpredictability. This provides both a practical and the strongest known method for mitigating the Freedom-of-Choice loophole in Bell test experiments.

A main technical contribution is our "Equivalence Lemma," which states that the performance of a physical extractor remains unchanged when its globally uniformly random input is replaced by an input uniform only to the devices. This principle for the secure composition of untrusted-device protocols has found several other applications.

Version differences. The main additions to this version are the definition of physical extractors and a technical improvement on the completeness of the master protocol through modifying the acceptance criterion and a corresponding new analysis. The master protocol now does not require the strong notion of sub-protocol completeness, and is now robust on all min-entropies, without the earlier constraint that $k = \Omega(\text{polylog}(n))$ on the (n, k) source. (Without robustness, the previous protocol already works on all min-entropies.)

[*] Institute of Information Science, Academia Sinica, Taiwan.

[†] Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48103, USA.

[‡] Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA and Simons Institute for the Theory of Computing, University of California, Berkeley, CA 94720, USA. Most of work was conducted while the author was a student at the University of Michigan, Ann Arbor.

1 Introduction

Background and motivations. Randomness is not only a universal human experience, but also a vital resource for modern day information processing. The wide range of applications relying on randomness include cryptography, fast randomized algorithms, accurate physical simulations, and gambling. In practice, randomness is generated through a "random number generator," such as Intel's on chip generator `RdRand` and Linux's software random number generator `/dev/random`.

An important question is: *How can one be certain that the output of an alleged random number generator is indeed random?* Since it is impossible to decide if a number is drawn from a uniform distribution or fixed [1], one reduces the output quality to assumptions on the input to the generator and the algorithmic property of the generator itself.

The Linux's random number generator, for example, assumes that its randomness sources provide sufficient quantity of randomness of little correlation, and that the deterministic stretched output is computationally infeasible for the adversary to differentiate from true randomness. All those assumptions can fail completely, as reported by a large body of computer security research (see, e.g., [13, 24, 14, 1].) The vulnerabilities of random number generators directly threaten the security of all cryptographic protocols, and risk invalid conclusions from computations assuming true randomness. It is therefore desirable to construct random number generators that are secure against all powerful adversaries with a minimal set of assumptions ensuring such security.

The classical theory for this objective is that of *randomness extractors* (see, e.g., [26].) In this theory, an extractor is a deterministic algorithm that transforms several sources of weak randomness into near-perfect randomness. The amount of randomness in a weak source is quantified by the notion of *min-entropy* (or conditional quantum min-entropy when the adversary is quantum), which describes the best chance of the source being correctly guessed by the adversary [29, 22, 23]. A fundamental limit discovered in this theory is that true randomness extraction is possible only when *two or more independent* sources are available. In particular, deterministic extraction, i.e. using just one weak source without additional independent randomness, is known to be impossible to produce even 1 bit of true randomness, as shown by Santha and Vazirani [25] for the highly random and highly structured Santa-Vazirani (SV) sources. Since independence is impossible to check [2] and difficult to guarantee in practice, the classical theory of randomness extractors inevitably relies on assuming *independence*. Can we get around this fundamental assumption?

Quantum mechanics promises true randomness in its postulate, thus appears to provide a simple solution to the above question. Indeed, commercial products are already available, touting fast and secure random number generation based on quantum technologies. [3] However, that the quantum devices work according to the specifications is again a strong assumption undesirable for at least three reasons. First, as classical beings, we can only perform classical operations, hence cannot directly verify the inner-workings of quantum devices. Second, we may not want to trust the claims of the manufacturers or the certifying government agencies. Finally, even if we decide to trust those parties, the quantum devices may not work properly due to technological limitations. No method has been reported for reliably implementing quantum devices in large scale.

Is it possible to generate true randomness from quantum devices *without* trusting their inner-workings? We point out that the existence of untrusted devices alone (i.e., without any min-entropy

[1] This is because the uniform distribution is a convex combination of deterministic "distributions."

[2] Because a convex combination of several independent distributions can be far from independent.

[3] E.g. the Quantis generators by IDQuantique.

source) is insufficient. Since the extraction procedure is deterministic, the devices can preprogram their deterministic answers without generating any randomness. We also note that the a single min-entropy source alone (i.e. without an additional resource) is also insufficient due to the impossibility of deterministic extraction. Thus, we arrive at a *minimal* set of assumptions, a single min-entropy source and several untrusted devices that may correlate with the source. It is natural to ask:

> *(Q) Can we generate (almost) uniform randomness against all-powerful quantum adversaries from an arbitrary min-entropy source and possibly correlated untrusted quantum devices?*

Physical Randomness Extractors. We note that (Q) is not entirely new as related questions have been studied in the paradigm of "untrusted-device," or "device-independent," quantum cryptography, where the goal is to *certify higher quality* randomness from untrusted devices using *lower quality* randomness. Previously, the questions come with two flavors—the task of *randomness expansion* for certifying *long* almost pure randomness from *short* uniform seeds, and the task of *randomness amplification* for certifying a single *close-to-uniform* bit from a Santha-Vazirani (SV) source.

Those studies naturally lead us to the following model of "Physical Randomness Extractor" (PRE) for a precise formulation for and an answer to (Q). In this model, we abandon min-entropy as the only description of a source, and allow an interactive "physical source," which is capable of generating true randomness yet is subject to the laws of physics. While the classical extraction theory does not refer to physical laws, the security of a PRE relies on the validity of physical theories. Such security may appear weaker, we argue, however, that it entails no loss practically since all randomness extractors will be eventually deployed in the physical world. On the other hand, this reliance on physical theories hopefully would further reduce the set of necessary assumptions. For concreteness, we give a formal definition of physical extractors with the physical resource being untrusted quantum devices. A schematic illustration of a physical randomness extractor is in Fig. 1.

Our affirmative answers to (Q). With the above formulation of PREs, we give a general method for their explicit construction, illustrated in Fig. 2. For a single and arbitrarily weak min-entropy source, our construction outputs close to uniform randomness, with a range of choices for the tradeoffs among the key parameters — the error parameter, the number of devices used, and the running time (which is typically proportional to the number of device usages.) [4] The error parameter describes both the chance of being fooled by the adversary and the failure probability on an honest implementation. Thus, instantiations of our general construction provide affirmative answers to (Q) in various scenarios. The main theorem is stated informally as Theorem 1.3 and formally as Theorem 6.3. Here we highlight two cases of particular interest.

The first is the extreme case when the input min-entropy is merely a constant while the length is polynomial in the security parameter. [5] The output of our construction for this case has a close to optimal error parameter and at the same time efficient (that is, runs in time polynomial in the security parameter.)

[4] Note that due to the existence of unbounded expansion protocols that use a constant number of devices [9, 19], the output length can be made arbitrarily large, thus is not essential for the tradeoffs. The error parameter, however, accumulates in each stage of the protocol.

[5] In cryptography, the security parameter is an increasing positive integer against which other parameters are measured.

Corollary 1.1 (Constant Error Extraction) *For any constant $\epsilon \in (0,1)$, there exists $k = k(\epsilon)$, such that on an arbitrary classical source of k min-entropy, the composed protocol in Fig. 2 with appropriately chosen parameters outputs an arbitrarily long string with error $\leq \epsilon$.*

A second important case is for high min-entropy rate.

Corollary 1.2 (High Min-entropy Extraction) *Suppose that both the input length and the input min-entropy are polynomially in the security parameter. With appropriately chosen parameters, the composed protocol in Fig. 2 achieves inverse polynomial error and is efficient.*

We point out two additional desirable features of our constructions. The first is that our construction (for all parameters [6]) can be made robust against a constant level of device imprecision, by making use of the Miller-Shi robust randomness expansion protocol [19]. The second is that we can always achieve a close-to-optimal error parameter for all min-entropy sources, at the expense of the running time and the number of devices. The final running time and the number of devices may still remain efficient if the security parameter is polynomially related to the output length and is sufficiently large with respect to the min-entropy.

Physical Implications. "Are there fundamentally random processes in nature?" Colbeck and Renner [8] first raised this fundamental question. As they pointed out, while quantum mechanics predicts the existence of true randomness, the experimental confirmation for such prediction (i.e. through Bell tests) requires that the experimental settings can be chosen "freely at random." This circular argument leaves it possible that our world may not have free randomness. Note that one has to assume that the world is not deterministic for the question to be valid[7]. They thus sought to identify the minimal conditions for amplifying "free randomness."

More precisely, they model weak randomness in Nature as a sequence of bits $X = x_0 x_1 \cdots x_n \cdots$, such that each x_i is of a constant bias ϵ, conditioned on previous bits and all side information about X. Such a source is precisely a *Santha-Vazirani* (SV) source, from which it is known that deterministically extracting even a single bit is impossible. The bias ϵ quantifies the amount of free randomness. Thus to amplify the free randomness is to generate a bit with a bias arbitrarily close to 0. Under a technical assumption that X is independent of the devices conditioned on the side information, they succeeded when the initial bias is sufficiently small, while the subsequent improvement by Gallego *et al.* [12] allows an arbitrarily small ϵ.

It appears to us that modeling weak randomness as a SV source is an unnecessarily restrictive assumption about Nature. This is because an SV source is highly structured and highly random (that is, the min-entropy is linear in its length.) In contrast, using the min-entropy as the only parameter (in addition to its length) for characterizing a weak source is much more general. This is not only a mathematical fact, but also allows the physical systems generating the weak randomness to consist of multiple, strongly correlated sub-systems. Since our protocol is valid on any arbitrarily weak random source and achieves close to optimal quality parameters, we arrive at the following "dichotomy" stronger than that in [12]. Unless the world is deterministic, we can create arbitrarily

[6] For the construction in the QIP version of this paper to be robust, it requires the min-entropy being at least polylogarithmic of the input length.

[7] Note that there is no logical contradiction between the validity of quantum mechanics and the world being deterministic. This is because although quantum mechanics makes correct predictions (about classical observables) in the world, it does not necessarily characterize the inner-workings of the world and there could be a deterministic alternative that makes exactly the same predictions.

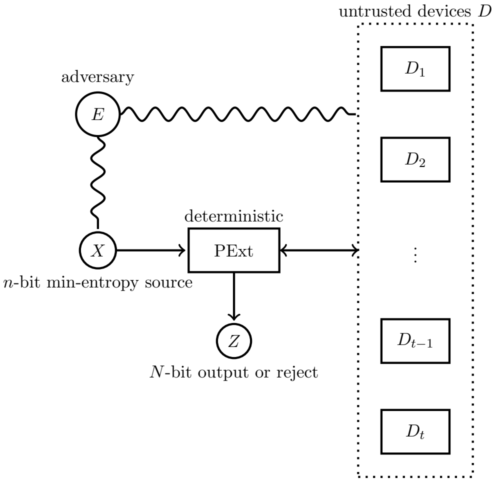

Figure 1: The general scheme of a physical randomness extractor. In the case of the physical resources being t untrusted and non-communicating quantum devices, each quantum device is represented as D_i, $1 \leq i \leq t$. The quantum adversary E may be correlated with the min-entropy source X and in an unknown quantum entanglement with the devices.

many and inherently random events (i.e. the joint distribution of those events are close to uniform) in laboratories and be confident of their unpredictability. In particular, each of those events is arbitrarily free.

Our work further provides a strongest possible mitigation to the “Freedom-of-Choice” loophole for rejecting hidden variable theory through experimentally observing the violation of Bell Inequalities. A sequence of recent research (e.g., see references in [8]) has demonstrated that such quantum violations require the classical signals used in the experiments to be close to uniform. The “Freedom-of-Choice” loophole refers to the possibility that the input signals do not reach the required level of randomness. Since the world may very well be deterministic, the loophole cannot be completely closed. Our method provides an approach for demonstrating Bell violations assuming only a constant amount of min-entropy in the initial randomness — by first running our protocol to produce true randomness, which is then used directly for the Bell tests. The robustness feature further facilitates practical implementations using the current technology.

Key elements of physical randomness extractors. We describe here several key elements in our formal definition of physical randomness extractors. They are instrumental in facilitating rigorous and intuitive reasonings, and provide the necessary vocabulary for a more technical summary and discussions of our results. A comprehensive technical treatment will be given in Section 3.

