Randomness Amplification under Minimal Fundamental Assumptions on the Devices

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

[1]*Institute of Theoretical Physics and Astrophysics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-308 Gdańsk, Poland*

[2]*Quantum Architectures and Computation Group, Microsoft Research, Redmond, Washington 98052, USA*

[3]*Department of Computer Science, University College London, WC1E 6BT London, United Kingdom*

[4]*Institute of Informatics, National Quantum Information Centre, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, 80-308 Gdańsk, Poland*

[5]*Faculty of Applied Physics and Mathematics, National Quantum Information Center, Gdańsk University of Technology, 80-233 Gdańsk, Poland*

[6]*Institute of Mathematics, Faculty of Mathematics, Physics and Chemistry, University of Silesia, Bankowa 14, 40-007 Katowice, Poland*

(Received 22 June 2016; published 30 November 2016)

Recently, the physically realistic protocol amplifying the randomness of Santha-Vazirani sources producing cryptographically secure random bits was proposed; however, for reasons of practical relevance, the crucial question remained open regarding 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 components and in a situation where the violation of a Bell inequality only guarantees that some outcomes of the device for specific inputs exhibit randomness? Here, we solve this question and present a device-independent protocol for randomness amplification of Santha-Vazirani sources using a device consisting of two nonsignaling components. We show that the protocol can amplify any such source that is not fully deterministic into a fully random source while tolerating a constant noise rate and prove the composable security of the protocol against general no-signaling adversaries. Our main innovation is the proof that even the partial randomness certified by the two-party Bell test [a single input-output pair $(\mathbf{u}^*, \mathbf{x}^*)$ for which the conditional probability $P(\mathbf{x}^*|\mathbf{u}^*)$ is bounded away from 1 for all no-signaling strategies that optimally violate the Bell inequality] can be used for amplification. We introduce the methodology of a partial tomographic procedure on the empirical statistics obtained in the Bell test that ensures that the outputs constitute a linear min-entropy source of randomness. As a technical novelty that may be of independent interest, we prove that the Santha-Vazirani source satisfies an exponential concentration property given by a recently discovered generalized Chernoff bound.

DOI: 10.1103/PhysRevLett.117.230501

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

We consider the task of randomness amplification, 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 rather, the bits Y_i produced by the source obey

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

Here, $0 \leq \varepsilon < \frac{1}{2}$ is a parameter describing the reliability of the source, the task being to convert a source with $\varepsilon < \frac{1}{2}$ into one with $\varepsilon \to 0$. Interestingly, this task is known to be impossible with classical resources, a single SV source cannot be amplified [1].

In [2], the nonlocal correlations of 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 critical value of $\varepsilon(\approx 0.06)$ [2,3], where device independence refers to the fact that one need not trust the internal workings of the device. An improvement was made in [4] 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 [5], we demonstrated a device-independent protocol which uses a constant number of spatially separated components and amplifies sources of arbitrary initial $\varepsilon < \frac{1}{2}$ while simultaneously tolerating a constant amount of noise in

its implementation. All of these protocols were shown to be secure against general adversaries restricted only by the no-signaling principle of relativity under a technical assumption of independence between the source and the device. In [6], a randomness amplification protocol was formulated for general min-entropy sources and shown to be secure against quantum adversaries without the independence assumption, the drawback of this protocol being that it requires a device with a large number of spatially separated components for its implementation. Other protocols have also been proposed [7,8], for which full security proofs are missing. For fundamental as well as practical reasons, it is vitally important to minimize the number of spatially separated components in the protocol. As such, devising a protocol with the minimum possible number of components (two spacelike 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.

