IOP Publishing Journal of Physics B: Atomic, Molecular and Optical Physics

J. Phys. B: At. Mol. Opt. Phys. **53** (2020) 045501 (6pp) https://doi.org/10.1088/1361-6455/ab5c33

Enhancing device-independent estimation of quantum randomness from real experimental data

Lu-Yan Wu[1,2,3], **Jian Li**[1,2,3], **Tong-Jun Liu**[1,2], **Chen-Xi Liu**[1,2],
Xiao-Rui Wang[1,2] **and Qin Wang**[1,2]

[1] Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, People's Republic of China
[2] Broadband Wireless Communication and Sensor Network Technology Key Lab of Ministry of Education, NUPT, Nanjing 210003, People's Republic of China

E-mail: qinw@njupt.edu.cn

Received 4 November 2019
Accepted for publication 27 November 2019
Published 24 January 2020

Abstract

In the protocols of device-independent quantum random number generator, it is essential to certify the randomness of the generated numbers. However, statistical fluctuations in measurement data might break the nosignaling conditions, making those data unphysical. In this letter, we proposed to circumvent this problem by using the standard constrained least-squares method. As examples, we apply our present approach on post-processing two different experimental data by utilizing either CHSH correlations or complete measurement statistics, and do comparisons with the original distribution. The post-processing results not only prove the effectiveness of our work to solve the unphysical problem, but also show that randomness certified by processing complete measurement statistics is always larger than through Bell-like inequalities.

Keywords: random numbers, statistical fluctuation, post-processing

(Some figures may appear in colour only in the online journal)

1. Introduction

Random number generators (RNGs) are important devices in the information processing field, ranging from gaming, simulations to cryptography. Traditionally, RNGs which are widely used mainly develop from the deterministic algorithm. These RNGs are also known as pseudo-random number generators [1] because the randomness supported by algorithm is inauthentic, which leads to the system vulnerability. As a counterpart, quantum random number generators (QRNGs) [2–4] provide true random numbers by the guarantee of unpredictability of quantum measurement outcomes. The reasons why QRNGs have not been widely used are listed as follows. On the one hand, the systematic errors caused by various imperfections in the experiment are difficult to estimate [5], which reduces the reliability of the QRNGs. On the other hand, it is a difficult task to mathematically characterize the randomness of the sequence generated by QRNGs under the adversarial attacks. Fortunately, with the in-depth understanding of the relation between the randomness [6] and non-locality of quantum theory, this problem can be circumvented by a device-independent way. In other words, it is possible to certify the randomness of QRNG protocols even with untrusted devices [7]. The device-independent protocols originated from the context of quantum key distribution [8, 9], following the DI-QRNG protocols [10, 11]. Moreover, the experimental realization of the DI-QRNG protocol was already demonstrated [12]. As shown in the subsequent study [13, 14], DI-QRNG protocols can largely reduce the threat of classical adversaries under some reasonable assumptions. Due to its high security against the adversarial attacks, efforts were made on DI-QRNG both theoretically [15, 16] and experimentally [17].

In DI-QRNG protocols, it is essential to certify the randomness of the generated numbers, which is usually quantified

---

[3] Lu-Yan Wu and Jian Li contributed equally to this work.

by guessing probability of the eavesdropper Eve. Taking the unavoidable system error of an experiment into consideration, the key for DI-QRNG protocols is how to bound Eve's guessing probability, which can only be limited by the laws of quantum physics. The answer can be given through the following way. Assuming a simple experimental setup consists of two parties, Alice and Bob. In the beginning, they choose their measurements from a finite set and perform on the systems immediately. After taking a series of measurements, the conditional probabilities derived from the measurement outcomes are used to obtain the violation of a prechosen Bell inequality [18]. Furthermore, Eve's best guessing probability can be computed numerically from the violation [12] as long as the systems satisfy some requirements, i.e. two parties are separated and do not interact with each other. The parameter of inequality can also be replaced with complete measurement statistics [19] to obtain the bound. Moreover, using the complete non-local behavior to characterize the randomness of raw data is equivalent to optimizing overall Bell inequalities which are compatible for experiments [19]. It is worth noting that these bound are achieved under the independent and identically distributed (i.i.d) assumption. Specifically, Alice and Bob should perform the same measurements on their quantum states in every stage of the protocol. There also exist some protocols [20–22] without i.i.d assumption, which we do not discuss more details here. While various protocols based on above methods have been proposed [16, 21, 23], an important issue following is how to realize the protocols experimentally. The underlying statistics distribution of the experiment was replaced by relative frequency, which may yield a unphysical behavior and leave the optimization problem unsolvable.

