Certifying single-system steering for quantum-information processing

Che-Ming Li,[1,2,*] Yueh-Nan Chen,[3,4] Neill Lambert,[2] Ching-Yi Chiu,[1] and Franco Nori[2,5]
[1]*Department of Engineering Science, National Cheng Kung University, Tainan 701, Taiwan*
[2]*CEMS, RIKEN, Wako-shi, Saitama 351-0198, Japan*
[3]*Department of Physics, National Cheng Kung University, Tainan 701, Taiwan*
[4]*National Center for Theoretical Sciences, Hsinchu 300, Taiwan*
[5]*Department of Physics, University of Michigan, Ann Arbor, Michigan 48109-1040, USA*
(Received 18 January 2015; revised manuscript received 15 October 2015; published 7 December 2015)

Einstein-Podolsky-Rosen (EPR) steering describes how different ensembles of quantum states can be remotely prepared by measuring one particle of an entangled pair. Here, we investigate quantum steering for *single* quantum d-dimensional systems (qudits) and devise efficient conditions to certify the steerability therein, which we find are applicable both to single-system steering *and* EPR steering. In the single-system case our steering conditions enable the unambiguous ruling out of generic classical means of mimicking steering. Ruling out "false-steering" scenarios has implications for securing channels against both cloning-based individual attack and coherent attacks when implementing quantum key distribution using qudits. We also show that these steering conditions also have applications in quantum computation, in that they can serve as an efficient criterion for the evaluation of quantum logic gates of arbitrary size. Finally, we describe how the nonlocal EPR variant of these conditions also function as tools for identifying faithful one-way quantum computation, secure entanglement-based quantum communication, and genuine multipartite EPR steering.

DOI: 10.1103/PhysRevA.92.062310 PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Lx

I. INTRODUCTION

Einstein-Podolsky-Rosen (EPR) steering was originally introduced by Schrödinger [1] in response to the EPR paradox [2]. Such steering is the ability of one party, Alice, to affect the state of another remote party, Bob, through her choice of measurement [1]. This relies on both the entanglement of the pair shared between Alice and Bob and the measurement settings chosen for each particle of the pair. Recently, the concept of EPR steering has been reformulated in terms of an information-theoretic task [3] showing that two parties can share entanglement even if the measurement devices of one of them are uncharacterized (or untrusted). This formulation also illustrates a strict hierarchy between Bell nonlocality, steering, and entanglement. It is worth noting that, as with Bell inequalities and entanglement witnesses, which have been widely used to verify quantum correlations, EPR steering inequalities [4] and steering measures [5] have been introduced to detect and quantify the steerability of bipartite quantum systems. It is also now understood that steering has applications in certain quantum key distribution (QKD) schemes, where one of the parties does not trust their measurement apparatus, i.e., one-sided device-independent QKD (1SDI-QKD) [6]. In addition to these theoretical breakthroughs several experimental demonstrations of EPR steering have been reported [7–9].

Since the reformulation of EPR steering by Wiseman *et al.* [3], there has been a range of investigations into steering's unique properties, quantification, and potential extensions. For example, it has been shown that there exist entangled states by which steering can be performed in only one direction [10–12], from Alice to Bob but not from Bob to Alice. In addition, the original bipartite steering effect has been generalized to genuine multipartite steering [13–16]. Moreover, a temporal analog of the steering inequality has been introduced [17], and a nontrivial operational meaning to violations of such an inequality was found through a connection to the security bounds of certain QKD schemes [17].

Given this range of breakthroughs in our understanding of quantum steering, a natural question arises: does there exist a strict and experimentally efficient criteria for quantum steering that can be used to certify the reliability of *both* quantum communication (like QKD) and quantum computation tasks? So far, it was been shown that 1SDI-QKD [6] benefits from EPR steering. However, there is no unified scheme for the use of quantum steering for generic quantum-information processing tasks. In fact, the role of quantum steering in quantum computation, if any, is not clear.

Here, we present a simple but unified picture to connect quantum steering with such generic quantum-information tasks. See Fig. 1 for a schematic illustration of a typical implementation. Two steering conditions are introduced to identify genuine single-system quantum steering in the presence of errors and which can be applied to both quantum computation and quantum communication using qudits (systems of arbitrary dimension). Both steering conditions need only the *minimum* of two local measurement settings for experimental implementation. Our results give a strict meaning of violating the temporal analog of the steering inequality [17] and extend the 1SDI-QKD from qubit [6] to qudit cases. Moreover, we show how these conditions can be applied in the standard nonlocal EPR setting and then used to validate quantum computation for both the quantum circuit model [18] and one-way quantum computing [19]. Finally, we discuss the implications for certifying genuine multipartite EPR steering and implementing multipartite secret sharing with partially uncharacterized measurement devices.

*cmli@mail.ncku.edu.tw

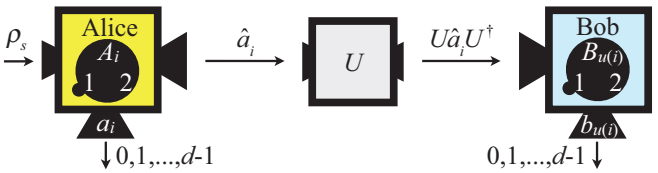

FIG. 1. (Color online) Single-system steering for quantum-information tasks. The state $\hat{a}_i$ is sent from Alice to Bob. Here $\hat{a}_i$ is a postmeasurement state of a qudit ρ_s under the measurement A_i for $i = 1,2$. By sharing certain information distributed via a classical communication channel (not shown), Alice can steer the state of Bob's particle by asking him to perform the quantum operation U. For example, by simply choosing U as an identity operator, Alice's steering enables them to realize QKD. When U is an arbitrary quantum logic gate, steering single systems is equivalent to performing quantum computation. To identify whether Alice can implement such steering, Bob can use the steering condition (7) or (9) to rule out the results mimicked by generic classical strategies. As illustrated, Bob performs measurements $B_{u(i)}$ to implement these certifications. These steering conditions ensure secure quantum communication and faithful quantum computation (see Table I). Here, it is allowed that Alice and Bob have no spatial separation but access the single system at different times.

II. QUANTUM STEERING FOR SINGLE SYSTEMS

In the scenario of single-system quantum steering, Alice's ability to affect the quantum state Bob has access to is based on both her ability to prepare an arbitrary quantum state to send to Bob and her knowledge, if any, about the state Bob finally receives (which may differ from her prepared state, for various reasons) [20]. If Alice has full information about the quantum system Bob is holding, she is capable of *steering* this system into an arbitrary state. Alice can follow two steps to achieve this (Fig. 1).

First, Alice prepares a specific state of a qudit with a given initial state state ρ_s generated from some quantum source, before sending it to Bob, by performing complementary measurements A_i for $i = 1,2$. Once the particle is measured with a chosen A_i, ρ_s becomes $\hat{a}_i \equiv |a_i\rangle_{ii}\langle a_i|$ for $a_i \in \mathbf{v} = \{0,1,\ldots,d-1\}$, where the d states constitute an orthonormal basis $\{|a_i\rangle_i\}$ [20]. The set of states $\{|a_2\rangle_2\}$ is complementary to the state set $\{|a_1\rangle_1\}$ by defining $|a_2\rangle_2 = 1/\sqrt{d}\sum_{a_1=0}^{d-1}\omega^{a_2a_1}|a_1\rangle_1$, with $\omega = \exp(i2\pi/d)$.

Second, the particle in the state $\hat{a}_i$ is sent to Bob. Here Bob does not know the state of particle $\hat{a}_i$ sent from Alice. To steer Bob's state $\hat{a}_i$ into other quantum states $\mathcal{U}(\hat{a}_i) \equiv U\hat{a}_iU^\dagger$, Alice can directly perform the unitary operation U by herself before the particle transmission, or publicly, via a classical channel, ask Bob to apply U on $|a_i\rangle_i$. While the quantum operation $\mathcal{U}$ is announced publicly, the state $\mathcal{U}(\hat{a}_i)$ is still unknown to Bob. It is clear that Alice has complete knowledge about the quantum system held by Bob since the state ρ_s, the measurement A_i, and the subsequent operation $\mathcal{U}$ are designed by Alice. When Bob performs measurements on his particle after the operation $\mathcal{U}$, his two complementary measurements $B_{u(i)}$ for $i = 1,2$ are specified by the orthonormal bases $\{|b_{u(i)}\rangle_{u(i)} \equiv U|b_i\rangle_i|b_{u(i)} = b_i \in \mathbf{v}\}$ with the results $\{b_{u(i)}\}$.

In an ideal case, the state received by Bob is the same as the initial state $\hat{a}_i$ prepared by Alice under the transformation $\mathcal{U}$. In practical situations, however, noise from the environment or other artificial effects introduce an unknown source of randomness. In order to explicitly qualify whether Alice can steer the states of the particles eventually held by Bob, and rule out either third-party eavesdropping, classical mimicry of the channel, or to qualify the quality of the channel itself, we consider the following generic *classical means* of describing state preparation, transitions between states, and the limits to which they can influence the measurement results of Bob.

