Robustness of quantum-randomness expansion protocols in the presence of noise

Piotr Mironowicz[1,2,*] and Marcin Pawłowski[3,4,†]

[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]*Department of Mathematics, University of Bristol, Bristol BC8 1TW, United Kingdom*

[4]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*

(Received 2 May 2013; published 18 September 2013)

In this paper we investigate properties of several randomness generation protocols in the device-independent framework. Using Bell-type inequalities it is possible to certify that the numbers generated by an untrusted device are indeed random. We present a selection of certificates which guarantee two bits of randomness for each run of the experiment in the noiseless case and require the parties to share a maximally entangled state. To compare them we study their efficiency in the presence of white noise. We find that for different amounts of noise different operators are optimal for certifying most randomness. Therefore, the vendor of the device should use different protocols depending on the amount of noise expected to occur. Another of our results that we find particularly interesting is that using a single Bell operator as a figure of merit is rarely optimal.

DOI: 10.1103/PhysRevA.88.032319 PACS number(s): 03.67.Bg, 03.67.Mn, 89.70.Cf

I. INTRODUCTION

One of the most striking properties of quantum mechanics is that it is intrinsically random. Moreover, if there exist only slightly random processes, then also ones of arbitrary high randomness do [1,2].

Random number generation is an important issue in computer science. Random numbers have many applications in such topics as cryptography, authentication [3], gambling, and system modeling.

Most of the random number generators (RNGs) are based on purely algebraical manipulation on initial seed. Since the series of numbers produced by such generators are created in a deterministic manner, these RNGs are called pseudorandom number generators (PRNGs). There also exist RNGs basing on some chaotic classical physical processes, such as electric or atmospheric noise or on estimating the entropy of hardware interrupts (for example, in */dev/random* RNG on Linux systems). To make sure that a given source of numbers is reliable, some statistical tests may be applied [4]. Still, these tests can never give a guarantee that the numbers were indeed trustworthy, that is they cannot be predicted by an adversary.

In this situation it is natural to try to use properties of quantum mechanics in order to generate entirely random sequences of numbers. There was effort making use of such quantum processes like nuclear decay (for example, HotBits [5]) or photons hitting a semitransparent mirror (for example, id Quantique RNGs [6]). However, when using one of the commercially available quantum random number generators (QRNGs) we still have to trust the vendor of the device.

Therefore, much effort has been made in quantum information theory to attain a reliability while not trusting the device and even not knowing how it works. Such an approach, introduced in [7], is called device independent. Instead of investigating the internal working of the device, in some cases it is sufficient to perform tests on its outputs.

Recently, the violation of certain Bell inequalities as a certificate of randomness for series from RNG has been used within the device-independent approach [8–11]. These protocols were randomness expanders, as they use some initial amount of randomness to obtain more of it. In [8,9] as a certificate of randomness the violation of the CHSH Bell inequality [12] was used, while in [10] the GHZ correlations were used instead.

A. Purpose of this paper

Suppose there is a honest vendor that wants to produce and sell QRNGs. His problem is the lack of trust among his potential customers. Since he does not want to cheat his clients, he can make the design of his device open. But still some parties may distrust that the device is construed in declared manner.

The laws of quantum mechanics give him a way to convince his customers that they do not need to know the internal working of the device to be sure that they get secure randomness. Using some form of Bell inequalities, they may check, after some statistical tests, that the device produces a certain amount of randomness, regardless of the way it has been constructed. Therefore, our honest vendor can propose that his customers use the protocol described in [9]. However, he still needs to decide which Bell inequality to use as a certificate.[1] This device will consist of three parts: two measurement apparatuses and a source of entangled states. The vendor's technology limits the quality (purity) of the states that his source can produce. Let's assume that they are Werner states $\rho_w = p|\psi^-\rangle\langle\psi^-| + (1-p)\frac{\mathbb{1}}{4}$, that is singlets with admixture of white noise. The question that we try to

*piotr.mironowicz@gmail.com

†maymp@bristol.ac.uk

[1]The choice of the certificate is his only choice. Therefore, in the whole paper we identify a certificate with a protocol and use these two terms interchangeably.

 ©2013 American Physical Society

answer in this paper is the following: which certificate allows one to guarantee the most randomness for the given quality of the source measured by p? Using it will allow our vendor to maximally exploit the source he has.

All Bell inequalities considered in this paper are maximally violated with pure singlet states. In the noisy case values attainable by Bell operators[2] are multiplied by p.

In this paper we first make a short inspection of min-entropy and Bell inequalities. Then we present six operators that in a noiseless situation may certify two bits of randomness. Three of them are based on known Bell inequalities: Braunstein-Caves family [13], CHSH [12], and $T3$ [11]. After that we describe a method we used to find other certificates. Then we give the three most interesting examples found this way. Using semidefinite programming we compare the robustness of the presented certificates. Finally, we investigate the potential of using CHSH inequality to improve presented protocols.

B. Min-entropy

One commonly used measure of randomness is min-entropy [14], denoted H_∞. For given discrete probability distribution $P = p_1, \ldots, p_n$ it is defined as

$$H_\infty(P) \equiv -\log_2 \left[\max_i (p_i)\right]. \tag{1.1}$$

Note that min-entropy is directly related to the guessing probability of the value of a particular variable with distribution P with strategy when one guesses the most probable result. In the context of guessing cryptographic keys, min-entropy is a measure of the difficulty of guessing the easiest single key in a given distribution of keys [3].

