Randomness amplification against no-signaling adversaries using two devices

Ravishankar Ramanathan,[1,2] Fernando G.S.L. Brandão,[3,4] Karol Horodecki,[1,5]
Michał Horodecki,[1,2] Paweł Horodecki,[1,6] and Hanna Wojewódka[1,2,7]

[1] *National Quantum Information Center of Gdańsk, 81-824 Sopot, Poland*
[2] *Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*
[3] *Quantum Architectures and Computations Group, Microsoft Research, Redmond, WA (USA)*
[4] *Department of Computer Science, University College London*
[5] *Institute of Informatics, University of Gdańsk, 80-952 Gdańsk, Poland*
[6] *Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-233 Gdańsk, Poland*
[7] *Institute of Mathematics, University of Gdańsk, 80-952 Gdańsk, Poland*

(Dated: April 27, 2015)

Recently the first physically realistic protocol amplifying the randomness of Santha-Vazirani sources using a finite number of no-signaling devices and with a constant rate of noise has been proposed, however there still remained the open question whether this can be accomplished under the minimal conditions necessary for the task. Namely, is it possible to achieve randomness amplification using only two no-signaling devices and in a situation where the violation of a Bell inequality implies only an upper bound for some outcome probability for some setting combination? Here, we solve this problem and present the first device-independent protocol for the task of randomness amplification of Santha-Vazirani sources using a device consisting of only *two* non-signaling components. We show that the protocol can amplify any such source that is not fully deterministic into a totally random source while tolerating a constant noise rate and prove the security of the protocol against general no-signaling adversaries. The minimum requirement for a device-independent Bell inequality based protocol for obtaining randomness against no-signaling attacks is that *every* no-signaling box that obtains the observed Bell violation has the conditional probability $P(\mathbf{x}|\mathbf{u})$ of at least a single input-output pair $(\mathbf{u}, \mathbf{x})$ bounded from above. We show how one can construct protocols for randomness amplification in this minimalistic scenario.

INTRODUCTION

Random number generators are ubiquitous, finding applications in varied domains such as statistical sampling, computer simulations and gambling scenarios. While certain physical phenomena such as radioactive decay or thermal noise have high natural entropy, there are also many computational algorithms that can produce sequences of apparently random bits. In many cryptographic tasks however, it may be necessary to have trustworthy sources of randomness. As such, developing so-called device-independent protocols for generating random bits is of paramount importance.

We consider the task of randomness amplification, that is to convert a source of partially random bits to one of fully random bits. The paradigmatic model of a source of randomness is the Santha-Vazirani (SV) source [1], a model of a biased coin where the individual coin tosses are not independent but that rather the bits Y_i produced by the source obey

$$\frac{1}{2} - \varepsilon \leq P(Y_i = 0 | Y_{i-1}, \ldots, Y_1, W) \leq \frac{1}{2} + \varepsilon \qquad (1)$$

for some $0 \leq \varepsilon < \frac{1}{2}$. Here ε is a parameter describing the reliability of the source of randomness, the task being to convert a source with $\varepsilon < \frac{1}{2}$ into one with $\varepsilon \to 0$. The random variable W denotes a knowledge of a potential adversary. Interestingly, this task is known to be impossible with classical resources, a single SV source cannot be amplified [1].

In [3], the non-local correlations in quantum mechanics were shown to provide an advantage in the task of amplifying an SV source. A device-independent protocol for generating truly random bits was demonstrated starting from a certain critical value of $\varepsilon (\approx 0.06)$, where the device-independence refers to the fact that one need not trust the internal workings of the device. An improvement was made in [5] where using an arbitrarily large number of spatially separated devices, it was shown that one could amplify randomness starting from any initial $\varepsilon < \frac{1}{2}$. In [6], we demonstrated a device-independent protocol which used a constant number of space-like separated components and amplified sources of arbitrary initial parameter $\varepsilon < \frac{1}{2}$ while at the same time tolerating a constant amount of noise in its implementation.

