

## Randomness Certification from Multipartite Quantum Steering for Arbitrary Dimensional Systems

Yi Li,<sup>1,2</sup> Yu Xiang<sup>1,3,\*</sup> Xiao-Dong Yu<sup>1,4</sup> H. Chau Nguyen<sup>1,5</sup> Otfried Gühne<sup>1,5</sup> and Qiongyi He<sup>1,3,6,7</sup>

<sup>1</sup>State Key Laboratory for Mesoscopic Physics, School of Physics, Frontiers Science Center for Nano-optoelectronics, Peking University, Beijing 100871, China

<sup>2</sup>Beijing Academy of Quantum Information Sciences, Beijing 100193, China


<sup>3</sup>Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan, Shanxi 030006, China

<sup>4</sup>Department of Physics, Shandong University, Jinan 250100, China

<sup>5</sup>Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, 57068 Siegen, Germany

<sup>6</sup>Peking University Yangtze Delta Institute of Optoelectronics, Nantong 226010, Jiangsu, China

<sup>7</sup>Hefei National Laboratory, Hefei 230088, China

 (Received 16 July 2023; revised 6 December 2023; accepted 24 January 2024; published 21 February 2024)

Entanglement in bipartite systems has been applied to generate secure random numbers, which are playing an important role in cryptography or scientific numerical simulations. Here, we propose to use multipartite entanglement distributed between trusted and untrusted parties for generating randomness of arbitrary dimensional systems. We show that the distributed structure of several parties leads to additional protection against possible attacks by an eavesdropper, resulting in more secure randomness generated than in the corresponding bipartite scenario. Especially, randomness can be certified in the group of untrusted parties, even when there is no randomness in either of them individually. We prove that the necessary and sufficient resource for quantum randomness in this scenario is multipartite quantum steering when each untrusted party has a choice between only two measurements. However, the sufficiency no longer holds with more measurement settings. Finally, we apply our analysis to some experimentally realized states and show that more randomness can be extracted compared with the existing analysis.

DOI: [10.1103/PhysRevLett.132.080201](https://doi.org/10.1103/PhysRevLett.132.080201)

*Introduction.*—Randomness plays an important role in scientific simulation and cryptography [1,2]. Different from the classical theory, where any system admits at least a deterministic description, measurements in quantum mechanics have an inherently random character [3]. As another remarkable feature of quantum theory, entanglement can be used to certify randomness. For example, measurement outcomes leading to a Bell inequality violation cannot be deterministically predicted within any no-signaling theory [4–6], thus intrinsic randomness exists among the outcomes. Therefore, some protocols for randomness generation were derived from this feature [7–20] and demonstrated experimentally [21–27].

Quantum steering is an intermediate type of quantum correlation between Bell nonlocality [4] and entanglement [28]. It describes the phenomenon where measurements performed by one party can remotely adjust the state of the other party [29–31]. In this scenario, entanglement can be verified without relying on any assumed models of the steering party’s devices [32]. This leads to a one-sided device-independent approach to certify randomness [19], which is more robust to noise than the fully-device-independent protocols based on Bell nonlocality [33–41].

In view of a potential real-world quantum network distributing multipartite entanglement, it is a relevant topic to explore the generation of randomness distributed over many nodes in an entanglement-based network. So far, multipartite quantum steering [42,43] has been successfully demonstrated in photonic networks [43–45], continuous-variable optical networks [46–49], and atomic ensembles [50]. The majority of theoretical studies and experiments for randomness generation, however, have focused specifically on the bipartite scenario [19–23], where a well-known theorem by Schrödinger [51–54] guarantees that any no-signaling state assemblage can originate from a global quantum state. Consequently, the considered task can be expressed in terms of a semidefinite programming (SDP) problem over all no-signaling bipartite assemblages. In the multipartite case, however, there exist no-signaling assemblages that do not admit a quantum realization [55]. Hence quantifying the amount of certifiable randomness accurately is now a serious challenge.

Moreover, in order to determine the minimal resources required for quantum cryptography, and also for fundamental interest, the relationship between quantum correlations and randomness has been discussed. Great effort

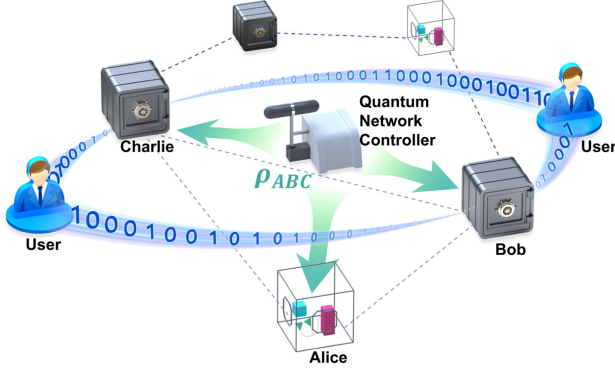


FIG. 1. Schematic view on randomness generation in a multipartite network as discussed in this Letter. A controller sends a tripartite state  $\rho_{ABC}$  to three nodes. Two of these nodes (Bob and Charlie) perform measurements with the aim to use the results as a source of randomness. The measurements of Bob and Charlie are not characterized, consequently they are represented by black boxes. A third trusted party (Alice) performs well-characterized measurements, determining the set of conditional states, thereby limiting the potential attacks by an eavesdropper. We find that the separation between Bob and Charlie allows us to generate more randomness than as if they are grouped together; the separation limits the observed correlations between them, but the potential attacks of an eavesdropper become even more limited. If Bob and Charlie have two measurement settings only, then randomness generation is equivalent to quantum steering.

has been devoted to demonstrating that entanglement, steering, and nonlocality are *necessary* for certifying randomness [13–21], but the *quantitative* connections remain subtle [11–14]. In these cases, the untrusted parties implemented two measurements only, but increasing the number of measurement settings could bring many benefits, e.g., additional nonlocal and steerable states can be found [56–61]. For the general cases, however, whether nonlocality or steering is *sufficient* for certifying randomness remains elusive.

