

Randomness Certification from Multipartite Quantum Steering for Arbitrary Dimensional Systems

Yi Li,^{1,2} Yu Xiang,^{1,3,*} Xiao-Dong, Yu,⁴ H. Chau Nguyen,⁵ Otfried Gühne,⁵ and Qiongyi He^{1,3,6,7}

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

²Beijing Academy of Quantum Information Sciences, Beijing 100193, China

³Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan, Shanxi 030006, China

⁴Department of Physics, Shandong University, Jinan 250100, China

⁵Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, 57068 Siegen, Germany

⁶Peking University Yangtze Delta Institute of Optoelectronics, Nantong 226010, Jiangsu, China

⁷Hefei National Laboratory, Hefei 230088, China

Entanglement in bipartite systems has been applied for the generation of 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 there is no randomness exists in either of them individually. We prove that the necessary and sufficient resource for quantum randomness in this scenario is multipartite quantum steering when two measurement settings are performed on the untrusted parties. 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 in comparison to the existing analysis.

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 intrinsically randomness exists among the outcomes. Therefore, some protocols for randomness generation were recently derived from this feature [7–19] and demonstrated in experiments [20–26].

Quantum steering is an intermediate type of quantum correlations between inseparability [27] and Bell nonlocality [4]. It describes the phenomenon that one party can remotely adjust the states of the other if they are entangled [28–30]. In such a scenario, the entanglement can be verified without relying on any assumed models of the steering party’s devices [31]. This leads to a one-sided device-independent approach to certify randomness [18], which is more robust to noise than the fully-device-independent protocols based on a Bell inequality violation [32–40].

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 [41, 42] has been successfully demonstrated in photonic networks [42–44], continuous-variable optical networks [45–48], and atomic ensembles [49]. The majority of theoretical studies and experiments for randomness generation, however, have focused specifically on the bipartite scenario [18–22], where a well-known theorem by Schrödinger [50–53] guarantees that any no-signalling

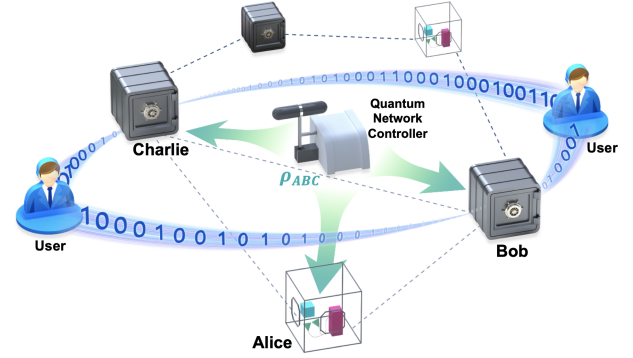


FIG. 1. Schematic view on randomness generation in a multipartite network as discussed in this paper. A controller sends a tripartite state ρ_{ABC} to three nodes. Two of these nodes (Bob and Charlie) perform measurements with the aim to use the results as a source of randomness. The measurements of 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 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.

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. This approach, however, cannot be extended to the multipartite case, since the aforementioned equivalence ceases to hold [54].

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 has been devoted to demonstrating that entanglement, steering and nonlocality are *necessary* for certifying randomness [12–20], but the *quantitative* connections are subtle [10–13]. 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 [55–60]. For the general cases, however, whether nonlocality or steering is *sufficient* for certifying randomness remains elusive.

In this paper, we present the certification of randomness in multipartite quantum systems of any dimension. As shown in Fig. 1, the scenario we consider 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). Qualitatively, from the definition of multipartite steering [42], we prove that multipartite steering with two-setting measurements on the untrusted nodes is *necessary and sufficient* for certifying randomness in the asymmetric network, independent of the number of outcomes and parties. 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 mentioned above, directly quantifying the amount of randomness cannot be equivalent to an SDP problem for the multipartite scenario. So we calculate lower bounds for the multipartite certified randomness in discrete-variable and continuous-variable systems using the Navascués-Pironio-Acín (NPA) hierarchy [61, 62], which tests for membership in the set of quantum behaviors. In order to demonstrate the tightness of the lower bounds, upper bounds are calculated by fixing the dimension of each system. We show that certain scenarios, each individual party cannot have certified randomness but, surprisingly, eavesdroppers cannot attack them simultaneously. That means, they can still collaborate to generate joint secured randomness. Finally, we adopt some existing experimental data [57] to certify randomness, which show that more randomness can be generated with our multipartite scenario than previous experiments in the bipartition scenario [26].

Randomness in multipartite quantum networks.—We focus on a tripartite scenario, in which three parties, Alice, Bob and Charlie, are located in distant laboratories and receive an unknown tripartite entangled state ρ_{ABC} from the Controller, as shown in Fig. 1. Neither Bob nor Charlie trusts their devices, which are consequently 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 $\{M_i\}_i$ that satisfies $\sum_i M_i = I$. Bob and Charlie apply measurements $M_{b|y}$ and $M_{c|z}$ labeled by $y \in \{0, \dots, m_B - 1\}$ and $z \in \{0, \dots, m_C - 1\}$, then generate outputs $b \in \{0, \dots, n_B - 1\}$ and $c \in \{0, \dots, n_C - 1\}$, respectively. 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 ρ_{ABCE} and wants to predict the outcomes b and c simultaneously, while giving the measurement choices y^* and z^* for Bob and Charlie. Since Eve knows which measurements Bob and Charlie will choose to extract randomness, she can optimize her attack to obtain information about these outcomes but still needs to be in line with the observed assemblage. Consequently, Eve gives guesses $e \in \{0, 1, \dots, n_B - 1\}$ and $e' \in \{0, 1, \dots, n_C - 1\}$ by performing a POVM measurement $\{M_{e,e'}\}_{e,e'}$. The total guessing probability that Eve’s guesses $e = b$ and $e' = c$ is given by

$$P_g(y^*, z^*) = \sum_{e,e'} P_{BCE}(b = e, c = e', e, e' | y^*, z^*). \quad (1)$$

Hence randomness, quantified by the min-entropy [63] $H_{\min} = -\log_2(P_g(y^*, z^*))$, can be certified whenever the guessing probability $P_g < 1$. This means Eve cannot be completely sure of both Bob’s and Charlie’s measurement results simultaneously.

In order to figure out the optimal strategy for Eve, we maximize her guessing probability (1) over all measurement strategies and the possible state accessible to her, which results in the following optimization problem:

$$\begin{aligned} \max \quad & P_g(y^*, z^*) = \sum_{e,e'} \text{Tr} \left[(M_{b=e|y^*} \otimes M_{c=e'|z^*} \otimes M_{e,e'}) \rho_{BCE} \right] \\ \text{w.r.t.} \quad & \rho_{ABCE}, \{M_{b|y}\}_{b,y}, \{M_{c|z}\}_{c,z}, \{M_{e,e'}\}_{e,e'} \\ \text{s.t.} \quad & \text{Tr}_{BC} \left[(I_A \otimes M_{b|y} \otimes M_{c|z}) \rho_{ABC} \right] = \sigma_{bc|yz}^{obs}, \quad \forall b, c, y, z, \\ & \rho_{ABCE} \geq 0, \quad \text{Tr}[\rho_{ABCE}] = 1, \\ & \{M_{b|y}\}_b, \{M_{c|z}\}_c, \{M_{e,e'}\}_{e,e'} \in \text{POVM}, \quad \forall y, z, \end{aligned} \quad (2)$$

where $\rho_{BCE} = \text{Tr}_A[\rho_{ABCE}]$, $\rho_{ABC} = \text{Tr}_E[\rho_{ABCE}]$ and $\{\sigma_{bc|yz}^{obs}\}_{b,c,y,z}$ is the assemblage observed by Alice. Note that the first constraint guarantees that the entire state 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 $\{\sigma_{bc|yz}^{obs}\}_{b,c,y,z}$ 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 [29, 42]. Combining this definition as well as certifiable randomness, we find that multipartite steering is *necessary* for the certification of 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: (1) Since the

assemblage $\sigma_{bc|yz}^{obs}$ 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 [29], the existence of multipartite steering is a necessary condition for generating randomness. (2) 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^* is the same as that generated by Eve's measurement $M_{e,e'}$. Thus, the state assemblage observed by Alice can be seen as generated from 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 [64, 65], and thus the assemblage is unsteerable by independent Bob and Charlie [66, 67]. 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 Appendix A. 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 [64, 65]). But it doesn't 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. [26] by considering bipartitions of the W state, in which the measurements performed by Bob and Charlie are global, i.e., $M_{(bc)|(yz)} \neq M_{b|y} \otimes M_{c|z}$. This can be considered as a special case of 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 [18]. However, in an actual tripartite scenario where the measurements performed by Bob and Charlie are local, there exist assemblages $\{\sigma_{bc|yz}^{obs}\}_{b,c,y,z}$ that satisfy the no-signaling principle but do not admit a quantum realization [54]. The technique to reduce problem (2) to an SDP thus generally fails for the multipartite scenario. In the following, we introduce a simplification of the problem (2), which subsequently allows for derivation of upper and lower bounds based on a see-saw application of SDPs and the NPA hierarchy, respectively (see Appendix B).