MOTIVATION - THE CHALLENGE OF MINIMAL ASSUMPTIONS

For fundamental as well as practical reasons, it is vitally important to minimize the number of spatially separated components used in a protocol. As such, devising a protocol with the minimum possible number of components (namely, two space-like separated ones for a protocol based on a Bell test) while at the same time, allowing for robustness to errors in its implementation is crucial. Note that since there are examples in quantum information where multi-partite protocols are easy to formulate while bipartite ones are difficult or even not known to exist (such as the bipartite NPT bound entanglement problem) the question about a two-device protocol was not just technical.

A necessary condition for a device-independent Bell-based protocol for obtaining randomness against no-signaling attacks is that for some input $\mathbf{u}^* \in \mathbf{U}$, output $\mathbf{x}^* \in \mathbf{X}$ and a constant $c < 1$, *every* no-signaling box $\{P(\mathbf{x}|\mathbf{u})\}$ that obtains the observed Bell violation has $P(\mathbf{x} = \mathbf{x}^*|\mathbf{u} = \mathbf{u}^*) \leq c$. i.e.,

$$\begin{aligned} \exists(\mathbf{x}^*, \mathbf{u}^*) \;\; \text{s.t.} \quad & \forall\{P(\mathbf{x}|\mathbf{u})\} \;\; \text{with} \;\; \mathbf{B}.\{P(\mathbf{x}|\mathbf{u})\} = 0 \\ & P(\mathbf{x} = \mathbf{x}^*|\mathbf{u} = \mathbf{u}^*) \leq c < 1, \end{aligned} \tag{2}$$

where $\mathbf{B}.\{P(\mathbf{x}|\mathbf{u})\} = 0$ denotes that the box achieves algebraic violation of the inequality. Note that while the Bell inequality violation guarantees Eq.(2) for some $\mathbf{x}^*, \mathbf{u}^*$ for each NS box, here the requirement is for a strictly bounded common entry $P(\mathbf{x} = \mathbf{x}^*|\mathbf{u} = \mathbf{u}^*)$ for all boxes leading to the observed Bell violation. It is straightforward to see that if Eq. (2) is not met, then no device-independent protocol for obtaining randomness can be built out of the observed non-local correlations. If in addition to the necessary condition in Eq. (2), we also had for the same input-output pair $(\mathbf{u}^*, \mathbf{x}^*)$ that

$$\tilde{c} \leq P(\mathbf{x} = \mathbf{x}^*|\mathbf{u} = \mathbf{u}^*) \tag{3}$$

for some constant $\tilde{c} > 0$, then clearly one can construct a device-independent protocol to extract randomness in this scenario. Here, we present a fully device-independent protocol that allows to amplify the randomness of any ε-SV source under the minimal necessary condition in Eq. (2) by observing that it is enough that the lower bound presented above holds for *some* box Q, which has quantum realization. A novel element of the protocol is an additional test (to the usual test for violation of a Bell inequality) that the honest parties perform, akin to partial tomography of the boxes, that ensures that additionally Eq.(3) is also met for a sufficient number of runs, demanding thereby that their box behave like a quantum box Q. The protocol uses a device consisting of only two no-signaling components and tolerates a constant error rate, we present a proof of security of the protocol against general no-signaling adversaries (not limited to the use of quantum boxes).

THE SCENARIO AND ASSUMPTIONS

We work in the following scenario: The honest parties, Alice and Bob has access each a device with two components one for each of them. A adversary Eve holds her own device. The honest parties has also access to the Santha-Vazirani source SV.

In this scenario the non-signaling assumption is important, that is that no component (or device) can change statistics of some component (or device). E.g. Eve, in no run of her device can change statistics of Alice's and Bob's components by changing her inputs. We will elaborate now more specifically about all assumptions (For detiles of them, under which we prove the security of the protocol see the Supplemental Material of [10]).

Apart from the above mentioned non-signaling assumption, there is also a time-ordered no-signaling structure assumed on different runs of a single component, the outputs in any run may depend on the previous inputs within the component but not on future inputs. Moreover, we also assume that the structure of the box is fixed independently of the SV source, in other words that the box is an unknown and arbitrary input-output channel that is independent of the SV source. It is worth noting that no randomness may be extracted under these assumptions in a classical setting, while the violation of the Bell inequality by certain quantum boxes allows to amplify randomness in a device-independent setting.