In this Letter, we present the certification of randomness in multipartite quantum systems of any dimension. As shown in Fig. 1, the scenario we considered is close to the actual situation where only a few of the users have knowledge of their measurement apparatuses (transparent boxes) while the remaining users do not (black boxes). By using the definition of multipartite steering [43], we prove as our first main result that in the protocols with two measurement settings on the untrusted nodes, multipartite steering is *necessary and sufficient* for certifying randomness, independent of the number of outcomes. In the case of more than two settings, this perfect equivalence is broken; some states become steerable but cannot be used to certify randomness. As our second main result, we demonstrate that in multipartite systems it can happen that each individual party cannot have certified randomness

but, surprisingly, the eavesdropper cannot attack them simultaneously. That means these parties can still collaborate to generate joint secured randomness. This result is acquired by accurately quantifying the amount of multipartite certified randomness. We calculate upper and lower bounds through the seesaw algorithm and the generalized Navascués-Pironio-Acín (NPA) hierarchy [62–64] which tests for membership in the set of quantum behaviors, respectively. Last but not least, we certify randomness for both discrete-variable and continuous-variable systems and adopt existing experimental data [58], showing that more randomness can be generated in the multipartite scenario than the previous experiment in the bipartition case [27].

*Randomness in multipartite quantum networks.*—We consider a tripartite scenario, in which three distant parties, Alice, Bob, and Charlie, receive an unknown tripartite entangled state  $\rho_{ABC}$  from the controller, as shown in Fig. 1. Neither Bob nor Charlie trusts their devices, which are treated as “black boxes.” Still, their measurements are given by an unknown positive operator valued measure (POVM), which is a set of positive semi-definite matrices  $\{M_i\}_i$  satisfying  $\sum_i M_i = I$ . Bob and Charlie apply measurements  $M_{b|y}$  and  $M_{c|z}$  with  $m_B$  and  $m_C$  inputs, and  $n_B$  and  $n_C$  outputs, respectively, where  $y \in [m_B]$ ,  $z \in [m_C]$ ,  $b \in [n_B]$  and  $c \in [n_C]$ . Note that  $[o] := \{0, 1, \dots, o-1\}$ . The third party, Alice, has complete knowledge of her device, which allows her to perform quantum state tomography, and thus to obtain a set of unnormalized states  $\sigma_{bc|yz} = \text{Tr}_{BC}[I_A \otimes M_{b|y} \otimes M_{c|z} \rho_{ABC}]$  (referred to as a state assemblage) conditioned on Bob’s and Charlie’s measurements and results.

We assume a potential eavesdropper, Eve, who has access to her part of a quadripartite state  $\rho_{ABCE}$  and wants to predict the outcomes  $b$  and  $c$  of measurements  $y^*$  and  $z^*$  simultaneously. Since Eve knows which measurements Bob and Charlie will choose to extract randomness, which is different from the works [24,34–40] that take the input distributions into account, she can optimize her attack to obtain the information about these outcomes but still needs to coincide with the observed assemblage. Consequently, Eve gives guesses  $e \in [n_B]$  and  $e' \in [n_C]$  by performing a POVM measurement  $\{M_{e,e'}\}_{e,e'}$ . The total guessing probability that Eve’s guesses  $e = b$  and  $e' = c$  is  $P_g(y^*, z^*) = \sum_{e,e'} P_{BCE}(b = e, c = e', e, e' | y^*, z^*)$ . Hence randomness, quantified by the min-entropy [65],  $H_{\min} = -\log_2[P_g(y^*, z^*)]$ , can be certified whenever the guessing probability  $P_g < 1$ . This means Eve cannot be completely sure of both Bob and Charlie’s measurement results simultaneously.

In order to figure out Eve’s optimal strategy, we maximize her guessing probability over all measurement strategies and the possible state accessible to her, which

results in the following optimization problem:

$$\begin{aligned}
 \max P_g(y^*, z^*) &= \sum_{e, e'} \text{Tr}[(M_{b=e|y^*} \otimes M_{c=e'|z^*} \otimes M_{e, e'}) \rho_{BCE}] \\
 \text{with respect to } &\rho_{ABCE}, \{M_{b|y}\}_{b, y}, \{M_{c|z}\}_{c, z}, \{M_{e, e'}\}_{e, e'} \\
 \text{such that } &\text{Tr}_{BC}[(I_A \otimes M_{b|y} \otimes M_{c|z}) \rho_{ABC}] = \sigma_{bc|yz}^{\text{obs}}, \quad \forall b, c, y, z, \\
 &\rho_{ABCE} \geq 0, \quad \text{Tr}[\rho_{ABCE}] = 1, \\
 &\{M_{b|y}\}_b, \{M_{c|z}\}_c, \{M_{e, e'}\}_{e, e'} \in \text{POVM}, \quad \forall y, z,
 \end{aligned} \tag{1}$$

where  $\rho_{BCE} = \text{Tr}_A[\rho_{ABCE}]$ ,  $\rho_{ABC} = \text{Tr}_E[\rho_{ABCE}]$  and  $\{\sigma_{bc|yz}^{\text{obs}}\}_{b, c, y, z}$  is the assemblage observed by Alice. The first constraint guarantees that Eve's strategy is compatible with the assemblage observed by Alice.