In this letter, we put forward an approach to solve the problems caused by statistical fluctuations. The core of our approach is in the form of the semidefinite hierarchy [24] to bound the set of quantum correlations. Details on constructing the bound are presented in section 3. We show that the approach is extremely efficient to tackle the problems caused by statistical fluctuations. The remainder of the paper is structured as follows. In section 2, we briefly review the DI-QRNG theoretical model and some notations as well as other preliminary materials about the nonlocal correlations. In section 4, we perform a numerical simulations and apply it on experimental data to show the usefulness of our approach. Finally, section 5 concludes with summary.

2. Preliminaries

In the scenario of standard DI-QRNG protocols, it consists of two separated non-communicating parties, usually called Alice and Bob. There also exist an adversary called Eve, who is committed to improve the guessing probability of random numbers through all feasible methods. The whole quantum system shared by Alice, Bob and Eve is marked as ρ_{ABE}. We label the measurements chose by Alice and Bob with $x \in \{1, \ldots, m_a\}$, $y \in \{1, \ldots, m_b\}$, and the outcomes after measured by corresponding settings with $a \in \{1, \ldots, o_a\}$, $b \in \{1, \ldots, o_b\}$. Hence, $p(ab|xy)$ denotes the joint probability of obtaining the output a, b given the input x, y. We refer to the set $\mathbf{P} = \{p(ab|xy)\}$ of all these probabilities as a behavior [24], which can be considered as a point $\mathbf{P} \in R^{m_a \times m_b \times o_a \times o_b}$ belonging to the probability space $\Omega \subset \mathbb{R}^{m_a \times m_b \times o_a \times o_b}$ [6].

Since DI-QRNG protocols are physically realizable, the behavior $\mathbf{P}$ must satisfy the no-signaling constraints [25]. To be specific, neither Alice nor Bob can transfer their choices of inputs to the other, which is formalized by the conditions:

$$\begin{aligned} \sum_b p(ab|xy) &= \sum_b p(ab|xy'),\ \forall\ a, x, y, y', \\ \sum_a p(ab|xy) &= \sum_a p(ab|x'y),\ \forall\ b, y, x, x'. \end{aligned} \tag{1}$$

We also use the symbol of $\mathcal{NS}$ to denote the set of behaviors satisfying the no-signaling constraints (1).

The behavior $\mathbf{P}$ belongs to the set of quantum behaviors $\mathcal{Q}$ if there exists a state ρ_{ABE} in a composite Hilbert space $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \otimes \mathcal{H}_{\mathcal{E}}$, a set of measurement operators $M_{a|x}$ for Alice, and a set of measurement operators $M_{b|y}$ for Bob. Thus for all a and b [24], we can obtain

$$p(ab|xy) = \langle \Psi_{ABE}| M_{a|x} \otimes M_{b|y} \otimes I_{\mathcal{E}}\ |\Psi_{ABE}\rangle, \tag{2}$$

where $I_{\mathcal{E}}$ is the identity operator for Eve's system. Formally, the set $\mathcal{L}$ of local behaviors is defined by the elements of $\mathbf{P}$ that admit a local model in the form of

$$p(ab|xy) = \int_{\Lambda} \lambda q(\lambda) p(a|x, \lambda) p(b|y, \lambda), \tag{3}$$

where λ is an arbitrary variable in the space Λ. $p(b|x, \lambda)$ denotes the probability of Alice (Bob) getting the outcome a (b) given λ and the choice of measurement x (y). Moreover, we have the strict inclusions $\mathcal{L} \subset \mathcal{Q} \subset \mathcal{NS}$. Alice and Bob' systems are then characterized by the finite set $\mathbf{P}$.