First, we assume that the state of the particle sent by Alice can be described by a classical realistic theory which predicts the particle is in a state described by a fixed set $(A_1 = a_1, A_2 = a_2)$. Suppose next that $P(a_1,a_2)$ is the probability that, before the measurements are performed, the particle is in a state (a_1,a_2). Under this assumption the marginal probability $P(a_i)$ and the conditional probability $P(a_i|a_j)$ for $i,j = 1,2$ and $i \neq j$ should follow the relation

$$P(a_1,a_2) = P(a_1)P(a_2|a_1) = P(a_2)P(a_1|a_2). \tag{1}$$

Second, we assume that the particle state can change, while it is being transmitted from Alice to Bob, from (a_1,a_2) to an unknown state ρ_λ with a transition probability $P[\lambda|(a_1,a_2)]$. Then, the state of the particle changes to $\sum_{a_1,a_2}P(a_1,a_2)\sum_\lambda P[\lambda|(a_1,a_2)]\rho_\lambda$. To connect this state with our steering scenario, where the state of the particle, and how it evolves, may depend on the choice to measure a_1 or a_2 individually, we rewrite the transition probability as $P[\lambda|(a_1,a_2)] = P(\lambda|a_i)P(a_j|\lambda,a_i)/P(a_j|a_i)$ [22]. From which, combined with the relation (1), the joint probability of finding (a_1,a_2) and observing λ as the final state can be explicitly represented by

$$\begin{aligned} P[(a_1,a_2),\lambda] &= P(a_1,a_2)P[\lambda|(a_1,a_2)] \\ &= P(a_i)P(\lambda|a_i)P(a_j|\lambda,a_i). \end{aligned} \tag{2}$$

As shown by (1) and (2), it does not matter what order Alice does a series of measurements, the joint probability will always be the same. The state of the particle that Bob holds is then

$$\rho_B = \sum_{a_i=0}^{d-1} P(a_i)\sum_\lambda P(\lambda|a_i)\rho_\lambda. \tag{3}$$

When summing over all a_1 and a_2, Eq. (2) becomes

$$P(\lambda) = \sum_{a_1} P(a_1)P(\lambda|a_1) = \sum_{a_2} P(a_2)P(\lambda|a_2). \tag{4}$$

With the above classical realistic description of Alice's states, the state received by Bob becomes independent of the measurement setting chosen by Alice, i.e., $\rho_B = \sum_\lambda P(\lambda)\rho_\lambda$, implying that Bob always has the same state whatever measurement A_i and operation $\mathcal{U}$ Alice designs. This means Alice cannot steer Bob's states. We call the states with this feature *unsteerable*. The above proof can be seen as equivalent to that used in the derivation of EPR steering inequalities and extended EPR steering conditions, where Alice's measurement results are assumed to be a classical distribution. See Appendix A for detailed discussions.

Finally, if Alice's state and the unknown states ρ_λ are described by a classical theory of realism, and thus only classically correlated with Bob's results, then the descriptions Eqs. (1), (2), and (4) are applicable to ρ_λ as well. However, here Bob's measurement results are assumed to be based on measurements on a quantum particle. Thus the expectation values of the two mutually unbiased measurements $B_{u(1)}$ and $B_{u(2)}$ with respect to the unknown quantum states ρ_λ obey the quantum uncertainty relation in the entropic form [23]

$$H(B_{u(1)}|\lambda) + H(B_{u(2)}|\lambda) \geqslant \log_2(d), \tag{5}$$

where $H(B_{u(i)}|\lambda) = -\sum_{b_{u(i)}=0}^{d-1} P(b_{u(i)}|\lambda)\log_2 P(b_{u(i)}|\lambda)$.

III. QUANTUM STEERING CONDITIONS

A. Steering conditions

In order to distinguish steerability from the results mimicked by the methods based on the classical theories considered above, in what follows we will introduce two quantum steering conditions of the from $\mathcal{S} > \alpha_R$, where $\mathcal{S}$ is the kernel of the criterion and α_R is the maximum value of the kernel supported by classical theories. For ideal steering, $\mathcal{S}$ will be maximized. Since ruling out classical mimicry is equivalent to excluding unsteerable states (3), exceeding the α_R will deny, or rule out, processes (e.g., noisy channels) that make once steerable states unsteerable and thus assist in confirming genuine quantum steering.

The kernel of our first steering condition is

$$\mathcal{S}_{dU} \equiv \sum_{i=1}^{2} \sum_{a_i=0;b_{u(i)}=a_i}^{d-1} P(a_i, b_{u(i)}). \tag{6}$$

For ideal steering the maximum value for the kernel is $\mathcal{S}_{dU} = 2$. Whereas, for the states described by Eq. (3), we have $\alpha_R = 1 + 1/\sqrt{d}$. Thus the quantum steering condition reads

$$\mathcal{S}_{dU} > 1 + \frac{1}{\sqrt{d}}. \tag{7}$$

For any unsteerable states the measured kernel will not violate this bound. To determine the maximum value of the kernel supported by realistic theories, we consider the expectation value of the kernel $\mathcal{S}_{dU}$ for the state ρ_B (3). Then $\mathcal{S}_{dU}$ becomes

$$\mathcal{S}_{dU,R} = \sum_{i=1}^{2} \sum_{a_i=0}^{d-1} \sum_{\lambda} \mathrm{Tr}[U|a_i\rangle_{ii}\langle a_i|U^\dagger \rho_\lambda] P(\lambda|a_i) P(a_i).$$

This can be further manipulated to give

$$\begin{aligned}\mathcal{S}_{dU,R} &\leqslant \sum_{\lambda} P(\lambda)(\mathrm{Tr}[|m\rangle_{11}\langle m|\rho_\lambda] + \mathrm{Tr}[|n\rangle_{22}\langle n|\rho_\lambda]) \\ &\leqslant 1 + \frac{1}{\sqrt{d}},\end{aligned}$$

where $m,n \in \mathbf{v}$. The first inequality is derived by using the relation (4) about $P(\lambda)$, and the classical bound $\alpha_R = 1 + 1/\sqrt{d}$ is then obtained by determining the maximum eigenvalue of the operator $|m\rangle_{11}\langle m| + |n\rangle_{22}\langle n|$.

Our second steering condition is based on the mutual information between Alice and Bob. From the point of view of information shared between sender and receiver, the ability for Alice to steer Bob's state is confirmed if the mutual dependence between the measurement results of Alice and Bob is stronger than the dependence of Bob's measurement outcomes on the unknown states ρ_λ and ρ_B. This condition of steerability can be represented in terms of the mutual information as follows:

$$\sum_{i=1}^{2} I(B_{u(i)}; A_i) > \sum_{i=1}^{2} I(B_{u(i)}; \{\lambda\}). \tag{8}$$

From the basic definition of mutual information, Eq. (8) implies that

$$\sum_{i=1}^{2} \sum_{a_i=0}^{d-1} P(a_i) H(B_{u(i)}|a_i) < \sum_{i=1}^{2} \sum_{\lambda} P(\lambda) H(B_{u(i)}|\lambda).$$

Imposing the relation (5) on the state ρ_λ, we obtain the second steering condition of the form

$$\mathcal{S}_{\mathrm{ent}U} = -\sum_{i=1}^{2} \sum_{a_i=0}^{d-1} P(a_i)\, H(B_{u(i)}|a_i) > \log_2\left(\frac{1}{d}\right). \tag{9}$$

In addition to the steering conditions devised here, violating the temporal steering inequality [17] can serve as an indicator of single-system steering. In Appendix B, we show that this inequality can be derived from these same classical conditions (1) and (3), which provides a stricter interpretation to violations of that inequality. As shown therein, the steering conditions are related to practical quantum-information tasks and can be more useful than the temporal steering inequality alone, from a practical point of view. See Appendix C for a concrete demonstration of the sensitivity of these conditions.

In particular, one of the main advantages of the steering criteria is that they can be efficiently implemented in experiments. A *minimum* of two measurement settings are sufficient to measure the kernels $\mathcal{S}_{dU}$ and $\mathcal{S}_{\mathrm{ent}U}$. In addition, they are robust against noise, which is demonstrated in Appendix D (alongside an analysis of the robustness of the steering inequality for single systems).

B. Implications of the steering conditions

We have used a generic classical description of state preparation and transitions between states to derive the threshold α_R for our steering conditions. The allows us to use these conditions to certify quantum steering (EPR steering and single-system steering) when the measurement apparatus of Alice is uncharacterized or when both Alice's measurement device and the operation U are not trustworthy.

It is important to note that ruling out such a classical description, or mimicry, is equivalent to excluding the set of unsteerable states (3). Thus satisfying these conditions will deny, or rule out, processes that make states unsteerable. For example, it is possible that, while the measurement devices of Alice functions as well as expected, any processes that can change the states of particles from $\hat{a}_1$ and $\hat{a}_2$ to unknown states belonging to $\{\rho_\lambda\}$ will cause Alice to be ignorant about the true connection between her true measurement outcomes and Bob's states. Such state changes make Bob's state unsteerable, as described by Eq. (3).

In practical situations, one usually does not know the full information about the noise from the environment, or

other artificial effects which introduce an unknown source of randomness. The steering conditions (7) and (9) can certify the ability of Alice to steer the states of the particles eventually held by Bob, and then rule out third-party eavesdropping, classical mimicry of the channel, and any processes that make the transmitted particles unsteerable. Hence these steering conditions can be considered as an objective tool to evaluate the reliability of quantum communication and quantum computation.