Firstly, since Eve only implements a single POVM, we can always use a joint classical-quantum state [68] $\rho_{ABCE} = \sum_{e,e'} |e, e'\rangle_E \langle e, e'| \otimes \sigma_{ABC}^{ee'}$ to describe the behavior of the parties without loss of generality. Here, $\sigma_{ABC}^{ee'}$ is an unnormalized quantum state conditioned on Eve's outcome e, e' . Thus, the maximization problem (2) can be simplified to maximize $\sum_{e,e'} \text{Tr}[(I_A \otimes M_{b=e|y^*} \otimes M_{c=e'|z^*}) \sigma_{ABC}^{ee'}]$ by searching for the triple $\{\sigma_{ABC}^{ee'}, M_{b|y}, M_{c|z}\}$, where the dimension of Eve's

system is not relevant anymore.

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

Finally, in order to give a more realistic range of quantum realizations, the generalized NPA hierarchy [29, 54] provides a series of tests which an assemblage must pass if it admits a quantum realization. Hence some lower bounds $H_{\min}^{Q_k}$ can be calculated by replacing the constraints from no-signaling set to the Q_k sets, where k corresponds to different NPA levels. See more details in Appendix B. We find that by optimizing $\{M_{b|y}, M_{c|z}\}$ independently, an actual multipartite scenario can bring more randomness than the bipartition scenario H_{\min}^{Glo} with optimizing global measurement $\{M_{(bc)|(yz)}\}$, although they are both multiple parties involved.

Besides, in the multipartite scenario, the amount of randomness generated on either party can also be considered individually. Now Eve only guesses the measurement outcomes on one of the untrusted parties. Therefore, the randomness solely on Bob's outcomes can be certified by changing the objective function of Eq. (2) 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 $\{\sigma_{bc|yz}^{obs}\}_{b,c,y,z}$ in a tripartite scenario, which is different from the previous bipartite case. Similarly, we can derive upper and lower bounds for the separate randomness generated only on Bob (or Charlie), more details can be found in Appendix B.

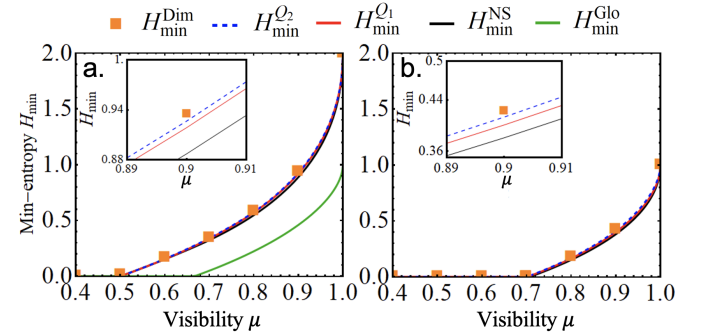


FIG. 2. Multipartite randomness certified on Bob and Charlie together (a) and the separate randomness on Bob or Charlie only (b) in GHZ states with $N = 3$, $d = 2$. Upper bounds with fixed dimensions $d_B = d_C = 10$ (orange square) are closed with the lower bounds that corresponds with different NPA levels (red solid curve for Q_1 and blue dashed line for Q_2). The lowest bound (black solid curve) is constrained by the no-signaling principle. The difference between the upper bound and the maximum lower bound is about 10^{-3} , which means the lower bounds are tight [69]. The green solid curve shows the certified randomness when Bob and Charlie's measurements are global.

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, $\rho_\mu = \mu|\Psi\rangle\langle\Psi| + \frac{1-\mu}{d^N}\mathbb{I}$, where $|\Psi\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle^{\otimes N}$ 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 assemblages $\{\sigma_{bc|yz}^{obs}\}_{b,c,y,z}$ are observed by Alice's tomography. Figure 2(a) shows upper and lower bounds for the min-entropy of the certifiable randomness on Bob and Charlie's outcomes generated by $y^* = z^* = \hat{X}$. In particular, 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}^{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 in the region of $\mu > 0.70$. Compared with Fig. 2(a), certifying randomness only in one party requires higher state visibility. In particular, when $0.50 < \mu \leq 0.69$, there exists nonzero randomness on the untrusted parties together, even though no separate randomness is induced in either parties 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 characterized while the well-characterized measurements are performed by the rest node. 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-setting measurements, the thresholds of multipartite randomness (generated on Bob and Charlie together) are consistent with the condition for showing multipartite steering. Observe that increasing the number of measurements decreases the thresholds of multipartite steering for the 3-qubit GHZ state from 0.5 (with

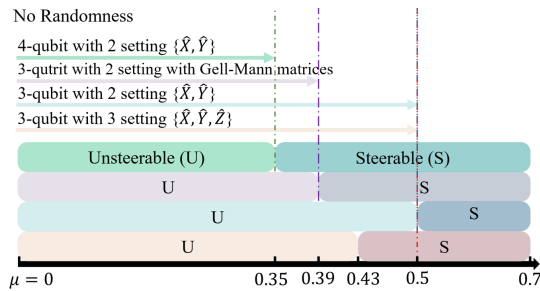


FIG. 3. The relationship of thresholds between the randomness on Bob and Charlie together and multipartite steering (from Bob and Charlie to Alice) in different GHZ states with two or three measurement settings. The left (right) blocks mean the observed assemblage is unsteerable (steerable). The arrows mean there is no randomness in their corresponding range of visibility. For the two-setting cases, the thresholds of randomness always agree with that of multipartite steering. However, for the three-setting case, the threshold of multipartite steering is decreased to 0.428 while the threshold of randomness remains unchanged.

TABLE I. Randomness certified on different parties with the experimental data in Ref. [57]. Here the optimal measurements are chosen to maximize the randomness.

Parties of Randomness	H_{\min}^{NS}	$H_{\min}^{Q_1}$	$H_{\min}^{Q_2}$	H_{\min}^{Dim}	H_{\min}^{Glo}
Bob Only	0.592	0.736	0.738	0.769	N/A
Charlie Only	0.595	0.739	0.740	0.774	N/A
Bob & Charlie	1.236	1.445	1.451	1.525	0.783

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-setting measurements.

(ii) *W-like state with experiment data*.— In Ref. [57], a class of W-like states $|\Psi_W\rangle = \alpha|001\rangle_{ABC} + \beta|010\rangle_{ABC} + \gamma|100\rangle_{ABC}$ were experimentally implemented to demonstrate the sharability of quantum steering with different measurement settings. Adopting their tomographic data for $(\alpha, \beta, \gamma) = (0.575, 0.582, 0.576)$, nearly a W state, we calculate the amount of randomness for different scenarios. The results are 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 by the method with global measurements adopted in the previous experiment [26].

(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 system with continuous variables, we can bin the homodyne measurement outputs into a finite number of outcomes like Fig. 4(b) [19, 70]. By analyzing the assemblage, we evaluate the upper and lower bounds of randomness on Bob's 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

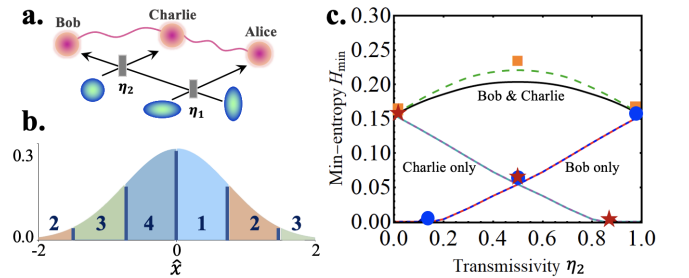


FIG. 4. Randomness certified in continuous-variable system. (a) Scheme of generating pure three-mode entangled Gaussian state by a linear optical network. (b) Bob's quadrature measurement \hat{x} is binned into 4 outcomes. (c) The lower (solid curve for H_{\min}^{NS} and dashed curve for $H_{\min}^{Q_1}$) 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.

periods $T_{\hat{x},Bob}, T_{\hat{x},Charlie} \in [2, 10]$ independently; more details in Appendix C.