In general, the DI-QRNG protocols eliminate the uncertainty of using untrusted devices in the schemes based on Bell inequality, which can distinguish the quantum system from a classical one. From the point of mathematics, there exists a hyperplane separating all the $\hat{\mathbf{P}} \in \mathcal{L}$ [1] from the point given by the behavior $\mathbf{P} \in \mathcal{Q}$. This hyperplane $\mathbf{H}$ then defines the Bell inequality written as

$$\mathbf{H}^{\mathbf{T}}\mathbf{P} = \sum_{abxy} h_{xy}^{ab} p(ab|xy) \leqslant S_k. \tag{4}$$

None of the knowledge about the internal functioning of the devices is used in this scenario. Hence, we only need the observing behavior which violates a Bell inequality to bound Eve's guessing probability. To guess the outcomes generated by Alice and Bob's measurements, Eve can perform an positive-operator valued measure (POVM) Z_a on his own subsystem to obtain the outcomes corresponding to the values a and b. The guessing probability is thus given by

$$p_{guess}(a|x^*, Z) = \langle \Psi_{ABE}| M_{a|x^*} \otimes I \otimes Z_a |\Psi_{ABE}\rangle. \tag{5}$$

Moreover, Eve can optimize all possible measurements to acquire the maximum guessing probability, which can be

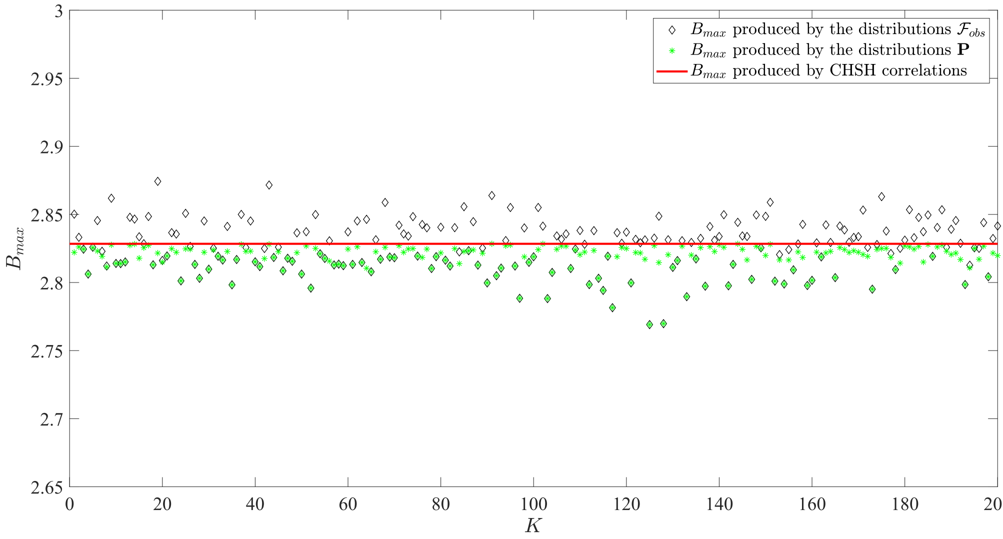

Figure 1. The maximal violation of CHSH inequality (B_{max}) of K trials. B_{max} produced by the behavior $\mathcal{F}_{obs}$ are marked by rhombi. B_{max} produced by the behavior **P** are marked by green-asterisks. The red-line represents the maximal CHSH violation of $2\sqrt{2}$. All the dots are obtained using the second order relaxation of the SDP hierarchy.

formulated as the following optimization problem:

$$\begin{aligned} &G(A|x^*, Z) = \max \ \sum_a p_{guess}(a|x^*, Z), \\ &s.t. \ \ \mathbf{H}^{\mathbf{T}}\mathbf{P} = Q, \\ &\mathbf{P} \in \mathcal{Q}, \end{aligned} \tag{6}$$

where the optimization is carried over all **P** compatible with the Bell violation Q.