IV. EXAMPLE APPLICATION TO QUANTUM COMMUNICATION

As an example of a practical application of our steering conditions in quantum communication we consider the following scenario. When the state of the qudit sent from Alice to Bob changes from the state $\hat{a}_i$ to a state $\mathcal{U}_{\text{real}}(\hat{a}_i)$ through a channel $\mathcal{U}_{\text{real}}$, the value of the kernel $\mathcal{S}_{dU}$ is

$$\mathcal{S}_{dU} = \sum_{i=1}^{2} \sum_{a_i=0}^{d-1} P(a_i)\, F(a_i, u(i)),$$

where the probabilities $P(a_i) = \text{Tr}[\rho_s \hat{a}_i]$ and the state fidelities [18] $F(a_i, u(i)) = \text{Tr}[\mathcal{U}_{\text{real}}(\hat{a}_i)\hat{a}_{u(i)}]$. Let us assume that an error is introduced by a quantum cloning machine [24] which copies equally well the states of both bases, $F(a_i, u(i)) = F$, for all $a \in \mathbf{v}$ [25]. If Alice wants to demonstrate steering of Bob's particle in the presence of such eavesdropping, they have to find $\mathcal{S}_{dU} = 2F > 1 + 1/\sqrt{d}$, or alternatively the state fidelity must satisfy the condition

$$F > \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right).$$

It is equivalent to saying that the disturbance, $D = 1 - F$, or error rate, has to be lower than a certain upper bound $D_{\text{ind}} = (1 - 1/\sqrt{d})/2$. This bound is exactly the same as the well-known security threshold [24].

For the second steering condition (9), we derive a second criterion on the state fidelity F [25]:

$$\tilde{F} > -\tfrac{1}{2}\log_2(d),$$

where $\tilde{F} \equiv F\log_2(F) + (1 - F)\log_2[(1 - F)/(d - 1)]$. This provides the upper bound, D_{coh}, on D under coherent attacks. If $D < D_{\text{coh}}$, then Alice can steer Bob's state. Interestingly, this bound D_{coh} exactly coincides with the existing result [24,26]. The above two conditions on F are summarized in Table I.

TABLE I. A summary of the steering conditions for quantum-information processing. The criteria derived from steering conditions for secure quantum communications and faithful quantum computations are represented in terms of the state fidelity F and the process fidelity F_{process}, respectively.

Condition	Communication	Computation
$\mathcal{S}_{dU} > 1 + \frac{1}{\sqrt{d}}$	$F > \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right)$	$F_{\text{process}} > \frac{1}{\sqrt{d}}$
$\mathcal{S}_{\text{ent}U} > \log_2\left(\frac{1}{d}\right)$	$\tilde{F} > -\frac{1}{2}\log_2(d)$	$F_{\text{process}} > 1 - 2D_{\text{coh}}$

V. EXAMPLE APPLICATION TO QUANTUM COMPUTATION

When the measured kernels $\mathcal{S}$ are larger than the maximum values α_R predicted by classical theories, the real process describing the state transitions $\mathcal{U}_{\text{real}}$ can be said to be close to the target unitary quantum operations $\mathcal{U}$ that Alice and Bob expect [27]. Validating such a unitary is a common, and sometimes difficult, task in quantum computation. To understand how to evaluate such a transformation using our steering conditions, we rewrite the condition (7) as

$$\frac{1}{d}\sum_{i=1}^{2}\sum_{a_i=0}^{d-1} \text{Tr}[\mathcal{U}_{\text{real}}(\hat{a}_i)\hat{a}_{u(i)}] > 1 + \frac{1}{d}.$$

Here, without losing any generality, we assume that $\rho_s = I/d$, where I is the identity matrix. The quantity

$$F_{\hat{a}_i \to \mathcal{U}(\hat{a}_i)} \equiv \frac{1}{d}\sum_{a=0}^{d-1} \text{Tr}[\mathcal{U}_{\text{real}}(\hat{a}_i)\hat{a}_{u(i)}]$$

can be considered as an average fidelity between $\mathcal{U}_{\text{real}}(\hat{a}_i)$ and $\hat{a}_{u(i)}$ over all the d states. With the average state fidelities $F_{\hat{a}_i \to \mathcal{U}(\hat{a}_i)}$ for the complementary bases A_1 and A_2, one can obtain the lower bound of the process fidelity $F_{\text{process}} \equiv \text{Tr}[\mathcal{U}_{\text{real}}\mathcal{U}]$ by $F_{\text{process}} \geqslant F_{\hat{a}_1 \to \mathcal{U}(\hat{a}_1)} + F_{\hat{a}_2 \to \mathcal{U}(\hat{a}_2)} - 1$ [28]. Hence, using the steering condition together with the above relation, we obtain a condition for a faithful quantum process in terms of process fidelity:

$$F_{\text{process}} > \frac{1}{d}.$$

Taking a two-qubit entangling gate for an example, this indicator coincides with the well-known criterion [28] in terms of the concurrence C [29]. Two qubits can be considered or recast as a single system with a level number $d = 2^2 = 4$. The entanglement capability of a two-qubit entangling gate, like a controlled-NOT operation, can be defined by the minimal amount of entanglement that can be generated by the real operation $\mathcal{U}_{\text{rel}}$. In terms of the concurrence C, a measure of quantum entanglement, it is found that $C \geqslant 2F_{\text{process}} - 1$ [28]. Then, for a nontrivial gate, one requires $C > 0$, which implies that $F_{\text{process}} > 1/2$. Our condition on F_{process} derived from the steering condition (7) coincides with this criterion. Note that the condition derived from the second steering condition (9) is $F_{\text{process}} > 62.14\%$, tighter than that resulted from the condition (7).

The above results can be efficiently implemented with a minimum of two measurement settings. This is especially useful to evaluate experimental quantum logic gates of arbitrary size, for example, an experimental three-qubit Toffoli gate with trapped ions [30]. For a three-qubit gate ($d = 2^3$), the condition on the process fidelity is $F_{\text{process}} > 1/\sqrt{8} \approx 35.36\%$. The process fidelity of the experimental quantum Toffoli gate with trapped ions reported in [30] is $F_{\text{process}} = 66.6(4)\%$, which can be identified as being functional according to our proposed criterion. When the number of qubits N increases, the classical bound will decrease with $\sqrt{d} = 2^{N/2}$ and approach zero when N is large.

The second steering condition (9) can be used to evaluate experimental quantum gates. When using the same conditions as D_{coh} to consider the quality of gate operations under

coherent attacks, one can obtain the condition on F_{process} in terms of D_{coh}:

$$F_{\text{process}} > 1 - 2D_{\text{coh}},$$

which is tighter than the criterion derived from the first condition (7). The relation $F = F_{\hat{a}_1 \to \mathcal{U}(\hat{a}_1)} = F_{\hat{a}_2 \to \mathcal{U}(\hat{a}_2)}$ is used above. Alternatively, the gate can be also qualified if the average state fidelity satisfies $F > 1 - D_{\text{coh}}$. Table I summarizes the above two conditions on F_{process}.

VI. EPR STEERING CONDITIONS AND APPLICATIONS

As discussed above, traditional EPR-steering and single-system-steering scenarios mirror each other. In the language we use, this can be understood from the fact that, by changing the role of λ [31], both steering conditions (7) and (9) can be used to detect EPR steering for *bipartite* d-level systems shared between Alice and Bob. See Appendix A 2 d. However, the converse is also true, such that EPR steering inequalities, for example, the inequalities used in the experiments [7,8], can serve as criteria for single-system steering (see Ref. [17] and Appendix B).

When using the bipartite counterpart of steering conditions (7) and (9) for quantum communication, one obtains security criteria for quantum channels that are the same as the single-system case, which can thus be considered as a d-level extension of 1SDI-QKD [6]. Similarly, the EPR steering conditions give criteria of computation performance for quantum gates realized in one-way modes [19]. A quantum gate U can be encoded in a bipartite maximally entangled state [32]:

$$|U\rangle = \frac{1}{\sqrt{d}} \sum_{a_i=0}^{d-1} |a_i\rangle_i |\text{Out}(a_i)\rangle,$$

where $|\text{Out}(a_i)\rangle \equiv U|\text{In}(a_i)\rangle$, and $|\text{In}(a_i)\rangle$ is the input state of the quantum gate U. A readout of the gate operation, $|\text{Out}(a_i)\rangle$, depends on the measurement result a_i, which is just the effect of EPR steering. See Appendix E for an application to a two-qubit gate realized in the one-way mode. Hence our EPR steering conditions can indicate reliable gate operations for experiments [33] in the presence of uncharacterized measurement devices.

The idea of bipartite steering conditions based on (7) and (9) can be straightforwardly generalized to genuine multipartite EPR steering. The main ingredient is to consider a kernel, from either the joint probabilities like Eq. (6) or the entropic conditions in Eq. (9), for a specific bipartition of a multipartite system. Then a complete kernel of a steering condition is composed of the joint probabilities, or entropic conditions, for all possible bipartitions of the multipartite system. See [16] for concrete examples for steering conditions based on (7). In particular, the entropic condition for genuine multipartite EPR steering using (9) could be useful for multipartite quantum secret sharing [34] when coherent attacks occur in the quantum network.

