Quantum randomness amplification and expansion

Yuyang Liu, Wenzler Nils

1 Introduction

Randomness is an important resource for many tasks in computer science, but especially for cryptography. Nearly all of now a days cryptographic primitives rely to some part on the existence of randomness.

Classically, randomness is obtained by use of pseudorandom number generators and randomness extractors. For pseudorandom number generators to be applicable, one must assume that a possible adversary is limited in his computational resources. Furthermore, one needs a considerable short uniform input seed to initialize a pseudorandom number generator, from which it generates a close to uniform significantly longer output. This task is therefore as well known as randomness expansion. In general the available randomness sources are not uniformly distributed, but so called weak randomness sources.

Randomness extractors take a weak random source as input and output an almost uniform random string. They can be used to transform a weak randomness source to uniform random source which can be used for pseudo random number generators. Furthermore, they do not rely on an adversary which has access to only limited computational resources. However, no purely classical approach can take a general min-entropy source, a common classification for weak randomness sources, as input and create almost uniform randomness as output. Classical randomness extractors are relying on a small random seed (seeded extractors) or multiple independent sources of randomness (multi-source) to be usable.

In a quantum context, both the issue of obtaining a seed for randomness extraction and the assumption of limited adversaries for randomness expansion can be overcome.

One of the key challenges that make this task non-trivial, lies within the fact that one does not want to blindly trust the possibly unknown physical implementation of quantum devices.

By use of games like CHSH [CHSH69], one can resolve this issue in implementing so-called device-independent protocols.

Throughout the following paper, we introduce the reader to the fascinating world of randomness extraction/amplification and randomness expansion, by first introducing the most basic foundations and explaining how one can obtain randomness out of so-called Santha-Vazirani sources and the earlier mentioned min-entropy sources.

2 Foundations

Before we can enter the mysterious world of randomness amplification and expansion, we will take a short moment to introduce some important and common notions of the field.

2.1 Sources of Randomness

Except for random sources which are uniformly distributed, there are a lot of different notions of less optimally distributed sources. In reality we are often only able to obtain such weak random sources. The most two important ones are the Santha-Vazirani source and the min-entropy source.

Definition. Santha-Vazirani source / ϵ-Santha-Vazirani source A Santha-Vazirani source (SV source) has uncertainty in each individual bit even conditioned on the value of its previous bits. Namely, a source X over $\{0,1\}^n$ is ϵ-SV if for every $i \in [n]$ and $x_{\leq i} \in \{0,1\}^i$, $\epsilon \leq Pr[X_i = x_i | X_{<i} = x_{<i}] \leq 1 - \epsilon$ [CSW14].

Many of the natural processes produce a sequence of bits in the chronological order which implies that each bit can only depend on the past and not on the future. Hence, a SV-source can describe such process in a realistic way [KAF17].

Although this definition may already seem a quite weak definition for a randomness source, the min-entropy is even less constrained.

Definition. Min-entropy and min-entropy source/k-source The min-entropy of a distribution X is given by

$$H_\infty(X) = \min_x \left\{ \log_2(\frac{1}{Pr[X = x]}) \right\}$$

A random variable X is a k-source if $H_\infty(X) \geq k$ or alternatively

$$\forall x \in X : Pr[X = x] \leq 2^{-k}$$

[Vad12]

For a min-entropy source, single bits of the output may be heavily correlated. It may as well be that some bits are constant throughout all outcomes.

When looking into research which focuses on randomness amplification and expansion it is often necessary to argue that two distributions are close to being the same. We therefore introduce the notion of ε-close distributions.

Definition. ε-close distributions Two distributions X, Y over the same domain are ε-close if for every event A, $|Pr[X \in A] - Pr[X \in B]| \leq \varepsilon$. [CSW16]

2.2 Randomness Expansion

In cryptography, algorithm design and some other fields, randomness is considered to be a resource. It therefore would be a valuable thing to be able to expand randomness. By randomness expansion, we describe a setting in which we are given a certain amount of uniformly random bits and try to create a larger number of still uniformly random bits out of those. It is clear that this is generally not possible in a classical context. A deterministic algorithm will only be able to produce n different outputs when given n different inputs.

In a quantum setting, it was shown that it is possible to perform exponential randomness expansion with two quantum devices and even infinite randomness expansion with a set of low number constant quantum devices [CY14].

