PAPER • OPEN ACCESS

Experimental certification of more than one bit of quantum randomness in the two inputs and two outputs scenario

IOP Publishing New J. Phys. 25 (2023) 113022 https://doi.org/10.1088/1367-2630/ad05a6

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
17 March 2023

REVISED
13 October 2023

ACCEPTED FOR PUBLICATION
20 October 2023

PUBLISHED
16 November 2023

PAPER

Experimental certification of more than one bit of quantum randomness in the two inputs and two outputs scenario

Alban Jean-Marie Seguinard[1], **Amélie Piveteau**[1], **Piotr Mironowicz**[1,2,*] and **Mohamed Bourennane**[1]

[1] Department of Physics, Stockholm University, S-10691 Stockholm, Sweden
[2] Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, Gdańsk, 80-233, Poland
* Author to whom any correspondence should be addressed.

E-mail: piotr.mironowicz@gmail.com

Keywords: randomness generation, randomness certification, Bell inequalities, quantum non-locality, entropy accumulation theorem

Abstract

One of the striking properties of quantum mechanics is the occurrence of the Bell-type non-locality. They are a fundamental feature of the theory that allows two parties that share an entangled quantum system to observe correlations stronger than possible in classical physics. In addition to their theoretical significance, non-local correlations have practical applications, such as device-independent randomness generation, providing private unpredictable numbers even when they are obtained using devices delivered by an untrusted vendor. Thus, determining the quantity of certifiable randomness that can be produced using a specific set of non-local correlations is of significant interest. In this paper, we present an experimental realization of recent Bell-type operators designed to provide private random numbers that are secure against adversaries with quantum resources. We use semi-definite programming to provide lower bounds on the generated randomness in terms of both min-entropy and von Neumann entropy in a device-independent scenario. We compare experimental setups providing Bell violations close to the Tsirelson's bound with lower rates of events, with setups having slightly worse levels of violation but higher event rates. Our results demonstrate the first experiment that certifies close to two bits of randomness from binary measurements of two parties. Apart from single-round certification, we provide an analysis of finite-key protocol for quantum randomness expansion using the Entropy Accumulation theorem and show its advantages compared to existing solutions.

1. Introduction

Randomness is one of the basic resources in information processing. Randomly generated numbers find applications in areas such as cryptography, where they are one of the key elements of protocols such as data encryption standard (DES) or advanced encryption standard (AES). The standard document *RFC 4086 - Randomness Requirements for Security* [1] lists such fields of application as creating private keys for algorithms used in digital signatures, keys and initialization values for encryption, generating secure PINs and passwords, keys for MAC (Message Authentication Code) algorithms or nonces, i.e. numbers that are being used just once in cryptographic communication and cannot be further reused.

It is a known fact that using classical computers, which operate on deterministic algorithms, it is not possible to generate truly random numbers, but only sequences of pseudo-random values, which at first glance resemble truly random numbers, but are not able to guaranteed to be unpredictable. Anyone who knows the algorithm used to create them and its input parameters, i.e. the so-called seed, can determine all the numbers that will ever be obtained using the deterministic generator.

The situation is conceptually different in quantum mechanics since its essence is processes that behave in a non-deterministic way. Thus, many quantum phenomena have intrinsic randomness. The so-called coherence of quantum states can be shown to be directly related to the complete unpredictability of certain quantities [2].

Nevertheless, verifying that a quantum device works as expected is much more difficult than checking the correctness of deterministic algorithms. Typically, we cannot tell if a quantum device behaves exactly as designed, and imperfections in both quantum states and measurements can cause the entire process to lose quantum characteristics, such as Bell inequality violation [3]. The situation is even worse due to the complexity of quantum devices and their finesse, as we are often unable to even check whether the components we use have not been intentionally manipulated by a malevolent adversary.

An important milestone towards solving this problem was the emergence of the so-called device-independent approach [4], which allows the assessment of the fidelity of a quantum device based on its visible external behavior. The early works containing experimental implementations of quantum randomness protocols presented a proof of concept [5], but they were not very efficient in terms of the generation ratio. Recently, a new result called the entropy accumulation theorem (EAT) was introduced and proven [6–8]. This theorem allowed for a determination of the amount of randomness that is certified to be generated by a particular quantum device with finite statistical description.

The results contained in our work concern two tightly related concepts within the realm of device-independent quantum cryptography, *viz.* quantum randomness certification and randomness expansion [9]. Quantum randomness certification primarily aims to verify the genuineness and quality of random outcomes generated by a quantum process, ensuring that they are not influenced by hidden variables or predictable patterns. The first implementations of the concept [5, 10, 11] were able to provide a guarantee that the numbers obtained from a quantum device are not possible to be pre-determined or predicted with certainty. On the other hand, the execution of the protocols itself consumes a certain amount of randomness for choosing the settings used by involved parties. Thus, the protocols were not providing a net gain, i.e. they used for their executions more randomness than they generated. For this reason, these protocols were providing only certification of randomness of the generated number, but no increase in its amount.

A trial to overcome this drawback was a distinction between generation and test rounds and the use of biased settings distributions which consumed less input randomness. Protocols that employ a particular setting for randomness generation are called spot-checking protocols [12]. This approach aimed to reduce the use of the randomness below the amount that is generated as the output of the device, thus providing a positive net gain. Since in the course of running a protocol the total amount of randomness increases, such protocols are called randomness expansion protocols [13–16]. In other words, randomness expansion goes beyond mere verification; it strives to extract additional random bits from a limited source of randomness, effectively expanding the available pool of random data.

While both concepts are vital in quantum cryptography and information processing, randomness certification focuses on the quality assurance of a single event, not taking into account the net gain of the amount of randomness. Randomness certification is particularly relevant for quantum randomness amplification scenarios and theoretical considerations [17, 18]. On the other hand, randomness expansion explores methods to maximize the number of random bits obtained from uncertain sources. These complementary approaches play crucial roles in enhancing the security and efficiency of quantum cryptographic protocols and applications. In this work, we cover both of them.

The basis for device-independent randomness certification and expansion is quantum entanglement between separated systems. This suggests that the more entangled quantum systems, up to a certain entanglement measure [19], the more randomness one could expect. In [20] this natural expectation was shown not to hold. For instance, protocols obtaining the maximal violation of the Clauser-Horne-Shimony-Holt (CHSH) Bell expression [21] certify 1.23 bits of min-entropy, and it is possible to certify arbitrarily close to 2 bits of min-entropy with almost unentangled states using the so-called tilted CHSH expressions. The protocols using the original CHSH are robust as even a tiny violation of the Bell inequality leads to a positive amount of certified randomness. For this reason, this expression has been used in a couple of physical implementations of randomness expansion protocols [15, 22]. The tilted CHSH has the drawback that when using states close to being unentangled, the protocols are not robust, since even tiny imperfections possibly lead to correlations possible in classical physics, and in consequence fail to certify randomness. The problem of non-trivial relation between non-locality, randomness, and entanglement has been further investigated in [23–27].