VII. CONCLUSION AND OUTLOOK

We investigated the concept of quantum steering for single quantum systems and pointed out its role in quantum information processing. We derived two steering conditions to certify such steering. These conditions ensure secure QKD using qudits and provide criteria for efficiently evaluating experimentally quantum logic gates of arbitrary computing size (see Table I). Moreover, the bipartite counterparts of our steering conditions can detect EPR steerability of bipartite d-level systems, and have practical uses for evaluating one-way quantum computing and quantum communication with entangled qudits and verifying genuine multipartite EPR steering. It may be interesting to investigate further the connection between single-system steering and other types of quantum steering such as one-way steering [10–12].

ACKNOWLEDGMENTS

This work was partially supported by the RIKEN iTHES Project, the MURI Center for Dynamic Magneto-Optics via the AFOSR Award No. FA9550-14-1-0040, the IMPACT program of JST, and a Grant-in-Aid for Scientific Research (A). C.-M.L. acknowledges the partial support from the Ministry of Science and Technology, Taiwan, under Grants No. MOST 101-2112-M-006-016-MY3 and No. MOST 104-2112-M-006 -016-MY3. Y.-N.C. was partially supported by the Ministry of Science and Technology, Taiwan, under Grant No. MOST 103-2112-M-006-017-MY4. N.L. was partially supported by the FY2015 Incentive Research Project.

APPENDIX A: COMPARING SINGLE-SYSTEM STEERING WITH EPR STEERING

In this section we compare EPR steering with single-system steering by discussing their basic assumptions and the classical mimicries, or simulation, of steering effects (Fig. 2). This provides a clear connection between EPR and single-system steering and the steering conditions for both cases discussed in our work. From this comparison, we show that classical mimicry or simulation can in both cases be considered as equivalent.

1. EPR steering for quantum-information processing (QIP)

Compared with the single-system steering [Fig. 2(a)], the scenario of EPR steering also consists of two steps: First, Alice generates a bipartite entangled system from an entanglement source (sometimes termed an EPR source) [Fig. 2(b)]. To have a concrete comparison, let us assume that this entangled state is of the form

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{a_1=b_1=0}^{d-1} |a_1\rangle_{A1} \otimes |b_1\rangle_{B1} \tag{A1}$$

where $\{|a_1\rangle_{A1} \equiv |a_1\rangle_1 | a_1 \in \mathbf{v}\}$ and $\{|b_1\rangle_{B1} \equiv |b_1\rangle_1 | b_1 \in \mathbf{v}\}$.

Second, Alice keeps one particle of the entangled pair and sends the other particle to Bob. A subsequent unitary operator U is applied on Bob's subsystem according to the instructions of Alice. This transformation can be done either by Bob after receiving the particle, or by Alice herself before the transmission of the particle. After such a transformation,

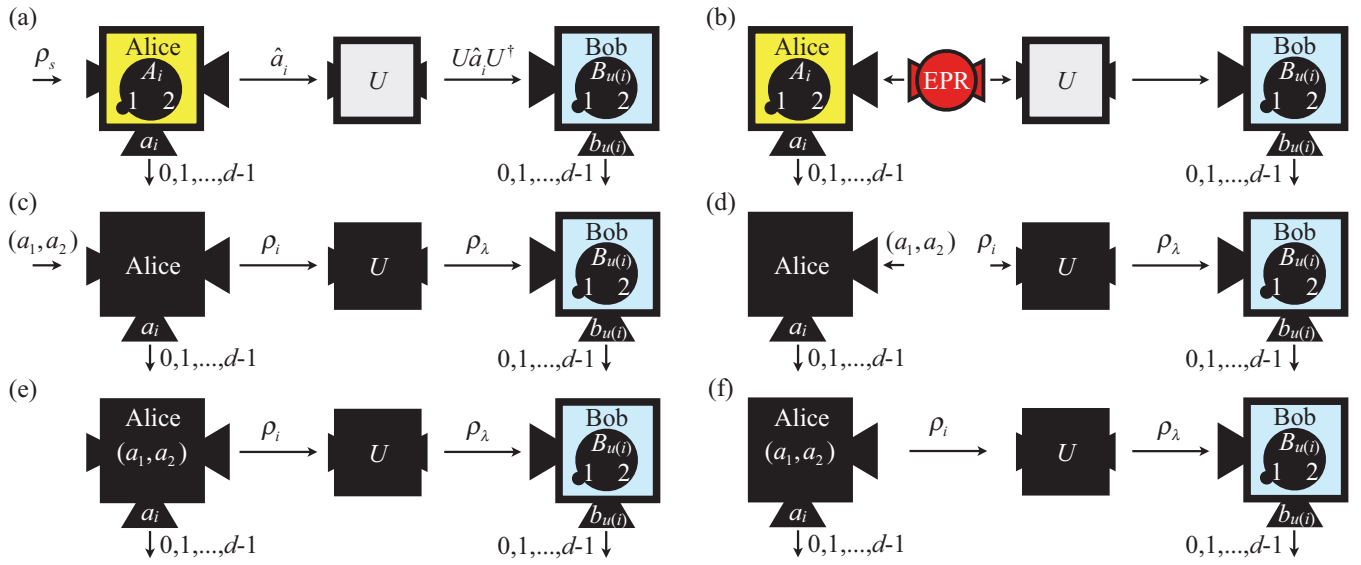

FIG. 2. (Color online) Comparison between single-system steering and EPR steering. We compare these two scenarios by, first, their basic concepts of ideal single-system steering (a) and ideal EPR steering (b), and, second, classical mimics of single-system steering (c),(e) and EPR steering (d),(f). For the ideal case, Alice can use the effect of EPR steering, by sharing the entangled states (EPR source), to implement the operation U on the state of Bob's qudit. While the resources utilized for quantum steering are different, the state of the particle finally held by Bob can be steered into a corresponding quantum state, $U\hat{a}_i U^\dagger$, for both quantum steering scenarios. To distinguish classical mimicry from genuine quantum steering, the respective classical models based on realistic theories (c) and (d) are introduced. These "classical simulations" can be concretely represented in the practical descriptions of, for example, unqualified measurements of Alice and the unqualified operation U performed by Alice or Bob [(e) and (f)]. As shown in (e) and (f), these effective simulations are equivalent.

the state vector of the bipartite system becomes

$$(I \otimes U)|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{a_1=b_1=0}^{d-1} |a_1\rangle_{A1} \otimes U|b_1\rangle_{B1}.$$

Then, depending on Alice's measurement result a_1, the state of the particle finally held by Bob can be steered into a corresponding quantum state, $U\hat{a}_1 U^\dagger$, which is the same as the result derived from single-system steering. When the state $|\Phi\rangle$ is represented in the bases $\{|a_2\rangle_{A2} \equiv |a_2\rangle_2 | a_2 \in \mathbf{v}\}$ and $\{|b_2\rangle_{B2} \equiv |b_2\rangle_2 | b_2 \in \mathbf{v}\}$, we have

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{a_2+b_2 \doteq 0} |a_2\rangle_{A2} \otimes |b_2\rangle_{B2}, \tag{A2}$$

where $\doteq$ denotes equality modulo d. Through the same method as that shown above, Alice can steer the state of Bob's particle into the quantum state, $U\hat{b}_2 U^\dagger$, by the measurement on her subsystem with a result a_2 satisfying the correlation $a_2 + b_2 \doteq 0$.

We remark that, for an EPR source creating entangled states that are different from $|\Phi\rangle$, the transformation U could be implemented in other ways. For example, when Alice and Bob share bipartite supersinglets [35], which are expressed as

$$|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{a_i+b_i=d-1} (-1)^{a_i} |a_i\rangle_{Ai} \otimes |b_i\rangle_{Bi}, \tag{A3}$$

for $i = 1,2$, Alice can steer the state of Bob by directly measuring her qudit in a basis featured in U. Since supersinglets are rotationally invariant [35], i.e., $(R \otimes R)|\Psi\rangle = |\Psi\rangle$, where R is a rotation operator, Alice's measurement in the basis $\{R|a_i\rangle_i\}$ will steer the state of Bob's qudit into a corresponding state, $R|b_i\rangle_i$, for $a_i + b_i = d - 1$. For $d = 2$, supersinglets become unitary invariant and provide a resource for implementing any unitary transformations U to Bob's qubit.

2. Steering conditions

For both ideal single-system and EPR steering scenarios, the state received by Bob, $\hat{b}_i$, is the same as or perfectly correlated with the initial state $\hat{a}_i$ prepared by Alice under the transformation U. However, for Bob's limited knowledge about the measurements used or the particle prepared by Alice, her measurement results become untrusted to Bob. He is uncertain whether these measurements and state preparation are qualified. In the worst case where Alice's measurement outcomes may be randomly generated from her apparatus, classical simulations then can describe Alice's measurement results. To show that Alice has true steerability in practical situations, we introduced the steering conditions (7) and (9), to distinguish genuinely quantum steering from classical mimicry. In what follows, we will detail this classical mimicry and its implication for practical applications. With these examples, it will be clear that the proof for single-system conditions can be seen as equivalent to that used in the derivation of EPR steering conditions.

a. Mimicry of single-system steering

In the case of single-system steering, as detailed in the main text, the classical mimicry of steering is based on the realistic assumptions that (1) the state of the particle sent by Alice can be described by a fixed set (a_1,a_2), and (2) the state can change from (a_1,a_2) to another state λ which corresponds to a quantum state of the qudit ρ_λ finally held by Bob; see

Fig. 2(c). In order to see this mimicry from a practical point of view, one can think that, for example, such a situation arises as a result of the unqualified measurement device and the states of particles sent to Bob. For some reason, Alice's measurement apparatus does not properly output real measurement results a_i but randomly generates outcomes with a distribution $P(a_1,a_2)$ [see Eq. (1)] that correspond to some output states ρ_i when the measurement setting i is chosen by Alice. After the unqualified operation U, the state ρ_i becomes the unknown state ρ_λ which constitutes an unsteerable state ρ_B [Eq. (3)]. Here the joint probability of finding (a_1,a_2) and observing λ as the final state satisfies the classical relation (2). It is equivalent to say that Alice can consider the joint set (a_1,a_2), with the probability of occurrence $P(a_1,a_2)$, as describing predetermined instructions for her to prepare and send a particle with final quantum state ρ_λ to Bob. See Fig. 2(e).

