

Robust amplification of Santha-Vazirani sources with three devicesPiotr Mironowicz,^{1,2} Rodrigo Gallego,³ and Marcin Pawłowski^{4,5}¹*Department of Algorithms and System Modelling, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Gdańsk 80-233, Poland*²*National Quantum Information Centre in Gdańsk, Sopot 81-824, Poland*³*Dahlem Center for Complex Quantum Systems, Freie Universitaet Berlin, 14195 Berlin, Germany*⁴*Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*⁵*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*

(Received 15 April 2014; published 23 March 2015)

We demonstrate that amplification of arbitrarily weak randomness is possible using quantum resources. We present a randomness amplification protocol that involves Bell experiments. We find a Bell inequality that can amplify arbitrarily weak randomness and give a detailed analysis of the protocol involving it. Our analysis includes finding a sufficient violation of the Bell inequality as a function of the initial quality of randomness. It has a very important property that for any quality the required violation is strictly lower than possible to obtain using quantum resources. Among other things, this means that the protocol takes a finite amount of time to amplify arbitrarily weak randomness.

DOI: [10.1103/PhysRevA.91.032317](https://doi.org/10.1103/PhysRevA.91.032317)

PACS number(s): 03.67.Ac, 03.65.Ud

I. INTRODUCTION

The application of the laws of quantum mechanics allows us to perform tasks impossible in classical information theory. The two most prominent examples are quantum computation [1] and cryptography [2]. Recently, another area where quantum information theory makes new things possible has been found. It is the amplification of weak randomness [3]. This procedure not only has obvious practical applications, but also sheds light on fundamental issues such as the completeness of quantum mechanics. However, so far the possibility of randomness amplification has been demonstrated only under very restrictive conditions. To explain what they are we must first rigorously state the problem.

We are given a source, which generates a sequence of bits $\vec{x} = x_0, x_1, \dots$ parametrized by a single constant ϵ . The bits may be correlated with each other and also with an agent, the eavesdropper, that holds a classical variable e . However, there is a certain intrinsic randomness in each of the bits quantified by ϵ in

$$\frac{1}{2} - \epsilon \leq P(x_i = 0 | x_0, \dots, x_{i-1}, e) \leq \frac{1}{2} + \epsilon \forall i. \quad (1)$$

If (1) holds we say that the sequence \vec{x} (or the source) is ϵ free. Here ϵ is called the bias of the source. A bias $\epsilon = 0$ corresponds to the case where the output of the source is perfectly random. When $\epsilon = \frac{1}{2}$ we cannot say anything about the source and it can be even deterministic. The aim of randomness amplification is to use some postprocessing of the sequence \vec{x} to generate another sequence \vec{y} that is ϵ' free and $\epsilon' < \epsilon$.

The source of randomness described above is usually referred to as a Santha-Vazirani source after the authors of [4], where they proved that classical randomness amplification is impossible. In their groundbreaking paper Colbeck and Renner [3] showed that it is not true in the quantum case. Their idea is based on performing a Bell experiment and applying a hashing function to the measurement outcomes. However, the protocol that they have presented works only if the source of randomness is almost perfect to begin with, more precisely, if the source is ϵ free with $\epsilon < 0.086$.

Recently, more papers on this issue appeared, aiming at amplification of any source with $\epsilon < \frac{1}{2}$. Unfortunately, they work only in the noiseless case [5], which is impossible in realistic experimental situations, require an unbounded number of devices [6], or have a zero rate of amplification [7,8]. These protocols assume only no signaling, but for the reasons mentioned fail to perform practically usable amplification.

Therefore, it remained an open question whether the amplification of arbitrarily weak randomness under realistic circumstances was possible. In this paper we answer this question affirmatively. We do so by presenting an amplification protocol that is based on the Mermin inequality [9]. It works for any $\epsilon < \frac{1}{2}$ and can tolerate a finite amount of noise and experimental imperfection depending on ϵ .

The aim of the paper is not to study the foundations of the quantum theory but the details of amplifying randomness in practice. Therefore, contrary to the majority of papers on the subject [3,5–8,10], we require the vendor of the devices to be bound by laws of quantum mechanics instead of only no signaling. This enables us to develop a simple, noise-tolerant protocol with only a few, three to be precise, reusable devices.¹

Recently, a protocol that is able to amplify any randomness (not only from Santha-Vazirani sources) was proposed [11]. While it is clearly more general than ours it is not specified how much experimental imperfection can be tolerated and the number of devices required for the operation is of the order of 10^7 [12], which is much more than the three devices required by ours.

II. THE TASK OF RANDOMNESS AMPLIFICATION

The main problem with randomness amplification lies in our almost complete ignorance about the inner workings of the source. It provides us with an infinite sequence of bits, yet all we know about it is expressed by a single number ϵ . For

¹By reusable we mean devices that can be used many times in a single run of the protocol.

every ϵ there exists an infinite number of ϵ -free sources and, while good randomness amplification procedures would work well for a vast majority of them, there will always be some that any given procedure fails to amplify. This is the essence of the Santha-Vazirani proof.

Another problem is that, since we are interested only in the quality of the sequences, we do not have access to any independent source of randomness. In other words, we assume that all the sources of randomness that we have access to can be correlated and form one big Santha-Vazirani source. Therefore, without loss of generality, any classical randomness amplification protocol can be reduced to applying a deterministic function to the output of the source to generate a new sequence: $\vec{y} = f(\vec{x})$.

Can quantum mechanics help? After all, it is a theory built on intrinsic randomness. On the other hand, we cannot simply use a quantum random number generator because, under our assumptions, it is also only ϵ free. The solution lies in Bell inequalities. They have already been found useful in the related problem of device-independent randomness expansion [13–18]. Briefly, the idea is to use the sequence \vec{x} to choose the settings of a Bell experiment and consider the outcomes as a new sequence \vec{y} . Based on these sequences, the violation of the Bell inequality is estimated and its value tells us if the amplification was successful or not. Let us elucidate.

