Self-Testing with Dishonest Parties and Device-Independent Entanglement Certification in Quantum Communication Networks

Gláucia Murta [*,†]
Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany

Flavio Baccari [*,‡]
Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Straße 1, 85748 Garching, Germany

(Received 5 June 2023; revised 4 August 2023; accepted 5 September 2023; published 3 October 2023)

We consider the task of device-independent quantum state certification in a network where some of the nodes may collude and act dishonestly. We introduce the paradigm of self-testing with dishonest parties and provide a certification protocol for the Greenberger-Horne-Zeilinger state in this framework, together with robust statements about the fidelity of the shared state. We extend our results to the cluster scenario, where many subgroups of parties may collude. Our findings provide a new operational motivation for the strong definition of genuine multipartite nonlocality originally introduced by Svetlichny.

DOI: 10.1103/PhysRevLett.131.140201

Introduction.—With recent progress in quantum communication networks, we are approaching the technological developments required to implement protocols that go beyond point-to-point quantum key distribution. In particular, proof-of-principle implementations of conference key agreement [1], as well as its generalization to an anonymous setup [2,3], have been recently realized [4,5], showing that the power of multipartite entanglement can be explored.

Genuine multipartite correlations, as e.g., the one encountered in the Greenberger-Horne-Zeilinger (GHZ) state [6], constitute the essential resource for important network tasks, such as secret sharing [7], multiparty quantum computation [8], and anonymous transmission [9]. Therefore, certifying the entanglement properties of the state distributed in a network is essential to ensure the correct implementation of such tasks.

Entanglement certification in a communication network can be achieved with different adversarial levels. If the parties in the network are honest and trust their measurement apparatuses, entanglement can be verified using quantum state tomography or entanglement witness schemes [10]. If, however, the devices of some (steering scenario) or all the parties (device-independent scenario) are untrusted, i.e., they could be partially characterized or potentially produced by an unturstworthy provider, then multipartite entanglement can be certified using steering inequalities [11] or Bell inequalities [12]. In particular, in the device-independent scenario, self-testing results lead to strong statements about the precise form of the shared state [13]. Finally, in the network scenario, we can have yet another adversarial level, namely some of the parties in the network may be dishonest and, in particular, collude with each other in order to jeopardize the state certification. In protocols where information needs to be concealed from some of the parties, such as in secret sharing and anonymous communication, the parties have an incentive to act maliciously throughout the protocol in order to try to access the hidden information.

The task of entanglement certification in a network with dishonest parties was first considered in [14]. Such a verification scheme lifted the anonymous communication protocol of [9] to the untrusted source scenario [15]. Subsequently the certification protocol of [14] was improved and implemented in [16], and more recently generalized to certify all graph states [17].

Here we consider the task of entanglement certification in a quantum communication network with dishonest parties and uncharacterized devices. We introduce the paradigm of self-testing with dishonest parties and self-test the GHZ state in this framework. We apply this result to design a protocol to certify the GHZ state in a network with dishonest parties and also provide robust statements about the fidelity of the shared state. Finally, we extend our results to the cluster scenario, where different subgroups of parties may collude during the state certification.

Network scenario.—We consider a network with N parties (or nodes) connected to a source (or server) that distributes an N-partite state. Every pair of parties in the network is connected by a private classical channel. The parties may be honest or dishonest. $\mathcal{H}$, $|\mathcal{H}| = k-1$, represents the set of honest parties, and $\mathcal{D}$, $|\mathcal{D}| = N-k+1$, the set of dishonest parties. While parties in $\mathcal{H}$ are assumed to follow all the specifications of the protocol, the unknown subset of $N-k+1$ dishonest parties may deviate arbitrarily from the protocol's

description and even control the source in order to jeopardize the state certification. We do not make any assumptions about the internal working of the devices of the honest parties, i.e., we consider a device-independent scenario. The goal of the parties is to certify the state distributed by the source in the presence of dishonest parties. In the following, one of the parties plays the role of the Verifier, who is required to be honest for the success of the certification protocol. This assumption can be relaxed by using a trusted common random source to pick the Verifier, as discussed in [14,17]. For this work we assume an identically and independently distributed (IID) setup, i.e., that the distributed quantum state and the strategies applied by the parties are the same in every round.