Let $\mathbf{U}$, $\mathbf{X}$ denote the input and output sets, respectively, of honest parties in a device-independent Bell-based protocol for randomness amplification. A necessary condition for obtaining randomness against general no-signaling (NS) 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.,

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

where $\mathbf{B}$ is an indicator vector [with entries $B(\mathbf{x}, \mathbf{u})$] encoding the Bell expression and $\mathbf{B} \cdot \{P(\mathbf{x}|\mathbf{u})\} = \sum_{\mathbf{x},\mathbf{u}} B(\mathbf{x}, \mathbf{u}) P(\mathbf{x}|\mathbf{u}) = 0$ denotes that the box $\{P(\mathbf{x}|\mathbf{u})\}$ algebraically violates 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 the observed Bell violation does not guarantee any randomness and a device-independent protocol for obtaining randomness cannot be built on the basis of this violation. 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, all the outputs for input $\mathbf{u}^*$ possess randomness, and extraction of this randomness may be feasible.

Here, we present a fully device-independent protocol that allows us to amplify the randomness of any ε-SV source under the minimal necessary condition in Eq. (2). A novel element of the protocol is an additional test (to the usual Bell test) akin to partial tomography of the boxes that the honest parties perform, to lower bound (in a linear number of runs) $P(\mathbf{x} = \mathbf{x}^*|\mathbf{u} = \mathbf{u}^*) =: \mathbf{D} \cdot \{P(\mathbf{x}|\mathbf{u})\}$. Here, $\mathbf{D}$ is an indicator vector with entries $D(\mathbf{x}, \mathbf{u})$ such that $D(\mathbf{x}, \mathbf{u}) = 1$ iff $(\mathbf{x}, \mathbf{u}) = (\mathbf{x}^*, \mathbf{u}^*)$. Additionally, this test ensures that Eq. (3) is also met for a sufficient number of runs, a detailed description is provided in the Supplemental Material [9]. The protocol uses a device consisting of only two no-signaling components and tolerates a constant error rate. We show that the output bits from the protocol satisfy universally composable security, the strongest form of cryptographic security, for any adversary limited only by the no-signaling principle.

Main result.—We present a two-party protocol to amplify the randomness of SV sources against no-signaling adversaries; formally, we show the following (the detailed security proof is presented in the Supplemental Material [9]).

Theorem 1 (informal).—For every $\varepsilon < \frac{1}{2}$, there is a protocol using an ε-SV source and a device consisting of two no-signaling components with the following properties: (i) Using the device $\text{poly}(n, \log(1/\gamma))$ times, the protocol either aborts or produces n bits which are γ close to uniform and independent of any no-signaling side information about the device and classical side information about the source (e.g., held by an adversary). (ii) Local measurements on many copies of a two-party entangled state, with $\text{poly}(1 - 2\varepsilon)$ error rate, give rise to a device that does not abort the protocol with probability larger than $1 - 2^{-\Omega(n)}$. The protocol is not explicit and runs in $\text{poly}(n, \log(1/\gamma))$ time. Alternatively, it can use an explicit extractor to produce a single bit of randomness that is γ close to uniform in $\text{poly}(\log(1/\gamma))$ time.

Protocol.—The protocol for the task of randomness amplification from ε-SV sources is given explicitly in Fig. 1 and illustrated in Fig. 2; its structure is as follows. 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

Protocol I

1. The ε-SV source is used to choose the measurement settings $u = (\mathbf{u}^1_{\leq n}, \mathbf{u}^2_{\leq n})$ for n runs on the single device consisting of two components. The device produces output bits $x = (\mathbf{x}^1_{\leq n}, \mathbf{x}^2_{\leq n})$.
2. The parties perform an estimation of the violation of the Bell inequality in the device by computing the empirical average $L_n(x, u) := \frac{1}{n} \sum_{i=1}^{n} B(\mathbf{x}_i, \mathbf{u}_i)$. The protocol is aborted unless $L_n(x, u) \leq \delta$ for fixed constant $\delta > 0$.
3. Conditioned on not aborting in the previous step, the parties subsequently check if $S_n(x, u) := \frac{1}{n} \sum_{i=1}^{n} D(\mathbf{x}_i, \mathbf{u}_i) \geq \mu_1$. The protocol is aborted if this condition is not met for fixed $\mu_1 > 0$.
4. Conditioned on not aborting in the previous steps, the parties apply an independent source extractor [10, 12] to the sequence of outputs from the device and further n bits from the SV source.

FIG. 1. Protocol for device-independent randomness amplification from a single device with two no-signaling components.