Having some string of characters from a source with given min-entropy per character it is possible to *extract* its randomness, that is create a shorter string with higher min-entropy per character [15–17]. We use min-entropy as the measure of the efficiency of the protocol throughout the paper.

C. NPA method

The key role in our numerical calculations plays the so-called *NPA* method. It was introduced and developed in Refs. [18,19]. This method brings out an infinite hierarchy of conditions that is satisfied by any set of quantum correlations. Each level of this hierarchy may be mapped to a semidefinite optimization problem. Such a problem may be efficiently solved numerically using the primal-dual interior point algorithm [20–22].

The idea of this method is as follows. We consider a set of projective measurement operators of Alice $\{\Pi_A^a\}$, and similarly for Bob. Because the measurements of Alice and Bob are separated, operators of Alice commute with operators of Bob. If the probability distribution $P(A,B|a,b)$ can be realized under the laws of quantum mechanics, then there must exist a pure state $|\Psi\rangle$ that, for all settings a and b and outcomes A and B, satisfies $P(A,B|a,b) = \langle\Psi|\Pi_A^a \Pi_B^b|\Psi\rangle$.

Since we do not have any assumption about the dimension of the state $|\Psi\rangle$, considering only von Neumann measurements and a pure state is not restrictive. This is because any POVM can be considered as a projective measurement in a space of larger dimension.

Let S be a certain subset of the set of all sequences of measurement operators of Alice and Bob. Let $O_i, O_j \in S$. Now, taking these operators as indices, we may construct the following matrix:

$$\Gamma_{O_i,O_j} \equiv \langle\Psi|O_i^\dagger O_j|\Psi\rangle. \tag{1.2}$$

In particular, $\Gamma_{\Pi_A^a,\Pi_B^b} = P(A,B|a,b)$.

It may be shown [18,19] that the Γ matrix is positively semidefinite. From this, we have some relaxation of the conditions on the probability distribution $P(A,B|a,b)$ that are allowed by quantum mechanics. Instead of assuming that the state $|\Psi\rangle$ and the proper measurement operators exist, we check if it is possible to construct such a positively semidefinite matrix Γ.

The larger set S we choose, the more restrictive is the relaxation. In [19] it was shown that the hierarchy of such relaxations converges to quantum mechanics. Hierarchy of level Q_2 means that the set S consists of all sequences of measurement operators of length 2, whereas in level Q_{1+AB}, S is a set of all sequences of length 1 and sequences with one operator of Alice and one of Bob. Obviously Q_2 gives larger S than Q_{1+AB}.

Applying this method to find lower bounds on min-entropy has become a standard [9,11,23]. The honest vendor of the device should expect that its users will apply this hierarchy to test his product.

II. RANDOMNESS CERTIFICATION PROTOCOLS

In this paper we investigate the applicability for randomness certification of selected Bell operators, described below. Since we are working in a device-independent scenario, it is worth noticing that we have no insight into the workings of the device. We do not know how Alice's and Bob's measurements are carried out; results may even have outcomes predetermined by the constructor of the apparatus. The only thing we have access to are outcomes that Alice and Bob get.

We assume that Alice's and Bob's devices are separated during the measurements. This assumption is essential, since only in this case the violation of Bell inequality has any meaning.[3] The separation may be, for example, spacelike, if we assume that the signal may not travel between Alice's and Bob's part before the results are collected.

If we want the randomness not only to be fair (for example, for gambling and system modeling purposes), but also to be confidential (for example, for cryptography or authentication), we also have to assume that the untrusted device does not

[2]We are assuming that Bell operators are linear functions of correlations, which is more restricted than the general case where the Bell operator is a linear combination of probabilities. All Bell operators used in this paper meet this condition.

[3]In fact, this is a way to assert in the device-independent scenario that Alice's and Bob's measurements may be treated algebraically as commuting.

MOST WIEDZY Downloaded from mostwiedzy.pl

communicate with the world outside. Without this assumption, even the fair RNG may send the results to the adversary.

We will measure the randomness of a given pair of settings using min-entropy. For each pair (a,b) of choices of Alice's and Bob's measurement settings, there exist a distribution $P(A,B|a,b)$ of pairs of outcomes. Min-entropy of the pair of (a,b) is the min-entropy of the distribution $P(A,B|a,b)$.

The general scheme is as follows. We consider a Bell operator (a set of Bell operators). Next we choose a pair of settings: a for Alice and b for Bob. Then we assume that the operator (operators) has (have) certain value (values). Under this assumption, we use the numerical method described above to evaluate what is the minimal value of the min-entropy of the distribution $P(A,B|a,b)$.

In the following we assume that all measurements give results $+1$ or -1.

