Securing quantum networking tasks with multipartite Einstein-Podolsky-Rosen steering

Chien-Ying Huang,[1,2] Neill Lambert,[3] Che-Ming Li,[1,*] Yen-Te Lu,[1] and Franco Nori[3,4]
[1]*Department of Engineering Science, National Cheng Kung University, Tainan 701, Taiwan*
[2]*Graduate Institute of Photonics and Optoelectronics, National Taiwan University, Taipei 10617, Taiwan*
[3]*Theoretical Quantum Physics Laboratory, RIKEN Cluster for Pioneering Research, Wako-shi, Saitama 351-0198, Japan*
[4]*Department of Physics, University of Michigan, Ann Arbor, Michigan 48109-1040, USA*

(Received 15 March 2018; published 2 January 2019)

Einstein-Podolsky-Rosen (EPR) steering is the explicit demonstration of the fact that the measurements of one party can influence the quantum state held by another distant party and do so even if the measurements themselves are untrusted. This has been shown to allow one-sided device-independent quantum information tasks between two remote parties. However, in general, advanced multiparty protocols for generic quantum technologies, such as quantum secret sharing and blind quantum computing for quantum networks, demand multipartite quantum correlations of graph states shared between more than two parties. Here, we show that when one part of a quantum multidimensional system composed of a two-colorable graph state (e.g., cluster and Greenberger-Horne-Zeilinger states) is attacked by an eavesdropper using a universal cloning machine, only one of the copy subsystems can exhibit multipartite EPR steering *but not both*. Such a no-sharing restriction secures both state sources and channels against cloning-based attacks for generic quantum networking tasks, such as distributed quantum information processing, in the presence of uncharacterized measurement apparatuses.

DOI: 10.1103/PhysRevA.99.012302

I. INTRODUCTION

Einstein-Podolsky-Rosen (EPR) steering [1] is a unique part of EPR nonlocality [2]. It determines which states can be remotely prepared at one location by performing a measurement at another. Since its operational definition introduced by [3], this "spooky action at a distance" appears to be a subtle form of quantum correlation intermediate between entanglement and Bell nonlocality. Recently, this operational formulation has been utilized to exploit EPR steering to perform quantum key distribution [4], even if one party's measurement devices are untrusted. Quantum information, however, involves many other types of applications. Indeed, in general, many quantum information tasks inevitably require transmitting, sharing, or processing quantum information between more than two spatially separated quantum nodes, representing separated quantum systems, via quantum channels [5–8], which together form distributed quantum networks.

The multipartite quantum correlations present in graph states [9,10] are thought to act as an important resource: a type of fuel that powers a wide range of quantum strategies and protocols for networking tasks, including distributed quantum information processing, such as quantum secret sharing (QSS) [11–14], universal measurement-based quantum computation (MBQC) [15–19], quantum error correction codes (QECC) [20–22], and blind quantum computing (BQC) [23,24]. Quantum metrology takes advantage of this fuel as well, to offer higher precision than classical methods [25], such as a quantum network of clocks [26]. Graph states are even used to establish the basic building blocks for general modular architectures of quantum networks [27]. An N-qudit (quantum d-dimensional systems) graph state can be represented by a graph $G(V, E)$ [9,10,16,28]. In general, the graph G comprises the vertex set V with a cardinality $|V| = N$, representing the qudits, and the edge set E, each of which joins two vertices, representing interacting pairs of qudits, see Fig. 1. If the vertices of the graph G can be divided into q sets and the vertices of each set are given a color such that adjacent vertices have different colors, then the graph is called a q-colorable graph [9,10]. See Appendix A 1 for a detailed illustration of graph states for $q = 2$.

Compared with the many broad formulations and potential applications of quantum technologies, there is, so far, only a very preliminary conceptual understanding of multipartite EPR steering [29]. While detecting the steerability of multipartite systems [30–32] and genuine multipartite EPR steering [29,33] is possible, the fundamental issue of the role of such high-order EPR steering in securing quantum information processing involving multiple participants remains unclear. Very recently, for relatively small numbers of participants, genuine tripartite steering for pure three-mode Gaussian states [34] was shown to empower a partially device-independent QSS protocol [35]. Moreover, many entangled systems in graph states have been created and manipulated coherently in various experimental implementations [36–40]. The technological challenges facing the eventual realization of quantum technology suggests that they will inevitably rely on uncharacterized facilities and involve partially untrusted participants. While verification protocols of multipartite entanglement in the presence of untrusted parties, based on entanglement witness, have been proposed, these protocols are task-oriented and currently limited to Greenberger-Horne-Zeilinger (GHZ) states [41,42]. On the other hand, according

*cmli@mail.ncku.edu.tw

to the operational definition of EPR steering [3], verifying steerability not only assures that the particles shared with the trusted parties are truly entangled but also excludes the presence of untrusted participants in the tasks. Therefore, such a physical model of steering can be utilized in the context of the trusted-untrusted-participant scenario of various distributed quantum information tasks. However, does the higher-order EPR steerability of graph states preserve the security of quantum information processing in such imperfect circumstances?

Here, in order to tackle the issue of security of quantum networks, we reveal the no-sharing of multipartite EPR steering for any two-colorable graph states [9,10,43], which includes cluster states and GHZ states (i.e., star-graph states) as prominent illustrations of this class of graph states for quantum technologies [10–27,44–46]. Our scenario for identifying such no-sharing characteristics requires only the minimum of two local measurement settings for each quantum node and can be applied to general quantum information protocols based on normal local operations and classical communication, for instance, QSS, MBQC, and BQC, mentioned earlier.

We start with a definition of graph states in Schmidt form. Details of ideal graph states and the Schmidt decomposition are provided in Appendix A. In Sec. II we then define multipartite steering and introduce a measurable criterion for the presence of steering in such states based on mutual information. In Appendix B we provide a concrete example, a complete derivation of the criterion in the Schmidt bases, and its tolerance to noise. In Sec. III we use this criterion to show that multipartite steering cannot be shared by a cloning machine, and thus its observation can be used to verify the security of a network, which is explicitly derived in Appendix C. Concrete examples based on QSS, MBQC, and BQC are illustrated in Sec. IV. Moreover, the steering is shown to set a lower bound on the key rate in the problem of QSS with a complete derivation provided in Appendix D. In Sec. V we finish with the implications of our results for general quantum networking tasks that demand two-colorable graph states [10–27]. Insights and the outlook of our work have been summarized in Sec. VI.

We assume that, after being created from a graph-state source (Fig. 1), N qudits (with dimension d) of the two-colorable graph state $|G_2\rangle$ are individually sent to N parties of quantum nodes. In the trusted-untrusted-participant scenario, the N parties are divided into two groups, say A_s and B_s. With respect to this given bipartition, A_s and B_s can perceive that the state $|G_2\rangle$ connects them together through correlations between qudits, as described by the Schmidt form [43]

$$|G_2\rangle = \frac{1}{\sqrt{d}} \sum_{v=0}^{d-1} |v\rangle_{A_s m} \otimes |v\rangle_{B_s m}, \tag{1}$$

where $\mathrm{A}_{sm}^{(S)} = \{|v_{Am}\rangle_{A_s m} | v_{Am} \in \mathbf{v}\}$ and $\mathrm{B}_{sm}^{(S)} = \{|v_{Bm}\rangle_{B_s m} | v_{Bm} \in \mathbf{v}\}$ are the orthonormal bases for A_s's and B_s's qudits with $m = 1, 2$ for two different Schmidt bases, respectively, and $\mathbf{v} = \{0, 1, \ldots, d-1\}$. Since there are d nonvanishing terms in the Schmidt form, the Schmidt rank [47] of the graph state is d. See Appendix A 2 for the derivation of the Schmidt decomposition (1).