For the proposed certification scheme, we will consider a Bell scenario involving dishonest parties. Assume that each party receives one dichotomic input $x_i \in \{0,1\}$ and has to provide a dichotomic output $a_i \in \{0,1\}$.

In a quantum realization, the action of the honest parties is described by measuring a binary observable $A_{x_i}^{(i)} = \Pi_{0|x_i} - \Pi_{1|x_i}$, where $\Pi_{a_i|x_i}$ is the positive operator-valued measure (POVM) element associated with outcome a_i for party i. In contrast, we associate a global observable for the action of the dishonest parties. Since we will consider a Bell inequality that only depends on the parity of the dishonest parties' outcomes, $J(\vec{a}_{\mathcal{D}}) = \bigoplus_{j\in\mathcal{D}} a_j$, we can define the following observable to describe their action:

$$M_{\vec{x}_{\mathcal{D}}}^{(\mathcal{D})} = \sum_{J(\vec{a}_{\mathcal{D}})=0} \Pi_{\vec{a}_{\mathcal{D}}|\vec{x}_{\mathcal{D}}} - \sum_{J(\vec{a}_{\mathcal{D}})=1} \Pi_{\vec{a}_{\mathcal{D}}|\vec{x}_{\mathcal{D}}}, \tag{1}$$

where $\Pi_{\vec{a}_{\mathcal{D}}|\vec{x}_{\mathcal{D}}}$ is the POVM element associated with the string $\vec{a}_{\mathcal{D}}$ of outcomes for input $\vec{x}_{\mathcal{D}}$. Upon collecting many rounds of outputs, the corresponding statistics is described by a collection of conditional distributions $p(a_1 \ldots a_N|x_1 \ldots x_N)$, and the correlations that can arise in the scenario with dishonest parties are of the form

$$p(a_1 \ldots a_N|x_1 \ldots x_N) = \mathrm{Tr}\left[\left(\bigotimes_{i\in\mathcal{H}} \Pi_{a_i|x_i} \otimes \Pi_{\vec{a}_{\mathcal{D}}|\vec{x}_{\mathcal{D}}}\right)\rho\right], \tag{2}$$

where ρ is the state distributed by the source. Note that any action of the dishonest parties (which in general is described by a quantum channel) can be mapped into the POVM elements describing their joint measurement. Moreover, since the dishonest parties can apply global POVMs, the marginal correlations of the dishonest set can be arbitrary, and in particular correspond to a signaling correlation.

A key ingredient of our result is a Bell inequality that witnesses genuine multipartite nonlocality in the sense that was first introduced by Svetlichny [18]. Specifically, we consider the family of N-partite Svetlichny inequalities [18,19] defined by the expression

$$S_N^{\pm} = \sum_{\vec{x}} (-1)^{\frac{w_{\vec{x}}(w_{\vec{x}}\pm 1)}{2}} \langle A_{x_1}^{(1)} A_{x_2}^{(2)} \ldots A_{x_N}^{(N)} \rangle, \tag{3}$$

where $\vec{x} = (x_1, x_2, \ldots, x_N) \in \{0,1\}^{\times N}$ is a string of N bits that labels the parties' inputs, and $w_{\vec{x}}$ is the Hamming weight of $\vec{x}$. The correlators are defined as

$$\langle A_{x_1}^{(1)} A_{x_2}^{(2)} \ldots A_{x_N}^{(N)} \rangle = \sum_{J(\vec{a})=0} p(\vec{a}|\vec{x}) - \sum_{J(\vec{a})=1} p(\vec{a}|\vec{x}), \tag{4}$$

where $\vec{a} = (a_1, a_2, \ldots, a_N) \in \{0,1\}^{\times N}$ is the string of outcomes, and $J(\vec{a}) = \bigoplus_{j=1}^{N} a_j$ is the parity of $\vec{a}$.

