Upper bound on certifiable randomness from a quantum black-box device

Ioannou, Marie; Brask, Jonatan Bohr; Brunner, Nicolas

Published in:
Physical Review A

Link to article, DOI:
10.1103/PhysRevA.99.052338

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Upper bound on certifiable randomness from a quantum black-box device

Marie Ioannou,[1] Jonatan Bohr Brask,[1,2] and Nicolas Brunner[1]
[1]*Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland*
[2]*Department of Physics, Technical University of Denmark, Fysikvej, Kongens Lyngby 2800, Denmark*

(Received 27 November 2018; published 23 May 2019)

Quantum theory allows for randomness generation in a device-independent setting, where no detailed description of the experimental device is required. Here we derive a general upper bound on the amount of randomness that can be certified in such a setting. Our bound applies to any black-box scenario, thus covering a wide range of scenarios from partially characterized to completely uncharacterized devices. Specifically, we prove that the number of random bits that can be certified is limited by the number of different input states that enter the measurement device. We show explicitly that our bound is tight in the simplest cases. More generally, our paper indicates that the prospects of certifying a large amount of randomness by using high-dimensional (or even continuous variable) systems will be extremely challenging in practice.

DOI: 10.1103/PhysRevA.99.052338

I. INTRODUCTION

Randomness is a characteristic feature of quantum theory. The unpredictability of measurements performed on a quantum system has deep implications for information processing, e.g., for quantum random number generation [1–3], arguably one of the most developed applications of quantum information science.

The initial idea for devising a quantum random number generator (QRNG) consisted in sending a single quantum particle (say a photon) onto a balanced beam splitter followed by two detectors [4–6]. According to quantum theory, it is completely unpredictable on which detector each particle will arrive, thus resulting in a perfectly random bit. The simplicity of this scheme makes it well suited to experimental implementations, and current commercially available QRNGs are mostly based on this principle. In practice, however, the implementation of this scheme is much more challenging than it may appear at first sight. The reason is that any experimental implementation is prone to technical imperfections that introduce unavoidable noise. A rigorous characterization of the devices is therefore required to separate technical noise from true quantum randomness, which is often cumbersome and challenging in practice [7–10].

Interestingly, these problems can in principle be overcome by using a more general approach known as device-independent (DI) certification of quantum randomness. Here a detailed description of the experimental devices is not required, and the user can estimate the amount of randomness generated (i.e., the entropy of the output) based on observed experimental data only, i.e., treating the measurement device as a "black box." Several forms of DI protocols have been considered, featuring different levels of security and practicality. The highest level of security is achieved in the so-called fully DI approach, based on a loophole-free demonstration of quantum nonlocality [11,12]. Alternative approaches, referred to as semi-DI (SDI) [13], were developed for prepare-and-measure setups, much easier to implement in practice. These schemes typically require a general assumption on the quantum systems involved, for instance an upper bound on the Hilbert-space dimension [14,15] or on the energy [16], or a lower bound on the overlap between states [17]. Other approaches to partially DI QRNGs have also been investigated (see e.g., Refs. [18–23]). Currently, there is a strong effort towards the implementation of DI and semi-DI QRNGs. State-of-the-art laboratories have demonstrated fully DI QRNGs [12,24–27]. Semi-DI QRNGs were also realized [28–30], and Ref. [17] recently reported performance comparable to commercial devices. This significant progress has triggered considerable attention, and it is now an important question to find novel schemes generating as much randomness as possible.

This then naturally raises the question of what the ultimate limits of randomness generation in DI and SDI scenarios are. More generally, given a setup involving a black-box measurement device, what is the maximal amount of randomness that can possibly be generated? Beyond the fundamental interest, this question is also relevant to the development of practical and efficient schemes, providing a benchmark for randomness generation protocols. Understanding the limits of randomness generation allows one to characterize the performance of a given scheme in a meaningful manner.