It is also possible that the operation U is qualified but the measurement device of Alice is not. The two realism assumptions are applicable to this case as well. The above classical mimicry scenario can be recast such that the output states ρ_i already correspond to the unknown state $\rho_\lambda^{(0)}$; see Fig. 3(a). It does not matter what the subsequent qualified operation on the particle U is, the final states held by Bob ρ_λ constitute an unsteerable state ρ_B. From a practical point of view, similarly, one can think that Alice's measurement apparatus randomly generates outcomes with the probability of occurrence $P(a_1,a_2)$ that correspond to unknown output states $\rho_\lambda^{(0)}$ [Fig. 3(c)].

b. Mimicry of EPR steering

The above scheme for mimicking single-system steering can be readily mapped to the case of EPR steering. Here, the mimicry of EPR steering depends on two similar assumptions: (1) the state of the particle held by Alice can be described by a fixed set obeying realism (a_1,a_2), and (2) a given set (a_1,a_2) corresponds to some quantum state, ρ_λ, of the qudit finally held by Bob; see Fig. 2(d). The unqualified bipartite state shared between her and Bob, and a subsequent unqualified operation, can result in such assumptions. For example, let us assume that the entanglement source does not create entangled pairs but a qudit with state ρ_i for Bob and another separable particle for Alice instead. For the state ρ_i there is a corresponding measurement setting i chosen by Alice, for which Alice's measurement device creates an output of a random signal with a distribution described by the probability $P(a_1,a_2)$ (1). The subsequent operation U takes ρ_i to an unknown state ρ_λ, and then the final state held by Bob is unsteerable (3). The classical relation (2) is again applicable to this transition between states. Here it is reasonable to incorporate the entanglement source into the measurement apparatus as a single unqualified experiment setup for Alice. See Fig. 2(f). Then it is effectively a scenario where Alice observes a set (a_1,a_2) appearing with probability $P(a_1,a_2)$ which creates a particle with a final quantum state ρ_λ for Bob.

As discussed in the above mimicry of single-system steering, it is possible that the operation U is qualified but Alice's measurement apparatus, including the EPR source, is not. In this case one can effectively consider that the unqualified EPR source outputs a fixed set (a_1,a_2) for Alice's particle and a qudit that is already in an unknown state $\rho_i = \rho_\lambda^{(0)}$ for Bob [Fig. 3(b)]. For any qualified operation U on the particle state $\rho_\lambda^{(0)}$, the final state held by Bob is still unsteerable. From the same practical point of view as introduced above, we can think that the joint set (a_1,a_2), with the probability of occurrence $P(a_1,a_2)$, resulting from the random outcomes of Alice's device, corresponds to a particle with final quantum state ρ_λ for Bob; see Fig. 3(d). It is clear that the joint probability of finding (a_1,a_2) and observing λ as the final state in this case satisfies the classical relation (2).

c. Equivalence between the steering mimicries

With the above concrete explanations of the classical mimicry for both the single-system steering and EPR steering, one can interpret these two classical scenarios as being equivalent to each other. See Figs. 2(e) and 2(f) and Figs. 3(c) and 3(d). Following the same approach based on the realistic assumptions and their practical scenarios, in what follows we will discuss two more cases to complete the proof of the equivalence between the steering mimicries.

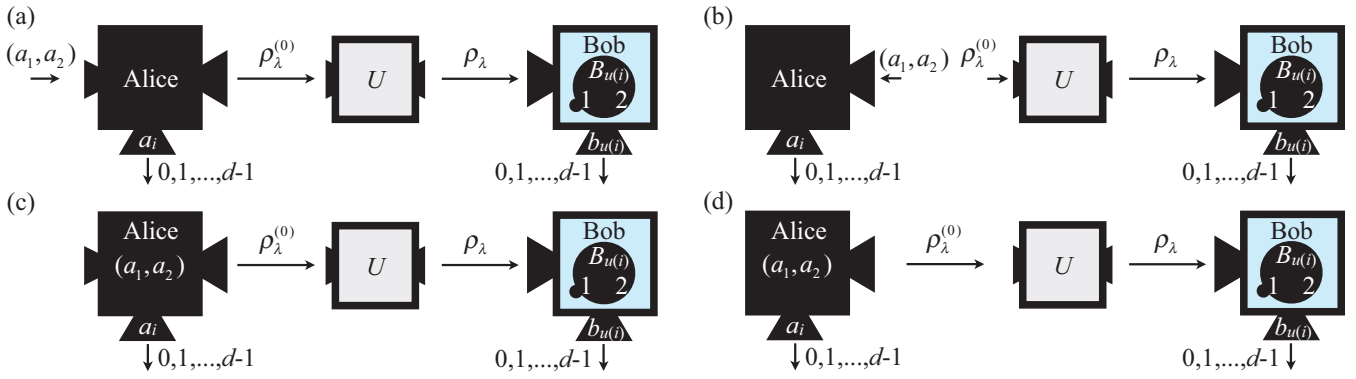

FIG. 3. (Color online) Steering mimicries where the operation U is qualified but the measurement device of Alice is not. The classical mimics of single-system steering (a) and EPR steering (b) are based on the realistic assumptions that (1) the state of the particle sent by Alice can be described by a fixed set (a_1,a_2), and (2) the state can change from (a_1,a_2) to another state λ which corresponds to a quantum state of the qudit ρ_λ finally held by Bob. One can concretely represent these scenarios in the practical descriptions of unqualified Alice's apparatus (c) and (d), respectively. These concrete simulations are then shown to be equivalent.

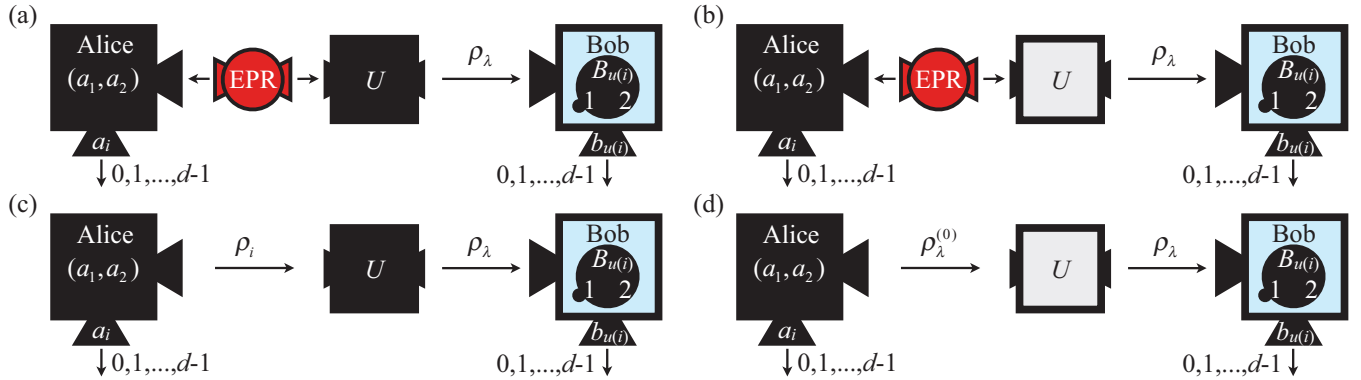

FIG. 4. (Color online) Mimicries of EPR steering where the EPR source is qualified but the measurement device of Alice is not. (a) The unqualified operation is used, and (b) the operation used is qualified in the mimicry. These two possible situations can be described by the two realism conditions and represented in practical descriptions (c) and (d), respectively. The demonstration (c) has the analog of single-system steering described by Fig. 2(e). The concrete mimicry (d) is equivalent to that of single-system steering depicted in Fig. 3(c).

The case where Alice's measurement apparatus is unqualified, while the EPR source functions as expected, can raise two other possible scenarios which again can be shown to be covered by "realism" assumptions. Figure 4(a) depicts one of the possibilities. As the operation U is unqualified, one can practically think that Alice's measurement apparatus generates random outcomes with a distribution $P(a_1,a_2)$, independent of the entangled pair generated from the EPR source. The subsequent operation makes the state of the qudit of the entangled pair sent to Bob, say ρ_i, change to ρ_λ as illustrated by Fig. 4(c). It is clear that such mimicry of EPR steering is equivalent to the simulation of single-system steering described by Fig. 2(e) [see also Fig. 2(c)].

