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 24, 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

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

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 $\varepsilon \to 0$. Interestingly, this task is known to be impossible with classical resources, a single SV source cannot be amplified [1].

In [5], 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 [7] 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 [8], 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.

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.,

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

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). 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. 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).

Main Result

In this paper we present 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 $1 - 2^{-\Omega(n)}$.*

PROTOCOL AND DESCRIPTION OF THE SETUP

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 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 some 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. Conditoned on not aborting in the previous steps, the parties apply the independent source extractor from [2] to the sequence of outputs from the device and a further n bits from the SV source.

FIG. 1: Protocol for device-independent randomness amplification from a single device with two no-signaling components using a non-explicit extractor.

The protocol for the task of randomness amplification from Santha-Vazirani sources is given precisely in Fig. 1, 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 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.

The setup of the protocol is as follows. The honest parties and Eve share a no-signaling box $\{P(x, z|u', w)\}$ where $u' = \mathbf{u'}_{\leq n}$ and $x = \mathbf{x}_{\leq n}$ denote the input and output respectively of the honest parties for the n runs of the protocol, with w and z the respective inputs and outputs of the adversary Eve. The devices held by the honest parties are separated into $m = 2$ 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., $u'^i = \mathbf{u'}^i_{\leq n}$ and $x^i = \mathbf{x}^i_{\leq n}$ where $\mathbf{u'}^i_{\leq n}$ is short for

$(\mathbf{u'}_1^i, \ldots, \mathbf{u'}_n^i)$ and similarly $\mathbf{x}_{\leq n}^i$ stands for $(\mathbf{x}_1^i, \ldots, \mathbf{x}_n^i)$. Here, for the j-th run of the Bell test, we label the measurement settings of Alice $\mathbf{u'}_j^1$ and those of Bob $\mathbf{u'}_j^2$ with the corresponding outcomes $\mathbf{x}_j^1$ and $\mathbf{x}_j^2$ respectively. 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 $s := Ext(x,t)$. 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 $\{P(x,z,u,t,e|u',w)\}$.

For $L_n(x,u) = \frac{1}{n}\sum_{i=1}^n B(\mathbf{x}_i, \mathbf{u}_i)$, the first test in the protocol is passed when $L_n(x,u) \leq \delta$, we define the set ACC_1 as the set of (x,u) such that this test (for the violation of the Bell inequality given by $B(\mathbf{x}_i, \mathbf{u}_i)$) is passed:

$$\text{ACC}_1 := \{(x,u) : L_n(x,u) \leq \delta\}. \tag{4}$$

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 $\varepsilon \to \frac{1}{2}$. Similarly, we define the set ACC_2 as the set of (x,u) for which the second test is passed, i.e., those for which $S_n(x,u) \geq \mu_1$

$$\text{ACC}_2 := \{(x,u) : S_n(x,u) \geq \mu_1\}. \tag{5}$$

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

$$\text{ACC}_u := \{x : (x,u) \in \text{ACC}\}. \tag{6}$$

After u is input as u' and conditioned on the acceptance of the tests ACC, applying the independent source extractor $s = Ext(x,t)$ one gets the following box

$$\begin{aligned} &p(s,z,e|w,\text{ACC}) \\ &\equiv \sum_u \sum_{Ext(x,t)=s} p(x,z,u,t,e|w,\text{ACC}) \end{aligned} \tag{7}$$

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

$$d_c = \sum_{s,e} \max_w \sum_z \left| p(s,z,e|w,\text{ACC}) - \frac{1}{|S|}p(z,e|w,\text{ACC}) \right|. \tag{8}$$

The assumptions under which we prove the security of the protocol (i.e., that the distance d_c vanishes) are stated formally in the Supplemental Material. Briefly, 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 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. As we shall see following the analysis in [8], d_c can be bounded as

$$d_c \leq |S| d. \tag{9}$$

with the distance d given as

$$d = \sum_{z,u,e} q(z,u,e|\text{ACC}) \sum_s \left| q(s|z,u,e,\text{ACC}) - \frac{1}{|S|} \right|, \tag{10}$$

for a derived distribution $q(x,u,z,t,e)$. The assumptions in the protocol imply that $q(x,u,z,t,e)$ obeys (for details see the Supplemental Material and [8])

$$\begin{aligned} q(x,z|u,t,e) &= q(x,z|u) \\ q(x|z,u,t,e) &= q_{t,e,z}(x|u) \text{ is time-ordered no-signaling} \\ q(u|z,e) \text{ and } q(t|z,u,e) &\text{obey the SV source conditions.} \end{aligned} \tag{11}$$

OUTLINE OF THE PROOF

The proof of security of the protocol follows along similar lines to the proof we presented in [8] but with some crucial differences which we now elaborate. As in previous works on randomness amplification [5, 7, 8], 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, 6] 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 (which we denote e) 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 [5], 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 [37] as noted in [5]. 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 [7] and [8] 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 $\mathbf{u}$ in the sense that for all such boxes

$$\frac{1}{2} - \gamma \leq P(f(\mathbf{x})|\mathbf{u}) \leq \frac{1}{2} + \gamma \tag{12}$$

for some $0 < \gamma < \frac{1}{2}$. We call Bell inequalities with property (12) 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 [35]. 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. Even though it does not guarantee the strong randomness in Eq.(12) 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

$$\begin{aligned} &0 \leq P(\mathbf{x} = \mathbf{x}^*|\mathbf{u} = \mathbf{u}^*) \leq \frac{1}{2} + \gamma \\ &\forall \{P(\mathbf{x}|\mathbf{u})\} \quad \text{s.t} \quad \mathbf{B} \cdot \{P(\mathbf{x}|\mathbf{u})\} = 0 \end{aligned} \tag{13}$$

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

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. We also 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 [2], namely one given by the outputs of the measurement and the other given by the SV source. As shown in [8], 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 [8] 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 [8]).

CONCLUSION AND OPEN QUESTIONS

In this article, we presented a device-independent protocol to amplify randomness from the most 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 non-signaling components, and works with correlations attainable by noisy quantum mechanical resources. Moreover the correctness of the protocol is not based on quantum mechanics and only requires the no-signaling principle.

Important open questions still remain. In particular, it is important to construct efficient protocols that in addition give a constant rate of random bits for each use of the device, note that the protocol here still has the drawback of zero rate. Another interesting open question 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 constant error rates and achieving constant key rates.

Acknowledgments. The paper is supported by ERC AdG grant QOLAPS, EC grant RAQUEL and by Foundation for Polish Science TEAM project co-financed by the EU European Regional Development Fund. FB 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.