Here, we address this question. Our main result is an upper bound on the amount of randomness that can be certified in any black-box scenario. Notably this bound applies to all scenarios where the measurement device is uncharacterized, hence covering in particular the DI and SDI cases. Specifically, we show that it is not only the number of measurements outcomes that limits the entropy of the output, but also the number of different input states entering the measurement device. For a measurement device providing l outputs and receiving k different input quantum states, the number of random bits that can be certified is upper bounded by $\log_2(\min\{l, k+1\})$. Moreover, we show that our bound is tight for the two simplest SDI scenarios with $k = 2, 3$. Finally, we conclude with a discussion of the implications of our results.

II. BASICS

For clarity we will present our result in the SDI picture, considering a prepare-and-measure scenario. The preparation device takes as input $x \in \{0, 1, ..., k-1\}$ and emits a quantum state ρ_x. The emitted state is sent to a measurement device, where a measurement is selected via an input $y \in \{0, ..., m-1\}$. The selected measurement is performed and provides an outcome $b \in \{0, ..., l-1\}$. The observed statistics is given by the probabilities

$$p(b|x, y) = \mathrm{Tr}[M_{b|y}\rho_x], \tag{1}$$

where $M_{b|y}$ are the elements of a positive-operator-valued measure (POVM) describing the measurement. Importantly, in this picture the observer chooses the inputs x and y and records the output b, but does not necessarily know what quantum states ρ_x and measurements $M_{b|y}$ are actually being implemented inside the black boxes.

To certify randomness in this SDI scenario, one needs to limit the set of possible states ρ_x that can be prepared. If not, all possible distributions $p(b|x, y)$ can be obtained, by simply encoding the input x in a set of k orthogonal quantum states. Hence, the observed data do not enable any differentiation between classical and quantum behaviours of the devices, and no randomness can be certified. Several possibilities to limit the set of prepared quantum states have been investigated, such as bounds on the Hilbert-space dimension, the energy, or the overlap. Here this choice is not important, as our result will apply in full generality, irrespective of which specific assumption is considered. In particular, the states could be completely characterized.

Our goal is to derive an upper bound on the number of random bits that can be certified from the output b in this black-box setting. Consider an observer (or a potential adversary) having complete knowledge of the inner workings of the devices, i.e., knowing exactly what the prepared states ρ_x and the measurements $M_{b|y}$ are. How well can such an observer predict b? Clearly, a first limit arises simply from the finite cardinality of b. As there are only l possible outcomes b, no more than $\log_2(l)$ bits of randomness can be certified. It is natural then to ask if this bound can be attained in general. This would be of particular interest for setups where the output alphabet is very large (or even infinite) as in continuous variable (CV) optics implementations (see, e.g., Refs. [31–33]), thus leading to the certification of a large number of random bits in each round. We will show, however, that this is not possible in general. Specifically, we prove that the number of random bits that can be certified is upper bounded by $\log_2(k+1)$. Hence, the maximal randomness depends not only on the properties of the measurement device but also on the preparation device. We also note that, although we do not explicitly account for classical or quantum side information in the following, such side information can only decrease the amount of certifiable randomness. Hence our upper bound also applies to scenarios with side information.

Before discussing our main result, we introduce some notation. For our analysis, it will be enough to consider finite-dimensional systems, i.e., qudits. These can be conveniently characterized via a generalized Bloch-sphere representation [34]:

$$\rho = \frac{1}{d}(\mathbb{1} + c_d \vec{n} \cdot \vec{\sigma}), \tag{2}$$

where $\vec{n} \in \mathbb{R}^{d^2-1}$, $c_d = \sqrt{\frac{d(d-1)}{2}}$ and $\vec{\sigma}$ is a vector of the generalized Gell-Mann matrices (for $d = 2$, this a vector of the three Pauli matrices). These $d^2 - 1$ matrices are traceless and form an orthogonal basis for the space of $d \times d$ Hermitian matrices, i.e., $\mathrm{Tr}[\sigma_i] = 0$ and $\mathrm{Tr}[\sigma_i\sigma_j] = 2\delta_{i,j}$. From this, it follows that ρ is self-adjoint and has unit trace. However, it is not guaranteed to be positive semidefinite unless further restrictions are placed on $\vec{n}$. For pure states, a simple criterion can be stated in terms of the so-called star product, defined by $(\vec{u} \star \vec{v})_i = \frac{c_d}{d-2}\sum_{j,k=1}^{d^2-1} d_{ijk}u_j v_k$ where d_{ijk} is a symmetric tensor given by the structure constants of the Lie algebra of SU(d). The expression (2) represents a valid pure state if and only if $|\vec{n}| = 1$ and $\vec{n} \star \vec{n} = \vec{n}$ [35].

