Certified randomness from a remote-state-preparation dimension witness

Xing Chen,[1] Kai Redeker,[2] Robert Garthoff,[2] Wenjamin Rosenfeld,[2] Jörg Wrachtrup,[1,3] and Ilja Gerhardt[1,*]

[1] *3rd Institute of Physics and Center for Integrated Quantum Science and Technology (IQST), University of Stuttgart, Pfaffenwaldring 57, D-70569 Stuttgart, Germany*

[2] *Fakultät für Physik, Ludwig-Maximilians-Universität München, D-80799 München, Germany*

[3] *Max Planck Institute for Solid State Research, Heisenbergstraße 1, D-70569 Stuttgart, Germany*

(Received 17 June 2020; accepted 9 March 2021; published 14 April 2021)

Randomness in Bell test data can be device-independently certified by Bell's theorem without placing assumptions about the experimental devices. The device-independent randomness has very demanding requirements about the experimental devices and relatively lower output randomness. With the same Bell test data we can extract substantially more randomness without using Bell's theorem. To achieve this goal, we introduce a remote-state-preparation dimension witness and a semi-device-independent randomness certification model which is based on it. This is one important step towards practical use of the Bell test in randomness generation.

DOI: 10.1103/PhysRevA.103.042211

I. INTRODUCTION

Random numbers have a wide variety of applications in daily life [1]. Their use covers gambling, scientific research [2], and, most importantly, cryptography [3]. Naturally, a given bit string cannot be proven to be random [1], and the *generation process* of a random number is the relevant measure. Quantum-mechanical processes are believed to be the only known source of randomness in nature, thus the generation of a random bit by a quantum mechanical superposition is desirable [4]. Many quantum mechanical measurements show a probabilistic outcome [5]; however, this can have technical causes [6,7] other than quantum mechanics.

For a reliable quantum random number, i.e., one which directly stems from a quantum process and is free from other noise sources or manipulation, we need to utilize a process which proves its "quantum nature" in a measurement. The use of fundamental physics inequalities can realize this goal. From Bell inequalities [8], for example, the Clauser-Horne-Shimony-Holt (CHSH) inequality [9], random numbers can be *certified* in a device-independent (DI) way [6,10–15].

Although Bell's theorem seems to be the ideal way to certify quantum randomness, this method remains experimentally challenging [16–19] and has a low randomness output rate [10,12]. Therefore, other *semi-device-independent* randomness certification methods have been developed. *Semi-device-independent* (SDI) means that the raw measurement outcomes reveal their quantumness, if a certain number of assumptions of the experimental setup can be guaranteed [20]. Among these we find the Kochen-Specker inequality [21,22] and the dimension witness [23–25].

Here, we certify and extract the randomness generated in a loophole-free Bell test [19], in a DI and a SDI manner (Fig. 1). The randomness is bounded by min-entropy [26]. For the DI approach we use the prior analysis from Ref. [10] to quantify the entropy in the data. For the SDI approach, we introduce a remote-state-preparation dimension witness. This allows for a significantly higher output rate of random bits.

CHSH scenario. For the CHSH inequality [9], an experiment with pairs of particles and two parties, Alice and Bob, is considered. In each round of the experiment, each party receives one particle of a pair and performs a local measurement on it, using one out of two measurement settings. The choice of the local measurement settings depends on the randomly chosen binary input x for Alice and y for Bob. The measurements produce a binary output a for Alice and a binary output b for Bob (Fig. 1).

The correlation value S of the CHSH inequality is $S = |\sum_{x,y}(-1)^{xy}[P(a=b|xy) - P(a \neq b|xy)]|$ [27], where $|.|$ denotes the absolute value, and $P(a=b|xy)$ [or $P(a \neq b|xy)$] is the probability that output $a=b$ (or $a \neq b$) when the measurement settings (x, y) are chosen. For all local realistic theories, S cannot exceed the maximum value of 2. In contrast, quantum mechanics allows the value of S to be between 2 and $2\sqrt{2}$ [8,9].