A. Biased nonlocal games

One way of interpreting Bell inequalities is to think of them as nonlocal games. Let us take the Clauser-Horne-Shimony-Holt (CHSH) inequality [19] as an example. If we treat it as a game, then we have a team of two players, Alice and Bob, playing against a referee. The referee sends bits a and b to Alice and Bob, respectively, and the players, without communication, announce their respective binary answers A and B . They win if $A \oplus B = ab$. Usually, it is assumed that the probability distribution of the inputs is uniform, i.e., $p(a,b) = \frac{1}{4}$. Under this condition the maximal winning probability for the parties having only classical resources is $\frac{3}{4}$, while entanglement allows them to reach the success probability up to $\frac{1}{2}(1 + \frac{1}{\sqrt{2}})$.

If we are to use ϵ -free string of bits as a source of settings, we cannot assume that the distribution of inputs is uniform anymore. Our game becomes a biased one, at least from the eavesdropper's point of view, with the success probability

$$P_s = \sum_{a,b} p(a,b|e)P(A \oplus B = ab|a,b,e), \quad (2)$$

where e is a variable held by the eavesdropper. The values of P_s for classical and quantum strategies for any distribution $p(a,b|e)$ are greater than their counterparts from the unbiased case. They have been found in [20]. For every Bell inequality, the larger the observed value of P_s is the more random the local outcomes must be. One can use the hierarchy of semidefinite programs (SDPs) from [21] to efficiently find a lower bound on this randomness for any given distribution $p(a,b|e)$. Unfortunately, we do not know this probability distribution. We cannot even estimate it because it may be

different in each round of the experiment and the choice of the distribution may be correlated with variable e held by the eavesdropper. The only thing that we know about $p(a,b|e)$ is that both bits a and b come from an ϵ -free source. However, the impossibility of the direct application of SDPs is not the last of the obstacles.

Let us assume that our ϵ -free source is always biased towards 0, i.e., for all i , $P(x_i = 0|x_0, \dots, x_{i-1}, e) = \frac{1}{2} + \epsilon$. Even if Alice and Bob know this and adopt their states and measurements accordingly, there is a value of ϵ above which quantum and classical P_s are the same. One can use the results from [20] to find this value to be $\epsilon_{\text{crit}} = \frac{1}{\sqrt{2}} - \frac{1}{2}$. In addition, if a classical model that gives certain success probability in a nonlocal game exists, then there is also a deterministic one achieving it [22]. Therefore, whenever the parties have a source with ϵ above ϵ_{crit} , whatever success probability they observe, their outcomes can be deterministic. Fortunately, the value of ϵ_{crit} depends on the Bell inequality chosen for the protocol. Therefore, our task is also to find Bell inequalities that are better for the purposes of randomness amplification than the CHSH inequality or the ones studied in [3].

B. Protocol: Notation and assumptions

The protocol of amplification of weak randomness considers two devices: the source of randomness (SOR) and the quantum box (QB). These two devices are operated by honest players, however they may have been manufactured by dishonest agents as long as they fulfill the assumptions that we make more explicit. The task of randomness amplification is performed in competition with a dishonest player, the eavesdropper, having a device that generates the random variable e . The goal is to generate a final bit y that is ϵ' free with respect to the eavesdropper, that is, $\frac{1}{2} - \epsilon' \leq P(y|e) \leq \frac{1}{2} + \epsilon'$.

In the scenario that we are considering, the eavesdropper, after preparing the SOR and QB, is quite passive. The whole randomness amplification procedure is performed in a shielded laboratory (see Fig. 3) and no information is sent outside. The eavesdropper does not even know at which time the protocol is run. This means that if one has any quantum side information (a system entangled with the devices one has produced), one learns the same amount if one measures one's system after or before the protocol. In fact, nothing changes even if one measures it before one gives the devices to the players. Therefore, in this scenario there is no difference between eavesdroppers with classical and quantum side information and our protocol is secure against both. Note that our protocol differs from the cryptographic scenario in that, after the amplification process, we do not need to keep the generated bits secret since we are interested only in their indeterminacy, not privacy.

The SOR is assumed to fulfill the assumptions of a Santha-Vazirani source, that is, the honest players can produce an arbitrarily large number of bits \vec{x} according to a probability distribution that fulfills (1). The QB receives as inputs k classical bits and produces k classical bits. The QB is reused an arbitrarily large number of times. Let us denote by $\vec{a}_j \in \{0,1\}^k$ and $\vec{A}_j \in \{0,1\}^k$ the inputs and outputs of the j th run,

respectively.² Let us also denote by \vec{X}_j all the inputs and outputs generated until the j th run. The behavior of the QB in the j th run on a given instance of e, \vec{x} , and \vec{X}_{j-1} is determined by the probability distribution $P(\vec{A}_j|\vec{a}_j, \vec{x}, \vec{X}_{j-1}, e)$. We define the success probability of the j th round as

$$P_s^j = \sum_{\vec{a}_j} P(F[\vec{a}_j, \vec{A}_j] = 0|\vec{a}_j, \vec{X}_{j-1}, \vec{x}, e)P(\vec{a}_j|\vec{X}_{j-1}, e, \vec{x}), \quad (3)$$

where $F[\vec{a}_j, \vec{A}_j] = 0$ is the function that determines the Bell inequality employed [cf. (2)]. Also, we refer to the average success probability of N runs of the QB as $P_{\text{ave}} := \frac{1}{N} \sum_{j=1}^N P_s^j$.

Now we elucidate the two assumptions about the QB.