We denote by A_+,A_- Alice's projector on results $+1$ and -1, respectively, and similarly B_+,B_- for Bob. Since outcomes are binary we have $A_+ + A_- = \mathbb{1}$, and the same for Bob's projectors. Then $C(a,b) = 4 \times A_+B_+ - 2 \times A_+ - 2 \times B_+ + \mathbb{1}$ is the correlation operator. We denote by $\mathrm{Cor}(a,b) \equiv P(A=1,B=1|a,b) + P(A=-1,B=-1|a,b) - P(A=1,B=-1|a,b) - P(A=-1,B=1|a,b)$ the correlations between the binary results obtained by Alice when she chooses measurement a with Bob's results with measurement settings set to b. If ρ is the state describing the whole device (including Alice's and Bob's parts, which may be entangled), then $\mathrm{Tr}[\rho C(a,b)] = \mathrm{Cor}(a,b)$ and $\mathrm{Cor}(a,b)$ may be estimated by collecting statistics of subsequent measurement results.

The measurement settings and the device have to be independent. One of the ways to assure that is to choose these settings randomly. Since in such a situation initial randomness is needed, protocols described below are randomness expanders.

From a theoretical point of view it is important to mention the possibility that, from a fundamental point of view, both measurement choices and results are predetermined. This loophole in Bell inequalities is called superdeterminism and makes all effort towards generation of randomness pointless.

Below we present six different randomness certification protocols. The first of them is based on a well-known Braunstein-Caves Bell inequality. The second one makes use of a pair of Bell operators, which are a decomposition of CHSH inequality. The third one consists of three Bell inequalities, with two of them being CHSH. Three remaining protocols make use of other Bell inequalities described below.

A. Braunstein-Caves inequalities

In [13] a family of chained Bell inequalities was introduced. The members of this family are parametrized by a natural number $n \geqslant 2$. The parameter gives the number of binary measurement settings for two parties. Operators from this family consist of chains of operators of correlation between subsequent measurement settings of Alice and Bob.

The general formula for nth Braunstein-Caves operator is

$$\begin{aligned} BC_n = {} & C(1,1) + C(1,2) + C(2,2) + C(2,3) + C(3,3) \\ & + C(3,4) + \cdots + C(n-1,n-1) + C(n-1,n) \\ & + C(n,n) - C(n,1). \end{aligned} \tag{2.1}$$

The maximal value obtainable in quantum mechanics for nth Braunstein-Caves inequality is $2n\cos(\frac{\pi}{2n})$ [24]. In particular,

$$\begin{aligned} BC_3 = {} & C(1,1) + C(1,2) + C(2,2) + C(2,3) \\ & + C(3,3) - C(3,1) \end{aligned} \tag{2.2}$$

is limited by $6\cos(\frac{\pi}{6}) \approx 5.19$. This value may be attained with singlet state and measurements projecting on vectors on the Bloch sphere of the form $\cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$ with angles $\frac{\pi}{6}$, $\frac{3\pi}{6}$, and $\frac{5\pi}{6}$ for subsequent measurements of Alice, and angles 0, $\frac{\pi}{3}$, and $\frac{2\pi}{3}$ for Bob.

If we consider the source's quality measured by p, then the maximal value is multiplied by p.

We check the min-entropy guaranteed by the violation of Braunstein-Caves inequality for the following three cases: (i) for $n=3$ for the min-entropy of first setting for Alice and third setting for Bob,[4] (ii) for $n=5$ of settings (1,4),[5] and (iii) for $n=7$ of settings (1,5).

The optimal angles for $BC5$ are 0, $\frac{\pi}{5}$, $\frac{2}{5}\pi$, $\frac{3}{5}\pi$, and $\frac{4}{5}\pi$ for Alice, and $\frac{\pi}{10}$, $\frac{3}{10}\pi$, $\frac{\pi}{2}$, $\frac{7}{10}\pi$, and $\frac{9}{10}\pi$ for Bob. In the case of $BC7$ the optimal angles for measurements of Alice are 0, $\frac{\pi}{7}$, $\frac{2}{7}\pi$, $\frac{3}{7}\pi$, $\frac{4}{7}\pi$, $\frac{5}{7}\pi$, and $\frac{6}{7}\pi$, and for Bob $\frac{\pi}{14}$, $\frac{3}{14}\pi$, $\frac{5}{14}\pi$, $\frac{\pi}{2}$, $\frac{9}{14}\pi$, $\frac{11}{14}\pi$, and $\frac{13}{14}\pi$.

B. E_0 and E_1

In this case instead of taking only a single operator corresponding to some Bell inequality, we use more than one for randomness certification.

A single CHSH operator may be decomposed into other Bell operators. Let us consider the following two operators:

$$E_0 = C(1,1) + C(1,2), \tag{2.3a}$$

$$E_1 = C(2,1) - C(2,2). \tag{2.3b}$$

From Uffink's inequality [25] it follows that the maximal values of Eqs. (2.3) lie on a circle of radius 2. Taking into account symmetries of these operators, their maximal values obtainable in quantum mechanics may be parametrized in the following manner:

$$E_{0,\max}(\phi) = 2\cos(\phi), \tag{2.4a}$$

$$E_{1,\max}(\phi) = 2\sin(\phi), \tag{2.4b}$$

for any $\phi \in [0,\frac{\pi}{2}]$. The optimal angles for Alice's measurements are 0 and $\frac{\pi}{2}$. ϕ parametrizes the optimal angles for Bob, which are ϕ and $-\phi$. The maximal quantum value of the sum of Eqs. (2.3) is equal to $2[\cos(\phi)+\sin(\phi)]$. The classical limit for the sum of values of these operators is 2. Thus for $\phi \in \{0,\frac{\pi}{2}\}$ classical and quantum limits are equal.