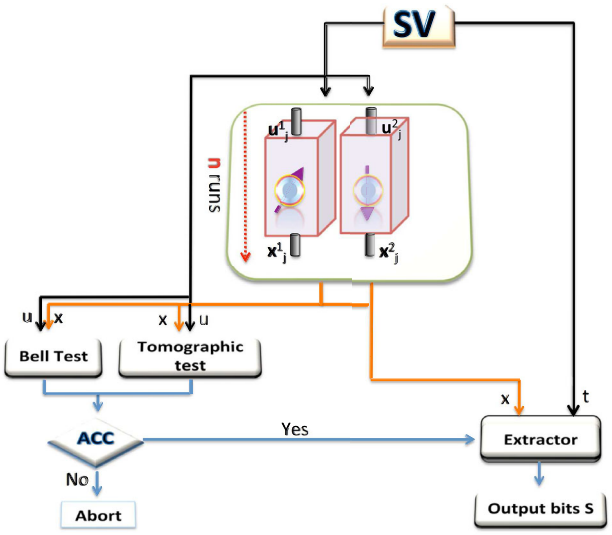

FIG. 2. An illustration of the protocol for randomness amplification using two no-signaling components. The bits from the SV source (black arrows) are used as inputs $(\mathbf{u}_j^1, \mathbf{u}_j^2)$ for the jth run of the two spatially separated devices, with $1 \le j \le n$, and the corresponding outputs $(\mathbf{x}_j^1, \mathbf{u}_j^2)$ are obtained. The inputs and outputs of all the n runs (u, x) are subjected to two tests: a Bell test for the violation of a specific Bell inequality and a (partial) tomographic test counting a specific number of input-output pairs $(\mathbf{u}^*, \mathbf{x}^*)$. If both tests are passed (denoted by ACC), the outputs x (orange arrows) are hashed together with further n bits t from the SV source using an extractor.

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 which ensures, when passed, that a sufficient number of runs were performed with boxes that have randomness in their outputs. If both tests 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.

Description of the setup.—The setup of the protocol is as follows. The honest parties and Eve share a no-signaling box $\{p(x, z|u', w)\}$ where $u' = \mathbf{u}'_{\le n} := (\mathbf{u}'_1, \ldots, \mathbf{u}'_n)$ and $x = \mathbf{x}_{\le n} := (\mathbf{x}_1, \ldots, \mathbf{x}_n)$ denote the input and output, respectively, of the honest parties for the n runs of the protocol, with w and z being the inputs and outputs of the adversary Eve. The devices held by the honest parties are separated into two components with corresponding inputs and outputs u'^i and x^i, respectively, for $i = 1, 2$, i.e., $u' = (u'^1, u'^2)$ and $x = (x^1, x^2)$. Note that u'^i, x^i themselves denote the inputs and outputs of the n runs of the protocol for party i, i.e., $u'^i = \mathbf{u}'^i_{\le n} := (\mathbf{u}'^i_1, \ldots, \mathbf{u}'^i_n)$ and $x^i = \mathbf{x}^i_{\le n} = (\mathbf{x}^i_1, \ldots, \mathbf{x}^i_n)$. Here, for the jth run of the Bell test, we have labeled the measurement settings of Alice $\mathbf{u}'^1_j$ and those of Bob $\mathbf{u}'^2_j$ with the corresponding outcomes $\mathbf{x}^1_j$ and $\mathbf{x}^2_j$ and denoted the joint inputs of Alice and Bob in this run as $\mathbf{u}'_j = (\mathbf{u}'^1_j, \mathbf{u}'^2_j)$ with corresponding joint output $\mathbf{x}_j = (\mathbf{x}^1_j, \mathbf{x}^2_j)$. The honest parties draw bits u from the SV source to input into the box; i.e., they set $u' = u$. They also draw further n bits t, which will be fed along with the outputs x into the randomness extractor to obtain the output of the protocol $s := \mathrm{Ext}(x, t)$. The adversary has classical information e correlated to u, t. The box we consider for the protocol is, therefore, given by the family of probability distributions $\{p(x, z, u, t, e|u', w)\}$.