[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] J. Barrett and N. Gisin. How Much Measurement Independence Is Needed to Demonstrate Nonlocality? Phys. Rev. Lett. **106**, 100406 (2011).
[4] M. J. W. Hall. Local Deterministic Model of Singlet State Correlations Based on Relaxing Measurement Independence. Phys. Rev. Lett. **105**, 250404 (2010).
[5] R. Colbeck and R. Renner. Free randomness can be amplified. Nature Physics **8**, 450 (2012).
[6] Xin-Li. Extractors for a constant number of independent sources with polylogarithmic min-entropy. (to appear in FOCS 2013).
[7] 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).
[8] 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).
[9] R. Ramanathan, F. G. S. L. Brandao, A. Grudka, K. Horodecki, M. Horodecki and P. Horodecki. Robust Device-Independent Randomness Amplification. arXiv: 1308.4635 (2013).
[10] O. Guehne, G. Toth, P. Hyllus and H. Briegel. Phys. Rev. Lett. **95**, 120405 (2005).
[11] P. Mironowicz, R. Gallego and M. Pawłowski. Robust amplification of Santha-Vazirani sources with three devices. Phys. Rev. A **91**, 032317 (2015).
[12] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski and R. Ramanathan. Free randomness amplification using bipartite chain correlations. arXiv:1303.5591 (2013).
[13] J. E. Pope and A. Kay. Limited Free Will in Multiple Runs of a Bell Test. arXiv:1304.4904 (2013).
[14] L. P. Thinh, L. Sheridan and V. Scarani. Bell tests with min-entropy sources. arXiv:1304.3598 (2013).
[15] M. Plesch and M. Pivoluska. Single Min-Entropy Random Source can be Amplified. arXiv:1305.0990 (2013).
[16] R. Augusiak, M. Demianowicz, M. Pawlowski, J. Tura and A. Acin. Monogamies of correlations and amplification of randomness. arXiv: 1307.6390 (2013).
[17] R. Colbeck and A. Kent. Private Randomness Expansion With Untrusted Devices. Journal of Physics A: Mathematical and Theoretical 44(9), 095305 (2011).
[18] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson. Simulating independence: New constructions of condensers, Ramsey graphs, dispersers, and extractors. Proceedings of the 37th Annual ACM Symposium on Theory of Computing, pp 110 (2005).
[19] A. Rao. Extractors for a constant number of polynomially small min-entropy independent sources. Proceedings of the 38th Annual ACM Symposium on Theory of Computing (2006).
[20] S. Pironio et al. Random numbers certified by Bell's theorem. Nature **464**, 1021 (2010).
[21] S. Pironio and S. Massar. Security of practical private randomness generation. Phys. Rev. A 87, 012336 (2013).
[22] S. Fehr, R. Gelles, and C. Schaffner. Security and Composability of Randomness Expansion from Bell Inequalities. arXiv:1111.6052 (2011).
[23] R. Colbeck, PhD dissertation. Quantum And Relativistic Protocols For Secure Multi-Party Computation. University of Cambridge, arXiv:0911.3814 (2009).
[24] A. Acin, S. Massar and S. Pironio. Randomness versus Nonlocality and Entanglement. Phys. Rev. Lett. **108**, 100402 (2012).
[25] J. Barrett, L. Hardy and A. Kent. No Signaling and Quantum Key Distribution. Phys. Rev. Lett. **95**, 010503 (2005).
[26] Ll. Masanes. Universally Composable Privacy Amplification from Causality Constraints. Phys. Rev. Lett. 102, 140501 (2009).
[27] E. Hänggi, R. Renner and S. Wolf. Efficient Device-Independent Quantum Key Distribution. EUROCRYPT 2010, 216 (2010).
[28] U. Vazirani and T. Vidick. Certifiable Quantum Dice - Or, testable exponential randomness expansion. arXiv:1111.6054 (2011).
[29] U. Vazirani and T. Vidick. Fully device independent quantum key distribution. arXiv:1210.1810 (2012).
[30] M. Coudron, T. Vidick, and H. Yuen. Robust Randomness Amplifiers: Upper and Lower Bounds. arXiv:1305.6626 (2013).
[31] F. G. S. L. Brandao and A. W. Harrow. Quantum de Finetti Theorems under Local Measurements with Applications. STOC 2013: 861-870. arXiv: 1210.6367 (2012).
[32] F. G. S. L. Brandao and A. W. Harrow. Product-state Approximations to Quantum Groundstates. STOC 2013: 871-880.
[33] 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).
[34] 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).
[35] L. Aolita, R. Gallego, A. Acín, A. Chiuri, G. Vallone, P. Mataloni and A. Cabello, Phys. Rev. A **85**, 032107 (2012).
[36] A. Cabello, Phys. Rev. Lett. **101** 210401 (2008).
[37] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).

Supplemental Material. Here, we present the formal proof of security of Protocol I.

ASSUMPTIONS

Let us first state formally the assumptions in our protocol, for details see [8].

- **No-signaling assumptions:** The box satisfies the constraint of no-signaling between the honest parties and Eve as well as a no-signaling condition between the different components of each device

$$\begin{aligned} p(x|u',w) &= p(x|u'), \\ p(z|u',w) &= p(z|w), \\ p(x^i|u') &= p(x^i|u'^i) \quad i=1,2. \end{aligned} \tag{14}$$

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

$$\begin{aligned} &p(x^i_k|z,u'^i,w,u,t,e) = \\ &\quad p(x^i_k|z,u'^i_{\leq k},w,u,t,e) \quad \forall k \in [n] \end{aligned} \tag{15}$$

  where $u'^i_{\leq k} := u'^i_1,\ldots,u'^i_k$.

- **SV conditions:** The variables (u,t,e) form an SV source, that is satisfy Eq. (1). In particular, $p(t|u,e)$ is also obeys the SV source condition.

- **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):

$$\begin{aligned} &\sum_{x,z} p(x,z,u,t,e|u',w) = p(u,t,e) \\ &\quad \forall (u,t,e,u',w). \end{aligned} \tag{16}$$

- **Assumption A2:** The box is fixed independently of the SV source:

$$\begin{aligned} &p(x,z|u',w,u,t,e) = p(x,z|u',w) \\ &\quad \forall (x,z,u',w,u,t,e). \end{aligned} \tag{17}$$

The composable security criterion is defined in terms of the distance d_c from Eq. (8)

$$d_c = \sum_{s,e} \max_w \sum_z \left| p(s,z,e|w,\mathrm{ACC}) - \frac{1}{|S|} p(z,e|w,\mathrm{ACC}) \right|. \tag{18}$$

Let us define the quantity d' as

$$\begin{aligned} d' \;:=\; &\sum_e p(e|\mathrm{ACC}) \max_w \sum_{z,u} p(z,u|e,w,\mathrm{ACC}) \times \\ &\sum_s \left| p(s|z,w,u,e,\mathrm{ACC}) - \frac{1}{|S|} \right| \end{aligned} \tag{19}$$

for any family of probability distributions $\{p(x,z,u,t,e|w)\}$. Now, for each e, let w_e and $p_{w_e}(x,z,u,t,e)$ denote the input of Eve and the corresponding probability distribution respectively that achieve the maximum d' in Eq. (19). By Assumption A1 and the no-signaling conditions, $p(e|w) = p(e)$ and $p(x,u|w) = p(x,u)$ so that the maximum is achieved by a distribution $q(x,z,u,t,e) = p(e)p_{w_e}(x,z,u,t|e)$. We can thus consider the quantity $d = d'$ given as

$$d = \sum_{z,u,e} q(z,u,e|\mathrm{ACC}) \sum_s \left| q(s|z,u,e,\mathrm{ACC}) - \frac{1}{|S|} \right|. \tag{20}$$

As shown in [8], we have

$$d_c \leq |S| d. \tag{21}$$

From the assumptions stated, it is seen that $q(x,u,z,t,e)$ obeys

$$\begin{aligned} q(x,z|u,t,e) &= q(x,z|u) \\ q(x|z,u,t,e) &= q_{t,e,z}(x|u) \text{is time-ordered no-signaling} \\ q(u|z,e) \;\text{ and }\; &q(t|z,u,e) \text{obey the SV source conditions.} \end{aligned} \tag{22}$$

THE BELL INEQUALITY

The Bell inequality we consider for the task of randomness amplification is a modified version of the bipartite inequality in [35]. The inequality belongs to the class $(2,9,4)$ signifying that it involves two parties Alice and Bob, each making one of nine possible measurements and obtaining one of four possible outcomes. We label the measurement settings of Alice $\mathbf{u}^1$ and those of Bob $\mathbf{u}^2$ with $\mathbf{u}^1,\mathbf{u}^2 \in \{1,\ldots,9\}$. The corresponding outcomes of Alice are labeled $\mathbf{x}^1$ and those of Bob $\mathbf{x}^2$ with $\mathbf{x}^1,\mathbf{x}^2 \in \{1,\ldots,4\}$. Note that from the notation in the main text these inputs and outputs would correspond to a particular run of the protocol $\mathbf{u}^i_j, \mathbf{x}^i_j$. Acting on a box $\{P(\mathbf{x}|\mathbf{u})\}$ with $\mathbf{x} = (\mathbf{x}^1,\mathbf{x}^2)$ and $\mathbf{u} = (\mathbf{u}^1,\mathbf{u}^2)$, the Bell expression may be written as

$$\mathbf{B} \cdot \{P(\mathbf{x}|\mathbf{u})\} = \sum_{\mathbf{x},\mathbf{u}} \mathbf{B}(\mathbf{x},\mathbf{u}) P(\mathbf{x}|\mathbf{u}) \geq 4, \tag{23}$$

Here $\mathbf{B}$ is an indicator vector with entries

$$\mathbf{B}(\mathbf{x},\mathbf{u}) = \begin{cases} 1 & : (\mathbf{x},\mathbf{u}) \in S_B \\ 0 & : \text{otherwise} \end{cases} \tag{24}$$

The minimum value achieved by local realistic theories for this combination of probabilities is 4 while general no-signaling theories can achieve the algebraic minimum value of 0. Crucially, there exist a quantum state and suitable measurements reaching this algebraic minimum.