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 η_2 of second beam splitter, as illustrated in Fig 4(c). However, when η_2 is in the range $[0, 0.11]$ or $[0.89, 1]$, Eve can guess the measurement outcomes of Bob or Charlie correctly with unit probability.

Conclusion.— We first present the certification of randomness generated from multiple untrusted parties in an asymmetric network and discussed the relation between multipartite steering and verifiable randomness. When the untrusted parties perform two-setting measurements locally, we proved that multipartite steering is necessary and sufficient for generating randomness in such an asymmetric network by connecting the randomness with incompatible measurements. Increasing the measurement setting contributes to demonstrating steering but does not necessarily certifies randomness in a larger parameter range, which helps us to determine the minimal resource in quantum cryptography. Furthermore, 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 quantum network.

So far, multipartite steering has been demonstrated in various platforms [42–49], which lays a favorable foundation for generating multipartite randomness. Our results make a significant advance in an in-depth understanding of quantum randomness as a fundamental resource and provide an important framework for the multipartite quantum 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, No. 12004011, and No. 12147148), Beijing Natural Science Foundation (Grant No. Z190005), the Key R&D Program of Guangdong Province (Grant No. 2018B030329001), 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, project numbers 447948357 and 440958198), the Sino-German Center for Research Promotion (Project M-0294), the ERC (Consolidator Grant 683107/TempoQ), the German Ministry of Education and Research (Project QuKuK, BMBF Grant No. 16KIS1618K).

APPENDIX A: RELATION BETWEEN STEERING AND RANDOMNESS

In this section, we prove that multipartite steering is *necessary* for the certification of multipartite randomness on the untrusted parties. Specifically, in the case of $m_B = m_C = 2$, multipartite steering is *necessary and sufficient* for certifying randomness. This perfect equivalence, however, ceases to hold with more measurement settings. This argument is generally valid for multipartite as well as bipartite scenarios. Here, we first give a proof in the bipartite scenario.

1. Bipartite scenario

In the bipartite scenario, Alice and Bob receive a bipartite state ρ_{AB} from Controller while they are located in distant laboratories. The measurement device on Bob is untrusted. He can choose which measurement $y \in \{0, \dots, m_B - 1\}$ to perform, each of which gives an outcome $b \in \{0, \dots, n_B - 1\}$. On the other side, Alice has complete knowledge of her device, which allows her to reconstruct every conditional state $\sigma_{b|y}^{obs} = \text{Tr}_B[I_A \otimes M_{b|y} \rho_{AB}]$ (unnormalized) she received.

For the observed assemblage, we can detect steering by solving the following SDP problem [29]:

$$\begin{aligned} & \text{find } \{\sigma_\lambda\}_\lambda \\ & \text{s.t. } \sigma_{b|y}^{obs} = \sum_\lambda D_{Local}(b|y, \lambda) \sigma_\lambda, \quad \forall b, y, \\ & \sigma_\lambda \geq 0, \quad \forall \lambda. \end{aligned} \tag{A1}$$

We can also quantify the amount of randomness on Bob's outputs by solving the SDP problem [18]:

$$\begin{aligned} P_g(y^*) &= \max_{\{\sigma_{b|y}^e\}_{e,b,y}} \text{Tr} \sum_e \sigma_{b=e|y^*}^e \\ & \text{s.t. } \sum_e \sigma_{b|y}^e = \sigma_{b|y}^{obs}, \quad \forall b, y, \end{aligned} \tag{A2}$$

$$\sum_b \sigma_{b|y}^e = \sum_b \sigma_{b|y'}^e, \quad \forall e, y, y',$$

$$\sigma_{b|y}^e \geq 0, \quad \forall b, y, e.$$

Next, we will show that if problem Eq. (A1) is feasible, then problem Eq. (A2) gives $P_g(y^*) = 1$ for any measurement settings m_A . Specifically, in the case of $m_A = 2$, problem Eq. (A1) must be feasible if problem Eq. (A2) gives $P_g(y^*) = 1$.

Steering is necessary for randomness. - If the problem Eq. (A1) is feasible, we have

$$\sigma_{b|y}^{obs} = \sum_{\lambda} D_{Local}(b|y, \lambda) \sigma_{\lambda} = \sum_{i=0}^{n_B-1} \sum_{\lambda \in \lambda^{(i)}} D_{Local}(b|y, \lambda) \sigma_{\lambda}, \quad \forall b, y, \quad (A3)$$

where the deterministic probability distribution is $D_{Local}(b|y, \lambda) = \delta_{b, \lambda_{(y)}}$ and $\lambda = (b_0, b_1, \dots, b_{m_B-1})$. We can divide all the extremal points of the local set into n_B classes: $\lambda^{(i)} := \{\lambda | \lambda_{(y^*)} = i\}$ with $i = 0, 1, \dots, n_B - 1$, and construct an ensemble $\sigma_{b|y}^e = \sum_{\lambda \in \lambda^{(e)}} D_{Local}(b|y, \lambda) \sigma_{\lambda}$, $\forall b, e, y$. Then, we can easily check that such an ensemble gives $P_g(y^*) = 1$ in Problem Eq. (A2):

$$P_g(y^*) = \text{Tr} \sum_e \sigma_{e|y^*}^e = \sum_{\lambda} p(\lambda) = 1,$$

$$\sum_e \sigma_{b|y}^e = \sum_{\lambda} D_{Local}(b|y, \lambda) \sigma_{\lambda} = \sigma_{b|y}^{obs}, \quad \forall b, y, \quad (A4)$$

$$\sum_b \sigma_{b|y}^e = \sum_{\lambda \in \lambda^{(e)}} \sigma_{\lambda} = \sum_b \sigma_{b|y'}^e, \quad \forall e, y, y'.$$

Hence, the fact that no randomness on Bob's outputs if the assemblage measured by Alice is unsteerable for any measurement settings m_B is proved.

Steering is sufficient for randomness. - In the case of $m_B = 2$, we set that $y \in \{y^*, \bar{y}^*\}$. If problem Eq. (A2) gives

$$P_g(y^*) = \text{Tr} \sum_e \sigma_{e|y^*}^e = \sum_e p(e, e|y^*) = \sum_e p(e|y^*, e) p(e) = 1, \quad (A5)$$

where $p(e, e|y) = p(e|y, e) p(e|y) = p(e|y, e) p(e)$ due to the no-signaling condition between Eve and Bob. Then we have $p(b|y^*, e) = \delta_{b,e}$, $\forall e, b$ without loss of generality, which means $\sigma_{b|y^*}^e = p(e) p(b|y^*, e) \rho_{b|y^*}^e = \delta_{b,e} \sigma_{b|y^*}^e$, $\forall e, b$. Further, since the optimal solution always satisfies with the observed assemblage and also the no-signaling condition, then

$$\sigma_{b|y^*}^{obs} = \sum_e \sigma_{b|y^*}^e = \sum_l \sigma_{l|\bar{y}^*}^b = \sum_q \sigma_{\lambda_{(y^*, \bar{y}^*)}=(b,q)} = \sum_{\lambda} D_{Local}(b|y^*, \lambda) \sigma_{\lambda}, \quad \forall b, \quad (A6)$$

$$\sigma_{b|\bar{y}^*}^{obs} = \sum_e \sigma_{b|\bar{y}^*}^e = \sum_q \sigma_{\lambda_{(y^*, \bar{y}^*)}=(q,b)} = \sum_{\lambda} D_{Local}(b|\bar{y}^*, \lambda) \sigma_{\lambda}, \quad \forall b.$$

where $\sigma_{\lambda_{(y^*, \bar{y}^*)}=(b,q)} = \sigma_{q|\bar{y}^*}^b \geq 0$. Therefore, in the two-setting measurement case, if there is no randomness on Bob's outputs, then $\{\sigma_{b|y}^{obs}\}_{b,y}$ is unsteerable.

