Randomness amplification using independent devices arbitrarily correlated with the Santha-Vasirani source [1]

K. Horodecki,[1] M. Horodecki,[2] P. Horodecki,[3,4] R. Ramanathan,[5] M. Stankiewicz,[4] and H. Wojewódka[6]

[1] *Institute of Informatics and National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-309 Gdańsk, Poland*

[2] *Institute of Theoretical Physics and Astrophysics and National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-309 Gdańsk, Poland*

[3] *Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, 80-233 Gdańsk, Poland*

[4] *National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-309 Gdańsk, Poland*

[5] *Laboratoire d'Information Quantique, Université Libre de Bruxelles, Belgium*

[6] *Institute of Mathematics, Faculty of Mathematics, Physics and Chemistry, University of Silesia, 40-007 Katowice, Poland*

The Randomness is very important not only in understanding of the fundamental laws of physics but also in many applications. For example there is no unconditionally secure cryptography without unconditionally secure randomness.

Problem if it is possible to amplify a weak source of randomness in order to get the perfect random bit was already asked by Santha and Vazirani in 1986 [2]. They formalized notion of the weak randomness source, now known as the Santha-Vazirani (SV) source, and proved that there is no universal deterministic extractor that can achieve even slight amplification.

In 2012 breakthrough result, Colbeck and Renner [3] suggested a device independent quantum randomness amplification protocol. In the protocol quantum device consists of sequence of bipartite boxes is used. To each box the honest parties inputs part of bits from the SV source. They compare results and check if there are compatible with the chain Bell inequality. At the end they use some more bits from SV source to decide from which box the final output bit of the protocol is taken. Unfortunately in their proof there are many independence assumptions between the quantum device and the SV source. Furthermore the proof work only for quite strong SV sources.

Up to now there have been many publications [4–14] that tried to weaken the above assumptions or improve the protocol in various ways for example by increasing rate or accept some level of noise.

In our recent result [1] we prove that the protocol of Colbeck and Renner is still secure when we allow arbitrary correlations between the source and the device. To be specific we allow the boxes to be correlated with the source parts that are used as inputs but also let the whole device to be correlated with the SV source bits which are used to choose the final box.

Although there are some problems in defining the composability for device independent protocols pointed out by Barrett et al. [15] and Arnon-Friedman et al. [16], we argue that our approach is in fact composably secure when the SV source is private and we do not reuse the devices.

The main method used in our proof, beside SV-condition for boxes from our previous paper [13], is notion of a independent tester. We assume that there is a tester who has access to the true randomness. According to the SV-condition for boxes, the SV source should remain SV source even given the outputs of any device to which the tester sets her inputs. The tester, basing on average number of observed contradictions, could potentially guess the number of the box that outputs the final bit. If the honest parties accept the protocol then we know that the number of the boxes close to classical called "bad" boxes is small. In that case if the adversary try to correlate strongly with only bad boxes then the tester would guess part of the weak source better than it is allowed by the SV condition. Therefore the danger correlations are limited, what means that in case of the asymptotic limit the true random bit can be obtained from the protocol.

It is worth mentioning that recent result by Chung et al. [12] proves that randomness amplification is possible with arbitrary correlations using a min-entropy source that is in fact weaker than the SV source. Although their result is highly important for understanding non deterministic nature of the world it is unpractical in applications because of doubly exponential complexity in terms of the number of devices used by the protocol. On the other hand our approach is based on polynomial protocol by Colbeck and Renner [3]. Furthermore we also present modification of the protocol based on the idea by Augusiak et al. [17] which gives as even lower complexity.

To summarize we proved that randomness amplification is possible in the framework where only unobvious assumption is that the boxes are independent. The question if we can omit that assumption remains open and it is topic of

ongoing work.

---

[1] K. Horodecki, M. Horodecki, P. Horodecki, R. Ramanathan, M. Stankiewicz, and H. Wojewódka, "Randomness amplification using independent devices arbitrarily correlated with the Santha-Vasirani source," (2017), unpublished.
[2] M. Santha and U. V. Vazirani, Journal of Computer and System Sciences **33**, 75 (1986).
[3] R. Colbeck and R. Renner, Nature Physics **8**, 450 (2012).
[4] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín, Nature Communications **4**, 2654 (2013).
[5] R. Ramanathan, F. G. S. L. Brandão, A. Grudka, K. Horodecki, M. Horodecki, and P. Horodecki, "Robust Device Independent Randomness Amplification," (2013), arXiv:1308.4635 [quant-ph].
[6] J. Bouda, M. Pawłowski, M. Pivoluska, and M. Plesch, Physical Review A **90**, 032313 (2014).
[7] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, and R. Ramanathan, Physical Review A **90**, 032322 (2014).
[8] K.-M. Chung, Y. Shi, and X. Wu, "Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions," (2014), arXiv:1402.4797 [quant-ph].
[9] P. Mironowicz, R. Gallego, and M. Pawłowski, Physical Review A **91**, 032317 (2015).
[10] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, and H. Wojewódka, Nature Communications **7**, 11345 (2016).
[11] R. Ramanathan, F. G. S. L. Brandão, K. Horodecki, M. Horodecki, P. Horodecki, and H. Wojewódka, Physical Review Letters **117**, 230501 (2016).
[12] K.-M. Chung, Y. Shi, and X. Wu, "General Randomness Amplification with Non-signaling Security," (2016), unpublished.
[13] H. Wojewódka, F. G. S. L. Brandão, A. Grudka, M. Horodecki, K. Horodecki, P. Horodecki, M. Pawłowski, R. Ramanathan, and M. Stankiewicz, "Amplifying the randomness of weak sources correlated with devices," (2016), arXiv:1601.06455 [quant-ph].
[14] M. Kessler and R. Arnon-Friedman, "Device-independent Randomness Amplification and Privatization," (2017), arXiv:1705.04148 [quant-ph].
[15] J. Barrett, R. Colbeck, and A. Kent, Physical Review Letters **110** (2013), 10.1103/physrevlett.110.010503.
[16] R. Arnon-Friedman, R. Renner, and T. Vidick, "Simple and tight device-independent security proofs," (2016), arXiv:1607.01797 [quant-ph].
[17] R. Augusiak, M. Demianowicz, M. Pawłowski, J. Tura, and A. Acín, Physical Review A **90**, 052323 (2014).