The set $S_B = \bigcup S^{\mathbf{u}}_B$ for which $\mathbf{B}(\mathbf{x},\mathbf{u}) = 1$ is defined using the orthogonality hypergraph in Fig. 2 which represents a Kochen-Specker set of vectors from [36] displaying state-independent contextuality in dimension 4. In this graph, the nine measurements are represented by the nine colored hyperedges each giving four outcomes,

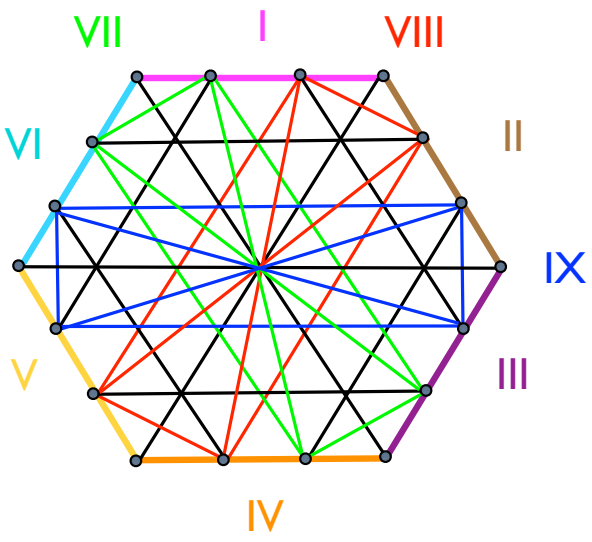

FIG. 2: Illustration of the Kochen-Specker set used in formulating the bipartite Bell inequality

where the vertices represent rank-one projectors corresponding to the outcomes. Each party performs the nine measurements corresponding to the KS set, the set S_B consists of all 81 pairs of measurements $\mathbf{u}$. For each $\mathbf{u}$, the pair of outcomes $\mathbf{x} \in S_B^{\mathbf{u}}$ if the vertex representing outcome $\mathbf{x}^1$ in $\mathbf{u}^1$ is connected by a hyperedge to the vertex representing outcome $\mathbf{x}^2$ in $\mathbf{u}^2$. A direct counting shows that out of the $4^2 \times 9^2 = 1296$ probabilities $P(\mathbf{x}|\mathbf{u})$, 504 enter the Bell expression. Moreover, in any deterministic assignment of $1's$ and $0's$ to these probabilities respecting the no-signaling and normalization constraints, at least four probabilities are assigned value 1 giving rise to the local realistic bound. In quantum theory and in general no-signaling theories however, all 504 probabilities may be set to 0 giving rise to the algebraic violation of the inequality.

In order to achieve the maximal violation within quantum theory, Alice and Bob share a maximally entangled state in dimension four, namely

$$|\Psi\rangle = \frac{1}{2}\sum_{i=1}^{4} |i\rangle \otimes |i\rangle. \tag{25}$$

The measurements they each perform correspond exactly to the 18 projectors defining the Kochen-Specker set in [36]. Specifically, these projectors correspond to the following vectors

$$\begin{array}{llll} |v_1\rangle = (1,0,0,0)^T & |v_2\rangle = (0,1,0,0)^T & |v_3\rangle = (0,0,1,1)^T & |v_4\rangle = (0,0,1,-1)^T \\ |v_5\rangle = (1,-1,0,0)^T & |v_6\rangle = (1,1,-1,-1)^T & |v_7\rangle = (1,1,1,1)^T & |v_8\rangle = (1,-1,1,-1)^T \\ |v_9\rangle = (1,0,-1,0)^T & |v_{10}\rangle = (0,1,0,-1)^T & |v_{11}\rangle = (1,0,1,0)^T & |v_{12}\rangle = (1,1,-1,1)^T \\ |v_{13}\rangle = (-1,1,1,1)^T & |v_{14}\rangle = (1,1,1,-1)^T & |v_{15}\rangle = (1,0,0,1)^T & |v_{16}\rangle = (0,1,-1,0)^T \\ |v_{17}\rangle = (0,1,1,0)^T & |v_{18}\rangle = (0,0,0,1)^T & & \end{array} \tag{26}$$

The nine measurements are defined by the following nine bases

$$\begin{array}{lll} M_1 = (|v_1\rangle, |v_2\rangle, |v_3\rangle, |v_4\rangle) & M_2 = (|v_4\rangle, |v_5\rangle, |v_6\rangle, |v_7\rangle) & M_3 = (|v_7\rangle, |v_8\rangle, |v_9\rangle, |v_{10}\rangle) \\ M_4 = (|v_{10}\rangle, |v_{11}\rangle, |v_{12}\rangle, |v_{13}\rangle) & M_5 = (|v_{13}\rangle, |v_{14}\rangle, |v_{15}\rangle, |v_{16}\rangle) & M_6 = (|v_{16}\rangle, |v_{17}\rangle, |v_{18}\rangle, |v_1\rangle) \\ M_7 = (|v_2\rangle, |v_9\rangle, |v_{11}\rangle, |v_{18}\rangle) & M_8 = (|v_3\rangle, |v_5\rangle, |v_{12}\rangle, |v_{14}\rangle) & M_9 = (|v_6\rangle, |v_8\rangle, |v_{15}\rangle, |v_{17}\rangle) \end{array} \tag{27}$$

For this state and measurements all the probabilities entering the Bell expression are identically zero, so that algebraic violation is achieved.

Apart from the fact that quantum mechanics violates the inequality, we would also like to ensure that a strong violation of the inequality guarantees randomness. Unfortunately, none of the bipartite Bell inequalities tested so far have this property. The above inequality though has the following redeeming feature. Let $\mathbf{u}^* \equiv (1,2)$ be a particular pair of measurement settings and $\mathbf{x}^* \equiv (1,3)$ a chosen pair of outcomes for this setting. For all no-signaling boxes which algebraically violate the inequality, it holds that

$$\begin{aligned} &0 \leq P(\mathbf{x} = \mathbf{x}^*|\mathbf{u} = \mathbf{u}^*) \leq \frac{3}{4} \\ &\forall \{P(\mathbf{x}|\mathbf{u})\} \quad \text{s.t} \quad \mathbf{B} \cdot \{P(\mathbf{x}|\mathbf{u})\} = 0 \end{aligned} \tag{28}$$

It should be noted that for the quantum box which al-

gebraically violates the inequality defined by the above state and measurements, we have $P_q(\mathbf{x}=\mathbf{x}^*|\mathbf{u}=\mathbf{u}^*)=\frac{1}{16}$ so that upon maximal violation, we expect a fixed number of outputs $\mathbf{x}^*$ for inputs $\mathbf{u}^*$ in the experiment. Moreover, for boxes with a Bell value δ, we will see in Lemma 2 that $0 \leq P(\mathbf{x}^*|\mathbf{u}^*) \leq \frac{1}{4}(3+2\delta)$. So that, when one has large violation of the inequality and a sufficient number of outputs and inputs $(\mathbf{x}^*, \mathbf{u}^*)$, it must be the case that a sufficient number of runs in the experiment were done with boxes that yield randomness.

(Partial)Randomness from an observed Bell value

Using the Azuma-Hoeffding inequality, we have that if the observed Bell value is small, then a linear fraction of the conditional boxes have a small Bell value for settings chosen with an SV source. To obtain a min-entropy source, we need to have that a linear fraction of the conditional boxes has randomness. In this section, we establish the consequence to randomness of the observed Bell value.

Let **U** denote all the settings appearing in the Bell expression. We consider first the uniform Bell value

$$\overline{B}^U := \frac{1}{|U|}\mathbf{B}.\{P(\mathbf{x}|\mathbf{u})\} = \frac{1}{|U|}\sum_{\mathbf{u},\mathbf{x}} B(\mathbf{x},\mathbf{u})P(\mathbf{x}|\mathbf{u}), \quad (29)$$

where $|U|$ denotes the cardinality of **U**, i.e. the total number of settings in the Bell expression ($|U|=81$ for the Bell inequality we consider). If the Bell function $B(\mathbf{x},\mathbf{u})$ is properly chosen, one can prove using linear programming that if $\overline{B}^U$ is small, the probabilities of any output are bounded away from 1. However, since our inputs to each device are chosen using a SV source, we will be only able to estimate the value of the following expression

$$\overline{B}^{SV} = \sum_{\mathbf{u},\mathbf{x}} \nu_{SV}(\mathbf{u})B(\mathbf{x},\mathbf{u})P(\mathbf{x}|\mathbf{u}), \quad (30)$$

where $\nu_{SV}(\mathbf{u})$ is the distribution from an (unknown) SV source. Let us note that the number of bits needed by each party to choose their settings is $\lceil \log 9 \rceil = 4$, so that **u** is chosen using $2\lceil \log 9 \rceil = 8$ bits. We will show that for the Bell function, when $\overline{B}^{SV}$ is small, $\overline{B}^U$ is also small which implies randomness (for suitably chosen $\delta > 0$).