Similarly like for previously described Bell operators, if the noise p occurs, then the limiting values (2.4) have to be multiplied by this value.

Below we will examine the min-entropy for a measurement settings pair (2,1) as a function of ϕ for maximal values

[4] Similar results would be obtained for these pairs of settings: (2,1) and (3,2).

[5] Similar results are for pairs (2,5), (3,1), (4,2), and (5,3).

MOST WIEDZY Downloaded from mostwiedzy.pl

of the operators (2.3) for different values of noise. Then we will find the optimal angle ϕ as a function of noise. To certify the randomness we assume that simultaneously $E_0 \geqslant 2p\cos(\phi)$ and $E_1 \geqslant 2p\sin(\phi)$. This way we have a family of conditions on the pair of Bell operators (2.3), parametrized by a continuous variable ϕ.

Let us note that this certificate requires both Alice's and Bob's parts of the device to have only two possible measurement settings. It is the smallest requirement among all presented protocols.

C. T_3 with an additional condition

Let us consider a scenario in which Alice has four possible measurement settings and Bob has three, each having two possible outcomes. In [11] the following Bell operator was used:

$$\begin{aligned} T_3 = {} & C(1,1) + C(2,1) + C(3,1) + C(4,1) \\ & + C(1,2) + C(2,2) - C(3,2) - C(4,2) \\ & + C(1,3) - C(2,3) + C(3,3) - C(4,3). \end{aligned} \tag{2.5}$$

Now let us take two additional Bell operators, which are identical to CHSH with certain choices of settings:

$$\mathrm{CHSH}_1 = C(1,1) + C(3,1) + C(1,2) - C(3,2), \tag{2.6a}$$

$$\mathrm{CHSH}_2 = C(2,1) + C(4,1) + C(2,2) - C(4,2). \tag{2.6b}$$

The maximal value of Eq. (2.5) that may be obtained in quantum mechanics is $4 \times \sqrt{3} \approx 6.928$, and for Eq. (2.6) is $2 \times \sqrt{2} \approx 2.82$, the same as for the standard CHSH.

The value $4 \times \sqrt{3}$ for the single operator $T3$ is obtained by operator (2.5) for measurements that projects on the vectors given in [26]. The NPA method confirms that this is the maximal possible value. The optimal angles of measurements for the protocol (with three operators) depends on the assumed noise parameter p.

If we impose on the device a condition that both operators (2.6) achieve the value of at least $0 \leqslant C \leqslant 2 \times \sqrt{2}$, then the maximal value of (2.5) is a function of C, $T_{3,\max} = T_{3,\max}(C)$. We require the device to obtain this maximal value. In the case when we cope with noise or imperfections of the device, where $0 < p < 1$, then we have to multiply all (2.5) and (2.6) by p.

Assuming these conditions we will check the lower bound on the min-entropy, as a function of C with maximal possible value of (2.5), for Alice's setting 1 and Bob's 3.

TABLE I. Number of Bell inequalities that have been randomly chosen depending on the min-entropy they certify under noise $p = 0.95$.

min-entropy	0–0.05	0.05–0.1	0.1–0.15	0.15–0.2
Bell inequalities	12 853	689	722	696
min-entropy	0.2–0.25	0.25–0.3	0.3–0.35	0.35–0.4
Bell inequalities	939	907	850	1324
min-entropy	0.4–0.45	0.45–0.5	0.5–0.55	0.55–0.6
Bell inequalities	1176	839	1062	678
min-entropy	0.6–0.65	0.65–0.7	0.7–0.75	0.75–0.8
Bell inequalities	493	155	91	15

TABLE II. Randomness certified by the CHSH inequality for different noises. The global randomness is the min-entropy of a pair of bits, where one is the outcome of Alice, and the second is the outcome of Bob. The local randomness is the min-entropy of the outcome of one of the parties.

p	Global	Local
0.999 99	1.217 57	0.990 90
0.999	1.122 31	0.911 55
0.95	0.584 11	0.472 34
0.9	0.377 57	0.307 18
0.8	0.135 10	0.113 62

D. Certificates obtained randomly

The three previous cases were chosen by us because they rely, at least to some extent, on known Bell inequalities. In order to learn more about Bell operators certifying randomness we have used some randomized method of finding them.

Most of the known interesting operators are in the form

$$\sum_{i,j} \alpha_{i,j} C(i,j), \tag{2.7}$$

where $\alpha \in \{-1,0,1\}$, i enumerates Alice's settings, and j Bob's settings.

We have considered operators that have this form with four settings for Alice and three settings for Bob. In this case there is around half a million different operators and we have randomly chosen a representative sample of around 25 000 for further studies. Then, for each choice we have computed min-entropy with noise parameter $p = 0.95$ using semidefinite programming (the method is described in more detail in Sec. IV with results). The histogram presenting the number of operators that certify given randomness is shown in Table I.

The most interesting operators are the ones which certify the most randomness. Among tested operators 41 certified more than 0.72 bits of randomness under high noise. These operators form four distinct groups that have identical maximal value and randomness certification properties. The first of these groups (with nine drawn instances) of them are revealed to be isomorphic[6] to BC_3 described in Sec. II A. The remaining three groups are described in Secs. II D1 (with six instances drawn) and II D2 (with 15 and 11 instances drawn, respectively).