The Svetlichny inequalities read as

$$|S_N^{\pm}| \overset{\mathcal{L}}{\leq} 2^{N-1} \overset{\mathcal{Q}}{\leq} 2^{N-1}\sqrt{2}, \tag{5}$$

where $\mathcal{L}(\mathcal{Q})$ denotes the classical (quantum) bound. The classical bound, $|S_N^{\pm}| \leq 2^{N-1}$, constrains all the distributions that can be decomposed into the form

$$p(a_1 a_2 \ldots a_N|x_1 x_2 \ldots x_N) = \int d\rho_\lambda \sum_{\mathcal{P}\subsetneq\{1,\ldots,N\}} p(\vec{a}_{\mathcal{P}}|\vec{x}_{\mathcal{P}}\lambda) p(\vec{a}_{\mathcal{P}^c}|\vec{x}_{\mathcal{P}^c}\lambda), \tag{6}$$

where $p(\vec{a}_{\mathcal{P}}|\vec{x}_{\mathcal{P}}\lambda)$ is an arbitrary distribution for the parties in set subset $\mathcal{P}$, and $\mathcal{P}^c$ is the complementary set.

By grouping the dishonest parties together, with respective observables $M_{\vec{x}_{\mathcal{D}}}^{(\mathcal{D})}$, as defined in (1), the Svetlichny expression (3) can be written in terms of k-partite correlators, involving the $k-1$ observables of honest parties and a joint observable of the dishonest group. The symmetries of the Svetlichny inequalities ensure that a violation of an N-partite inequality in this setting implies a violation of a k-partite inequality for the noncommunicating honest parties and the group of dishonest parties, as stated in the following proposition.

Proposition 1.—If a strategy achieves value s_N for an N-partite Svetlichny inequality, then the same strategy achieves value s_k for a k-partite Svetlichny inequality, with

$$s_k \geq \frac{s_N}{2^{N-k}}, \tag{7}$$

where $k-1$ parties perform their respective individual strategy, and $N-k+1$ parties are grouped together, potentially performing a joint strategy, with their joint outcome defined by $a' = J(\vec{a}_{\mathcal{D}})$.

Proposition 1 is proved in the Supplemental Material, Sec. A [20]. The proof relies on the fact that an N-partite Svetlichny inequality can be decomposed as a sum of k-partite Svetlichny inequalities. This property has been previously explored in the context of nonlocality depth [21] and complementarity of multipartite nonlocality [22].

Here we show that it is also the key to construct a certification scheme involving dishonest parties.

Self-testing with dishonest parties.—Now we prove that a strong characterization of the distributed state and performed measurements can be achieved when the maximal violation of the Svetlichny inequality is observed. For that, let us introduce a notion of self-testing that is suitable to the scenario with dishonest parties. To make the following expressions more concise, we take $\mathcal{D} = \{k, k+1 \ldots, N\}$, which can always be obtained by relabeling the parties.

Definition 1.—A set of observed correlations $p(\vec{a}|\vec{x})$ self-tests the k-partite state $|\Phi\rangle$ in a dishonest parties scenario if, for any state ρ with purification $|\psi\rangle$ compatible with $p(\vec{a}|\vec{x})$ for some measurements described by observables $A^{(1)}_{x_1}, \ldots, A^{(k-1)}_{x_{k-1}}, M^{(\mathcal{D})}_{\vec{x}_\mathcal{D}}$, there exist local isometries $\{\Lambda_i\}_{i=1}^{k-1}$ for the honest parties and a global isometry $\Lambda_\mathcal{D}$ for the dishonest parties such that

$$\Lambda_1 \otimes \ldots \otimes \Lambda_{k-1} \otimes \Lambda_\mathcal{D}(|\psi\rangle) = |\Phi\rangle_{1\ldots k-1\mathcal{D}} \otimes |\zeta\rangle, \quad (8)$$