Lemma 2. *Consider a two-party no-signaling box $\{P(\boldsymbol{x}|\boldsymbol{u})\}$ satisfying*

$$\overline{B}^{SV} \leq \delta, \quad (31)$$

for some constant $\delta \geq 0$, where $\overline{B}^{SV}$ is given by Eq. (30) with $B(\boldsymbol{x},\boldsymbol{u})$ given by Eq. (24). Then for the particular measurement setting $\boldsymbol{u}^*$ and particular output $\boldsymbol{x}^*$, we have

$$P(\boldsymbol{x}=\boldsymbol{x}^*|\boldsymbol{u}=\boldsymbol{u}^*) \leq \frac{1}{4}\left(3+\frac{2\delta}{(\frac{1}{2}-\epsilon)^8}\right). \quad (32)$$

Proof. From the definition of an ε-SV source we have

$$\left(\frac{1}{2}-\varepsilon\right)^8 \leq \nu_{SV}(\mathbf{u}) \leq \left(\frac{1}{2}+\varepsilon\right)^8. \quad (33)$$

so that

$$\frac{1}{(\frac{1}{2}+\varepsilon)^8|U|}\overline{B}^{SV} \leq \overline{B}^U \leq \frac{1}{(\frac{1}{2}-\varepsilon)^8|U|}\overline{B}^{SV} \quad (34)$$

We can therefore work with the Bell value for uniformly chosen settings, relating it to the Bell value with SV source settings through Eq. (34). For $\overline{B}^{SV} \leq \delta$, Eq.(34) gives that $\overline{B}^U \leq \frac{\delta}{(\frac{1}{2}-\varepsilon)^8|U|} =: \frac{\tilde{\delta}}{|U|}$.

Consider a bipartite no-signaling box $P(\mathbf{x}|\mathbf{u})$ satisfying

$$\overline{B}^U := \frac{1}{|U|}\mathbf{B}.\{P(\mathbf{x}|\mathbf{u})\} \leq \frac{\tilde{\delta}}{|U|}, \quad (35)$$

with **B** the indicator vector for the Bell expression in Eq. (23) and $|U|=81$ the number of settings in the Bell expression.

The maximum probability for the chosen output and input for the given (uniform) Bell value can be computed by the following linear program

$$\begin{aligned} &\max_{\{P\}} : M^T_{\mathbf{u}^*,\mathbf{x}^*} \cdot \{P(\mathbf{x}|\mathbf{u})\} \\ &s.t.\ \ A \cdot \{P(\mathbf{x}|\mathbf{u})\} \leq c. \end{aligned} \quad (36)$$

Here, the indicator vector $M_{\mathbf{u}^*,\mathbf{x}^*}$ is a $4^2 \times 9^2$ element vector with entries $M_{\mathbf{u}^*,\mathbf{x}^*}(\mathbf{x},\mathbf{u}) = \mathtt{I}_{\mathbf{u}=\mathbf{u}^*}\mathtt{I}_{\mathbf{x}=\mathbf{x}^*}$, i.e., $M_{\mathbf{u}^*,\mathbf{x}^*}(\mathbf{x},\mathbf{u}) = 1$ for $(\mathbf{x},\mathbf{u}) = (\mathbf{x}^*,\mathbf{u}^*)$ and 0 otherwise. The constraint on the box $\{P(\mathbf{x}|\mathbf{u})\}$ written as a vector with $4^2 \times 9^2$ entries is given by the matrix A and the vector c. These encode the no-signaling constraints between the two parties, the normalization and the positivity constraints on the probabilities $P(\mathbf{x}|\mathbf{u})$. In addition, A and c also encode the condition that $\mathbf{B}.\{P(\mathbf{x}|\mathbf{u})\} \leq \tilde{\delta}$ for a constant $\tilde{\delta} \geq 0$.

The solution to the primal linear program in Eq. (36) can be bounded by a feasible solution to the dual program which is written as

$$\begin{aligned} &\min_{\lambda_{\mathbf{u}^*,\mathbf{x}^*}} : c^T \cdot \lambda_{\mathbf{u}^*,\mathbf{x}^*} \\ &s.t.\ \ A^T \cdot \lambda_{\mathbf{u}^*,\mathbf{x}^*} = M_{\mathbf{u}^*,\mathbf{x}^*}, \\ &\qquad \lambda_{\mathbf{u}^*,\mathbf{x}^*} \geq 0. \end{aligned} \quad (37)$$

We find a feasible $\lambda_{\mathbf{u}^*,\mathbf{x}^*}$ satisfying the constraints to the dual program above that gives $c^T\lambda_{\mathbf{u}^*,\mathbf{x}^*} \leq \frac{1}{4}(3+2\tilde{\delta})$. [1]

[1] The explicit vector $\lambda_{\mathbf{u}^*,\mathbf{x}^*}$ that is feasible for the dual program in Eq. (37) and gives the bound can be computed by standard techniques and is available upon request.

We therefore obtain by standard duality of linear programming that

$$P(\mathbf{x}=\mathbf{x}^*|\mathbf{u}=\mathbf{u}^*) \leq \frac{1}{4}(3+2\tilde{\delta}). \tag{38}$$

Noting that $\tilde{\delta} = \frac{\delta}{(\frac{1}{2}-\varepsilon)^8}$, we obtain the required bound. □

FROM EMPIRICAL VALUES TO TRUE PARAMETERS OF THE BOX

In this section, we state the lemmas based on the Azuma-Hoeffding inequality and the Generalized Chernoff bound which we will use to estimate the arithmetic average of Bell values for the conditional boxes as well as the fraction of boxes which have a lower bound. Let us state the following Lemma 3 based on the Azuma-Hoeffding inequality which we will use to estimate the arithmetic average of Bell values for the conditional boxes as well as the straightforward Lemma 4 whose proofs can be found in [8].

Lemma 3. *Consider arbitrary random variables W_i for $i = 0, 1, \ldots, n$, and binary random variables B_i for $i = 1, \ldots n$ that are functions of W_i, i.e. $B_i = f_i(W_i)$ for some functions f_i. Let us denote $\overline{B}_i = \mathbb{E}(B_i|W_{i-1}, \ldots, W_1, W_0)$ for $i = 1, \ldots, n$ and (i.e. $\overline{B}_i$ are conditional means). Define for $k = 1, \ldots, n$, the empirical average*

$$L_k = \frac{1}{k}\sum_{i=1}^{k} B_i \tag{39}$$

and the arithmetic average of conditional means

$$\overline{L}_k = \frac{1}{k}\sum_{i=1}^{k} \overline{B}_i. \tag{40}$$

Then we have

$$\Pr(|L_n - \overline{L}_n| \geq s) \leq 2e^{-n\frac{s^2}{2}} \tag{41}$$

Lemma 4. *If the arithmetic average $\overline{L}_n$ of n conditional means satisfies $\overline{L}_n \leq \delta$ for some parameter $\delta > 0$, then in at least $(1-\sqrt{\delta})n$ of positions i we have $\overline{B}_i \leq \sqrt{\delta}$*

Proving the lower bound for a fraction of boxes

In this section, we estimate the fraction of boxes for which $q(\mathbf{x}_i = \mathbf{x}^*|\mathbf{u}_i = \mathbf{u}^*, \mathbf{u}_{<i}, \mathbf{x}_{<i}, z, e)$ is lower bounded by a constant. To do so, we perform a test using the random variables $D_i^u(x)$ for any fixed u

$$D_i^u(x) := D(\mathbf{x}_i, \mathbf{u}_i) = \begin{cases} 1 & : \mathbf{x}_i = \mathbf{x}^* \wedge \mathbf{u}_i = \mathbf{u}^* \\ 0 & : \text{otherwise} \end{cases}$$

for $i = 1, \ldots, n$. The test function is defined as

$$S_n(x,u) := \frac{1}{n}\sum_{i=1}^{n} D(\mathbf{x}_i, \mathbf{u}_i) \tag{42}$$

with the corresponding average $\overline{S}_n(x,u,z,e)$ defined as

$$\overline{S}_n(x,u,z,e) := \frac{1}{n}\sum_{i=1}^{n} \mathbb{E}_{\sim q(\mathbf{x}_i|\mathbf{x}_{<i},u,z,e)} D(\mathbf{x}_i, \mathbf{u}_i). \tag{43}$$

The test checks if

$$S_n(x,u) \geq \mu_1 \tag{44}$$

for a fixed $\mu_1 > 0$.