Assumptions.—First, let us formally state the assumptions on $\{p(x, z, u, t, e|u', w)\}$, see, also, [5]. (i) No-signaling (shielding) assumption: The box satisfies the constraint of no signaling between the honest parties and Eve as well as between the different components of the device

$$\begin{aligned} p(x|u', w) &= p(x|u'), \\ p(z|u', w) &= p(z|w), \\ p(x^i|u') &= p(x^i|u'^i) \qquad i = 1, 2. \end{aligned} \tag{4}$$

Each device component also obeys a time-ordered no-signaling (TONS) condition for the $k \in [n]$ runs performed on it

$$p(x^i_k|z, u'^i, w, u, t, e) = p(x^i_k|z, u'^i_{\le k}, w, u, t, e) \quad \forall\ k \in [n], \tag{5}$$

where $u'^i_{\le k} := u'^i_1, \ldots, u'^i_k$. (ii) SV conditions: The variables (u, t, e) form an SV source, that satisfies Eq. (1). In particular, $p(t|u, e)$ and $p(u|e)$ also obey the SV source conditions. The fact that e cannot be perfectly correlated to u, t is called the private SV source assumption [5]. (iii) Assumption A1: The devices do not signal to the SV source; i.e., the distribution of (u, t, e) is independent of the inputs (u', w)

$$\sum_{x,z} p(x, z, u, t, e|u', w) = p(u, t, e) \ \ \forall\ (u, t, e, u', w). \tag{6}$$

(iv) Assumption A2: The box is fixed independently of the SV source

$$p(x, z|u', w, u, t, e) = p(x, z|u', w) \quad \forall\ (x, z, u', w, u, t, e). \tag{7}$$

In words, the main assumptions are that the different components of the device do not signal to each other and to the adversary Eve. Additionally, there is also a TONS 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 $p(x, z|u', w)$ is fixed independently of the SV source $p(u, t, e)$; i.e., the box is an unknown and arbitrary input-output channel independent of the SV source. This precludes malicious correlations such as in the scenario where for each bit string u taken from the source, a different (possibly local) box tuned to u is supplied, in which case the Bell test may be faked by local boxes [13]. Finally, it is worth noting that no

randomness may be extracted under the assumptions stated above in a classical setting, whereas the Bell violation by quantum boxes allows us to amplify randomness in a device-independent setting.

Security definition.—For $L_n(x,u) = (1/n)\sum_{i=1}^{n} \times B(\mathbf{x}_i, \mathbf{u}_i)$, the first (Bell) test in the protocol is passed when $L_n(x,u) \leq \delta$. We define the set Accept-1 (ACC_1) as the set of (x, u) such that this test is passed

$$\mathrm{ACC}_1 := \{(x,u) : L_n(x,u) \leq \delta\}. \tag{8}$$

The δ is the noise parameter in the Bell test which is chosen to be a positive constant depending on the initial ε of the SV source, going to zero in the limit of $\varepsilon \to \frac{1}{2}$ (see Theorem 8 in the Supplemental Material [9]). Similarly, we define Accept-2 (ACC_2) as the set of (x, u) for which the second test is passed, i.e.,

$$\mathrm{ACC}_2 := \{(x,u) : \mathcal{S}_n(x,u) \geq \mu_1\}. \tag{9}$$

We also define the set Accept (ACC) as $\mathrm{ACC} = \mathrm{ACC}_1 \cap \mathrm{ACC}_2$ of (x, u) for which both tests in the protocol are passed and Accept-u (ACC_u) as the cut

$$\mathrm{ACC}_u := \{x : (x,u) \in \mathrm{ACC}\}. \tag{10}$$

After u is input as u' and conditioned on the acceptance of the tests ACC, applying the independent source extractor [14–16] $s = \mathrm{Ext}(x,t)$, one gets the box

$$p(s,z,e|w,\mathrm{ACC}) \equiv \sum_{u} \sum_{\mathrm{Ext}(x,t)=s} p(x,z,u,t,e|w,\mathrm{ACC}). \tag{11}$$