*Multipartite steering as a resource for certified randomness.*—Multipartite steering is defined when both Bob and Charlie hold the untrusted devices and the assemblage  $\{\sigma_{bc|yz}^{\text{obs}}\}_{b, c, y, z}$  cannot be explained by a fully separable model, i.e.,  $\rho^{A:B:C} \neq \sum_{\lambda} p_{\lambda} \rho_{\lambda}^A \otimes \rho_{\lambda}^B \otimes \rho_{\lambda}^C$ . For this, strong tests in terms of SDPs exist [30,43]. Combining this definition with certifiable randomness, we find that multipartite steering is *necessary* for certifying multipartite randomness on Bob and Charlie. Specifically, in the case of  $m_B = m_C = 2$ , multipartite steering is *necessary and sufficient* for certifying randomness. However, in the case of more settings, sufficiency no longer holds.

The ideas of the arguments are as follows: (i) Since the assemblage  $\sigma_{bc|yz}^{\text{obs}}$  is unsteerable if it can be described by a local hidden state model, where the distribution can be written as a convex sum of local deterministic distributions [30], the existence of multipartite steering is a necessary condition for generating randomness. (ii) For the reverse direction, we start with the case of  $m_B = m_C = 2$ , i.e., Bob measures  $\{y^*, \bar{y}^*\}$  and Charlie measures  $\{z^*, \bar{z}^*\}$ . No verifiable randomness on Bob and Charlie's sides means that Eve can predict their outcomes of measurements  $y^*$  and  $z^*$  perfectly, which implies the conditional states at Alice's side generated by  $y^*$  and  $z^*$  are the same as those generated by Eve's measurement  $M_{e, e'}$ . Thus, the state assemblage observed by Alice can be seen as generated by the set of measurements  $\{M_{e, e'}, \bar{y}^*, \bar{z}^*\}$ . Eve's measurement  $M_{e, e'}$  is, however, compatible with Bob's and Charlie's measurements  $\bar{y}^*$  and  $\bar{z}^*$  since they are made locally on separate parties. This compatibility ensures that the joint probability distribution of Bob and Charlie is local [66,67], and thus the assemblage is unsteerable by independent Bob and Charlie [68,69]. Hence, the fact that quantum steering in an actual multipartite scenario is sufficient to certify nonzero randomness is proved; more details can be found in the Supplemental Material [70]. However, the proof also shows that this sufficiency can be broken with more settings. For instance, when  $m_B \geq 3$ , the additional

measurement settings can bring incompatibility to the set of Bob's measurements (expressing steerability [66–68]). But it does not affect Eve's unit guessing probability for  $y^*$  (still zero randomness). Notice that the above argument is generally valid for multipartite as well as bipartite scenarios.

*Quantification of certified randomness in multipartite scenarios.*—Steering-based randomness in multipartite scenarios was first studied in Ref. [27] by considering bipartitions of the W state, where the measurements performed by Bob and Charlie are global, e.g., a global setting  $M_{(bc)|(yz)} \neq M_{b|y} \otimes M_{c|z}$ . This can be considered as a special case of a bipartite scenario, where the task of randomness certification can be expressed in terms of an SDP over all no-signaling bipartite assemblages within quantum theory [19]. However, in an actual multipartite scenario where the measurements performed by Bob and Charlie are local, the technique to reduce problem (1) to an SDP generally fails. In the following, we simplify the problem (1), which subsequently allows for derivation of upper and lower bounds based on a seesaw application of SDPs and the generalized NPA hierarchy, respectively [70].

First, since Eve only implements a single POVM, we can always use a joint classical-quantum state [72]  $\rho_{ABCE} = \sum_{e, e'} |e, e'\rangle_E \langle e, e'| \otimes \sigma_{ABC}^{e, e'}$  to describe their behaviors without loss of generality. Here,  $\sigma_{ABC}^{e, e'}$  is an unnormalized quantum state conditioned on Eve's outcome  $e, e'$ . Thus, the maximization problem (1) can be simplified to maximize  $\sum_{e, e'} \text{Tr}[(I_A \otimes M_{b=e|y^*} \otimes M_{c=e'|z^*}) \sigma_{ABC}^{e, e'}]$  by searching for the triple  $\{\sigma_{ABC}^{e, e'}, M_{b|y}, M_{c|z}\}$ , where the dimension of Eve's system is not relevant anymore.