(i) *The Markov condition.* We assume that given a value of e and the inputs \vec{a} , the output probability distribution of the QB is independent of the bits generated by the SOR. That is,

$$\begin{aligned} P(\vec{A}_1, \dots, \vec{A}_N|\vec{a}_1, \dots, \vec{a}_N, \vec{x}, e) \\ = P(\vec{A}_1, \dots, \vec{A}_N|\vec{a}_1, \dots, \vec{a}_N, e). \end{aligned} \quad (4)$$

Note that this assumption does not imply at all that the SOR and QB are uncorrelated. It just states that they have to be correlated only through the random variable e possessed by the eavesdropper. In this way, the QB is for every e a well-defined channel applicable to the bits \vec{x} generated by the SOR. Indeed, in our protocol the inputs \vec{a} are generated by the SOR, so $\vec{a} = (x_1, \dots, x_N)$. Let us denote by \vec{h} the rest of the bits generated by the SOR that are not explicitly used as inputs of the QB. Then the Markov condition (4) implies that

$$\begin{aligned} P(\vec{A}_1, \dots, \vec{A}_N, \vec{h}|\vec{a}_1, \dots, \vec{a}_N, e) \\ = P(\vec{A}_1, \dots, \vec{A}_N|\vec{a}_1, \dots, \vec{a}_N, e) \times P(\vec{h}|\vec{a}_1, \dots, \vec{a}_N, e). \end{aligned} \quad (5)$$

(ii) *Quantum behavior.* As stated in the Introduction, we assume that the devices fulfill the rules of quantum mechanics. Therefore, we assume that for all j there exist a k -partite quantum state $\rho(e\vec{X}_{j-1})$ and measurement operators $M_{A_j}^{\vec{a}_j}(e, \vec{X}_{j-1}) \equiv \bigotimes_{i=1}^k M_{A_i}^{\vec{a}_i}(e, \vec{X}_{j-1})$, with

$\sum_{A_i} M_{A_i}^{\vec{a}_i}(e, \vec{X}_{j-1}) = \mathbb{I}$ for all i , such that

$$P(\vec{A}_j|\vec{a}_j, \vec{X}, e) = \text{tr}[\rho(e\vec{X})M_{A_j}^{\vec{a}_j}(e, \vec{X})]. \quad (6)$$

C. Sketch of the protocol and proof

The protocol of randomness amplification is based on the fact that a probability distribution with a sufficiently large success probability for a certain Bell game can be certified to possess some intrinsic randomness. We employ the SOR to generate the inputs of the QB at every run. The remaining bits generated by the SOR are referred to as \vec{h} . The behavior of the j th run of the QB box is characterized by $P(\vec{A}_j|\vec{a}_j, \vec{X}_{j-1}, e)$ (note that it does not depend on \vec{h} due to the

Markov assumption). In Sec. III we show that there exists a Bell inequality such that one of the bits produced by the QB can be shown to be ϵ_j free, with ϵ_j being a function of P_s^j and ϵ . More precisely,

$$\frac{1}{2} - \epsilon_j \leq P(A_j^1|\vec{a}_j, \vec{X}_{j-1}, e) \leq \frac{1}{2} + \epsilon_j, \quad (7)$$

with $\epsilon_j = g(P_s^j, \epsilon)$, where we have chosen the first of k bits A_j^1 generated by the QB in the j th run.

Unfortunately, the success probability P_s^j of each run cannot be estimated. By using the QB N times, we only have access to one event of each run; hence we deal with the estimated success probability P_{est} (the number of runs that won the game divided by the number of runs N). We cannot employ standard estimation results in nonlocality because now the distribution of measurement settings is unknown. The standard scenario [14,17,18,23] assumes that it is possible to use an estimator of the form

$$\hat{I} = \frac{1}{N} \sum_{j=1}^N \sum_{\vec{A}, \vec{a}} c_{\vec{A}, \vec{a}} \frac{\chi(\vec{A}, \vec{a})}{P(\vec{a})}. \quad (8)$$

This time the values of $P(\vec{a})$ can differ in each round in a way that cannot be predicted without knowledge of the internal working of the SOR. However, we can bound the winning probability of a virtual game (an unbiased one played with the same states and measurements) and from it obtain the bounds on the average bias of the N bits $\epsilon_{\text{ave}} := \frac{1}{N} \sum_{j=1}^N \epsilon_j$.

Clearly, bounds on the average bias of all the bits generated do not complete the proof. One may have very good bounds on the average bias, however some fraction of the bits $\{A_j^1\}_j$ may not be random at all. Hence, one cannot certify that one of them, chosen at random by employing the SOR, will possess any randomness. This approach (of using the SOR to chose some of the output bits) was used in [3,5,10]. It was slightly modified in [6], where a constant number of rounds is chosen and the SOR of the outcomes is the final value. However, if the devices are allowed to have even the tiniest imperfections, this strategy (i.e., using the SOR to pick a constant number of bits) cannot amplify sources with $\epsilon \geq \frac{2e-1}{4e+2} \approx 0.345$ regardless of the Bell inequality chosen and the level of imperfections. This is shown in Appendix B by providing an explicit classical attack. In this work, we employ a more sophisticated postprocessing based on techniques in Ref. [24] that allows one to extract a fully random bit.

III. BELL INEQUALITIES

We are considering a protocol of a certain structure, where the estimate of a winning probability in some nonlocal game is the only parameter used to check if the amplification was successful. To find a candidate for a Bell inequality to be used in randomness amplification protocol we first need to ask ourselves what properties are we looking for. To this end, let us consider one particular way of cheating.³ The measurement devices prepare an optimal classical strategy so they know in

²In the particular scenario of $k = 2$ or 3 we employ for ease of notation a_j, b_j, c_j and A_j, B_j, C_j as inputs and outputs of the j th run, respectively.

³By cheating we here mean violating Bell inequality with deterministic outcomes.

advance that for most of the messages from the referee they will produce a good answer, but they also know that for some they will fail. The devices also know for which inputs they will fail. They can be tuned to the source of randomness in such a way that the inputs for the case when the devices fail are least likely to happen. We see that the weaker the randomness, the higher the average success probability. If the randomness is very weak, the success probability is close to 1. If we want to amplify arbitrarily weak randomness, then to be certain that our device does not play this trick, the success probability with a quantum strategy has to be even higher. Obviously, it cannot be greater than 1, so we have to look for nonlocal games for which it is equal to 1.