Thus, one of the important problems is how to obtain the largest possible amount of certified randomness in terms of individual rounds by using a given device with the simplest configuration of settings and outcomes which is at the same time robust. It is easy to see that a device involving two components, A and B, each generating one output bit, allows for a maximum of two random bits generation per round. The first protocols allowing certification of the maximal amount of two bits with the maximally entangled state where one of the parties uses three measurement settings are presented in [28]. Simpler protocols that use non-maximally entangled states but the maximal Bell violation for certification of 2 bits of randomness in

setups with two binary measurements by the introduction of novel Bell expressions were given in [29] and were shown to be more robust than the tilted CHSH expressions. In this work, we present an experimental implementation of these protocols, along with the analysis of certified randomness using numerical techniques to provide a lower bound on the randomness generated per round [13, 14]. We consider min-entropy as in [20, 22] and also the von Neumann entropy, where the latter quantity is always lower bounded by the former, and is also more relevant for randomness extraction protocols.

2. Methods

For a given behavior of a quantum device, our task is to specify lower bounds on the generated randomness. To this end, it is necessary to perform a complex optimization taking into account all devices implementing this behavior allowed by the laws of quantum physics. This optimization is essentially a consideration of the set of all possible probability distributions obtainable by quantum devices that satisfy certain observable constraints. There are no known tools to optimize accurately over such sets of probability distributions.

Fortunately, there are approximate techniques that determine the so-called relaxations of the sets of all possible constrained distributions of quantum probabilities. It turns out that if the optimization over probability distributions is allowed to cover a set slightly wider than that allowed by quantum mechanics, the optimization problem can be dealt with efficiently using convex optimization techniques, in particular, semi-definite programming (SDP) [30–32], e.g. using the Navascués-Pironio-Acin (NPA) [33, 34] in the variant we discuss in section 2.1. Next, in section 2.2 we describe the Bell expressions that we use as certificates for the randomness certification and expansion. In section 2.3 we mention a technique that allows us to evaluate the amount of the certified for practical applications involving finite statistics.

Min-entropy and von Neumann entropy are measures of uncertainty in different contexts within quantum information theory. The classical min-entropy, denoted as H_∞ quantifies the minimum amount of unpredictability associated with a probability distribution by taking the negative logarithm of the largest probability, i.e. the guessing probability, within that distribution, *viz.* $H_\infty[\{p_i\}_i] = -\log_2(\max_i p_i)$. It is often used in the context of privacy amplification and randomness extraction, emphasizing security-critical applications [35–38].

The other quantity, i.e. von Neumann entropy, denoted as H, measures the overall mixedness or impurity of a quantum state. It is defined for density matrices and captures the degree of entanglement and information encoded within a quantum system. For a state ρ_A in a space Q_A the von Neumann entropy is given by $H(Q_A)_\rho \equiv -\mathrm{Tr}[\rho\log_2(\rho)]$. For multipartite states, e.g. on space Q_A and Q_E with a state ρ_{AE}, the conditional von Neumann entropy is defined as $H(Q_A|Q_E)_{\rho_{AB}} \equiv H(Q_AQ_E)_{\rho_{AE}} - H(Q_E)_{\rho_{AE}}$. Pure states have zero von Neumann entropy and maximally mixed states have it equal to the logarithm of the dimension of the Hilbert space. Von Neumann entropy is used in EAT. While min-entropy is concerned with single-shot predictability of the classical probability distribution of the measurement results, von Neumann entropy describes the global properties of quantum states, emphasizing their entanglement and quantum correlations [39]. It can be shown that the min-entropy is a lower bound on the Shannon entropy of a given random variable.

2.1. Numerical calculation of von Neumann entropy

The NPA hierarchy is used to formulate SDPs which after being solved provide an upper bound on the probability of guessing the value of a random number by an adversary [36]. Thus, the values obtained using this method are suitable for certification of the generated randomness from quantum devices. The technique is limited only to optimizing functions that are linear expressions of probabilities. Let us consider the set of all conditional probability distributions $\{P(a,b|x,y)\}$, where a and b are the outcomes of the measurements performed by Alice and Bob, when their measurement settings are x and y, respectively. The general form of a Bell expression, which is a linear functional of the conditional probability distributions, is

$$\sum_{a,b,x,y} c_{a,b,x,y} P(a,b|x,y)\,, \tag{1}$$

where the coefficients $\{c_{a,b,x,y}\}$ are real numbers. One of the proposed protocols from [28] used the following Bell operator as a randomness privacy certificate:

$$C(0,1) + C(0,2) + C(1,0) + C(1,1) - C(1,2)\,, \tag{2}$$

where the correlators are defined as follows:

$$C(x,y) \equiv P(0,0|x,y) + P(1,1|x,y) - P(0,1|x,y) - P(1,0|x,y)\,. \tag{3}$$

One may note that (2) consists of a well-known CHSH expression [21] plus an additional term. The maximal value allowed in quantum mechanics, i.e. the Tsirelson bound, of (2) is $1+2\sqrt{2}$. When the Tsirelson bound is achieved, then the quantum state and all measurement operators are uniquely determined [40], and for the pair of settings $x=0, y=0$, the measurement results are uniformly distributed, $\forall a,b P(a,b|0,0)=0.25$. A full analysis of the protocol of randomness generation using (2) including randomness accumulation and extraction aspect has been presented in [14].

In a recent work [41] SDP was used to produce an approximation of the matrix logarithm function, resulting in a numerical method for efficient optimization of expressions on the quantum relative entropy [42]. Furthermore, this method has been used to determine the lower bounds of the conditional von Neumann entropy certified in the device-independent approach [43] using the extended NPA [44] with the NCPOL2SDPA tool [45].