The aforementioned experiment is performed as a loophole-free Bell test [19]. In this Bell test, Alice and Bob each operate an atom trap for a single rubidium atom. The atom trap on each side, which are separated by 398 m, are independently operated, making up their own laser system and control electronics. The atomic qubits are encoded in the $m_F = \pm 1$ Zeeman sublevel of the $5S_{1/2}, F = 1$ ground state, with $|\uparrow\rangle_z$ corresponding to $m_F = +1$ and $|\downarrow\rangle_z$ corresponding to $m_F = -1$.

For the creation of the entangled atom-photon pairs, each atom is excited to the $5P_{3/2}, F' = 0, m_F = 0$ state via a short laser pulse. The subsequent spontaneous emission yields to a photon whose polarization is entangled with the atomic qubit state. Both photons are coupled into single-mode fibers and are guided to a Bell state measurement (BSM) setup, where two-photon interference on a fiber beam splitter together with

[*] Corresponding author: i.gerhardt@pi3.uni-stuttgart.de

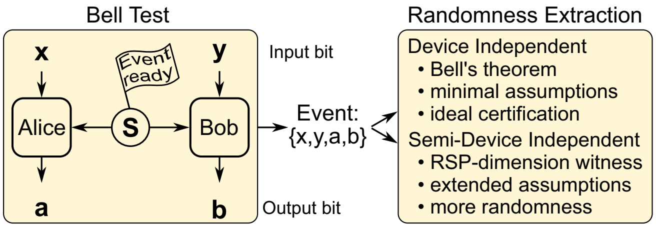

FIG. 1. A Bell test involves two physically separated systems, and two given input bits, x and y, generate outcomes a and b. The Bell correlation value S in a DI scenario allows one to quantify the amount of randomness; another scenario is to extract SDI randomness when a remote-state-preparation (RSP) dimension witness is utilized.

photon polarization analysis is employed to project the photons on two out of the four possible Bell states. The photonic measurement heralds the creation of one of the entangled atom states, $|\Psi^{\pm}\rangle = 1/\sqrt{2}(|\uparrow\rangle_x|\downarrow\rangle_x \pm |\downarrow\rangle_x|\uparrow\rangle_x)$, where $|\uparrow\rangle_x = (1/\sqrt{2})(|\uparrow\rangle_z + |\downarrow\rangle_z)$ and $|\downarrow\rangle_x = (i/\sqrt{2})(|\uparrow\rangle_z - |\downarrow\rangle_z)$.

After entanglement is created between Alice and Bob, they start a fast atomic state measurement process based on state selective ionization and subsequent detection of the ionization fragments. The measurement setting is determined by the polarization of a laser pulse exciting the atom before ionization. For the choice of the setting each party employs a quantum random number generator (QRNG) outputting freshly generated random bits on demand. The total time needed from the generation of the input x or y to receiving the output a or b is less than 1.1 μs; together with a separation of the atom traps of 398 m this enables spacelike separation of the measurements [28]. Thus, the experiment enforced the assumptions made for deriving the CHSH inequality. In total, 55 568 rounds were recorded, 27 885 with the $|\Psi^+\rangle$ prepared and 27 683 with the $|\Psi^-\rangle$ prepared.

DI certification protocol. As outlined above, device independence can be linked to the violation of the Bell inequality [29]. This implies that, as long as the Bell inequality is guaranteed to be violated, true randomness can be generated.

Although the randomness certified by Bell's theorem *can* be device independent, we still need some extra assumptions to bound the randomness in this model [10]: (i) the remote parties perform local and independent measurements on their ideally spacelike separated (=perfectly shielded) devices; (ii) the measurement settings (*x,y*) are not determined beforehand and are unpredictably chosen; and (iii) the measurement process is described by quantum mechanics, and nature is not, e.g., predetermined as a whole. In a loophole-free Bell test the assumption (i), which is required for a loophole-free Bell test is fulfilled. Assumption (ii) means that the ith inputs x_i and y_i are not known to the experimental devices until the ith run of the experiment.