Although we can find the optimal solution listed as equation (6), the information obtained in a Bell experiment is much more than the parameter of a prechosen Bell inequality [19]. In other words, more randomness can be obtained from the same observed behavior. The above optimization problem can be transformed to a convex problem:

$$\begin{aligned} &G(A|x^*, Z) = \max_{\{\tilde{\mathbf{p}}^a\}} \sum_a \tilde{p}^a(a|x^*), \\ &s.t. \ \ \sum_a \tilde{\mathbf{p}}^a = \mathbf{P}, \\ &\tilde{\mathbf{p}}^a \in \widetilde{\mathcal{Q}}, \ \ a = 1,\ldots,o_a, \end{aligned} \tag{7}$$

where $\tilde{\mathbf{p}}^a$ are unnormalized behavior and $\widetilde{\mathcal{Q}}$ denotes the convex set of the unnormalized quantum behaviors. Equations (6) and (7) hence provide a sophisticated formulas for calculating $G(A|x^*, Z)$. Smaller guessing probability of Eve certifies more randomness of the generated random numbers transformed between Alice and Bob.

3. A general procedure for DI-protocols robust against statistical fluctuations

Although we have equations (6) and (7) to estimate the randomness theoretically, it is widely ignored that the observed behavior $\mathcal{F}_{obs}$ may not belonging to $\mathcal{Q}$ even $\mathcal{NS}$ experimentally. With sufficient trials, the observed behavior satisfies $\mathcal{F}_{obs} \approx N_{abxy}/N$, where N is the total number of coincidence counting and N_{abxy} is the count of obtaining the outcome a and b while measuring along x and y respectively. However, since one can only perform a finite number of experimental trials, the correlations described by measured data contains statistical fluctuations which can not be neglected.

Our task is to remove the influence of statistical fluctuations acting on the observed behavior $\mathcal{F}_{obs}$. In other words, we need to find a set of quantum correlations in $\mathcal{Q}$ to formulate $\mathcal{F}_{obs}$. To solve this problem, we use the least-squares approximation $D(\mathbf{P}, \mathcal{F}_{obs}) = \|\mathbf{P} - \mathcal{F}_{obs}\|_2^2$ with $\|u\|_2 = (u^\top u)^{1/2}$ as the degree of difference between two behaviors.

Since the set of quantum correlations can not be described by a finite number of extreme points, optimization over the full set of quantum correlations is infeasible. To solve this problem, we can resort to the NPA hierarchy [24], which yields a nested set of semidefinite criteria for a given probability to have a quantum model. According to the convex optimization [26], the above problem is easily cast and solved as standard constrained least-squares:

$$\begin{aligned} &minimize \ \ \|\mathbf{P} - \mathcal{F}_{obs}\|_2^2 \\ &s.t. \qquad \mathbf{P} \in \mathcal{Q}_k, \ \ k = 1, 2, 3\ldots, \end{aligned} \tag{8}$$

where k is the level of NPA hierarchy. By minimizing $D(\mathbf{P}, \mathcal{F}_{obs})$, the above problems can be solved. In addition, handling the unphysical behavior with the least-squares approximation is originated from [27]. In order to demonstrate the effect of the least-squares approximation, a numerical simulation with $K = 200$ instances is performed. Meanwhile supposing the violation of K trials are subject to poisson distribution with mean value of $2\sqrt{2}$, which is the maximal quantum limit of CHSH inequality. In this case, it yields then our observed behavior $\mathcal{F}_{obs}$. The numerical result is shown in figure 1. It is clear that each observed behavior

Table 1. The behavior $\mathcal{F}_{obs}$ of the experiment in [12]. The inequality is violate with $Q \approx 2.414\,525\,317\,94$. Suffering from the statistical fluctuations, $\mathcal{F}_{obs}$ does not satisfy the no-signaling constraints. The values are conditional probabilities of obtaining ab while given xy for Alice and Bob.

xy ab	00	01	10	11	$\sum_b p(a=0, b\|xy)$	$\sum_b p(a=1, b\|xy)$
00	0.3896	0.150	0.0931	0.3923	0.5396	0.4854
01	0.3968	0.0932	0.0985	0.4115	0.4900	0.5100
10	0.4003	0.0976	0.0905	0.4116	0.4979	0.5021
11	0.0844	0.4218	0.3834	0.1104	0.5062	0.4938

Table 2. The behavior **P** calculating from equation (8) is the least-squares approximate of $\mathcal{F}_{obs}$. The inequality is violated with $Q \approx 2.414\,525\,318\,28$. **P** satisfies the no-signaling constraints within the desired tolerance. The values are conditional probabilities of obtaining ab while given xy for Alice and Bob.