An *untrusted-device (UD) physical system* consists of a min-entropy source X, a set of t untrusted devices $D = (D_1, \cdots, D_t)$, and an adversary E. The *state of the system* is a classical-quantum-quantum state ρ_{XDE}, where DE may be entangled arbitrarily, and together they hold certain quantum side information about X. As devices are untrusted, we do not assume their inner-workings and only allow classical interactions with them. Given such a physical system, a physical randomness extractor PExt is a (*classical*) *deterministic* algorithm that operates on X and D (through classical interactions), and outputs a decision $O = \mathsf{Acc}$ (for accept) or $O = \mathsf{Rej}$ (for reject), as well as a string $Z \in \{0,1\}^*$.

For a composite quantum system having a classical component X and a quantum component R, X is called (n,k)*-random-to-*R if $X \in \{0,1\}^n$ and the conditional quantum min-entropy of X on component R is at least k. Similarly, X is called *uniform-to-*R if $\rho_{XR} = \mathcal{U}_X \otimes \rho_R$, where $\mathcal{U}_X$ refers to the uniform distribution on X and ρ_{XR}, ρ_R are the reduced density operators for the subsystems XR and R, respectively. When the system is equipped with a decision bit $O \in \{\mathsf{Acc}, \mathsf{Rej}\}$, we call X *uniform-to-*R on Acc if $\rho_{XR}^{\mathsf{Acc}} = \mathcal{U}_X \otimes \rho_R^{\mathsf{Acc}}$, where ρ^{Acc} refers to the subnormalized state corresponding to accept. One can also extend the above definition to the approximate case. Namely, X is said to be ϵ-uniform-to-R in a state ρ if ρ is within trace distance ϵ to another state ρ' in which X is uniform-to-R.

A PRE PExt has a soundness error ϵ_s if on all implementations and any initial state of interest, the resulting system state is ϵ_s close to a state uniform-to-XE on Acc. It has a completeness error ϵ_c under a noise level η, if there exists an *ideal* implementation of the devices such that all devices deviating from this ideal implementation by at most an η level of noise must reject with $\leq \epsilon_c$ probability. When $\epsilon_c = \epsilon_s$, we refer to them by the "error parameter." Thus the error parameter describes both the chance of accepting an undesirable output (soundness) and the chance of mistakenly rejecting an honest (and possibly reasonably noisy) implementation (completeness.) An omitted η is assumed to be 0. We define noise in the same way as in [19]: an implementation $\tilde{\Pi}$ is within a noise level η from another implementation Π if on all input states and all interaction transcripts, the average (over the number of interactions) statistical distance between the output distributions of one use of the devices in Π and $\tilde{\Pi}$, conditioned on the same outcome of the previous interactions, is no more than η. This "black-box" definition of noise is fairly general as it includes adaptive adversarial noise, and is independent of the implanting technology.

Communication restrictions. Our framework of physical randomness extractors automatically includes a single classical min-entropy source and untrusted devices, which might be arbitrarily correlated with each other and with the adversary. This turns out to be a minimal set of assumptions as we argued in the previous section.

However, to achieve our main result, we need to impose communication restrictions on when and which untrusted devices can communicate. While there are occasional relaxations, our default assumption is to forbid any device-adversary and intra-device communications.

We remark that the device-adversary communication restriction is necessary, since otherwise, devices can leak all the generated entropy to the adversary and randomness extraction becomes trivially impossible. Similarly, some restriction on communications among devices is also necessary. Otherwise, the use of multiple untrusted devices can be effectively simulated by a single one, which can hence be simulated by a classical even deterministic device.[8] Our extraction task in that case is equivalent to deterministic extraction, which is simply impossible.

It may be desirable to allow intra-device communications at some fixed time during the protocol. As demonstrated in [19], their intra-device communication in-between rounds of playing the non-local games reduces the quantum memory requirement to a unit size. Special relativity provides a method for enforcing such short-lived communication restriction, by placing the devices at a distance too far for communication to be possible within the period of restriction. The required distance may be too far for restrictions of a long period of time. There may be additional reasons such that other alternatives to spatial separation may be more effective in practice.

[8] This is because deterministic devices are extreme points of the set of general classical randomized devices.

It is worthwhile to compare the assumptions we make here to the ones in traditional randomness extractors. We first note that the no-communication assumption is in fact implicit in traditional randomness extractors, since no-communication restriction from the sources to the adversary (which is not explicitly modeled) is again necessary and no-communication restriction among sources holds trivially. More importantly, recall that traditional randomness extractors require at least two *independence* sources, each with a certain amount of min-entropy. Here, we remove the independence assumption completely, and our main construction only requires a single source with $O(1)$ bits of min-entropy with respect to untrusted devices.

Technical challenges and our solution. The central idea behind all untrusted-device protocols is to exploit randomized interactions with the devices for the purpose of certifying their super-classical behavior. The interactions consist of multiple rounds of playing a "non-local game" with two or more non-communicating devices. The game is carefully selected so that the optimal quantum strategy performs better than the optimal classical strategy. For example, in the well-known CHSH game [7], two non-communicating players Alice and Bob are each given a bit x or y, respectively, and each outputs a bit a or b, respectively. They win the game if $a \oplus b = x \wedge y$. When the input bits are uniformly and independently distributed, the best winning chance for quantum strategies is $\cos^2 \pi/8 \approx .85$, comparing to .75 for classical strategies. The now standard "Bell tests" for rejecting local hidden variable theories are to play repeatedly such games with a theoretical quantum-classical gap, and verify that the observed winning statistics are significantly above the classical bound, which indicates that the strategies employed by the devices are genuinely quantum. Those quantum strategies often have the desired property that one party's outputs are close to uniform.

However, the above reasoning critically relies on the input bits for the non-local games being highly random. In particular, the quantum-classical gap is sensitive to the distribution of the input randomness, to an extent beyond its dependence on the usual measure (e.g., min-entropy) of the amount of randomness. For example, in the CHSH test, if the input distribution is uniform over just $\{(0,0),(0,1),(1,0)\}$, the quantum advantage vanishes even though the input still has a lot of min-entropy. Therefore, a distorted input distribution may completely fail to detect the quantum/classical separation, even if its min-entropy is just one bit below the ideal distribution.

This stringent requirement on the input distribution forces almost all existing results to rely on a fixed input distribution, such as the uniform distribution used in most results. Indeed, there are several protocols using uniform inputs, thus are *seeded* PREs. Those include protocols for randomness expansion [28, 9, 19], untrusted-device quantum key distribution [3, 27, 19], and delegation of quantum computation to untrusted devices [21].

The only exceptions are randomness amplification protocols using a single SV source, of which the distribution is not completely specified. However, SV sources are excellent "approximates" of uniform bits and behave similarly in many settings. Crucially relying on this fact, the analysis of [8, 12] exploits a brute-force approach which treats SV sources as if they were uniform bits. Although this tweak seems intuitive and reasonable, the analysis becomes much more complicated. To make it work technically, the protocol in [12] becomes non-constructive and loses almost all good properties when the source is uniform. In particular, it outputs only a single bit, which is significantly shorter than the min-entropy of the source.

We now need to deal with an arbitrary min-entropy source. The above difficulty amplifies since the source does not have the nice structure of SV sources. A naive approach is to improve the quality of the source to (almost) uniform, so that the problem is reduced to the seeded case (for which several

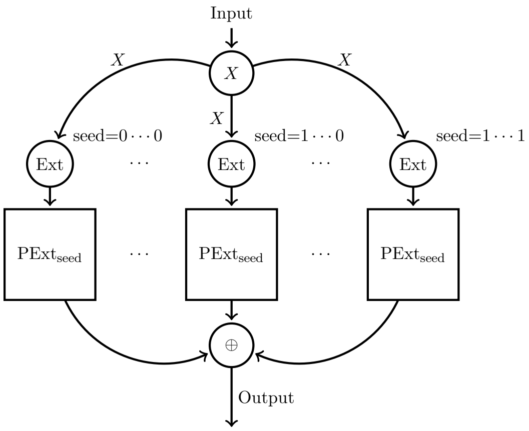

Figure 2: Illustration of Our Physical Randomness Extractor PExt.

solutions are available.) However, this reduction idea may appear too wishful for at least two reasons. First, generating uniform bits is precisely the original goal, thus cannot be used as an intermediate step. Second, due to the impossibility of deterministic extraction, it is hopeless to do so by deterministic operations on the source, before the application of a seeded extraction.

What we accomplish is precisely such a general reduction from seedless extraction with an arbitrary min-entropy source to seeded extraction. We circumvent both of the above difficulties through two steps. In the first step, we generate what we call "quantum somewhere randomness," which consists of blocks of strings one of which is guaranteed to be (close to) uniformly random with respect to the device-adversary system. We make use of existing constructions of quantum-proof classical seeded strong extractors to accomplish this step. What we need next is a certification protocol that is "randomness decoupling," in the sense that it transforms uniform-to-device input to a secure output (i.e. almost uniform to the adversary.) A central technical result of this work is an "Equivalence Lemma," which states that for any certification protocol, replacing its globally uniform input to one that is just uniform-to-device does not change its performance parameters. The equivalence lemma thus allows one to use any seeded PRE $\mathrm{PExt}_{\mathrm{seed}}$ as a randomness decoupler. The last subtlety in our proof is to bound the soundness error of our protocol. Our definition of soundness simplifies the analysis. A schematic illustration of our composition scheme is in Fig. 2. We state our main theorem below and explain with some more details on each of the key concepts involved.

Theorem 1.3 (Main Theorem; formally stated in Theorem 6.3) *Given any quantum-proof strong randomness extractor* Ext *and any seeded PRE* $\mathrm{PExt}_{\mathrm{seed}}$ *(with appropriate parameters), their composition as illustrated in Fig. 2 gives a PRE* PExt *for any random-to-device min-entropy source (with corresponding parameters.) Furthermore, if* $\mathrm{PExt}_{\mathrm{seed}}$ *is robust, so is* PExt*.*

Somewhere Random Source. A classical somewhere random source $\mathbf{S}$ is simply a sequence of random variables $\mathbf{S} = (S_1, \ldots, S_r)$ such that the marginal distribution of some block S_{i^*} is (close to) uniform (but there could be arbitrary correlation among them.) It is not hard to see that one can turn a source X into a somewhere random source $\mathbf{S}$ using a strong randomness extractor Ext by simply letting $S_i = \mathrm{Ext}(X, i)$ for every possible seed i, and the property of extractor ensures that at least one block S_{i^*} (actually many of them) is close to uniform. In the quantum setting, one just needs to choose a *quantum-proof* strong randomness extractor Ext (see Section 5 for more details) such that at least one block S_{i^*} (actually many of them) is close to uniform even against the quantum adversary.

Given the existence of such a "close-to-uniform" block S_{i^*}, it becomes hopeful to make use of known protocols in the uniform case ($\mathrm{PExt}_{\mathrm{seed}}$ in this case.) Since the index i^* is unknown, we invoke $\mathrm{PExt}_{\mathrm{seed}}$ to each block S_i with *distinct* set of devices D_i, each of which outputs a decision bit $O_i \in \{\mathsf{Acc}, \mathsf{Rej}\}$ and an output string Z_i. The PRE then accepts iff $\forall i, O_i = \mathsf{Acc}$, and outputs $Z = \bigoplus_i Z_i$ in that case.

Intuitively, this could work since on the "close-to-uniform" block S_{i^*}, if $O_{i^*} = \mathsf{Acc}$, then Z_{i^*} is close to uniform with respect to the environment by the property of $\mathrm{PExt}_{\mathrm{seed}}$, which seems to imply that $Z = Z_{i^*} \oplus \left(\bigoplus_{i \neq i^*} Z_i\right)$ is also close to uniform.

However, there is a serious flaw in the above argument. To identify the issue, it is helpful to note that while S_{i^*} is close to uniform, $\bigoplus_i S_i$ is not necessarily close to uniform, due to the possible correlation among them. Our key observation here is to prevent such correlation among Z_i's by exploiting the property of seeded PREs. It is hoped that by considering the remaining system S_{-i^*}, D_{-i^*} as the adversary for $\mathrm{PExt}_{\mathrm{seed}}$ applied on (S_{i^*}, D_{i^*}), one can be sure that its output Z_{i^*} is close to uniform with respect to S_{-i^*}, D_{-i^*}, and hence Z_{i^*} is close to uniform *even conditioned on all other* Z_{-i^*}, which is then sufficient to imply that $Z = Z_{i^*} \oplus \left(\bigoplus_{i \neq i^*} Z_i\right)$ is close to uniform.