In Ref. [10], the marginal guessing probability $p(a|x)$ had been connected to the correlation value S of the CHSH inequality. This allows one to bound the entropy of the output data to 1 bit per event when $S = 2\sqrt{2}$. Due to the finite data size, the confidence level is introduced. Using the analytical model in Ref. [10], and taking the confidence level as 0.99 [10,25], the min-entropy in our Bell test data can be quantified. For the $|\Psi^+\rangle$ state, the data resulted in $S = 2.085$, and with a total number of events $n = 27\,885$, no DI randomness can be certificated for this entangled state. Performing the same task for the 27 683 events from the $|\Psi^-\rangle$ state, the value of S amounts to 2.177. The min-entropy of the DI randomness amounts to 531 bits, which is much smaller than our SDI randomness as we show in the following text.

SDI certification protocol. For the certification of the randomness from the Bell test data, Bell inequalities must be violated. Unfortunately, the loophole-free Bell experiments [16–19] did not reach the maximally allowed values for quantum mechanics. Thus only a small amount of randomness per round can be certified in the DI manner. As we have shown above, sometimes no randomness can be certified [30]. However, when we introduce additional assumptions and leave the DI scenario, this situation changes. To build the experimental devices, it is necessary to have some knowledge about the way they function; e.g., the devices are error prone but not maliciously built. This knowledge allows for a higher bound of the randomness per event for the same experiment. Using a *dimension witness* is one possible way for such a higher bound of the randomness.

The concept of dimension witness was introduced in Ref. [31]. After this paper, a substantial number of studies have been performed on this concept [23,32–35].

Before applying the dimension witness to the Bell experiment, we first show that the experiment admits a two-dimensional quantum representation [23,31,32].

In our Bell test, there are two inputs, x and y, and two outputs, a and b. When Alice does one of her two measurements, the entangled state of Bob's side will randomly collapse into one specific state. Since Alice has two different measurement settings and each one has two different measurement results, when she does her two measurements randomly multiple times, Bob's side will get four quantum states. These four quantum states in Bob's side are represented as x', and $p(b|x', y) = p(b|x, a, y) = p(ab|xy)/p(a|x, y)$, since (see Supplemental Material [36])

$$p(b|x', y) = \mathrm{Tr}\big(\rho_{a|x} M^B_{b|y}\big), \tag{1}$$

where $\rho_{a|x}$ is the state on Bob's side when Alice performs her measurement x and gets a result a. $M^B_{b|y}$ is the measurement operator on Bob's side. $\rho_{a|x}$ and $M^B_{b|y}$ are acting on $\mathbb{C}^2$ (a two-dimensional complex coordinate space). So, $p(b|x', y)$ admits a two-dimensional quantum representation [37]. This shows that we can use the two-dimensional dimension witness [23] to quantify the quantumness in our Bell test.

Different kinds of dimension witnesses can be used in a two-dimensional quantum representation. The dimension witness we used here was introduced in Ref. [23]. The advantage of this nonlinear dimension witness is that it can be used for a nonconvex set and is robust to technical imperfections. Most importantly, it can be used to certify randomness [23]. It is defined as

$$W = \begin{vmatrix} p(1|0, 0) - p(1|1, 0) & p(1|2, 0) - p(1|3, 0) \\ p(1|0, 1) - p(1|1, 1) & p(1|2, 1) - p(1|3, 1) \end{vmatrix}, \tag{2}$$

where $p(b|x', y)$ is defined in Eq. (1), and the result b is chosen as "1" in the above definition. The definition equation of the dimension witness here is the same as that in Ref. [23], but the state x' differs. Here, the state x' is on Bob's side, but its preparation is completed by the projective measurement of Alice, so the state x' is remotely prepared [38,39]. To emphasize this difference, we name it the remote-state-preparation (RSP) dimension witness.