Then, upper bounds on the randomness  $H_{\min}^{\text{Dim}}$  with a fixed dimension can be achieved by optimizing over individual variables of the triple, each corresponding to an SDP (seesaw algorithm). Furthermore, a lower bound  $H_{\min}^{\text{NS}}$  can be obtained by relaxing the constraints on Eve to the impossibility of superluminal signaling. This means that  $H_{\min}^{\text{NS}}$  can be calculated by solving an SDP problem over an assemblage  $\sigma_{bc|yz}^{e, e'} = \text{Tr}[I_A \otimes M_{b|y} \otimes M_{c|z} \sigma_{ABC}^{e, e'}]$  with no-signaling constraint.

Finally, in order to give a more realistic range of quantum realizations, the generalized NPA hierarchy [64] provides a series of tests, which an assemblage must pass if it admits a quantum realization. Hence some lower bounds  $H_{\min}^{Q_k}$  are given by replacing the constraints from the no-signaling set to the  $Q_k$  sets, where  $k$  corresponds to different generalized NPA levels; more details in the Supplemental Material [70]. We find that by optimizing  $\{M_{b|y}, M_{c|z}\}$  independently, an actual multipartite scenario can bring more randomness than the bipartition scenario with optimizing the global measurement  $\{M_{(bc)|(yz)}\}$ , denoted as  $H_{\min}^{\text{Glo}}$ , although they are both multiple parties involved.

Besides, in the multipartite scenario, the separate randomness generated by either party can also be considered. Now Eve only guesses the measurement outcomes of one untrusted party. Therefore, the randomness solely on Bob's outcomes can be certified by changing the objective function of Eq. (1) into  $\sum_e \text{Tr}[M_{b=e|y^*} \otimes M_e] \rho_{BE}$  where  $\rho_{BE} = \text{Tr}_{AC}[\rho_{ABCE}]$ , and so for Charlie. Note that this randomness is still constrained by the observed assemblage  $\{\sigma_{bc|yz}^{\text{obs}}\}_{b,c,y,z}$  in a tripartite scenario, which is different from the previous bipartite case. Similarly, we can derive upper and lower bounds for the separate randomness [70].

Now, we apply our findings to various experiment-relevant multipartite states, from discrete-variable to continuous-variable systems.

(i) *GHZ state.*—Consider a  $d$ -dimension GHZ state over  $N$  subsystems mixed with white noise,  $\rho_\mu = \mu|\Psi\rangle\langle\Psi| + [(1-\mu)/d^N]\mathbb{I}$ , where  $|\Psi\rangle = (1/\sqrt{d})\sum_{i=0}^{d-1}|i\rangle^{\otimes N}$  and visibility  $\mu \in [0, 1]$ . Starting with the simplest case of  $N = 3$  and  $d = 2$ , Bob and Charlie both perform three Pauli measurements  $\{\hat{X}, \hat{Y}, \hat{Z}\}$ , and the assemblage  $\{\sigma_{bc|yz}^{\text{obs}}\}_{b,c,y,z}$  is observed by Alice's tomography. Figure 2(a) shows the upper and lower bounds for the certifiable randomness on Bob and Charlie's outcomes generated by  $y^* = z^* = \hat{X}$ . The min-entropy is positive for  $\mu > 0.5$  and achieves its maximum of 2 bits at  $\mu = 1$ . Compared with the randomness  $H_{\min}^{\text{Glo}}$  for the bipartition scenario, more randomness can be certified.

Figure 2(b) shows the separate randomness generated solely on Bob's (or Charlie's) side, which exists when  $\mu > 0.70$ . This means when  $\mu \leq 0.69$ , Eve can guess Bob's (or Charlie's) outcome perfectly with her optimal strategy for Bob (or Charlie), but with the same observed assemblage and setups, she cannot guess the outcome of the other party with unit probability [70]. Compared with Fig. 2(a), certifying separate randomness requires higher state visibility. In particular, when  $0.50 < \mu \leq 0.69$ , there exists nonzero randomness on the untrusted parties together, even though Eve can predict one of them individually, which leads to additional protection against possible attacks.

We further investigate general cases of GHZ states with different numbers of parties  $N$  and dimensions  $d$ . For four parties, the measurements of three nodes are not

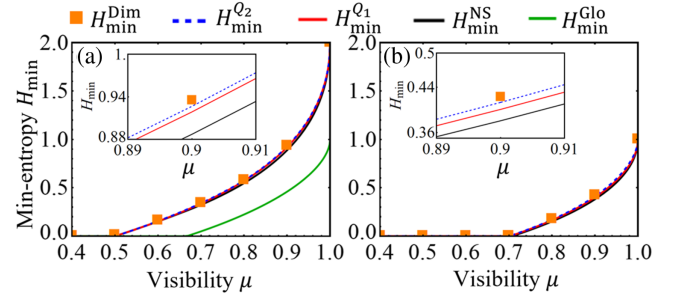


FIG. 2. Randomness certified in a noisy GHZ state with  $N = 3$ ,  $d = 2$ . (a) Multipartite randomness certified on Bob and Charlie together. (b) Separate randomness that Eve only guesses the outcomes of Bob (or Charlie). Upper bounds with fixed dimensions  $d_B = d_C = 10$  (orange square) are close to the lower bounds that correspond with different generalized NPA levels (red solid curve for  $Q_1$ , blue dashed line for  $Q_2$ ) and the no-signaling principle (black solid curve) [73]. The green solid curve shows the certified randomness when Bob and Charlie's measurements are global.

characterized while the rest node performs well-characterized measurements. The results are shown in Fig. 3, which agree with our above qualitative discussions. In particular, it is clearly seen that for the case of two measurement settings, the thresholds of multipartite randomness (generated on the untrusted parties together) are consistent with the conditions for showing multipartite steering. Increasing the number of measurements decreases the threshold of multipartite steering for the 3-qubit GHZ state from 0.5 (with measurements  $\hat{X}$  and  $\hat{Y}$ ) to 0.428 (with measurements  $\hat{X}$ ,  $\hat{Y}$ , and  $\hat{Z}$ ). However, the threshold for certified randomness remains at 0.5 even for three measurement settings.