We now show that when the test accepts, with probability $1 - 2\exp\left(-n\frac{\mu_1^2}{8}\right)$ at least $\frac{\mu_1 - 2\kappa}{2(1-\kappa)}n$ boxes have randomness in the output for input setting $\mathbf{u}^*$, specifically that $q(\mathbf{x}_i = \mathbf{x}^*|\mathbf{u}_i = \mathbf{u}^*, \mathbf{u}_{<i}, \mathbf{x}_{<i}, z, e) \geq \kappa$ for fixed $\kappa > 0$.

Lemma 5. *Assume that the test given by Eq. (44) for the box $q(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n|\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n, z, e)$ accepts (for fixed $\mu_1 > 0$). Consider the set $I_\kappa(u) := \{i : \boldsymbol{u}_i = \boldsymbol{u}^* \wedge q(\boldsymbol{x}_i = \boldsymbol{x}^*|\boldsymbol{u}_i = \boldsymbol{u}^*, \boldsymbol{u}_{<i}, \boldsymbol{x}_{<i}, z, e) \geq \kappa\}$. With probability at least $1 - 2\exp\left(-n\frac{\mu_1^2}{8}\right)$, $|I_\kappa(u)| \geq \frac{\mu_1 - 2\kappa}{2(1-\kappa)}n$.*

Proof. When the test is passed, i.e., when $S_n(x,u) \geq \mu_1$, by Lemma 3 with probability at least $1 - 2\exp\left(-n\frac{\mu_1^2}{8}\right)$, we have that $\overline{S}_n(x,u,z,e) \geq \frac{\mu_1}{2}$. In other words, we have

$$\sum_i q(\mathbf{x}_i = \mathbf{x}^*|\mathbf{u}_i = \mathbf{u}^*, \mathbf{u}_{<i}, \mathbf{x}_{<i}, z, e) \;\geq\; \frac{\mu_1}{2}, \tag{45}$$

where we used the no-signaling condition $q(\mathbf{x}_i = \mathbf{x}^*|u,z,e) = q(\mathbf{x}_i = \mathbf{x}^*|\mathbf{u}_i = \mathbf{u}^*, \mathbf{u}_{<i}, \mathbf{x}_{<i}, z, e)$. Consider the set $I_\kappa(u)$, we have that

$$(n - |I_\kappa(u)|)\kappa + |I_\kappa(u)| \geq \frac{\mu_1}{2}\, n \tag{46}$$

or

$$|I_\kappa(u)| \geq \frac{\mu_1 - 2\kappa}{2(1-\kappa)}n. \tag{47}$$

Therefore, with probability at least $1 - 2\exp\left(-n\frac{\mu_1^2}{8}\right)$ the set of boxes with $\mathbf{u}_i = \mathbf{u}^*$ and $q(\mathbf{x}_i = \mathbf{x}^*|\mathbf{u}_i = \mathbf{u}^*, \mathbf{u}_{<i}, \mathbf{x}_{<i}, z, e) \geq \kappa$ for fixed $\mu_1 > 0$, $0 < \kappa < \frac{1}{2}$ is of size at least $\frac{\mu_1 - 2\kappa}{2(1-\kappa)}n$.

□

A min-entropy source from randomness of conditional boxes

In this section we show that if a device is such that a linear number of conditional boxes have randomness (in the weak sense that the probability of

the outputs is bounded away from one for any one setting and this particular setting appears a linear fraction of times), then the distribution on outputs constitutes a min-entropy source. Let any sequence $(z, e, \mathbf{x}_1, \mathbf{u}_1, \ldots, \mathbf{x}_n, \mathbf{u}_n)$ be such that $\mathbf{x}_i$ and $\mathbf{u}_i$, $i \in \{1, \ldots, n\}$, are of the form of $\mathbf{x} = (\mathbf{x}^1, \mathbf{x}^2)$ and $\mathbf{u} = (\mathbf{u}^1, \mathbf{u}^2)$, respectively. Consider that with large probability over sequences $(z, e, \mathbf{x}_1, \mathbf{u}_1, \ldots, \mathbf{x}_n, \mathbf{u}_n)$, a particular setting $\mathbf{u}^*$ appears a linear fraction μn times and that within this fraction, the probability of $\mathbf{x}^*$ and its complementary outcome $\bar{\mathbf{x}}^*$ is bounded away from 1, then the total probability distribution is close in variational distance to a min-entropy source. To show this, we use the following lemma from [8]

Lemma 6. *Fix any measure P on the space of sequences $(z, e, \boldsymbol{x}_1, \boldsymbol{u}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{u}_n)$. Suppose that for a sequence $(z, e, \boldsymbol{x}_1, \boldsymbol{u}_1, \ldots, \boldsymbol{x}_n, \boldsymbol{u}_n)$, there exists $K \subseteq [n]$ of size larger than μn, such that for all $l \in K$ we have $\boldsymbol{u}_l = \boldsymbol{u}^*$ and the conditional boxes $P_{\boldsymbol{x}_{<l}, \boldsymbol{u}_{<l}}(\boldsymbol{x}_l | \boldsymbol{u}_l, z, e)$ satisfy*

$$P_{\boldsymbol{x}_{<l}, \boldsymbol{u}_{<l}}(\boldsymbol{x}_l | \boldsymbol{u}_l = \boldsymbol{u}^*, z, e) \leq \gamma. \tag{48}$$

Then, $P(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n | \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n, z, e)$ satisfies

$$P(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n | \boldsymbol{u}_1, \ldots, \boldsymbol{u}_n, z, e) \leq \gamma^{\mu n}. \tag{49}$$

SECURITY PROOF

Let us first recall the definition of a min-entropy source and the notion of an independent source randomness extractor, specifying the extractor we will use to obtain randomness in our protocol. The min-entropy of a random variable S is given by

$$H_{min}(S) = \min_{s \in supp(S)} \log \frac{1}{P(S = s)}, \tag{50}$$

where $supp(S)$ denotes the support of S. For $S \in \{0,1\}^n$, the source is called an $(n, H_{min}(S))$ min-entropy source. An independent source extractor $Ext : (\{0,1\}^n)^k \to \{0,1\}^m$ is a function that acts on k independent min-entropy sources and outputs m bits that are ξ close to uniform, i.e., for k independent $(n, H_{min}(S_i))$ sources (with $i \in \{1, \ldots, k\}$) we have

$$\|Ext(S_1, \ldots, S_k) - U_m\|_1 \leq \xi, \tag{51}$$

where $\|.\|_1$ is the variational distance between the two distributions and U_m denotes the uniform distribution on the m bits. For use in Protocol I, we use a (non-explicit) deterministic extractor from [2] that, given two independent sources of min-entropy larger than h, outputs $\Omega(h)$ bits $2^{-\Omega(h)}$-close to uniform.