The issue is that if S_{-i^*}, D_{-i^*} is part of the adversary for $\mathrm{PExt}_{\mathrm{seed}}(S_{i^*}, D_{i^*})$, then the seed S_{i^*} is *not* close to uniform with respect to the adversary, due to the correlation between S_{i^*} and S_{-i^*}. This violates the premise of the soundness of seeded PREs and it is thus not guaranteed that Z_{i^*} is uniform to S_{-i^*}, D_{-i^*} at all. However, we note that the seed S_{i^*} is still close to uniform w.r.t. the device D_{i^*}.

Randomness Decoupler. To resolve the aforementioned issue, we identify a class of untrusted-device protocols, called "randomness decouplers", which take uniform-to-device inputs and generate uniform-to-all outputs with respect to the decision bit. We remark that randomness decouplers solve the exact issue we are facing and it is hence highly desirable to find such protocols with good properties.

Somewhat surprisingly, there do exist untrusted-device protocols that are designed for much harder tasks (such as delegation of quantum computation [21] and strong monogamy [18, 6]) and can serve as randomness decouplers. However, since the goals of these protocols are to deal with much stronger requirements, they exploit heavy machineries in their designs at the price of losing desirable parameters or properties. In particular, the output of both protocols is shorter than the seed. On the other side, seeded PREs for randomness expansion (e.g., [28, 19]) bear much better parameters and desirable properties, but cannot be directly applied since their security results were established under the globally uniform seed. Is it possible to prove a stronger security for such seeded PREs?

This is a challenging question, as existing analyzing methods for randomness expansion protocols completely break down when the seed is only uniform-to-device. Take the analysis in [28] for example. Normal randomness expansion protocols consist of the following two parts: the first one to generate high min-entropy output and the second one to convert the output to uniform randomness by applying a quantum-proof strong extractor. The security of the first part in [28] is established by analyzing the so-called "guessing game", which is a non-local game played by Alice together with Bob and the adversary as a single player. If the seed can be correlated with the adversary, such a game is no longer non-local as Bob and the adversary can predict the input to Alice, which hence breaks down the analysis. The issue of the second part is more serious. This is because the seed used in the quantum-proof strong extractor could be arbitrarily correlated with the adversary, under which situation no uniform randomness can be extracted against the adversary.

Equivalence Lemma. Somewhat surprisingly, we prove such a stronger security for general seeded PREs (in particular, for those from randomness expansion protocols) by using a completely different approach in the analysis. Our first observation is to treat any seeded PRE as a single procedure, rather than to conduct analysis on each component of that PRE. This helps us to avoid the seed issue when dealing with quantum-proof extractors. A main technical contribution of this work is the following *equivalence lemma*, proved by using a black-box analysis.

Lemma 1.4 (Equivalence Lemma (EL) — informal) *The performance parameters (soundness, completeness and noise level) of any seeded PRE (established under a* uniform-to-all *seed) remain valid under a* uniform-to-device *seed.*

The proof for the completeness parameter (and the level of noise tolerated) is trivial. We will sketch the proof for the soundness by contradiction as follows. Fix any seeded PRE $\mathrm{PExt}_{\mathrm{seed}}$ with soundness error ϵ_s. Thus by assumption, there exists a physical system ρ in which the source X is only uniform-to-device, and for such ρ, the soundness error of $\mathrm{PExt}_{\mathrm{seed}}$ is greater than ϵ_s. Namely, there exists a distinguisher P that can tell $\mathrm{PExt}_{\mathrm{seed}}$'s output on ρ from uniform with advantage greater than ϵ_s. Our strategy is to construct another physical system ρ' in which the source X is uniform-to-all, and for such ρ', we construct a distinguisher P' that can distinguish $\mathrm{PExt}_{\mathrm{seed}}$'s output on ρ' from uniform with advantage greater than ϵ_s. The latter contradicts the fact that $\mathrm{PExt}_{\mathrm{seed}}$ is a seeded PRE with soundness error ϵ_s.

To that end, we construct ρ' from ρ by a unitary operation C that *commutes* with $\mathrm{PExt}_{\mathrm{seed}}$ (i.e., $\rho' = C(\rho)$.) Then we choose the distinguisher $P' = P \circ C^{-1}$. To see that works, it suffices to observe that applying P' on $\mathrm{PExt}_{\mathrm{seed}}(\rho')$ is equivalent to applying P on $\mathrm{PExt}_{\mathrm{seed}}(\rho)$. This is because $P'(\mathrm{PExt}_{\mathrm{seed}}(\rho'))=P(C^{-1}(\mathrm{PExt}_{\mathrm{seed}}(C(\rho))))=P(C^{-1}(C(\mathrm{PExt}_{\mathrm{seed}}(\rho)))) =P(\mathrm{PExt}_{\mathrm{seed}}(\rho))$, where we crucially use that fact that C commutes with $\mathrm{PExt}_{\mathrm{seed}}$.

To construct such C, we first note that in the physical system ρ, for each classical value of X, the rest system (D, E) can be assumed to a *pure* state. This is because any distinguisher for a partial system is a distinguisher for the purified system. Moreover, since X is uniform-to-D and by Uhlmanns theorem, one can construct such C that is a unitary operation on E *controlled* by X. This allows C to commute with $\mathrm{PExt}_{\mathrm{seed}}$ as the latter can be viewed as a quantum operation on D controlled by X. As we discussed before, it is impossible to establish an analog of EL in the context of traditional randomness extractors. Technically, this is because we cannot make an analog assumption of (D, E) system being a pure state for every value of X in that context. They are necessarily *mixed* states by the nature of randomness extractors (i.e., under which situation randomness extractors are known to work..)

Other applications of EL. EL provides a strong security lift for a fundamental primitive (i.e., seeded PRE), thus is useful for proving composition security of untrusted-device protocols. It is not surprising that since its discovery for our purpose, this fundamental principle and powerful tool has found several other important applications. We highlight two such applications.

The first application is to achieve **unbounded randomness expansion using a constant number of devices**. It was known by randomness expansion protocols that one can generate exponentially long uniform strings with short seeds by using only two untrusted devices. What is the maximal length of uniform strings that can be generated with short seeds?

A natural strategy [11] is to run two such protocols on separate sets of untrusted devices, and repeatedly use the output of one protocol as the input to the other. However, the output of a certain device cannot be uniform with respect to the device itself. Thus, when this output is cross-fed to another set of devices, it is necessarily *uniform-to-device* only, which gives rise to exactly the same seed issue. This issue was first resolved in the context of unbounded expansion by an independent work [9], which introduces the heavy machinery of [21] into this context. As a result, they derive a protocol that makes use of 8 devices and requires a very complicated analysis. In contrast, EL implies that such a seed issue in fact does not cause any security problem in the cross-feeding composition. Thus *any* seeded PRE can be securely used to achieve unbounded expansion (and with just 4 devices.)

A second application is to achieve **expanding untrusted-device quantum key distribution (QKD) without sharing an initial secret key.** The QKD protocol in [19] is the first (and only known) untrusted-device protocol that achieves at the same time exponential expansion of randomness. The protocol is adapted from a randomness expansion protocol, which requires a short uniform-to-all seed to start with. By using EL, the two parties only need to share uniform-to-device seeds before the protocol starts. Thus, one of them could generate a seed using his/her local randomness and send it to the other party over the public channel after they possess the untrusted devices. Although the seed is completely leaked to the adversary, it remains uniform-to-device and thus guarantees the security of the protocol.

Related Works. This work was directly inspired by the randomness amplification works of Colbeck and Renner [8] and Gallego *et al.* [12], who were already asking for minimal conditions for generating one free random bit. Their works, however, differ from ours significantly on the model. Their model, referred to as the Colbeck-Renner model, is non-signaling on the tripartite input-devices-adversary correlation, while the devices' correlation is quantum. Our model is solely quantum. While this may seem to make our model weaker, there are two additional assumptions on their model that make its quantum restriction a proper subset of ours. Conditioned on the adversary's input-output pair, the first assumption is that the source is an SV-source, and the second assumption is that the input and the devices are independent (i.e. on any input to the devices, the resulting joint distribution of the (protocol) input is in product with the devices' output.) It is not clear to us what the quantum portion of their model is[9]. On the other hand, their quantum restriction is a proper subset of our model, since it excludes the case that input is a non-SV min-entropy source and that the devices hold side information on X even under measurement of the adversary. In addition, Corollary 1.2 applies to this restriction.

The focus of the above mentioned works within the Colbeck-Renner model is to produce one output bit. This objective suffices for their physics motivation for amplifying the amount of "free randomness" for each bit. Given that the concatenation of SV-sources is itself SV, those results can be trivially extended for outputting multiple bits by increasing the input length. Such a "black-box" composition, however, fails for our case of general min-entropy input, since the min-entropy assumption is made on the whole input string, and there is no additional structure of the source to ensure a division of the input into pieces of guaranteed min-entropy.

Our physical randomness extractor notion provides a unified and rigorous framework for random-

[9] The following initial state $\rho_{XDE} = \mu_X \otimes \rho_{DE}$, where μ_X is an SV source, clearly satisfies the Colbeck-Renner model. One may also apply a Markov process that non-destructively measures E, then conditioned on the result, operates on X and D independently without changing the SV structure of X. It is not clear to us if those are the only initial quantum states consistent with the Colbeck-Renner model.

ness expansion and (quantum restriction of) amplification — randomness expansion is *seeded* PRE and randomness amplification is a PRE using SV source. Core components of this framework — the notions of soundness error, states with various approximately uniform classical component — facilitate the reasoning of those protocols. Those notions were also developed concurrently in the companion work by Miller and one of us (Shi) [19]. The extractor perspective allows one to quantify the various resources and constraints involved, to identify minimal assumptions, and to discuss the tradeoffs among those quantities at a deeper and richer level than in previous works. It also emphasizes a more appropriate interpretation of the roles of the devices and the weak source in untrusted-device protocols. The source of the output randomness comes from the untrusted devices while the weak source is to prevent cheating. In contrast, previous works in randomness expansion emphasize the certification aspect of the protocols, thus focus on the translation from the input length to the output length. Works in amplification were motivated mostly by physics considerations, thus are much less demanding than us on reducing the randomness of the classical source and optimizing other parameters.

Three works concurrent to us are worth special attention. Brandão *et al.* [5] considered randomness amplification starting with an SV source that is *independent* of the devices and the adversary. Their protocol uses only a (universal) constant number of devices and is secure against a non-signaling adversary, tolerating a level of device imprecision that depends on the bias of the SV source. The independence requirement of the source makes their result incomparable to other works in randomness expansion or amplification, including ours, where the devices and the adversary hold quantum side information about the source.

Miller-Shi [19] overlaps with us on several components of the model formulation (soundness error, various approximate notions of uniform classical components in a classical-quantum state), but focuses on randomness expansion. Their result subsumes previous works in randomness expansion with several desirable features, and in particular provides the first robust expansion protocol. Thus the Miller-Shi protocol is the best to use in our construction scheme among all alternatives (e.g. the non-robust Vazirani-Vidick protocol for expansion [28] and the robust but linear-rate Vazirani-Vidick protocol for certification [27].)

The combination of Miller-Shi's robust one-shot expansion protocol with our Equivalence Lemma leads to the first *robust* unbounded expansion protocol using a (universal) constant number of devices. This conclusion and its brief justification are provided in [19]. Coudron and Yuen [9] were the first to claim non-robust unbounded expansion with a constant number of devices and their work was developed independently of a previous writing of this work [6], which contains the core substance of this writing (the PRE framework, the composition scheme and its security analysis, in particular the Equivalence Lemma.) The current writing includes statements that make use of robust unbounded expansion over a constant number of devices. The amplification result claimed in an earlier version of [9] was obtained by composing their unbounded expansion protocol with the protocol of Brandão *et al.*, thus the restrictions of the latter work discussed above holds on the composed protocol.

We note that there is a recent direction of extracting randomness from quantum systems that differs from our approach. For example, Berta *et al.* [4] studied how much randomness *trusted* measurements can be produced from an unknown quantum state. Those "quantum to classical randomness extractors" provide a perspective complementary to physical extractors for how randomness can be obtained from quantum systems.

Limitations of our work and major open problems. The main limitation of our result is that the number of devices depends at least inverse-polynomially in the error parameter. Consequently, we cannot achieve simultaneously close to optimal error parameter and efficiency in the number of devices and the running time when when the input min-entropy is super-logarithmic in the security parameter. It remains a major open problem if the desirable features of our result and those of the Miller-Shi seeded PRE can be simultaneously achieved in a single protocol.

Many other new questions arise from our framework of PRE. For example, what quantities about the untrusted-device determine the maximum amount of output randomness? Can one quantify the restrictions on communication to shed light on its tradeoff with other parameters? Barrett, Colbeck and Kent [2] pointed out additional potential security pitfalls in composing untrusted-device protocols. An important direction is to develop a security model in which one can design PREs and prove composition security in a broader composition setting.