[6]Up to the following two operations. First is a reordering of measurement settings, and second is a change of signs of results for one setting of one party.

TABLE III. Comparison of min-entropies certified by $T3$ (2.5) alone and with two additional CHSH conditions (Sec. II C).

p	$T3$	$T3C$
0.999 99	1.3294	1.7871
0.999	1.2171	1.4101
0.95	0.558 73	0.5931
0.9	0.195 15	0.3072
0.8	0	0.1136

MOST WIEDZY Downloaded from mostwiedzy.pl

TABLE IV. Certificate II D1 with additional CHSH condition compared to the original one.

p	Original II D1	Improved II D1
0.999 99	1.9764	1.9764
0.999	1.7751	1.7751
0.95	0.7775	0.780 24
0.9	0.4365	0.454 43
0.8	0.0468	0.1342

1. Modified CHSH

Now let us consider the following Bell operator which is similar to one used in [27]. We call it modified CHSH because it is a CHSH operator with one additional correlation function.

Let us take an operator of the following form:

$$C(1,2)+C(1,3)+C(2,1)+C(2,2)-C(2,3). \quad (2.8)$$

Under quantum mechanics its value is limited to $1+2\times\sqrt{2}$. The maximal value is obtained with angles 0 and $\frac{\pi}{2}$ for Alice, and $\frac{\pi}{2}$, $\frac{\pi}{4}$, and $-\frac{\pi}{4}$ for Bob. Four terms of this operator form a CHSH operator.

The protocol requires the device to reach the maximal value of this operator (multiplied by p in a case with noise). Further in the paper we will examine the min-entropy with a pair of settings (1,1).

2. Other inequalities

Let us consider the following Bell inequalities:

$$\begin{aligned} I_1 &= C(1,2)-C(1,3)-C(2,1)-C(2,2) \\ &\quad +C(3,1)+C(3,3)+C(4,1) \\ &\leqslant 1+6\cos\left(\frac{\pi}{6}\right)\approx 6.19 \end{aligned} \quad (2.9)$$

and

$$\begin{aligned} I_2 &= -C(1,2)+C(1,3)+C(2,1)+C(2,2)+C(2,3) \\ &\quad +C(3,2)-C(3,3)+C(4,1)+C(4,2)+C(4,3) \\ &\leqslant 2+4\times\sqrt{2}\approx 7.66. \end{aligned} \quad (2.10)$$

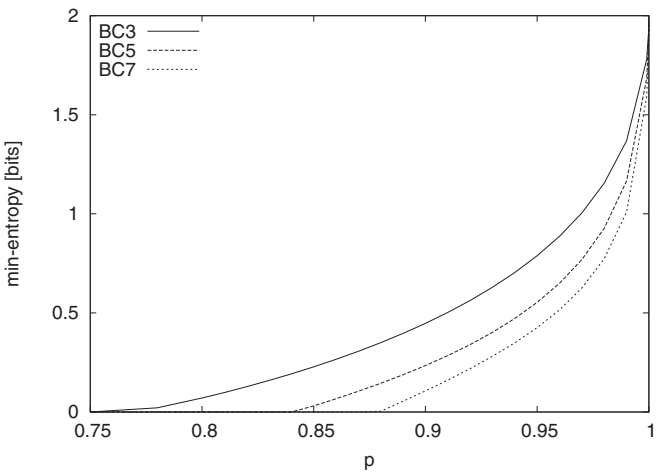

FIG. 1. Lower bounds on min-entropies for protocols described in Sec. II A (based on Braunstein-Caves inequalities) as a function of noise.

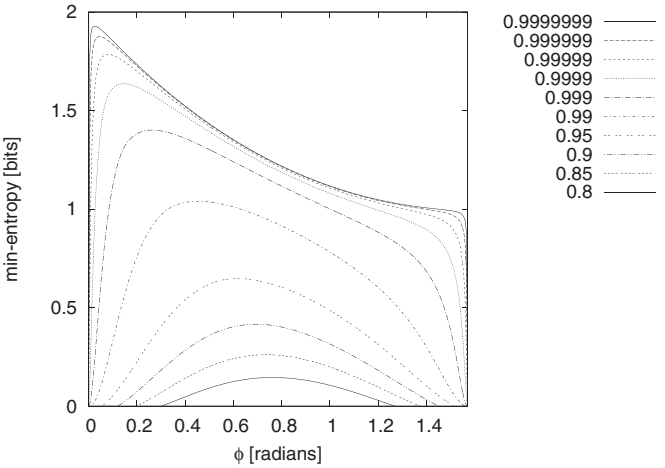

FIG. 2. Lower bound on min-entropy for protocol described in Sec. II B (E_0 with E_1) as a function of ϕ [see Eq. (2.4)] for different noises.

The optimal angles for measurements for operator (2.9) are 0, $\frac{4}{3}\pi$, $\frac{2}{3}\pi$, $\frac{\pi}{2}$ and $\frac{\pi}{2}$, $\frac{\pi}{6}$, $\frac{5}{6}\pi$, for Alice and Bob, respectively. These are the optimal measurement angles for operator (2.10), for Alice: 0, $\frac{\pi}{2}$, π, and $\frac{\pi}{2}$; and for Bob: $\frac{\pi}{2}$, $\frac{3}{4}\pi$, and $\frac{\pi}{4}$.