Let Q_A, Q_B, and Q_E be the Hilbert spaces of devices of Alice, Bob, and adversary, respectively, and ρ_{Q_A,Q_B,Q_E} their shared tri-partite quantum system. The numerical technique can be applied to calculate a lower bound on the conditional von Neumann entropy

$$H(Q_A,Q_B|x=x^*,y=y^*,Q_E)_{\rho_{Q_A,Q_B,Q_E}}. \tag{4}$$

Let $\{\{M_{a|x}\}_a\}_x$ and $\{\{N_{b|y}\}_b\}_y$ denote operators of the positive operator valued measurements performed by Alice and Bob, respectively. This employs the Gauss–Radau quadrature rule to lower bound (4). Let w_i and t_i be the nodes and weights defined by this quadrature. A lower bound on (4) can be obtained from [46]:

$$\sum_i c_i \sum_{a,b=0,1} \inf_{\substack{Z_{a,b}\in B(Q_E),\\ \mathrm{cond}(P)}} \left(1+F\left[M_{a|x^*},N_{b|y^*},Z_{a,b},t_i\right]\right), \tag{5}$$

where $F[M_{a|x^*},N_{b|y^*},Z_{a,b},t_i]$ is defined as $\mathrm{Tr}\left[\rho_{Q_A,Q_B,Q_E}(O_1+O_2)\right]$. In (5) $\mathrm{cond}(P)$ expresses that the probability distribution $P(a,b|x,y)\equiv \mathrm{Tr}[\rho_{Q_A,Q_B}M_{a|x^*}\otimes N_{b|y^*}]$ satisfies a certain, specified by the protocol, set of linear constraints. The operators O_1 and O_2 are defined by

$$O_1 \equiv M_{a|x^*}\otimes N_{b|y^*}\otimes\left(Z_{a,b}+Z_{a,b}^\dagger+(1-t_i)Z_{a,b}Z_{a,b}^\dagger\right), \tag{6a}$$

$$O_2 \equiv t_i\left(\mathbb{1}_{Q_AQ_B}\otimes Z_{a,b}Z_{a,b}^\dagger\right). \tag{6b}$$

c_i are coefficients calculated from the Gauss–Radau quadrature as $c_i\equiv w_i/(t_i\log(2))$. The index i in the summation (5) takes the values indexing the nodes in the quadrature, omitting the last one.

2.2. Bell certificates

To certify the randomness, we employed the recently announced two families of Bell expressions [29]. First of them is, parametrized by $\delta\in(0,\pi/6]$, defined as

$$I_\delta \equiv C(0,0)+\frac{1}{\sin\delta}\left(C(0,1)+C(1,0)\right)-\frac{1}{\cos 2\delta}C(1,1). \tag{7}$$

The members of this family have self-testing properties, use two settings for each party, and can certify two bits of randomness for the measurement settings $x^*=y^*=0$.

The second family, parametrized by $\gamma\in[0,\pi/12]$ defines the Bell expressions:

$$J_\gamma \equiv C(0,0)+\left(4\cos^2\left[\gamma+\pi/6\right]-1\right)\left(C(0,1)+C(1,0)-C(1,1)\right). \tag{8}$$

These Bell expressions also use two settings and have self-testing properties, yet in most cases do not certify two bits of randomness.

The Tsirelson bounds for (7) and (8) are $I_\delta^Q\equiv 2\cos^3\delta/\left(\cos(2\delta)\sin\delta\right)$, and $J_\gamma^Q\equiv 8\cos^3\left[\gamma+\pi/6\right]$, respectively. The relative Bell value is defined as $I_\delta^{exp}/I_\delta^Q$ and $J_\gamma^{exp}/J_\gamma^Q$, where I_δ^{exp} and J_γ^{exp} are the values of the Bell expressions (7) and (8) obtained in the experiment, respectively. The relative Bell value attains the value of 1 in the noiseless cases. For correlation-based Bell expressions, like those analyzed in this paper, if η is the relative value of the Bell expression, and the relative value η is attained with the noised state:

$$\eta\rho_{Q_A,Q_B}^{\mathrm{optimal}}+(1-\eta)\rho_{Q_A,Q_B}^{\mathrm{white}}, \tag{9}$$

where $\rho_{Q_A,Q_B}^{\mathrm{optimal}}$ and $\rho_{Q_A,Q_B}^{\mathrm{white}}$ are the quantum state providing the Tsirelson bound and the maximally mixed state, respectively.

2.3. Randomness expansion with finite statistics

In real-world applications, one needs to consider the case when the observed quantities, like the values of the certificates, are known only with some limited certainty, due to a finite number of statistics gathered to estimate them. This is to be contrasted with the asymptotic case, valid in the idealized situation of an infinite number of repetitions of the experiment. One of the methods to cover such uncertainties is based on the concept of smooth entropies [47, 48]. In this work we apply the EAT method [6–8], which we recapitulate here in a limited scope; we refer to [14] for a detailed discussion.

In the performed experiments, ith step can be viewed as an application of a completely positive trace-preserving channel $\mathcal{N}_i$ acting on a quantum register R_{i-1}, and transforming its state on a quantum register R_i, and, at the same time, preparing states of classical registers A_i, B_i, X_i, and Y_i, which store the measurement results a and b together with the measurement settings x and y of the ith round of the experiments. The following form of the Markov chain condition holds: $I(A^{i-1}B^{i-1} : X_i Y_i | X^{i-1}Y^{i-1}E)$, where the superscript notation means a vector containing the values of given registers in subsequent steps up to the step specified in the superscript value, and E is an arbitrary quantum system possibly entangled with the registers $\{R_i\}$. A collection of such channels in the framework of EAT is called EAT channels. For the measurement settings x and y and results a and b we define the score function U of the Bell expression (1) as

$$U(a,b,x,y) \equiv \sum_{a,b,x,y} c_{a,b,x,y}\chi(a,b,x,y)/P(x,y), \tag{10}$$

where $\chi(\cdot,\cdot,\cdot,\cdot)$ is the indicator of a given measurement event, and $P(x,y)$ is the probability of the given pair of settings.

For given EAT channels and fixed i, a joint quantum state σ_{RE} on the register R_{i-1} and the space E is called feasible if cond(P) holds for $a = A_i$, $b = B_i$, $x = X_i$ and $y = Y_i$. For a given EAT channel, their min-tradeoff function f is any real function affine in $P \equiv \{P(a,b|x,y)\}$ such that for all i for any feasible joint quantum state σ_{RE} on the register R_{i-1} and the space E it holds $f[P] \leqslant H(Q_A, Q_B|x,y,Q_E)$. These definitions using the EAT theorem allow to provision of explicit warranties on the quality of the generated random numbers [49]. We provide such analysis of our experiments in section 3.3.

3. Results

In this section, we describe the experimental setup and report regarding the analysis of the randomness generated in the series of experiments.

3.1. Experimental setup

Ultraviolet light centered at a wavelength of 390 nm is focused onto two 2 mm thick β barium borate nonlinear crystals placed in interferometric configuration to produce photon pairs emitted into two spatial modes (a) and (b) through the second order degenerate type-I spontaneous parametric down-conversion process. The spatial, spectral, and temporal distinguishability between the down-converted photons is carefully removed by coupling to single-mode fiber, passed through narrow-bandwidth interference filters (F) and quartz wedges respectively. We have realized these quantum protocols by using polarization entangled pairs of photons $|\phi+\rangle = |HH\rangle + |VV\rangle$.