xy ab	00	01	10	11	$\sum_b p(a=0, b\|xy)$	$\sum_b p(a=1, b\|xy)$
00	0.3855	0.1168	0.1013	0.3964	0.5023	0.4977
01	0.3961	0.1063	0.0855	0.4122	0.5024	0.4977
10	0.4003	0.1017	0.0864	0.4115	0.5020	0.4979
11	0.0892	0.4129	0.3924	0.1056	0.5021	0.4980

$\mathcal{F}_{obs}$ is converted into the behavior **P** belonging to a quantum behavior by our method. The simulation runs with MATLAB toolbox QETLAB [28] and CVX [29].

4. Applications

In this section, we present two examples using different inequalities to verify the method mentioned above.

CHSH correlations from the ion experiment.—We reanalyze the data from the ion experiment [12]. Tables 1 and 2 show the distribution $\mathcal{F}_{obs}$ of the raw data [12] and the distribution **P** of the processed data. Through the process of equation (8), the marginal distribution in table 2 always satisfies the non-signaling condition, i.e. $\sum_b p(a=0, b|00) \approx \sum_b p(a=0, b|01)$. However, compared with the CHSH violation achieved by the raw data, the processed data reached an approximate value at 2.4145. In other words, it certifies that the standard constrained least-squares method does no harm to the Bell test and removes the statistical fluctuations in experiments. We regard the method efficient when the no-signaling constraints are taking into consideration for experiments.

The advantage of getting the data processed is more eminent in the field of randomness certification. Table 3 presents bounds on the guessing probability $G(A|x^*, Z)$. When we certify the randomness by the full non-local behavior way, no solution of equation (7) is found for the raw distribution $\mathcal{F}_{obs}$. It is because that the raw distribution $\mathcal{F}_{obs}$ does not satisfy the no-signaling constraints due to the statistical fluctuations, which is also proved in table 1. After processed by least-squares approximation of equation (8), the behavior **P** in table 2 satisfies the no-signaling constraints within the desired tolerance. In table 3, Eve achieves nearly the same guessing probability before and after process by CHSH inequality, which means our method do no harm to the Bell test. Less guessing probability is achieved only after process, which certifies more randomness of the generated random numbers transformed between Alice and Bob.

Table 3. The first and the second rows in the table correspond to the value in either the original distribution or after post-processing through our present approach individually. The first and the second columns represent the results using either CHSH inequality or complete measurement statistics, respectively. Here in our approach, we use the NPA hierarchy up to the second level.

	CHSH fixed	Full non-local behavior
Before	0.842 491 748 979 439	Infeasible
After	0.842 491 748 979 064	0.821 296 659 433 661

Gisin's elegant Bell inequality (EBI) in optical experiments [30]—Moreover, we consider the following set of correlations of Gisin's EBI obtained from [31] and combine equations (6), (7) with our method to calculate the $G(A|x^*, Z)$.

The EBI can be written as follows

$$S \equiv E_{1,1} + E_{1,2} - E_{1,3} - E_{1,4} + E_{2,1} - E_{2,2} + E_{2,3} - E_{2,4} + E_{3,1} - E_{3,2} - E_{3,3} + E_{3,4} \leqslant 6. \quad (9)$$

Then Alice should perform three projective measurements $A_1 = \sigma_z$, $A_2 = \sigma_x$, $A_3 = \sigma_y$, while Bob should perform the following four projective measurements

$$B_1 = \frac{1}{\sqrt{3}}(\sigma_z + \sigma_x - \sigma_y), \quad (10a)$$

$$B_2 = \frac{1}{\sqrt{3}}(\sigma_z - \sigma_x + \sigma_y), \quad (10b)$$

$$B_3 = \frac{1}{\sqrt{3}}(-\sigma_z + \sigma_x + \sigma_y), \quad (10c)$$

Table 4. The behavior $\mathcal{F}_{obs}$ inferred for the experiment reported in [31].The inequality is violate with $Q \approx 6.813\,799\,426\,31$. The values are conditional probabilities of obtaining *ab* while given *xy* for Alice and Bob.