A measurement is represented by a POVM acting on this d-dimensional Hilbert space. Considering rank-1 POVMs with N outcomes $\mathbb{P}_N$, there exists a set of positive coefficients $\{\lambda_b\}$ such that $\mathbb{P}_N = \{\lambda_b E_b\} = \{M_b\}$ and $\sum_{b=1}^{N} \lambda_b E_b = \mathbb{1}$ where E_b are rank-1 projectors (see e.g., Ref. [36]). Using the generalized Bloch-sphere representation, E_b can be written as

$$E_b = \frac{1}{d}(\mathbb{1}_d + c_d \vec{v}_b \cdot \vec{\sigma}), \tag{3}$$

where again $\vec{v}_b \in \mathbb{R}^{d^2-1}$ is a unit vector satisfying $\vec{v}_b \star \vec{v}_b = \vec{v}_b$. The validity of a rank-1 POVM is ensured by

$$\sum_b \lambda_b = d, \quad \sum_b \lambda_b \vec{v}_b = \vec{0}, \quad \lambda_b \geqslant 0\,. \tag{4}$$

We will need to consider convex combinations of POVMs and POVMs with different numbers of outcomes. Given two POVMs $\mathbb{P}^{(1)}$ and $\mathbb{P}^{(2)}$, their convex combination $p\mathbb{P}^{(1)} + (1-p)\mathbb{P}^{(2)}$ is a POVM with the ith element given by $pM_i^{(1)} + (1-p)M_i^{(2)}$, for some $p \in [0, 1]$. A POVM is called extremal when it cannot be expressed as a convex combination of other POVMs. Any POVM can be decomposed into extremal ones, and since convex combinations can be obtained via classical postprocessing, clearly no POVM can generate more randomness than the best extremal entering in its decomposition. Thus, while we consider a scenario with l-outcome measurements, it will be interesting to consider POVMs that can be decomposed into extremal ones with fewer outcomes. By $\mathbb{P}_N$ we denote a POVM with N nonzero elements (and thus $l - N$ zero elements), and by $\mathcal{P}_N$ we denote the set of POVMs which can be written as convex combinations of N-outcome POVMs.

III. MAIN RESULT

Our main result is a general upper bound on the amount of randomness that can be certified in a black-box scenario. Below we prove the result for the SDI prepare-and-measure scenario. Then we discuss the extension to the fully DI scenario, based on a Bell test.

Let us first give the intuition behind the result. In the black-box scenario, any setup featuring k different prepared quantum states can always be modeled by considering a set

of states ρ_x living in a Hilbert space of dimension $d = k$, i.e., $\mathbb{C}^k$. In turn, this implies that the measurement operators $\{M_{b|y}\}$ can also be considered to act on $\mathbb{C}^k$. Now, any POVM acting on $\mathbb{C}^k$ can be simulated from extremal POVMs and classical postprocessing. As any extremal POVM acting on $\mathbb{C}^k$ features at most k^2 outcomes [37], it follows directly that no more than $2\log_2(k)$ random bits can be certified per round.

This simple argument explains why randomness is bounded by the number of possible preparations k. However, the above bound is far from being tight, and we now derive a much stronger one. The intuition is the following. With only k preparations, their corresponding Bloch vectors span a k-dimensional real space and any component of the measurements acting outside this space will not contribute to randomness generation, so only a subset of POVMs acting on $\mathbb{C}^k$ will be relevant. For the relevant subset, we find that all extremal POVMs have at most $k+1$ outputs, and it follows that no more than $\log_2(k+1)$ bits can actually be certified.