Organization. The rest of this paper is organized as follows. Necessary background and notation about quantum information is surveyed in Section 2. We formally introduce our model of physical randomness extractors in Section 3. Our key technical contributions, i.e., equivalence lemma, quantum somewhere random source, our main construction theorem and its instantiations are stated in Section 4, Section 5 and Section 6 respectively.

2 Preliminaries

We assume familiarity with standard concepts from quantum information and summarize our notation as follows.

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 matrix with trace 1, over $\mathcal{A}$. The set of all quantum states in $\mathcal{A}$ is denoted by $\mathrm{Dens}\,(\mathcal{A})$.

The Hilbert-Schmidt inner product on the operator space of $\mathcal{A}$ (denoted $\mathrm{L}\,(\mathcal{A})$) is defined by $\langle X, Y\rangle = \mathrm{tr}(X^*Y)$ for all $X, Y \in \mathrm{L}\,(\mathcal{A})$, where $*$ is the adjoint operator. Let $\mathsf{id}_{\mathcal{X}}$ denote the identity operator over $\mathcal{X}$, which might be omitted if it is clear in the context. Any operator $U \in \mathrm{L}\,(\mathcal{X})$ is a unitrary if $UU^* = U^*U = \mathsf{id}_{\mathcal{X}}$, the set of which is denoted by $U(\mathcal{X})$.

For any multi-partite state, e.g. $\rho_{ABE} \in \mathrm{Dens}\,(\mathcal{A}\otimes\mathcal{B}\otimes\mathcal{E})$, its reduced state on some subsystem is represented by the same state with the corresponding subscript, e.g. the reduced state on $\mathcal{A}$ system is represented by $\rho_A = \mathrm{tr}_{\mathcal{B}\mathcal{E}}(\rho_{ABE})$.

Any classical part of any multi-partite state is denoted as c-part. Respectively, any quantum part is denoted as q-part. Thus a cq-state $\rho \in \mathrm{Dens}\,(\mathcal{A}\otimes\mathcal{B})$ indicates the $\mathcal{A}$ is classical and $\mathcal{B}$ is quantum.

We use $|\psi\rangle$ to denote the density operator (i.e., $|\psi\rangle\langle\psi|$) of the pure state $|\psi\rangle$ when it is clear from the context. Moreover, let $\mathcal{U}_A$ denote the maximum mixed state on any space $\mathcal{A}$, i.e., $\mathcal{U}_A = \frac{1}{\dim(\mathcal{A})}\mathsf{id}_{\mathcal{A}}$.

Norms. 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 defined $\|X\|_{\mathrm{tr}} = \sum_{i=1}^{d}\sigma_i$. The trace distance between two quantum states ρ_0 and ρ_1 is defined as $\|\rho_0 - \rho_1\|_{\mathrm{tr}}$.

Another important distance measure, *quantum fidelity*, between two quantum states ρ_0, ρ_1 (denoted $\mathrm{F}(\rho_0, \rho_1)$) is defined as

$$\mathrm{F}(\rho_0, \rho_1) = \|\sqrt{\rho_0}\sqrt{\rho_1}\|_{\mathrm{tr}}\,, \tag{2.1}$$

and admits the following connection with the trace distance.

Lemma 2.1 (Fuchs-van de Graaf) *For any $\rho_0, \rho_1 \in \mathrm{Dens}(\mathcal{A})$, we have*

$$1 - \frac{1}{2}\left\|\rho_0 - \rho_1\right\|_{\mathrm{tr}} \leq \mathrm{F}(\rho_0, \rho_1) \leq \sqrt{1 - \frac{1}{4}\left\|\rho_0 - \rho_1\right\|_{\mathrm{tr}}^2}. \tag{2.2}$$

Moreover, the fidelity between subsystems of quantum states could be preserved in the following sense.

Lemma 2.2 (e.g., [15, Lemma 7.2]) *Let $\rho, \xi \in \mathrm{Dens}(\mathcal{A})$ and $\rho' \in \mathrm{Dens}(\mathcal{A} \otimes \mathcal{B})$ be density operators with $\mathrm{tr}_{\mathcal{B}}\, \rho' = \rho$. There exists a density operator $\xi' \in \mathrm{Dens}(\mathcal{A} \otimes \mathcal{B})$ with $\mathrm{tr}_{\mathcal{B}}\, \xi' = \xi$ and $\mathrm{F}(\rho', \xi') = \mathrm{F}(\rho, \xi)$.*

Quantum Operations. Super-operators from $\mathcal{X}$ to $\mathcal{Y}$ are linear mappings of the following form

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

Physically realizable *quantum operations* are represented by *admissible* super-operators that are completely positive and trace-preserving. Thus any quantum protocol could be viewed as an admissible super-operator. We shall use this abstraction in our analysis and make use of the following observation.

Fact 2.3 (Monotonicity of trace distances) *For any admissible super-operator $\Psi : \mathrm{L}(\mathcal{X}) \to \mathrm{L}(\mathcal{Y})$ and $\rho_0, \rho_1 \in \mathrm{Dens}(\mathcal{X})$, we have*

$$\left\|\Psi(\rho_0) - \Psi(\rho_1)\right\|_{\mathrm{tr}} \leq \left\|\rho_0 - \rho_1\right\|_{\mathrm{tr}}.$$

A unitary operation $U \in U(\mathcal{X})$ is a special type of admissible quantum operations that are *inversible.* For any unitary U, its corresponding super-operator Ψ_U is defined as

$$\Psi_U(\cdot) = U \cdot U^{\dagger}.$$

A unitary operation $U \in U(\mathcal{X} \otimes \mathcal{Y})$ is called a *controled-U* (by $\mathcal{X}$) if

$$U = \sum_{x \in \mathcal{X}} |x\rangle\langle x| \otimes U_x,$$

where U_x is a unitary on $\mathcal{Y}$ indexed by x.

Min-entropy. For any c-q state ρ_{XE}, the amount of *extractable* randomness of some source is characterized by the *(smooth) conditional min-entropy.*

Definition 2.4 (conditional min-entropy) *Let $\rho_{XE} \in \mathrm{Dens}(\mathcal{X} \otimes \mathcal{E})$. The* min-entropy *of X conditioned on E is defined as*

$$\mathrm{H}_{\infty}(X|E)_{\rho} \stackrel{def}{=} \max\{\lambda \in \mathbb{R} : \exists \sigma_E \in \mathrm{Dens}(\mathcal{E}), \text{s.t. } 2^{-\lambda} \mathsf{id}_X \otimes \sigma_E \geq \rho_{XE}\}.$$

3 Model of Physical Randomness Extractors

In this section, we present a unified definitional framework for certifiable randomness extraction from physical systems with the goal of minimizing assumptions. We start by an informal discussion to introduce the notion of physical systems and physical randomness extractors. We then provide formal definitions, and explicitly discuss the assumptions we make and their necessity.

At a high level, we envision a scenario where a *physical randomness extractor* PExt is given a classical source and multiple untrusted-devices as potential sources of randomness with the goal of extracting certifiable randomness that looks uniform from a certain environment (e.g., the device manufacturer), where PExt may accept and generate (hopefully uniform) output, or decide to reject when it detects misbehavior of the devices.

To formalize this, we introduce the notion of a *physical system* $\mathcal{S} = (X, D, E)$ that consists of a source X, multiple untrusted-devices $D = (D_1, \ldots, D_t)$, and an adversary E. The source X is a distribution over finite fixed-length string with certain *assumed* min-entropy. (We shall specify how the min-entropy is measured later.) An untrusted-device D_i is a black-box with unknown inner working that allows classical interactions. That is, on classical input queries, D_i generates (potentially random) classical outputs. As we assume the world obeys quantum mechanics, D_i can be modelled as an interactive, stateful quantum algorithm (with unknown initial state and potentially unbounded algorithm). The adversary E is simply a state that captures any partial information possessed by the environment through correlation and entanglement with X and D.

A *physical randomness extractor* PExt for a physical system $\mathcal{S} = (X, D, E)$ is a classical, deterministic procedure that given the source X and classical interaction with D, outputs a decision bit $O \in \{\mathsf{Acc}, \mathsf{Rej}\}$ and an output string $Z \in \{0,1\}^*$. Intuitively, we require *completeness*, which says there are some "honestly manufactured" devices such that PExt accepts with high probability and *soundness*, which says that PExt does not accept yet produce far from uniform outputs except with small probability. We note that we formalize soundness in a different way from existing related works which enables us to simplify the analysis of composition of physical randomness extractors.

Like the traditional notion of randomness extractors, we quantify physical randomness extractors PExt by the (assumed) min-entropy in physical systems and the amount that PExt can extract (as well as the errors from uniform). For the source X, we can quantify it by its length n and assumed min-entropy k. Note that since we drop the independence assumption, we need to specify how the min-entropy is measured, say, with respect to the devices D, the adversary E, or both. (Looking ahead, it suffices for our construction that X has min-entropy with respect to D.) For each untrusted device D_i, we do not want to assume min-entropy in its answers, but instead only quantify its total output length m, which provides an upper bound on how much entropy D_i can provide. Ideally, we would like PExt to extract as close to $k + tm$ bits of randomness as possible.

In addition to making an assumption on the amount of min-entropy in the source X, we also assume that there is no communication from the source X and the devices D to the adversary E and no communication among the devices D as well. As argued in the introduction, such communication restrictions are necessary assumptions.

It is worthwhile to compare our notion of physical randomness extractors with the traditional notion of randomness extractors. Recall that at least two *independent* random sources are necessary for randomness extractors, whereas such independence assumption can be removed for physical randomness extractors. On the other hand, note that the communication restrictions are in fact implicit assumed for randomness extractors. The crux for removing the independence assumption comes from introducing untrusted devices as a new interactive physical source of randomness and the ability of rejecting misbehavior devices.

Physical Systems. We now proceed with formal definitions. We first formalize the notion of physical systems.

Definition 3.1 (Physical System) *A* physical system $\mathcal{S}$ *on space* $X \otimes D \otimes E$ *with a source* X*,* t *untrusted devices* $D = (D_1, \cdots, D_t)$ *and an adversary* E *is defined as follows.*

- *The entire system is characterized by a* system *state* $\rho \in \mathrm{Dens}\,(X \otimes D \otimes E)$*, which lies in an arbitrarily large but finite Hilbert space. Note that the correlation among the source, untrusted devices, and the adversary could be arbitrary.*
- *Each untrusted device* D_i *is further specified by a quantum,* interactive*, and* stateful *algorithm* A_{D_i} *that applies on* D_i*. In particular,* A_{D_i} *can be described by a quantum circuit, which on input query* $q \in \Sigma_{in}$ *for some input space* $\Sigma_{in} \subset \{0,1\}^*$*, generates output* $a \in \Sigma_{out}$ *in some output space* $\Sigma_{out} \subset \{0,1\}^*$ *and updates the internal state by applying* A_{D_i} *on* $\Sigma_{in} \otimes D_i$*.*
- *Any such* $\mathcal{S}$ *might be equipped with optional register* $O \otimes \mathcal{Z}$*, where* O *is the decision bit after applying any protocol on* $\mathcal{S}$ *and* $\mathcal{Z}$ *corresponds to its output. Note that* X, O, Z *are classical components of the system.*

In other words, $\mathcal{S}$ *is specified by a system state* ρ *and a collection of untrusted device algorithms* $\{A_{D_i}\}$*, denoted as* $\mathcal{S}(\rho, \{A_{D_i}\})$*, or* $\mathcal{S}(\rho)$*, or* ρ *for short when* $\{A_{D_i}\}$ *is irrelevant in the context.*

We note that the assumption of communication restriction among the devices is formally captured by the fact that each device algorithm A_{D_i} operates only on its corresponding space D_i. For a physical system $\mathcal{S}(\rho, \{A_{D_i}\})$, let Y be a classical component of $\mathcal{S}$. We say Y has k bits of min-entropy-to-R if $\mathrm{H}_\infty(Y|R)_\rho \geq k$, where R is some components of $\mathcal{S}$. We say that Y is an (n,k)*-source-to-*R if $Y \in \{0,1\}^n$ and Y has k bits of min-entropy-to-R. When R is D, E, or the rest of the system, we refer to R as *device, adversary,* and *all* respectively. For example, we say X has k bits of min-entropy-to-device if $\mathrm{H}_\infty(X|D)_\rho \geq k$, and X is an (n,k)-source-to-all if $X \in \{0,1\}^n$ and $\mathrm{H}_\infty(X|D,E)_\rho \geq k$.