From the above definition, the RSP dimension witness W_B for Bob's side is constructed. Similarly, W_A can be constructed for Alice's side. We define $W_{\text{rsp}} = \min\{W_A, W_B\}$, and we use W_{rsp} as the RSP dimension witness in the following model. The RSP dimension witness captures the quantumness of the preparation and measurements in our Bell test. If the preparations are classical, one has $W_{\text{rsp}} = 0$, while a quantum preparation and measurement leads to $0 < W_{\text{rsp}} \leqslant 1$.

Although S and W_{rsp} are based on the same experimental data, they are not directly linked: S cannot be used to calculate the value of W_{rsp}; it only affects the lower limit of W_{rsp}. For example, when $S = 2$, $W_{\text{rsp}} \in [0, 1]$, and when $S = 2\sqrt{2}$, $W_{\text{rsp}} = 1$.

Before using the RSP dimension witness to bound the randomness generated during the experiment, we discuss the required assumptions. As before, we require that the above (DI) assumptions, (i)–(iii), hold true. Besides, there are some extra assumptions [25]: (iv) the information in the measurement results of each side is contained in a two-dimensional quantum subspace; and (v) the system is memoryless and subsequent outcomes are not directly correlated.

In the RSP-dimension witness model, it is important that the state preparation and measurement are independent from each other. This requirement is fulfilled by assumptions (i) and (ii) in the following way. Let us take W_B as an example. For W_B, the states x' on Bob's side are remotely prepared by Alice's quantum measurements, which cannot be affected by Bob's device or measurement, so the states x' are independent from Bob's device and measurement y. This independence requirement is naturally fulfilled by our loophole-free Bell test [19]. The prepared states x' might be affected by Alice's device, but that is not a problem for our model. Because if x' is affected by the device on Alice's side, the state on Bob's side will not be properly prepared, and the value of the RSP dimension witness will be decreased. Thus, the independence of x' is quantified by the value of the RSP dimension witness, and no postselection is needed to increase the independence of x'. Assumption (i) also implies that the experimental devices do not have any preestablished correlations among each other; this also indicates that the devices that are used to generate the input strings x and y are not correlated with the measurement devices. Subsequently, x and y can be pseudorandom numbers, as long as they are independent from each other and the measurement apparatus.

Assumption (iv) means that the information contained in the measurement result of measuring x' does not exceed 1 bit; a possible violation would be that the information about x' is duplicated by or correlated with extra qubits. Assumption (iv) can be relaxed by the spacelike separation of Alice and Bob in our Bell test. In general, a bipartite entangled state shared between Alice and Bob has two different measurement results on each side with one measurement setting—the measurement results are binary and can be described by a qubit. The measurement results are binary does not mean that the entangled state shared between Alice and Bob has to be confined in a two-dimensional Hilbert space; it only means that with the measurement done by Alice or Bob the results information is contained in a qubit.

As for the given experiment, the state preparation of the RSP dimension witness is independently completed by two sides: one side performs the measurement and the other side gets the state simultaneously. Under spacelike separation, when the state is prepared by one side, the measurement is performed outside the light cone of state preparation. Thus, it is impossible for the state-preparation devices to send extra qubits of the prepared states to the measurement devices without lowering the values of W_{rsp} [40]. As long as $W_{\text{rsp}} > 0$, the remote measurements are exceeding a classical correlation.