Taking this all into account, we choose the tripartite Mermin inequality [9] as our candidate. In this scenario Alice, Bob, and Charlie each receive one input bit a, b , and c , respectively. There is a promise that $a \oplus b \oplus c = 1$. Each of them also returns a single bit denoted by A, B , and C . They win if $A \oplus B \oplus C = abc$. In the unbiased version of this game the classical success probability is $\frac{3}{4}$ and quantum mechanics allows us to reach 1.

IV. BOUNDING THE RANDOMNESS

As we mentioned before, finding lower bounds on the quality of randomness generated by playing a biased nonlocal game is highly nontrivial. Because of the promise put on the choices of the settings, one can write the success probability of a nonlocal biased game based on the tripartite Mermin inequality as

$$P_s = \sum_{a,b} p(a,b|e) P(A \oplus B \oplus C = ab|a,b,e). \quad (9)$$

Our aim is to find an upper bound on the quantity

$$P_{\max} = \max_{a,b,c,X,i,e} P(X = i|a,b,c,e), \quad (10)$$

as a function of ϵ and P_s under constraints

$$\sum_{a,b} p(a,b|e) P(A \oplus B \oplus C = ab|a,b,e) \geq P_s, \quad (11)$$

$$\frac{1}{2} - \epsilon \leq p(a|e) \leq \frac{1}{2} + \epsilon, \quad (12)$$

$$\frac{1}{2} - \epsilon \leq p(b|a,e) \leq \frac{1}{2} + \epsilon, \quad (13)$$

where $X \in \{A, B, C\}$ denotes the outcome of one of the parties. Because the conditions (11)–(13) are nonlinear we cannot use semidefinite programming to solve this problem. Moreover, we are not able to construct the expression $\sum_{a,b} p(a,b|e) P(A \oplus B \oplus C = ab|a,b,e) \geq P_s$ since the values $p(a,b|e)$ are not constant (in contrast to standard scenario with the SOR without memory).

To cope with this, let us consider what would the success probability be if an unbiased game was played using the same states and measurements. Let us define it by

$$P_s^{\text{ub}} = \frac{1}{4} \sum_{a,b} P(A \oplus B \oplus C = ab|a,b,e). \quad (14)$$

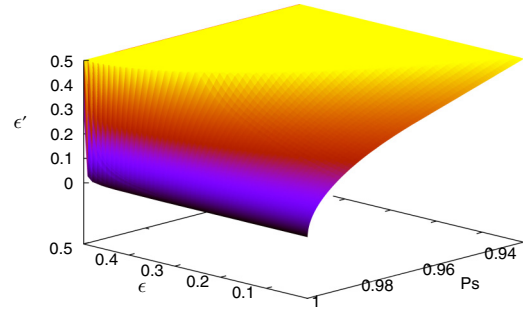


FIG. 1. (Color online) Maximal bias of the measurement outcome as a function of the weakness of randomness and success probability of winning in a nonlocal game based on the tripartite Mermin inequality. This plot can be also understood as a critical value of the success probability required to take inputs from ϵ -free source and get outcomes with bias less than ϵ' .

The fact that the same states and measurements are used for this virtual game means that the probabilities $P(A \oplus B \oplus C = ab|a,b,e)$ in formula (14) are exactly the same as in (11). We can use this to bound P_s^{ub} from below. Let $P_m = \min_{a,b} P(A \oplus B \oplus C = ab|a,b,e)$. We have that

$$P_s^{\text{ub}} \geq P_m. \quad (15)$$

The highest value of P_s that is still consistent with P_m is attained if $P(A \oplus B \oplus C = ab|a,b,e) = 1$ for all a and b except for the ones used to get P_m . Moreover, the coefficient $(a,b|e)$ in front of P_m should be as small as possible for something coming out of a Santha-Vazirani source parametrized by ϵ , i.e., $(\frac{1}{2} - \epsilon)^2$. This implies

$$\begin{aligned} P_s &\leq 1 - (\frac{1}{2} - \epsilon)^2 + (\frac{1}{2} - \epsilon)^2 P_m \\ &\leq 1 - (\frac{1}{2} - \epsilon)^2 (1 - P_s^{\text{ub}}) \end{aligned} \quad (16)$$

or, alternatively,

$$P_s^{\text{ub}} \geq 1 - \frac{1 - P_s}{(1/2 - \epsilon)^2}. \quad (17)$$

Now we can bound P_{\max} by considering only the constraint

$$\frac{1}{4} \sum_{a,b} P(A \oplus B \oplus C = ab|a,b,e) \geq P_s^{\text{ub}} \quad (18)$$

and using (17) to put a lower bound on P_s^{ub} by P_s , which is a quantity that we can experimentally estimate.

We find that one can obtain good bounds on P_{\max} already with the first intermediate level of the hierarchy $Q_{1+AB+AC+BC}$ from [21]. The main result of our analysis so far is that for any⁴ $\epsilon < \frac{1}{2}$ there exists $P_s < 1$ such that $P_{\max} < 1$. A function $g(P_s, \epsilon)$, giving a concave upper bound on \tilde{P}_{\max} and thus on P_{\max} , is plotted in Fig. 1. The critical value of $P_{\text{crit}}(\epsilon)$ such that for all $P_s > P_{\text{crit}}(\epsilon)$ we have $g(P_s, \epsilon) < \frac{1}{2}$ is shown in Fig. 2.

⁴In fact, we have numerically checked only $\epsilon \leq 0.499$, but conjecture that this is true for all $\epsilon < \frac{1}{2}$.