The measurements for Alice are performed by a half-wave plate (HWP) oriented θ_{A0} or θ_{A1}, and the measurements for Bob are performed by an HWP-oriented θ_{B0} or θ_{B1}. The polarization measurement was performed using PBS and single-photon detectors (D) placed at the two output modes of the PBS. Our detectors are actively quenched Si-avalanche photodiodes. All single-detection events were registered using a VHDL-programmed multichannel coincidence logic unit, with a time coincidence window of 1.7 ns.

We performed the experiment for the Bell expressions (7) at a low rate (approximately 675 two-photon coincidences per second). At these low rates, the multi-photon pair emissions are small, and accidental events can be neglected. We benchmark the state preparation by measuring the average visibility in the diagonal polarization basis of 99.07. Each of the measurement runs was taken 180 times with each run with a collection time of 250 s. We have also performed a state tomography to estimate the fidelity of the state and obtained 99.63 ± 0.04.

For the Bell expressions (8), the rate was around 780 two-photon coincidences per second with 160 measurements of 250 s and the visibility in the diagonal polarization basis of 99.13%. We were able to increase the rate slightly while maintaining visibility above 99%. The fidelity of the state obtained by state tomography is 99.75 ± 0.02. For these two experiments, the total average number of events is around 120 million.

We have also performed an experiment for the Bell expressions (7) at a higher rate of 2000 two-photon coincidences per second, the visibility was on average 98.73 in diagonal polarization basis. For this

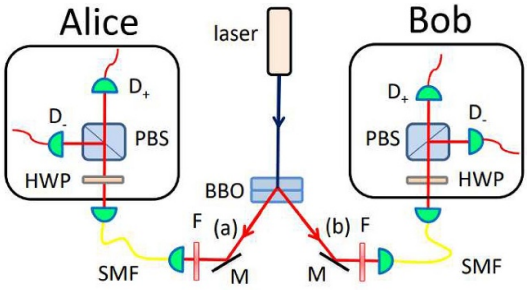

Figure 1. Experimental setup. Entangled photon pairs are generated through the SPDC process. The emitted photons in modes (a) and (b) are coupled to single mode fiber (SMF) and signal is filtered (F). Each of the two stations' measurements is composed of a halfwave plate (HWP), a polarization beam splitter (PBS) and single photon detectors (D_+ and D_-). (See main text for details).

measurement, we have opted to work at a higher rate to send more information per second. However, increasing the rate has the effect of increasing the multi-photon pair emission and therefore reducing visibility. Each of the measurement runs was taken 100 times with each run with a collection time of 250 s. For this experiment, the total average number of events is around 200 million.

To reduce experimental errors in the measurements, we used computer-controlled high-precision motorized rotation stages to set the orientation of wave-plates with repeatability precision 0.02°. The error was estimated for each of the experiments by taking the standard deviation of the measurements.

The experimental setup is illustrated in figure 1. The angles of the HWPs for the experiments are provided in the appendix.

3.2. Certified randomness in asymptotic case

To calculate the guessing probability, we reflected the experimental results by imposing on the maximization a constraint that the value of the Bell expression is equal to the one observed in the experiment.

To calculate the conditional von Neumann entropy, we have considered two different sets of constraints for the certification of the von Neumann entropy using the optimization (5). The standard approach [5] is to impose a constraint that the value of the relevant Bell expression is equal to the one from the experiment. A more involved method [28, 50–52] is to constrain the optimization with more than one parameter. The purpose of this is to increase the amount of the certified randomness, at a price of more demanding error analysis for finite data sets, and complicated numerical calculations. We imposed a constraint that each of the correlators $C(0,0)$, $C(0,1)$, $C(1,0)$, and $C(1,1)$ are equal to those from the experiment. Note that the latter constraints are stronger than the former one, as the Bell expressions (7) and (8) are functions of correlators.

To be more precise, we have further relaxed the above constraints. We formulated the single parameter constraint in a form that the value of the relevant Bell expression is not smaller than the one from the experiment. The constraints for more parameters we formulated in a manner that each of the correlators $C(0,0)$, $C(0,1)$ and $C(1,0)$ are not smaller than the one obtained in the experiment, and $C(1,1)$ is not greater than the one from the experiment. It is easy to see that the minimization of the conditional von Neumann entropy with equalities as a constraint will be lower bound by the minimization with inequalities. The reason behind this relaxation is that this improves the stability of the numerical optimization, as the feasible region has a wider interior than with equality constraints. Similarly, for the guessing probability calculations, we relaxed the equality with an inequality imposing a constraint of the optimization that the value of the Bell is not smaller than the one obtained in the experiment. The relaxation of the equality constraints by replacing them with inequalities does not weaken the security proofs. Indeed, the proofs employ the lower bounds on the entropies, and relaxing the constraints of minimization procedures will only decrease the resulting values. Thus the conclusions we draw about the certified randomness are even more cautious than if we had not used these relaxed constraints.

As mentioned, the method [43] requires specifying the number of nodes in the quadrature. We calculated both variants of constraints with 6 nodes, and the optimization with the correlation constraints also with 8 nodes. To improve the certification of entropy, one can increase the number of nodes, but this comes with the price of a longer optimization time.

3.2.1. I_δ Bell expressions and high relative violation

Firstly, we performed the experiment for the Bell expressions (7). We concentrated on the quality of the source, at the cost of the generated events rate. The experiment has been performed for $\delta = 0.45, 0.5, 0.52$.

Table 1. Randomness certified by Bell expressions (7) for the experiment concentrated on high relative violation of the Bell inequality in the asymptotic case.

	von Neumann entropy			
δ	Cor. (8 Radau)	Cor. (6 Radau)	Bell viol. (6 Radau)	H_∞
0.52	1.88	1.87	1.77	1.50
0.5	1.77	1.76	1.64	1.33
0.45	1.77	1.76	1.61	1.28

Table 2. The experimental values of the Bell expression (7) for the experiment concentrated on high relative violation of the Bell inequality.

δ	$I_\delta^{\text{Classique}}$	$I_\delta^{\text{Quantique}}$	$I_\delta^{\text{Experimental}}$
0.52	5	5.2	5.179 ± 0.006
0.5	5.022	5.218	5.187 ± 0.006
0.45	5.207	5.4	5.366 ± 0.007

Table 3. Randomness certified in the experiment by Bell expressions (8) in the asymptotic case.

	von Neumann entropy			
γ	Cor. (8 Radau)	Cor. (6 Radau)	Bell viol. (6 Radau)	H_∞
0	1.81	1.80	1.72	1.43
$\frac{\pi}{24}$	1.76	1.75	1.68	1.21
$\frac{\pi}{12}$	1.55	1.54	1.39	0.98

Table 4. The experimental values of the Bell expression (8).