Since the inputs x and y are independent from each other, and in the experiment different choices of the measurement settings are uniformly random, thus each combination of x and y occurs with probability 1/4 [25]. Then, the guessing probability p_{guess} of $p(ab|xy)$ is (see Supplemental Material [36])

$$
\begin{aligned}
p_{\text{guess}}(ab|xy) &= \frac{1}{4}\sum_{x,y}\max_{a,b} p(ab|xy)\\
&\leqslant \max_{x,a} p(a|x)\frac{1}{2}\sum_{y}\max_{x,a,b} p[b|(x,a),y]\\
&\leqslant \left(\frac{1+\sqrt{1-W_{\text{rsp}}^2}}{2}\right)\frac{1}{2}\\
&\quad\times\left(1+\sqrt{\frac{1+\sqrt{1-W_{\text{rsp}}^2}}{2}}\right). \qquad (3)
\end{aligned}
$$

As we can see, the equation of the guessing probability $p_{\text{guess}}(ab|xy)$ from W_{rsp} is not the same as the one from Ref. [25]. The difference is caused by $\max_{x,a} p(a|x)$, which represents the quantum measurement from the state-preparation process.

The conditional min-entropy $H_\infty(AB|XY)$ in this situation is $H_\infty(AB|XY) = -\log_2 p_{\text{guess}}(ab|xy)$. This equation allows us to bound the randomness in the experimental data in a SDI way. The randomness per event from the RSP dimension witness model is depicted in Fig. 2. Compared to Ref. [25], the introduction of quantum measurements in the state preparation process gives us a significant advantage to bound the randomness in our experimental data. For instance, the maximum certified randomness in our model is 1.23 bits per event, which is significantly larger than the previous dimension witness model [25].

The presented RSP dimension witness model can certify substantially more randomness in the Bell test from a different perspective. Only a few more extra assumptions are required for this. Moreover, when S is below the classicality bound 2, the W_{rsp} can still be larger than 0 (see example below).

In a practical Bell test, because of the imperfect measurements or entangled states, the Bell inequality might not be violated. In this case, no randomness can be certified by previous models [10–12,41,42]. With the RSP dimension witness

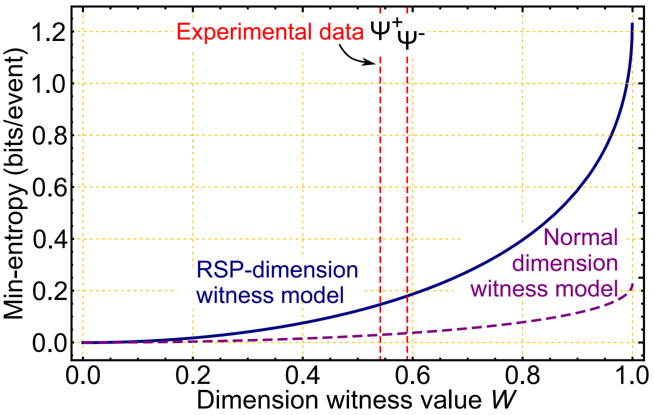

FIG. 2. Output randomness utilizing the dimension witness. The nonzero RSP dimension witness $W_{\rm rsp}$ gives us a different perspective to bound the randomness in the experimental data. The blue curve displays the randomness certified by the $W_{\rm rsp}$, while the dashed purple curve represents the randomness certified by the previously defined dimension witness [23]. Clearly, the combination of remote state preparation and the dimension witness increases the bound of randomness per event, as compared to a normal dimension witness certification model in Ref. [25].

model, randomness in the experimental data can be certified without using Bell's theorem. For instance, let Alice and Bob share a Bell state, then they measure it with two identical measurement settings $\widehat{x}$ and $\widehat{z}$ on each side (which corresponds to the BBM92 quantum key distribution scheme [43]). In this case, Bell inequalities will not be violated, but the bound of randomness is 1.23 bits per event data from $W_{\rm rsp}$.

This example manifests that, by rotating Alice and Bob's measurement basis, the RSP-dimension witness is not changed, and it also shows the robustness of our SDI protocol. The corresponding S value would of course be decreased. This demonstrates that, without using Bell's theorem, randomness in the Bell test data can still be certified.