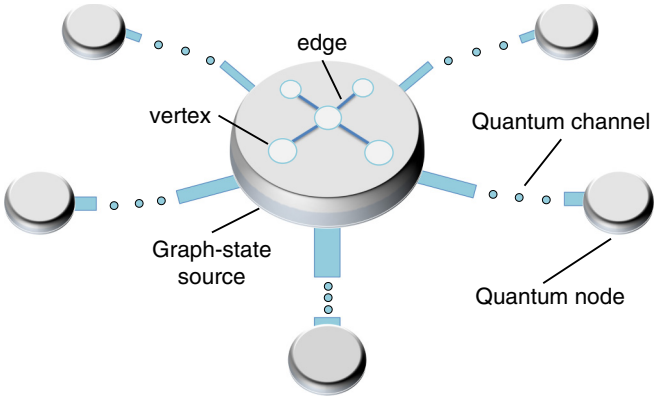

FIG. 1. Graph states for quantum networks. Graph states are created from a graph-state source, such as the star-graph states shown here, with the goal of using them for quantum information tasks. Each qudit is sent from the source to the corresponding quantum node through a quantum channel to implement said task, such as QSS [11–14] or MBQC [15–19], whereas for BQC [23,24], a specific initial state is sent from quantum nodes to the source for creating blind graph states. This construction is the essence of the modular and plug-and-play quantum network architecture [27].

II. EPR STEERING BETWEEN MULTI-QUANTUM NODES

In order to concretely represent the multipartite EPR steering of the state $|G_2\rangle$ (1), we consider a general model to describe states in the presence of uncharacterized measurement apparatuses. In our scenario, two possible measurements can be performed on each particle ($m_k = 1, 2$ for the kth particle), and each local measurement has d possible outcomes, $v_k^{(m_k)} \in \mathbf{v}$. That is, each party can implement quantum measurements of observables with the nondegenerate eigenvectors $\{|0\rangle_{k,1} = |0\rangle_k, |1\rangle_{k,1} = |1\rangle_k, \ldots, |d-1\rangle_{k,1} = |d-1\rangle_k\}$ for $m_k = 1$ and $\{|0\rangle_{k,2} = \hat{\mathrm{F}}_k|0\rangle_k, |1\rangle_{k,2} = \hat{\mathrm{F}}_k|1\rangle_k, \ldots, |d-1\rangle_{k,2} = \hat{\mathrm{F}}_k|d-1\rangle_k\}$ for $m_k = 2$, where $\hat{\mathrm{F}}_k$ is the quantum Fourier transformation (see detailed definition in Appendix A 1). We assume that the measurement devices used by the parties in A_s are uncharacterized, i.e., untrustworthy. In the worst case, A_s's measurement outcomes may be randomly generated from the measurement apparatuses themselves. In general, an unqualified source of the graph state, or noisy channels, may also lead to the same effect. Classical simulations, under the assumption of realism, can then describe the measurement results of A_s, which empowers A_s's ability to mimic the target state according to classical realism. Such an ability makes EPR steerability a strictly stronger quantum correlation than entanglement, which corresponds to the trusted-trusted-participant scenario in terms of operational definitions. In this case, with respect to a given bipartite splitting of the N parties, say α, the final state of the N particles can be specified by classical realistic theories, which predict that the particles are in a state belonging to a fixed set

$$\left\{v_k^{(1)}, v_k^{(2)}, \lambda_\alpha \middle| \forall k \in \mathbf{a}_s\right\}, \tag{2}$$

where the random variable λ_α corresponds to an unknown quantum state ρ_{λ_α} shared by the parties in B_s, and $\mathbf{a}_s$ denotes the indexing set for the parties in A_s.

The final states of the N-particle system may depend on unknown sources of randomness from the measurement apparatuses, graph-state source or channels, such that the above deterministic scenario becomes a probabilistic one. For a given bipartition α, they can then be characterized by the state probabilities, $P_\alpha(v_k^{(1)}, v_k^{(2)}, \lambda_\alpha|\forall k \in \mathbf{a}_s)$, to be

$$\rho_{B_s} = \sum_{v_k^{(1)}, v_k^{(2)}} \sum_{\lambda_\alpha} P_\alpha\big(v_k^{(1)}, v_k^{(2)}, \lambda_\alpha\big|\forall k \in \mathbf{a}_s\big)\rho_{\lambda_\alpha}. \tag{3}$$

If a state can offer stronger correlations between A_s and B_s than any strategies involving ρ_{B_s} for all possible λ_α, which can be explained by classical realistic theories in the presence of uncharacterized measurement apparatuses, we say that it possesses multipartite EPR steerability. Typically, intricate optimization processes are needed to characterize multipartite EPR steerability in (3), and thus a practical way to efficiently detect EPR steering for large-scale quantum systems is still an open problem. Here, in order to circumvent this difficulty, we utilize the Schmidt decomposition [43] introduced above and the entropic uncertain relation [48,49] to propose an efficient criterion to verify multipartite EPR steerability.

For all two-colorable graph states, $|G_2\rangle$, there are steering correlations between A_s and B_s which cannot be mimicked by the states ρ_{B_s}, Eq. (3). We first use the definition of information shared between A_s and B_s to certify that the nonclassical mutual dependence between the results of A_s's and B_s's measurements on $|G_2\rangle$ is larger than the dependence of B_s's measurement outcomes on the state ρ_{B_s}. Hence the ability for A_s to steer B_s's state is confirmed if the mutual dependence between the measurement results of A_s and B_s is stronger than the dependence of B_s's measurement outcomes on the state ρ_{B_s}. This steering condition can be concretely represented in terms of the mutual information as follows:

$$I_{A_sB_s} \equiv \sum_{m=1}^{2} I_{A_{sm}B_{sm}} > \sum_{m=1}^{2} I_{\lambda_\alpha B_{sm}}, \tag{4}$$

where

$$I_{A_{sm}B_{sm}} = H_m(B_s) - H_m(B_s|A_s)$$

and

$$I_{\lambda_\alpha B_{sm}} = H_m(B_s) - H_m(B_s|\lambda_\alpha).$$

Such a steering criterion generalizes the existing steering condition for two qudits [50,51] to multipartite systems. We assume that each particle is locally measured by its holder, and the parties, who implement quantum measurements, can perform positive operator valued measurements (POVMs) with sets of measurement operators composed of locally measurable operators, A_{sm} and B_{sm}, that are extracted from and commutative with the elements of the Schmidt bases $\mathrm{A}_{sm}^{(S)}$ and $\mathrm{B}_{sm}^{(S)}$ [43]. See Appendix B 1 for a detailed example. The measurement outcomes of A_s and B_s, $\{a_{s,1}, b_{s,1}\}$ and $\{a_{s,2}, b_{s,2}\}$, are then obtained from the measurements, which corresponds to $(\mathrm{A}_{s1}, \mathrm{B}_{s1})$ and $(\mathrm{A}_{s2}, \mathrm{B}_{s2})$, respectively. They are used to determine the entropy of B_s's outcomes:

$$H_m(B_s) = -\sum_{b_{s,m}} P(b_{s,m}) \log_2 P(b_{s,m}),$$

and the entropy conditioned on A_s's results:

$$H_m(B_s|A_s) = \sum_{a_{s,m}} P(a_{s,m}) H_m(B_s|a_{s,m}).$$

For the two-colorable graph states, $|G_2\rangle$, here we derive the overall correlation between A_s and B_s in terms of mutual information using corresponding quantum measurements, A_{sm} and B_{sm}. The entropy of B_s's outcomes is

$$H_1(B_s) = H_2(B_s) = \log_2 d,$$

and the entropy conditioned on A_s's results is

$$H_1(B_s|A_s) = H_2(B_s|A_s) = 0.$$

Therefore, the mutual information of A_s's and B_s's measurements becomes

$$I_{A_{s1}B_{s1}} = I_{A_{s2}B_{s2}} = \log_2 d.$$

We can thus obtain

$$I_{A_sB_s} = 2\log_2 d. \tag{5}$$

This result can be easily seen from the example of the three-qubit star-graph state given in Appendix B 1. These two-colorable graph states held by trusted parties with perfect conditions are useful resources for a variety of quantum information tasks, such as QSS [11–14], MBQC [15–19], and BQC [23,24].