γ	$J_\gamma^{\text{Classique}}$	$J_\gamma^{\text{Quantique}}$	$J_\gamma^{\text{Experimental}}$
0	5	5.19	5.174 ± 0.007
$\frac{\pi}{24}$	3.55	3.99	3.968 ± 0.005
$\frac{\pi}{12}$	2	2.83	2.811 ± 0.003

The obtained relative Bell values were 0.994, 0.994, and 0.997, respectively, and the certified randomness is shown in table 1.

We observed 675 events per second, and thus the randomness generation rate for $\delta = 0.52$ is 1270 bits of von Neumann entropy or 1012 bits of min-entropy, per second.

If only finite statistics are taken into account, one should consider also the uncertainty in evaluation e.g. the Bell expression value. In the case of the considered experiment, the values are shown in table 2 with theoretical boundaries for comparison, for $\delta = 0.45, 0.5, 0.52$, respectively. The Gauss–Radau approximation with six nodes showed that this Bell violation allows certifying 1.54, 1.58, and 1.72 bits of von Neumann entropy, respectively, thus slightly less than the asymptotic case of table 1.

3.2.2. J_γ Bell expressions

Secondly, we investigated the Bell expressions (8). We considered the value $\gamma = 0, \pi/24, \pi/12$. The obtained relative Bell values are 0.996, 0.993, and 0.994, respectively. The certified randomness is shown in table 3.

The observed event rate was 780 per second, giving the randomness generation rate 1300 bits of von Neumann entropy or 1030 bits of min-entropy, per second.

The violation of Bell's inequality is given in table 4.

3.2.3. I_δ Bell expressions and high event rate

The third of the performed experiments concerned also the Bell expressions (7). We performed it for values $\delta = 0.5, 0.4, 0.3$ observing the relative Bell values 0.987, 0.991, and 0.991, respectively. We show the certified randomness in table 5.

The rate of observed events was 2000 per second, so the randomness generation rate, when taking $\delta = 0.4$ is 3180 bits of von Neumann entropy or 2120 bits of min-entropy, per second.

The violation of Bell's inequality is given in table 6.

Table 5. Randomness certified by Bell expressions (7) in the asymptotic case for the experiment concentrated on the high rate of the observed events.

	von Neumann entropy			
δ	Cor. (8 Radau)	Cor. (6 Radau)	Bell viol. (6 Radau)	H_∞
0.5	1.50	1.50	1.26	0.89
0.4	1.59	1.58	1.41	1.06
0.3	1.52	1.51	1.21	0.85

Table 6. The experimental values of the Bell expression (7) for the experiment concentrated on the high rate of the observed events.

δ	$I_\delta^{\text{Classique}}$	$I_\delta^{\text{Quantique}}$	$I_\delta^{\text{Experimental}}$
0.5	5.02	5.22	$5.15 \pm 0,01$
0.4	5.57	5.76	$5.71 \pm 0,01$
0.3	6.98	7.15	7.09 ± 0.01

3.3. Finite statistics analysis for randomness expansion with I_δ

Let us now concentrate on the case of the I_δ Bell expression (7) for $\delta = 0.52$ and high relative violation, as presented in section 3.2.1. Recall that the Bell value was in that case $I_{0.52}^{\text{Experimental}} = 5.179$ with the standard deviation $\sigma_{I,0.52} = 0.006$, whereas the Tsirelson bound is 5.1967. Let us assume that close to the observed value the error distribution is near to Gaussian.

For the confidence interval of one standard deviation, we perform numerical optimization with the constraint that the Bell value is equal at least $w_1 = I_{0.52}^{\text{Experimental}} - \sigma_{I,0.52}$. We note that this constraint is weaker than the one stating that the Bell value is within the range

$$\left[I_{0.52}^{\text{Experimental}} - \sigma_{I,0.52}, I_{0.52}^{\text{Experimental}} + \sigma_{I,0.52}\right], \tag{11}$$

so in fact the actual confidence interval can be expected to be higher than 68%. The certified von Neumann entropy for the violation equals at least w_1 calculated at level 2 of NPA with 6 noded of the quadrature is $r_1 = 1.7162$. To calculate the properties of the min-tradeoff function for EAT channels we calculated the certified entropy in the neighborhood of the violation value w_1, *viz.* at points $w_1 - \Delta$ and $w_1 + \Delta$ for $\Delta = 0.001$, and we obtained the values $r_{1-} = 1.7060$ and $r_{1+} = 1.7265$, respectively. This means, by the convexity of the bounding function, that the line tangent to the von Neumann entropy lower bound is of the form $g_1(x) \equiv r_1 + b_1 \cdot (x - w_1)$ with a certain, specified but unknown precisely, value of b_1 in the set $\left[\frac{r_1 - r_{1-}}{\Delta}, \frac{r_{1+} - r_1}{\Delta}\right] \approx [10.239, 10.259]$.

Now, for the EAT theorem, we need to specify the range of the min-tradeoff function, see lemma III.1 in [14]. The minimal value of $I_{0.52}$ allowed in quantum mechanics is equal to the negation of the Tsirelson bound, *viz.* $-I_{0.52}^Q$. The algebraic bound on $I_{0.52}^{Alg}$ is obtained with $C(0,0) = C(1,0) = C(0,1) = -C(1,1) = 1$ in (7) and is equal 7.0005. Thus the range of g_1 is within the set

$$\left[r_1 + \frac{r_{1+} - r_1}{\Delta} \cdot \left(-I_{0.52}^Q - w_1\right), r_1 + \frac{r_{1+} - r_1}{\Delta} \cdot \left(I_{0.52}^{Alg} - w_1\right)\right], \tag{12}$$

which has a diameter equal

$$d_1 \equiv \frac{r_{1+} - r_1}{\Delta} \cdot \left(I_{0.52}^{Alg} + I_{0.52}^Q\right) \approx 125.13. \tag{13}$$

A crucial parameter describing spot-checking protocols that use EAT is the probability of a test round, denoted usually by γ. We follow the EAT formulation of theorem II.1 in [14] and define:

$$\epsilon_V(\beta, \gamma, d) \equiv \frac{\beta \cdot \ln(2)}{2} \cdot \left[\log_2\left(2 \cdot 4^2 + 1\right) + \sqrt{d^2/\gamma + 2}\right]^2, \tag{14a}$$

$$\epsilon_K(\beta, d) \equiv \frac{\beta^2 \cdot \left(2^{\beta \cdot \left(\log_2(4) + d\right)}\right)}{6(1-\beta)^3 \cdot \ln(2)} \cdot \left[\ln(2) \cdot \left(\log_2(4) + d\right) + 2\right]^3, \tag{14b}$$

$$\epsilon_\Omega(\beta, p_\Omega, \epsilon_S) \equiv \left(1 - \log_2\left(p_\Omega \cdot \epsilon_S\right)\right)/\beta. \tag{14c}$$