We further consider the following two-qubit Werner state (4) as an example:

$$\rho_z = z|\Psi^+\rangle\langle\Psi^+| + \frac{1-z}{4}\mathbf{I}, \tag{4}$$

where $0 \leqslant z \leqslant 1$ is the noise parameter. For this state the relationship between $W_{\rm rsp}$ and S can be derived. On one hand, the relationship between z and S is $S = 2\sqrt{2}z$. On the other hand, following Ref. [23], the relationship between z and the RSP dimension witness is derived as $W_{\rm rsp} = z^2$. Subsequently, the relationship between $W_{\rm rsp}$ and S is calculated as $W_{\rm rsp} = S^2/8$. From this relationship we can also see that $W_{\rm rsp}$ is nonzero when $0 < S \leqslant 2$. This shows again that, without using Bell's theorem, randomness in the Bell test data can be certified.

Our SDI model and the DI model in Ref. [10] both utilize quantum correlations to certify the quantum randomness. The DI model uses the correlation between the measurement results to form a CHSH inequality, the violation of the CHSH inequality guarantees that the randomness is certified. In the SDI model, the correlation between Alice and Bob's measurement results is not quantified by Bell's theorem, but by our nonlinear RSP dimension witness. This RSP dimension witness can quantify the quantum correlation which cannot be quantified by the CHSH inequality, such as is the case in the BBM92 scenario and the two-qubit Werner state.

Next we apply the SDI model to bound the randomness produced in the Bell test [19] and then extract the randomness with hashing functions. In the following randomness extraction, due to the finite data size, the confidence level of the model and the error of hashing functions [44] are introduced. The confidence level is again taken as 99%, and the hashing error is chosen as 0.001. We use universal hashing functions to extract the bounded randomness (see Supplemental Material [36]). Considering the $|\Psi^+\rangle$ state, the collected data resulted in $S = 2.085$ and a total number of events $n = 27\,885$. We calculate the RSP dimension witness value for this entangled state as $W_{\rm rsp} = 0.542$. The SDI randomness extracted in all events amounts to 3821 bits, which is a tremendous improvement compared to the 0 bits in the DI model of Ref. [10].

Performing the same task for the 27 683 events from the $|\Psi^-\rangle$ state, the value of S amounts to 2.177, and the RSP dimension witness value is $W_{\rm rsp} = 0.591$. The extracted SDI randomness amounts to 4660 bits, which is much larger than the 531-bit DI randomness [45].

Conclusion. We have presented two methods to bound the randomness in our Bell test data. The DI model from Ref. [10] is based on Bell's theorem, and its applicability holds especially for the CHSH variant of the test [9]. For all the 55 568 events' data, the min-entropy of the DI randomness is 531 bits, which is 10^{-2} bits per event data. An extended RSP dimension witness model is designed in this work for the same version of the Bell test. For all the 55 568 events' data, the total min-entropy of the extracted SDI randomness is 8481 bits, corresponding to 0.153 bits per event data, which is significantly higher than 10^{-2} bits per event data.

Our RSP dimension witness model improves the bound of the randomness from the data tremendously without using Bell's theorem and it is still possible to extract randomness with this model when the Bell inequality is not violated as shown in the paper. Of course, the model offers security guarantees for randomness that are weaker than the security guarantees of the DI model, but it is still certified randomness under SDI conditions. Also, the requirements in the SDI model can be fulfilled by standard technologies, which are much less complex than the loophole-free Bell test.

ACKNOWLEDGMENTS

We acknowledge the financial support from the Center for Integrated Quantum Science and Technology (IQ$^{\rm ST}$).

[1] D. E. Knuth, *The Art of Computer Programming, Volume 2 : Seminumerical Algorithms*, 3rd ed. (Addison-Wesley, Boston, 1997).

[2] F. Galton, Nature (London) **42**, 13 (1890).

[3] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).

[4] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).

[5] L. D. Landau and E. M. Lifshitz, *Quantum Mechanics: Non-relativistic Theory*, Course of Theoretical Physics Vol. 3 (Elsevier, Amsterdam, 2013).

[6] A. Acín and L. Masanes, Nature (London) **540**, 213 (2016).

[7] X. Chen, J. N. Greiner, J. Wrachtrup, and I. Gerhardt, Sci. Rep. **9**, 18474 (2019).

