Semi-device-independent random-number expansion without entanglement

Hong-Wei Li,[1,2] Zhen-Qiang Yin,[1,*] Yu-Chun Wu,[1] Xu-Bo Zou,[1] Shuang Wang,[1] Wei Chen,[1]
Guang-Can Guo,[1] and Zheng-Fu Han[1,*]
[1]*Key Laboratory of Quantum Information,University of Science and Technology of China, Hefei 230026, China*
[2]*Zhengzhou Information Science and Technology Institute, Zhengzhou 450004, China*
(Received 14 July 2011; published 14 September 2011)

By testing the classical correlation violation between two systems, true random numbers can be generated and certified without applying classical statistical method. In this work, we propose a true random-number expansion protocol without entanglement, where the randomness can be guaranteed only by the two-dimensional quantum witness violation. Furthermore, we only assume that the dimensionality of the system used in the protocol has a tight bound, and the whole protocol can be regarded as a semi-device-independent black-box scenario. Compared with the device-independent random-number expansion protocol based on entanglement, our protocol is much easier to implement and test.

DOI: 10.1103/PhysRevA.84.034301 PACS number(s): 03.67.Ac, 05.40.−a

I. INTRODUCTION

True random numbers have significant applications in numerical simulation, lottery games, biological systems, and cryptography [1]. More particularly, security of the quantum key distribution (QKD) protocol [2] is based on the random selection of the state preparation and measurement. If the state preparation and measurement are pecisely known by the eavesdropper, she can apply the man-in-the-middle attack [3] to get all of the secret information without being discovered. True random numbers should be unpredictable for the third party, so most true random-number-generation protocols are based on unpredictable physical processes [4–11]. Unfortunately, the true random numbers generated by these protocols can only be characterized with the classical statistical method, such as the Statistical Test Suite from NIST [12,13]. Inspired by the device-independent quantum information processing based on nonlocal correlations of entanglement particles [14–16], Colbeck *et al.* [17,18] have proposed the true random-number-generation protocol based on the Greenberger-Horne-Zeilinger (GHZ) test and Pironio *et al.* [19,20] have proposed the true random-number-generation protocol certified by the Bell inequality violation. They have also given a proof-of-concept experimental demonstration of their protocol by approximately a one meter distance. The true random-number-generation protocol based on entanglement requires no assumption about the internal working of the device in both states of measurement, thus the true random number cannot be generated with only the classical method, and the randomness of their experimental result can only be certified by the Bell-inequality violation. Since the protocol requires the preestablished true random number to select the measurement bases, it can also be called a device-independent random-number expansion protocol, correspondingly. In comparison with the random-number-generation protocol certified by the classical statistical method, the device-independent random-number expansion protocol offers a new method to unequivocally quantify the observed random numbers.

Both of the device-independent random-number expansion protocols strongly suggest that only entanglement-based protocols are suitable for establishing the quantified true random numbers [17–20]. However, the entanglement-based protocol has much more complicated experimental setups compared with the one-way system, where the first black box prepares an arbitrary quantum state and sends it to the other black box to perform an arbitrary measurement. Furthermore, most commerical true random-number-generation systems are based on one-way protocols. Inspired by the method of device-independent test of the classical and quantum dimensions given by Gallego *et al.* [21], Pawlowski *et al.* [22] have proposed a semi-device-independent one-way QKD protocol with four input states and two measurement bases, security of which was based on the two-dimensional quantum witness and the quantum random access code. Here, we propose the one-way semi-device-independent random-number expansion protocol without entanglement, the randomness of which can be quantified with two-dimensional quantum witness violation, and the experimental demonstration can be established by combining the commerical QKD setup with different modulation protocols, the randomness of which can be proved in the following section by applying the numerical calculation method. Similar to Colbeck and Pironio's models, our protocol requires no assumption about the internal working of the state preparation and measurement device, except that the two-dimensional quantum system and collective attacks are bounded. However, we need the quantum state to be prepared and measured in the same safe area; the quantum state and classical information should not be divulged to the eavesdropper in the unsafe area.