Definition 3.2 *A physical system* $\mathcal{S}(\rho, \{A_{D_i}\})$ *is an* (n,k,t,m)*-physical system with random-to-device (resp., random-to-all) source if*

- X *is an* (n,k)*-source-to-devices (resp.,* (n,k)*-source-to-all).*
- $D = (D_1, \ldots, D_t)$ *and each device* D_i *outputs at most* m *bits in total (namely, it halts after outputting* m *bits).*

We note that the assumption on the amount of min-entropy in the source is quantified in the above definition.

Physical Randomness Extractors We next define the syntax of physical randomness extractors.

Definition 3.3 (Physical Randomness Extractor) *A physical randomness extractor* PExt *for a physical system* $\mathcal{S}$ *on* $X \otimes D \otimes E$ *is a classical, deterministic procedure that given the source* X *and* *classical interaction with the untrusted devices $D = (D_1, \ldots, D_t)$, output the decision bit $O \in \{\mathsf{Acc}, \mathsf{Rej}\}$ and an output string $Z \in \{0,1\}^*$ to a new space $O \otimes \mathcal{Z}$. (See Fig. 1)*

Combined with devices' algorithms $\{A_{D_i}\}$, the whole extraction can be considered as an admissible quantum operation Φ_{PExt}:

$$\Phi_{\mathrm{PExt}} : \mathrm{L}(X \otimes D) \to \mathrm{L}(O \otimes \mathcal{Z} \otimes X \otimes D).$$

In particular, Φ_{PExt} is determined by PExt *and the inner workings of the devices D (given by $\{A_{D_i}\}$), and keeps a copy of the input X. We use* $\mathrm{PExt}(\mathcal{S})$ *to denote the post-extraction physical system.*

Towards defining properties (in particular, soundness) of physical randomness extractors, we formalize a new and natural distance-to-uniform measure for the output component Z of $\mathrm{PExt}(\mathcal{S})$ (w.r.t. E and O) which we find useful in particular for analyzing composition. We start by the following definitions.

Let $\mathcal{S}(\rho, \{A_{D_i}\})$ be a physical system, Y a classical component, and R some components of $\mathcal{S}$. We say that Y is *uniform-to-R* if $\rho_{YR} = \mathcal{U}_Y \otimes \rho_R$. Suppose $\mathcal{S}$ is equipped with a decision bit O, then we say Y is *uniform-to-R on* Acc if $\rho_{YR}^{\mathsf{Acc}} = \mathcal{U}_Y \otimes \rho_R^{\mathsf{Acc}}$, where ρ^{Acc} (sub-normalized) is from the following decomposition of ρ with respect to the decision bit, $\rho = |\mathsf{Acc}\rangle\langle\mathsf{Acc}| \otimes \rho^{\mathsf{Acc}} + |\mathsf{Rej}\rangle\langle\mathsf{Rej}| \otimes \rho^{\mathsf{Rej}}$. We define the set of uniform-to-R states and uniform-to-R-on-Acc states as

$$R\text{-Uni}(\mathcal{S}) = \{\xi : \xi_{YR} = \mathcal{U}_Y \otimes \xi_R\}, \text{ and } R\text{-Uni}^{\mathsf{Acc}}(\mathcal{S}) = \{\xi : \xi_{YR}^{\mathsf{Acc}} = \mathcal{U}_Y \otimes \xi_R^{\mathsf{Acc}}\}, \text{respectively.}$$

We can then define a distance-to-uniform measure by the minimal trace distance to such uniform-to-R(-on-Acc) states. Specifically, we say that Y is ϵ-uniform-to-R (resp., on Acc) if $\mathrm{dist}(\rho, R\text{-Uni}(\mathcal{S})) \le \epsilon$ (resp., $\mathrm{dist}(\rho, R\text{-Uni}^{\mathsf{Acc}}(\mathcal{S})) \le \epsilon$), where $\mathrm{dist}(\rho, C) = \min_{\xi \in C} \|\rho - \xi\|_{\mathrm{tr}}$ denotes the distance from any ρ to a convex set C. It is interesting to note that for any ρ, ρ', we have $|\mathrm{dist}(\rho, C) - \mathrm{dist}(\rho', C)| \le \|\rho - \rho'\|_{\mathrm{tr}}$.

We are now ready to define properties of physical randomness extractors.

Definition 3.4 *A physical randomness extractor* PExt *is an* (n,k,t,m)-PRE for random-to-device *(resp.,* random-to-all*)* source *with output length N, completeness error ϵ_c and soundness error ϵ_s if the output $Z \in \{0,1\}^N$ and it satisfies the following completeness and soundness properties.*

- *(Completeness) There exist honest devices $D = (D_1, \cdots, D_t)$ with internal state σ_D and algorithms $\{A_{D_i}\}_{i=1}^t$ with each device D_i outputting at most m bits such that for any (n,k,t,m)-physical system $\mathcal{S}(\rho, \{A_{D_i}\})$ with random-to-device (resp., random-to-all) sources satisfying $\rho_D = \sigma_D$, we have*

  $$\mathbf{Pr}[\mathsf{Acc}(\mathrm{PExt}, \mathcal{S})] \ge 1 - \epsilon_c,$$

  where $\mathsf{Acc}(\mathrm{PExt}, \mathcal{S})$ *denotes the event that* PExt *accepts when applied to $\mathcal{S}$.*

- *(Soundness) For any (n,k,t,m)-physical system $\mathcal{S}(\rho, \{A_{D_i}\})$ with random-to-device (resp., random-to-all) source, the output Z in the post-extraction state* $\mathrm{PExt}(\mathcal{S})$ *is ϵ_s-uniform-to-XE on* Acc*. Precisely, the soundness error is given by $\Delta(\mathrm{PExt}, \rho)$ defined as*

  $$\Delta(\mathrm{PExt}, \rho) \overset{def}{=} \mathrm{dist}(\Phi_{\mathrm{PExt}}(\rho), XE\text{-}Uni^{\mathsf{Acc}}(\mathrm{PExt}(\mathcal{S}))) \le \epsilon_s.$$

Note that in our definition, we allow the honest devices in the completeness property to share arbitrary correlation/entanglement with other components of the system, and as long as the devices have "correctly implemented" inner working and the source has assumed min-entropy-to-devices/all, PExt accepts with high probability, and by combining with the soundness property, generates close to uniform output. Also note that our soundness definition requires the output to be uniform with respect to both the source X and the adversary E, which implies that the randomness PExt extracts is from the devices D.

We remark that we use the above-defined distance-to-uniform measure to define soundness, which differs from existing definitions (in the untrusted-device quantum cryptography literature) in the following two ways. First, we define the distance using the global system state, as opposed to the reduced system that traced out the device component, which makes the definition more stringent. On the other hand, we measure distance to any uniform-to-XE(-on-Acc) states, which for example, does not require the E component to be unchanged; This makes the definition weaker (but only by a factor of 2 by standard triangle inequality argument). We find such definition particularly both natural and convenient for analyzing composition of PREs.

Variants of PRE and Equivalence Lemma. As mentioned, we introduce the notion of physical randomness extractors as a unified definitional framework that encompasses existing models for certifying randomness such as randomness expansion and randomness amplification. Our main motivation is to provide a more refined perspective of randomness extraction that better quantifies the source of randomness being extracted, as well as a basis to rigorously reason about properties and compositions of PREs.

We now discuss formally how previous models can be cast in our framework as variants/special cases of physical randomness extractors, which in turn will be used as building blocks for our construction. The task of randomness amplification can be viewed as physical randomness extractors for Santha-Vezirini sources for extracting a single bit. Recall that the task of randomness expansion is to certify long almost pure randomness from short uniform seeds. In our language, randomness expansion protocols are *seeded physical randomness extractors.*

Definition 3.5 *A physical randomness extractor* PExt *is a* (n, t, m)-seeded-PRE for uniform-to-device *(resp.,* uniform-to-all*)* source *with output length N, completeness error ϵ_c and soundness error ϵ_s iff* PExt *is a (n, n, t, m)-PRE for random-to-device (resp., random-to-all) source with corresponding N, ϵ_c and ϵ_s parameters.*

We note that seeded physical randomness extractor for random-to-*all* sources is *equivalent* to the notion of quantum-secure randomness expansion protocols [28, 19] (up to a small parameter loss in both directions due to different error measures in the definition of soundness). On the other hand, seeded physical randomness extractor for random-to-*device* sources is the *randomness decoupler* discussed in the introduction that is needed in our construction. Interestingly, known analysis for randomness expansion protocols only shows the construction is a seeded physical randomness extractor for random-to-*all* sources, but the proof breaks down in the setting of seeded physical randomness extractor for random-to-*device* sources (see the introduction for detailed discussions).

Perhaps surprisingly, our key technical contribution is to show that seeded physical randomness extractor for uniform-to-*all* sources and that for uniform-to-*device* sources are in fact *equivalent objects.*

Lemma 3.6 (Equivalence Lemma) *Any (n, t, m)-seeded-PRE for uniform-to-all sources is also a (n, t, m)-seeded-PRE for uniform-to-device source with the same parameters.*

Additional desired properties Finally, we note that for physical randomness extractors to have practical meaning, it is crucial to make sure that the honest devices can be implemented in a reliable way with low cost/complexity.

4 Equivalence Lemma

As one of our main technical contributions, we prove that any seeded PRE with uniform-to-all seeds should work as well with uniform-to-device seeds. As mentioned in the introduction part, we take a black-box approach in our analysis, which is completely different from previous analysis for either randomness expansion protocols (such as [28]) or protocols that are designed for much harder tasks (such as delegation of quantum computation [21] and strong monogamy [18, 6]).

Lemma 4.1 *Any seeded PRE* $\mathrm{PExt}_{\mathrm{seed}}$ *for uniform-to-all seeds is also a seeded PRE for uniform-to-device seeds with the same set of parameters.*

Proof. First note that by definition, the output length N remains the same for both settings. Moreover, by definition, the event $\mathsf{Acc}(\mathrm{PExt}, \mathcal{S})$ only depends on the source and the devices, thus the probability of which in uniform-to-device systems remains the same for the same set of honest devices from uniform-to-all systems. Therefore, the completeness error of $\mathrm{PExt}_{\mathrm{seed}}$ remains the same for uniform-to-device seeds.

It suffices to show that its soundness error with respect to uniform-to-device seeds remains the same as the one with respect to uniform-to-all seeds. Fix a physical system $\mathcal{S}$ on $X \otimes D \otimes E$ and let $\Phi_{\mathrm{PExt}_{\mathrm{seed}}}$ denote the admissible quantum operation performed by $\mathrm{PExt}_{\mathrm{seed}}$ on $\mathcal{S}$.

For any system state ξ in which X is uniform-to-D, namely, $\xi_{XD} = \mathcal{U}_X \otimes \xi_D$, we have

$$\xi_{XDE} = \sum_x \frac{1}{\dim(X)} |x\rangle\langle x| \otimes |\psi^x\rangle\langle\psi^x|_{DE},$$

in which without loss of generality we can assume for any given x, the quantum state of (D, E) is a *pure* state [10]. Moreover, we have $\mathrm{tr}_E(|\psi^x\rangle\langle\psi^x|_{DE}) = \xi_D$ for every x. Let $\left|\psi^0\right\rangle_{DE} \in \mathrm{Dens}\,(D \otimes E)$ be any purification of ξ_D. By unitary equivalence of purifications (Uhlmann's Theorem), there exists a unitary operation U_E^x on E system for every x such that

$$|\psi^x\rangle_{DE} = (\mathsf{id}_D \otimes U_E^x) \left|\psi^0\right\rangle_{DE}. \tag{4.1}$$

Let Φ_C denote the quantum operation of a controlled-unitary C over $X \otimes E$ such that $C = \sum_x |x\rangle\langle x| \otimes U_E^x$. Thus, we can construct another system state ξ' that has uniform-to-all X from ξ simply by choosing $\xi' = \Phi_C(\xi)$. By (4.1), we have

$$\xi' = \mathcal{U}_X \otimes \left|\psi^0\right\rangle\langle\psi^0\right|_{DE}, \tag{4.2}$$

in which X is uniform-to-all.