[8] J. S. Bell, Phys. Phys. Fiz. **1**, 195 (1964).

[9] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[10] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning *et al.*, Nature (London) **464**, 1021 (2010).

[11] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 459 (2018).

[12] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam *et al.*, Nature (London) **556**, 223 (2018).

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

[14] E. Knill, Y. Zhang, and P. Bierhorst, Phys. Rev. Research **2**, 033465 (2020).

[15] Y. Zhang, H. Fu, and E. Knill, Phys. Rev. Research **2**, 013016 (2020).

[16] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán *et al.*, Nature (London) **526**, 682 (2015).

[17] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán *et al.*, Phys. Rev. Lett. **115**, 250401 (2015).

[18] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman *et al.*, Phys. Rev. Lett. **115**, 250402 (2015).

[19] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, Phys. Rev. Lett. **119**, 010402 (2017).

[20] For the semi-device-independent protocols mentioned in this article, the assumptions about the experimental devices should be general, which means they are not supposed to characterize the devices in detail, and they do not belong to source-independent or measurement-device-independent protocols.

[21] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967).

[22] M. Um, X. Zhang, J. Zhang, Y. Wang, Y. Shen, D.-L. Deng, L.-M. Duan, and K. Kim, Sci. Rep. **3**, 1627 (2013).

[23] J. Bowles, M. T. Quintino, and N. Brunner, Phys. Rev. Lett. **112**, 140407 (2014).

[24] M. Jerger, Y. Reshitnyk, M. Oppliger, A. Potocnik, M. Mondal, A. Wallraff, K. Goodenough, S. Wehner, K. Juliusson, N. K. Langford *et al.*, Nat. Commun. **7**, 12930 (2016).

[25] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).

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

[27] To allow for a violation of the CHSH inequality, for certain state and measurement setting combinations, a permutation of the values of a and b might be necessary.

[28] J.-Å. Larsson, J. Phys. A: Math. Theor. **47**, 424003 (2014).

[29] R. Colbeck, Ph.D. dissertation, University of Cambridge, Cambridge, England, 2009.

[30] This may be caused by (i) the finite amount of events or (ii) simply that the Bell inequality is not violated.

[31] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. A. Méthot, and V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008).

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

[33] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011).

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

[35] H.-W. Li, P. Mironowicz, M. Pawłowski, Z.-Q. Yin, Y.-C. Wu, S. Wang, W. Chen, H.-G. Hu, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **87**, 020302(R) (2013).

[36] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.103.042211 for the proof of $p(b|x', y) = \mathrm{Tr}(\rho_{a|x} M^B_{b|y})$, the derivation of $p_{\mathrm{guess}}(ab|xy)$, and the extraction of bounded randomness by universal hashing functions.

[37] The entangled state shared between Alice and Bob can be in a higher dimension; it does not need to be reduced to a lower dimension. Alice and Bob only measure this entangled state in a two-dimensional Hilbert space. Thus, the input and output data will form a distribution $p(b|x', y)$, which admits a two-dimensional quantum representation. As long as the inputs x and y and the outputs a and b form a two-dimensional quantum representation, regardless of its nonconvexity and its origins, the nonlinear dimension witness can be applied.

[38] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, Phys. Rev. Lett. **87**, 077902 (2001).

[39] C. H. Bennett, P. Hayden, D. W. Leung, P. W. Shor, and A. Winter, IEEE Trans. Inf. Theory **51**, 56 (2005).

[40] This means, the extra qubits sent out by the state preparation devices can be treated as classical noise in this situation.

[41] A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).

[42] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).

[43] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[44] The hashing error means the extracted random string is at most $\Delta-$ far from a uniform random distribution [46].

[45] The 531-bit randomness is the bounded randomness from the DI model, not considering the hashing error. If we take the 0.001 hashing error into consideration, this value will decrease to 495 bits.

[46] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 5524 (2011).