In addition, since the unknown quantum state ρ_{λ_α} satisfies the entropic uncertainty relation under the two POVMs, B_{s1} and B_{s2}, which are complementary to each other [48,49],

$$H_1(B_s|\lambda_\alpha) + H_2(B_s|\lambda_\alpha) \geqslant \log_2 d, \tag{6}$$

the steering criterion (4) then puts a bound on $I_{A_sB_s}$ as

$$I_{A_sB_s} > \log_2 d. \tag{7}$$

It is clear that from the above derivation the trusted and untrusted roles of A_s and B_s can be exchanged. Hence, given the knowledge of which group is trusted, the criterion (7) negates the possibility that either A_s's or B_s's measurement results can be classically simulated. As shown in Appendix B 2, the steering condition can also be described in the Schmidt bases $(\mathrm{A}_{sm}^{(S)}, \mathrm{B}_{sm}^{(S)})$. Moreover, the criterion (7) is robust against white noise, independent of the number of participants, N. See the detailed discussions in Appendix B 3.

III. NO-SHARING OF MULTIPARTITE EPR STEERING

A universal cloning machine can produce a clone of an unknown state with high fidelity [52]. This result of quantum mechanics has significant implications in understanding quantum systems and profound applications in quantum information. Here we use it as an eavesdropping attack as used on the protocols of quantum cryptography [53].

Suppose A_s's and B_s's qudits are in a state $|G_2\rangle$ and, before receipt, B_s's qudits are sent to a universal cloning machine [52,53]. A third party, C_s, with an ancilla C_s', receives some of the output qudits of the cloning machine (see Fig. 2). We examine the mutual information between the results of measurements of B_s and C_s with those of A_s, where A_s, B_s, and C_s implement the complementary measurements $\mathrm{A}_{sm}^{(S)}$,

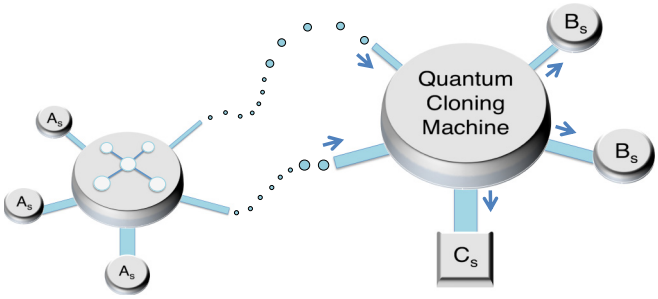

FIG. 2. Sharing multipartite EPR steering with a quantum cloner. The party C_s with an ancilla C_s' (not shown) wants to share the multipartite EPR steerability of $|G_2\rangle$, between the groups A_s and B_s, by using a quantum cloning machine. See Appendix C for detailed discussions.

$B_{sm}^{(S)}$, and $C_{sm}^{(S)}$, respectively, on their qudits in the Schmidt bases (see Appendixes B 1 and B 2). Hence we derive the following relationship between the mutual information of B_s and C_s with A_s,

$$\sum_{m=1}^{2} I_{A_{sm}C_{sm}} + \sum_{m=1}^{2} I_{A_{sm}B_{sm}} \leqslant 2\log_2 d, \tag{8}$$

for any multipartite graph states $|G_2\rangle$, including the simplest two-qudit graph state [51]. See Appendix C for details of the derivation.

The criterion (8) reveals that when the correlation between the qudits shared by A_s and one of the two groups, say B_s, is identified as steering by Eq. (7), the steering effect provides stronger correlations than the mutual dependence between A_s and C_s that cannot be replicated by a quantum cloning machine. To explain intuitively, criterion (8) concretely describes the total correlation that A_s can share with B_s and C_s individually under cloning attacks. The importance of criterion (8) is further supported by criterion (7) to confirm the steerability. In other words, multipartite EPR steering powers this type of nonclassical mutual information between A_s and B_s that cannot be shared with the third party C_s by a universal quantum cloner. Hence the criteria (7) and (8) can be used to rule out *both* untrusted participants and cloning-based attacks for quantum networks and thus can be exploited to secure a variety of quantum networking tasks (see Fig. 3).

IV. SECURING DISTRIBUTED QUANTUM INFORMATION PROCESSING

The no-sharing of multipartite steering has direct applications to quantum information protocols involving multiple participants. For example, for quantum computation, following the MBQC protocol [15–19], we assume that A_s and B_s share a state $|G_2\rangle$ and that the inputs for a computation task are prepared by measurements on the qudits held by A_s. The outputs of the computation can then be obtained by performing local operations on B_s's qudits according to A_s's measurement results. The criterion (7) can quantitatively describe how the statistical dependence between A_s's inputs and B_s's outputs in terms of the mutual information $I_{A_sB_s}$ go beyond the "cheating scenario" using the states ρ_{B_s}. In

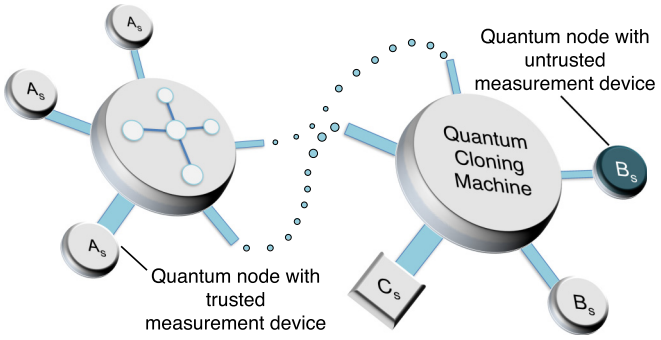

FIG. 3. Quantum networks under both a quantum cloner attack and with untrusted measurements for quantum nodes. In addition to the cloning attack, the quantum-node holders may lose control over their measurement devices such that the system state may be in ρ_{B_s} (3) in the worst case. For concreteness, it may happen in QSS where the untrusted parties in the group B_s attempt to use their own measurements and the cloner to obtain knowledge of A_s's key without collaboration with the rest of the trusted parties in B_s. The no-sharing of multipartite EPR steering can be used to secure QSS by excluding such a possibility with criteria (7) and (8).

particular, the criteria (7) and (8) together imply that such dependence between inputs and outputs cannot be copied by the eavesdropper to deduce the computation result, which secures the quantum computation task. This concept and method can be extended and applied to BQC as well to enable a client, who delegates a computation to a quantum server [23,24], to evaluate the uncharacterized facilities of the server and the security of the underlying quantum networks.

In addition to quantum computation, the no-sharing restriction plays an important role in securing QSS [11–14] and related applications, such as third-man quantum cryptography [12,54] in the presence of untrusted participants. For example, A_s is a dealer who sends a key to B_s. All the parties in B_s are required by A_s to collaborate to decode the key. If we assume that the dealer is trusted and C_s is the eavesdropper who uses a quantum cloner to attack the quantum network between A_s and B_s, the lower bound of the secret key rate for A_s and B_s can be determined by the Devetak-Winter formula [55]:

$$R \geqslant I_{A_{sm}B_{sm}} - \chi_{A_{sm}C_{sm}}, \tag{9}$$

where the Holevo quantity is defined by

$$\chi_{A_{sm}C_{sm}} \equiv S(\rho_{C_sC_s'}) - \sum_{v_{Am}=0}^{d-1} P(v_{Am}) S(\rho_{C_sC_s'|v_{Am}}).$$

Here $S(\rho_{C_sC_s'})$ is the von Neumann entropy of the reduced state $\rho_{C_sC_s'}$, and $\rho_{C_sC_s'|v_{Am}}$ is the state conditioned on A_s's result v_{Am}. Note that the role of C_s can also be played by the untrusted parties in B_s, who lie about their measurements and use the quantum cloner to obtain maximal knowledge of the dealer's key without collaboration with the trusted parties, as described in the unconditional security proof for partially device-independent QSS protocols [35] (see Fig. 3).