We note that any POVM element with rank higher than 1 can always be decomposed into a combination of rank-1 operators. By assigning separate outcomes to these operators, one obtains a rank-1 POVM with additional outcomes. The original POVM can be obtained from this larger POVM by classical postprocessing (by binning several outcomes together) [36,38]. Since classical postprocessing cannot increase the amount of randomness, we can restrict our analysis to rank-1 POVMs.

Theorem 1. In a prepare-and-measure setup with k prepared states, and m measurements providing l outputs, one can certify at most $\log_2(\min\{l, k+1\})$ random bits per round.

Proof. The fact that no more than $\log_2(l)$ random bits can be generated trivially follows from the fact that one can simply guess at random the output b. The main aspect of the proof is therefore to show that the number of random bits is bounded by $\log_2(k+1)$. Also note that the following arguments hold for any y, and thus the bound holds irrespective of m.

Given k different prepared quantum states, we can without loss of generality consider that all states ρ_x act on a Hilbert-space dimension $d = k$. The statistics can thus be expressed using the generalized Bloch-sphere representation:

$$p(b|x,y) = \frac{\lambda_{b|y}}{d}[1 + (d-1)\vec{v}_{b|y}\cdot\vec{n}_x]. \tag{5}$$

First, note that the components of $\vec{v}_{b|y}$ orthogonal to $\vec{n}_x$ will not contribute to the statistics. Therefore, it is sufficient in general to consider POVMs the Bloch vectors $\vec{v}_{b|y}$ of which live in the space spanned by $\{\vec{n}_0, ..., \vec{n}_{d-1}\}$. Secondly, as $p(b|x,y)$ is linear in $M_{b|y}$, it is sufficient to focus on extremal POVMs. Indeed, if $M_{b|y}$ is not extremal, i.e., it can be written as a convex combination $M_{b|y} = pM^{(1)}_{b|y} + (1-p)M^{(2)}_{b|y}$ with $p \in [0,1]$, then $M_{b|y}$ cannot generate more randomness than $M^{(1)}_{b|y}$ or $M^{(2)}_{b|y}$.

To summarize, we need to focus on extremal rank-1 POVMs with Bloch vectors $\vec{v}_b$ living in the d-dimensional space spanned by $\{\vec{n}_0, ..., \vec{n}_{d-1}\}$. Specifically, we would like to determine the maximal number of outputs of any these POVMs. In the following we will show that this maximal number is $d+1$.

In $\mathbb{R}^d$ one needs d vectors to span a solid angle. Given $d+1$ vectors either (i) one of them lies in the solid angle spanned by the others and is thus a conical combination of them or (ii) the solid angles spanned by all the possible subsets of d vectors cover the entire $(d-1)$ sphere. Hence, any additional vector will necessarily fall in the solid angle spanned by d of the original vectors and thus be a conical combination of them. Thus, in dimension d, given $d+2$ or more vectors, at least one is always a conical combination of d others. The theorem then follows from the following lemma by induction. ■

Lemma 1. Given a rank-1 POVM with l outputs $\mathbb{P}_l$, if one of the generalized Bloch vectors is a conical combination of $l' \leqslant l-1$ of the others, then the POVM can be written as a convex combination of two rank-1 POVMs with $l-1$ outcomes each, i.e., $\mathbb{P}_l = p\mathbb{P}^{(1)}_{l-1} + (1-p)\mathbb{P}^{(2)}_{l-1}$.

Proof. Let us consider a rank-1 POVM with l elements $\mathbb{P}_l = \{M_b\}$, $b = 0, \ldots, l-1$. The POVM elements are given by $M_b = \lambda_b E_b$ where E_b are expressed in the generalized Bloch-like representation (3). The parameters λ_b and $\vec{v}_b$ satisfy the conditions (4) such that the M_b's form a valid POVM.