Let us define the set $Az_1^{\delta_{Az}}$ as

$$Az_1^{\delta_{Az}} := \{(z,u,e) : \Pr_{\sim q(x|z,u,e)} \left(\bar{L}_n(x,u,z,e) \geq L_n(x,u) + \delta_{Az}\right) \leq \epsilon_{Az1}\} \tag{52}$$

and the cut

$$Az_1^{\delta_{Az}}(u) := \{(z,e) : (z,u,e) \in Az_1^{\delta_{Az}}\}. \tag{53}$$

Let us also define the set $Az_2^{\mu_1}(u)$ for any fixed u as

$$Az_2^{\mu_1}(u) := \{(z,e) : \Pr_{\sim q(x|z,u,e)} \left(\overline{S}_n(x,u,z,e) \leq S_n(x,u) - \frac{\mu_1}{2}\right) \leq \epsilon_{Az2}\} \tag{54}$$

with $\epsilon_{Az1} = 2e^{-n\frac{1}{4}\delta_{Az}^2}$ and $\epsilon_{Az2} = 2e^{-n\frac{\mu_1^2}{16}}$ and the set $Az(u)$ as

$$Az(u) := Az_1^{\delta_{Az}}(u) \cap Az_2^{\mu_1}(u). \tag{55}$$

Note that despite the apparent similarity in the nomenclature of $Az_1^{\delta_{Az}}(u)$ and $Az_2^{\mu_1}(u)$, they differ in the respect that $Az_2^{\mu_1}(u)$ is a set of large measure for every u (as seen in Eq. (58)) while $Az_1^{\delta_{Az}}(u)$ is a set of large measure only for most (typical) u. Here

$$\begin{aligned} L_n(x,u) &= \frac{1}{n}\sum_{i=1}^n B(\mathbf{x}_i, \mathbf{u}_i), \\ \bar{L}_n(x,u,z,e) &= \frac{1}{n}\sum_{i=1}^n \mathbb{E}_{q(\mathbf{x}_i, \mathbf{u}_i | \mathbf{x}_{<i}, \mathbf{u}_{<i}, z, e)} B(\mathbf{x}_i, \mathbf{u}_i) \end{aligned} \tag{56}$$

Similarly,

$$\begin{aligned} S_n(x,u) &= \frac{1}{n}\sum_{i=1}^n D(\mathbf{x}_i, \mathbf{u}_i), \\ \overline{S}_n(x,u,z,e) &= \frac{1}{n}\sum_{i=1}^n \mathbb{E}_{q(\mathbf{x}_i, | \mathbf{x}_{<i}, u, z, e)} D(\mathbf{x}_i, \mathbf{u}_i). \end{aligned} \tag{57}$$

Applying Lemma 3, taking $W_0 = (z,e)$, $W_i = (\mathbf{x}_i, \mathbf{u}_i)$ for $i = 1, \ldots, n$, we obtain by a direct application of the Markov inequality that

$$\begin{aligned} \sum_{(z,u,e) \in Az_1^{\delta_{Az}}} q(z,u,e) &\geq 1 - \epsilon_{Az1} \\ \sum_{(z,e) \in Az_2^{\mu_1}(u)} q(z,e|u) &\geq 1 - \epsilon_{Az2}. \end{aligned} \tag{58}$$

To elaborate, we get from Lemma 3 that

$$\begin{aligned} &\Pr_{(x,u,z,e) \sim q(x,u,z,e)} \left(\bar{L}_n(x,u,z,e) \geq L_n(x,u) + \delta_{Az}\right) \leq \epsilon_{Az1}^2 \\ &\Pr_{(z,u,e) \sim q(z,u,e)} [\Pr_{x \sim q(x|z,u,e)} \left(\bar{L}_n(x,u,z,e) \geq L_n(x,u) + \delta_{Az}\right) \\ &\qquad \geq \epsilon_{Az1}] \leq \epsilon_{Az1} \end{aligned} \tag{59}$$

and the second inequality in Eq.(58) is obtained similarly.

Also, as stated previously we define the sets ACC_1 and ACC_2 as the sets of (x,u) for which the tests in the protocol are passed, i.e.,

$$\begin{aligned}\text{ACC}_1 &:= \{(x,u) : L_n(x,u) \leq \delta\} \\ \text{ACC}_2 &:= \{(x,u) : S_n(x,u) \geq \mu_1\},\end{aligned} \tag{60}$$

and the set $\text{ACC} = \text{ACC}_1 \cap \text{ACC}_2$ of (x,u) for which both tests in the protocol are passed. Let us also define

$$\text{ACC}_u := \{x : (x,u) \in \text{ACC}\}. \tag{61}$$

We are now ready to formulate the following lemma.

Lemma 7. *Consider the measure $q(x,z,u,t,e)$ satisfying Eq.(22). For constant $\delta_1 > 0$, we have that*

$$\begin{aligned}&\Pr_{\sim q(z,u,e|ACC)}\left(\max_x q(x|z,u,e,ACC) \leq \sqrt{\frac{\delta_1}{q(ACC)}}\right) \\ &\quad \geq 1 - \sqrt{\frac{\delta_1}{q(ACC)}}.\end{aligned} \tag{62}$$

Proof. Let us write

$$\begin{aligned}&\sum_{z,u,e} q(z,u,e|\text{ACC}) \max_x q(x|z,u,e,\text{ACC}) \\ &= \sum_{(z,u,e)\notin Az_1^{\delta_{Az}}} q(z,u,e|\text{ACC}) \max_x q(x|z,u,e,\text{ACC}) \\ &\quad + \sum_{(z,u,e)\in Az_1^{\delta_{Az}}} q(z,u,e|\text{ACC}) \max_x q(x|z,u,e,\text{ACC}).\end{aligned} \tag{63}$$

and bound the two terms separately. The first term can be simply bounded as

$$\begin{aligned}&\sum_{(z,u,e)\notin Az_1^{\delta_{Az}}} q(z,u,e|\text{ACC}) \max_x q(x|z,u,e,\text{ACC}) \\ &\overset{\max_x q(x|z,u,e,\text{ACC})\leq 1}{\leq} \sum_{(z,u,e)\notin Az_1^{\delta_{Az}}} q(z,u,e|\text{ACC}) \\ &\overset{q(z,u,e,\text{ACC})\leq q(z,u,e)}{\leq} \sum_{(z,u,e)\notin Az_1^{\delta_{Az}}} \frac{q(z,u,e)}{q(\text{ACC})} \\ &\overset{Eq.(58)}{\leq} \sum_u \frac{\epsilon_{Az1}}{q(\text{ACC})}.\end{aligned} \tag{64}$$

For the second term, with $(z,u,e) \in Az_1^{\delta_{Az}}$, we have that for fixed u, $(z,e) \in Az_1^{\delta_{Az}}(u)$. We therefore split the second term as

$$\begin{aligned}&\sum_{(z,u,e)\in Az_1^{\delta_{Az}}} q(z,u,e|\text{ACC}) \max_x q(x|z,u,e,\text{ACC}) \\ &= \sum_{u\ (z,e)\in Az_1^{\delta_{Az}}(u)\cap Az_2^{\mu_1}(u)} q(z,u,e|\text{ACC}) \max_x q(x|z,u,e,\text{ACC}) + \sum_{u\ (z,e)\in Az_1^{\delta_{Az}}(u)\cap \left(Az_2^{\mu_1}(u)\right)^c} q(z,u,e|\text{ACC}) \max_x q(x|z,u,e,\text{ACC}),\end{aligned} \tag{65}$$

where $(Az_2^{\mu_1}(u))^c$ denotes the complement of the set $Az_2^{\mu_1}(u)$. Let us first consider the case when $(z,e) \in Az_1^{\delta_{Az}}(u) \cap Az_2^{\mu_1}(u)$, i.e., $(z,e) \in Az(u)$. We define the sets

$$\begin{aligned}X_{g1}^{(z,u,e)} &= \{x : \bar{L}_n(x,u,z,e) \leq L_n(x,u) + \delta_{Az}\}, \\ X_{g2}^{(z,u,e)} &= \{x : \overline{S}_n(x,u,z,e) \geq S_n(x,u) - \frac{\mu_1}{2}\},\end{aligned} \tag{66}$$

and the complements $\left(X_{g1}^{(z,u,e)}\right)^c, \left(X_{g2}^{(z,u,e)}\right)^c$.