Figure 4(b) illustrates the other situation where the entanglement source and the operation U are qualified but Alice's measurement apparatus is not. A possible concrete example for this case is the following. The unqualified measurement device of Alice always measures her particle of the entangled pair, say $|\Phi\rangle$, in the first basis $\{|a_1\rangle_1 | a_1 \in \mathbf{v}\}$ intrinsically whatever measurement setting Alice chooses, and it announces random signals a_1 or a_2 as an outcome. Such a measurement, combined with the random signals, make the state of the qudit sent to Bob unsteerable, i.e., $\rho_i = \rho_\lambda^{(0)}$ belongs to the same set $\{|b_1\rangle_1 | b_1 \in \mathbf{v}\}$ whatever measurement setting chosen by Alice and as such then constitutes an unsteerable state ρ_B after the operation U; see Fig. 4(d). This is an analog of EPR-steering mimicry to that of single-system steering described by Fig. 3(c) [see also Fig. 3(a)].

d. EPR steering conditions for QIP

As shown above, the mimicry of single-system steering is equivalent to that mimicking EPR steering. Then the steering conditions (7) and (9) derived for single systems can be mapped onto, and subsequently be used for verification of, EPR steering for bipartite d-dimensional systems. Then, such EPR steering conditions can certify the reliability of QIP scenarios where entangled pairs are shared between Alice and Bob. When the state $|\Phi\rangle$ is used to mediate steering the EPR steering condition that corresponds to (7) is of the form

$$\mathcal{S}_{dU\Phi}^{(\mathrm{EPR})} \equiv \sum_{a_1=b_{u(1)}=0}^{d-1} P(a_1,b_{u(1)}) + \sum_{a_2+b_{u(2)}\doteq 0} P(a_2,b_{u(2)}) > 1+\frac{1}{\sqrt{d}}. \quad \text{(A4)}$$

Similarly, with proper changes to the above joint probabilities, we have the following steering condition for supersinglets:

$$\mathcal{S}_{dR\Psi}^{(\mathrm{EPR})} \equiv \sum_{a_{u(1)}+b_{u(1)}=d-1} P(a_{u(1)},b_{u(1)}) + \sum_{a_{u(2)}+b_{u(2)}=d-1} P(a_{u(2)},b_{u(2)}) > 1+\frac{1}{\sqrt{d}}, \quad \text{(A5)}$$

where, for Alice who implements quantum measurements, the measurement outcomes $\{a_{u(i)}\}$ result from the measurement described by the basis $\{|a_{u(i)}\rangle_{u(i)} \equiv R|a_i\rangle_i | a_{u(i)} = a_i \in \mathbf{v}\}$. Here Bob uses the same measurements as those used by Alice. For the EPR steering conditions represented in the entropic forms, we have

$$\mathcal{S}_{\mathrm{ent}U\Phi}^{(\mathrm{EPR})} \equiv -\sum_{i=1}^{2}\sum_{a_i=0}^{d-1} P(a_i)\, H(B_{u(i)}|a_i) > \log_2\left(\frac{1}{d}\right), \quad \text{(A6)}$$

for the state $|\Phi\rangle$ shared by Alice and Bob, and

$$\mathcal{S}_{\mathrm{ent}R\Psi}^{(\mathrm{EPR})} \equiv -\sum_{i=1}^{2}\sum_{a_{u(i)}=0}^{d-1} P(a_{u(i)})\, H(B_{u(i)}|a_i) > \log_2\left(\frac{1}{d}\right), \quad \text{(A7)}$$

for the supersinglets.

As detailed above, the mimicry of single-system steering based on realistic theories is equivalent to that of EPR steering where Alice's outcomes follow realist theories but Bob performs quantum measurements. Hence the proof for the conditions (7) and (9) can be readily applied to the above EPR steering conditions. In addition, following the same analysis of quantum communication based on single-system steering

as introduced in the main text, these bipartite counterparts of steering conditions provide security criteria for quantum channels that are equivalent to the single-system cases.

APPENDIX B: EPR STEERING INEQUALITY FOR SINGLE-SYSTEM STEERING

The classical condition (1) and its implications, Eqs. (2) and (3), provide a strict meaning of violating the single-system analog of the EPR steering inequality used in the experiment of Smith *et al.* [8], i.e., the temporal steering inequality introduced in [17]. The kernel of this steering inequality reads

$$S_N \equiv \sum_{i=1}^{N} E\left[\left\langle B_{i,t_B}\right\rangle^2_{A_{i,t_A}}\right], \tag{B1}$$

where

$$E\left[\left\langle B_{i,t_B}\right\rangle^2_{A_{i,t_A}}\right] = \sum_{a=0}^{1} P(A_{i,t_A}=a)\left\langle B_{i,t_B}\right\rangle^2_{A_{i,t_A}=a} \tag{B2}$$

and $N=2$ or 3 is the number of measurement for Alice and Bob. The probability of measuring $A_i=a$ at the time t_A is denoted by $P(A_{i,t_A}=a)$. The expectation value about Bob's measurement at the time t_B, conditioned on the measurement result of Alice, is defined by

$$\left\langle B_{i,t_B}\right\rangle_{A_{i,t_A}=a} = \sum_{b=0}^{1}(-1)^b\, P\left(B_{i,t_B}=b\middle|A_{i,t_A}=a\right).$$

To obtain the upper bound derived from generic classical means, we first introduce the final state of Bob's particle (3) into the above equation and then have

$$\begin{aligned}\left\langle B_{i,t_B}\right\rangle_{A_{i,t_A}=a} &= \sum_{b=0}^{1}(-1)^b\sum_{\lambda}P\left(B_{i,t_B}=b|\lambda\right)P\left(\lambda|A_{i,t_A}=a\right)\\ &= \sum_{\lambda}P\left(\lambda|A_{i,t_A}=a\right)\left\langle B_{i,t_B}\right\rangle_{\lambda}.\end{aligned}$$

Then it is clear that

$$\begin{aligned}&E\left[\left\langle B_{i,t_B}\right\rangle^2_{A_{i,t_A}}\right]\\ &\leqslant \sum_{a=0}^{1}P\left(A_{i,t_A}=a\right)\sum_{\lambda}P\left(\lambda|A_{i,t_A}=a\right)\left\langle B_{i,t_B}\right\rangle^2_{\lambda}.\end{aligned}$$

Second, we use the result (4) derived from the criterion on state transition (2) in the main text to obtain

$$P(\lambda)=\sum_{a=0}^{1}P\left(A_{i,t_A}=a\right)P\left(\lambda|A_{i,t_A}=a\right),$$

for all measurements i. The temporal inequality is

$$S_N \leqslant \sum_{i=1}^{N}\sum_{\lambda}P(\lambda)\left\langle B_{i,t_B}\right\rangle^2_{\lambda} \leqslant \sum_{\lambda}P(\lambda)=1.$$

Thus $S_N>1$ can be considered as a condition for single-system steering and deny processes that make states unsteerable.

APPENDIX C: COMPARISON BETWEEN STEERING CONDITIONS AND THE TEMPORAL STEERING INEQUALITY

One of the main differences between the steering conditions and the temporal steering inequality is in their practical applications to quantum-information tasks. In what follows we will illustrate a simple example to show that, compared with the temporal steering inequality, the steering conditions can fulfill certain requirements so as to be useful as checks for the reliability of QIP.

Let us assume that a source generates particles in the state $\rho_s=|0\rangle_{11}\langle 0|$ for Alice's subsequent use for steering. The task of Alice and Bob is to perform an identity operation I, or alternatively, to maintain the states of the particles during the particle transmission. For such an information task, the steering condition (7) for $d=2$ and $U=I$ used by them to check the steerability can be of the form

$$\mathcal{S}_{2I}\equiv\sum_{a_1=b_1=0}^{1}P(a_1,b_1)+\sum_{a_2=b_2=0}^{1}P(a_2,b_2)>1+\frac{1}{\sqrt{2}}.$$

When the particles are transmitted without any disturbance, they will have $\mathcal{S}_{2I}=2$. To concretely show the undesired situation, e.g., a wrong gate operation in quantum computation, or an unwanted interaction between the qubit and the quantum channel in quantum communication, we assume that there exists an effective operation $X=|0\rangle_{11}\langle 1|+|1\rangle_{11}\langle 0|$ on the qubit such that the final state of the qubit held by Bob is $X|b_i\rangle_i$. Such an operation can make the qubit flip when the state is prepared in $|0\rangle_1$ or $|1\rangle_1$. Then the value of the kernel $\mathcal{S}_{2I}$ becomes $\mathcal{S}_{2I}=1$, i.e., the reliability of the qubit state is not certified by the steering condition (7).

Using the same number of measurement settings ($N=2$), the temporal steering inequality is still violated by $S_N=2$, and this cannot reveal the real effect of a qubit flip on the particle during transmission. Hence, the present form of the temporal steering inequality cannot be used in practical quantum-information tasks, while our steering conditions can because of their stricter behavior. However, after properly revising the kernel S_N by introducing a quantum operation U, the revised version of the temporal inequality also can serve the same role as the steering conditions. Its derivation and experimental demonstrations will be detailed elsewhere.