Our key observation is to make use of Φ_C's following two additional properties. First, we note that Φ_C commutes with $\Phi_{\mathrm{PExt}_{\mathrm{seed}}}$ because Φ_C is a controlled operation on E by X and $\Phi_{\mathrm{PExt}_{\mathrm{seed}}}$ is

[10] This is because holding pure states can only increase the adversary's power to cheat. We remark that an analogue of this assumption cannot be made in the context of strong randomness extractors. This is because their security is established when the source is classical. Thus, system D that corresponds to the source in that setting is necessarily *classical* and *mixed*.

a controlled operation on D by X. Second, Φ_C (or its inverse Φ_C^{-1}) only operates on $X \otimes E$. Let the post-extraction system be $\mathrm{PExt}(\mathcal{S})$ and let $T(\mathcal{S})$ denote XE-$\mathrm{Uni}^{\mathsf{Acc}}(\mathrm{PExt}(\mathcal{S}))$. Thus, it is easy to see that Φ_C (or similarly, its inverse Φ_C^{-1}) does not change $T(\mathcal{S})$ when applied on it. Namely, $\Phi_C(T(\mathcal{S})) \overset{\text{def}}{=} \{\Phi_C(\xi) : \xi \in T(\mathcal{S})\} = T(\mathcal{S})$ (similarly for Φ_C^{-1}).

Finally, let ϵ_s be $\mathrm{PExt}_{\mathsf{seed}}$'s soundness error with respect to uniform-to-all seeds. Thus we have,

$$\Delta(\mathrm{PExt}_{\mathsf{seed}}, \xi') = \mathrm{dist}(\Phi_{\mathrm{PExt}_{\mathsf{seed}}}(\xi'), T(\mathcal{S})) \leq \epsilon_s.$$

By the first property of Φ_C, we have

$$\Phi_{\mathrm{PExt}_{\mathsf{seed}}}(\xi') = \Phi_{\mathrm{PExt}_{\mathsf{seed}}}(\Phi_C(\xi)) = \Phi_C(\Phi_{\mathrm{PExt}_{\mathsf{seed}}}(\xi)).$$

By the second property of Φ_C and the definition of $\mathrm{dist}(\cdot,\cdot)$, for any state τ, we have

$$\mathrm{dist}(\Phi_C(\tau), T(\mathcal{S})) = \mathrm{dist}(\tau, \Phi_C^{-1}(T(\mathcal{S}))) = \mathrm{dist}(\tau, T(\mathcal{S})).$$

Therefore, for any uniform-to-device state ξ,

$$\begin{aligned}\Delta(\mathrm{PExt}_{\mathsf{seed}}, \xi) &= \mathrm{dist}(\Phi_{\mathrm{PExt}_{\mathsf{seed}}}(\xi), T(\mathcal{S})) = \mathrm{dist}(\Phi_C(\Phi_{\mathrm{PExt}_{\mathsf{seed}}}(\xi)), T(\mathcal{S})) \\ &= \mathrm{dist}(\Phi_{\mathrm{PExt}_{\mathsf{seed}}}(\xi'), T(\mathcal{S})) = \Delta(\mathrm{PExt}_{\mathsf{seed}}, \xi') \leq \epsilon_s,\end{aligned}$$

which completes the proof. ■

5 Quantum Somewhere Random Source

Before we introduce somewhere random sources in our protocol construction, we review quantum-proof randomness extractors, which turn a min-entropy source to quantum-secure output.

Definition 5.1 (Quantum-proof Strong Randomness Extractor) *A function* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a* quantum-proof *(or simply* quantum*)* (k,ϵ)-strong randomness extractor*, if for all states ρ_{XE} classical on X with $\mathrm{H}_\infty(X|E) \geq k$, and for a uniform seed Y independent of ρ_{XE}, we have*

$$\left\| \rho_{\mathrm{Ext}(X,Y)YE} - \mathcal{U}_m \otimes \rho_Y \otimes \rho_E \right\|_{\mathrm{tr}} \leq \epsilon. \tag{5.1}$$

We state the following two quantum strong randomness extractors in [10] that will be useful for us to instantiate our physical randomness extractors.

Theorem 5.2 ([10], Corollary 5.4) *For every $n, k \in \mathbb{N}$ and $\epsilon > 0$ with $k \geq 4\log(1/\epsilon) + O(1)$, there exists a quantum (k,ϵ)-strong randomness extractor* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with $m = k - 4\log(1/\epsilon) - O(1)$ and $d = O(\log^2(n/\epsilon)\log m)$.*

Theorem 5.3 ([10], Corollary 5.6) *Let $0 < \gamma < \alpha < 1$ and $a > 0$ be constants. For sufficiently large n, there exists a quantum (k,ϵ)-strong randomness extractor* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with, $k = n^\alpha$ and $\epsilon = n^{-a}$, $m = O(n^{\alpha-\gamma})$, and $d = O\left(\frac{(1+a)^2)}{\gamma}\log n\right)$.*

An apparent problem when one tries to apply the above extractors in our setting is that we do not have the required uniform seeds. Our solution is to enumerate all the possible seed values and run the extractors on the fixed seed values. The output property of the extractor now translates to a guarantee that the output of at least one instance (in fact, a large fraction of them) of the fixed-seeded extractors is close to uniform. The output together forms what we call *quantum somewhere randomness.* In classical setting, a somewhere random source $\mathbf{S}$ is simply a sequence of random variables $\mathbf{S} = (S_1, \ldots, S_r)$ such that the marginal distribution of some block S_i is uniform (but there could be arbitrary correlation among them). Somewhere random sources are useful intermediate objects for several constructions of randomness extractors (see, e.g., [20, 17]), but to the best of our knowledge, its quantum analogue has not been considered before.

Definition 5.4 (Quantum-SR Source) *A cq-state $\rho \in \mathrm{Dens}(S_1 \otimes \cdots \otimes S_r \otimes E)$ with classical part $S_1, S_2, \cdots, S_r \in \{0,1\}^m$ and quantum part E is a (r,m)-*quantum somewhere random (SR) source *against E if there exists $i \in [t]$ such that*

$$\rho_{S_i E} = \mathcal{U}_m \otimes \rho_E,$$

*where $\rho_{S_i E}$ and ρ_E are reduced states of ρ on $S_i \otimes \mathcal{E}$ and $\mathcal{E}$ systems respectively. We say ρ is a (r,m,ϵ)-*quantum somewhere random source *if there exists $i \in [t]$ such that*

$$\| \rho_{S_i E} - \mathcal{U}_m \otimes \rho_E \|_{\mathrm{tr}} \leq \epsilon.$$

We remark that the fact that ρ is a (r,m,ϵ)-quantum somewhere random source does not necessarily imply that ρ is ϵ-close in trace distance to some (r,m)-quantum somewhere random source ρ'. In contrast, the analogous statement is true for classical somewhere random source. However, by Lemma 2.2, one can show that they are $2\sqrt{\epsilon}$ close. On the other hand, just like its classical counterpart, one can convert a weak source X to a somewhere random source by applying a (quantum-proof) strong randomness extractor to X with all possible seeds (each seed yields one block).

Proposition 5.5 *Let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a* quantum-proof (k,ϵ)-strong extractor. *Let ρ_{XE} be a cq-state with $\mathrm{H}_\infty(X|E) \geq k$. For every $i \in \{0,1\}^n$, let $S_i = \mathrm{Ext}(X,i)$. Then the cq-state*

$$\rho_{S_1 \ldots S_{2^d} E} \overset{def}{=} \sum_x p_x \, |S_1\rangle\langle S_1| \otimes \cdots \otimes |S_{2^d}\rangle\langle S_{2^d}| \otimes \rho_E^x,$$

is a $(2^d, m, \epsilon)$-quantum SR source. Moreover, the expectation of $\| \rho_{S_i E} - \mathcal{U}_m \otimes \rho_E \|_{\mathrm{tr}}$ over a uniform random index $i \in \{0,1\}^n$ is at most ϵ.

Proof. Since Ext is a quantum-proof (k,ϵ)-strong extractor and $\mathrm{H}_\infty(X|E) \geq k$, we have that

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

which is equivalent to

$$\sum_{i=1}^{2^d} \frac{1}{2^d} \left\| \rho_{\mathrm{Ext}(X,i)E} - \mathcal{U}_m \otimes \rho_E \right\|_{\mathrm{tr}} \leq \epsilon.$$

Thus immediately we have that there exists an index $i \in [2^d]$ such that

$$\left\| \rho_{\mathrm{Ext}(X,s_i)E} - \mathcal{U}_m \otimes \rho_E \right\|_{\mathrm{tr}} \leq \epsilon,$$

or equivalently $\| \rho_{S_i E} - \mathcal{U}_m \otimes \rho_E \|_{\mathrm{tr}} \leq \epsilon$. ■

Physical Randomness Extractor PExt

Let Ext : $\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be a quantum-proof strong randomness extractor.

Let $\mathrm{PExt}_{\mathrm{seed}}$ be a seeded PRE with seed length m that uses t_{seed} devices. Let $0 < \eta < 1$.

PExt operates on an input source X over $\{0,1\}^n$ and $t_{\mathsf{PRE}} = 2^d \cdot t_{\mathsf{seed}}$ devices $D = (D_1, \ldots, D_{2^d})$, where each D_i denotes a set of t_{seed} devices, as follows.

1. For every $i \in \{0,1\}^d$, let $S_i = \mathrm{Ext}(X, i)$ and invoke $(O_i, Z_i) \leftarrow \mathrm{PExt}_{\mathrm{seed}}(S_i, D_i)$.
2. If there exist η fraction of $O_i = \mathsf{Rej}$, then PExt outputs $O = \mathsf{Rej}$; otherwise, PExt outputs $(O, Z) = (\mathsf{Acc}, \bigoplus_{i\in[2^d]} Z_i)$.

Figure 3: Our Main Construction of Physical Randomness Extractor PExt.

6 Construction of PREs for any min-entropy source

In this section, we develop a systematic approach to construct a PRE PExt for any min-entropy source based on any quantum-proof strong randomness extractor Ext and any seeded PRE $\mathrm{PExt}_{\mathrm{seed}}$.

Our construction follows directly from the informal discussion in Section 1 (see Fig. 2). On input a weak source X, PExt first uses the extractor Ext to turn X into a somewhere random source $(S_1, \ldots, S_{2^d})$ where d is the seed length of Ext and $S_i = \mathrm{Ext}(X, i)$, and then for each $i \in [2^d]$, invokes the seeded PRE $\mathrm{PExt}_{\mathrm{seed}}$ with seed S_i and *distinct* set of devices D_i, each of which outputs (O_i, Z_i). If any η fraction of them reject, then PExt rejects; Otherwise, PExt accepts and outputs $Z = \bigoplus_{i\in[2^d]} Z_i$. A formal description of the protocol can be found in Figure 3.

At a high level, PExt works because some block S_{i^*} (in fact most fractions of them) will be close to uniform and thus can be used as the seed for some randomness decoupler to certify that the output Z_{i^*} is close to uniform *even conditioned on everything except* D_{i^*}, which includes source X (hence S_{-i^*}), the adversary E, the devices D_{-i^*} used by other blocks (since we can view all of them as the adversary of the randomness decoupler). Thanks to the equivalence lemma (Lemma 4.1), we can choose any seeded PRE $\mathrm{PExt}_{\mathrm{seed}}$ as the randomness decoupler. Therefore, we have that Z_{i^*} is close to uniform conditioned on the outputs Z_{-i^*} of other blocks, and thus $Z = Z_{i^*} \oplus \left(\bigoplus_{j\neq i} Z_j\right)$ is close to uniform.

Before we proceed to the proof of the main theorem, we need the following lemmas that will be used later in the main proof.