In fact, $P_g(y^*) = 1$ gives $\sigma_{b|y^*}^e = \text{Tr}_{EB}[M_e \otimes I_A \otimes M_{b|y^*} \rho_{EAB}] = \delta_{e,b} \text{Tr}_{EB}[M_e \otimes I_A \otimes M_{b|y^*} \rho_{EAB}]$, $\forall b, e$. Then

$$\sum_l \text{Tr}_{EB}[M_b \otimes I_A \otimes M_{l|y^*} \rho_{EAB}] = \sum_l \text{Tr}_{EB}[M_l \otimes I_B \otimes M_{b|y^*} \rho_{EAB}] = \sigma_{b|y^*}^{obs} = \sigma_{b|y^*}^b, \quad \forall b, \quad (A7)$$

which means the measurement y^* on Bob can be regarded as a measurement performed on Eve: $\sigma_{b|y^*}^{obs} = \text{Tr}_{EB}[M_b \otimes I_A \otimes I_B \rho_{EAB}] = \text{Tr}_{EB}[I_E \otimes I_A \otimes M_{b|y^*} \rho_{EAB}]$. For the other measurement \bar{y}^* , $\sigma_{b|\bar{y}^*}^{obs} = \text{Tr}_{EB}[I_E \otimes I_A \otimes M_{b|\bar{y}^*} \rho_{EAB}]$. Therefore, the assemblage must be unsteerable since measurements $\{M_e \otimes I_B\}_e$ and $\{I_E \otimes M_{b|\bar{y}^*}\}_b$ are compatible [64–66]. However, in the case of $m_B \geq 3$, the additional measurements $\{M_{b|\bar{y}^*}\}_b$ could be incompatible with measurement \bar{y}^* and hence express steerability, but do not involve in generating the randomness, i.e. Eve still gives $P_g(y^*) = 1$.

2. Tripartite scenario

Now we generalize the above proofs to the tripartite scenario, we will show if the assemblage has no multipartite steering, problem Eq. (2) in the main text would give $P_g(y^*, z^*) = 1$. Also the opposite direction is true when $m_B = m_C = 2$.

Steering is necessary for randomness.- Similarly, for the observed assemblage, we can also detect multipartite steering by solving this SDP problem [42]:

$$\begin{aligned} \text{find} \quad & \{\sigma_{\mu\nu}\}_{\mu\nu} \\ \text{s.t.} \quad & \sum_{\mu,\lambda} D(b|y,\mu)D(c|z,\nu)\sigma_{\mu\nu} = \sigma_{bc|yz}^{obs}, \quad \forall b, c, y, z, \\ & \sigma_{\mu\nu} \geq 0, \quad \forall \mu, \nu, \end{aligned} \quad (\text{A8})$$

If problem Eq. (A8) is feasible, we have

$$\sigma_{bc|yz}^{obs} = \sum_{\lambda} D_{Local}(bc|yz, \lambda)\sigma_{\lambda} = \sum_{e,e'} \sum_{\lambda \in \lambda(e,e')} D_{Local}(bc|yz, \lambda)\sigma_{\lambda}, \quad \forall b, c, y, z. \quad (\text{A9})$$

Here the deterministic probability distribution is

$$D_{Local}(bc|yz, \lambda) = \begin{cases} 1, & \text{if } b = b_y \text{ and } c = c_z, \\ 0, & \text{otherwise,} \end{cases} \quad (\text{A10})$$

where $\lambda = (b_0, b_1, \dots, b_{m_B-1}; c_0, c_1, \dots, c_{m_C-1})$ and $\lambda^{(e,e')} := \{\lambda | \lambda_{(y^*, z^*)} = (e; e')\}$, $\forall e, e'$. Similarly, we construct an ensemble $\sigma_{bc|yz}^{ee'} = \sum_{\lambda \in \lambda^{(e,e')}} D_{Local}(bc|yz, \lambda)\sigma_{\lambda}$. It can be easily checked that such an ensemble gives $P_g(y^*, z^*) = 1$ in the problem Eq. (2) with simplification (Eq. (B1)) in the main text:

$$\begin{aligned} P_g(y^*, z^*) &= \text{Tr} \sum_{e,e'} \sigma_{ee'|y^*z^*}^{ee'} = \sum_{e,e'} \sum_{\lambda \in \lambda^{(e,e')}} D_{Local}(ee'|y^*z^*, \lambda)p(\lambda) = \sum_{\lambda} p(\lambda) = 1, \\ \sum_{e,e'} \sigma_{bc|yz}^{ee'} &= \sum_{e,e'} \sum_{\lambda \in \lambda^{(e,e')}} D_{Local}(bc|yz, \lambda)\sigma_{\lambda} = \sum_{\lambda} D_{Local}(bc|yz, \lambda)\sigma_{\lambda} = \sigma_{bc|yz}^{obs}, \quad \forall b, c, y, z, \\ \sigma_{bc|yz}^{ee'} &= \sum_{\lambda \in \lambda^{(e,e')}} D_{Local}(bc|yz, \lambda)\sigma_{\lambda} = \text{Tr}_{BC}[I_A \otimes M_{b|y} \otimes M_{c|z} \sigma_{ABC}^{ee'}], \quad \forall b, c, y, z, e, e', \end{aligned} \quad (\text{A11})$$

where

$$\begin{aligned} M_{b|y} &= I_0 \otimes \dots \otimes |b\rangle_y \langle b| \otimes \dots \otimes I_{m_B-1}, \quad \sum_b |b\rangle \langle b| = I, \\ M_{c|z} &= I_0 \otimes \dots \otimes |c\rangle_z \langle c| \otimes \dots \otimes I_{m_C-1}, \quad \sum_c |c\rangle \langle c| = I, \\ \sigma_{ABC}^{ee'} &= \sum_{\lambda \in \lambda^{(e,e')}} \rho_{BC}^{\lambda} \otimes \sigma_{\lambda}, \\ \rho_{BC}^{\lambda=(b_0, \dots, b_{m_B-1}; c_0, \dots, c_{m_C-1})} &= |b_0\rangle_{B_0} \langle b_0| \otimes \dots \otimes |b_{m_B-1}\rangle_{B_{m_B-1}} \langle b_{m_B-1}| \otimes |c_0\rangle_{C_0} \langle c_0| \otimes \dots \otimes |c_{m_C-1}\rangle_{C_{m_C-1}} \langle c_{m_C-1}|. \end{aligned} \quad (\text{A12})$$

Therefore, multipartite steering is necessary for certifying randomness on Bob and Charlie.

Steering is sufficient for randomness.- In the case of $m_B = m_C = 2$, Bob measures $y \in \{y^*, \bar{y}^*\}$ and Charlie measures $z \in \{z^*, \bar{z}^*\}$, respectively. If problem Eq. (A2) gives

$$P_g(y^*, z^*) = \text{Tr} \sum_{e,e'} \sigma_{ee'|y^*z^*}^{ee'} = \sum_{e,e'} p(ee', ee'|y^*z^*) = \sum_{e,e'} p(ee'|y^*z^*, ee')p(ee') = 1, \quad (\text{A13})$$

where $p(ee', ee'|yz) = p(ee'|yz, ee')p(ee'|yz) = p(ee'|yz, ee')p(ee')$ due to no-signaling condition, we have $p(bc|y^*z^*, ee') = \delta_{b,e}\delta_{c,e'}$, $\forall e, e', b, c$. Then, $p(bc|\bar{y}^*z^*, ee') = \delta_{c,e'}p(bc|y^*z^*, ee')$ and $p(bc|y^*z^*, ee') = \delta_{b,e}p(bc|\bar{y}^*z^*, ee')$ can also be derived due to the no-signaling condition. Since the optimal solution satisfies with the observed assemblage and also the no-signaling condition, then

$$\begin{aligned} \sigma_{bc|y^*z^*}^{obs} &= \sum_{e,e'} \sigma_{bc|y^*z^*}^{ee'} = \sigma_{bc|y^*z^*}^{bc} = \sum_{k,l} \sigma_{kl|\bar{y}^*z^*}^{bc}, \quad \forall b, c, \\ \sigma_{bc|\bar{y}^*z^*}^{obs} &= \sum_{e,e'} \sigma_{bc|\bar{y}^*z^*}^{ee'} = \sum_e \sigma_{bc|\bar{y}^*z^*}^{ec} = \sum_{k,l} \sigma_{bl|\bar{y}^*z^*}^{kc}, \quad \forall b, c, \end{aligned} \quad (\text{A14})$$

$$\begin{aligned}\sigma_{bc|y^*z^*}^{obs} &= \sum_{e,e'} \sigma_{bc|y^*z^*}^{ee'} = \sum_{e'} \sigma_{bc|y^*z^*}^{be'} = \sum_{k,l} \sigma_{kc|\bar{y}^*z^*}^{bl}, \quad \forall b, c, \\ \sigma_{bc|\bar{y}^*z^*}^{obs} &= \sum_{e,e'} \sigma_{bc|\bar{y}^*z^*}^{ee'} = \sum_{k,l} \sigma_{bc|\bar{y}^*z^*}^{kl}, \quad \forall b, c,\end{aligned}$$

where $\sigma_{b\bar{y}^*, c\bar{z}^*|\bar{y}^*z^*}^{b\bar{y}^* c\bar{z}^*} = \sigma_{\lambda=(b\bar{y}^*, b\bar{y}^*; c\bar{z}^*, c\bar{z}^*)}$, i.e. the observed assemblage can be decomposed as $\sigma_{bc|yz}^{obs} = \sum_{\lambda} D_{Local}(bc|yz, \lambda) \sigma_{\lambda}$. Therefore, in the case of $m_B = 2$ and $m_C = 2$, if there is no randomness can be certified on Bob's and Charlie's outputs, then $\{\sigma_{bc|yz}^{obs}\}_{b,c,y,z}$ is unsteerable.