2.3 Randomness Amplification

To perform randomness expansion, one does still need an initial uniformly random seed. In reality it is hard to obtain such a uniformly random seed. This becomes clearly visible when picturing the parameters which are used in modern operating systems for pseudo-random number generation. These algorithms use parameters such as mouse movement, time, process scheduling, and similar ones to generate pseudo random numbers. Although one can suspect that there is some randomness in such parameters, it is hard to justify those to be uniformly random. They more likely resemble weak randomness sources such as introduced earlier.

Randomness amplification is the problem of generating a uniform random output when given a weak randomness source as an input. The notion of min-entropy measures how many bits of randomness would be theoretically located in the output of a min-entropy source. Therefore, it offers an upper-bound on the possible effectiveness of randomness amplification.

Randomness amplification is a well researched topic in a classical context. The most important takeaways for this work are that one can not use a classical (and therefore deterministic) randomness extractor to perform randomness amplification on a weak randomness source. The second takeaway is that one can use so-called seeded randomness extractors which are given an additional short and uniformly random seed to

extract uniform randomness out of a weak randomness source. Those deterministic and classical algorithms are defined as follows:

Definition. Seeded randomness extractor A function $E : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (k, ε)-extractor / seeded randomness extractor if for every distribution X over $\{0,1\}^n$ with $H_\infty(X) \geq k$, $E(X, Y)$ is ε-close to uniform (where Y is distributed uniformly over $\{0,1\}^d$ and is independent of X) [Sha11].

2.4 Device-independent Protocols, Non-signalling and Non-locality

One big issue in quantum computing is how to know whether the physical quantum devices are really implementing the protocol that we asked us. Especially in randomness expansion and randomness amplification, where we rely on quantum protocols to be an essential part of our protocols, we have to make sure that these devices are not able to fool us. With this in mind, the notion of device-independent protocols was developed. For device-independent protocols we look at the quantum devices as black-boxes and only consider their classical interface. Even just looking at this interface, we can enforce that the devices implement the necessary quantum strategy by letting them play special quantum games, such as the well known CHSH game and evaluating their chance of winning the game. If their winning chances are close to the optimal winning strategies, they have to implement a quantum strategy to win the game.

For the following discussion to hold true, we have to agree on the following two assumptions [CSW16]:

- The rules, laws and predictions of modern Quantum Theory hold true.
- Without the exchange of information, one system may not affect the observable behavior of another system.

Without these assumptions, we are not able to argue that the quantum setting is able to produce real randomness in contrast to the classical world.

The second assumption is also called non-signalling.

Such a assumption can be enforced by dividing a set of devices by huge distance. Since information can only travel at a maximum of the speed of light, if the devices are divided by a large enough distance.

But if we divide our devices by such a huge distance and want the devices still have an advantage over classical devices when they play a game together, how can that be possible.

This is possible by the important concept of quantum non-locality which is closely related to entanglement. Although quantum devices are not able to share information by use of entangled qubits, they are able to share a common state which gives enough advantage in those specially designed games to perform significantly better than their classical counterparts.

3 Frontiers

After having introduced the necessary foundations in the last section, we will present the most recent findings concerning how to perform randomness amplification in this section.

We therefore present the general way of how randomness amplification is currently thought of for min-entropy sources as well as for SV sources. Figure 1 gives a thorough overview and comparison over the different different works on the topic of randomness amplification considering different aspects of the constraints. In this paper we present two selected approaches.

3.1 Frontiers for Santha-Vazirani sources

Started with a SV source with $\mu \in (0, 0.5)$, λ means the bits before adversary, Eve, creates the device. λ also includes other classical information that Eve may use. E is the quantum side information $E = E(\lambda)$ that Eve can take advantage later on. Alice then creates final random string K from the device along with the bit from input I and Z. We have the assumption that history λ and Eve's knowledge E are independent from $I \circ Z$. The protocol is described as: the devices take inputs from I one by one and creates output O. Alice calculates the mean of the violation of a Bell inequality from the output. Alice would abort the game

Work	Source	Adversary	Number of Devices	Public source?	Arbitrary bias?	Robust?	Efficient?
[CR12]	SV	Q & NS	2	✓	✗	✗	zero
[GMdlT+13]	SV	NS	poly	✓	✓	✓	zero
[BRG+16]	SV	NS	4	✗	✓	✓	✓
[KAF17]	SV	Q	2	✓	✓	✓	✓
[CSW14]	min-entropy	Q	poly	✓	✓	slightly	zero
[CSW16]	min-entropy	NS	exp	✓	✓	slightly	zero
[BPPP14]	min-entropy	Q & NS	poly	✓	N.A.	slightly	N.A.