(ii) *W-like state.*—In Ref. [58], a class of W-like states  $|\Psi_W\rangle = \alpha|001\rangle_{ABC} + \beta|010\rangle_{ABC} + \gamma|100\rangle_{ABC}$  were experimentally prepared to demonstrate the shareability of quantum steering with different measurement settings. Adopting their tomographic data for  $(\alpha, \beta, \gamma) = (0.575, 0.582, 0.576)$ ,

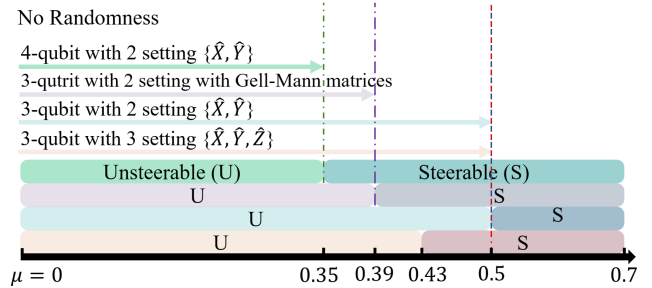


FIG. 3. The relationship of thresholds between the randomness on the untrusted parties together and multipartite steering in different GHZ states with two or three measurement settings. The left (right) blocks mean the observed assemblage is unsteerable (steerable). The arrows mean there is no randomness in their corresponding ranges of visibility.

TABLE I. Randomness certified on different parties with the experimental data in Ref. [58]. Here the optimal measurements are chosen to maximize the randomness.

Parties of randomness	$H_{\min}^{\text{NS}}$	$H_{\min}^{Q_1}$	$H_{\min}^{Q_2}$	$H_{\min}^{\text{Dim}}$	$H_{\min}^{\text{Glo}}$
Bob only	0.592	0.736	0.738	0.769	...
Charlie only	0.595	0.739	0.740	0.774	...
Bob and Charlie	1.236	1.445	1.451	1.525	0.783

nearly a W state, we calculate the amount of randomness for different scenarios, as listed in Table I. It can be seen that the amount of reliable random bits  $H_{\min}^{Q_2}$  certified by local measurements is significantly higher than that achieved by the method with global measurements adopted in the previous experiment [27].

(iii) *Three-mode squeezed vacuum state.*—A three-mode entangled Gaussian state can be generated by mixing two squeezed inputs with squeezing level  $r$  and one extra vacuum state as shown in Fig. 4(a). For the continuous-variable systems, we can bin the homodyne measurement outputs into a finite number of outcomes like Fig. 4(b) [20,74], where each outcome is associated with a conditional state. By analyzing the corresponding assemblage, we evaluate the upper and lower bounds of randomness on Bob and Charlie’s measurement results as well as the separate randomness on Bob or Charlie only. Note that the min-entropy is maximized over binning periods  $T_{\hat{x},\text{Bob}}, T_{\hat{x},\text{Charlie}} \in [2, 10]$  independently; more details in the Supplemental Material [70]. As Bob and Charlie always steer Alice together with quadrature measurements  $\{\hat{x}, \hat{p}\}$ , the multipartite randomness on Bob and Charlie exists for any transmission factor  $\eta_2$  of the second beam splitter, as illustrated in Fig. 4(c). However, when  $\eta_2$  is in the range of  $[0, 0.11]$  or  $[0.89, 1]$ , Eve can guess right the measurement outcomes of Bob or Charlie individually.

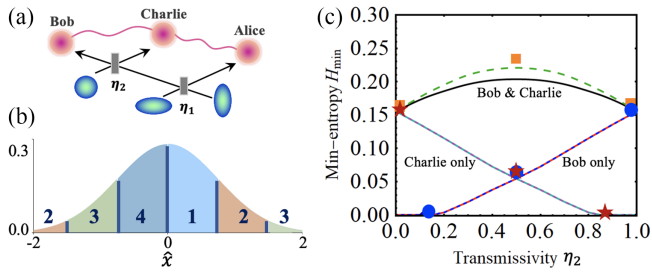


FIG. 4. Randomness certified in continuous-variable system. (a) Scheme of generating three-mode squeezed vacuum state by a linear optical network. (b) Bob’s quadrature measurement  $\hat{x}$  is binned into 4 outcomes. (c) The lower (solid curve for  $H_{\min}^{\text{NS}}$  and dashed curve for  $H_{\min}^{Q_1}$ ) and upper bounds (orange square for Bob and Charlie together, red pentagram for Charlie only and blue circle for Bob only) of randomness. Here we set  $r = 0.345$  (corresponding to  $-3$  dB quadrature noise),  $\eta_1 = 1/2$ ,  $y^* = z^* = \hat{x}$ , and cut off the Fock basis to one photon.