II. MODEL DESCRIPTION

We first illustrate the semi-device-independent random-number expansion protocol, where only two black boxes in the same safe area should be considered. The two black boxes can be used for illustrating the state preparation and measurement, respectively. A detailed scenario is depicted precisely in Fig. 1.

In the semi-device-independent random-number expansion protocol, we randomly select four classical input bits $a \in \{00,01,10,11\}$ in the first black box. When pressing the button

[*] Authors to whom correspondence should be addressed: yinzheqi@ustc.edu.cn; zfhan@ustc.edu.cn

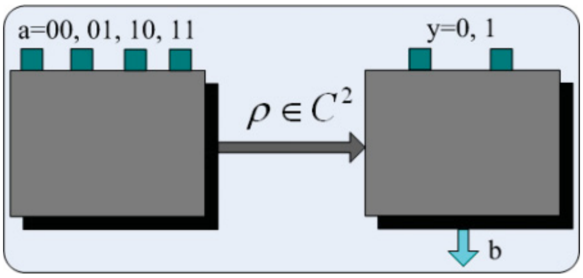

FIG. 1. (Color online) Semi-device-independent random-number expansion protocol. The protocol requires the state preparation black box and the state measurement black box, respectively. Both of the black boxes are in the same safe area.

a, the first black box will emit the classical or quantum state ρ_a, then the prepared state ρ_a will be sent to the second black box, correspondingly. When pressing the button $y = \{0,1\}$, the second black box will emit the measurement outcome $b = \{0,1\}$. Similar to the previous analysis based on quantum dimension witness violation, we suppose that only a two-dimensional system will be considered in this protocol, thus $\rho_a \in C^2$.

Formally, we can estimate the probability distribution by repeating this procedure many times, which can be illustrated precisely as the following equation:

$$P(b|ay) = \mathrm{tr}\big(\rho_a M_y^b\big), \tag{1}$$

where M_y^b is the measurement operator acting on two-dimensional Hilbert space with input parameter y and output parameter b by considering the prepared state ρ_a. In this protocol, the true random number can be produced by only considering the date table $P(b|ay)$. More precisely, we do not require any assumption on how the probability was obtained with two black boxes, except that the state preparation and measurement can be guaranteed with two-dimensional quantum witness.

We will use the following expectation value to illustrate the probability distribution for the convenient analysis in the following section:

$$E_{ay} = P(b = 0|ay), \tag{2}$$

where $P(b = 0|ay) + P(b = 1|ay) = 1$; the set of probability distributions E_{ay} can be used for illustrating the quantum dimension witness. From the theoretical aspect, two types of two-dimensional quantum witness inequalities have been proposed, respectively [21,22]. We will apply the following tight two-dimensional classical witness in our randomness analysis

$$\begin{aligned} T \equiv\ & E_{000} + E_{001} + E_{010} - E_{011} \\ & - E_{100} + E_{101} - E_{110} - E_{111} \leqslant 2, \end{aligned} \tag{3}$$

where we only consider the four state preparation and two measurement bases case in this inequation. The other similar expression with the three state preparation and two measurement bases case has also been given in Ref. [21], but we can simply verify that the two-dimensional quantum witness in this case cannot be used for generating true random numbers.

More precisely, the tight two-dimensional quantum witness can be given as the following inequation (more detailed information about this inequation can also be found in Ref. [22]):

$$\begin{aligned} T \equiv\ & E_{000} + E_{001} + E_{010} - E_{011} \\ & - E_{100} + E_{101} - E_{110} - E_{111} \leqslant 2.828. \end{aligned} \tag{4}$$

The maximal value of the two-dimensional quantum witness can be calculated numerically. More interestingly, it can also be analyzed by applying the 2-to-1 quantum random access code protocol [22,25], where Alice receives two uniformly distributed bits a and sends the encoded physical system ρ_a to Bob, and Bob is asked to guess one of Alice's bits randomly. This two-dimensional quantum witness is the main tool to analyze the proposed random-number expansion protocol, and our main result is to establish the relationship between the randomness of the measurement outcome and its expected two-dimensional quantum witness violation.