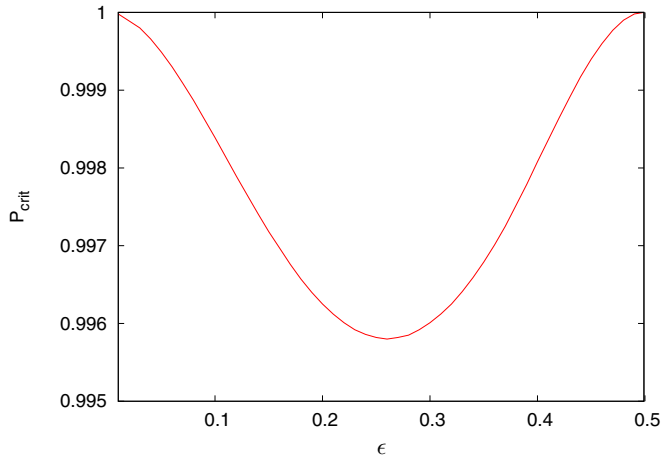


FIG. 2. (Color online) Sufficient winning probability for randomness amplification in a nonlocal game based on the tripartite Mermin inequality as a function of the sources' freedom. If P_s is above the plot it means that the bias of the final bit y is lower than that of the Santha-Vazirani (SV) source. Note that higher values of P_s are required for extremal initial ϵ . This is because if ϵ is large, the initial quantity of randomness is bad, which makes the amplification difficult. On the other hand, if ϵ is already low, then to amplify it we need to obtain an even more random bit, which is again difficult.

V. FULL RANDOMNESS AMPLIFICATION PROTOCOL

If, in every round of the experiment, the device would have the same probability of success, we could simply take the outcomes of the experiment as our final sequence A and know that each of them is ϵ' free with $\epsilon' = g(P_s, \epsilon)$. Unfortunately, we cannot assume that and have to apply some classical postprocessing. We also cannot randomly choose a single bit from the measurements outcomes like it was done in [3] because for such postprocessing amplification of randomness with $\epsilon > 0.345$ is impossible regardless of the Bell inequality chosen as a certificate.⁵ Therefore, we need to use a different protocol, but before we present it, let us clarify the task at hand.

We are given a device that is a source of randomness guaranteed to be ϵ free. We assume that the vendor of the device, which may be the eavesdropper, has access to some parameter e that influences its behavior. Moreover, any other device that we have access to (e.g., a source of entangled states) is also supplied by the same vendor and its behavior is also dependent on e . We are able to place the source of randomness and all the other devices we need in a laboratory shielded from the environment in such a way that it leaks no data to the outside world during the amplification process, especially to the said vendor. In this laboratory a single bit y is generated.⁶ We choose some target $\epsilon' < \epsilon$ and a desired probability of

⁵This claim is proved in Appendix B.

⁶If we have a procedure that allows us to generate a single bit with the required ϵ' freedom, then we can repeat the same procedure any number of times, including the bits already obtained in e to get a sequence of any length.

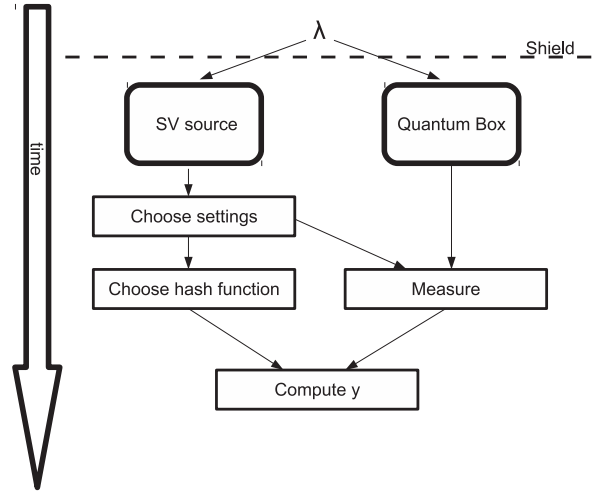


FIG. 3. Schematic diagram of the randomness amplification protocol.

success p in generating a final bit that fulfills

$$\frac{1}{2} - \epsilon' \leq P(y = 0|e) \leq \frac{1}{2} + \epsilon'. \quad (19)$$

To this end, we use the following amplification protocol.

(1) Place in a shielded laboratory an ϵ -free SOR and a QB. The latter is composed of measurement devices sharing an entangled state, designed for demonstrating violation of the tripartite Mermin inequality.

(2) Use the SOR to draw $2N$ bits for the measurement settings for the QB for N rounds of the experiment and make the measurements.

(3) Use the SOR to draw N bits representing a hashing function. Label them h_1, \dots, h_N .

(4) Calculate $y = \bigoplus_{i=1}^N h_i A_i$, where A_i is the outcome of Alice in the i th round. Then estimate the average Bell inequality violation P_{est} of the QB to compute the probability that y is ϵ' free. If it fulfills

$$g(P_{\text{est}} - r(p, N, \epsilon), \epsilon) < \frac{1}{1 + 2\epsilon} - \frac{1}{2}, \quad (20)$$

with $r(p, N) = \sqrt{-\ln(1-p)N^{-1/2}}$ and g from Fig. 1, keep y ; otherwise abort.

The protocol is schematically pictured in Fig. 3. The high probability mentioned in the last step is made explicit by the following theorem.

Theorem 1. For any $\epsilon < \frac{1}{2}$, $\epsilon' > 0$, and $p < 1$ there exists N such that in the protocol presented above the bit y is ϵ' free with a probability of at least p when $g(P_{\text{est}}, \epsilon) > \frac{1}{1+2\epsilon} - \frac{1}{2}$.

A proof is given in Appendix A.

VI. CONCLUSION

We have demonstrated that amplification of arbitrarily weak randomness is possible using quantum resources. We were able to derive the necessary bounds on the violation of Bell inequalities as a function of the quality of the randomness. These bounds are below the maximum achievable by quantum resources for arbitrarily weak initial randomness. We have also presented a protocol that uses Bell inequalities for randomness amplification and calculated all of its parameters.