These two were taken as examples from wider groups of inequalities that use four measurement settings of Alice and three of Bob, and consist of seven, respectively ten, correlations. Inequalities in both of these groups have the same efficiency in generating min-entropy with noise. Inequalities from the first group are similar to these from the Braunstein-Caves family. The pair of measurement settings for which the min-entropy will be investigated is (1,1).

The same as in protocols based on Braunstein-Caves inequalities (II A) and modified CHSH (II D1), random number generation protocols using these inequalities require the device to reach the maximal value of appropriate operator (multiplied by p in the case of noise).

III. IMPROVING CERTIFICATES WITH THE CHSH INEQUALITY

Although the CHSH inequality is not able to certify two bits of randomness even for $p=1$, it is quite efficient for $p\leqslant 0.9$. In fact in this case it is able to guarantee more randomness than most of the two bit protocols. The robustness of this inequality

TABLE V. Optimal angle between E_0 and E_1 depending on noise.

p	ϕ
0.999 999 9	0.0252
0.999 999	0.0452
0.999 99	0.0811
0.9999	0.1460
0.999	0.2638
0.99	0.4562
0.95	0.6179
0.9	0.6948
0.85	0.7357
0.8	0.7617

MOST WIEDZY Downloaded from mostwiedzy.pl

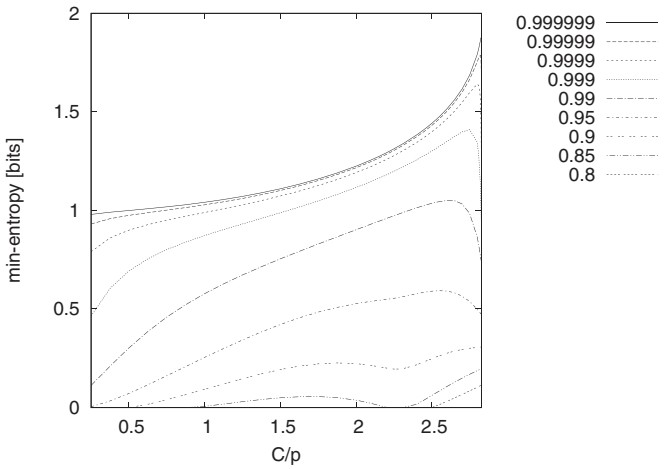

FIG. 3. Lower bound on min-entropy for protocol described in Sec. II C ($T3C$) as a function of C (see text) for different noises.

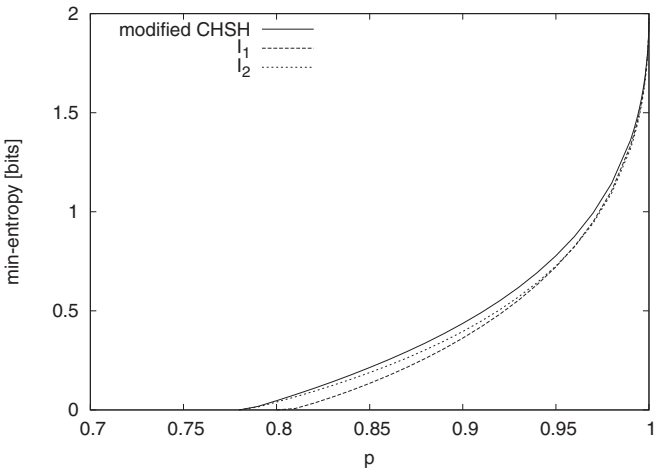

FIG. 4. Lower bounds on min-entropies for protocols described in Secs. II D1 (modified CHSH) and II D2 (other randomly generated protocols) as a function of noise.

in means of the certified min-entropy depending on the noise parameter is shown in Table II. We refer to the randomness of one bit of outcome of one of the parties as a *local* randomness. The *global* randomness is the one that is contained in a pair of bits, where one is the outcome of Alice and the other is the outcome of Bob.

Knowing this property some of the above certificates may be improved if an additional condition for CHSH inequality is imposed. This can be done only when the original certifying operator includes CHSH, which is the case in (2.5) and (2.8).

In Table III certificate II C ($T3C$) is compared with its version taking into the account only the maximal violation of (2.5) attainable for the given amount of noise.

CHSH inequality has also demonstrated its effectiveness for improving certificate II D1 (modified CHSH). Combining it with a condition $C(1,2)+C(1,3)+C(2,2)-C(2,3) \geqslant p2\times\sqrt{2}$ gives the results shown in Table IV.

This protocol for low noises is almost as efficient as II A (BC_3, which is the most efficient in this case), while requiring fewer measurement settings. For high noises this protocol is very close to II B (E_0 with E_1), while not requiring to fit parameters for a particular p parameter. For intermediate amounts of noise it's the best one.

The CHSH operator appears also in (2.10), but in this case imposing its violation does not help. The reason for this is the fact that the operator (2.10) and CHSH cannot simultaneously attain their maximal values. Thus when one of these operators has a considerable value to certify the randomness, the other one is too small to have a significant impact.