The ensemble we concerned is $\sigma_{BCA}^{ee'} = \text{Tr}_E[M_{e,e'} \otimes I_B \otimes I_C \otimes I_{A\rho_{E_1E_2BCA}}]$, which can also be obtained by another global state $\rho'_{EBCA} = \sum_{e,e'} |e\rangle_{E_1} \langle e| \otimes |e'\rangle_{E_2} \langle e'| \otimes \sigma_{BCA}^{ee'}$ as well as Eve's measurement $\{|e\rangle_{E_1} \langle e| \otimes |e'\rangle_{E_2} \langle e'|\}_{e,e'}$. Therefore, we can regard Eve as two local parts (E_1 and E_2) without loss of generality, then $P_g(y^*, z^*) = 1$ gives

$$\text{Tr}[M_e^1 \otimes M_{e'}^2 \otimes M_{b|y} \otimes M_{c|z} \otimes I_{A\rho_{E_1E_2BCA}}] = \begin{cases} \delta_{e,b} \delta_{e',c} p(b, c, e, e'|y, z), & \text{for } y = y^* \text{ and } z = z^*, \\ \delta_{e,b} p(b, c, e, e'|y, z), & \text{for } y = y^* \text{ and } z = \bar{z}^*, \\ \delta_{e',c} p(b, c, e, e'|y, z), & \text{for } y = \bar{y}^* \text{ and } z = z^*, \\ p(b, c, e, e'|y, z), & \text{otherwise,} \end{cases} \quad \forall e, e', b, c, \quad (\text{A15})$$

which means

$$\begin{aligned}\sum_{k,l} \text{Tr}_{E_1E_2BC}[M_b^1 \otimes M_c^2 \otimes M_{k|y^*} \otimes M_{l|z^*} \otimes I_{A\rho_{E_1E_2BCA}}] &= \sum_{k,l} \text{Tr}_{E_1E_2BC}[M_k^1 \otimes M_l^2 \otimes M_{b|y^*} \otimes M_{c|z^*} \otimes I_{A\rho_{E_1E_2BCA}}], \quad \forall b, c, \\ \sum_k \text{Tr}_{E_1E_2BC}[M_b^1 \otimes M_{e'}^2 \otimes M_{k|y^*} \otimes M_{c|\bar{z}^*} \otimes I_{A\rho_{E_1E_2BCA}}] &= \sum_k \text{Tr}_{E_1E_2BC}[M_k^1 \otimes M_{e'}^2 \otimes M_{b|y^*} \otimes M_{c|\bar{z}^*} \otimes I_{A\rho_{E_1E_2BCA}}], \quad \forall b, c, e', \\ \sum_l \text{Tr}_{E_1E_2BC}[M_e^1 \otimes M_c^2 \otimes M_{b|\bar{y}^*} \otimes M_{l|z^*} \otimes I_{A\rho_{E_1E_2BCA}}] &= \sum_l \text{Tr}_{E_1E_2BC}[M_e^1 \otimes M_l^2 \otimes M_{b|\bar{y}^*} \otimes M_{c|z^*} \otimes I_{A\rho_{E_1E_2BCA}}], \quad \forall b, c, e.\end{aligned} \quad (\text{A16})$$

Then, the observed assemblage can be written as

$$\begin{aligned}\sigma_{bc|y^*z^*}^{obs} &= \text{Tr}_{E_1E_2BC}[M_b^1 \otimes M_c^2 \otimes I_B \otimes I_C \otimes I_{A\rho_{E_1E_2BCA}}], \quad \forall b, c, \\ \sigma_{bc|y^*\bar{z}^*}^{obs} &= \text{Tr}_{E_1E_2BC}[M_b^1 \otimes I_{E_2} \otimes I_B \otimes M_{c|\bar{z}^*} \otimes I_{A\rho_{E_1E_2BCA}}], \quad \forall b, c, \\ \sigma_{bc|\bar{y}^*z^*}^{obs} &= \text{Tr}_{E_1E_2BC}[I_{E_1} \otimes M_c^2 \otimes M_{b|\bar{y}^*} \otimes I_C \otimes I_{A\rho_{E_1E_2BCA}}], \quad \forall b, c, \\ \sigma_{bc|\bar{y}^*\bar{z}^*}^{obs} &= \text{Tr}_{E_1E_2BC}[I_{E_1} \otimes I_{E_2} \otimes M_{b|\bar{y}^*} \otimes M_{c|\bar{z}^*} \otimes I_{A\rho_{E_1E_2BCA}}], \quad \forall b, c.\end{aligned} \quad (\text{A17})$$

Since the measurements $\{M_b^1 \otimes I_B\}_b$ and $\{I_{E_1} \otimes M_{b|\bar{y}^*}\}_b$ must be compatible, and so as $\{M_c^2 \otimes I_C\}_c$ and $\{I_{E_2} \otimes M_{c|\bar{z}^*}\}_c$. Hence, the observed assemblage is unsteerable in a multipartite scenario. However, in the case of $m_B \geq 3$ or $m_C \geq 3$, the additional measurements could express steerability with measurements other than y^* or z^* but do not be involved in generating the randomness.

APPENDIX B: QUANTIFICATION OF CERTIFIED RANDOMNESS IN MULTIPARTITE SCENARIO

First of all, we simplify the problem Eq. (2) in the main text to the following problem based on the classical-quantum state.

$$\begin{aligned}\max_{e,e'} \quad & \sum \text{Tr}[(I_A \otimes M_{b=e|y^*} \otimes M_{c=e'|z^*}) \sigma_{ABC}^{ee'}] \\ \text{w.r.t.} \quad & \{\sigma_{ABC}^{ee'}\}_{e,e'}, \{M_{b|y}\}_{b,y}, \{M_{c|z}\}_{c,z} \\ \text{s.t.} \quad & \sum_{e,e'} \text{Tr}_{BC}[(I_A \otimes M_{b|y} \otimes M_{c|z}) \sigma_{ABC}^{ee'}] = \sigma_{bc|yz}^{obs}, \quad \forall b, c, y, z, \\ & \sigma_{ABC}^{ee'} \geq 0, \quad \forall e, e', \quad \sum_{e,e'} \text{Tr}[\sigma_{ABC}^{ee'}] = 1, \\ & \{M_{b|y}\}_b, \{M_{c|z}\}_c \in \text{POVM}, \quad \forall y, z.\end{aligned} \quad (\text{B1})$$

Here we don't have to fix the dimension of Eve during the calculations of the upper bound of randomness.