Lemma 6.1 *For any PRE* PExt *and any two system states ρ, ρ' of some physical system $\mathcal{S}$, we have*

$$|\Delta(\mathrm{PExt}, \rho) - \Delta(\mathrm{PExt}, \rho')| \leq \left\|\rho - \rho'\right\|_{\mathrm{tr}}.$$

Proof. Note that ρ, ρ' are from the same $\mathcal{S}$. Thus, by definition and Fact 2.3, we have,

$$|\Delta(\mathrm{PExt}, \rho) - \Delta(\mathrm{PExt}, \rho')| \leq \left\|\Phi_{\mathrm{PExt}}(\rho) - \Phi_{\mathrm{PExt}}(\rho')\right\|_{\mathrm{tr}} \leq \left\|\rho - \rho'\right\|_{\mathrm{tr}}.$$

■

Lemma 6.2 *Let* $\mathrm{PExt}_{\mathrm{seed}}$ *be any seeded PRE with completeness error* ϵ_c *and soundness error* ϵ_s*. For any* $\epsilon > 0$*, we have*

- *There exists an honest device* D *with internal state* σ_D *and algorithm* A_D *such that for any physical system* $\mathcal{S}(\rho, A_D)$ *such that* $\rho_D = \sigma_D$ *and* $\|\rho_{XD} - \mathcal{U}_X \otimes \rho_D\|_{\mathrm{tr}} \le \epsilon$*, we have*

$$\mathbf{Pr}[\mathsf{Acc}(\mathrm{PExt}_{\mathrm{seed}}, \mathcal{S}(\rho))] \ge 1 - \epsilon_c - \epsilon.$$

- *Let* $\mathcal{S}(\rho)$ *be any physical system in which* $\|\rho_{XD} - \mathcal{U}_X \otimes \rho_D\|_{\mathrm{tr}} \le \epsilon$ *(i.e., the seed is* ϵ *close to uniform-to-device). The post-extraction state* $\mathrm{PExt}_{\mathrm{seed}}(\mathcal{S}(\rho))$ *is* $\epsilon_s + 2\sqrt{\epsilon}$*-uniform-to-*$XE$ *on* Acc*, i.e.,*

$$\Delta(\mathrm{PExt}_{\mathrm{seed}}, \rho) \le \epsilon_s + 2\sqrt{\epsilon}.$$

Proof. The claim follows easily from the completeness and the soundness of $\mathrm{PExt}_{\mathrm{seed}}$.

- By completeness, there exists such a device D with σ_D and A_D so that for any physical system $\mathcal{S}(\tau, A_D)$ in which $\tau_{XD} = \mathcal{U}_X \otimes \sigma_D$, we have $\mathbf{Pr}[\mathsf{Acc}(\mathrm{PExt}_{\mathrm{seed}}, \mathcal{S}(\tau))] \ge 1 - \epsilon_c$. For any physical system $\mathcal{S}(\rho, A_D)$, note that the event $\mathsf{Acc}(\mathrm{PExt}_{\mathrm{seed}}, \mathcal{S}(\rho))$ only depends on $X \otimes D$ system and $\|\rho_{XD} - \tau_{XD}\|_{\mathrm{tr}} \le \epsilon$. Thus we have,

$$\mathbf{Pr}[\mathsf{Acc}(\mathrm{PExt}_{\mathrm{seed}}, \mathcal{S}(\rho))] \ge \mathbf{Pr}[\mathsf{Acc}(\mathrm{PExt}_{\mathrm{seed}}, \mathcal{S}(\tau))] - \epsilon \ge 1 - \epsilon_c - \epsilon.$$

- By Lemma 2.2 and Lemma 2.1, there exists a physical system τ in which the seed is uniform-to-device such that $\|\rho_{XD} - \tau_{XD}\|_{\mathrm{tr}} \le \epsilon$ and $\|\rho - \tau\|_{\mathrm{tr}} \le 2\sqrt{\epsilon}$. By soundness, we have $\Delta(\mathrm{PExt}_{\mathrm{seed}}, \tau) \le \epsilon_s$. By Lemma 6.1,

$$\Delta(\mathrm{PExt}_{\mathrm{seed}}, \rho) \le \Delta(\mathrm{PExt}_{\mathrm{seed}}, \tau) + \|\rho - \tau\|_{\mathrm{tr}} \le \epsilon_s + 2\sqrt{\epsilon}.$$

■

Theorem 6.3 (Main) *Let* $0 < \eta < 1$ *be the rejection threshold. Let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a quantum* (k, ϵ)*-strong randomness extractor and* $\mathrm{PExt}_{\mathrm{seed}}$ *be a* $(m, t_{\mathsf{seed}}, l)$*-seeded-PRE for uniform-to-all seeds and with seed length* m*, completeness error* ϵ_c*, and soundness error* ϵ_s*. Then* PExt *(as shown in Fig. 3) is a* $(n, k, 2^d t_{\mathsf{seed}}, l)$*-PRE for random-to-device sources with completeness error* $(\epsilon_c + \epsilon)/\eta$ *and soundness error* $\epsilon_s + 2\sqrt{\epsilon} + 2\eta$*.*

Proof. Let $S = (S_1, \ldots, S_{2^d})$ and $D = (D_1, \ldots, D_{2^d})$. Consider any physical system $\mathcal{S}(\rho)$ on $X \otimes D \otimes E$ such that $\mathrm{H}_\infty(X|D) \ge k$. Let w_i denote $\|\rho_{S_i D_i} - \mathcal{U}_{S_i} \otimes \rho_{D_i}\|_{\mathrm{tr}}$ for each $i = 1, \cdots, 2^d$. Thus, by the construction of the protocol in Fig. 3 and Proposition 5.5, we have

$$\mathrm{E}_{i \sim \mathcal{U}}[w_i] = \frac{1}{2^d} \sum_{i=1}^{2^d} \|\rho_{S_i D_i} - \mathcal{U}_{S_i} \otimes \rho_{D_i}\|_{\mathrm{tr}} \le \epsilon, \tag{6.1}$$

where $\mathrm{E}_{i \sim \mathcal{U}}$ denotes the expectation over uniformly selected index i. Let Acc (resp. Rej) denote the indicator of the event of acceptance (resp. rejection) of PExt and Acc^i (resp. Rej^i) denote the indicator of the event of acceptance (resp. rejection) of $\mathrm{PExt}_{\mathrm{seed}}$ on $S_i \otimes D_i$. Note that the parameters $(n, k, 2^d t_{\mathsf{seed}}, l)$ of PExt follow directly from the construction. It suffices to prove the bounds for completeness and soundness errors.

(Completeness): For each $i = 1, \cdots, 2^d$, by completeness of $\mathrm{PExt}_{\mathrm{seed}}$ and Lemma 6.2, there exists a honest device D_i such that for the corresponding S_i, we have

$$\mathbf{Pr}[\mathsf{Acc}(\mathrm{PExt}_{\mathrm{seed}}, S_i \otimes D_i)] \geq 1 - \epsilon_c - w_i.$$

Namely, $\mathrm{E}[\mathsf{Rej}^i] \leq \epsilon_c + w_i$. By the linearity of expectation, we have

$$\mathrm{E}[\frac{1}{2^d}\sum_{i=1}^{2^d} \mathsf{Rej}^i] = \frac{1}{2^d}\sum_{i=1}^{2^d} \mathrm{E}[\mathsf{Rej}^i] \leq \mathrm{E}_{i \sim \mathcal{U}}[\epsilon_c] + \mathrm{E}_{i \sim \mathcal{U}}[w_i] \leq \epsilon_c + \epsilon.$$

Moreover, we can choose the honest devices of PExt to be the tensor product of honest devices for $\mathrm{PExt}_{\mathrm{seed}}$ on each block. Therefore, by Markov inequality, we have

$$\mathbf{Pr}[\mathsf{Acc}(\mathrm{PExt}, \mathcal{S})] = 1 - \mathbf{Pr}[\frac{1}{2^d}\sum_{i=1}^{2^d} \mathsf{Rej}^i \leq \eta] \geq 1 - (\epsilon_c + \epsilon)/\eta,$$

which, by definition, implies that PExt has completeness error $(\epsilon_c + \epsilon)/\eta$.

(Soundness): To prove the soundness of PExt, it suffices to show the post-extraction state $\Phi_{\mathrm{PExt}}(\rho)$ is very close to uniform-to-XE on Acc. To that end, we need to find out such a uniform-to-XE on Acc state that is close to $\Phi_{\mathrm{PExt}}(\rho)$. For each index i, we demonstrate as follows how to construct a uniform-to-XE on Acc state γ_i to which the distance of $\Phi_{\mathrm{PExt}}(\rho)$ can be bounded.

To construct γ_i, first observe that by the soundness of $\mathrm{PExt}_{\mathrm{seed}}$, the distance of the output of the ith block to uniform on Acc^i is bounded by some function of w_i and ϵ_s. If we were to only output the Acc^i part in our final Acc part, then the distance between $\Phi_{\mathrm{PExt}}(\rho)$ and γ_i can be bounded by the same function. However, the final Acc part also possibly contains the Rej^i part, which potentially increases the distance between $\Phi_{\mathrm{PExt}}(\rho)$ and γ_i. We upper bound such an increase by the probability of the event $\mathsf{Acc} \wedge \mathsf{Rej}^i$.

Although we don't have a good control on every w_i and the probability of the event $\mathsf{Acc} \wedge \mathsf{Rej}^i$, we know the averages of them respectively are small. Thus, we could simply bound the distance between $\Phi_{\mathrm{PExt}}(\rho)$ and the average of γ_i, which by definition is still a uniform-to-XE on Acc state.

The above intuition is technically achieved by Lemma 6.4, which states that for each i, there exists such a $\gamma_i \in XE\text{-}\mathrm{Uni}^{\mathsf{Acc}}(\mathcal{S})$ so that

$$\|\Phi_{\mathrm{PExt}}(\rho) - \gamma_i\|_{\mathrm{tr}} \leq \epsilon_s + 2\sqrt{w_i} + 2\mathbf{Pr}[\mathsf{Acc} \wedge \mathsf{Rej}^i].$$

Thus, by taking the average of γ_i (i.e., $\mathrm{E}_{i \sim \mathcal{U}}[\gamma_i]$), we have

$$\begin{aligned} \Delta(\mathrm{PExt}, \rho) &\leq \|\Phi_{\mathrm{PExt}}(\rho) - \mathrm{E}_{i \sim \mathcal{U}}\gamma_i\|_{\mathrm{tr}} \leq \mathrm{E}_{i \sim \mathcal{U}}\|\Phi_{\mathrm{PExt}}(\rho) - \gamma_i\|_{\mathrm{tr}} \\ &\leq \mathrm{E}_{i \sim \mathcal{U}}[\epsilon_s] + \mathrm{E}_{i \sim \mathcal{U}}[2\sqrt{w_i}] + \mathrm{E}_{i \sim \mathcal{U}}[2\mathbf{Pr}[\mathsf{Acc} \wedge \mathsf{Rej}^i]]. \end{aligned}$$

The first term is simply ϵ_s. By concavity of the square root function, we have $\mathrm{E}_{i \sim \mathcal{U}}[2\sqrt{w_i}] \leq 2\sqrt{\mathrm{E}_{i \sim \mathcal{U}}[w_i]} \leq 2\sqrt{\epsilon}$. For the third term, first let $\mathsf{Acc} \wedge \mathsf{Rej}^i$ also denote the indicator of the event. Thus, we have $\mathrm{E}[\mathsf{Acc} \wedge \mathsf{Rej}^i] = \mathbf{Pr}[\mathsf{Acc} \wedge \mathsf{Rej}^i]$. Then observe that by our protocol, the event Acc implies that the rejection fraction is no more than η. Namely, we have $\mathrm{E}_{i \sim \mathcal{U}}[\mathsf{Acc} \wedge \mathsf{Rej}^i] \leq \eta$. By the linearity of expectation, we have $\mathrm{E}_{i \sim \mathcal{U}}[2\mathbf{Pr}[\mathsf{Acc} \wedge \mathsf{Rej}^i]] = 2\,\mathrm{E}[\mathrm{E}_{i \sim \mathcal{U}}[\mathsf{Acc} \wedge \mathsf{Rej}^i]] \leq 2\,\mathrm{E}[\eta] \leq 2\eta$. Therefore,

$$\Delta(\mathrm{PExt}, \rho) \leq \epsilon_s + 2\sqrt{\epsilon} + 2\eta,$$

which, by definition, shows that PExt has soundness error $\epsilon_s + 2\sqrt{\epsilon} + 2\eta$. ■

Lemma 6.4 *For each i with $\|\rho_{S_iD_i} - \mathcal{U}_{S_i} \otimes \rho_{D_i}\|_{\mathrm{tr}} \leq w_i$, there exists $\gamma_i \in XE$-Uni$^{\mathsf{Acc}}(\mathcal{S})$ such that*

$$\|\Phi_{\mathrm{PExt}}(\rho) - \gamma_i\|_{\mathrm{tr}} \leq \epsilon_s + 2\sqrt{w_i} + 2\mathbf{Pr}[\mathsf{Acc} \wedge \mathsf{Rej}^i].$$

Proof. We will construct such a γ_i by analyzing the protocol PExt which is decomposed into the following three steps. The first step is to apply $\mathrm{PExt}_{\mathrm{seed}}$ on (S_i, D_i) and obtain (O_i, Z_i). The second step is to finish all operations on the rest system (S_{-i}, D_{-i}) and obtain (O, Z_i), where O indicates the global acceptance according to the protocol and $Z_{-i} = \oplus_{j \neq i} Z_j$. The final step is to XOR Z_i with Z_{-i} when $O = \mathsf{Acc}$.