*Conclusion.*—We first presented the randomness certification from multiple untrusted parties in an asymmetric network and discussed the relation between multipartite steering and certifiable randomness. When the untrusted parties perform two measurement settings locally, we proved that the multipartite steering is necessary and sufficient for generating randomness by connecting the randomness with incompatible measurements. Increasing measurement settings contributes to demonstrating steering but does not necessarily certify randomness in a larger parameter range, which helps us to determine the minimal resource in quantum cryptography. Second, we quantified multipartite randomness on some typical states from discrete-variable to continuous-variable systems. The results showed that the amount of multipartite randomness is significantly improved, which can promise additional security in networks. So far, multipartite steering has been demonstrated in various platforms [23,43–50], which lays a favorable foundation for generating multipartite randomness. Further, as the loss of events in real-world applications will open a “detection loophole” whenever parties are untrusted, we also provide evidence that the loss does not affect the relation between randomness and multipartite steering [70]. Several experiments of quantum random number generation based on a loophole-free Bell test have been successfully implemented [36–40]. We also expect the state-of-the-art experiment would perform a loophole-free demonstration of certifying randomness in such an asymmetric network.

We acknowledge enlightening discussions with Paul Skrzypczyk and experimental data from Kai Sun. This work is supported by the National Natural Science Foundation of China (Grants No. 11975026, No. 12125402, and No. 12004011), and the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0301500). X. D. Y. acknowledges support by the National Natural Science Foundation of China (Grants No. 12205170 and No. 12174224) and the Shandong Provincial Natural Science Foundation of China (Grant No. ZR2022QA084). H. C. N. and O. G. were supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation, Projects No. 447948357 and No. 440958198), the Sino-German Center for Research Promotion (Project M-0294), the ERC (Consolidator Grant No. 683107/TempoQ), the German Ministry of Education and Research (Project QuKuK, BMBF Grant No. 16KIS1618K).

\*xiangy.phy@pku.edu.cn

- [1] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, *Rev. Mod. Phys.* **89**, 015004 (2017).
- [2] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, *npj Quantum Inf.* **2**, 16021 (2016).

- [3] M. Born, Zur Quantenmechanik der Stoßvorgänge, *Z. Phys.* **37**, 863 (1926).
- [4] J. S. Bell, On the Einstein Podolsky Rosen paradox, *Phys. Phys. Fiz.* **1**, 195 (1964).
- [5] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
- [6] L. Masanes, A. Acín, and N. Gisin, General properties of nonsignaling theories, *Phys. Rev. A* **73**, 012112 (2006).
- [7] S. Sarkar, J. J. Borkała, C. Jebarathinam, O. Makuta, D. Saha, and R. Augusiak, Self-testing of any pure entangled state with the minimal number of measurements and optimal randomness certification in a one-sided device-independent scenario, *Phys. Rev. Appl.* **19**, 034038 (2023).
- [8] L. Woollorton, P. Brown, and R. Colbeck, Tight analytic bound on the trade-off between device-independent randomness and nonlocality, *Phys. Rev. Lett.* **129**, 150403 (2022).
- [9] Z. Cao, H. Zhou, and X. Ma, Loss-tolerant measurement-device-independent quantum random number generation, *New J. Phys.* **17**, 125011 (2015).
- [10] S. Fehr, R. Gelles, and C. Schaffner, Security and composability of randomness expansion from Bell inequalities, *Phys. Rev. A* **87**, 012335 (2013).
- [11] G. de la Torre, M. J. Hoban, C. Dhara, G. Pretico, and A. Acín, Maximally nonlocal theories cannot be maximally random, *Phys. Rev. Lett.* **114**, 160502 (2015).
- [12] E. Woodhead, J. Kaniewski, B. Bourdoncle, A. Salavrakos, J. Bowles, A. Acín, and R. Augusiak, Maximal randomness from partially entangled states, *Phys. Rev. Res.* **2**, 042028(R) (2020).