Using a similar method as employed in Eq. (8) (see Appendix D for a complete derivation), we can arrive at the

following lower bound for the secret key rate:

$$R \geqslant I_{A_s B_s} - \log_2 d. \tag{10}$$

The multipartite steerability for systems with arbitrary party number identified by the criteria (7) and (8) guarantees that B_s is trustworthy, and A_s and B_s can establish a secret key with a nonzero rate by which the importance of multipartite steering to QSS for tripartite systems [34] and even arbitrarily large systems can be appreciated.

Note that the magnitude of the mutual information $I_{A_s B_s}$, beyond the steering threshold $\log_2 d$, determines the lower bound of the key rate:

$$R_L = I_{A_s B_s} - \log_2 d.$$

As shown by Eq. (8), the attack of the quantum cloner can decrease the mutual information $I_{A_s B_s}$ and then reduce the lower bound of the key rate R_L. For the worst case, the error due to the quantum cloner even causes a zero key rate, $R_L = 0$. Such an error can be quantitively described by a value called the critical disturbance of the quantum cloner [53], D_c, and can be numerically determined as shown in Appendix D. For example, we have $D_c \approx 11\%$ for $d = 2$. This exactly coincides with the existing result based on the best eavesdropping with a coherent attack for bipartite quantum key distribution [56]. Therefore, the attack with a cloning machine is optimal for this case. While it is not clear whether a quantum cloner is optimal for attacks on quantum networks with more than two participants, $N > 2$, the optimal result for $N = 2$ illustrates that there exists a deep relationship between the security of quantum communication and the no-cloning theorem. The criterion on the key rate (10) based on the attack with a quantum cloner and the no-sharing of multipartite EPR steering could play a crucial role in ultimately securing generic quantum networking tasks.

In addition to the errors from the quantum cloner, any destructive influence on the steering reduces the lower bound of the key rate. See Fig. 4 for concrete illustrations with noisy graph states. When transmitting graph states without suffering from any loss or interference, the key rate achieves the maximum: $R = \log_2 d$, independent of the qudit number.

It is worth noting that testing the criterion (7) requires only two local measurement settings for each quantum node, which is naturally suitable for generic quantum information protocols using graph states. For instance, the measurements A_s and B_s can be chosen to coincide with those required in a MBQC task [15–19].

V. GENERAL QUANTUM NETWORKING TASKS

In addition to distributed quantum information, all the graph-state-based networking tasks require the distribution of graph states. The criteria (7) and (8) enable a task verifier or trusted participants to actively examine whether the received states are capable of preventing eavesdroppers from learning *any* task information with a quantum cloner, as demonstrated by the examples of MBQC, BQC, and QSS. This secures both state sources and channels against cloning-based attacks.

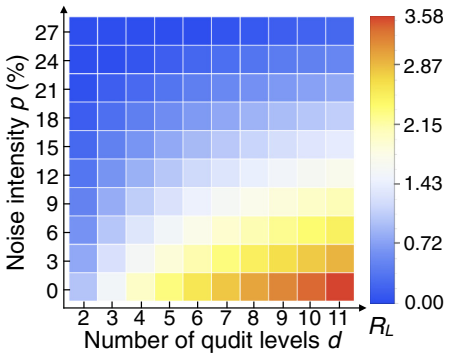

FIG. 4. The lower bound of the secret key rate R_L derived from noisy graph states. As demonstrated, the reduction in R_L by white noise (with intensity p) on $|G_2\rangle$ is independent of N. R_L can be increased by increasing d. This trend is comparable to the increase in the certified multipartite steering with d, i.e., the noise tolerance of the criterion (7) (Appendix B 3). Here the measurements used for creating secret keys, A_{sm} and B_{sm}, are extracted from Schmidt bases $\mathrm{A}_{sm}^{(S)}$ and $\mathrm{B}_{sm}^{(S)}$ [43] and satisfy the uncertainty relation under the two POVMs [48,49] as introduced above, and each POVM is composed of two operator elements, respectively. See Appendix B 1 for details. Note that for any cases where $I_{A_s B_s} - \log_2 d < 0$, the corresponding key rates are set as zero.

VI. CONCLUSION AND OUTLOOK

We have developed a formalism to explore the role of multipartite EPR steerability of two-colorable graph states in securing distributed quantum information tasks and showed that such high-order EPR steering cannot be shared by an eavesdropper using a universal quantum cloning machine, even in circumstances where a set of untrusted participants are involved. With a series of examples we illustrated how multipartite steering powers distributed quantum information processing in a secure manner. We expect that our criteria secure the initialization of network nodes in the joint graph states for generic quantum networking tasks.

This conclusion motivates several questions for future work: Apart from the two-colorable graph states shown here, does this quantum characteristic exist in *any* graph state? If this is the case, how do we confirm its existence in an experimentally efficient way? Moreover, in addition to multipartite steering, are the entropy-based criteria (7) and (8) useful for verifying genuine multipartite EPR steerability of graph states? Finally, because the assumption of a trusted group is made for the steering criterion (7), how a verifier, such as the dealer in QSS, can perform a reliable and objective evaluation of which node can be identified as trusted or untrusted becomes critical for large-scale networking tasks. The error and imperfections in the creation and manipulation of graph states grow with the system size, which increases the participants' uncertainty about the created states and the total quantum network. This question poses an interesting and significant challenge for partially device-independent applications.

ACKNOWLEDGMENTS

C.-M.L is partially supported by the Ministry of Science and Technology, Taiwan, under Grants No. MOST 104-

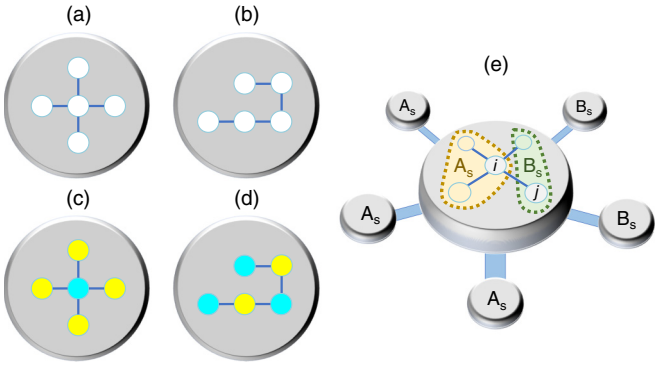

FIG. 5. Two-colorable graph states: (a) five-qudit star-graph state and (b) five-qudit chain graph state. The vertices of these graphs can be divided into two sets. The vertices of each set can be given a color such that adjacent vertices have different colors, as shown in (c) and (d). An edge, $(i, j) \in E$, corresponds to a unitary two-qudit transformation $U_{(i,j)}$ (A1) to cause a nonclassical correlation between qudits (e). The Schmidt form of a graph state, such as the star graph (e), with respect to the A_s subsystem (golden) and B_s subsystem (green) can be shown by first choosing a qudit in A_s (the ith qudit shown here) and then following the introduced procedure to find the state vector (A4) for the final Schmidt decomposition (A5).

2112-M-006-016-MY3 and No. MOST 107-2628-M-006-001-MY4. F.N. is supported in part by the MURI Center for Dynamic Magneto-Optics via the Air Force Office of Scientific Research (AFOSR) (FA9550-14-1-0040), the Army Research Office (ARO) (Grant No. W911NF-18-1-0358), the Asian Office of Aerospace Research and Development (AOARD) (Grant No. FA2386-18-1-4045), the Japan Science and Technology Agency (JST) (Q-LEAP program, ImPACT program, and CREST Grant No. JPMJCR1676), the Japan Society for the Promotion of Science (JSPS) (JSPS-RFBR Grant No. 17-52-50023, and JSPS-FWO Grant No. VS.059.18N), the RIKEN-AIST Challenge Research Fund, and the John Templeton Foundation. N.L. acknowledges partial support from JST PRESTO through Grant No. JPMJPR18GC.

