Amplifying the randomness of weak sources correlated with devices

H. Wojewódka (Faculty of Mathematics, Physics & Informatics, University of Gdańsk)
F.G.S.L. Brandão (Quantum Architectures & Computation Group, Microsoft Research, Redmond, Department of Computer Science, University College London)
A. Grudka (Faculty of Physics, Adam Mickiewicz University, Poznań)
K. Horodecki (Faculty of Mathematics, Physics & Informatics, University of Gdańsk)
M. Horodecki (Faculty of Mathematics, Physics & Informatics, University of Gdańsk)
P. Horodecki (Faculty of Applied Physics & Mathematics, Gdańsk University of Technology)
M. Pawłowski (Faculty of Mathematics, Physics & Informatics, University of Gdańsk)
R. Ramanathan (Faculty of Mathematics, Physics & Informatics, University of Gdańsk)

The problem of device-independent randomness amplification against no-signaling adversaries has so far been studied under the assumption that the weak source of randomness is uncorrelated with the (quantum) devices used in the amplification procedure. Here we propose a protocol for randomness amplification against a no-signaling adversary, that is based on a weaker assumption. As a weak source of randomness we use a Santha-Vazirani (SV) source. We introduce an SV-like condition for devices, namely that any string of SV source bits remains weakly random conditioned upon any other bit string from the same SV source and the outputs obtained when this further string is input into the devices. Assuming this condition, we show that a quantum device using a singlet state to violate the chained Bell inequalities leads to full randomness in the asymptotic scenario of a large number of settings, for a restricted set of SV sources (with $0 \leq \varepsilon < \frac{(2^{(1/12)}-1)}{2(2^{(1/12)}+1)} \approx 0.0144$).

Although we observe that amplifying the randomness of weak sources arbitrarily correlated with devices is not possible without further assumptions, we do not rule out the possibility that the assumptions proposed in our paper cannot be even more relaxed. We leave the case of a yet more general attack on the amplification protocol as an interesting open problem.

Introduction. In many applications, and in particular in quantum cryptography, free randomness is desired due to the fact that a wide range of results is based on it. In practice, however, random sources are rarely private and usually only weak sources of randomness are available. That is why the problem of randomness amplification became useful and worth investigating. Overall, the idea is to use inputs from a partially random source and obtain perfectly random output bits.

Although amplifying the randomness of a single weak source is unattainable in classical information theory (see [1] for proof), it becomes possible, if the no-signaling principle is assumed and quantum-mechanical correlations (revealed operationally through the violation of Bell inequalities) are used. In this paper we mainly focus on the chained Bell inequality (see [2]), which has already been used in the research on randomness and privacy amplification (see [3], [4] or [5]).

As a weak source to be amplified, we consider an ε-SV source (named for Santha and Vazirani [1]), where ε is a parameter which indicates how far we are from full randomness. An ε-SV source is given by a probability distribution $P(\varphi_1, \ldots, \varphi_n, \ldots)$ over bit strings such that

$$\begin{aligned} &(0.5-\varepsilon) \leq P(\varphi_1|e) \leq (0.5+\varepsilon), \\ &(0.5-\varepsilon) \leq P(\varphi_{i+1}|\varphi_1, \ldots, \varphi_i, e) \leq (0.5+\varepsilon) \qquad \text{for every } 1 \leq i \leq n, \end{aligned} \tag{1}$$

where the e represents an arbitrary random variable prior to φ_1, which can influence $\varphi_1, \ldots, \varphi_n, \ldots$. Note that, when $\varepsilon = 0$, bits are fully random, while they are fully deterministic, when $\varepsilon = 0.5$.

In our study we use a family of probability distributions, usually called a box, denoted by $P(O|I)$, where I and O are random variables describing the vectors of inputs and outputs, respectively. To amplify randomness we need boxes which satisfy the no-signaling condition. In the simplest case, when there are only two parties: Alice and Bob, the no-signaling assumption is that

$$\begin{aligned} \textstyle\sum_y P\left(O=(x,y)|I=(u,v)\right) &= \textstyle\sum_y P\left(O=(x,y)|I=(u,v')\right) \quad \text{for every } u,v,v',x, \\ \textstyle\sum_x P\left(O=(x,y)|I=(u,v)\right) &= \textstyle\sum_x P\left(O=(x,y)|I=(u',v)\right) \quad \text{for every } u,u',v,y. \end{aligned} \tag{2}$$

Research background. In the research on randomness amplification, the paper of Colbeck and Renner [3] is certainly crucial. It is also a starting point for our idea. The authors consider the bipartite scenario of the chained Bell inequality and prove that, under certain assumptions, it is possible to amplify randomness of ε-SV sources, provided $\varepsilon < \left(\sqrt{2}-1\right)^2/2 \approx 0.086$.

Further results were obtained in [6], [7], [8], [4], [9] etc. The problem has been considered from different points of view and a lot of obstacles, such as the requirement of an infinite number of devices or no tolerance for noise, have already been overcome. However, relaxing the assumption about independence between a source and a device has not yet been widely studied and even not studied at all against a no-signaling adversary.

So far, only Chung et al. [8] have tried to weaken the independence assumption, however they approach the problem in a quantum formalism. We propose to consider randomness amplification against a no-signaling adversary, assuming condition which is weaker than independence between a weak source of randomness and a device.

Our results. The aim of our research was to make randomness amplification even more realistic and secure. We have relaxed the assumption that the weak source of randomness and a device used in the amplification precedure (against a no-signaling adversary) are independent. We have reconsidered the original protocol of Colbeck and Renner [3] on randomness amplification, using an SV source, and proven that, under the SV-like condition for devices, randomness amplification is still possible in the asymptotic scenario of a large number of settings, for a restricted set of SV sources (with $0 \le \varepsilon < \frac{(2^{(1/12)}-1)}{2(2^{(1/12)}+1)} \approx 0.0144$).