Figure 1: Comparisons among results from [KAF17] and previous works. N.A. relates to unknown, or not mentioned by author

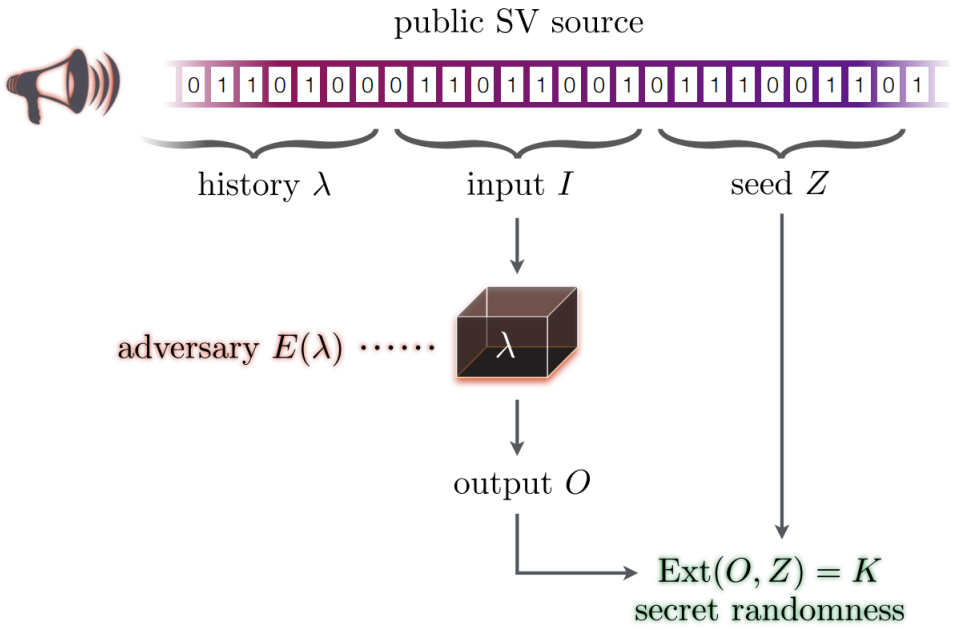

Figure 2: Protocol from Kessler et al. [KAF17] on Device-independent Randomness Amplification and Privatization

if the violation value is not high enough, otherwise she would use the randomness extractor against O along with the seed Z to generate K.

Definition. μ-MDL source[PRB+14] Let S be any source producing binary random variables X_i and Y_i that can depend on some side information λ. For any $\mu = \{\mu_{min}, \mu_{max}\} \in (0, \frac{1}{4}) \times (\frac{1}{4}, 1)$, S is called a μ-MDL source if the outputs have the following distributions that depends on λ:

$$\mu_{min} \leq P_{X_i Y_i | X^{i-1} Y^{i-1}, \lambda}(x_i y_i | x^{i-1} y^{i-1}) \leq \mu_{max} \ \forall x^i, y^i.$$

Lemma. *For all* $0 \leq \mu \leq \frac{1}{2}$ *a* μ*-SV source is a* $\{(\frac{1}{2} - \mu)^2, (\frac{1}{2} + \mu)^2\}$*-MDL source.*

Definition. von Neumann entropy[Neu27] Let $\mathcal{H}_A$ and $\mathcal{H}_E$ be two Hilbert spaces and ρ_{AE}(density operator) a quantum state on $\mathcal{H}_A \otimes \mathcal{H}_E$. Then the von Neumann entropy is defined as:

$$H(AE)_{\rho_{AE}} = -\text{Tr}(\rho_{AE} log \rho_{AE})$$

and the conditional von Neumann entropy is:

$$H(A|E)_{\rho_{AE}} = H(AE)_{\rho_{AE}} - H(E)_{\rho_{AE}}$$

Definition. Smooth min-entropy[KAF17] Let $\mathcal{H}_A$ and $\mathcal{H}_E$ be two Hilbert spaces and $\rho_{AE} = \sum_a p_a |a\rangle\langle a| \otimes \rho_E^a$(density operator) a quantum state on $\mathcal{H}_A \otimes \mathcal{H}_E$. Then the conditional min-entropy is:

$$H_{min}^{\varepsilon}(A|E)_{\rho_{AE}} = \max_{\sigma_{AE} \in \beta^{\varepsilon}(\rho_{AE})} -log \max_{\{M_E^a\}_a} \left| \sum_a p_a \mathrm{Tr}(M_E^a \rho_E^a) \right|$$

where the maximization ranges over all sets of POVMs $\{M_E^a\}_a$ on E.

3.1.1 Bell inequality

As the device and inputs I can correlate via λ, the Bell inequality "measurement dependent locality(MDL)" from [PRB+14] is adapted by [KAF17] to support any bias of the source, which accounts for the dependency between the device and the side information. The Bell inequality from CHSH cannot be used for bias; other Bell inequalities considering the bias need more components for the device. A new Bell inequality - a MDL inequality [PRB+14]:

$$S_\mu = \mu_{min} P_{ABXY}(0000) - \mu_{max}(P_{ABXY}(0101) + P_{ABXY}(1010) + P_{ABXY}(0011)) \leq 0$$

For any bias from the source, there is always a quantum strategy that creates a large margin of violation of the inequality[PRB+14]. In fact the maximum violation margin can be computed numerically[KAF17].

3.1.2 Randomness from MDL violation from per use of device

Non-local games usually assume that input challenges are uniformly distributed (measurement independence).

Relaxing the independence assumption where Eve can influence the distributions of the input challenges leads to a MDL source. In the paper of [KAF17], a lower-bound on the amount of knowledge Eve can gain from the violation of MDL inequality in the context of von Neumann entropy is derived:

$$H(O_i|I_i E, \lambda) \geq t$$

where I_i and O_i are the input and output for the i'th iteration; $t \geq 0$ depends on the bias of the source and the violation of the MDL inequality:

$$t = H(AB|XYE) \geq 1 - h\Big(\frac{1}{2} + \frac{1}{\mu_{min} * \mu_{max}} \sqrt{S_\mu (S_\mu + \mu_{min} * \mu_{max})}\Big)$$

where $S_\mu > 0$.

The lower-bound is non-trivial if the MDL inequality is violated, and trivial (conditional entropy = 0) if the device is playing classic strategy. This nice property enables maximal tolerance regarding noise.

3.1.3 Total amount of min-entropy from multiple uses of device

If the usage of the device is independent and identical each time, we could have summed up the entropy gained at each round. However, the adversary could prepare the device in a way that violates this assumption.

With the entropy accumulation theorem (EAT)[DFR16] under the framework proposed in [AFRV16], one can bound the accumulated smooth min-entropy using von Neumann entropy from each step.

Theorem. *Entropy Accumulation Theorem*

$$H_{min}^{\varepsilon}(A^n B^n | I^n E)_{\rho|\Omega} \geq nt - v\sqrt{n}$$

where $v = 2(log(1 + 2d_{A_i B_i}) + \lceil \|\nabla f_{min}\|_\infty \rceil)\sqrt{1 - 2log(\varepsilon_s \cdot \rho|_\Omega)}$ *and* $d_{A_i B_i}$ *means the dimension of* $A_i B_i$.

Please refer to [KAF17] for the definition of Min-tradeoff function f_{min}, it defines the worst case von Neumann entropy accumulated in each round of the protocol. $\rho|_\Omega$ is the state in the end of the protocol conditioned on not aborting. n is the number of rounds of the protocol and t is the minimal amount of entropy accumulated in each step.

To get the lower-bound of the total conditional smooth min-entropy: $H_{min}^{\varepsilon_s}(O|IE, \lambda)$ where $\varepsilon_s \in (0, 1)$. By EAT, we can see the first order term of the bound is $nH(O_i|I_i E, \lambda)$. $H_{min}^{\varepsilon_s}(O|IE, \lambda) \in \Omega(n)$ which is optimal.