Let $\Phi^i_{\mathrm{PExt}_{\mathrm{seed}}}$ denote the super-operator of the first step. Note that $\|\rho_{S_iD_i} - \mathcal{U}_{S_i} \otimes \rho_{D_i}\|_{\mathrm{tr}} \leq w_i$, while S_i might be correlated with the environment $E' = (S_{-i}, D_{-i}, X, E)$. Recall that for any $\tau \in \mathrm{Dens}\,(O_iZ_iS_iD_iE')$, one can decompose it with respect to O_i as follows:

$$\tau_{O_iZ_iS_iE'} = \left|\mathsf{Acc}^i\right\rangle\!\left\langle\mathsf{Acc}^i\right| \otimes \tau^{\mathsf{Acc}^i}_{Z_iS_iE'} + \left|\mathsf{Rej}^i\right\rangle\!\left\langle\mathsf{Rej}^i\right| \otimes \tau^{\mathsf{Rej}^i}_{Z_iS_iE'}.$$

Let $\rho_{O_iZ_iS_iD_iE'} = \Phi^i_{\mathrm{PExt}_{\mathrm{seed}}} \otimes \mathsf{id}_{E'}(\rho_{S_iD_iE'})$. By Lemma 4.1, $\mathrm{PExt}_{\mathrm{seed}}$ works for uniform-to-device seeds. Thus by the soundness of $\mathrm{PExt}_{\mathrm{seed}}$ and Lemma 6.2, there exists $\tau \in \mathrm{Dens}\,(O_iZ_iS_iD_iE')$ such that

$$\tau \in S_iE'\text{-Uni}^{\mathsf{Acc}^i}(\mathcal{S}) \text{ and } \|\rho_{O_iZ_iS_iD_iE'} - \tau_{O_iZ_iS_iD_iE'}\|_{\mathrm{tr}} \leq \epsilon_s + 2\sqrt{w_i}. \tag{6.2}$$

Namely, the output Z_i is uniform-to-S_iE' on Acc^i in τ.

Let Φ^{-i} denote the joint super-operator of the second and the third step. We claim that $\Phi^{-i}(\tau)$ is $2\mathbf{Pr}[\mathsf{Acc} \wedge \mathsf{Rej}^i]$ close to a uniform-to-XE on Acc state, which is γ_i that we construct. Therefore, by Fact 2.3 and by definition, the final state of PExt (i.e., $\Phi_{\mathrm{PExt}}(\rho)$), which is given by $\Phi^{-i}(\rho_{O_iZ_iS_iD_iE'})$, is $\epsilon_s + 2\sqrt{w_i} + 2\mathbf{Pr}[\mathsf{Acc} \wedge \mathsf{Rej}^i]$ close to γ_i.

To that end, we analyze the procedure of applying Φ^{-i} to τ. Let $E'' = (S, X, E)$. After the second step, the resultant state is $\tau_{O_iZ_iOZ_{-i}DE''}$ and its reduced state without D system is

$$\left|\mathsf{Acc}^i, \mathsf{Acc}\right\rangle \otimes \mathcal{U}_{Z_i} \otimes \tau^{\mathsf{Acc}^i,\mathsf{Acc}}_{Z_{-i}E''} + \left|\mathsf{Rej}^i, \mathsf{Acc}\right\rangle \otimes \tau^{\mathsf{Rej}^i,\mathsf{Acc}}_{Z_iZ_{-i}E''} + \left|\mathsf{Acc}^i, \mathsf{Rej}\right\rangle \otimes \mathcal{U}_{Z_i} \otimes \tau^{\mathsf{Acc}^i,\mathsf{Rej}}_{Z_{-i}E''} + \left|\mathsf{Rej}^i, \mathsf{Rej}\right\rangle \otimes \tau^{\mathsf{Rej}^i,\mathsf{Rej}}_{Z_iZ_{-i}E''}.$$

The last step is to take $Z = Z_i \oplus Z_{-i}$ when $O = \mathsf{Acc}$. Therefore, only two terms $\left|\mathsf{Acc}^i, \mathsf{Acc}\right\rangle \otimes \mathcal{U}_{Z_i} \otimes \tau^{\mathsf{Acc}^i,\mathsf{Acc}}_{Z_{-i}E''}$, $\left|\mathsf{Rej}^i, \mathsf{Acc}\right\rangle \otimes \tau^{\mathsf{Rej}^i,\mathsf{Acc}}_{Z_iZ_{-i}E''}$ will appear in the Acc part. Let Φ_{XOR} denote the operation that outputs $Z = Z_1 \oplus Z_2$ given inputs Z_1, Z_2. For the first term, it is easy to see that

$$\Phi_{\mathrm{XOR}} \otimes \mathsf{id}_{E''}(\mathcal{U}_{Z_i} \otimes \tau^{\mathsf{Acc}^i,\mathsf{Acc}}_{Z_{-i}E''}) = \mathcal{U}_Z \otimes \tau^{\mathsf{Acc}^i,\mathsf{Acc}}_{E''},$$

in which Z is uniform-to-XE on Acc. The second term does enjoy the guarantee as above. However, we know that $\mathrm{tr}(\left|\mathsf{Rej}^i, \mathsf{Acc}\right\rangle \otimes \tau^{\mathsf{Rej}^i,\mathsf{Acc}}_{Z_iZ_{-i}E''}) = \mathbf{Pr}[\mathsf{Acc} \wedge \mathsf{Rej}^i]$.

We hence construct γ_i as follows; We keep all but the $\left|\mathsf{Rej}^i, \mathsf{Acc}\right\rangle \otimes \tau^{\mathsf{Rej}^i,\mathsf{Acc}}_{ZE''}$ part of $\Phi_{-i}(\tau)$, which is replaced by $\left|\mathsf{Rej}^i, \mathsf{Acc}\right\rangle \otimes \mathcal{U}_Z \otimes \tau^{\mathsf{Rej}^i,\mathsf{Acc}}_{E''}$. It is easy to see that by definition $\gamma_i \in XE$-Uni$^{\mathsf{Acc}}(\mathcal{S})$. Moreover, we have $\left\|\Phi^{-i}(\tau) - \gamma_i\right\|_{\mathrm{tr}} \leq 2\mathbf{Pr}[\mathsf{Acc} \wedge \mathsf{Rej}^i]$. Finally, by the triangle inequality, Fact 2.3 and (6.2), we have

$$\|\Phi_{\mathrm{PExt}}(\rho) - \gamma_i\|_{\mathrm{tr}} \leq \left\|\Phi^{-i}(\rho_{O_iZ_iS_iD_iE'}) - \Phi^{-i}(\tau)\right\|_{\mathrm{tr}} + \left\|\Phi^{-i}(\tau) - \gamma_i\right\|_{\mathrm{tr}} \leq \epsilon_s + 2\sqrt{w_i} + 2\mathbf{Pr}[\mathsf{Acc} \wedge \mathsf{Rej}^i].$$

■

Instantiations. The Miller-Shi seeded PRE (and its unbounded expansion composition via EL) subsumes all other constructions, thus is preferred to use in our instantiations. Thus the main choice is the quantum-proof classical strong extractors. We use two known methods for constructing such extractors, both based on the work of Konig and Terhal [16] showing that any classically secure one-bit extractor is automatically secure against quantum adversaries (with slightly worse parameters.) The first method is to take a single-bit extractor and increase the output length by using independent copies of the seeds. The second is to apply Trevisan's compositions of the single-bit extractor, which was proved to be quantum-secure by De *et al.* [10].

The instantiation in Corollary 1.1 is obtained using the first method, setting the error parameter of the single-bit extractor (e.g. in Proposition 5.3 of [10]) to be $\Theta(\epsilon/\log^c(1/\epsilon))$, where c is a universal constant from Miller-Shi [19], and the number of independent seeds to be $O(\log^c(1/\epsilon))$. This requires the min-entropy to be $O(\log^c 1/\epsilon)$. The number of devices is $(n/\epsilon)^{O(\log^c(1/\epsilon))}$, thus is efficient for constant ϵ.

Corollary 1.2 uses a Trevisan's extractor (Corollary 5.6 of [10]). The extractor requires only $O(\log(n/\epsilon))$ seed length for an input length n and error ϵ. Thus with polynomial $1/\epsilon$, the number of devices remains a polynomial in the security parameter.

References

[1] N.S.A. able to foil basic safeguards of privacy on web. *The New York Times*, September 5, 2013.

[2] J. Barrett, R. Colbeck, and A. Kent. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.*, 110:010503, Jan 2013.

[3] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, Jun 2005.

[4] M. Berta, O. Fawzi, and S. Wehner. Quantum to classical randomness extractors. *IEEE Transactions on Information Theory*, 60(2):1168–1192, 2014.

[5] F. G. Brandão, R. Ramanathan, K. H. Andrzej Grudka, M. Horodecki, and P. Horodecki. Robust device-independent randomness amplification with few devices. *QIP 2014*, arXiv:1310.4544.

[6] K.-M. Chung, X. Wu, and Y. Shi. Physical randomness extractors. *QIP 2014*, arXiv:1402.4797, 2014.

[7] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, October 1969.

[8] R. Colbeck and R. Renner. Free randomness can be amplified. *Nature Physics*, 8:450–453, 2012.

[9] M. Coudron and H. Yuen. Infinite randomness expansion and amplification with a constant number of devices. To appear in *STOC 2014*, arXiv:1310.6755.

[10] A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan's extractor in the presence of quantum side information. *SIAM Journal on Computing*, 067(258932), 2012.

[11] S. Fehr, R. Gelles, and C. Schaffner. Security and composability of randomness expansion from Bell inequalities. *Phys. Rev. A*, 87:012335, Jan 2013.

[12] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita, and A. Acín. Full randomness from arbitrarily deterministic events. *Nature Communications*, 4:2654, 2013.

[13] Z. Gutterman, B. Pinkas, and T. Reinman. Analysis of the linux random number generator. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, SP '06, pages 371–385, Washington, DC, USA, 2006. IEEE Computer Society.

[14] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman. Mining your ps and qs: Detection of widespread weak keys in network devices. In *Proceedings of the 21st USENIX Security Symposium*, 2012.

[15] R. Jain, S. Upadhyay, and J. Watrous. Two-message quantum interactive proofs are in PSPACE. In *Proceedings of the 50th IEEE Symposium on Foundations of Computer Science (FOCS 2009)*, pages 534–543, 2009. arXiv:0905.1300v1 [quant-ph].

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

[17] X. Li. New independent source extractors with exponential improvement. *In Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, 2013.

[18] L. Masanes. Universally composable privacy amplification from causality constraints. *Phys. Rev. Lett.*, 102:140501, Apr 2009.

[19] C. A. Miller and Y. Shi. Self-testing quantum dice certified by a uncertainty principle. Personal communication, 2013.

[20] A. Rao. *Randomness Extractors for Independent Sources and Applications.* PhD thesis, The Univeristy of Texas at Austin, 2007.

[21] B. W. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. *Nature*, 496:456–460, April 2013.

[22] R. Renner. Security of quantum key distribution, Jan. 11 2005. Comment: PhD thesis; index added.

[23] R. Renner, S. Wolf, and J. Wullschleger. The single-serving channel capacity. In *Proceedings of the 2006 IEEE International Symposium on Information Theory (ISIT)*, Aug. 02 2006. Comment: 4 pages, latex.

[24] T. Ristenpart and S. Yilek. When good randomness goes bad: Virtual machine reset vulnerabilities and hedging deployed cryptography. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2010, San Diego, California, USA, 28th February - 3rd March 2010.* The Internet Society, 2010.

[25] M. Santha and U. V. Vazirani. Generating quasi-random sequences from slightly-random sources. In *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS 1984)*, page 434, 1984.

[26] S. Vadhan. The unified theory of pseudorandomness. *SIGACT News*, 38(3):39–54, September 2007.

[27] U. Vazirani and T. Vidick. Fully device independent quantum key distribution. In *Proceedings of The 5th Innovations in Theoretical Computer Science (ITCS)*, 2014. arXiv:1210.1810v2.

[28] U. V. Vazirani and T. Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In H. J. Karloff and T. Pitassi, editors, *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 61–76. ACM, 2012.

[29] D. Zuckerman. General weak random sources. In *Foundations of Computer Science, 1990. Proceedings., 31st Annual Symposium on*, pages 534–543 vol.2, 1990.