xy ab	00	01	10	11	$\sum_b p(a=0, b\vert xy)$	$\sum_b p(a=1, b\vert xy)$
00	0.3935	0.0992	0.1189	0.3883	0.4927	0.5072
01	0.4018	0.1076	0.0900	0.4115	0.5094	0.5015
02	0.1110	0.3720	0.4001	0.1169	0.4830	0.5170
03	0.1085	0.3805	0.4033	0.1078	0.4885	0.5111
10	0.3809	0.1212	0.1307	0.3673	0.5021	0.4980
11	0.1212	0.3876	0.3670	0.1242	0.5088	0.4912
12	0.4075	0.0918	0.0925	0.4082	0.4993	0.5007
13	0.1014	0.4125	0.3985	0.0876	0.5139	0.4861
20	0.4188	0.0904	0.0841	0.4067	0.5092	0.4908
21	0.1037	0.4018	0.3961	0.0983	0.5055	0.4944
22	0.1303	0.3740	0.3822	0.1134	0.5043	0.4956
23	0.3794	0.1190	0.1232	0.3784	0.4984	0.5016

Table 5. The behavior **P** calculating from equation (8) is the least-squares approximate of $\mathcal{F}_{obs}$. The inequality is violate with $Q \approx 6.813\,799\,425\,74$.The values are conditional probabilities of obtaining *ab* while given *xy* for Alice and Bob.

xy ab	00	01	10	11	$\sum_b p(a=0, b\vert xy)$	$\sum_b p(a=1, b\vert xy)$
00	0.3922	0.1013	0.1168	0.3897	0.4935	0.5065
01	0.3946	0.0989	0.0987	0.4078	0.4935	0.5065
02	0.1146	0.3789	0.3933	0.1132	0.4935	0.5065
03	0.1073	0.3862	0.3975	0.1090	0.4935	0.5065
10	0.3815	0.1244	0.1275	0.3666	0.5059	0.4941
11	0.1224	0.3836	0.3709	0.1231	0.5060	0.4940
12	0.4148	0.0912	0.0931	0.4009	0.5060	0.4940
13	0.0999	0.4061	0.4049	0.0892	0.5060	0.4941
20	0.4194	0.0849	0.0896	0.4061	0.5043	0.4957
21	0.0998	0.4045	0.3935	0.1022	0.5043	0.4957
22	0.1280	0.3764	0.3799	0.1157	0.5044	0.4956
23	0.3834	0.1209	0.1213	0.3743	0.5043	0.4956

Table 6. The first and the second rows in the table correspond to the value either calculating using the original distribution or after post-processing through our present approach individually. The first and the second columns represent the results using either EBI inequality or complete measurement statistics, respectively. Here in our approach, we use the NPA hierarchy up to the second level.

	EBI fixed	Full non-local behavior
Before	0.537 747 004 477 726	Infeasible
After	0.537 747 004 851 328	0.489 875 193 431 422

$$B_4 = \frac{1}{\sqrt{3}}(-\sigma_z - \sigma_x - \sigma_y), \qquad (10d)$$

where σ_z, σ_x, σ_y are pauli operations.

The raw and processed distribution of $\mathcal{F}_{obs}$ and **P** is listed in tables 4 and 5 respectively. Through least-square approximation, distribution satisfy the no-signaling condition. Table 6 presents the bounds of Eve's guessing probability $G(A|x^*, Z)$. Unsuprisingly, the raw distribution $\mathcal{F}_{obs}$ can not find a solution following equation (7). However, after post-processing, an optimal solution of $G(A|\ x^*, Z) \approx 0.489\,875$ is found. It also shows that our method can be applied to various correlations.

5. Conclusion

In conclusion, we have proposed an approach on the basis of least-squares approximation and NPA, to handle the no solution problem in dealing with randomness certification of DI-QRNG protocols. The unphysical behavior caused by experimental statistical fluctuations can be solved by carrying out post-processing, i.e. to replace the unphysical $\mathcal{F}_{obs}$ with a similar quantum behavior **P**, and weigh the similarity between $\mathcal{F}_{obs}$ and **P** through the least-squares approximations. Then we implement the above approach onto analyzing two experimental data through either Bell-like inequalities or complete measurement statistics. We find that, after post-processing, the guessing probability remains unchanged through arbitrary Bell-like inequalities, while more randomness can be verified by utilizing complete measurement statistics. Therefore, our work can provide valuable post-processing methods for analyzing DI-QRNG experimental data, and pave its way towards practical implementations in the near future.