We find of a particular interest the fact that the inequality we have demonstrated to perform well in randomness amplification does so only in quantum theory; it cannot amplify any randomness of any quality when only no signaling is assumed, because the adversary, though unable to make the whole output of all the parties deterministic, can always fix any single bit of it [5]. Although a different protocol based on the same inequality might work, we find it interesting that for the one presented here the difference between quantum and no-signaling theory is qualitative rather than quantitative. This result is in contrast with protocols based on other Bell inequalities where the theory of the adversary only influences the efficiency of the protocol but not the possibility of its secure execution [25].

As our paper solves an open problem it also poses some new ones. Are there any protocols more efficient than ours in terms of the ratio of random bits generated to random bits used? What is the lowest violation of the Bell inequality required for amplification of a certain ϵ source with three devices?

ACKNOWLEDGMENTS

This work was supported by United Kingdom EPSRC, FNP TEAM, NCN Grant No. 2013/08/M/ST2/00626, ERC QOLAPS, and Polish Ministry of Science and Higher Education Grant IDEAS PLUS (IdP2011 000361). SDP was implemented in Octave using the SeDuMi toolbox [26].

APPENDIX A: PROOF OF THEOREM 1

After performing steps 1–4 one has N bits A_1, \dots, A_N generated by the QB and N bits h_1, \dots, h_n generated by the SOR. The rest of the bits generated in the process, such as bits for the measurement settings or the QB outputs that are *not* employed to construct A_1, \dots, A_N , are referred to as \vec{X} for ease of notation. To summarize, let us recall the three elements that will come into play in the following proof.

(i) By the assumption on the behavior of the SOR, bits h_1, \dots, h_n fulfill

$$\frac{1}{2} - \epsilon \leq P(h_i | h_1, \dots, h_{i-1}) \leq \frac{1}{2} + \epsilon \quad \forall i \leq N.$$

(ii) The observed statistics reveal an estimated success probability P_{est} , calculated simply as the number of rounds when the parties won divided by the total number of rounds N , that fulfills Eq. (20), i.e.,

$$g(P_{\text{est}} - \sqrt{-\ln(1-p)}N^{-1/2}, \epsilon) < \frac{1}{1+2\epsilon} - \frac{1}{2},$$

where p is the probability of generating successfully the final bit with bias ϵ' (see Theorem 1).

(iii) The QB and the SOR fulfill the Markov assumption, so for any value of e ,

$$\begin{aligned} P(A_1, \dots, A_N, h_1, \dots, h_n | \vec{X}, e) \\ = P(A_1, \dots, A_N | \vec{X}, e) \times P(h_1, \dots, h_n | \vec{X}, e). \end{aligned} \quad (\text{A1})$$

The first step in the proof is to bound how much the observed average success probability P_{est} deviates from the real average probability of success $P_{\text{ave}} := \frac{1}{N} \sum_{j=1}^N P_s^j$, where P_s^j is the success probability of the j th use of the tripartite box in the QB. Note that P_s^j may indeed depend on the

previous bits generated in the QB for the $j-1$ previous runs of the QB. That is, P_s^j should be understood as the probability of success of the j th round conditioned on $A_1, \dots, A_{j-1}, \vec{X}_1, \dots, \vec{X}_{j-1}, h_1, \dots, h_n, e$. We can follow the reasoning from [14, 17, 18] and use the Azuma-Hoeffding inequality to establish that

$$\text{Prob}(P_{\text{ave}} \leq P_{\text{est}} - x) \leq \exp\left(-\frac{1}{2}x^2N\right). \quad (\text{A2})$$

Let us define P^* as the success probability fulfilling $g(P^*, \epsilon) = \frac{1}{1+2\epsilon} - \frac{1}{2}$. Then, by (20) we have that

$$P_{\text{est}} > P^* + \sqrt{-\ln(1-p)}N^{-1/2}.$$

Note that by taking $x = \sqrt{-\ln(1-p)}N^{-1/2}$ one obtains that

$$\text{Prob}(P_{\text{ave}} \leq P^*) \leq 1 - p$$

or, equivalently, with probability p it is fulfilled that $g(P_{\text{ave}}, \epsilon) \leq g(P^*, \epsilon) = \frac{1}{1+2\epsilon} - \frac{1}{2}$. For ease of presentation in the following we assume that this latter condition is fulfilled. Results obtained under this assumption can be only be certified to occur with probability p . Let us define the bias of each of the runs of the QB by

$$\frac{1}{2} - \epsilon_j \leq P(A_j | \vec{a}_j, \vec{X}_{j-1}, e) \leq \frac{1}{2} + \epsilon_j. \quad (\text{A3})$$

We can then use the concavity of the function g to derive

$$\begin{aligned} \epsilon_{\text{ave}} &= \frac{1}{N} \sum_{j=1}^N \epsilon_j \leq \frac{1}{N} \sum_{j=1}^N g(P_s^j, \epsilon) \\ &\leq g(P_{\text{ave}}, \epsilon) < \frac{1}{1+2\epsilon} - \frac{1}{2}. \end{aligned} \quad (\text{A4})$$

Let us note that this bound on the average bias allows one to place an upper bound on the probability of obtaining a certain combination of A_1, \dots, A_n . That is,

$$P(A_1, \dots, A_n | \vec{X}, e) \leq \prod_{j=1}^n \left(\frac{1}{2} + \epsilon_j\right) \leq \left(\frac{1}{2} + \epsilon_{\text{ave}}\right)^n. \quad (\text{A5})$$

Equivalently, by assumption, the SOR produces bits h_1, \dots, h_n that fulfill

$$P(h_1, \dots, h_n | \vec{X}, e) \leq \left(\frac{1}{2} + \epsilon\right)^n. \quad (\text{A6})$$

This together with (A1) will be sufficient to distill a final random bit of an arbitrarily small bias. Note that (A1) implies that conditioned on any value of \vec{X}, e , the sources producing A and h are independent. Results on distillation of random bits from independent imperfect random sources were first derived in Ref. [4]. Here we employ a more recent distillation method that is best suited for our scenario [24].