APPENDIX A: TWO-COLORABLE GRAPH STATES

1. State vectors

A two-colorable graph has vertices that can be divided into two sets, where each set corresponds to a color such that adjacent vertices relate two different colors, such as star and chain graphs, see Figs. 1 and 5. For a given two-colorable graph $G(V, E)$ [9,10] used for networking tasks, an edge, $(i, j) \in E$, corresponds to a unitary two-qudit transformation among the two qudits (vertices) i and j,

$$U_{(i,j)} = \sum_{v=0}^{d-1} |v\rangle_{ii}\langle v| \otimes (Z_j)^v, \tag{A1}$$

where $\{|v\rangle_i | v \in \mathbf{v}\}$ with $\mathbf{v} = \{0, 1, \ldots, d-1\}$ is an orthonormal basis of the ith qudit and

$$Z_j = \sum_{v=0}^{d-1} \omega^v |v\rangle_{jj}\langle v|, \tag{A2}$$

with $\omega = \exp(i2\pi/d)$. The state vector of the target two-colorable colorable graph state can be obtained by applying $U_{(i,j)}$ to an initial state $|F_0\rangle = \bigotimes_{k=1}^{N} \hat{\mathrm{F}}_k |0\rangle_k$ [28] according to the edge set E:

$$|G_2\rangle = \prod_{(i,j)\in E} U_{(i,j)} |F_0\rangle, \tag{A3}$$

where $\hat{\mathrm{F}}_k$ is the quantum Fourier transformation defined by $\hat{\mathrm{F}}_k |v'\rangle_k = \sum_{v=0}^{d-1} \omega^{v'v} |v\rangle_k / \sqrt{d}$.

Regarding the topology of two-colorable graphs, it has been shown that genuine multipartite entanglement [43] and genuine multipartite Einstein-Podolsky-Rosen (EPR) steering [33] for states close to all two-colorable graph states $|G_2\rangle$ can be efficiently identified with two local measurement settings. This feature has also been used in deriving the entropic criterion for multipartite EPR steering (7) and the relationship (8).

2. The Schmidt form of $|G_2\rangle$

For a bipartite splitting of N quantum nodes of a N-qudit two-colorable graph state, one always can find a vertex in the A_s subsystem, let us say the ith qudit ($i \in V_{A_s}$), with vertices in the B_s subsystem forming edges $(i, j) \in E$, where $j \in V_{B_s}$. V_{A_s} and V_{B_s} denote the set of vertices of the subsystems A_s and B_s, respectively, where $|V_{A_s}| + |V_{B_s}| = |V| = N$, see Fig. 5(e). When the ith qudit is represented in the basis $\{|v\rangle_{if} = \hat{\mathrm{F}}_i |v\rangle_i | v \in \mathbf{v}\}$, the state vector of the graph state reads [43]

$$|G_2\rangle = d^{-\frac{|N(i)|}{2}} \sum_{v_1,\ldots,v_N; s_{ik} \doteq 0} \left[|v_i\rangle_{if} \bigotimes_{k\in V_{A_s}} (|v_k\rangle_a |v_k\rangle_k) \right] \otimes \left[\bigotimes_{k\in V_{B_s}} (|v_k\rangle_b |v_k\rangle_k) \right], \tag{A4}$$

where $s_{ik} = -v_i + \sum_{k\in N(i)} v_k$. The state vectors $|v_k\rangle_a$ and $|v_k\rangle_b$ are composed of qudits in V_{A_s} and V_{B_s}, respectively, and are accompanied by $|v_k\rangle_k$ for $k \in N(i)$, where $N(i)$ is the set of vertices that forms edges with the ith vertex. For instance, we have $N(i) = 4$ in Fig. 5(e).

Since the connection between v_i, v_j, and v_k for $k \in N(i)$ is constrained by $s_{ik} = -v_i + \sum_{k\in V_A} v_k + \sum_{k\in V_B} v_k \doteq 0$, where $\doteq$ denotes equality modulo d, the state vector (A4) can be explicitly represented as

$$|G_2\rangle = \frac{1}{\sqrt{d}} \sum_{v=0}^{d-1} |v\rangle_{A_s m} \otimes |v\rangle_{B_s m}, \tag{A5}$$

where

$$|v\rangle_{A_s m} = d^{-\frac{|V_{A_s}|-1}{2}} \sum_{v_1,\ldots,v_N; s_{ikv} \doteq 0} |v_i\rangle_{if} \bigotimes_{k\in V_{A_s}} (|v_k\rangle_a |v_k\rangle_k),$$

$$|v\rangle_{B_s m} = d^{-\frac{|V_{B_s}|-1}{2}} \sum_{v_1,\ldots,v_N; s_k \doteq v} \bigotimes_{k\in V_{B_s}} (|v_k\rangle_b |v_k\rangle_k), \tag{A6}$$

$s_{ikv} = -v_i + \sum_{k\in V_{A_s}} v_k + v$, and $s_k = \sum_{k\in V_{B_s}} v_k$. The state vectors $|v\rangle_{A_s m}$ and $|v\rangle_{B_s m}$ constitute two orthonormal bases $\mathrm{A}_{sm}^{(S)} = \{|v\rangle_{A_s m}\}$ and $\mathrm{B}_{sm}^{(S)} = \{|v\rangle_{B_s m}\}$. Hence the above representation is the Schmidt form of $|G_2\rangle$, as shown in Eq. (1)

in the main text. Note that the subscript $m = 1, 2$ reminds us that the state $|G_2\rangle$ can be represented in two different Schmidt bases $(\mathrm{A}_{sm}^{(S)}, \mathrm{B}_{sm}^{(S)})$, which are complementary to each other.

APPENDIX B: STEERING CRITERION

1. Measurements in the steering criterion

The design of the measurements required to implement the steering criterion (7) is based on the characteristics of the two-colorable graph states represented in the Schmidt bases (A5). For all two-colorable graph states, only the minimum two local measurement settings $(\mathrm{A}_{s1}, \mathrm{B}_{s1})$ and $(\mathrm{A}_{s2}, \mathrm{B}_{s2})$ are sufficient to verify multipartite EPR steering.

The measurement outcomes $\{a_{s,1}, b_{s,1}\}$ and $\{a_{s,2}, b_{s,2}\}$ obtained from the measurements $(\mathrm{A}_{s1}, \mathrm{B}_{s1})$ and $(\mathrm{A}_{s2}, \mathrm{B}_{s2})$, respectively, are used to determine the mutual information $I_{A_sB_s}$ for the steering criterion. Here A_{sm} and B_{sm} are general as POVMs. The POVM operator elements for each POVM depend on the type of bipartite splitting and the characteristics of the target graph state, and each POVM operator element can be locally measured on individual quantum nodes. These operators are extracted from the basis vectors (A6) of the Schmidt bases $\mathrm{A}_{sm}^{(S)}$ and $\mathrm{B}_{sm}^{(S)}$ such that they are commutative with the measurement operators in the Schmidt bases. Moreover, when measuring with the two POVMs, B_{s1} and B_{s2}, which are complementary bases, the entropic uncertainty relation (6) always holds for the quantum states ρ_{λ_α} [see Eq. (3)].