We quantify the randomness of the measurement outcome b conditioned on the input values a and y by the following min-entropy function [26]:

$$H_\infty(B|A,Y) \equiv -\log_2[\max_{b,a,y} P(b|a,y)]. \tag{5}$$

From this equation, we can see that the purpose of this paper is to obtain the upper bound of the conditional probability distribution $P(b|a,y)$ for a given two-dimensional quantum witness T. More precisely, the maximal probability distribution $\max_{b,a,y} P(b|a,y)$ denotes the solution to the following optimization problem:

$$\begin{aligned} & \max_{b,a,y} P(b|a,y) \\ & \text{subject to}: \\ E_{ay} &= \mathrm{tr}\big(\rho_a M_y^0\big), \\ & E_{000} + E_{001} + E_{010} - E_{011} \\ & \quad - E_{100} + E_{101} - E_{110} - E_{111} = T, \end{aligned} \tag{6}$$

where the optimization is carried out by arbitrary quantum states $\{\rho_{00},\rho_{01},\rho_{10},\rho_{11}\}$ and measurement operators $\{M_0^0, M_1^0\}$ defined over two-dimensional Hilbert space. In the most general case, we should consider the positive-operator-valued measure (POVM) $\{M_0^0, M_0^1\}$ and $\{M_1^0, M_1^1\}$, where $M_0^0 + M_0^1 = M_1^0 + M_1^1 = I$. Fortunately, Masanes [27] has proved that only the projective measurement should be considered in the case of two-observable and two-measurement outcomes. Since T is the linear expression of the probabilities, we can only consider pure states [21] preparation in our numerical calculation. Without loss of generality, the state preparation and measurement in our numerical calculation can be illustrated precisely with the following equations, respectively:

$$\rho_a = |\varphi(a)\rangle\langle\varphi(a)|, \tag{7}$$

$$|\varphi(a)\rangle = \begin{pmatrix} \cos(\frac{\theta_a}{2}) \\ e^{i\eta_a}\sin(\frac{\theta_a}{2}) \end{pmatrix}, \tag{8}$$

$$M_0^0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{9}$$

$$M_1^0 = \begin{pmatrix} \cos^2(\frac{\theta}{2}) & \frac{1}{2}e^{-i\eta}\sin(\theta) \\ \frac{1}{2}e^{i\eta}\sin(\theta) & \sin^2(\frac{\theta}{2}) \end{pmatrix}, \tag{10}$$

where $a \in \{00,01,10,11\}$, $0 \leqslant \theta_a, \theta \leqslant \pi$, $0 \leqslant \eta_a, \eta \leqslant 2\pi$. By solving the maximization problem, we get the min-entropy bound of the measurement outcome for given two-dimensional quantum witness T. A detailed expression of the relationship between the two-dimensional quantum witness violation and the min-entropy boundis depicted precisely in Fig. 2.

The calculation result show that if the the violation of the two-dimensional quantum witness is larger than 2.64, the semi-device-independent true random number can be expanded correspondingly. The maximal value of the min-entropy bound in our numerical calculation is 0.206, which can be satisfied in cases where the two-dimensional quantum witness violation is 2.828.