Lemma. Let us define an (N, b) source that produces N bits s_1, \dots, s_N such that $P(s_1, \dots, s_N | k) \leq 2^{-b}$. Consider two independent sources (N, b_1) and (N, b_2) producing bits s_1, \dots, s_N and p_1, \dots, p_N , respectively. The independence condition reads

$$\begin{aligned} P(s_1, \dots, s_N, p_1, \dots, p_N | k) \\ = P(s_1, \dots, s_N | k) \times P(p_1, \dots, p_N | k). \end{aligned}$$

Then the inner product $y = \bigoplus_{i=1}^N s_i \cdot p_i$ is an ϵ' -free bit, that is, $\frac{1}{2} - \epsilon' \leq P(y|k) \leq \frac{1}{2} + \epsilon'$, if

$$b_1 + b_2 \geq N + 2 + 2 \log_2 \frac{1}{\epsilon'}.$$

The lemma can be straightforwardly applied to our scenario. As derived above, the QB and SOR are two independent sources when conditioned on \vec{X}, e with bounds (A5) and (A6). This implies that they are (N, b_1) and (N, b_2) sources with

$$\begin{aligned} b_1 &= N \log_2 \left(\frac{1}{2} + \epsilon_{\text{ave}} \right)^{-1}, \\ b_2 &= N \log_2 \left(\frac{1}{2} + \epsilon \right)^{-1}. \end{aligned} \quad (\text{A7})$$

Hence, the bit $y = \bigoplus_{i=1}^N A_i \cdot h_i$ is an ϵ' -free bit [i.e., it fulfills $\frac{1}{2} - \epsilon' \leq P(y|\vec{X}, e) \leq \frac{1}{2} + \epsilon'$] as long as

$$N \log_2 \left[\left(\frac{1}{2} + \epsilon_{\text{ave}} \right)^{-1} \left(\frac{1}{2} + \epsilon \right)^{-1} \right] \geq N + 2 + \log_2 \frac{1}{\epsilon'}.$$

This can be achieved for any value of ϵ' by increasing the value of N if $\log_2 \left[\left(\frac{1}{2} + \epsilon_{\text{ave}} \right)^{-1} \left(\frac{1}{2} + \epsilon \right)^{-1} \right] > 1$ or, equivalently, if $\epsilon_{\text{ave}} < \frac{1}{1+2\epsilon} - \frac{1}{2}$, which is satisfied with probability p , as derived above.

APPENDIX B: BOUNDS ON AMPLIFICATION WITH TRIVIAL HASHING FUNCTION

As described in previous sections, our protocol for randomness amplification makes use of bits h_1, \dots, h_N taken from the SOR to construct a hashing function. This method distinguishes our protocol from the one in [3], where a trivial hashing function is applied to obtain the final random bit. That is, the final random bit is assigned to one of the outputs A_i , where i is chosen by use of the SOR. In [5] a deterministic hashing function is applied; nonetheless, their protocol allows for amplification up to $\epsilon' = \frac{1}{4}$ from arbitrarily deterministic sources by applying a trivial hashing function. In this appendix we show that such a trivial hashing function is useful for amplification only in the noise-free case. If the quantum resources available are not perfect, every set of measurements on each entangled state has a probability larger than zero of not fulfilling the conditions of the nonlocal game. Hence, for large values of N , the estimated success probability will converge to $P_{\text{est}} = 1 - \kappa$, with $\kappa > 0$. Next, we show that for every value of $\kappa > 0$, if a trivial hashing function is applied to the outputs A_1, \dots, A_N , no randomness amplification is possible for $\epsilon > 0.345$. This is shown by constructing an explicit attack that (i) provides a value of $\kappa \rightarrow 0$ in the limit of large N and (ii) the eavesdropper possesses a classical variable λ perfectly correlated with the final random bit y . The attack is defined independently of the nonlocal game or quantum states employed.

The attack is defined as follows.

(a) The eavesdropper has to provide $N \equiv 2^k$ nonlocal boxes. The classical variables used as inputs of the nonlocal boxes are chosen by tossing a fair coin without any intervention by the eavesdropper.

(b) When the trivial hashing function is applied, k bits h_1, \dots, h_k are provided by the SOR, whose bias is controlled by the eavesdropper. These bits are used to choose one of the

N nonlocal boxes whose output A_{h_1, \dots, h_k} would be chosen to be the final bit y of the protocol. That is, each nonlocal box is labeled by a value of the string h_1, \dots, h_k .

(c) The eavesdropper chooses a string $\tilde{h}_1, \dots, \tilde{h}_k$. The bias on the SOR prepared by the eavesdropper is such that

$$\begin{aligned} P(h_j = \tilde{h}_j | h_1, \dots, h_{j-1}, h_{j+1}, \dots, h_k) \\ = P(h_j = \tilde{h}_j) = \frac{1}{2} + \epsilon \end{aligned} \quad (\text{B1})$$

for every value of $h_1, \dots, h_{j-1}, h_{j+1}, \dots, h_k$ and j . That is, each bit is independently and identically biased.

(d) Let us denote by G_t the group of nonlocal boxes labeled by a string h_1, \dots, h_k that fulfills $\sum_{j=1}^k h_j \oplus \tilde{h}_j = t$. As such, $t \in \{0, \dots, k\}$ and G_t contains $\binom{k}{t}$ elements. Boxes in the groups G_t with $t \in \{0, \dots, \lfloor (\frac{1}{2} - \alpha)k \rfloor\}$, where $0 < \alpha < \frac{1}{2}$, are chosen by the eavesdropper to be classical deterministic boxes. In order to simplify further calculations let us take the worst case scenario where the classical deterministic have null success probability in the nonlocal game. The rest are perfect quantum states with unit success probability in the nonlocal game.