To elaborate, here we give a concrete example of a three-qubit star-graph state, where qubit 1 in A_s is connected with qubit 2 and qubit 3 in B_s. According to (A5) and (A6), its state vector can be expressed as

$$|G_{star}\rangle = \frac{1}{\sqrt{2}} \sum_{v=0}^{1} |v\rangle_{A_sm} \otimes |v\rangle_{B_sm},$$

where

$$\begin{aligned}
\mathrm{A}_{s1}^{(S)} &= \{|0\rangle_{A_s1} = |0\rangle_1, |1\rangle_{A_s1} = |1\rangle_1\},\\
\mathrm{B}_{s1}^{(S)} &= \{|0\rangle_{B_s1} = |{+}{+}\rangle_{23}, |1\rangle_{B_s1} = |{-}{-}\rangle_{23}\},\\
\mathrm{A}_{s2}^{(S)} &= \{|0\rangle_{A_s2} = |+\rangle_1, |1\rangle_{A_s2} = |-\rangle_1\},\\
\mathrm{B}_{s2}^{(S)} &= \{|0\rangle_{B_s2} = \frac{1}{\sqrt{2}}(|00\rangle_{23} + |11\rangle_{23}),\\
|1\rangle_{B_s2} &= \frac{1}{\sqrt{2}}(|01\rangle_{23} + |10\rangle_{23})\},
\end{aligned}$$

and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. By examining the Schmidt bases, $\mathrm{A}_{s1}^{(S)}$, $\mathrm{B}_{s1}^{(S)}$, $\mathrm{A}_{s2}^{(S)}$, and $\mathrm{B}_{s2}^{(S)}$, we then obtain the following POVMs in the locally measurable bases:

$$\begin{aligned}
\mathrm{A}_{s1} &= \{|0\rangle_{11}\langle 0|, |1\rangle_{11}\langle 1|\},\\
\mathrm{B}_{s1} &= \{|{+}{+}\rangle_{2323}\langle{+}{+}| + |{+}{-}\rangle_{2323}\langle{+}{-}|,\\
&\quad |{-}{+}\rangle_{2323}\langle{-}{+}| + |{-}{-}\rangle_{2323}\langle{-}{-}|\},\\
\mathrm{A}_{s2} &= \{|+\rangle_{11}\langle +|, |-\rangle_{11}\langle -|\},\\
\mathrm{B}_{s2} &= \{|00\rangle_{2323}\langle 00| + |11\rangle_{2323}\langle 11|,\\
&\quad |01\rangle_{2323}\langle 01| + |10\rangle_{2323}\langle 10|\}.
\end{aligned}$$

It is clear that these POVM operator elements are commutative with the Schmidt bases such that Eq. (5) holds, and the trusted and untrusted roles of A_s and B_s can be exchanged. Following the same procedure, our method can be easily extended to the graph states with arbitrary N and d.

2. Criterion in the Schmidt bases

In addition to the steering criterion in the form of (7) under the measurement settings $(\mathrm{A}_{sm}, \mathrm{B}_{sm})$, the steering condition can also be concretely represented in terms of the mutual information under the Schmidt bases $(\mathrm{A}_{sm}^{(S)}, \mathrm{B}_{sm}^{(S)})$ as follows:

$$I_{A_sB_s}^{(S)} \equiv \sum_{m=1}^{2} I_{A_{sm}B_{sm}}^{(S)} > \sum_{m=1}^{2} I_{\lambda_\alpha B_{sm}}^{(S)}, \tag{B1}$$

where $I_{A_{sm}B_{sm}}^{(S)}$ and $I_{\lambda_\alpha B_{sm}}^{(S)}$ are the mutual information between their results derived from the measurements $\mathrm{A}_{sm}^{(S)}$ and $\mathrm{B}_{sm}^{(S)}$ in the Schmidt bases. The measurement outcomes of $A_s^{(S)}$ and $B_s^{(S)}$, $\{a_{s,1}^{(S)}, b_{s,1}^{(S)}\}$ and $\{a_{s,2}^{(S)}, b_{s,2}^{(S)}\}$, are then obtained from the measurements, which corresponds to $(\mathrm{A}_{s1}^{(S)}, \mathrm{B}_{s1}^{(S)})$ and $(\mathrm{A}_{s2}^{(S)}, \mathrm{B}_{s2}^{(S)})$, respectively. The entropy of B_s's outcomes and the entropy conditioned on A_s's results are therefore derived from these measurement results. In addition, since the unknown quantum state ρ_{λ_α} satisfies the entropic uncertainty relation under the two complementary bases, $\mathrm{B}_{s1}^{(S)}$ and $\mathrm{B}_{s2}^{(S)}$ [48,49], the steering criterion (B1) in the Schmidt bases becomes

$$I_{A_sB_s}^{(S)} > \log_2 d. \tag{B2}$$

For any two-colorable graph states, as illustrated in Eq. (5), quantum measurements on the qudits can show that

$$I_{A_sB_s}^{(S)} = 2\log_2 d.$$

Therefore their dependence is stronger than the correlation between B_s and ρ_{B_s}.

3. Noise tolerance

To examine the steering criterion from the viewpoint of robustness against noise, we consider the minimum amount of uncolored noise added to $|G_2\rangle$ such that the noisy state cannot be identified by the steering criterion (7), i.e.,

$$I_{A_sB_s} = \log_2 d.$$

Suppose that in the presence of white noise the pure state $|G_2\rangle$ becomes

$$\rho_{G_2}(p) = \frac{p}{d^N}\hat{\mathrm{I}} + (1-p)|G_2\rangle\langle G_2|,$$

where p is the intensity of uncolored noise. The noise tolerance of criterion (7) is quantified by the noise threshold p_{noise} such that if $p < p_{\mathrm{noise}}$ then

$$I_{A_sB_s}(\rho_{G_2}(p)) > \log_2 d,$$

see Fig. 6. Here the A_{sm} and B_{sm} are extracted from Schmidt bases (A6) and satisfy the uncertainty relation under the two POVMs [48,49] as introduced above, and each POVM is composed of two operator elements. It is worth noting that this certification is independent of the node number N and

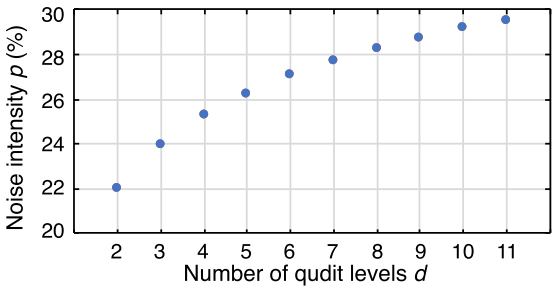

FIG. 6. Noise tolerance of the steering criterion, $I_{A_sB_s} > \log_2 d$, for arbitrarily two-colorable graph states.

becomes more robust against noise as the dimension of the quantum nodes (qudits) increases.

APPENDIX C: NO-SHARING OF MULTIPARTITE EINSTEIN-PODOLSKY-ROSEN STEERING

In what follows, we will prove Eq. (8) introduced in the main text for no-sharing of multipartite EPR steering. This criterion describes the relationship between the mutual information of B_s and C_s with A_s. First, we consider $|G_2\rangle$ to be an input of a quantum cloner, see Fig. 2. After cloning [52,53], the output state of the total system becomes

$$|\Psi\rangle_{A_sB_sC_sC_s'} = \sum_{j,k=0}^{d-1} \sqrt{\gamma_{jk}} |\Psi_{jk}\rangle_{A_sB_s} |\Psi_{j,d-k}\rangle_{C_sC_s'}, \tag{C1}$$

where

$$|\Psi_{jk}\rangle_{n'n} = \frac{1}{\sqrt{d}} \sum_{v=0}^{d-1} \omega^{vk} |v\rangle_{n'1} |v +_d j\rangle_{n1}, \tag{C2}$$

with $|\Psi_{00}\rangle_{n'n} = |G_2\rangle$ for $(n', n) = (A_s, B_s), (C_s, C_s')$, and $+_d$ denotes addition modulo d. The qudits of A_s and B_s are in the reduced state

$$\rho_{A_sB_s} = \sum_{j,k=0}^{d-1} \gamma_{jk} |\Psi_{jk}\rangle_{A_sB_sA_sB_s} \langle\Psi_{jk}|, \tag{C3}$$

and C_s's qudits with the ancilla C_s' have the reduced state

$$\rho_{C_sC_s'} = \sum_{j,k=0}^{d-1} \gamma_{jk} |\Psi_{j,d-k+1}\rangle_{C_sC_s'C_sC_s'} \langle\Psi_{j,d-k+1}|. \tag{C4}$$