1. Randomness certified on Bob and Charlie together

Lower Bounds.— A lower bound H_{\min}^{NS} can be calculated with the no-signaling constraint:

$$\begin{aligned}
 & \max_{\{\sigma_{bc|yz}^{ee'}\}_{e,e',b,c,y,z}} \text{Tr} \left[\sum_{e,e'} \sigma_{bc|yz}^{ee'} \right] \\
 \text{s. t. } & \sum_{e,e'} \sigma_{bc|yz}^{ee'} = \sigma_{bc|yz}^{obs}, \quad \forall b, c, y, z, \\
 & \sigma_{bc|yz}^{ee'} \geq 0, \quad \forall e, e', b, c, y, z, \\
 & \sum_b \sigma_{bc|yz}^{ee'} = \sum_b \sigma_{bc|y'z}^{ee'}, \quad \forall e, e', c, z, y, y', \\
 & \sum_c \sigma_{bc|yz}^{ee'} = \sum_c \sigma_{bc|yz'}^{ee'}, \quad \forall e, e', b, y, z, z'.
 \end{aligned} \tag{B2}$$

For each e, e' , when the optimal solution $\sigma_{bc|yz}^{ee'}$ can be written as

$$\sigma_{bc|yz}^{ee'} = \text{Tr}_{BCE} \left[I_A \otimes M_{b|y} \otimes M_{c|z} \otimes M_{ee'} \rho_{ABCE} \right], \quad \forall e, e', \tag{B3}$$

the optimal P_g solved in Eq. (B2) is equivalent to that in Eq. (2) in the main text. Unfortunately, in the tripartite scenario, the constraint with no-signaling principle do not equivalent to the quantum realization constraint. With the NPA hierarchy [61, 62], we can obtain a series of tighter lower bounds $H_{\min}^{Q_k}$ by considering the constraint $\{\sigma_{bc|yz}^{ee'}\}_{b,c,y,z} \in Q_k$ for each e, e' and a positive integer k .

Upper Bound (see-saw Algorithm).— The upper bound of the min-entropy can be calculated by fixing the dimension of each subsystem. Here we use d_A, d_B, d_C to denote the dimensions of Alice, Bob and Charlie, respectively. However, even by fixing the dimensions, the problem Eq. (B1) is neither an SDP problem nor a linear problem. Here we use the see-saw algorithm to convert this problem into three SDPs.

Firstly, we set the POVMs $\{M_{b|y}\}_{b,y}$ and ensemble $\{\sigma_{ABC}^{ee'}\}_{ee'}$ by random. In order to get matrices $M_{b|y}^{(0)} \geq 0$, we take $n_B m_B d_B^2$ real numbers between -1 and 1 from uniform distribution to write $n_B m_B$ tridiagonal matrices $\{T_{b|y}\}_{b,y}$. Then, we have $n_B m_B$ random hermitian and positive semi-definite matrices $\{M_{b|y}^{(0)} = T_{b|y}^\dagger T_{b|y} / \text{Tr}[T_{b|y}^\dagger T_{b|y}]\}_{b,y}$. We note that the set of matrices may not be satisfy with $\sum_b M_{b|y}^{(0)} = I$. But in the following steps, we set this condition as a constraint in SDP, then the feasible set is still constrained by POVM condition, i.e., the final optimal solution $\{M_{b|y}\}_{b,y}$ are POVMs. For the set of matrices $\{\sigma_{ABC}^{ee'(0)}\}_{e,e'}$, we take $2n_B n_C d_A d_B d_C$ real numbers between -1 and 1 from uniform distribution to generate the amplitude terms as well as phase terms of $n_B n_C$ pure states $\{\rho_{ABC}^{ee'(0)}\}_{e,e'}$. We also take $n_B n_C$ positive numbers between 0 and 1 from uniform distribution to generate probability $p(e, e')$ with normalization $\sum_{e,e'=0}^{n_B n_C - 1} p(e, e') = 1$. Hence, the random state $\sigma_{ABC}^{ee'(0)} = p(e, e') \rho_{ABC}^{ee'(0)}$ is obtained. After giving the initial POVMs $\{M_{b|y}^{(0)}\}_{b,y}$ and ensemble $\{\sigma_{ABC}^{ee'(0)}\}_{e,e'}$, we can solve the following SDP:

$$\begin{aligned}
 & \max_{\substack{\{M_{c|z}\}_{c,z} \\ \{\lambda_{bc|yz}\}_{b,c,y,z}}} \sum_{e,e'} \text{Tr} \left[\left(M_{b=e|y^*}^{(0)} \otimes M_{c=e'|z^*} \right) \sigma_{BC}^{ee'(0)} \right] - \mu \sum_{b,c,y,z} \lambda_{bc|yz} \\
 \text{s. t. } & -\lambda_{bc|yz} I \leq \sum_{e,e'} \text{Tr}_{BC} \left[I_A \otimes \left(M_{b|y}^{(0)} \otimes M_{c|z} \right) \sigma_{ABC}^{ee'(0)} \right] - \sigma_{bc|yz}^{obs} \leq \lambda_{bc|yz} I, \quad \forall b, c, y, z. \\
 & \{M_{c|z}\}_c \in \text{POVM}, \quad \forall z, \quad \lambda_{bc|yz} \geq 0, \quad \forall b, c, y, z,
 \end{aligned} \tag{B4}$$

where $\sigma_{BC}^{ee'(0)} = \text{Tr}_A[\sigma_{ABC}^{ee'(0)}]$. In this step, an optimal solution $\{M_{c|z}^{(1)}\}_{c,z}$ can be found easily. Here we use a penalty to change the first equality constraint in Eq. (B1) to an inequality constraint, where μ is about $1e2 \sim 1e3$. This is because the first constraint in Eq. (B1) could not be satisfied easily when the POVMs $\{M_{b|y}^{(0)}\}_{b,y}$ and states $\{\sigma_{ABC}^{ee'(0)}\}_{ee'}$ are set by random. Then Eq. (B4) will probably be infeasible without penalty.

In the second step, we fix the optimal solution $\{M_{c|z}^{(1)}\}_{c,z}$ and also the initial states $\{\sigma_{ABC}^{ee'(0)}\}_{e,e'}$. Then we can also find an optimal solution $\{M_{b|y}^{(1)}\}_{b,y}$ by changing the variables in Eq. (B4). Now the optimal solution $\{M_{b|y}^{(1)}\}_{b,y}$ is already a POVM and can be easily found in this step.

In the third step, we fix POVMs $\{M_{b|y}^{(1)}\}_{b,y}$ and $\{M_{c|z}^{(1)}\}_{c,z}$ to find an optimal set of states $\{\sigma_{ABC}^{ee'(0)}\}_{e,e'}$ that maximize Eq. (B4). Note that the third step will take much time than the first two steps, so we iterate the first two steps until the guessing probability reaches its convergency.

We iterate these steps until $\max\{\lambda_{bc|yz}\}$ decreases to about $1e-9$ and the optimal guessing probability reaches its convergency, hence an upper bound H_{\min}^{Dim} can be calculated. Furthermore, when we find that the guessing probability changes with a very slow rate, adding some random POVMs and states (with tiny weight) is helpful for finding a larger P_g . We note that the solution we found by see-saw algorithm may not be a global optimal solution, which means the optimal P_g we got is less than the global solution. So the solution in this part is still an upper bound of actual randomness.

2. Randomness certified on Bob or Charlie solely

In a multipartite scenario, we can also consider that Eve only guess the measurement results of Bob or Charlie solely. Here we give a definition of the randomness generated from only Bob, and it is the same with Charlie. In this case, the guessing probability P_g^B is given by

$$\begin{aligned} & \max_{\substack{\{\sigma_{ABC}^e\}_e \\ \{M_{b|y}\}_{b,y} \\ \{M_{c|z}\}_{c,z}}} \sum_e \text{Tr} [M_{b=e|y^*} \sigma_B^e] \\ \text{s. t. } & \sum_e \text{Tr}_{BC} [(I_A \otimes M_{b|y} \otimes M_{c|z}) \sigma_{ABC}^e] = \sigma_{bc|yz}^{obs}, \quad \forall b, c, y, z, \\ & \sigma_{ABC}^e \geq 0, \quad \forall e, \quad \sum_e \text{Tr} [\sigma_{ABC}^e] = 1, \\ & \{M_{b|y}\}_{b,y}, \{M_{c|z}\}_{c,z} \in \text{POVM}, \end{aligned} \quad (\text{B5})$$

where $\sigma_B^e = \text{Tr}_{AC}[\sigma_{ABC}^e]$. The main difference between Eq. (B5) and Eq. B1 is just the objective function, which means we certify the randomness on Bob still in a real tripartite scenario, which is different from the previous bipartite scenario. So we still can not solve the above optimization problem directly.