Acknowledgments

We gratefully acknowledge the financial supports from the National Key R&D Program of China (Grant Nos. 2018YFA0306400, 2017YFA0304100), the National Natural Science Foundation of China (Grants Nos. 61475197, 11774180, 61590932), and the Postgraduate Research and Practice Innovation Program of Jiangsu Province (KYCX18-0913).

ORCID iDs

Qin Wang https://orcid.org/0000-0002-6314-4250

References

[1] Herrero-Collantes M and Garcia-Escartin J C 2017 *Rev. Mod. Phys.* **89** 015004
[2] Jennewein T, Achleitner U, Weihs G, Weinfurter H and Zeilinger A 2000 *Rev. Sci. Instrum.* **71** 1675–C1680
[3] Wei W and Guo H 2009 *Opt. Lett.* **34** 1876–8
[4] Ren M, Wu E, Liang Y, Wu G A and Zeng H P 2011 *Phys. Rev.* A **83** 023820
[5] Moroder T, Kleinmann M, Schindler P, Monz T, Ghne O and Blatt R 2010 *Phys. Rev. Lett.* **110** 180401
[6] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 *Rev. Mod. Phys.* **86** 419
[7] Pironio S, Scarani V and Vidick T 2016 *New J. Phys.* **18** 100202
[8] Mayers D and Yao A 1998 *Proc. 39th Annual Symp. on Foundations of Computer Science* pp 503–C509
[9] Barrett J, Hardy L and Kent A 2005 *Phys. Rev. Lett.* **95** 010503
[10] Colbeck R 2006 (arXiv:0911.3814)
[11] Colbeck R and Kent A 2011 *J. Phys. A: Math. Theor.* **44** 095305
[12] Pironio S *et al* 2010 *Nature* **464** 1021
[13] Pironio S and Massar S 2013 *Phys. Rev.* A **87** 012336
[14] Fehr S, Gelles R and Schaffner C 2013 *Phys. Rev.* A **87** 012335
[15] Nieto-Silleras O, Bamps C, Silman J and Pironio S 2018 *New J. Phys.* **20** 023049
[16] Brown P J, Ragy S and Colbeck R 2018 (arXiv:1810.13346)
[17] Liu Y *et al* 2018 *Phys. Rev. Lett.* **120** 010503
[18] Bell J S 1964 *Phys. Phys. Fiz.* **1** 195–200
[19] Nieto-Silleras O, Pironio S and Silman J 2014 *New J. Phys.* **16** 013035
[20] Arnon-Friedman R, Renner R and Vidick T 2019 *Siam J. Comput.* **48** 181–225
[21] Assad S M, Thearle O and Lam P K 2016 *Phys. Rev.* A **94** 012304
[22] Knill E, Zhang Y B and Bierhorst P 2017 (arXiv:1709.06159)
[23] Acín A, Pironio S, Vértesi T and Wittek P 2016 *Phys. Rev.* A **93** 040102
[24] Navascués M, Pironio S and Acín A 2008 *New J. Phys.* **10** 073013
[25] Barrett J, Linden N, Massar S, Pironio S, Popescu S and Roberts D 2005 *Phys. Rev.* A **71** 022101
[26] Boyd S and Vandenberghe L 2004 *Convex Optimization* (Cambridge: Cambridge University Press)
[27] Lin P S, Rosset S, Zhang Y B, Bancal J D and Liang Y C 2018 *Phys. Rev.* A **97** 032309
[28] Johnston N 2016 QETLAB: A MATLAB Toolbox for Quantum Entanglement, Version 0.9 (https://doi.org/10.5281/zenodo.44637)
[29] Grant M and Boyd S 2014 CVX: Matlab Software for Disciplined Convex Programming, Version 2.1
[30] Bancal J D, Sheridan L and Scarani V 2014 *New J. Phys.* **16** 033011
[31] Chen-Xi Liu *et al* 2019 *J. Phys. B: At. Mol. Opt. Phys.* **52** 145501