Device-independent Randomness Amplification and Privatization*

(Abstract submitted to QCrypt 2017)

Max Kessler[1] and Rotem Arnon-Friedman[1]

[1] *Institute for Theoretical Physics, ETH-Zürich, CH-8093, Zürich, Switzerland*

Abstract

Randomness is an essential resource for many applications, and, most notably, for cryptography. In most applications perfect, and sometimes private, randomness is needed, while it is not even clear that such a resource exists. It is well known that the tools of classical computer science do not allow us to create perfect and secret randomness from a single weak public source. Quantum physics, on the other hand, allows for such a process, even in the most paranoid cryptographic sense termed "quantum device-independent cryptography". In this work we propose and prove the security of a new device-independent protocol that takes any single public Santha-Vazirani source as input and creates a secret close to uniform string in the presence of a quantum adversary.

Our work is the first to achieve randomness amplification with all the following properties: (1) amplification and "privatization" of a public Santha-Vazirani source with arbitrary bias (2) the use of a device with only two components (3) non-vanishing extraction rate and (4) maximal noise tolerance. In particular, this implies that our protocol is the first protocol that can possibly be implemented with reachable parameters. We are able to achieve these by combining three new tools: a particular family of Bell inequalities, a proof technique to lower bound entropy in the device-independent setting, and a special framework for quantum-proof multi-source extractors.

Motivation – creating private perfect randomness from public weak sources

Randomness is beneficial for many applications and essential for cryptography. Unfortunately, we will never be able to know for sure that randomness even exists; it might as well be that everything in nature is completely deterministic. Furthermore, even if we assume the existence of some sources of randomness in nature, it is not clear at all that there are sources of *perfect* randomness. Physical sources of randomness, such as radioactive decay or thermal noise, can be used to produce unpredictable bit strings, but those are usually partially biased and correlated bits. Even worse, how unpredictable these sources of randomness are depends on the knowledge of the observer regarding the physical system. For a person who can keep track of all microscopic degrees of freedom the outcomes can be completely predictable. The question addressed in this work is familiar:

> Can *perfect and secret* randomness be created from *weak and public* randomness in the presence of a quantum adversary?

By weak randomness we mean that the produced bits can be correlated and biased (though not completely deterministic). One such source, investigated in many works and of relevance for the current one, is the so called "Santha-Vazirani source", or SV-source, [1] — a source that produces a sequence of bits, where each bit has *some* randomness given all previous ones. Public randomness means that anyone can see the random string once it is produced. This is the case, for example, for the random numbers produced by the NIST randomness beacon; they are publicly available over the internet.

The tools of classical computer science do not allow us to create perfect and secret randomness from a single weak public source. Quantum physics, on the other hand, allows for such a process, even in the most paranoid cryptographic sense, using a "device-independent (DI) randomness amplification protocol". As already well know, this is done by exploiting the phenomena of quantum non-locality and Bell inequalities.

[*] Full version appears below.

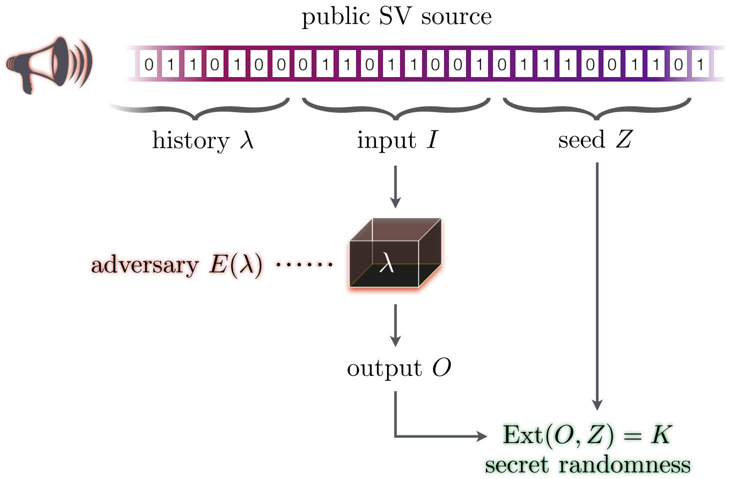

Figure 1: An illustration of the considered setting. We start with a public SV source and a device which was created by the adversary. The bits produced by the SV-source when running the protocol, I and Z, and the device can be correleated via the previous bits of the source, λ, and the adversary E.

Our contribution – the results and their importance

The first challenge when dealing with randomness amplification is to find a realistic and interesting setting to consider and devise a protocol that can be proven secure in that setting. Previous works considered different scenarios and have several crucial disadvantages.

The setting that we consider is illustrated in Figure 1. We start with an arbitrary, public, SV-source with bias $\mu \in (0, 0.5)$. We denote by λ all the bits produced before the adversary, Eve, prepares the device for the honest party, Alice. λ can also include any other piece of classical information from the past that might be of relevance to Eve. Eve then creates the device, denoted by the black box in the figure, depending on λ. She can keep quantum side information $E = E(\lambda)$ correlated with the device for herself. Once Alice holds the device she can use it together with additional bits produced by the source, I and Z in the figure, to create her final secret random string K. The SV-source can be controlled by an untrusted party but we assume that every bit, when produced, has some randomness conditioned on all side information. Mathematically, for the first bit of I, I_1, for example, we have $\frac{1}{2} - \mu \leq \Pr[I_1 = 0|\lambda] \leq \frac{1}{2} + \mu$.