For the lower bounds of Eq. (B5), it can also be calculated by utilizing the no-signaling principle:

$$\begin{aligned} & \max_{\{\sigma_{bc|yz}^e\}_{e,b,c,y,z}} \text{Tr} \left[\sum_{e,c} \sigma_{b=e,c|y^*0}^e \right] \\ \text{s. t. } & \sum_e \sigma_{bc|yz}^e = \sigma_{bc|yz}^{obs}, \quad \forall b, c, y, z, \\ & \sigma_{bc|yz}^e \geq 0, \quad \forall e, b, c, y, z, \\ & \sum_b \sigma_{bc|yz}^e = \sum_b \sigma_{bc|y'z}^e, \quad \forall e, c, z, y, y', \\ & \sum_c \sigma_{bc|yz}^e = \sum_c \sigma_{bc|yz'}^e, \quad \forall e, b, y, z, z'. \end{aligned} \quad (\text{B6})$$

Also some tighter lower bounds can be found by adding NPA hierarchy constraints $\{\sigma_{bc|yz}^e\}_{b,c,y,z} \in Q_k, \forall e$.

For the upper bound, we can also use see-saw algorithm to calculate the upper bound H_{\min}^{Dim} in this scenario when we fix the dimension of each subsystems. The steps are same with the method presented in section .

APPENDIX C: EXAMPLE OF CONTINUOUS-VARIABLE CASE

Here we give an example to certify randomness in the continuous-variable system. The pure state $|\Psi\rangle_{CV}$ generated from the setup shown in Fig. 4(a) in the main text is

$$\hat{U}_{T_2}^{BC} \hat{U}_{\eta_1}^{AB} \hat{S}(\xi_A) \hat{S}(\xi_B) |0_A\rangle |0_B\rangle |0_C\rangle = \sum_{p=0}^{\infty} \sum_{k_1=0}^p \sum_{k_2=0}^{k_1} \sum_{k_3=0}^{p-(2k_2-k_1)} \frac{(\tanh r)^p}{2^p \cosh r} \left(4 \sqrt{\eta_1 (1-\eta_1)} \right)^{p-k_1} (2\eta_1 - 1)^{k_1} (-1)^{p-(3k_2+k_3)} \quad (\text{C1})$$

$$\frac{\sqrt{(p + (2k_2 - k_1))! (p - (2k_2 - k_1))!}}{(p - k_1)! (k_1 - k_2)! k_2!} \sqrt{C_{p-(2k_2-k_1)}^{k_3} \frac{\eta_2^{k_3}}{(1 - \eta_2)^{k_3 - (p - (2k_2 - k_1))}}} |p + (2k_2 - k_1)\rangle_A |k_3\rangle_B |p - (2k_2 - k_1 + k_3)\rangle_C$$

where $\hat{S}(\xi) = e^{\frac{1}{2}(\xi^* \hat{a}^2 - \xi (\hat{a}^\dagger)^2)}$ is the squeezed operator and $\xi = r e^{i\theta}$.

In order to generate the assemblage measured by Alice, we bin the homodyne measurement results on Bob and Charlie by the coarse-graining scheme [19, 70]. For example, the measurements on Bob can be written as:

$$M_{b|y} = \int_{\mathbb{R}} f_b(z, T_y) |z\rangle_y \langle z| dz, \quad (C2)$$

where $y = \hat{x}, \hat{p}$ is the input, T_y is the period, and $f_b(z, T_y)$ is a function:

$$f_b(z, T_y) = \begin{cases} 1, & bs_y \leq z \bmod T_y < (b+1)s_y \\ 0, & \text{otherwise} \end{cases} \quad (C3)$$

where $s_y = T_y/n_B$ is the width of the bins and n_B is the number of outcomes, i.e. $b \in \{0, 1, \dots, n_B - 1\}$. Here we set $T_{\hat{p}} = 2\pi n_B / T_{\hat{x}}$ to ensure mutual unbiasedness. So based on such POVMs, the assemblage measured by Alice is $\sigma_{bc|yz}^{obs} = \text{Tr}_{BC}[I_A \otimes M_{b|y} \otimes M_{c|z} |\Psi\rangle_{CV} \langle \Psi|]$.

In Fig. 4 in the main text, we set $r = 3\text{dB}$ and fix the transmissivity of the first beam splitter, to $\eta_1 = 1/2$. The state $|\Psi\rangle_{CV}$ changes with the second beam splitter transmissivity η_2 . Then by analyzing the assemblage on Alice, we can calculate an upper bound and some lower bounds of H_{\min} on Bob's and Charlie's measurement results ($y^* = z^* = \hat{x}$). Here we cut off the Fock basis to one photon which is enough in our case, although higher "cut off basis" would give higher H_{\min}^{NS} . Note that H_{\min}^{NS} is maximised over binning periods in the range $T_{\hat{x}}(\text{Bob}) \in [2, 10]$ for Bob and $T_{\hat{x}}(\text{Charlie}) \in [2, 10]$ for Charlie independently. Then $H_{\min}^{Q_1}$ is calculated in these optimized periods $T_{\hat{x}}(\text{Bob})$ and $T_{\hat{x}}(\text{Charlie})$. Moreover, we also give the randomness on only Bob or only Charlie based on the same steps.

APPENDIX D: RANDOMNESS CERTIFIED BY A STEERING INEQUALITY VIOLATION

The randomness on Bob's and Charlie's measurement results can also be certified by observing a violation of steering inequality V , which can be solved by the following optimisation problem:

$$\begin{aligned} & \max_{\substack{\{\sigma_{ABC}^{ee'}\}_{e,e'} \\ \{M_{b|y}\}_{b,y} \\ \{M_{c|z}\}_{c,z}}} \sum_{e,e'} \text{Tr} \left[\left(M_{b=e|y^*} \otimes M_{c=e'|z^*} \right) \sigma_{BC}^{ee'} \right] \\ & \text{s. t.} \quad \sum_{\substack{a,b,c, \\ x,y,z \\ e,e'}} F_{abc|xyz} \text{Tr} \left[M_{a|x} \otimes M_{b|y} \otimes M_{c|z} \sigma_{ABC}^{ee'} \right] = V, \\ & \sigma_{ABC}^{ee'} \geq 0, \quad \forall e, e', \quad \sum_{e,e'} \text{Tr} \left[\sigma_{ABC}^{ee'} \right] = 1, \\ & \{M_{b|y}\}_{b,y}, \{M_{c|z}\}_{c,z} \in \text{POVM}, \end{aligned} \quad (D1)$$

where $\sigma_{BC}^{ee'} = \text{Tr}_A[\sigma_{ABC}^{ee'}]$, $F_{abc|xyz}$ are the coefficients of the given inequality. Note that it is still considered in a real tripartite scenario, so the actual min-entropy need to be described by its lower and upper bounds. Also it can be easily extended to the case that randomness only on Bob or Charlie solely, and the method is similar with Appendix B.

For example, when Bob and Charlie are untrusted, a genuine tripartite steering can be observed if [42]

$$\alpha \langle A_3 B_3 \rangle + \alpha \langle A_3 Z \rangle + \alpha \langle B_3 Z \rangle + \beta \langle A_1 B_1 X \rangle - \beta \langle A_1 B_2 Y \rangle - \beta \langle A_2 B_1 Y \rangle - \beta \langle A_2 B_2 X \rangle - 1 \leq 0 \quad (D2)$$

is violated, in which $\alpha = 0.1831$ and $\beta = 0.2582$. A violation of Eq. (D2) implies the assemblage could not arise from measurements on a bi-separable state $\rho^{\text{bisep}} = \sum_{\lambda} p_{\lambda}^{\text{A:BC}} \rho_{\lambda}^{\text{A}} \otimes \rho_{\lambda}^{\text{BC}} + \sum_{\lambda} p_{\lambda}^{\text{B:AC}} \rho_{\lambda}^{\text{B}} \otimes \rho_{\lambda}^{\text{AC}} + \sum_{\lambda} p_{\lambda}^{\text{AB:C}} \rho_{\lambda}^{\text{AB}} \otimes \rho_{\lambda}^{\text{C}}$ [42]. Taking it into Eq. (D1), the randomness bounded by a genuine tripartite steering inequality violation is shown in Fig. D1.