Our main result is a two-party protocol to amplify the randomness of SV sources. Formally we prove the following:

Theorem 1. *For every $\varepsilon < \frac{1}{2}$, there is a protocol using an ε-SV source and two non-signaling devices with the following properties:*

- *Using the devices $\mathrm{poly}(n, 1/\delta)$ times, the protocol either aborts or produces n bits which are δ-close to uniform and independent of any side information.*
- *Local measurements on many copies of a two-party entangled state, with $\mathrm{poly}(1-2\varepsilon)$ error rate, give rise to devices that do not abort the protocol with probability larger than $1 - 2^{-\Omega(n)}$.*

The protocol for the task of randomness amplification from Santha-Vazirani sources has the following structure. The two honest parties Alice and Bob use bits from the ε-SV source to choose the inputs to their no-signaling boxes in multiple runs of a Bell test and obtain their respective outputs. They check for the violation of a Bell inequality and abort the protocol if the test condition is not met. The novel part of the protocol is a subsequent test that the honest parties perform that ensures when passed the presence of sufficient number of runs performed with boxes that have randomness in their outputs. If both tests in the protocol are passed, the parties apply a randomness extractor to the output bits and some further bits taken from the SV source. The output bits of the extractor constitute the output of the protocol, which we show to be close to being fully random and uncorrelated from any no-signaling adversary.

OUTLINE OF THE PROOF

The proof of security of the protocol follows along similar lines to the proof we presented in [6] but with some crucial differences which we now elaborate. As in previous works on randomness amplification [3, 5, 6], the idea of the protocol is to use the ε-SV source to choose the measurement settings in a Bell test. After verifying that the expected violation of the Bell inequality is obtained and conditioned upon another test being passed (the requirement of a new test in our protocol is explained below), the measurement outcomes are combined along with further bits from the SV source using a randomness extractor [2, 4] to yield the final random bits S. The devices may have been prepared by a supra-quantum adversary Eve who may have used arbitrary no-signaling resources for the task. Eve could also have had access to the SV source and therefore could have a classical random variable correlated to the bits from the SV source as long as the constraint in Eq.(1) is obeyed.

Let us first recall that for the task of randomness amplification of SV sources, one needs Bell inequalities where quantum mechanics can achieve the maximal no-signaling value of the inequality [3], failing this condition for sufficiently small ε, the observed correlations may be faked with classical deterministic boxes. However, Bell inequalities with this property are not sufficient, this is exemplified by the tripartite Mermin inequality [11] as noted in [3]. This inequality is algebraically violated in quantum theory using a GHZ state, however for any function of the measurement outcomes one can find no-signaling boxes which achieve the maximum violation of the inequality and for which this particular function is deterministic thereby providing an attack for Eve to predict with certainty the final output bit. While [5] and [6] considered Bell inequalities with more parties, the problem of finding two-party algebraically violated Bell inequalities (alternatively known as pseudo-telepathy games) with the property of randomness for some function of the measurement outcomes was open. Unfortunately, none of the bipartite Bell inequalities tested so far have the property that *all* no-signaling boxes which maximally violate the inequality have randomness for some function of the measurement outcomes $f(\mathbf{x})$ for some input $\mathbf{u}$ (the same for all boxes) in the sense that for all such boxes

$$\frac{1}{2} - \gamma \leq P(f(\mathbf{x})|\mathbf{u}) \leq \frac{1}{2} + \gamma \tag{4}$$

for some $0 < \gamma < \frac{1}{2}$. We call Bell inequalities with property (4) as guaranteeing *strong randomness*.

The Bell inequality we consider for the task of randomness amplification is a modified version of the bipartite inequality based on Kochen-Specker games in [7]. The inequality involves two parties Alice and Bob, each making one of nine possible measurements and obtaining one of four possible outcomes and is explained further in the Supplemental Material of [10]. The box Q which the honest provider of device can produce to create it is obtained by measuring observables from this Bell inequality on a two-qubit maxially entangled state. Even though it does not guarantee the strong randomness in Eq.(4) for any function of the measurement outcomes $f(\mathbf{x})$ for any input $\mathbf{u}$, it has the redeeming feature of giving *weak randomness* in the following sense. For all no-signaling boxes which algebraically violate the inequality, there exists one measurement setting $\mathbf{u}^*$ and one outcome $\mathbf{x}^*$ for this setting such that

$$\begin{aligned} &0 \leq P(\mathbf{x} = \mathbf{x}^*|\mathbf{u} = \mathbf{u}^*) \leq \frac{1}{2} + \gamma \\ &\forall \{P(\mathbf{x}|\mathbf{u})\} \quad \text{s.t} \quad \mathbf{B} \cdot \{P(\mathbf{x}|\mathbf{u})\} = 0 \end{aligned} \tag{5}$$

for some $0 < \gamma < \frac{1}{2}$. The above fact is checked by use of a standard linear programming technique elaborated in the Supplemental Material of [10].