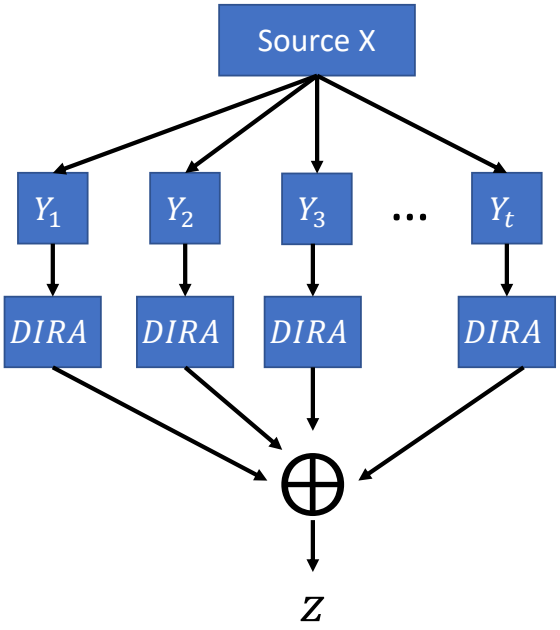

Figure 3: For each possible seed i one randomness amplification game with the input $Y_i = Ext(X, i)$ and each using new devices is created. One of the inputs Y_i will be ε-uniform distributed.

3.1.4 Extract the randomness

Regular extractors (seeded or multi-source) are unable to handle only one SV-source. [AFRV16] proved that any (strong) multi-source extractor is also a (strong) quantum-proof multi-source extractor in the Markov model, with some loss in parameters.

$$I(O : Z|IE, \lambda) = 0$$

meaning that given I, E, and λ, O and Z are independent. With high entropy from the previous EAT in O and high entropy in Z from the SV-source, one can apply the special extractor to generate clos to uniform string $K = Ext(O, Z)$

3.2 Frontiers for Min-Entropy sources

Research has shown that there exists an efficient protocol to perform Randomness Amplification with only two devices when working with SV-sources [KAF17]. But even when considering the less structured min-entropy sources, it is possible to implement quantum protocols which allow for randomness amplification. Bouda et al. [BPPP14] have shown that one can do so by using, poly(n) number of devices, which is at time of writing this report the best result considering the number of devices being use. Nonetheless, we present the approach of Chung et al. [CSW16] which uses exp(n) number of devices, but is easier to understand and basically relies on the same concepts.

One issue when trying to perform quantum randomness amplification, is that you have to enforce that the used devices have to implement a truly random quantum strategy to comply with the requirements of the protocol. If the devices would be able to secretly comply with the protocol without using a truly random quantum strategy there is no known way to certify that the outputs are truly random. Sadly, it seems that the only way of enforcing this is to use close to uniform random inputs for the devices. In the context of Randomness Amplification we do not have access to uniform random inputs.

Chung et al. use the concept of classical seeded randomness extractors, which are able to produce a ε-close uniform distribution, given any source X of length n and a uniform seed of length d. Since we can not obtain a uniform random seed as well, Chung et al. solve this issue by using a brute-force approach in their protocol.

Since there is no access to a uniform random seed, one can proceed by continuing with a set of i different inputs Y_i which one obtains by applying a classical randomness extractor to X and i, such that $Y_i = Ext(X, i)$. Overall we obtain 2^d of such Y_i.

It is easy to see, that at least one of these Y_i will be ε-close to a uniform distribution. Let's call this input Y_i^*.

If we would know which $Y_i = Y_i^*$, we could use that Y_i to play e.g. the GHSH game with two devices and Y_i as an input. Let z_i denote the output of the corresponding game. By measuring the success rate of the devices in winning GHSH, we can make sure that the devices have implemented a quantum strategy and can therefore be sure, that their output contains true randomness.

Indeed, Chung et al. [CSW16] do emphasize that you do not have to use the CHSH game, but you can use one of a set what they call device-independent randomness amplification protocols. One can think of those as games that are based on violating the Bell inequality (such as CHSH or the earlier mentioned MDL game) with an additional verification, that the game is being played with a close to optimal quantum strategy. By use of this verification, one can verify that the output will be ε-close to uniform random. An other possible game is based on the Mermin inequality introduced by Bouda et al. [BPPP14] in their work. An interesting aspect of this game is that the quantum strategy to the game succeeds in 100% of cases.