We can find an obvious distinction between the curves of H_{\min}^{NS} and $H_{\min}^{Q_1}$. This is reasonable because there are many different assemblages corresponds with a same violation. Thus, the difference between the no-signaling set and the quantum set widens, resulting in a significant difference in randomness. Furthermore, because genuine multipartite steering is not necessary for

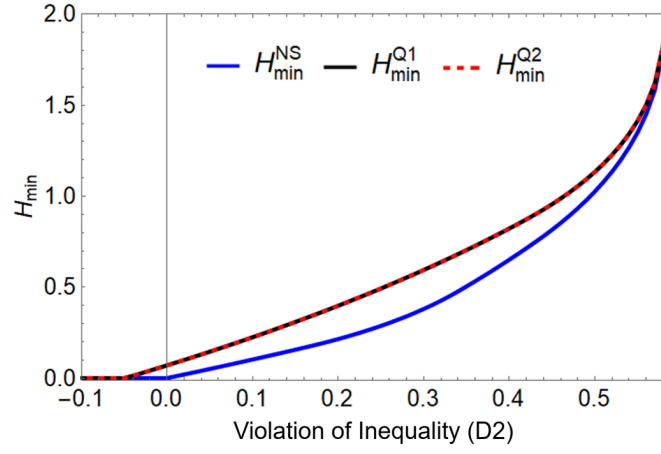


FIG. D1. Randomness certified by observing a violation of genuine tripartite steering inequality.

randomness, there is extra randomness can be certified without violating Eq. (D2).

* 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 Information* **2**, 16021 (2016).
- [3] M. Born, Zur Quantenmechanik der Stoßvorgänge, *Zeitschrift für Physik* **37**, 863 (1926).
- [4] J. S. Bell, On the Einstein Podolsky Rosen paradox, *Physics Physique Fizika* **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] L. Woollerton, P. Brown, and R. Colbeck, Tight Analytic Bound on the Trade-Off between Device-Independent Randomness and Nonlocality, *Phys. Rev. Lett.* **129**, 150403 (2022).
- [8] Z. Cao, H. Zhou, and X. Ma, Loss-tolerant measurement-device-independent quantum random number generation, *New Journal of Physics* **17**, 125011 (2015).
- [9] S. Fehr, R. Gelles, and C. Schaffner, Security and composability of randomness expansion from Bell inequalities, *Phys. Rev. A* **87**, 012335 (2013).
- [10] 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).
- [11] E. Woodhead, J. m. k. Kaniewski, B. Bourdoncle, A. Salavrakos, J. Bowles, A. Acín, and R. Augusiak, Maximal randomness from partially entangled states, *Phys. Rev. Res.* **2**, 042028 (2020).
- [12] P. Skrzypczyk and D. Cavalcanti, Maximal Randomness Generation from Steering Inequality Violations Using Qudits, *Phys. Rev. Lett.* **120**, 260401 (2018).
- [13] A. Acín, S. Massar, and S. Pironio, Randomness versus Nonlocality and Entanglement, *Phys. Rev. Lett.* **108**, 100402 (2012).
- [14] D.-L. Deng and L.-M. Duan, Fault-tolerant quantum random-number generator certified by Majorana fermions, *Phys. Rev. A* **88**, 012323 (2013).
- [15] E. Woodhead, B. Bourdoncle, and A. Acín, Randomness versus nonlocality in the Mermin-Bell experiment with three parties, *Quantum* **2**, 82 (2018).
- [16] J.-D. Bancal, L. Sheridan, and V. Scarani, More randomness from the same data, *New Journal of Physics* **16**, 033011 (2014).
- [17] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, Quantum randomness extraction for various levels of characterization of the devices, *Journal of Physics A: Mathematical and Theoretical* **47**, 424028 (2014).
- [18] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, Optimal randomness certification in the quantum steering and prepare-and-measure scenarios, *New Journal of Physics* **17**, 113010 (2015).
- [19] 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).
- [20] 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).
- [21] 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).
- [22] 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).
- [23] M.-H. Li, X. Zhang, W.-Z. Liu, S.-R. Zhao, B. Bai, Y. Liu, Q. Zhao, Y. Peng, J. Zhang, Y. Zhang, W. J. Munro, X. Ma, Q. Zhang, J. Fan,

- and J.-W. Pan, Experimental realization of device-independent quantum randomness expansion, *Phys. Rev. Lett.* **126**, 050503 (2021).
- [24] 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).
- [25] D. G. Marangon, G. Vallone, and P. Villoresi, Source-Device-Independent Ultrafast Quantum Random Number Generation, *Phys. Rev. Lett.* **118**, 060503 (2017).
- [26] 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 Science and Technology* **2**, 015011 (2017).
- [27] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, *Rev. Mod. Phys.* **81**, 865 (2009).
- [28] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, Quantum steering, *Rev. Mod. Phys.* **92**, 015001 (2020).
- [29] D. Cavalcanti and P. Skrzypczyk, Quantum steering: a review with focus on semidefinite programming, *Reports on Progress in Physics* **80**, 024001 (2016).
- [30] Y. Xiang, S. Cheng, Q. Gong, Z. Ficek, and Q. He, Quantum Steering: Practical Challenges and Future Directions, *PRX Quantum* **3**, 030102 (2022).
- [31] 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).
- [32] A. Acín and L. Masanes, Certified randomness in quantum physics, *Nature* **540**, 213 (2016).
- [33] 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, *Nature Physics* **17**, 448 (2021).
- [34] 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, *Nature Physics* **17**, 452 (2021).
- [35] 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).
- [36] 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).
- [37] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Experimentally generated randomness certified by the impossibility of superluminal signals, *Nature* **556**, 223 (2018).
- [38] 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* **562**, 548 (2018).
- [39] 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).
- [40] 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* **464**, 1021 (2010).
- [41] Q. Y. He and M. D. Reid, Genuine Multipartite Einstein-Podolsky-Rosen Steering, *Phys. Rev. Lett.* **111**, 250403 (2013).
- [42] 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, *Nature Communications* **6**, 7941 (2015).
- [43] 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).
- [44] 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).
- [45] 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, *Nature Physics* **11**, 167 (2015).
- [46] 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).
- [47] 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).
- [48] 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 (2020).
- [49] 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).
- [50] E. Schrödinger, Probability relations between separated systems, *Mathematical Proceedings of the Cambridge Philosophical Society* **32**, 446–452 (1936).
- [51] E. T. Jaynes, Information Theory and Statistical Mechanics. II, *Phys. Rev.* **108**, 171 (1957).
- [52] L. P. Hughston, R. Jozsa, and W. K. Wootters, A complete classification of quantum ensembles having a given density matrix, *Physics Letters A* **183**, 14 (1993).
- [53] N. Gisin, Stochastic quantum dynamics and relativity, *Helvetica Physica Acta* **62**, 363 (1989).
- [54] A. B. Sainz, N. Brunner, D. Cavalcanti, P. Skrzypczyk, and T. Vértesi, Postquantum Steering, *Phys. Rev. Lett.* **115**, 190403 (2015).
- [55] T. Vértesi, S. Pironio, and N. Brunner, Closing the Detection Loophole in Bell Experiments Using Qudits, *Phys. Rev. Lett.* **104**, 060401 (2010).
- [56] 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).
- [57] 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).
- [58] M. D. Reid, Monogamy inequalities for the Einstein-Podolsky-Rosen paradox and quantum steering, *Phys. Rev. A* **88**, 062108 (2013).

- [59] T. Vértesi, More efficient Bell inequalities for Werner states, *Phys. Rev. A* **78**, 032112 (2008).
- [60] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Experimental EPR-steering using Bell-local states, *Nature Physics* **6**, 845 (2010).
- [61] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, *Phys. Rev. Lett.* **98**, 010401 (2007).
- [62] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, *New Journal of Physics* **10**, 073013 (2008).
- [63] R. König, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, *IEEE Transactions on Information Theory* **55**, 4337 (2009).
- [64] M. T. Quintino, T. Vértesi, and N. Brunner, Joint Measurability, Einstein-Podolsky-Rosen Steering, and Bell Nonlocality, *Phys. Rev. Lett.* **113**, 160402 (2014).
- [65] R. Uola, T. Moroder, and O. Gühne, Joint Measurability of Generalized Measurements Implies Classicality, *Phys. Rev. Lett.* **113**, 160403 (2014).
- [66] 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).
- [67] 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).
- [68] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Entropic uncertainty relations and their applications, *Rev. Mod. Phys.* **89**, 015002 (2017).
- [69] One may think the distinction between H_{\min}^{NS} and $H_{\min}^{Q_k}$ is tiny. 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 $p^{obs}(abc|xyz)$ (See Appendix D), which shows a non-ignorable distinction between different lower bounds.
- [70] D. S. Tasca, P. Sánchez, S. P. Walborn, and L. Rudnicki, Mutual Unbiasedness in Coarse-Grained Continuous Variables, *Phys. Rev. Lett.* **120**, 040403 (2018).