Given such a strategy,

$$\kappa \leq \sum_{t=0}^{\lfloor (1/2-\alpha)k \rfloor} \binom{k}{t} / 2^k, \quad (\text{B2})$$

which tends to zero with k tending to infinity. This ensures that condition (i) above is fulfilled.

When the variables h_1, \dots, h_k are produced by the SOR, if a box from G_t with $t \in \{0, \dots, \lfloor (\frac{1}{2} - \alpha)k \rfloor\}$ is chosen, then, since these boxes are classical and deterministic, the eavesdropper possesses a classical variable perfectly correlated with the final bit. Let us now denote that probability of choosing one of such classical nonlocal boxes by P_{attack} . Note that, according to (B1), each box in a group G_t is chosen with probability $(\frac{1}{2} + \epsilon)^{k-t} (\frac{1}{2} - \epsilon)^t$. Hence,

$$\begin{aligned} 1 - P_{\text{attack}} \\ = \sum_{t=\lfloor (1/2-\alpha)k \rfloor+1}^k \left(\frac{1}{2} + \epsilon \right)^{k-t} \left(\frac{1}{2} - \epsilon \right)^t \binom{k}{t} \\ \leq \sum_{t=\lfloor (1/2-\alpha)k \rfloor+1}^k \left(\frac{1}{2} + \epsilon \right)^{k-t} \left(\frac{1}{2} - \epsilon \right)^t \left(\frac{ke}{t} \right)^t \end{aligned} \quad (\text{B3})$$

$$\begin{aligned} \leq \sum_{t=\lfloor (1/2-\alpha)k \rfloor+1}^k \left(\frac{1}{2} + \epsilon \right)^{k-t} \left(\frac{1}{2} - \epsilon \right)^t \left(\frac{ke}{(1/2-\alpha)k} \right)^t \\ = \left(\frac{1}{2} + \epsilon \right)^k \sum_{t=\lfloor (1/2-\alpha)k \rfloor+1}^k \left(\frac{(1/2-\epsilon)e}{(1/2+\epsilon)(1/2-\alpha)} \right)^t. \end{aligned} \quad (\text{B4})$$

which tends to zero for $N, k \rightarrow \infty$ if $(\frac{1}{2} - \epsilon)e / ((\frac{1}{2} + \epsilon)(\frac{1}{2} - \alpha)) \leq 1$. This is fulfilled for $\alpha \rightarrow 0$ if $\epsilon \geq \frac{2e-1}{4e+2} \approx 0.345$. If instead of a single round the SOR is used to choose a constant number K of them, the same condition on ϵ holds as the probability of choosing at least one nondeterministic round is $(1 - P_{\text{attack}})^K$, which also tends to zero for $N, k \rightarrow \infty$ when $\epsilon \geq \frac{2e-1}{4e+2} \approx 0.345$.

- [1] D. DiVincenzo, *Science* **270**, 255 (1995).
- [2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [3] R. Colbeck and R. Renner, *Nat. Phys.* **8**, 450 (2012).
- [4] M. Santha and U. Vazirani, in *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science* (IEEE, Piscataway, 1984), p. 434.
- [5] R. Gallego, Ll. Masanes, G. de la Torre, C. Dhara, L. Aolita, and A. Acin, *Nat. Commun.* **4**, 2654 (2013).
- [6] R. Ramanathan, F. G. S. L. Brandao, A. Grudka, K. Horodecki, M. Horodecki, and P. Horodecki, [arXiv:1308.4635](https://arxiv.org/abs/1308.4635).
- [7] F. G. S. L. Brandao, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, and P. Horodecki, [arXiv:1310.4544](https://arxiv.org/abs/1310.4544).
- [8] M. Coudron and H. Yuen, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing, STOC '14* (ACM, New York, 2014), pp. 427–436.
- [9] N. D. Mermin, *Phys. Rev. Lett.* **65**, 1838 (1990).
- [10] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski, and R. Ramanathan, *Phys. Rev. A* **90**, 032322 (2014).
- [11] K.-M. Chung, Y. Shi, and X. Wu, [arXiv:1402.4797](https://arxiv.org/abs/1402.4797).
- [12] R. Gross and S. Aaronson, [arXiv:1410.8019](https://arxiv.org/abs/1410.8019).
- [13] R. Colbeck, Ph.D. thesis, University of Cambridge, 2006.
- [14] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, *Nature (London)* **464**, 1021 (2010).
- [15] R. Colbeck and A. Kent, *J. Phys. A: Math. Theor.* **44**, 095305 (2011).
- [16] U. Vazirani and T. Vidick, *Philos. Trans. R. Soc. London Ser. A* **370**, 3432 (2012).
- [17] S. Fehr, R. Gelles, and Ch. Schaffner, *Phys. Rev. A* **87**, 012335 (2013).
- [18] S. Pironio and S. Massar, *Phys. Rev. A* **87**, 012336 (2013).
- [19] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).
- [20] T. Lawson, N. Linden, and S. Popescu, [arXiv:1011.6245](https://arxiv.org/abs/1011.6245).
- [21] M. Navascues, S. Pironio, and A. Acin, *New J. Phys.* **10**, 073013 (2008).
- [22] A. Fine, *Phys. Rev. Lett.* **48**, 291 (1982).
- [23] S. L. Braunstein and C. M. Caves, *Ann. Phys. (N.Y.)* **202**, 22 (1990).
- [24] B. Chor and O. Goldreich, *SIAM J. Comput.* **17**, 230 (1988).
- [25] Ll. Masanes, A. Acin, and N. Gisin, *Phys. Rev. A* **73**, 012112 (2006).
- [26] J. F. Sturm, *Optim. Methods Softw.* **11**, 625 (1999).