By the definition of $Az_1^{\delta_{Az}}(u)$, for $(z,e) \in Az_1^{\delta_{Az}}(u)$ and $x \in \left(X_{g1}^{(z,u,e)}\right)^c$, we have

$$q(x|z,u,e) \leq \epsilon_{Az1} \tag{67}$$

for $\epsilon_{Az1} = 2e^{-n\frac{1}{4}\delta_{Az}^2}$. Similarly, by the definition of $Az_2^{\mu_1}(u)$, for $(z,e) \in Az_2^{\mu_1}(u)$ and $x \in \left(X_{g2}^{(z,u,e)}\right)^c$, we

have

$$q(x|z,u,e) \leq \epsilon_{Az2} \tag{68}$$

for $\epsilon_{Az2} = 2e^{-n\frac{\mu_1^2}{16}}$. Therefore, for $(z,e) \in Az(u)$ and $x \in \left(X_{g1}^{(z,u,e)} \cap X_{g2}^{(z,u,e)}\right)^c \cap \text{ACC}_u$, we have that

$$q(x|z,u,e) \leq \epsilon_{Az1} + \epsilon_{Az2}. \tag{69}$$

Now let us look at the case when $(z,e) \in Az(u)$ and $x \in \left(X_{g1}^{(z,u,e)} \cap X_{g2}^{(z,u,e)}\right) \cap \text{ACC}_u$. By the definition of ACC_1, we have $L_n(x,u) \leq \delta$, and by the definition of $X_{g1}^{(z,u,e)}$ we have that

$$\bar{L}_n(x,u,z,e) \leq \delta + \delta_{Az}. \tag{70}$$

By Lemma 4, for at least $\mu_2 n$ positions i where $\mu_2 = 1 - \sqrt{\delta + \delta_{Az}}$, there is

$$\mathbb{E}_{q(\mathbf{x}_i,\mathbf{u}_i|\mathbf{x}_{<i},\mathbf{u}_{<i},z,e)} B(\mathbf{x}_i,\mathbf{u}_i) \leq \sqrt{\delta + \delta_{Az}} = \sqrt{2\delta}, \tag{71}$$

where we have simply set $\delta_{Az} = \delta$ for constant $\delta > 0$. Therefore, by Lemma 2, at these $\mu_2 n$ positions i, we have that for the particular input and output pair $\mathbf{u}_i = \mathbf{u}^*$ and $\mathbf{x}_i = \mathbf{x}^*$

$$q_{x_{<i},u_{<i},z,e}(\mathbf{x}_i = \mathbf{x}^*|\mathbf{u}_i = \mathbf{u}^*) \leq \frac{1}{4}\left(3 + \frac{2\sqrt{2\delta}}{(\frac{1}{2}-\epsilon)^8}\right). \tag{72}$$

Note that we will choose δ such that

$$\frac{1}{4}\left(3 + \frac{2\sqrt{2\delta}}{(\frac{1}{2}-\epsilon)^8}\right) < 1$$
$$\text{i.e., } 0 < \delta < \frac{(\frac{1}{2}-\varepsilon)^{16}}{8} \tag{73}$$

to have the above probability bounded below unity. Similarly, by the definition of ACC_2, $S_n(x,u) \geq \mu_1$, and by the definition of $X_{g2}^{(z,u,e)}$, we have that

$$\overline{S}_n(x,u,z,e) \geq \frac{\mu_1}{2}. \tag{74}$$

By Lemma 5, for at least $\mu_3 n$ positions i, where $\mu_3 = \frac{\mu_1 - 2\kappa}{2(1-\kappa)}$ for fixed $\kappa > 0$, we have

$$q_{\mathbf{x}_{<i},\mathbf{u}_{<i},z,e}(\mathbf{x}_i = \mathbf{x}^*|\mathbf{u}_i = \mathbf{u}^*) \geq \kappa. \tag{75}$$

Therefore, for $(z,e) \in Az(u)$ and $x \in \left(X_{g1}^{(z,u,e)} \cap X_{g2}^{(z,u,e)}\right) \cap \text{ACC}_u$, we have that there are at least $\mu_4 n$ positions i with $\mu_4 = (\mu_3 + \mu_2 - 1)$ for which

$$q_{\mathbf{x}_{<i},\mathbf{u}_{<i},z,e}(\mathbf{x}_i|\mathbf{u}_i = \mathbf{u}^*) \leq \gamma \tag{76}$$

for $\mathbf{x}_i = \mathbf{x}^*$ as well as $\mathbf{x}_i \neq \mathbf{x}^*$. Here,

$$\gamma = \max\left\{(1-\kappa), \frac{1}{4}\left(3 + \frac{2\sqrt{2\delta}}{(\frac{1}{2}-\epsilon)^8}\right)\right\}. \tag{77}$$

In order to have $\mu_4 > 0$, i.e., $\mu_3 + \mu_2 > 1$ we will choose constant $\delta > 0$ such that

$$\frac{\mu_1 - 2\kappa}{2(1-\kappa)} - \sqrt{2\delta} > 0,$$
$$\text{i.e., } \delta < \frac{1}{2}\left[\frac{\mu_1 - 2\kappa}{2(1-\kappa)}\right]^2. \tag{78}$$

Combining Eq. (73) and Eq.(78) we have that

$$\delta < \min\left\{\frac{(\frac{1}{2}-\varepsilon)^{16}}{8}, \frac{1}{2}\left[\frac{\mu_1 - 2\kappa}{2(1-\kappa)}\right]^2\right\} \tag{79}$$

Therefore, for any $(z,e) \in Az(u)$ and $x \in \text{ACC}_u$, combining Eq. (69) and Eq.(76) we have from Lemma 6 that

$$\begin{aligned}\max_x q(x|z,u,e,\text{ACC}) &= \frac{\max_{x\in\text{ACC}_u} q(x|z,u,e)}{q(\text{ACC}|z,u,e)} \\ &\leq \frac{\max\{\epsilon_{Az1} + \epsilon_{Az2}, \gamma^{\mu_4 n}\}}{q(\text{ACC}|z,u,e)}.\end{aligned} \tag{80}$$

From the above considerations, we can bound

$$\begin{aligned}&\sum_{\substack{u \\ (z,e)\in Az(u)}} q(z,u,e|\text{ACC}) \max_x q(x|z,u,e,\text{ACC}) \\ &\overset{\text{Eq. (80)}}{\leq} \sum_{\substack{u \\ (z,e)\in Az(u)}} q(z,u,e|\text{ACC}) \frac{\max\{\epsilon_{Az1} + \epsilon_{Az2}, \gamma^{\mu_4 n}\}}{q(\text{ACC}|z,u,e)} \\ &\leq \max\{\epsilon_{Az1} + \epsilon_{Az2}, \gamma^{\mu_4 n}\} \sum_{(z,u,e)} \frac{q(z,u,e)}{q(\text{ACC})} \\ &\leq \frac{\max\{\epsilon_{Az1} + \epsilon_{Az2}, \gamma^{\mu_4 n}\}}{q(\text{ACC})}.\end{aligned} \tag{81}$$

We can also simply bound

$$\sum_{\substack{u \\ (z,e)\in Az_1^{\delta_{Az}}(u)\cap\left(Az_2^{\mu_1}(u)\right)^c}} q(z,u,e|\mathrm{ACC}) \max_x q(x|z,u,e,\mathrm{ACC})$$

$$\leq \sum_{\substack{u \\ (z,e)\in Az_1^{\delta_{Az}}(u)\cap\left(Az_2^{\mu_1}(u)\right)^c}} q(z,u,e|\mathrm{ACC}) \overset{q(z,u,e,\mathrm{ACC})\leq q(z,u,e)}{\leq} \sum_{\substack{u \\ (z,e)\in\left(Az_2^{\mu_1}(u)\right)^c}} \frac{q(u)q(z,e|u)}{q(\mathrm{ACC})} \overset{Eq.(58)}{\leq} \frac{\epsilon_{Az2}}{q(\mathrm{ACC})}. \quad (82)$$

Inserting the bounds from Eqs. (81) and (82) into Eq.(65) gives

$$\sum_{(z,u,e)\in Az_1^{\delta_{Az}}} q(z,u,e|\mathrm{ACC}) \max_x q(x|z,u,e,\mathrm{ACC}) \leq \frac{\epsilon_{Az1}+2\epsilon_{Az2}+\gamma^{\mu_4 n}}{q(\mathrm{ACC})} \quad (83)$$

Finally, inserting the bounds from Eqs.(64) and (83) into Eq. (63) gives

$$\sum_{(z,u,e)} q(z,u,e|\mathrm{ACC}) \max_x q(x|z,u,e,\mathrm{ACC}) \leq \frac{2(\epsilon_{Az1}+\epsilon_{Az2})+\gamma^{\mu_4 n}}{q(\mathrm{ACC})} \quad (84)$$

Applying Markov inequality, setting $\delta_1 = 2(\epsilon_{Az1} + \epsilon_{Az2}) + \gamma^{\mu_4 n}$, we get that

$$\Pr_{\sim q(z,u,e|\mathrm{ACC})}\left(\max_x q(x|z,u,e,\mathrm{ACC}) \leq \sqrt{\frac{\delta_1}{q(\mathrm{ACC})}}\right) \geq 1-\sqrt{\frac{\delta_1}{q(\mathrm{ACC})}}. \quad (85)$$

This completes the proof. □

We now note the following lemma which follows from the assumptions stated in the text (for a proof see [8])

Lemma 8. *For any probability distribution $q(x,z,u,t,e)$ satisfying Eq.(22) it holds that*

$$q(x|z,u,t,e,ACC) = q(x|z,u,ACC). \quad (86)$$

We use Lemma 8 along with Lemma 7 to obtain the following theorem whose proof follows a similar statement in [8] showing that either the tests in the protocol are passed with vanishing probability or we obtain $|S| = 2^{\Omega(n^{1/4})}$ secure random bits.