First, the operation consists in extracting $\mathbb{P}^{(1)}_{l-1}$ from $\mathbb{P}_l$. Without loss of generality, we make the assumption that $\vec{v}_0$ is a conical combination of $l-1$ vectors $\vec{v}_0 = \sum_{b=1}^{l-1} c_b\vec{v}_b$ with $0 \leqslant c_b$. The parameters $\lambda^{(1)}_b$ and $\vec{v}^{(1)}_b$ of $M^{(1)}_b$ are given by $\vec{v}^{(1)}_b = \vec{v}_b$, $\lambda^{(1)}_0 = 0$, $\lambda^{(1)}_b = \frac{1}{N}(\lambda_b + \lambda_0 c_b)$, where N is a normalization coefficient to be fixed in order to satisfy the first condition in (4). The second condition in (4) is also fulfilled:

$$\begin{aligned}\sum_{b=0}^{l-1}\lambda^{(1)}_b\vec{v}_b &= \lambda^{(1)}_0\vec{v}_0 + \sum_{b=1}^{l-1}\frac{1}{N}(\lambda_b + \lambda_0 c_b)\vec{v}_b \\ &= \frac{1}{N}\left(\sum_{b=1}^{l-1}\lambda_b\vec{v}_b + \lambda_0\sum_{b=1}^{l-1}c_b\vec{v}_b\right) \\ &= \frac{1}{N}(-\lambda_0\vec{v}_0 + \lambda_0\vec{v}_0) = \vec{0}.\end{aligned} \tag{6}$$

The last condition is straightforward to verify, i.e., $\lambda^{(1)}_b \geqslant 0$. The first step is done: $\mathbb{P}^{(1)}_{l-1} = \{M^{(1)}_b\}$ is a valid POVM.

Next, the coefficient of the convex combination p is defined as follows:

$$p = \min_b \frac{\lambda_b}{\lambda^{(1)}_b}. \tag{7}$$

Here, $p \in [0,1]$ since $\sum_{b=0}^{l-1}\lambda_b = \sum_{b=0}^{l-1}\lambda^{(1)}_b = d$.

Finally, $\mathbb{P}^{(2)}_{l-1}$ can be fixed by defining the parameters of $M^{(2)}_b$ as $\vec{v}^{(2)}_b = \vec{v}_b$, $\lambda^{(2)}_b = \frac{\lambda_b - p\lambda^{(1)}_b}{1-p}$. Assuming that the minimum of (7) occurs for b^*, this implies $\lambda^*_b = 0$ and thus a POVM with $m-1$ outcomes. Let us check that the first condition of (4) is fulfilled:

$$\sum_{b=0}^{l-1}\lambda^{(2)}_b = \frac{1}{1-p}(d - pd) = d. \tag{8}$$

Using (4) and (6) it is straightforward to verify that

$$\sum_{b=0}^{l-1}\lambda^{(2)}_b\vec{v}^{(2)}_b = \sum_{b=0}^{l-1}\frac{\lambda_b - p\lambda^{(1)}_b}{1-p}\vec{v}_b = \vec{0}. \tag{9}$$

The positivity of $\lambda_b^{(2)}$ is ensured by the choice of p (7). Hence, $\mathbb{P}_{l-1}^{(2)} = \{M_b^{(2)}\}$ is also a valid POVM. And by construction, $\mathbb{P}_l$ is a convex combination of the two extracted POVMs, $\mathbb{P}_l = p\mathbb{P}_{l-1}^{(1)} + (1-p)\mathbb{P}_{l-1}^{(2)}$. ■

We note that Lemma 1 could also be of independent interest, for example, in the context of the simulation of certain POVMs using other measurements [39–41].

Theorem 1 is also relevant in the context of randomness certification in the fully DI scenario. Consider a Bell test with two spatially separated parties, Alice and Bob, sharing a quantum state $\rho \in \mathcal{C}^d \otimes \mathcal{C}^d$. Upon receiving an input x for Alice and y for Bob, they output a and b, respectively. When Alice performs measurement x and obtains output a, Bob's system is steered into the (un-normalized) state $\sigma_{a|x} = \mathrm{Tr}_A[\rho(M_{a|x} \otimes \mathbb{1}_B)]$, where $M_{a|x}$ is the POVM element for Alice's measurement. Bob can thus receive at most $|x|\cdot|a|$ different states. From Theorem 1, Corollary 1 then directly follows.