We propose a novel technique in the form of a second test akin to partial tomography subsequent to the Bell test which allows us to extract randomness in this minimal scenario of weak randomness. This second test simply checks for the number of times the output $\mathbf{x}^*$ appears when the measurement setting $\mathbf{u}^*$ is chosen, the analysis of this test is done as for the Bell test by an application of the Azuma-Hoeffding inequality.

Clearly to do the above mentioned tomography, one needs enough number of $\mathbf{u}^*$ settings to appear when chosen from SV source. Where SV an i.i.d. distribution say with probability p of $\mathbf{u}^*$, by Chernoff bound, we would be sure to expect np times in n runs this measurement to occure with probability exponentially close to 1. Now, despite the SV source is not an i.i.d distribution, it is pretty random, in a sense that it obeys the so called Generalized Chernoff bound [8, 9], that ensures that with high probability when the inputs are chosen with such a source, the measurement setting $\mathbf{u}^*$ appears in a linear fraction of the runs. Thus, conditioned on both tests in the protocol being passed (which happens with large probability with the use of the SV source and good quantum boxes by the honest parties), we obtain that with high probability over the input, the output is a source of linear min-entropy.

This allows us to use known results on randomness extractors for two independent sources of linear min-entropy [2], namely one given by the outputs of the measurement and the other given by the SV source. As shown in [6], one can use extractors secure against classical side information even in the scenario of general no-signaling adversaries by accepting a loss in the rate of the protocol, i.e., by increasing the output error. The randomness extractor used in the protocol is a non explicit extractor from [2]. It readily follows from the results in [6] that one can also get a protocol with an explicit extractor using a device with three no-signaling components with an additional de-Finetti theorem for no-signaling devices with subsystems chosen using a Santha-Vazirani source (see Protocol II with the use of Lemma 13 in [6]). Counting the devices components, with Protocol II, we obtain robust randmoness amplification with 2 devices (4 comoponents) with explicit extractor, and with Protocol I, we achieve the same with *single device* (2 components) with non-expilicit extractor.

[1] M. Santha and U. V. Vazirani. Generating Quasi-Random Sequences from Slightly-Random Sources. Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS'84), 434 (1984).

[2] B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. SIAM Journal on Computing, 17(2): 230 (1988).

[3] R. Colbeck and R. Renner. Free randomness can be amplified. Nature Physics **8**, 450 (2012).

[4] Xin-Li. Extractors for a constant number of independent sources with polylogarithmic min-entropy. (to appear in FOCS 2013).

[5] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita and A. Acin. Full randomness from arbitrarily deterministic events. arXiv:1210.6514 (2012).

[6] F. G. S. L. Brandao, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek and H. Wojewodka. Robust Device-Independent Randomness Amplification with Few Devices. arXiv: 1310.4544 (2013).

[7] L. Aolita, R. Gallego, A. Acín, A. Chiuri, G. Vallone, P. Mataloni and A. Cabello, Phys. Rev. A **85**, 032107 (2012).

[8] A. Panconesi and A. Srinivasan. Randomized distributed edge coloring via an extension of the Chernoff-Hoeffding bounds. SIAM Journal on Computing **26**, 350-368 (1997).

[9] R. Impagliazzo and V. Kabanets. APPROX/RANDOM'10 Proceedings of the 13th international conference on Approximation, and the International conference on Randomization, and combinatorial optimization: algorithms and techniques, 617-631 (2010).

[10] Randomness amplification against no-signaling adversaries using two devices arXiv:1504.06313 Ravishankar Ramanathan, Fernando G.S.L. Brandao, Karol Horodecki, Michal Horodecki, Pawel Horodecki and Hanna Wojewodka

[11] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).