The mutual information between A_s and B_s of the reduced state $\rho_{A_sB_s}$ is

$$I^{(S)}_{A_{sm}B_{sm}} = \log_2 d + \sum_{t=0}^{d-1} q_m^t \log_2 q_m^t, \tag{C5}$$

where $q_1^t = \sum_{k=0}^{d-1} \gamma_{tk}$ and $q_2^t = \sum_{j=0}^{d-1} \gamma_{j,d-t+1}$. The variables q_m^t denote the probabilities of observing $v_{Bm} - v_{Am} = t$ or $v_{Bm} - v_{Am} = t - d$ for $t \in \mathbf{v}$ [56]. Their sum is then

$$\sum_{m=1}^{2} I^{(S)}_{A_{sm}B_{sm}} = 2\log_2 d - \sum_{m=1}^{2} H\left(q_m^t\right). \tag{C6}$$

To determine the mutual information $I^{(S)}_{A_{sm}C_{sm}}$ between the results of measurements $\mathrm{A}^{(S)}_{sm}$ and $\mathrm{C}^{(S)}_{sm}$, we first consider the mutual dependence between v_{Am} and the results derived from measurements on C_s's qudits and ancilla C_s' by their mutual information $I^{(S)}_{A_{sm}(C_{sm}C'_{sm})}$. It is clear that

$$I^{(S)}_{A_{sm}C_{sm}} \leqslant I^{(S)}_{A_m(C_{sm}C'_{sm})}. \tag{C7}$$

In addition, $I^{(S)}_{A_{sm}(C_{sm}C'_{sm})}$ is constrained by the Holevo bound by

$$I^{(S)}_{A_{sm}(C_{sm}C'_{sm})} \leqslant \chi_{A_{sm}C_{sm}}, \tag{C8}$$

where the Holevo quantity is

$$\chi_{A_{sm}C_{sm}} = S\left(\rho_{C_sC_s'}\right) - \sum_{v_{Am}=0}^{d-1} P(v_{Am}) S\left(\rho_{C_sC_s'|v_{Am}}\right).$$

Here, the von Neumann entropy of the reduced state $\rho_{C_sC_s'}$ is defined by

$$S\left(\rho_{C_sC_s'}\right) = -\sum_{j,k=0}^{d-1} \gamma_{jk} \log_2 \gamma_{jk} \equiv H(\gamma). \tag{C9}$$

$\rho_{C_sC_s'|v_{Am}}$ is the state conditioned on A_s's result v_{Am}, the von Neumann entropy of which is

$$S\left(\rho_{C_sC_s'|v_{Am}}\right) = -\sum_{t=0}^{d-1} q_m^t \log_2 q_m^t \equiv H\left(q_m^t\right). \tag{C10}$$

In order to derive the upper bound of $I^{(S)}_{A_{sm}(C_{sm}C'_{sm})}$, by examining the difference between $S(\rho_{C_sC_s'})$ and $\sum_{v_{Am}=0}^{d-1} P(v_{Am}) S(\rho_{C_sC_s'|v_{Am}})$, we substitute $\gamma_{j,d-k} = g(j,k) q_1^j$ into $q_2^t = \sum_{j=0}^{d-1} \gamma_{j,d-t}$, where $\sum_{k=0}^{d-1} g(j,k) = 1$, and then obtain $q_2^t = \sum_{k=0}^{d-1} g(t,k) q_1^k$. For each t all $g(t,k) = q_2^t$ shows the maximum of the difference. Then we have

$$H(\gamma) = H\left(q_1^t\right) + \sum_t q_1^t H(f(t)) = H\left(q_1^t\right) + H\left(q_2^t\right). \tag{C11}$$

With Eqs. (C7)–(C11), the upper bound of the mutual information $I^{(S)}_{A_{sm}C_{sm}}$ is then shown as

$$I^{(S)}_{A_{sm}C_{sm}} \leqslant H\left(q_1^t\right) + H\left(q_2^t\right) - H\left(q_m^t\right),$$

which implies that

$$\sum_{m=1}^{2} I^{(S)}_{A_{sm}C_{sm}} \leqslant \sum_{m=1}^{2} H\left(q_m^t\right). \tag{C12}$$

Combining Eq. (C6) with Eq. (C12), we obtain

$$\sum_{m=1}^{2} I^{(S)}_{A_{sm}C_{sm}} + \sum_{m=1}^{2} I^{(S)}_{A_{sm}B_{sm}} \leqslant 2\log_2 d. \tag{C13}$$

For the simple bipartite case $N = 2$, the above relation recovers the criterion used by Chiu *et al.* [51] to show no-cloning of EPR steering. For general $N \geqslant 3$, since the measurement operators in the Schmidt bases and those in the locally measurable bases A_{sm}, B_{sm}, and C_{sm} commute with each other,

we have the relations

$$\sum_{m=1}^{2} I^{(S)}_{A_{sm}C_{sm}} = \sum_{m=1}^{2} I_{A_{sm}C_{sm}} \tag{C14}$$

and

$$\sum_{m=1}^{2} I^{(S)}_{A_{sm}B_{sm}} = \sum_{m=1}^{2} I_{A_{sm}B_{sm}}. \tag{C15}$$

Thus, through Eqs. (C13)–(C15) we arrive at Eq. (8):

$$\sum_{m=1}^{2} I_{A_{sm}C_{sm}} + \sum_{m=1}^{2} I_{A_{sm}B_{sm}} \leqslant 2\log_2 d.$$

As the correlation between the qudits shared by A_s and B_s is identified as multipartite steering by Eq. (7), the mutual dependence between A_s and C_s then cannot show the steering effect.

APPENDIX D: LOWER BOUND OF THE SECRET KEY RATE FOR QUANTUM SECRET SHARING BLUE AND THE CRITICAL DISTURBANCE OF THE QUANTUM CLONER

To determine the lower bond of the secret key rate for QSS, as described by Eq. (9) [55], we consider the following quantity:

$$I_{A_{sm}B_{sm}} - \max \chi_{A_{sm}C_{sm}}.$$

From Eqs. (C9)–(C11), (C15), (C14), and

$$I_{A_{sm}B_{sm}} = \log_2 d - H\left(q_m^t\right), \tag{D1}$$

we get $\max \chi_{A_{sm}C_{sm}} = 2\log_2 d - I_{A_sB_s} - H(q_m^t)$. Therefore we obtain the following lower bound of the secret rate:

$$R_L = I_{A_sB_s} - \log_2 d, \tag{D2}$$

as shown in Eq. (10). The multipartite steerability identified by the criterion (7) then enables A_s and B_s to collaboratively generate a secret key with a nonzero rate. Combined with the noise tolerance obtained above, we can thus find the lower bound of the secret key rate R_L derived from noisy graph states, as illustrated in Fig. 4 in the main text.

Equation (D2) can be used to evaluate the critical disturbance of the quantum cloner that makes $R_L = 0$. We first note that the variables q_m^t for $t \neq 0$ quantitatively describe the errors introduced by the cloner. See the explanation for q_m^t in Eq. (C5). Then suppose that the quantum cloner is phase covariant [53], which copies equally well the states of both bases, we have $H(q_1^t) = H(q_2^t) = H(D)$, where

$$H(D) = -(1-D)\log_2(1-D) - D\log_2\frac{D}{d-1}, \tag{D3}$$

and $D = 1 - q_m^0$ is the disturbance due to the attack of a quantum cloner. With $H(D)$, the critical disturbance D_c for $R_L = 0$ can be derived by solving the equation

$$(1-D_c)\log_2(1-D_c) + D\log_2\frac{D_c}{d-1} = -\frac{1}{2}\log_2 d. \tag{D4}$$

For example, the critical disturbance is $D_c \approx 11.00\%$ for $d = 2$ and $D_c \approx 15.95\%$ for $d = 3$.

[1] E. Schrödinger, Discussion of probability relations between separated systems, Math. Proc. Cambridge Philos. Soc. **31**, 555 (1935).

[2] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. **47**, 777 (1935).

[3] 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).

[4] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering, Phys. Rev. A **85**, 010301(R) (2012).