Corollary 1. Consider a Bell scenario with Alice having $|x|$ inputs and $|a|$ outputs, and Bob having $|y|$ inputs and $|b|$ outputs. Then, Alice can locally certify at most $\log_2(\min\{|a|, |y|\cdot|b|+1\})$ random bits per round, and similarly for Bob. Together, Alice and Bob can certify at most $\log_2(\min\{|a|\cdot|b|, (|y|\cdot|b|+1)|b|, (|x|\cdot|a|+1)|a|\})$ bits of global randomness per round.

IV. TIGHTNESS

Theorem 1 gives a general upper bound on the output entropy that can be certified. It is thus natural to ask whether this bound is tight. Here we consider the two simplest cases of a SDI prepare-and-measure setup with $k = 2, 3$ preparations. In both cases, the bound of Theorem 1 can be reached asymptotically.

Consider a preparation device emitting $|\psi_x\rangle$ with $x \in \{0, \ldots, k-1\}$. Following Ref. [17] we consider an assumption on the distinguishability of the states; specifically, we lower bound their overlap $|\langle\psi_i|\psi_j\rangle| \geqslant \delta$ for all i, j. Note that such an assumption is well suited for optical setups, as it corresponds to an upper bound on the intensity of the light source. To quantify the genuine randomness in b, we use the minimum entropy $H_{\min} = -\log_2(p_{\text{guess}})$ [42], where p_{guess} is the probability that an observer with complete knowledge of the inner workings of the devices has to guess the output b.

For $k = 2$, without loss of generality the two qubit preparations are given by Bloch vectors $\{\vec{n}_0, \vec{n}_1\}$ in the xz plane of the Bloch sphere, distributed symmetrically around the z axis. From Lemma 1, we can focus on extremal ternary POVMs $\mathbb{P}_3 = \{M_1, M_2, M_3\}$ such that all Bloch vectors are in the the xz plane. Specifically, we consider POVMs of the form $M_b = \frac{\lambda_b}{2}(\mathbb{1}_2 + \vec{\sigma}\cdot\vec{u}_b)$, with $\sum_{b=0}^2 \lambda_b = 2$, $\sum_{b=0}^2 \lambda_b \vec{u}_b = 0$, and $\lambda_b \geqslant 0$. Moreover, all Bloch vectors are of the form $\vec{u}_b = (\cos\theta_b, 0, \sin\theta_b)$ with $|\vec{u}_b| = 1$ (as the POVM is extremal).

Next, a maximization of the entropy $H_{\min}$ is performed over the free parameters θ_1, θ_2, and λ_1, for different values of the overlap δ. This is implemented as a heuristic optimization; for each set of parameters, a lower bound on the entropy is obtained via a semidefinite program, as in Ref. [17]. We find

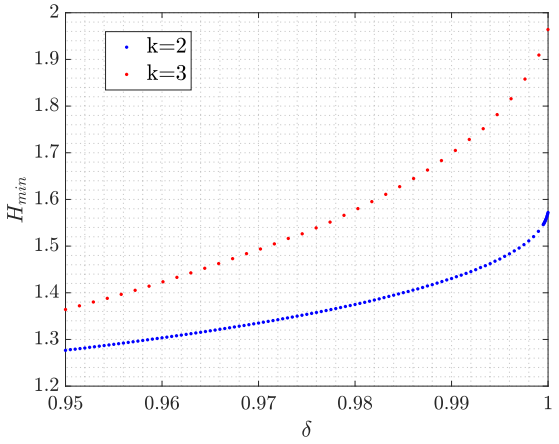

FIG. 1. Plot of the output entropy $H_{\min}$ as a function of the overlap δ for $k = 2, 3$ preparations. In the limit of almost indistinguishable states $\delta \to 1$, the output entropy becomes asymptotically maximal, i.e., $H_{\min} = \log_2(3)$ for $k = 2$ and $H_{\min} = \log_2(4)$ for $k = 3$. This shows that the bound of Theorem 1 can be attained in those two cases.