Since we do not know which $Y_i = Y_i^*$, we simply perform the whole setup for every single Y_i. At least one $z_i = z_i^*$ is ε-uniform random. Therefore the XOR over all outputs $\bigoplus_i z_i = z$ will be ε-uniform random.

Some observations concerning this approach:

1. **Why is the quantum game needed if the input to the game is already ε-uniform random?**
   As mentioned in the introduction, there is no classical protocol which is able to amplify randomness of SV-sources. The same holds true for min-entropy sources. If we would not use the quantum game and would directly XOR the different Y_i, this would not necessarily lead to an ε-uniform output. The reason for that being the possible correlation between single Y_i. This correlation could lead to a non-uniform output when not using the quantum devices. The quantum devices are not really used to amplify the randomness in this protocol, but to make the single outputs independent and therefor eliminating the possibility of any kind of correlations.

2. **Why does at least one output Y_i have to be ε-uniform random?**
   By the properties of a seeded $(k, \varepsilon)-$extractor, it follows that for a randomly sampled i it holds true that $E(X, i)$ will be ε-close to a uniform random distribution. Since we look at the set of all possible i, it is clear, that at least one has to fulfil that property for our input distribution X. Indeed, it can be shown, that most Y_i fulfil this property [CSW14].

With this approach one is able to generate true random outputs when only given a min-entropy source as input. This approach uses exponential many devices. Bouda et al. [BPPP14] did show that the same thing can be accomplished by using a sophisticated hash function and a special game to only need a polynomial number of devices. The general idea is the same though.

4 Conclusions

In this paper we gave a broad introduction into the fields of randomness amplification and randomness extraction. We did mostly focus on the aspect of randomness extraction/amplification, since we think of this field as having more potential for possible improvements, i.e. concerning the number of devices which have to be used to implement the protocols. For randomness expansion, research has already provided protocols which can implement it by using a very low number of constant devices.

After a introduction of the basic notions, we did show an example of how SV sources can be amplified and afterwards showed how state of the art min-entropy amplification approaches work.

We did offer reference of the most recent and relevant papers concerning approaches to randomness extraction/amplification and a short comparison of their main properties.

The field is stil being heavily researched and one can be optimistic, that still more efficient approaches to randomness amplification will be found within the upcoming years.

References

[AFRV16] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs, 2016.

[BPPP14] Jan Bouda, Marcin Pawłowski, Matej Pivoluska, and Martin Plesch. Device-independent randomness extraction from an arbitrarily weak min-entropy source. *Physical Review A*, 90(3):032313, 2014.

[BRG+16] Fernando G. S. L. Brandão, Ravishankar Ramanathan, Andrzej Grudka, Karol Horodecki, Michał Horodecki, Paweł Horodecki, Tomasz Szarek, and Hanna Wojewódka. Realistic noise-tolerant randomness amplification using finite number of devices. *Nature communications*, 7:11345, 2016.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[CR12] Roger Colbeck and Renato Renner. Free randomness can be amplified. 2012.

[CSW14] Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu. Physical randomness extractors: Generating random numbers with minimal assumptions, 2014.

[CSW16] Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu. General randomness amplification with non-signaling security. 2016.

[CY14] Matthew Coudron and Henry Yuen. Infinite randomness expansion with a constant number of devices. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 427–436. ACM, 2014.

[DFR16] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation, 2016.

[GMdlT+13] Rodrigo Gallego, Lluís Masanes, Gonzalo de la Torre, Chirag Dhara, Leandro Aolita, and Antonio Acín. Full randomness from arbitrarily deterministic events. *Nature communications*, 4:2654, 2013.

[KAF17] Max Kessler and Rotem Arnon-Friedman. Device-independent randomness amplification and privatization, 2017.

[Neu27] J. von Neumann. Thermodynamik quantenmechanischer gesamtheiten. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1927:273–291, 1927.

[PRB+14] Gilles Pütz, Denis Rosset, Tomer Jack Barnea, Yeong-Cherng Liang, and Nicolas Gisin. Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality. *Phys. Rev. Lett.*, 113:190402, Nov 2014.

[Sha11] Ronen Shaltiel. An introduction to randomness extractors. In *International Colloquium on Automata, Languages, and Programming*, pages 21–41. Springer, 2011.

[Vad12] Salil Vadhan. Pseudorandomness, 2012.