Theorem 9. *Suppose we are given $\epsilon > 0$. For fixed $\mu_1 > 0$, $0 < \kappa < \frac{\mu_1}{2}$, set $\delta > 0$ such that*

$$\delta < \min\left\{\frac{(\frac{1}{2}-\varepsilon)^{16}}{8}, \frac{1}{2}\left[\frac{\mu_1-2\kappa}{2(1-\kappa)}\right]^2\right\} \quad (87)$$

Then for any probability distribution $p_w(x,z,u,t,e)$ satisfying Eq.(22) there exists an extractor Ext producing $Ext(x,t) = s$ with $|S| = 2^{\Omega(n^{1/4})}$ values, such that

$$d_c \cdot p(ACC) \leq 2^{-\Omega(n^{1/4})}, \quad (88)$$

where d_c is given by Eq. (8).

PASSING THE TESTS WITH QUANTUM BOXES

Finally, we check that for suitable parameters δ and μ_1 both tests in the protocol are passed with the use of good quantum boxes by the honest parties.

Generalized Chernoff bound for Santha-Vazirani sources

The final part of the proof is to show that if the honest parties use good quantum boxes, the tests in the protocol are passed with high probability. We first show that the Santha-Vazirani source satisfies an exponential concentration property given by the following generalized Chernoff bound, which will imply that the second test in the protocol is feasible, i.e., that in a linear fraction of the runs the setting $\mathbf{u}^*$ appears.

Theorem 10. ***(Generalized Chernoff bound)****[33, 34] Let X_i for $i \in [n]$ be Boolean random variables such that for some $0 \leq \zeta \leq 1$, we have that, for every subset $S \subseteq [n]$ $\Pr[\wedge_{i\in S} X_i = 1] \leq \zeta^{|S|}$. Then, for any $0 \leq \zeta \leq \gamma \leq 1$*

$$\Pr\left[\sum_{i=1}^n X_i \geq \gamma n\right] \leq e^{-nD(\gamma||\zeta)}, \quad (89)$$

where $D(\cdot||\cdot)$ is the relative entropy function. In particular $D(\gamma||\zeta) \geq 2(\gamma-\zeta)^2$.

We show now that the SV source satisfies the assumption of the above theorem, i.e., that probability of not obtaining the input $\mathbf{u}^*$ in a subset of size k is upper bounded by ζ^k for $\zeta = \left[1-\left(\frac{1}{2}-\epsilon\right)^{2m}\right]$ with $2m$ being the number of bits the two parties need to choose a single $\mathbf{u}$ ($2m = 2\lceil\log 9\rceil = 8$ for the Bell inequality we consider).

Lemma 11. *For any non-empty subset of k indices $(i_1, ..., i_k) \subseteq [n]$, and n consecutive instances of random variable U chosen according to measure ν using $2mn$ bits from an ϵ-SV source (where $2m$ is the number of bits required to choose a single instance $\boldsymbol{u}$), for any fixed $\boldsymbol{u}^*$ in the range of U, we have*

$$Pr_{\sim\nu}(\boldsymbol{u}_{i_1} \neq \boldsymbol{u}^*, \ldots, \boldsymbol{u}_{i_k} \neq \boldsymbol{u}^*) \leq \left[1 - \left(\frac{1}{2} - \epsilon\right)^{2m}\right]^k \tag{90}$$

Proof. Let us assume, w.l.o.g. that $i_k \geq i_{k-1} \geq ... \geq i_1$. We have

$$\begin{aligned}
&\underset{\sim\nu}{\Pr}(\mathbf{u}_{i_1} \neq \mathbf{u}^*, \ldots, \mathbf{u}_{i_k} \neq \mathbf{u}^*) \\
&= \sum_{\{\mathbf{u}_{i_j}\}: i_j \notin \{i_1,\ldots,i_k\}} \underset{\sim\nu}{\Pr}(\mathbf{u}_1, \ldots, \mathbf{u}_{i_1} \neq \mathbf{u}^*, \ldots, \mathbf{u}_{i_k} \neq \mathbf{u}^*, \ldots, \mathbf{u}_n) \\
&= \sum_{\{\mathbf{u}_{i_j}\}: i_j \notin \{i_1,\ldots,i_k\}} \underset{\sim\nu}{\Pr}(\mathbf{u}_1) \underset{\sim\nu}{\Pr}(\mathbf{u}_{i_1} \neq \mathbf{u}^* | \mathbf{u}_1, \ldots, \mathbf{u}_{i_1-1}) \ldots \underset{\sim\nu}{\Pr}(\mathbf{u}_{i_k} \neq \mathbf{u}^* | \mathbf{u}_1, \ldots, \mathbf{u}_{i_k-1}) \ldots \underset{\sim\nu}{\Pr}(\mathbf{u}_n | \mathbf{u}_1, \ldots, \mathbf{u}_{n-1}) \\
&\leq \left[1 - \left(\frac{1}{2} - \epsilon\right)^{2m}\right]^k
\end{aligned} \tag{91}$$

The last inequality is obtained by noting that for terms with $i_j \in \{i_1, \ldots, i_k\}$, by the definition of the SV source $P(\mathbf{u}_{i_j} \neq \mathbf{u}^* | \mathbf{u}_1, \ldots, \mathbf{u}_{i_j-1}) \leq \left[1 - \left(\frac{1}{2} - \epsilon\right)^{2m}\right]$ with $2m$ being the number of bits required to obtain any input $\mathbf{u}$, and for the terms with $i_j \notin \{i_1, \ldots, i_k\}$, the sum over $\mathbf{u}_{i_j}$ gives unity by normalization. □

Consider the random variable X_i defined as

$$X_i := \begin{cases} 1 & : \mathbf{u}_i \neq \mathbf{u}^* \\ 0 & : \text{otherwise} \end{cases}$$

for $\mathbf{u}_i$ chosen using the SV source $\nu(\cdot)$. Theorem 10 together with Lemma 11 gives that

$$\Pr\left[\sum_{i=1}^{n} X_i \geq \gamma n\right] \leq e^{-2n(\gamma-\zeta)^2}, \tag{92}$$

or equivalently

$$\Pr\left[\sum_{i=1}^{n} X_i < \gamma n\right] \geq 1 - e^{-2n(\gamma-\zeta)^2}, \tag{93}$$

for $\zeta = \left[1 - \left(\frac{1}{2} - \epsilon\right)^{2m}\right]$ and $0 \leq \zeta \leq \gamma \leq 1$. For $\tilde{U}(u) := \{i : \mathbf{u}_i = \mathbf{u}^*\}$ and $Ch := \{u : |\tilde{U}(u)| \geq \mu_5 n\}$ for some constant $\mu_5 > 0$, Eq. (93) gives that

$$\sum_{u \in Ch} \nu(u) \geq 1 - e^{-2n(1-\mu_5-\zeta)^2}. \tag{94}$$

Therefore, we obtain that with probability $1 - e^{-2n(1-\mu_5-\zeta)^2}$, $\mathbf{u}_i = \mathbf{u}^*$ for a fraction μ_5 of the n runs. We note that with the use of the state and measurements from Eqs.(25), (26) and (27), we obtain a box $\{P_q(\mathbf{x}|\mathbf{u})\}$ that achieves maximal violation of the Bell inequality, i.e., $\mathbf{B}.\{P_q(\mathbf{x}|\mathbf{u})\} = 0$ and also has $P_q(\mathbf{x} = \mathbf{x}^* | \mathbf{u} = \mathbf{u}^*) = \frac{1}{16}$. Therefore, for suitably chosen $\delta, \mu_1 > 0$ the two tests in the protocol are passed with high probability with the use of good quantum boxes.