The composable security criterion is now defined in terms of the distance of $p(s,z,e|w,\mathrm{ACC})$ to an ideal box $p^{id} = (1/|S|)p(z,e|w,\mathrm{ACC})$ with $p(z,e|w,\mathrm{ACC}) = \sum_s p(s,z,e|w,\mathrm{ACC})$. Formally, the security is given by the distance d_c defined as

$$d_c := \sum_{s,e} \max_{w} \sum_{z} \left| p(s,z,e|w,\mathrm{ACC}) - \frac{1}{|S|} p(z,e|w,\mathrm{ACC}) \right|. \tag{12}$$

Outline of the proof.—The proof of security of the protocol is a modification of the proof we presented in [5] with the crucial differences being due to the weak randomness that the two-party Bell inequality violation gives and an additional partial tomographic test imposed on the device.

To amplify SV sources, one needs Bell inequalities where quantum theory can achieve the maximal no-signaling value of the inequality [2], failing which, 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 [2,17]. 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 its maximum violation and for which this particular function is deterministic thereby providing an attack for Eve to predict with certainty the final output bit. While [4] and [5] considered Bell inequalities with more parties, the problem of finding two-party algebraically violated Bell inequalities (known as pseudotelepathy games) [18] 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 in any function of the measurement outcomes $f(\mathbf{x})$ for some input $\mathbf{u}$ in the sense that for all such boxes

$$\frac{1}{2} - \kappa \leq p(f(\mathbf{x})|\mathbf{u}) \leq \frac{1}{2} + \kappa, \tag{13}$$

for some $0 < \kappa < \frac{1}{2}$. We say that Bell inequalities with property (13) guarantee strong randomness.

The Bell inequality we consider for the task of randomness amplification is a modified version of a Kochen-Specker game from [19]. The inequality involves two parties Alice and Bob, each making one of nine possible measurements and obtaining one of four possible outcomes, which is explained further in the Supplemental Material [9]. Even though it does not guarantee the strong randomness in Eq. (13) for any function of the measurement outcomes $f(\mathbf{x})$, for any input $\mathbf{u}$, it has the redeeming feature of guaranteeing 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

$$\begin{aligned} &0 \leq p(\mathbf{x} = \mathbf{x}^*|\mathbf{u} = \mathbf{u}^*) \leq \gamma \\ &\forall \{p(\mathbf{x}|\mathbf{u})\} \quad \text{s.t.} \quad \mathbf{B} \cdot \{p(\mathbf{x}|\mathbf{u})\} = 0, \end{aligned} \tag{14}$$

for some $0 < \gamma < 1$. The above fact is checked by linear programming and is shown in Lemma 1 in the Supplemental Material [9].

The novel technique in the form of a partial tomographic test, subsequent to the Bell test, allows us to extract randomness in this minimal scenario of weak randomness. This simply checks for the number of times a particular input-output pair $(\mathbf{u}^*, \mathbf{x}^*)$ appears, the analysis of this test is done by an application of the Azuma-Hoeffding inequality. We show that the SV source obeys a generalized Chernoff bound 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 [14,16], namely, one given by the outputs of the measurement and the other given by the SV source. As shown in Proposition 16 of [5], 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., increasing the output error. The randomness extractor used in the protocol is not an explicit extractor from [14]. Alternatively, there is an explicit extractor that can be employed in the protocol that has been found recently [16], but then, it can produce just one bit of randomness. It also follows from [5] that there exists a protocol to obtain more bits with an explicit extractor using a device with three no-signaling components by additionally employing a de-Finetti theorem for no-signaling devices [20] (see Protocol II in [5]).

Conclusion and Open Questions.—We presented a device-independent protocol to amplify randomness in the minimal conditions under which such a task is possible and used it to obtain secure random bits from an arbitrarily (but not fully) deterministic Santha-Vazirani source. The protocol uses a device consisting of only two nonsignaling components, and works with correlations attainable by noisy quantum mechanical resources. Moreover, its correctness is not based on quantum mechanics and only requires the no-signaling principle.