- [13] P. Skrzypczyk and D. Cavalcanti, Maximal randomness generation from steering inequality violations using qudits, *Phys. Rev. Lett.* **120**, 260401 (2018).
- [14] A. Acín, S. Massar, and S. Pironio, Randomness versus nonlocality and entanglement, *Phys. Rev. Lett.* **108**, 100402 (2012).
- [15] D.-L. Deng and L.-M. Duan, Fault-tolerant quantum random-number generator certified by Majorana fermions, *Phys. Rev. A* **88**, 012323 (2013).
- [16] E. Woodhead, B. Bourdoncle, and A. Acín, Randomness versus nonlocality in the Mermin-Bell experiment with three parties, *Quantum* **2**, 82 (2018).
- [17] J.-D. Bancal, L. Sheridan, and V. Scarani, More randomness from the same data, *New J. Phys.* **16**, 033011 (2014).
- [18] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, Quantum randomness extraction for various levels of characterization of the devices, *J. Phys. A* **47**, 424028 (2014).
- [19] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, Optimal randomness certification in the quantum steering and prepare-and-measure scenarios, *New J. Phys.* **17**, 113010 (2015).
- [20] M. Ioannou, B. Longstaff, M. V. Larsen, J. S. Neergaard-Nielsen, U. L. Andersen, D. Cavalcanti, N. Brunner, and J. B. Brask, Steering-based randomness certification with squeezed states and homodyne measurements, *Phys. Rev. A* **106**, 042414 (2022).
- [21] Y. Guo, S. Cheng, X. Hu, B.-H. Liu, E.-M. Huang, Y.-F. Huang, C.-F. Li, G.-C. Guo, and E. G. Cavalcanti, Experimental measurement-device-independent quantum steering and randomness generation beyond qubits, *Phys. Rev. Lett.* **123**, 170402 (2019).
- [22] J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco *et al.*, Multidimensional quantum entanglement with large-scale integrated optics, *Science* **360**, 285 (2018).
- [23] D. J. Joch, S. Slussarenko, Y. Wang, A. Pepper, S. Xie, B.-B. Xu, I. R. Berkman, S. Rogge, and G. J. Pryde, Certified random-number generation from quantum steering, *Phys. Rev. A* **106**, L050401 (2022).
- [24] M.-H. Li, X. Zhang, W.-Z. Liu, S.-R. Zhao, B. Bai, Y. Liu, Q. Zhao, Y. Peng, J. Zhang, Y. Zhang *et al.*, Experimental realization of device-independent quantum randomness expansion, *Phys. Rev. Lett.* **126**, 050503 (2021).
- [25] F. Xu, J. H. Shapiro, and F. N. C. Wong, Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring, *Optica* **3**, 1266 (2016).
- [26] D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent ultrafast quantum random number generation, *Phys. Rev. Lett.* **118**, 060503 (2017).
- [27] A. Máttar, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. S. Ribeiro, S. P. Walborn, and D. Cavalcanti, Experimental multipartite entanglement and randomness certification of the W state in the quantum steering scenario, *Quantum Sci. Technol.* **2**, 015011 (2017).
- [28] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, *Rev. Mod. Phys.* **81**, 865 (2009).
- [29] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, Quantum steering, *Rev. Mod. Phys.* **92**, 015001 (2020).
- [30] D. Cavalcanti and P. Skrzypczyk, Quantum steering: A review with focus on semidefinite programming, *Rep. Prog. Phys.* **80**, 024001 (2016).
- [31] Y. Xiang, S. Cheng, Q. Gong, Z. Ficek, and Q. He, Quantum steering: Practical challenges and future directions, *PRX Quantum* **3**, 030102 (2022).
- [32] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox, *Phys. Rev. Lett.* **98**, 140402 (2007).
- [33] A. Acín and L. Masanes, Certified randomness in quantum physics, *Nature (London)* **540**, 213 (2016).
- [34] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan *et al.*, Device-independent randomness expansion against quantum side information, *Nat. Phys.* **17**, 448 (2021).
- [35] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji *et al.*, Device-independent randomness expansion with entangled photons, *Nat. Phys.* **17**, 452 (2021).
- [36] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li *et al.*, High-speed device-independent quantum random number generation without a detection loophole, *Phys. Rev. Lett.* **120**, 010503 (2018).
- [37] L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, and C. Kurtsiefer, Randomness extraction from Bell violation with continuous parametric down-conversion, *Phys. Rev. Lett.* **121**, 150402 (2018).