The above consideration is also true for the bipartite nonlocal counterpart. When Alice and Bob share the state $|\Phi\rangle=\frac{1}{\sqrt{2}}\sum_{a_1=b_1=0}^{1}|a_1\rangle_{A1}\otimes|b_1\rangle_{B1}$ to perform the same task as above, they can certify the reliability by using the steering condition (A4) for $d=2$ and $U=I$,

$$\mathcal{S}^{(\mathrm{EPR})}_{dU\Phi}\equiv\sum_{a_1=b_1=0}^{1}P(a_1,b_1)+\sum_{a_2=b_2=0}^{1}P(a_2,b_2)>1+\frac{1}{\sqrt{2}}.$$

If there is a bit flip error in the transmission of Bob's qubit, then the state suffering from such effect $(I\otimes X)|\Phi\rangle$ cannot give results that satisfy the above condition to act as a reliability check ($\mathcal{S}^{(\mathrm{EPR})}_{dU\Phi}=1$) but still can violate the inequality ($S_N=2>1$). Then, the EPR steering inequality cannot respond to the effect of a qubit flip in the bipartite nonlocal scenario.

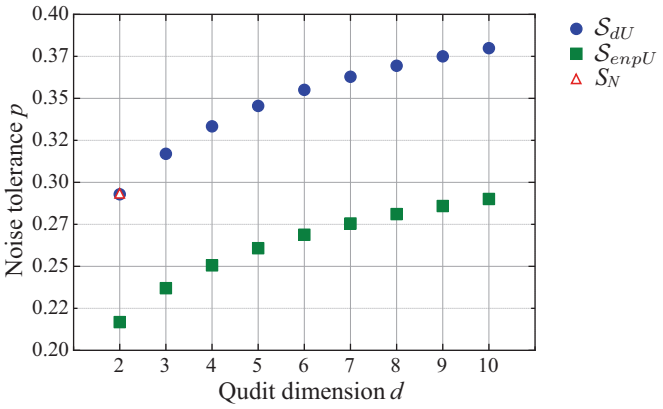

FIG. 5. (Color online) Noise tolerance of steering conditions (7) and (9). If the probability of white nose $p_{\text{noise}} < p$, then the single-system steering, that underlies the qudits sent by Alice with the states $\rho_i(a_i, p_{\text{noise}})$, can be certified by the steering conditions (7) or (9). Here the threshold of noise intensity p is an indicator showing the noise tolerance of these steering criteria. Note that the noise tolerance of the certification based on violating the EPR steering inequality, i.e., $S_N > 1$, implemented with two measurement settings ($N = 2$) is the same as that of the steering condition (7) for two-dimensional systems (the EPR steering inequality introduced by Smith *et al.* [8] is applicable to $d = 2$ only). For large d, both the conditions (7) and (9) are robust against noise up to $p = 50\%$.

APPENDIX D: ROBUSTNESS OF STEERING CONDITIONS

We consider the following scenario to determine the robustness of the proposed steering conditions. Let us suppose that in the presence of white noise the pure state $|a_i\rangle_i$ of the qudit prepared by Alice's measurements will become

$$\rho_i(a_i, p_{\text{noise}}) = \frac{p_{\text{noise}}}{d} I + (1 - p_{\text{noise}})\hat{a}_i, \tag{D1}$$

where p_{noise} is the probability of uncolored noise. Then the steerability revealed by using the qudits with states $\rho_i(p_{\text{noise}})$ is certified by our steering conditions if the intensity of uncolored noise p_{noise} is smaller than some noise threshold, $p_{\text{noise}} < p$. Here p can be considered as an indicator showing the noise tolerance of the steering conditions; see Fig. 5. We determine the noise threshold p by considering the critical noise intensity such that $\mathcal{S}(p_{\text{noise}}) = \alpha_R$. For the steering condition (7), we have

$$p = \frac{\left(1 - \frac{1}{\sqrt{d}}\right)}{2\left(1 - \frac{1}{d}\right)}, \tag{D2}$$

which shows that the steering condition is robust and the noise is even tolerable up to $p = 50\%$ for large d. The robustness of the steering condition (9) is similar to that of the condition (7), and its noise tolerance in terms p also can be up to $p = 50\%$ for large d.

APPENDIX E: EPR STEERING FOR ONE-WAY QUANTUM COMPUTING

A cluster state can be represented by an array of vertices, where each vertex is initially in the state of $(|0\rangle + |1\rangle)/\sqrt{2}$ where $|0\rangle$ and $|1\rangle$ constitutes an orthonormal basis. Every connected line (edge) between vertices realizes a controlled-phase (CPHASE) gates acting as $|m\rangle \otimes |n\rangle \to \omega^{mn}|m\rangle \otimes |n\rangle$, where $\omega = \exp(i2\pi/2)$ and $m,n \in \{0,1\}$ [19]. In the present illustration, we consider a four-qubit chain-type cluster state of the form

$$|C_4\rangle = \sum_{m=0}^{1}\sum_{n=0}^{1}\sum_{j=0}^{1}\sum_{k=0}^{1} \omega^{mn+nj+jk}|n\rangle_{A_1} \times \otimes |j\rangle_{A_2} \otimes |m\rangle_{B_1} \otimes |k\rangle_{B_2} \tag{E1}$$

where $|q\rangle_{A_l} = |q\rangle_{B_r} \equiv |q\rangle$ for $q = 0,1$ and $l,r = 1,2$. The state $|C_4\rangle$ represented in a horseshoe graph is shown in Fig. 6(a). Here we assume that Alice holds two of the qubits, A_1 and A_2, and Bob has the rest, B_1 and B_2.

When sharing such a genuine four-partite entangled state between them, Alice's quantum measurements on her qubits can realize a quantum gate operation U on the state of the qubits held by Bob:

$$U = (H \otimes H)\text{CPHASE}, \tag{E2}$$

where H is the Hadamard operation; see Fig. 6(b). To clearly see the gate operation realized in this one-way model, we

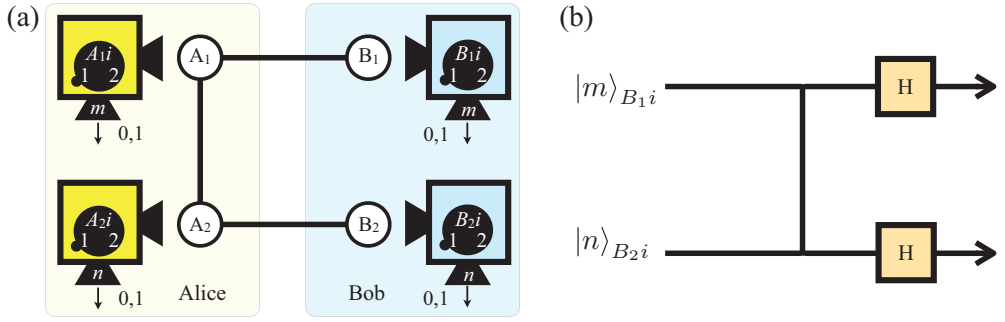

FIG. 6. (Color online) EPR steering for one-way quantum computing. (a) A genuine four-qubit chain-type cluster state shared by Alice and Bob is represented by a fully connected horseshoe graph. Alice, who performs the measurements $A_1 i$ and $A_2 i$ for $i = 1,2$ on her qubits A_1 and A_2, respectively, can reveal the EPR steering effect to realize the gate operation U on the qubits of Bob B_1 and B_2. (b) The state $|m\rangle_{B_1 i} \otimes |n\rangle_{B_2 i}$ is an input of the quantum gate U composed of one two-qubit CPHASE gate and two single-qubit Hadamard operations. For one-way quantum computing, the outcomes of Alice's measurements, m and n, corresponding to the postmeasurement state $|m\rangle_{A_1 i} \otimes |n\rangle_{A_2 i}$, determines the output state of the gate operation, $U(|m\rangle_{B_1 i} \otimes |n\rangle_{B_2 1 i})$.

rephrase the state vector of $|C_4\rangle$ in the following form:

$$|C_4\rangle = \sum_{m=0}^{1}\sum_{n=0}^{1} |m\rangle_{A_1 1} \otimes |n\rangle_{A_2 1} \otimes U\left(|m\rangle_{B_1 1} \otimes |n\rangle_{B_2 1}\right) \quad \text{(E3)}$$

where $|q\rangle_{A_l 1} = |q\rangle_{B_r 1} \equiv (|0\rangle + (-1)^q|1\rangle)/\sqrt{2}$ for $q = 0,1$ and $l,r = 1,2$. One can consider the state $|m\rangle_{B_1 1} \otimes |n\rangle_{B_2 1}$ as an input of the quantum gate U. Then the outcomes of Alice's measurements $A_1 1$ and $A_2 1$, m and n, corresponding to the post measurement state $|m\rangle_{A_1 1} \otimes |n\rangle_{A_2 1}$, determines the output state of the gate operation, $U(|m\rangle_{B_1 1} \otimes |n\rangle_{B_2 1})$. For example, as Alice performs measurements and has the results $m = 0$ and $n = 0$, the state of Bob's qubits $(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)/2$ will be transformed by U into an entangled state $(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle)/2$. Alice can perform different measurements to transform input states prepared in different basis by the same gate operation U. The cluster state also can be of the form

$$|C_4\rangle = \sum_{m=0}^{1}\sum_{n=0}^{1} |m\rangle_{A_1 2} \otimes |n\rangle_{A_2 2} \otimes U\left(|m\rangle_{B_1 2} \otimes |n\rangle_{B_2 2}\right) \quad \text{(E4)}$$

where $|q\rangle_{A_l 2} = |q\rangle_{B_r 2} \equiv (|0\rangle + (-1)^q i|1\rangle)/\sqrt{2}$ for $q = 0,1$ and $l,r = 1,2$.