III. EXAMPLE DESCRIPTION

In this section, we give a practical protocol to illustrate the semi-device-independent random-number expansion protocol. This protocol is equal to the (2,1,0.85) quantum random access code protocol [22–25]. In this particular protocol, the state preparation in the first black box can be illustrated precisely as the following equations:

$$\begin{aligned}|\varphi(00)\rangle &= \cos\left(\frac{\pi}{8}\right)|0\rangle + \sin\left(\frac{\pi}{8}\right)|1\rangle,\\ |\varphi(01)\rangle &= \cos\left(\frac{7\pi}{8}\right)|0\rangle + \sin\left(\frac{7\pi}{8}\right)|1\rangle,\\ |\varphi(10)\rangle &= \cos\left(\frac{3\pi}{8}\right)|0\rangle + \sin\left(\frac{3\pi}{8}\right)|1\rangle,\\ |\varphi(11)\rangle &= \cos\left(\frac{5\pi}{8}\right)|0\rangle + \sin\left(\frac{5\pi}{8}\right)|1\rangle.\end{aligned} \tag{11}$$

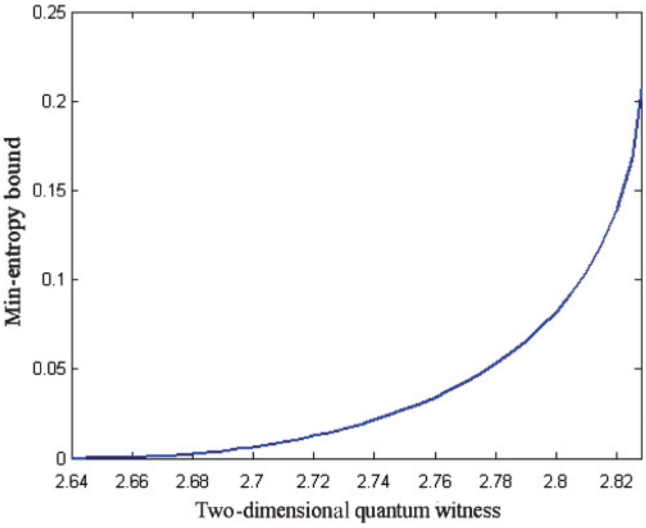

FIG. 2. (Color online) The relationship between the two-dimensional quantum witness and the the min-entropy bound. The min-entropy starts at zero in the two-dimensional classical witness case; systems that violate the two-dimensional quantum witness 2.64 have a positive min-entropy.

For the state measurement in the second black box, we will apply the two projective measurements with the following bases:

$$\begin{aligned}&\{M_0^0 = |0\rangle\langle 0|, \quad M_0^1 = |1\rangle\langle 1|\},\\ &\{M_1^0 = |+\rangle\langle +|, \quad M_1^1 = |-\rangle\langle -|\},\end{aligned} \tag{12}$$

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The two-dimensional quantum witness in this protocol is 2.828, which is the maximal two-dimensional quantum witness violation. Combining this state preparation and measurement protocol with the true random-number extraction analysis result, we can numerically calculate that min-entropy bound of the expanded random bit is 0.206. Note that we only need true random numbers a and y to estimate dimension witness value. No more random numbers should be preestablished by two black boxes, thus our random-number expansion protocol only needs few true random number seeds.

Since the BB84 protocol is also based on the four input states and two measurement bases case, one natural question is to consider whether the BB84 protocol can be used for generating true random numbers, applying our randomness analysis method. Unfortunately, the quantum dimension witness value in this case does not violate 2.64. More precisely, the state preparation in the BB84 protocol can be illustrated as

$$\begin{aligned}&\widetilde{\varphi}(00)\rangle = |0\rangle, \qquad |\widetilde{\varphi}(01)\rangle = |-\rangle,\\ &|\widetilde{\varphi}(10)\rangle = |+\rangle, \qquad |\widetilde{\varphi}(11)\rangle = |1\rangle.\end{aligned} \tag{13}$$

The measurement bases are equal to the (2,1,0.85) quantum random access code case $\{M_0^0 = |0\rangle\langle 0|,\ M_0^1 = |1\rangle\langle 1|\}$ and $\{M_1^0 = |+\rangle\langle +|,\ M_1^1 = |-\rangle\langle -|\}$. Then the dimension witness achieves $T = 2$, which indicates that no true random numbers can be generated and certified by considering the semi-device-independent random -number expansion protocol.