- [38] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam *et al.*, Experimentally generated randomness certified by the impossibility of superluminal signals, *Nature (London)* **556**, 223 (2018).
- [39] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan *et al.*, Device-independent quantum random-number generation, *Nature (London)* **562**, 548 (2018).
- [40] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu *et al.*, Experimental low-latency device-independent quantum randomness, *Phys. Rev. Lett.* **124**, 010505 (2020).
- [41] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, *Nature (London)* **464**, 1021 (2010).
- [42] Q. Y. He and M. D. Reid, Genuine multipartite Einstein-Podolsky-Rosen steering, *Phys. Rev. Lett.* **111**, 250403 (2013).
- [43] D. Cavalcanti, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. S. Ribeiro, and S. P. Walborn, Detection of entanglement in asymmetric quantum networks and multipartite quantum steering, *Nat. Commun.* **6**, 7941 (2015).
- [44] C.-M. Li, K. Chen, Y.-N. Chen, Q. Zhang, Y.-A. Chen, and J.-W. Pan, Genuine high-order Einstein-Podolsky-Rosen steering, *Phys. Rev. Lett.* **115**, 010402 (2015).
- [45] H. Lu, C.-Y. Huang, Z.-D. Li, X.-F. Yin, R. Zhang, T.-L. Liao, Y.-A. Chen, C.-M. Li, and J.-W. Pan, Counting classical nodes in quantum networks, *Phys. Rev. Lett.* **124**, 180503 (2020).
- [46] S. Armstrong, M. Wang, R. Y. Teh, Q. Gong, Q. He, J. Janousek, H.-A. Bachor, M. D. Reid, and P. K. Lam, Multipartite Einstein-Podolsky-Rosen steering and genuine tripartite entanglement with optical networks, *Nat. Phys.* **11**, 167 (2015).
- [47] X. Deng, Y. Xiang, C. Tian, G. Adesso, Q. He, Q. Gong, X. Su, C. Xie, and K. Peng, Demonstration of monogamy relations for Einstein-Podolsky-Rosen steering in Gaussian cluster states, *Phys. Rev. Lett.* **118**, 230501 (2017).
- [48] M. Wang, Y. Xiang, H. Kang, D. Han, Y. Liu, Q. He, Q. Gong, X. Su, and K. Peng, Deterministic distribution of multipartite entanglement and steering in a quantum network by separable states, *Phys. Rev. Lett.* **125**, 260506 (2020).
- [49] Y. Cai, Y. Xiang, Y. Liu, Q. He, and N. Treps, Versatile multipartite Einstein-Podolsky-Rosen steering via a quantum frequency comb, *Phys. Rev. Res.* **2**, 032046(R) (2020).
- [50] P. Kunkel, M. Prüfer, H. Strobel, D. Linnemann, A. Frölian, T. Gasenzer, M. Gärtner, and M. K. Oberthaler, Spatially distributed multipartite entanglement enables EPR steering of atomic clouds, *Science* **360**, 413 (2018).
- [51] E. Schrödinger, Probability relations between separated systems, *Math. Proc. Cambridge Philos. Soc.* **32**, 446 (1936).
- [52] E. T. Jaynes, Information theory and statistical mechanics. II, *Phys. Rev.* **108**, 171 (1957).
- [53] L. P. Hughston, R. Jozsa, and W. K. Wootters, A complete classification of quantum ensembles having a given density matrix, *Phys. Lett. A* **183**, 14 (1993).
- [54] N. Gisin, Stochastic quantum dynamics and relativity, *Helv. Phys. Acta* **62**, 363 (1989).
- [55] A. B. Sainz, N. Brunner, D. Cavalcanti, P. Skrzypczyk, and T. Vértesi, Postquantum steering, *Phys. Rev. Lett.* **115**, 190403 (2015).
- [56] T. Vértesi, S. Pironio, and N. Brunner, Closing the detection loophole in Bell experiments using qudits, *Phys. Rev. Lett.* **104**, 060401 (2010).
- [57] X.-M. Hu, C. Zhang, B.-H. Liu, Y. Guo, W.-B. Xing, C.-X. Huang, Y.-F. Huang, C.-F. Li, and G.-C. Guo, High-dimensional Bell test without detection loophole, *Phys. Rev. Lett.* **129**, 060402 (2022).
- [58] Z.-Y. Hao, K. Sun, Y. Wang, Z.-H. Liu, M. Yang, J.-S. Xu, C.-F. Li, and G.-C. Guo, Demonstrating shareability of multipartite Einstein-Podolsky-Rosen steering, *Phys. Rev. Lett.* **128**, 120402 (2022).
- [59] M. D. Reid, Monogamy inequalities for the Einstein-Podolsky-Rosen paradox and quantum steering, *Phys. Rev. A* **88**, 062108 (2013).
- [60] T. Vértesi, More efficient Bell inequalities for Werner states, *Phys. Rev. A* **78**, 032112 (2008).
- [61] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Experimental EPR-steering using Bell-local states, *Nat. Phys.* **6**, 845 (2010).
- [62] M. Navascués, S. Pironio, and A. Acín, Bounding the set of quantum correlations, *Phys. Rev. Lett.* **98**, 010401 (2007).
- [63] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, *New J. Phys.* **10**, 073013 (2008).
- [64] M. Navascués, G. de la Torre, and T. Vértesi, Characterization of quantum correlations with local dimension constraints and its device-independent applications, *Phys. Rev. X* **4**, 011011 (2014).
- [65] R. König, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, *IEEE Trans. Inf. Theory* **55**, 4337 (2009).
- [66] M. T. Quintino, T. Vértesi, and N. Brunner, Joint measurability, Einstein-Podolsky-Rosen steering, and Bell non-locality, *Phys. Rev. Lett.* **113**, 160402 (2014).
- [67] R. Uola, T. Moroder, and O. Gühne, Joint measurability of generalized measurements implies classicality, *Phys. Rev. Lett.* **113**, 160403 (2014).
- [68] R. Uola, C. Budroni, O. Gühne, and J.-P. Pellonpää, One-to-one mapping between steering and joint measurability problems, *Phys. Rev. Lett.* **115**, 230402 (2015).
- [69] O. Gühne, E. Haapasalo, T. Kraft, J.-P. Pellonpää, and R. Uola, Colloquium: Incompatible measurements in quantum information science, *Rev. Mod. Phys.* **95**, 011003 (2023).
- [70] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.132.080201> for all the proof and detailed calculations in the main text. The Supplemental Material contains additional Ref. [71].
- [71] L. P. Thinh, G. de la Torre, J.-D. Bancal, S. Pironio, and V. Scarani, Randomness in post-selected events, *New J. Phys.* **18**, 035007 (2016).

- [72] P.J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Entropic uncertainty relations and their applications, *Rev. Mod. Phys.* **89**, 015002 (2017).
- [73] One may think the distinction between  $H_{\min}^{\text{NS}}$  and  $H_{\min}^{Q_k}$  is tiny ( $\sim 10^{-3}$  in Fig. 2). This is because we certify randomness by an assemblage for some given quantum states. We also analyze the certified multipartite randomness when only a violation of steering inequality is observed via a joint probability distribution  $p^{\text{obs}}(abc|xyz)$  [70], which shows a nonignorable distinction between different lower bounds.
- [74] D. S. Tasca, P. Sánchez, S. P. Walborn, and Ł. Rudnicki, Mutual unbiasedness in coarse-grained continuous variables, *Phys. Rev. Lett.* **120**, 040403 (2018).