[5] H. J. Kimble, The quantum internet, Nature (London) **453**, 1023 (2008).

[6] L.-M. Duan and C. Monroe, *Colloquium*: Quantum networks with trapped ions, Rev. Mod. Phys. **82**, 1209 (2010).

[7] T. E. Northup and R. Blatt, Quantum information transfer using photons, Nat. Photonics **8**, 356 (2014).

[8] A. Reiserer and G. Rempe, Cavity-based quantum networks with single atoms and optical photons, Rev. Mod. Phys. **87**, 1379 (2015).

[9] M. Hein, J. Eisert, and H. J. Briegel, Multiparty entanglement in graph states, Phys. Rev. A **69**, 062311 (2004).

[10] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, in *Quantum Computers, Algorithms and Chaos, Proceedings of the International School of Physics "Enrico Fermi"*, edited by G. Casati, D. L. Shepelyansky, P. Zoller, and G. Benenti (IOS, Amsterdam, 2006), Vol. 162; see also arXiv:quant-ph/0602096.

[11] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[12] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography, Phys. Rev. Lett. **95**, 200502 (2005).

[13] D. Markham and B. C. Sanders, Graph states for quantum secret sharing, Phys. Rev. A **78**, 042309 (2008).

[14] B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, Experimental demonstration of graph-state quantum secret sharing, Nat. Commun. **5**, 5480 (2014).

[15] R. Raussendorf and H. J. Briegel, A One-Way Quantum Computer, Phys. Rev. Lett. **86**, 5188 (2001).

[16] R. Raussendorf, D. E. Browne, and H. J. Briegel, Measurement-based quantum computation with cluster states, Phys. Rev. A **68**, 022312 (2003).

[17] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Experimental one-way quantum computing, Nature (London) **434**, 169 (2005).

[18] K. Chen, C.-M. Li, Q. Zhang, Y.-A. Chen, A. Goebel, S. Chen, A. Mair, and J.-W. Pan, Experimental Realization of

One-Way Quantum Computing with Two-Photon Four-Qubit Cluster States, Phys. Rev. Lett. **99**, 120503 (2007).

[19] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, Measurement-based quantum computation, Nat. Phys. **5**, 19 (2009).

[20] D. Schlingemann and R. F. Werner, Quantum error-correcting codes associated with graphs, Phys. Rev. A **65**, 012308 (2001).

[21] S. Y. Looi, L. Yu, V. Gheorghiu, and R. B. Griffiths, Quantum-error-correcting codes using qudit graph states, Phys. Rev. A **78**, 042303 (2008).

[22] B. A. Bell, D. A. Herrera-Martí, M. S. Tame, D. Markham, W. J. Wadsworth, and J. G. Rarity, Experimental demonstration of a graph state quantum error-correction code, Nat. Commun. **5**, 3658 (2014).

[23] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *Proceedings of the 50th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, CA, 2009), pp. 517–526.

[24] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Demonstration of blind quantum computing, Science **20**, 303 (2012).

[25] V. Giovannetti, S. Lloyd, and L. Maccone, Advances in quantum metrology, Nat. Photonics **5**, 222 (2011).

[26] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, A quantum network of clocks, Nat. Phys. **10**, 582 (2014).

[27] A. Pirker, J. Wallnöfer, and W. Dür, Modular architectures for quantum networks, New J. Phys. **20**, 053054 (2018).

[28] D. L. Zhou, B. Zeng, Z. Xu, and C. P. Sun, Quantum computation based on d-level cluster state, Phys. Rev. A **68**, 062303 (2003).

[29] Q. Y. He and M. D. Reid, Genuine Multipartite Einstein-Podolsky-Rosen Steering, Phys. Rev. Lett. **111**, 250403 (2013).

[30] 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).

[31] D. Cavalcanti, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. Souto Ribeiro, and S. P. Walborn, Detection of entanglement in asymmetric quantum networks and multipartite quantum steering, Nat. Commun. **6**, 7941 (2015).

[32] 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).

[33] 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).

[34] Y. Xiang, I. Kogias, G. Adesso, and Q. Y. He, Multipartite Gaussian steering: Monogamy constraints and quantum cryptography applications, Phys. Rev. A **95**, 010101(R) (2017).

[35] I. Kogias, Y. Xiang, Q. Y. He, and G. Adesso, Unconditional security of entanglement-based continuous-variable quantum secret sharing, Phys. Rev. A **95**, 012315 (2017).

[36] T. Monz, P. Schindler, J. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, 14-Qubit Entanglement: Creation and Coherence, Phys. Rev. Lett. **106**, 130506 (2011).

[37] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell *et al.*, Superconducting quantum circuits at the surface code threshold for fault tolerance, Nature (London) **508**, 500 (2014).

[38] J. Kelly, R. Barends, A. G. Fowler, A. Megrant, E. Jeffrey, T. C. White, D. Sank, J. Y. Mutus, B. Campbell, Y. Chen *et al.*, State preservation by repetitive error detection in a superconducting quantum circuit, Nature (London) **519**, 66 (2015).

[39] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li *et al.*, Experimental Ten-Photon Entanglement, Phys. Rev. Lett. **117**, 210502 (2016).

[40] X.-L. Wang, Y.-H. Luo, H.-L. Huang, M.-C. Chen, Z.-E. Su, C. Liu, C. Chen, W. Li, Y.-Q. Fang, X. Jiang *et al.*, 18-qubit Entanglement with Six Photons's Three Degrees of Freedom, Phys. Rev. Lett. **120**, 260502 (2018).

[41] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, Multipartite Entanglement Verification Resistant against Dishonest Parties, Phys. Rev. Lett. **108**, 260502 (2012).

[42] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis *et al.*, Experimental verification of multipartite entanglement in quantum networks, Nat. Commun. **7**, 13251 (2016).

[43] C.-M. Li, K. Chen, A. Reingruber, Y.-N. Chen, and J.-W. Pan, Verifying Genuine High-Order Entanglement, Phys. Rev. Lett. **105**, 210504 (2010).

[44] T. Tanamoto, Y. X. Liu, S. Fujita, X. Hu, and F. Nori, Producing Cluster States in Charge Qubits and Flux Qubits, Phys. Rev. Lett. **97**, 230501 (2006).

[45] J. Q. You, X. B. Wang, T. Tanamoto, and F. Nori, Efficient one-step generation of large cluster states with solid-state circuits, Phys. Rev. A **75**, 052319 (2007).

[46] T. Tanamoto, Y. X. Liu, X. Hu, and F. Nori, Efficient Quantum Circuits for One-Way Quantum Computing, Phys. Rev. Lett. **102**, 100501 (2009).

[47] B. M. Terhal and P. Horodecki, Schmidt number for density matrices, Phys. Rev. A **61**, 040301(R) (2000).

[48] M. Tomamichel and R. Renner, Uncertainty Relation for Smooth Entropies, Phys. Rev. Lett. **106**, 110506 (2011).

[49] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Entropic uncertainty relations and their applications, Rev. Mod. Phys. **89**, 015002 (2017).

[50] C.-M. Li, Y.-N. Chen, N. Lambert, C.-Y. Chiu, and F. Nori, Certifying single-system steering for quantum-information processing, Phys. Rev. A **92**, 062310 (2015).

[51] C.-Y. Chiu, N. Lambert, T.-L. Liao, F. Nori, and C.-M. Li, No-cloning of quantum steering, npj Quantum Inf. **2**, 16020 (2016).

[52] V. Bužek and M. Hillery, Quantum copying: Beyond the no-cloning theorem, Phys. Rev. A **54**, 1844 (1996).

[53] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Quantum cloning, Rev. Mod. Phys. **77**, 1225 (2005).

[54] M. Żukowski, A. Zeilinger, M. A. Horne, and H. Weinfurter, Quest for GHZ states, Acta Phys. Pol., A **93**, 187 (1998).

[55] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. London, Ser. A **461**, 207 (2005).

[56] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, Phys. Rev. A **82**, 030301 (2010).