TABLE VI. Optimal value of parameter C for protocol II C ($T3C$) depending on noise.

p	0.999 999	0.999 99	0.9999	0.999
$\frac{C}{p}$	2.826	2.82	2.8	2.75
p	0.99	0.95	0.9	0.8
$\frac{C}{p}$	2.6	2.55	2.828	2.828

IV. RESULTS

The following results were obtained using level Q_2 of the *NPA* hierarchy; only results for Braunstein-Caves inequality for $n = 7$ were calculated in level Q_{1+AB} due to the high computer's memory consumption. Since the conditions of these levels do not contain all the laws of quantum mechanics, when computing min-entropy we get a *lower* bound of its value, so all of the examined protocols may give even more randomness than the presented data shows.[7] In fact each of the levels of the hierarchy corresponds to some set of polynomial conditions of a finite degree. In all the cases we take into account the worst case, that is maximize each of the probabilities of given output, independently.

The results for the protocol II A, that uses Braunstein-Caves operators as a function of noise, are shown in Fig. 1. For all values of noise the simplest operator, BC_3 [see (2.2)], gives the highest min-entropy.

In Fig. 2 the results for protocol described in II B (E_0 with E_1) are shown. For parameter ϕ equal to 0 and $\frac{\pi}{2}$ the min-entropy is 0, since then the possible values of (2.3) in quantum and classical cases are the same, so the device's behavior may be implemented classically giving no warranty on randomness.

[7]In other words, we assume less than quantum mechanics. In particular, we do not assume no-signaling principle.

TABLE VII. Comparison of protocols BC_3, BC_5, BC_7 (II A), E_0E_1 (II B), and $T3C$ (II C) for different noises.

p	BC_3	BC_5	BC_7	E_0E_1[a]	$T3C$
0.999 99	1.9769	1.9656	1.9537	1.7854	1.7871
0.999	1.7792	1.6841	1.5917	1.4013	1.4101
0.95	0.7885	0.5534	0.4258	0.6484	0.5931
0.9	0.4474	0.2342	0.1064	0.4163	0.3072
0.8	0.0709	0.0000	0.0000	0.1461	0.1136

[a]Values for optimal angle parameter.

MOST WIEDZY Downloaded from mostwiedzy.pl

TABLE VIII. Comparison of protocols: improved II D1 (modified CHSH) and II D2 (I_1 and I_2) for different noises.

p	Modified CHSH	I_1	I_2
0.999 99	1.9764	1.9753	1.9742
0.999	1.7751	1.7649	1.7558
0.95	0.780 24	0.7219	0.7262
0.9	0.454 43	0.3625	0.3959
0.8	0.1342	0.0000	0.0398

An important result is that the optimal angle between average values of operators (2.3) depends on the noise parameter p. This dependence is shown in Table V.

Figure 3 shows the results for protocol described in II C ($T3C$). It is worth noticing that as parameter C approaches it maximal value $2 \times \sqrt{2}$, then the min-entropy tends to 1 (in the case without noise). The min-entropy strongly depends on C. This dependence is shown in Table VI.

Considering the bound on the value of the operator $T3$ [(2.5), not shown in the figure], it is maximal for $C = 2.309\,411\,6$. For high noises ($p < 0.95$) min-entropy has local minimum near this point.

Figure 4 contains the results for protocols using inequalities described in II D1 (modified CHSH) and II D2 (other randomly generated operators).

It can be seen that the protocol II A using Bell inequality (2.2) ($BC3$) gives the largest amount of randomness comparing to other described protocols, when the noise parameter p is larger than 0.9. Different operators from the Braunstein-Caves family give less min-entropy for all amounts of noise and require more settings for each party.[8]

For high noises ($p \approx 0.8$) the largest min-entropy is obtained using protocol II B (E_0 with E_1). The main disadvantage of this protocol is the necessity to choose the angle parameter individually for each noise.

The certificate II C ($T3C$) shares with II B (E_0 with E_1) the need for choosing its parameter (in this case C) for the given noise. Similarly, it gives good results for high noises ($p \approx 0.8$), but not as good as II B. It also requires more measurement settings.

Using modified CHSH (II D1) and certificates I_1 and I_2 (II D2) for smaller noises ($p \geqslant 0.9$), the amount of achieved randomness is slightly smaller that the randomness from the protocol BC_3 [II A with Bell inequality (2.2)]. However, protocol based on modified CHSH inequality requires less measurement settings than BC_3.

Protocols with more complicated Bell inequalities I_1 and I_2 slightly differ depending on the amount of noise. For $p \geqslant 0.999$ the inequality I_1 (2.9) gives more randomness than I_2 (2.10), while for $p \leqslant 0.999$ I_2 gives more randomness than I_1.

Comparison of all protocols described in this paper may be found in Tables VII and VIII.

[8]It is important for a protocol to use not many measurement settings, as they require more initial randomness for expansion.