In the above explained scenario it holds that, given the history λ and Eve's knowledge E, the device D and the sequence of bits $I \circ Z$ are independent. That is,[1] for $\mathrm{I}(\bullet : \bullet|\bullet)$ the conditional mutual information,

$$\mathrm{I}(D : I \circ Z|\lambda E) = 0 \; . \tag{1}$$

We remark that the considered scenario is realistic and relevant for actual applications. The chronological order of events is such that Eve can prepare the device depending only on past information (the history) but not on the bits which will be produced after delivering the device. This implies that all correlations between the following bits produced by the source and the device are due to past events and Eve's side information. Thus, Equation (1) holds. Previous works, e.g., [2–4], considered similar settings.

Our main contribution is stated in the following theorem:

Theorem 1 (Informal). *Given any public SV-source with bias $\mu \in (0, 0.5)$ there exists a DI randomness amplification protocol, requiring a two-component device, such that:*

1. *(Soundness) For any device D used to implement the protocol such that Equation* (1) *holds, either the protocol aborts with high probability or an ε-close to uniform (given the adversary's knowledge) string K is produced.*

[1] This should be understood on the intuitive level; the formal condition is given in the main text.

2. (Completeness) There exists an honest implementation of the device such that the protocol aborts with negligible probability when using this device, even in the presence of noise.

The security parameter ε depends on the bias of the source, μ, as well as the parameters of an extractor used in our protocol to create K. The formal statement is given in the main text.

Theorem 1 improves upon the prior state of the art in several significant aspects:

1. **Device requirement** – we only require that the device includes two components (the lowest possible). Previous works that considered a public weak source had to use, at the least, polynomial (in the number of bit used from the source) number of components, which is not realistic.

2. **Extraction rate (efficiency)** – we can extract a linear fraction of bits while maintaining cryptographic security level, compared to a vanishing extraction rate in previous works. Using an extractor with sufficiently good parameters, ε can be made exponentially small in the number of bits taken from the SV-source while extracting linear fraction of bits. Previous works could not achieve this, independently of the extractor used in the protocol.

3. **Robustness** – we are able to tolerate the maximal amount of noise, compared to low noise levels in previous works. The completeness statement holds for any amount of noise in the implementation which still results in a violation of the Bell inequality.

These properties imply that our protocol is the first protocol that can possibly be implemented.

Apart from randomness amplification, our protocol can also be used as a main building block for DI randomness expansion and key distribution using weak sources of randomness.

Theorem 1 *cannot* be derived by improving previously known techniques. We present a new proof, which can be of independent interest. One particular example is our investigation of a new type of Bell inequalities where we show, for the first time, that they can also be used in a cryptographic setting.

Main steps in the proof. Our proof uses three different tools which were developed recently and were not used before in the context of randomness amplification. We employ a family of Bell inequalities called "measurement dependent locality (MDL) inequalities" [5]. The special property about those inequalities is that they accommodate the dependency between the device and the side information for any bias of the source (in contrast to the CHSH inequality). The first part of our proof is devoted to deriving a relation between the violation of the MDL inequality and the amount of knowledge Eve can gain regarding the output in a single use of the device, quantified by the conditional von Neumann entropy. We then use the framework of DI security proofs developed in [6] to derive a lower bound on the total amount of the conditional smooth min-entropy of the raw data in the end of the protocol. Finally we show that, while "standard" extractors fail to work, the setting that we consider (as in Figure 1) implies that a newly developed model for quantum-proof multi-source extractors [7], termed the "Markov model", can be used to extract the private randomness in the raw data while using additional public bits from the source.

Previous works. Randomness amplification was first considered in [2], where a "proof of concept" was given. Following that, [3] improved by considering a protocol that can accommodate arbitrary bias of the SV-source and tolerate some noise. They focused on non-signalling adversaries. Unfortunately, the protocol required the use of a polynomial number of devices, which is unrealistic in any implementation.

In [4, 8] a protocol using a constant number of devices was constructed. However, for the security proof to hold the SV-source must be private, i.e., no information about the bits produced by the source can leak to the adversary at any point (also not after the end of the protocol).

In two more recent works [9, 10] a protocol that can amplify a public min-entropy source and allows for possibly stronger correlations between the device and the source was suggested and its security was proven. However, their proof technique leads to a polynomial number of devices in [9] and exponential in [10]. Furthermore, in both works the security parameter is inverse polynomial in the number of bits used from the source, the efficiency of the protocols vanishes, and the amount of tolerated noise is low.

References

[1] M. Santha and U. V. Vazirani. Generating quasi-random sequences from slightly-random sources. In *25th Annual Symposium on Foundations of Computer Science, 1984.*, pages 434–440, Oct 1984.

[2] R. Colbeck and R. Renner. Free randomness can be amplified. *Nat Phys*, 8(6):450–453, Jun 2012.

[3] 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 EP –, Oct 2013. Article.

[4] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, and H. Wojewódka. Realistic noise-tolerant randomness amplification using finite number of devices. *Nature communications*, 7, 2016.

[5] G. Pütz, D. Rosset, T. J. Barnea, Y. C. Liang, and N. Gisin. Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality. *Phys. Rev. Lett.*, 113:190402, Nov 2014.

[6] R. Arnon-Friedman, R. Renner, and T. Vidick. Simple and tight device-independent security proofs. *ArXiv e-prints*, Jul 2016.

[7] R. Arnon-Friedman, C. Portmann, and V. B. Scholz. Quantum-Proof Multi-Source Randomness Extractors in the Markov Model. In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, volume 61 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:34, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[8] R. Ramanathan, F. G. S. L. Brandão, K Horodecki, M. Horodecki, P. Horodecki, and H. Wojewódka. Randomness amplification against no-signaling adversaries using two devices. *arXiv preprint arXiv:1504.06313*, 2015.

[9] K.-M. Chung, Y. Shi, and X. Wu. Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions. *ArXiv e-prints*, Feb 2014.

[10] K.-M. Chung, Y. Shi, and X. Wu. General randomness amplification with non-signaling security.