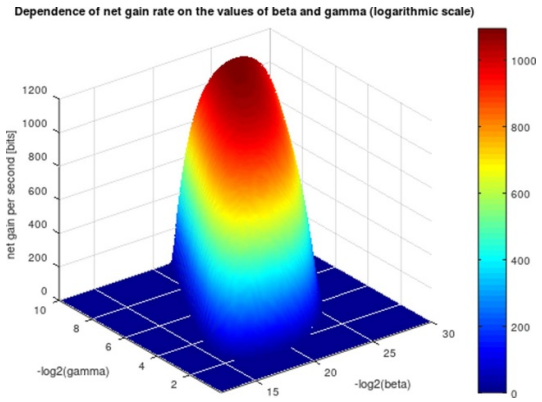

Figure 2. Plot of the dependence of net gain rate on the values of β and γ parameters from (14) in logarithmic scale for the protocol using the certificate (7) with $\delta = 0.52$ and one standard deviation confidence interval. We note that the optimal values are on a constant ratio between $\log_2(\beta)$ and $\log_2(\gamma)$.

The value d correspond to the difference $\mathrm{Max}[g] - \mathrm{Min}[g]$ in lemma III.1. We used a slightly modified formula for ε_K compared to [14], *viz.* we first used the identity $\forall_x \ln(2^x) = x \ln 2$, and then concavity of logarithm, to split the expression into a sum of two logarithms, to avoid numerical round-off errors. The entropy consumption is $2n^{\mathrm{test}}$ bits for choosing settings for test rounds and $h_2(\gamma)$ bits for selecting which rounds are used for testing, where h_2 is the binary entropy.

In the experiment, we performed $n^{\mathrm{test}} \approx 120\,000\,000$ rounds testing the value of the score function. In the experiment, we did not perform the actual series of generation rounds, and thus our work aims to test the feasibility of the novel certificates in near future implementation. Let n denote a hypothetical number of generation rounds performed by a device of similar quality as the one presented in this paper. For the sake of comparison with an approach involving a high rate of rounds with low violation of CHSH inequality, we juxtapose our results with the ones given in [15].

The parameter describing the quality of the raw randomness obtained in a random numbers generator is the soundness error ϵ_S reflecting the probability of distinguishing the generated sequence from the uniform one. In [15] the value $\epsilon_S = 3.09 \times 10^{-12}$ was reported, with the total time of running the experiment was 19.2 h, taking as the input 6.778×10^8 bits and returning the output containing 9.350×10^8 bits of certified randomness. This resulted in a net gain of 2.57×10^8 bits or a net gain rate of $3718.2\,\mathrm{bit\,s^{-1}}$. The ratio between entropy consumption to production is 0.72.

In our experiment, the n^{test} rounds were performed in 180 000 s. We consider hypothetical generation rounds performed with the same device, intertwined with the test rounds occurring with probability given by some value of γ which we establish below, where we consider the parameters range providing the same soundness error as in [15] and compare the net gain rates.

First, let us consider the confidence interval of one standard deviation. In theorem II.1 of [14] we use $t = r_1$, $p_\Omega = 0.68$, $d = d_1$ and assume the same event rate as in the test rounds. We consider a wide range of parameters β and γ, as shown in figure 2. For instance $\beta = 10^{-7}$ and $\gamma = 0.01$ would provide net gain rate of $1033.3\,\mathrm{bit\,s^{-1}}$ when about 1.2×10^{10} rounds would be needed; the ratio of entropy consumption to production is 0.06.

For a confidence interval of three standard deviations, the Bell value is equal to at least $w_3 = I_{0.52}^{\mathrm{Experimental}} - 3\sigma_{I,0.52} \approx 5.161$, certifying at least $r_3 = 1.5943$ bits of von Neumann entropy. The tangent line is $g_3(x) \equiv r_3 + b_3 \cdot (x - w_3)$ with $b_3 \in [10.09, 10.102]$. The diameter of the range set of g_3 is $d_3 \approx 123.22$. The optimal net gain rate in that case would be about $1013.4\,\mathrm{bit\,s^{-1}}$; the ratio of entropy consumption to production is about 0.07. Even though it is lower than the net gain rate obtained in the case with one standard deviation confidence interval, this case provides a success probability of the protocol much higher (0.997) than the other one (0.68).

For the higher rate experiment from section 3.2.3 with $\delta = 0.5$ we have $n^{\mathrm{test}} \approx 2\,000\,000\,000$ obtained in 100 000 s. For three standard deviations confidence interval, we get the randomness lower bound $w_h = 1.1743$, and diameter $d_h = 121.34$, resulting in a net gain rate of about $1951.5\,\mathrm{bit\,s^{-1}}$; the ratio of entropy consumption to production is 0.09. We show the parameter dependence in figure 3.

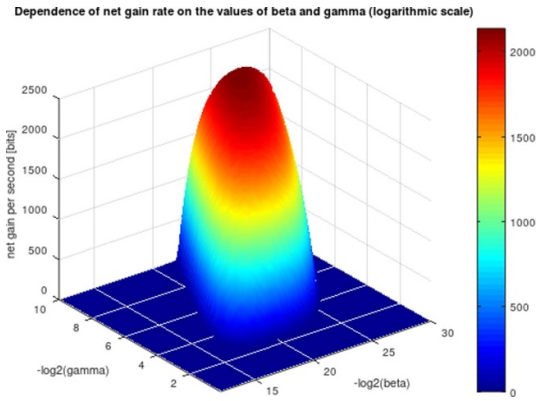

Figure 3. Plot of the dependence of net gain rate on the values of β and γ parameters from (14) in logarithmic scale for the protocol using the certificate (7) with $\delta = 0.5$ and three standard deviation confidence interval for the experiment with increased rate of events (see section 3.2.3).