Through the connection between Alice's measurements on her qubits and the resulting states of Bob's qubits as illustrated above, one can think of the quantum gate U as being encoded in a bipartite maximally entangled state

$$|U\rangle = \frac{1}{2}\sum_{a_i=0}^{3} |a_i\rangle_i \otimes |\mathrm{Out}(a_i)\rangle, \quad \text{(E5)}$$

where $|a_i\rangle_i \equiv |m\rangle_{A_1 i} \otimes |n\rangle_{A_2 i}$ with $a_i = m \times 2^1 + n \times 2^0$ and $|\mathrm{Out}(a_i)\rangle \equiv U|\mathrm{In}(a_i)\rangle$, and $|\mathrm{In}(a_i)\rangle \equiv |m\rangle_{B_1 i} \otimes |n\rangle_{B_2 i}$ is the input state of the quantum gate U. Hence the effect of EPR steering reveals that a readout of the gate operation, $|\mathrm{Out}(a_i)\rangle$, depends on the measurement result a_i.

Our EPR steering conditions serves as a useful tool to identify reliable gate operations for experiments in the presence of uncharacterized (or untrusted) measurement devices. For example, for the above concrete case, we have the following EPR steering conditions:

$$\mathcal{S}^{(\mathrm{EPR})}_{dUC_4} \equiv \sum_{a_1=b_{u(1)}=0}^{3} P(a_1, b_{u(1)}) + \sum_{a_2=b_{u(2)}=0}^{3} P(a_2, b_{u(2)}) > 3/2, \quad \text{(E6)}$$

where $\{b_{u(i)}\}$ denotes the results obtained from Bob's measurement specified by $\{|b_{u(i)}\rangle_{u(i)} \equiv U|\mathrm{In}(b_i)\rangle | b_{u(i)} = b_i \in \mathbf{v}\}$. It is easy to find that the kernel $\mathcal{S}^{(\mathrm{EPR})}_{dUC_4}$ and its condition for EPR steering are exactly the same as their single-system analogs (6) and (7).

It is worth noting that the idea of bipartite EPR steering effects and the steering condition (E6) for one-way quantum computing is rather different from that based on genuine multipartite EPR steering [16]. The present steering condition detects EPR steering with respect to the fixed bipartite splitting of the four qubits A_1, A_2 and B_1, B_2. When certifying *genuine* four-partite EPR steering for one-way quantum computing, one needs the concept and method introduced in [16] to consider and verify quantum steering with respect to all bipartite splittings of the four qubits.

[1] E. Schrödinger, Naturwissenschaften **23**, 807 (1935); **23**, 823 (1935); **23**, 844 (1935).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[3] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

[4] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).

[5] P. Skrzypczyk, M. Navascues, and D. Cavalcanti, Phys. Rev. Lett. **112**, 180404 (2014).

[6] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).

[7] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Nat. Phys. **6**, 845 (2010).

[8] D.-H. Smith, G. Gillett, M. P. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H. M. Wiseman, S. W. Nam, and A. G. White, Nat. Commun. **3**, 625 (2012).

[9] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, and A. Zeilinger, New J. Phys. **14**, 053030 (2012).

[10] S. L. W. Midgley, A. J. Ferris, and M. K. Olsen, Phys. Rev. A **81**, 022101 (2010).

[11] M. K. Olsen, Phys. Rev. A **88**, 051802 (2013).

[12] J. Bowles, T. Vértesi, M. T. Quintino, and N. Brunner, Phys. Rev. Lett. **112**, 200402 (2014).

[13] Q. Y. He and M. D. Reid, Phys. Rev. Lett. **111**, 250403 (2013).

[14] S. Armstrong, M. Wang, R. Y. Teh, Q. Gong, Q. He, J. Janousek, H.-A. Bachor, M. D. Reid, and P. K. Lam, Nat. Phys. **11**, 167 (2015).

[15] D. Cavalcanti, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. Souto Ribeiro, and S. P. Walborn, Nat. Commun. **6**, 7941 (2015).

[16] C.-M. Li, K. Chen, Y.-N. Chen, Q. Zhang, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett. **115**, 010402 (2015).

[17] Y.-N. Chen, C.-M. Li, N. Lambert, S.-L. Chen, Y. Ota, G.-Y. Chen, and F. Nori, Phys. Rev. A **89**, 032112 (2014).

[18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[19] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001); R. Raussendorf and H. J. Briegel, *ibid.* **86**, 5188 (2001).

[20] In normal EPR steering, Alice can steer Bob's state into arbitrary target states only when the pair of particles are entangled and she knows the state structure of the entangled pair shared between them. The state information enables Alice to choose a proper measurement basis to demonstrate steering. This is the same

for single-system steering. Such an equivalence means that, with steering conditions alone, Bob cannot tell whether his quantum system is one part of the entangled pair or a single particle preprepared and sent from Alice (though a scheme can be devised to distinguish these two [17], as can a case-by-case analysis of the allowed correlations between measurement results [21]). As with the role of entanglement played in EPR steering, the essence of single system *steerability* is the quantum characteristics of the states $\hat{a}_i$, for example, quantum coherence and uncertainty relations.

[21] K. Ried, M. Agnew, L. Vermeyden, D. Janzing, R. W. Spekkens, and K. J. Resch, Nat. Phys. **11**, 414 (2015).

[22] Here we have utilized the relation $P(\lambda,a_j|a_i) = P(a_j|a_i)P[\lambda|(a_1,a_2)] = P(\lambda|a_i)P(a_j|\lambda,a_i)$. The transition probability $P[\lambda|(a_1,a_2)]$ is then connected with the individual transition probability $P(\lambda|a_i)$.

[23] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[24] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[25] If all the states before Bob's measurements $\mathcal{U}_{\text{real}}(\hat{a}_i)$ are identical to the states $\hat{a}_{u(i)}$, i.e., $F(a_i,u(i)) = 1$, it is clear that $\mathcal{S}_{dU} = 2$. Whereas, if there exists an error source which reduces the state fidelity $F(a_i,u(i))$, the value of the kernel $\mathcal{S}_{dU}$ will decrease as well. If a cloner makes all the state fidelities under the same measurement setting have the same value, say $F(a_1,u(1)) = F$ and $F(a_2,u(2)) = \bar{F}$, for all $a \in \mathbf{v}$, then $\mathcal{S}_{dU}$ becomes $\mathcal{S}_{dU} = F + \bar{F}$. When the cloning machine copies equally well the states of both bases, then the state fidelities in both bases are identical, $F = \bar{F}$. For the second criterion on the state fidelity, it is worth noting that the conditional entropy can be represented by $H(B_{u(i)}|a_i) = -F(a_i,u(i))\log_2 F(a_i,u(i)) - \sum_{b\neq a}\Omega(b_{u(i)}a_i)\log_2\Omega(b_{u(i)}a_i)$, where $\Omega(b_{u(i)}a_i)$ denotes the probability of error state transition from a_i to $b_{u(i)}$ for $b_{u(i)} \neq a_i$. When taking the same condition as on the quantum cloning machine for the first criterion into consideration and assuming that the possible errors are equiprobable $\Omega(b_{u(i)}a_i) = (1 - F)/(d - 1)$, we derive a second criterion on the state fidelity F from the second steering condition (9).

[26] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301(R) (2010).

[27] This evaluation is based on whether the process $\mathcal{U}_{\text{real}}$ goes beyond the classical descriptions of the input states and their state evolution, and gives us a tool by which to evaluate a given real transformation.

[28] H. F. Hofmann, Phys. Rev. Lett. **94**, 160504 (2005).

[29] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).

[30] T. Monz, K. Kim, W. Hansel, M. Riebe, A. S. Villar, P. Schindler, M. Chwalla, M. Hennrich, and R. Blatt, Phys. Rev. Lett. **102**, 040501 (2009).

[31] One can change the role of λ from that of variables for describing correlations between Bob and Alice's results via unknown states to hidden random variables for describing correlations between Alice's classical state and Bob's quantum one.

[32] A one-way quantum computer relies on genuine multipartite cluster states [19] to perform gate operations. Here the state $|U\rangle$ for one-way quantum computing is the Schmidt form of cluster states with respect to a fixed bipartition, which splits the total systems into measurement part and readout of quantum gate. The Schmidt rank d, of the state $|U\rangle$, then represents the size of computation. For example [33] (see also Appendix E), a four-qubit cluster state can be used to implement quantum circuit composed of two-qubit gates, and its Schmidt rank is $d = 4$ for such a bipartition.

[33] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Nature (London) **434**, 169 (2005); K. Chen, C.-M. Li, Q. Zhang, Y.-A. Chen, A. Goebel, S. Chen, A. Mair, and J.-W. Pan, Phys. Rev. Lett. **99**, 120503 (2007).

[34] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[35] A. Cabello, Phys. Rev. Lett. **89**, 100402 (2002); J. Mod. Opt. **50**, 1049 (2003).