IV. DISCUSSION

We have proposed a true random-number expansion protocol in this paper. The generated random numbers can be quantified with two-dimensional quantum witness violation, not based on the classical statistical method. Compared with the quantified random-number expansion protocol based on entanglement, we provide a much simpler method. Our protocol does not need any entanglement, which is a complicated to produce and high-cost resource. Unfortunately, since the maximal ratio of the expanded random number is 0.206, our protocol has a much lower random-number expansion efficiency. However, since our semi-device-independent random-number expansion protocol is much easier to implement than the full-device-independent protocol based on entanglement, thus the semi-device-independent protocol will generate much more random numbers than the full-device-independent protocols in the same period of time.

The question remains on whether a much higher efficiency random-number expansion protocol can be found in future research based on quantum dimension witness violation. We suppose that the n-to-m ($n > 2$) quantum random access code protocol may be used for generating much more true random numbers. Similar to the security analysis given by Pironio *et al.* [20], it also will be very interesting to analytically prove the min-entropy bound $H(B|A,Y)$ by considering the quantum dimension witness violation T.

Device-independent quantum information processing has attracted much attention for its higher-level security in comparison with the protocol based on trusted devices. Combining the semi-device-independent random-number expansion protocol with the device-independent QKD protocol, we hope to get a much higher-level security than the QKD protocol based solely on some mathematical methods certified random numbers. More interestingly, we can also apply this min-entropy bound to estimate the upper bound of the eavesdropper's information in the security proof of semi-device-indepdnent one-way QKD protocol [22].

ACKNOWLEDGMENTS

Hong-Wei Li would like to thank Dr. Marcin Pawlowski from University of Bristol for his helpful discussion and comments. This work was supported by the National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200), National Natural Science Foundation of China (Grants No. 60921091, and No. 10974193), and China Postdoctoral Science Foundation (Grant No. 20100480695).

[1] D. Knuth., *The Art of Computer Programming Vol. 2, Seminumerical Algorithms* (Addison-Wesley, Reading, MA, 1981).

[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[3] M. Peev, M. Nolle, O. Maurhardt, T. Lornser, M. Suda, A. Poppe, R. Ursin, A. Fedrizzi, and A. Zeilinger, e-print arXiv:quant-ph/0407131.

[4] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).

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

[6] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109 (2008).

[7] U. Atsushi *et al.*, Nat. Photonics **2**, 728 (2008).

[8] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, Phys. Rev. A **75**, 032334 (2007).

[9] Y. Shen, L. Tian, and H. Zou, Phys. Rev. A **81**, 063814 (2010).

[10] W. Wei and H. Guo, Opt. Lett. **34**, 1876 (2009).

[11] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, Phys. Rev. A **83**, 023820 (2011).

[12] NIST Statistical Tests Suite [http://csrc.nist.gov].

[13] D. Branning and M. Bermudez, J. Opt. Soc. Am. B **27**, 1594 (2010).

[14] D. Mayers and A. Yao, FOCS' 98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science, (1998), pp. 503–509.

[15] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[16] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[17] R. Colbeck and A. Kent, J. Phys. A: Math. Theor. **44**, 095305 (2011).

[18] R. Colbeck, Ph.D. thesis, University of Cambridge, 2009.

[19] S. Pironio *et al.*, Nature (London) **464**, 1021 (2010).

[20] S. Pironio and A. Acin, Nat. Commun. **2**, 238 (2011).

[21] R. Gallego, N. Brunner, C. Hadley, and A. Acin, Phys. Rev. Lett. **105**, 230501 (2010).

[22] M. Pawlowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011).

[23] S. Wiesner, SIGACT News **15**, 78 (1983).

[24] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. ACM **49**, 496 (2002).

[25] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, New J. Phys. **8**, 129 (2006).

[26] R. Koenig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[27] L. Masanes, e-print arXiv:0512100.