We believe that these results give a new insight into the problem and, due to the clarity of assumptions, will also be significant in the more general task of obtaining secure key bits in cryptography.

Motivation and toy example. To justify the importance of our results, we now exemplify a possible attack that utilizes correlations between a weak source and device in the simplest scenario of boxes with binary inputs and outputs.

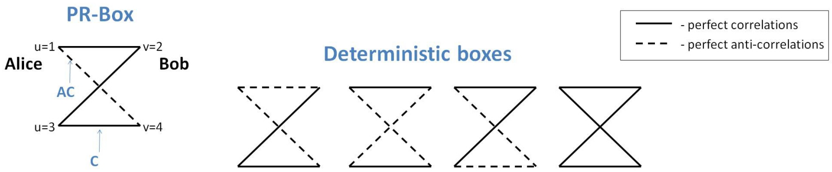

Fig. 1. Examples of bipartite boxes with binary inputs and outputs denoted by graphs. The Popescu-Rohrlich box (on the left) and local (deterministic) boxes (on the right).

Even though these boxes do not constitute a resource for randomness amplification, the attack can already be described in terms of these.

Imagine that Alice and Bob share a box L which is a mixture of local boxes L_{ij}, where $i = 1, 3$ label Alice's inputs and $j = 2, 4$ label Bob's inputs:

$$L = \frac{1}{4}\left(L_{12} + L_{32} + L_{34} + L_{14}\right). \tag{3}$$

(See Fig. 1 where the PR box and local deterministic boxes are presented and Fig. 2, where the boxes L_{ij} are given explicitly). The bits from an ε-SV source are perfectly correlated to local boxes as

$$P\left(L_{ij} \mid S = (k,l)\right) = \delta_{ik;jl} = \begin{cases} 1, & i = k \;\&\; j = l, \\ 0, & \text{otherwise}, \end{cases} \tag{4}$$

where S is the random variable describing bits from an ε-SV source.

In the protocols proposed so far (such as the Colbeck and Renner protocol [3]) it is demanded that I and S are perfectly correlated, i.e.

$$P(I = (u, v) \mid S = (k, l)) = \delta_{uk;vl} = \begin{cases} 1, & u = k \;\&\; v = l, \\ 0, & \text{otherwise}, \end{cases} \tag{5}$$

which means that bits from the ε-SV source are used as inputs to the box. All the correlations are indicated in Fig. 2.

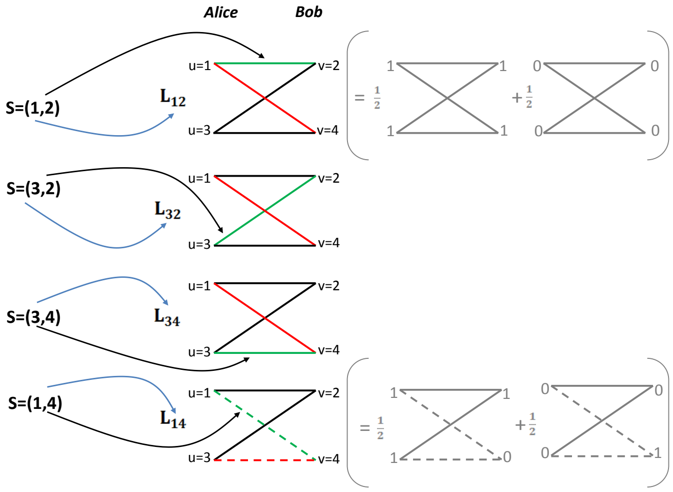

Fig. 2. Bits from an ε-SV source (on the left) are perfectly correlated with local boxes supplied to honest parties (on the right). Correlations decribed by Eq. (4) are indicated by blue arrows. Additionally, bits from an ε-SV source are perfectly correlated with the inputs to boxes (see Eq. (5)), which is indicated by black arrows. These correlations allow only for measuring green edges and hence Alice and Bob always observe an optimal Bell value. If red edges could be measured, the locality of boxes would be detected.

Now, we see that although the box L is manifestly local, the honest parties do not detect it in the protocols proposed so far. Indeed, correlations (4) and (5) imply that input $I = (k, l)$ may only be introduced to box L_{kl}, adapted exactly to this input, so that L mimics the action of the PR box on any input. On the other hand, if there was independence between the ε-SV source and the boxes, the parties would recognize that the object L is local.

Justification for our assumptions. To conclude, this toy example clearly illustrates that perfect correlation of inputs and devices excludes any possibility of randomness amplification. To circumvent this type of attack, we introduce the SV-condition for boxes, which is the weakest assumption (thus far) that still allows for randomness amplification.

References

[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), 434–440 (1984).

[2] S.L. Braunstein & C.M. Caves, *Wringing out better Bell inequalities*, Annals of Physics 202, 22 (1990).

[3] R. Colbeck and R. Renner, *Free randomness can be amplified*, Nature Physics 8, 450-454 (2012).

[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, Article number: 11345 (2016).

[5] R. Arnon-Friedman and A. Ta-Shma, *Limits of privacy amplification against non-signalling memory attacks*, Phys. Rev. A 86, 062333 (2012).

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

[7] P. Mironowicz, R. Gallego and M. Pawłowski, *Amplification of arbitrarily weak randomness*, Phys. Rev. A 91, 032317 (2015).

[8] K.M. Chung, Y. Shi and X. Wu, *Physical randomness extractors: generating random numbers with minimal assumptions*, Preprint at http://arxiv.org/abs/1402.4797 (2014).

[9] 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*, Preprint at http://arxiv.org/abs/1504.06313 (2015).