Important open questions still remain. One interesting question is whether the requirement of strict independence between the SV source and the devices can be relaxed to only require limited independence [13]. Another is to amplify the randomness of more general min-entropy sources that do not possess the structure of the Santha-Vazirani source. Finally, a significant open problem is to realize device-independent quantum key distribution with an imperfect source of randomness, tolerating a constant error rate and achieving a constant key rate.

The Letter is supported by ERC AdG Grant No. 291348 QOLAPS, EU Grant No. 323970 RAQUEL and by the Foundation for Polish Science TEAM project cofinanced by the EU European Regional Development Fund. F. B. acknowledges support from EPSRC and Polish Ministry of Science and Higher Education Grant No. IdP2011 000361. Part of this work was done in National Quantum Information Center of Gdańsk. Part of this work was done when F. B., R. R., K. H., and M. H. attended the program "Mathematical Challenges in Quantum Information" at the Isaac Newton Institute for Mathematical Sciences in the University of Cambridge.

*Corresponding author.
hanna.wojewodka@us.edu.pl

[1] M. Santha and U. V. Vazirani, Generating quasi-random sequences from slightly-random sources, in *25th Annual Symposium on Foundations of Computer Science (FOCS'84), Singer Island, Fla., 1984* (IEEE Computer Society Press, New York, 1984), pp. 434–440.

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

[3] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, and R. Ramanathan, Free randomness amplification using bipartite chain correlations, Phys. Rev. A **90**, 032322 (2014).

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

[5] 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. Nat. Commun. **7**, 11345 (2016).

[6] K. M. Chung, Y. Shi, and X. Wu, Physical randomness extractors: generating random numbers with minimal assumptions, arXiv:1402.4797.

[7] P. Mironowicz, R. Gallego, and M. Pawłowski, Robust amplification of Santha-Vazirani sources with three devices, Phys. Rev. A **91**, 032317 (2015).

[8] M. Plesch and M. Pivoluska, Device-independent randomness amplification with a single device, Phys. Lett. A **378**, 2938 (2014).

[9] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.117.230501 for the formal proof of security of the device-independent randomness amplification protocol presented in the main text, which includes Refs. [10–12].

[10] A. Cabello, Experimentally Testable State-Independent Quantum Contextuality, Phys. Rev. Lett. **101**, 210401 (2008).

[11] A. Panconesi and A. Srinivasan, Randomized distributed edge coloring via an extension of the Chernoff-Hoeffding bounds, SIAM J. Comput. **26**, 350 (1997).

[12] R. Impagliazzo and V. Kabanets, in *Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques; 13th International Workshop, APPROX 2010, and 14th International Workshop, RANDOM 2010, Barcelona, Spain, 2010; Proceedings* (Springer, Berlin, 2010), 617–631.

[13] H. Wojewódka, F. G. S. L. Brandão, A. Grudka, M. Horodecki, K. Horodecki, P. Horodecki, M. Pawłowski, and R. Ramanathan, Amplifying the randomness of weak sources correlated with devices, arXiv:1601.06455.

[14] B. Chor and O. Goldreich, Unbiased bits from sources of weak randomness and probabilistic communication complexity, SIAM J. Comput. **17**, 230 (1988).

[15] X. Li, Extractors for a constant number of independent sources with polylogarithmic min-entropy, in *54th Annual Symposium on Foundations of Computer Science (FOCS'13), Berkeley, CA, 2013* (IEEE Computer Science Press, New York, 2013), pp. 100–109.

[16] E. Chattopadhyay and D. Zuckerman, Electronic Colloquium on Computational Complexity, Report No. 119, 2015 (unpublished).

[17] N. D. Mermin, Simple Unified Form for the Major no-Hidden-Variables Theorems, Phys. Rev. Lett. **65**, 3373 (1990).

[18] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

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

[20] F. G. S. L. Brandão and A. W. Harrow, Quantum de Finetti theorems under local measurements with applications, in *STOC '13 Proceedings of the ACM Symposium on Theory of Computing Conference, Palo Alto, CA, 2013* (ACM, New York, 2013), pp. 861–870.