4. Discussion

The protocol used in the experiments presented in this work was shown to be able to achieve the performance of device-independent randomness expansion secure against a quantum adversary with the rate of about 1.0 kbps net gain with high violation and 2.0 kbps for slightly lower violation of the Bell expression (7) but higher source rate. This is less than another device-independent protocol based on a high rate source and low violation of CHSH where the net gain rate of 3.7 kbps was achieved [15]. Another recent protocol [16] achieved 5.0 kbps in a semi-device independent scenario, where the quantum state preparation was trusted. Earlier works presenting device-independent randomness expansion using a low violation of CHSH include [53] obtaining a net gain rate of about 0.1 kbps, and the work [22] where the net gain rate was 0.24 kbps. Our result shows that using a lower rate source with high violation of Bell inequalities other than CHSH can provide a net gain rate of von Neumann randomness of similar performance. One can expect that an effort to increase the source rate in our experiment would potentially lead to significantly more efficient protocols. The version of the experiment that operates with slightly lower, but still very high, Bell violation but a higher source rate revealed to be more efficient. This indicates a clear engineering tradeoff between violation and source frequency in the high-fidelity regime. The proposed protocols have a much better ratio between entropy consumption and production than, for instance, the protocol of [53], which can also serve as an advantage.

An important aspect of Bell's expressions are the possible loopholes [54], primarily the freedom-of-choice loophole, the detection efficiency loophole, and the communication loophole; see [55–57] for experiments closing these loopholes. The freedom-of-choice loophole arises when the assumption that the choice of measurement settings is independent of the properties of the entangled particles is not valid. The detection efficiency loophole stems from the fact that in real-world experiments, it is difficult to achieve perfect detection efficiency for all particles involved. If some particles are not detected or their properties are not accurately measured, it can introduce biases in the results, which can be exploited by the malevolent constructor.

The communication, or locality, loophole refers to the possibility of information exchange between entangled particles during the measurement process. This loophole is addressed in experiments by a space-like separation between events occurring in the parties measuring the entangled states. For instance in two randomness expansion experiments presented in [58, 59] the parties Alice and Bob were separated by about 200 m. A novel method for overcoming the locality loophole is given in [60] where a method of quantifying the amount of crosstalk was estimated. A complementary approach exhibiting crosstalk in experiments, but not considered in the framework of randomness certification was delivered by some of us in [61]. In this work, we do not address the problem of closing the loopholes, and leave them for future work.

5. Conclusions

We have presented an experimental setup aiming to generate close to the maximum amount of randomness possible in the binary measurement setup with two parties. We have realized experiments for two different families of Bell expressions and obtained up to 1.88 bits per round, which is close to the theoretical maximum of two bits. We have also performed a comparison of different approaches to randomness, the von Neumann

and min-entropy. The min-entropy is smaller than the von Neumann entropy, whereas some applications take advantage of the latter one. Finally, we have shown, that it may be beneficial for the randomness generation rate, to increase the events rate at the cost of decreasing the quality of the quantum realization. We expect that having close to two bits per elementary event will simplify the randomness extraction procedure, in terms of both requirements for the extractor's seed, and the extraction processing time.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgments

This work was supported by the Knut and Alice Wallenberg Foundation through the Wallenberg Centre for Quantum Technology (WACQT), the Swedish Research Council (VR), and NCBiR QUANTERA/2/2020 (www.quantera.eu) an ERA-Net cofund in Quantum Technologies under the project eDICT. The numerical calculation we conducted using NCPOL2SDPA [45], and MOSEK Solver [62].

Table 7. HWP's angle for the expression (7) for different values of δ.

δ	0.3	0.4	0.45	0.5	0.52
HWP_{A1}	0	0	0	0	0
HWP_{A2}	−63.20	−61.77	−61.05	−60.34	−60.05
HWP_{B1}	22.5	22.5	22.5	22.5	22.5
HWP_{B2}	85.70	84.27	83.55	82.84	82.55

Table 8. HWP's angle for the expression (8) for different values of δ.

γ	0	$\frac{\pi}{24}$	$\frac{\pi}{12}$
HWP_{A1}	0	0	0
HWP_{A2}	30	26.25	22.5
HWP_{B1}	22.5	16.88	11.25
HWP_{B2}	82.5	80.63	78.75

Appendix. Angles

Experiments 1 and 3 are based on the expression (7), which has 4 terms for each δ value. These four terms correspond to the four possible combinations for two HWPs with two angles each. Table 7 shows the angles of these HWPs for each δ value used in our experiments.

The second experiment is based on expression (8). As with the previous expression, four combinations of two HWPs are required for each γ value. Table 8 groups these angles for each gamma used.

For these two equations, several values of each angle were possible, we have chosen to present only those used.

The value of the angles has been rounded to two digits, as we used computer-controlled high-precision motorized rotation stages to set the orientation of wave-plates with repeatability precision 0.02°.

ORCID iD

Piotr Mironowicz https://orcid.org/0000-0003-4122-5372

References

[1] Eastlake 3rd Donald E, Schiller J and Crocker S 2005 Randomness requirements for security *Request for Comments: 4086* (The Internet Engineering Task Force)
[2] Yuan X, Zhou H, Cao Z and Ma X 2015 Intrinsic randomness as a measure of quantum coherence *Phys. Rev.* A **92** 022124
[3] Bell J S 1964 On the Einstein Podolsky Rosen paradox *Phy. Phys. Fiz.* **1** 195
[4] Mayers D and Yao A 1998 Quantum cryptography with imperfect apparatus *Proc. 39th Annual Symp. on Foundations of Computer Science* (*Cat. No. 98CB36280*) (IEEE) pp 503–9
[5] Pironio S *et al* 2010 Random numbers certified by Bell's theorem *Nature* **464** 1021
[6] Dupuis F, Fawzi O and Renner R 2020 Entropy accumulation *Commun. Math. Phys.* **379** 867
[7] Arnon-Friedman R, Renner R and Vidick T 2019 Simple and tight device-independent security proofs *SIAM J. Comput.* **48** 181
[8] Arnon-Friedman R, Dupuis F, Fawzi O, Renner R and Vidick T 2018 Practical device-independent quantum cryptography via entropy accumulation *Nat. Commun.* **9** 459
[9] Colbeck R and Kent A 2011 Private randomness expansion with untrusted devices *J. Phys. A: Math. Theor.* **44** 095305
[10] Pironio S and Massar S 2013 Security of practical private randomness generation *Phys. Rev.* A **87** 012336
[11] Fehr S, Gelles R and Schaffner C 2013 Security and composability of randomness expansion from Bell inequalities *Phys. Rev.* A **87** 012335
[12] Miller C A and Shi Y 2017 Universal security for randomness expansion from the spot-checking protocol *SIAM J. Comput.* **46** 1304
[13] Brown P 2019 On constructions of quantum-secure device-independent randomness expansion protocols *PhD Thesis* University of York
[14] Brown P J, Ragy S and Colbeck R 2019 A framework for quantum-secure device-independent randomness expansion *IEEE Trans. Inf. Theory* **66** 2964
[15] Liu W-Z *et al* 2021 Device-independent randomness expansion against quantum side information *Nat. Phys.* **17** 448
[16] Wang C, Primaatmaja I W, Ng H J, Haw J Y, Ho R, Zhang J, Zhang G and Lim C 2023 Provably-secure quantum randomness expansion with uncharacterised homodyne detection *Nat. Commun.* **14** 316
[17] Colbeck R and Renner R 2012 Free randomness can be amplified *Nat. Phys.* **8** 450
[18] Mironowicz P, Gallego R and Pawłowski M 2015 Robust amplification of Santha-Vazirani sources with three devices *Phys. Rev.* A **91** 032317
[19] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865
[20] Acín A, Massar S and Pironio S 2012 Randomness versus nonlocality and entanglement *Phys. Rev. Lett.* **108** 100402
[21] Clauser J F, Horne M A, Shimony A and Holt R A 1969 Proposed experiment to test local hidden-variable theories *Phys. Rev. Lett.* **23** 880