that, when the two states become almost indistinguishable (i.e., $\delta \to 1$), the entropy approaches $H_{\min} = \log_2(3)$ (see Fig. 1). This shows that the bound of Theorem 1 is tight in this case. The optimal POVM can be parametrized as follows: $\theta_1 = 0$, $\lambda_2 = \lambda_3 = \lambda$ $\theta_2 = -\theta_3 = \arccos(\frac{1}{\lambda} - 1)$, $\lambda_1 = 2(1-\lambda)$, where

$$\lambda = \frac{0.7323\delta^3 - 6.077\delta^2 + 4.017\delta + 5.742}{\delta^3 - 7.645\delta^2 + 4.903\delta + 7.147}. \tag{10}$$

For the case $k = 3$, Lemma 1 implies that one can focus on extremal POVMs with all generalized Bloch vectors contained in the space spanned by the three Bloch vectors of the preparations. As for $k = 2$, an optimization of the entropy $H_{\min}$ is performed over the free parameters describing the POVM. Again, when the states become almost indistinguishable, the entropy approaches $H_{\min} = 2$ (see Fig. 1).

It would be interesting to see whether the bound of Theorem 1 is tight for any number of preparations k. For $k > 3$, the above method becomes computationally challenging.

V. DISCUSSION

We presented an upper bound on the amount of randomness that can be certified in a black-box scenario. This bound is given by the number of different quantum states that enter the measurement device, irrespective of whether these states are fully characterized, partially characterized, or uncharacterized, and holds with and without classical or quantum side information. Hence, even when considering measurements with a large number of outputs (or infinite as in CV systems), the amount of certifiable randomness is still limited by the source, specifically by the number of different preparations. The number of preparations required scales exponentially with the number of random bits to be certified per round. Thus, while certifying a large number of random bits per round is in theory possible, this would be challenging in practice. Indeed, in any

experiment, the number of rounds is finite, which in turn limits the number of possible different preparations (even more so if good statistics is required). For instance, to certify ten random bits per round, more than 10^3 different preparations would be required (even without considering randomness extraction).

ACKNOWLEDGMENTS

We thank Matt Pusey for helpful comments. Financial support by the Swiss National Science Foundation (starting grant DIAQ, Bridge project "Self-testing QRNG," NCCR-QSIT) and the European Union Quantum Flagship project QRANGE is gratefully acknowledged.

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).

[2] M. N. Bera, A. Acin, M. Kus, M. Mitchell, and M. Lewenstein, Randomness in quantum mechanics: Philosophy, physics and technology, Rep. Prog. Phys. **80**, 124001 (2017).

[3] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, npj Quant. Info. **2**, 16021 (2016).

[4] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, Quantum random-number generation and key sharing, J. Mod. Opt. **41**, 2435 (1994).

[5] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, Optical quantum random number generator, J. Mod. Opt. **47**, 595 (2000).

[6] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, A fast and compact quantum random number generator, Rev. Sci. Instrum. **71**, 1675 (2000).

[7] D. Frauchiger, R. Renner, and M. Troyer, True randomness from realistic quantum devices, arXiv:1311.4547 (2013).

[8] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Post-processing for quantum random-number generators: Entropy evaluation and randomness extraction, Phys. Rev. A **87**, 062327 (2013).

[9] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Maximization of Extractable Randomness in a Quantum Random-Number Generator, Phys. Rev. Appl. **3**, 054004 (2015).

[10] M. W. Mitchell, C. Abellan, and W. Amaya, Strong experimental guarantees in ultrafast quantum random number generation, Phys. Rev. A **91**, 012314 (2015).

[11] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. Thesis, University of Cambridge, 2009, arXiv:0911.3814.

[12] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by bell's theorem, Nature (London) **464**, 1021 (2010).

[13] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302(R) (2011).

[14] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device-independent random-number expansion without entanglement, Phys. Rev. A **84**, 034301 (2011).

[15] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Semi-device-independent randomness certification using $n \rightarrow 1$ quantum random access codes, Phys. Rev. A **85**, 052308 (2012).

[16] T. V. Himbeeck, E. Woodhead, R. S. Garcia-Patron, N. Cerf, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, Quantum **1**, 33 (2016).

[17] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination, Phys. Rev. Appl. **7**, 054018 (2017).