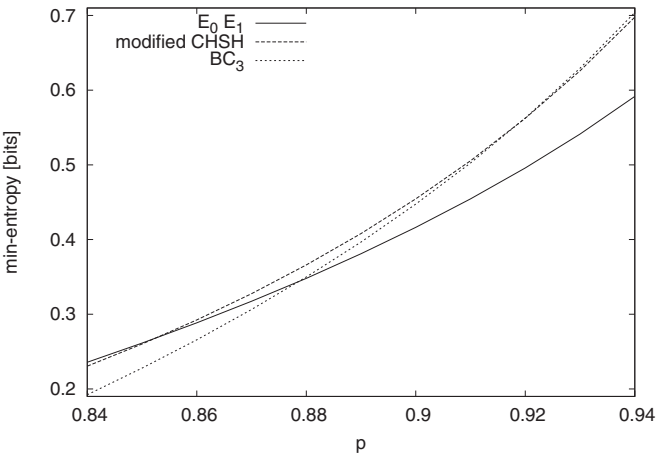

FIG. 5. Comparison of the three most efficient of investigated protocols for $0.84 \leqslant p \leqslant 0.94$.

V. CONCLUSIONS

In this paper we presented several certificates for randomness generation protocols. We find that there is no unequivocally most efficient one for all the amounts of noise. On the other hand, some are clearly better than the others.

For low noises ($p \geqslant 0.92$) the most randomness may be obtained using the certificate II A based on the Braunstein-Caves inequality. This protocol requires three binary measurements for Alice and for Bob and uses only one inequality.

In the case of intermediate noise ($0.85 \leqslant p \leqslant 0.92$) the protocol II D1 with additional CHSH condition (III) certifies most randomness. It requires two binary measurements for Alice and three for Bob.

Protocol II B based on a pair of operators, E_0 and E_1, certifies most randomness among all the compared protocols for high noises ($p \leqslant 0.85$). It requires two binary measurements for both Alice and Bob and has a parameter ϕ that has to be chosen for a particular noise p for optimal results.

A comparison of these three protocols is shown in Fig. 5.

The conclusion of this paper is that a honest vendor of QRNGs should use one of these three protocols, depending on the amount of noise he is expecting the device will have to cope with.

The first interesting fact that our research has revealed is that there is no single optimal certificate. But what is even more remarkable is that the three best ones fall into three distinct categories. Certificate II A is just a Bell operator, II D1 is a combination of two, and E_0 and E_1 are not even Bell inequalities; furthermore, they have to be considered with different weights. This proves that there is more than one place to look for optimal certificates and although Bell inequality violation is a necessary condition for device-independent certification of randomness, it is not always a good measure of it.

ACKNOWLEDGMENTS

SDP was implemented in OCTAVE using SeDuMi [20] toolbox. This work is supported by FNP TEAM, IDEAS PLUS (IdP2011 000361), NCN Grant 2013/08/M/ST2/00626 and U.K. EPSRC.

MOST WIEDZY Downloaded from mostwiedzy.pl

[1] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita, and A. Acin, arXiv:1210.6514.
[2] P. Mironowicz and M. Pawłowski, arXiv:1301.7722.
[3] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbu, NIST Special Publication 800-63-2 – Electronic Authentication Guideline (National Institute of Standards and Technology, U.S. Department of Commerce, 2013), http://csrc.nist.gov/publications/PubsSPs.html#800-63-Rev2.
[4] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, Special Publication 800-22 Revision 1a–A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (National Institute of Standards and Technology, U.S. Department of Commerce, 2010), http://csrc.nist.gov/publications/PubsSPs.html#800-22.
[5] www.fourmilab.ch/hotbits
[6] www.idquantique.com
[7] D. Mayers and A. Yao, in *FOCS'98:Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, DC, USA, 1998), p. 503.
[8] R. Colbeck, Ph.D. thesis, University of Cambridge, 2007.
[9] 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).
[10] R. Colbeck and A. Kent, J. Phys. A: Math. Theor. **44**, 095305 (2011).
[11] H.-W. Li, P. Mironowicz, M. Pawłowski, Z.-Q. Yin, Y.-C. Wu, S. Wang, W. Chen, H.-G. Hu, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **87**, 020302(R) (2013).
[12] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[13] S. L. Braunstein and C. M. Caves, Phys. Rev. Lett. **61**, 662 (1988).
[14] R. Koenig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Th. **55**, 9 (2009).
[15] L. Trevisan, J. ACM **48**, 860 (2001).
[16] A. De, C. Portmann, T. Vidick, and R. Renner, SIAM J. Comput. **41**, 915 (2012).
[17] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Th. **57**, 5524 (2011).
[18] M. Navascues, S. Pironio, and A. Acin, Phys. Rev. Lett. **98**, 010401 (2007).
[19] M. Navascues, S. Pironio, and A. Acin, New J. Phys. **10**, 073013 (2008).
[20] J. F. Sturm, *SeDuMi, A Matlab Toolbox for Optimization Over Symmetric Cones*, http://sedumi.ie.lehigh.edu/
[21] J. F. Sturm, Optimization Methods Softw. **11**, 625 (1999).
[22] J. F. Sturm, *Implementation of Interior Point Methods for Mixed Semidefinite and Second Order Cone Optimization Problems*, Vol. 157 (Kluwer, Dordrecht, 2000).
[23] L. Masanes, S. Pironio, and A. Acin, Nat. Commun. **2**, 238 (2011).
[24] S. Wehner, Phys. Rev. A **73**, 022110 (2006).
[25] J. Uffink, Phys. Rev. Lett. **88**, 230406 (2002).
[26] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).
[27] R. Gallego, N. Brunner, C. Hadley, and A. Acin, Phys. Rev. Lett. **105**, 230501 (2010).

MOST WIEDZY Downloaded from mostwiedzy.pl