[22] Shen L et al 2018 Randomness extraction from bell violation with continuous parametric down-conversion Phys. Rev. Lett. 121 150402
[23] Dhara C, Prettico G and Acín A 2013 Maximal quantum randomness in Bell tests Phys. Rev. A 88 052116
[24] Law Y Z, Thinh L P, Bancal J-D and Scarani V 2014 Quantum randomness extraction for various levels of characterization of the devices J. Phys. A: Math. Theor. 47 424028
[25] Bamps C and Pironio S 2015 Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing Phys. Rev. A 91 052111
[26] Acín A, Pironio S, Vértesi T and Wittek P 2016 Optimal randomness certification from one entangled bit Phys. Rev. A 93 040102
[27] Woodhead E, Kaniewski J, Bourdoncle B, Salavrakos A, Bowles J, Acín A and Augusiak R 2020 Maximal randomness from partially entangled states Phys. Rev. Res. 2 042028
[28] Mironowicz P and Pawłowski M 2013 Robustness of quantum-randomness expansion protocols in the presence of noise Phys. Rev. A 88 032319
[29] Wooltorton L, Brown P and Colbeck R 2022 Tight analytic bound on the trade-off between device-independent randomness and nonlocality Phys. Rev. Lett. 129 150403
[30] Skrzypczyk P and Cavalcanti D 2023 Semidefinite Programming in Quantum Information Science (IOP Publishing) pp 2053–563
[31] Mironowicz P 2023 Semi-definite programming and quantum information (arXiv:2306.16560)
[32] Tavakoli A, Pozas-Kerstjens A, Brown P and Araújo M 2023 Semidefinite programming relaxations for quantum correlations (arXiv:2307.02551)
[33] Navascués M, Pironio S and Acín A 2007 Bounding the set of quantum correlations Phys. Rev. Lett. 98 010401
[34] Navascués M, Pironio S and Acín A 2008 A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations New J. Phys. 10 073013
[35] Chor B and Goldreich O 1988 Unbiased bits from sources of weak randomness and probabilistic communication complexity SIAM J. Comput. 17 230
[36] Impagliazzo R, Levin L A and Luby M 1989 Pseudo-random generation from one-way functions Proc. 21st Annual ACM Symp. on Theory of Computing pp 12–24
[37] Konig R, Renner R and Schaffner C 2009 The operational meaning of min-and max-entropy IEEE Trans. Inf. Theory 55 4337
[38] Issa I and Wagner A B 2017 Measuring secrecy by the probability of a successful guess IEEE Trans. Inf. Theory 63 3783
[39] Tomamichel M, Colbeck R and Renner R 2009 A fully quantum asymptotic equipartition property IEEE Trans. Inf. Theory 55 5840
[40] Šupić I and Bowles J 2020 Self-testing of quantum systems: a review Quantum 4 337
[41] Fawzi H, Saunderson J and Parrilo P A 2019 Semidefinite approximations of the matrix logarithm Found. Comput. Math. 19 259
[42] Fawzi H and Fawzi O 2018 Efficient optimization of the quantum relative entropy J. Phys. A: Math. Theor. 51 154003
[43] Brown P, Fawzi H and Fawzi O 2021 Device-independent lower bounds on the conditional von Neumann entropy (arXiv:2106.13692)
[44] Pironio S, Navascués M and Acin A 2010 Convergent relaxations of polynomial optimization problems with noncommuting variables SIAM J. Optim. 20 2157
[45] Wittek P 2015 Algorithm 950: Ncpol2sdpa-sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables ACM Trans. Math. Softw. 41 1
[46] Brown P J 2022 Example scripts for computing rates of device-independent protocols (available at: https://github.com/peterjbrown519/DI-rates)
[47] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 Tight finite-key analysis for quantum cryptography Nat. Commun. 3 634
[48] Tomamichel M 2015 Quantum Information Processing with Finite Resources: Mathematical Foundations vol 5 (Springer)
[49] Dupuis F and Fawzi O 2019 Entropy accumulation with improved second-order term IEEE Trans. Inf. Theory 65 7596
[50] Nieto-Silleras O, Pironio S and Silman J 2014 Using complete measurement statistics for optimal device-independent randomness evaluation New J. Phys. 16 013035
[51] Bancal J-D, Sheridan L and Scarani V 2014 More randomness from the same data New J. Phys. 16 033011
[52] Nieto-Silleras O, Bamps C, Silman J and Pironio S 2018 Device-independent randomness generation from several Bell estimators New J. Phys. 20 023049
[53] Liu Y et al 2018 High-speed device-independent quantum random number generation without a detection loophole Phys. Rev. Lett. 120 010503
[54] García-Patrón R, Fiurášek J, Cerf N J, Wenger J, Tualle-Brouri R and Grangier P 2004 Proposal for a loophole-free Bell test using homodyne detection Phys. Rev. Lett. 93 130409
[55] Hensen B et al 2015 Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres Nature 526 682
[56] Giustina M et al 2015 Significant-loophole-free test of Bell's theorem with entangled photons Phys. Rev. Lett. 115 250401
[57] Shalm L K et al 2015 Strong loophole-free test of local realism Phys. Rev. Lett. 115 250402
[58] Liu Y et al 2018 Device-independent quantum random-number generation Nature 562 548
[59] Shalm L K et al 2021 Device-independent randomness expansion with entangled photons Nat. Phys. 17 452
[60] Fyrillas A et al 2023 Certified randomness in tight space (arXiv:2301.03536)
[61] Hameedi A, Marques B, Mironowicz P, Saha D, Pawłowski M and Bourennane M 2020 Experimental test of nonclassicality with arbitrarily low detection efficiency Phys. Rev. A 102 032621
[62] Mosek ApS 2021 Mosek Modeling Cookbook 3rd edn (Mosek ApS)