[18] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Quantum randomness certified by the uncertainty principle, Phys. Rev. A **90**, 052327 (2014).

[19] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, Quantum randomness extraction for various levels of characterization of the devices, J. Phys. A **47**, 424028 (2014).

[20] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acin, Optimal randomness certification in the quantum steering and prepare-and-measure scenarios, New J. Phys. **17**, 113010 (2015).

[21] Z. Cao, H. Zhou, and X. Ma, Loss-tolerant measurement-device-independent quantum random number generation, New J. Phys. **17**, 125011 (2015).

[22] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-Independent Quantum Random Number Generation, Phys. Rev. X **6**, 011020 (2016).

[23] D. G. Marangon, G. Vallone, and P. Villoresi, Source-Device-Independent Ultrafast Quantum Random Number Generation, Phys. Rev. Lett. **118**, 060503 (2017).

[24] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, Detection-Loophole-Free Test of Quantum Nonlocality, and Applications, Phys. Rev. Lett. **111**, 130406 (2013).

[25] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. Stevens, and L. K. Shalm, Experimentally generated randomness certified by the impossibility of superluminal signals, Nature (London) **556**, 223 (2018).

[26] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan *et al.*, Device-independent quantum random-number generation, Nature (London) **562**, 548 (2018).

[27] L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, and C. Kurtsiefer, Randomness Extraction from Bell Violation with Continuous Parametric Down-Conversion, Phys. Rev. Lett. **121**, 150402 (2018).

[28] T. Lunghi, J. B. Brask, Charles Ci Wen Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Self-Testing Quantum Random Number Generator, Phys. Rev. Lett. **114**, 150501 (2015).

[29] G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, Experimental quantum randomness generation invulnerable to the detection loophole, arXiv:1410.3443 (2014).

[30] F. Xu, J. H. Shapiro, and F. N. C. Wong, Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring, Optica **3**, 1266 (2016).

[31] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, A generator for unique quantum random numbers based on vacuum states, Nat. Photonics **4**, 711 (2010).

[32] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, High-speed quantum random number generation by measuring phase noise of a single-mode laser, Opt. Lett. **35**, 312 (2010).

[33] T. Symul, S. M. Assad, and P. K. Lam, Real time demonstration of high bitrate quantum random number generation with coherent laser light, Appl. Phys. Lett. **98**, 231103 (2011).

[34] D. Aerts and M. Sassoli de Bianchi, The extended Bloch representation of quantum mechanics and the hidden-measurement solution to the measurement problem, Ann. Phys. **351**, 975 (2014).

[35] S. K. Goyal, B. N. Simon, R. Singh, and S. Simon, Geometry of the generalized Bloch sphere for qutrits, J. Phys. A **49**, 165203 (2016).

[36] G. Sentìs, B. Gendra, S. D. Bartlett, and A. C. Doherty, Decomposition of any quantum measurement into extremals, J. Phys. A: Math. Theor. **46**, 375302 (2013).

[37] G. M. D'Ariano, P. L. Presti, and P. Perinotti, Classical randomness in quantum measurements, J. Phys. A **38**, 5979 (2005).

[38] E. Haapasalo, T. Heinosaari, and J.-P. Pellonpää, Quantum measurements on finite dimensional systems: Relabeling and mixing, Quant. Info. Proc. **11**, 1751 (2012).

[39] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Simulating Positive-Operator-Valued Measures with Projective Measurements, Phys. Rev. Lett. **119**, 190501 (2017).

[40] F. Hirsch, M. T. Quintino, T. Vértesi, M. Navascués, and N. Brunner, Better local hidden variable models for two-qubit Werner states and an upper bound on the Grothendieck constant $K_G(3)$, Quantum **1**, 3 (2017).

[41] L. Guerini, J. Bavaresco, M. Terra Cunha, and A. Acín, Operational framework for quantum measurement simulability, J. Math. Phys. **58**, 092102 (2017).

[42] R. Konig, R. Renner, and C. Schaffner, The Operational Meaning of Min- and Max-Entropy, IEEE Trans. Inf. Theory **55**, 4337 (2009).