where $|\zeta\rangle$ denotes some uncorrelated degrees of freedom. Additionally, the same correlation self-tests a set of target measurements $\bar{A}^{(i)}_0, \bar{A}^{(i)}_1$, for $i = 1, \ldots, k-1$, and $\bar{A}^{(k)}_{\vec{x}_\mathcal{D}}$, for $\vec{x}_\mathcal{D} \in \{0,1\}^{\times|\mathcal{D}|}$, if it follows that, for all input choices,

$$\begin{aligned}\Lambda_1 \otimes \ldots \otimes \Lambda_{k-1} \otimes \Lambda_\mathcal{D}(A^{(1)}_{x_1} \otimes \ldots \otimes A^{(k-1)}_{x_{k-1}} \otimes M^{(\mathcal{D})}_{\vec{x}_\mathcal{D}}|\psi\rangle) \\ = (\bar{A}^{(1)}_{x_1} \otimes \ldots \otimes \bar{A}^{(k-1)}_{x_{k-1}} \otimes \bar{A}^{(k)}_{\vec{x}_\mathcal{D}}|\Phi\rangle) \otimes |\zeta\rangle. \quad (9)\end{aligned}$$

Note that the self-testing statement accounts for collective operations of the dishonest parties, since one cannot *a priori* exclude that all the $N-k+1$ parties cooperate as a joint effective party. Moreover, if the dishonest set controls the source, the self-testing correlations can be achieved using only classical communication between the source and the dishonest parties, with the source manipulating the extra systems accordingly. For that reason, the best one can hope for is to self-test an entangled state shared between the honest parties and a single additional party, representing the dishonest ones as a collective (which may include the source's system). In other words, the self-tested state $|\Phi\rangle$ belongs to a k-partite Hilbert space. With that in mind, we are able to show what follows.

Theorem 1.—The maximum violation of an N-partite Svetlichny inequality with a set of dishonest parties $\mathcal{D}$, $|\mathcal{D}| = N-k+1$, self-tests that a k-partite GHZ state is shared by the honest parties and the set of dishonest parties. Moreover, the same correlations also self-test a set of Pauli observables for the measurements performed by the honest parties and the joint measurements of the dishonest parties.

Theorem 1 follows from a suitably chosen sum-of-squares decomposition for the Svetlichny inequality, which is based on the Clauser-Horne-Shimony-Holt inequality [23]. From the decomposition, we derive that the state maximally violating the Sveltichny inequality with $N-k+1$ dishonest parties satisfies the stabilizing conditions of a k-partite GHZ state [24]. We then construct the isometries that self-test the state and the measurements using techniques of [25]. The complete proof and a description of the self-tested measurements are presented in the Supplemental Material, Sec. B [20].

Theorem 1 is a stronger form of self-testing that allows us to infer the existence of a specific shared state even in the presence of dishonest parties. Indeed, when the dishonest parties implement a joint measurement leading to the maximal violation of the N-partite Svetlichny inequality, the resulting statistics will maximally violate a k-partite Svetlichny inequality, where now we have the standard Bell scenario with the $k-1$ honest parties and the group of dishonest parties acting separately. As a collorary of Theorem 1, when $|\mathcal{D}| \leq 1$ we obtain a standard self-testing result for the Svetlichny inequalities.

Corollary 1.—The maximal violation of an N-partite Svetilichny inequality, in the standard Bell scenario, self-tests the N-partite GHZ state, and the respective Pauli observables that lead to maximal violation of $S^{\pm}_N$.

Note that even though the family of Mermin-Ardehali-Belinskii-Klyshko Bell inequalities [26–28] can be used to self-test the GHZ state in the standard Bell scenario, it fails to provide a self-testing statement in the presence of dishonest parties. Indeed, the strong form of genuine multipartite nonlocality witnessed by the Svetlichny inequality seems to be a crucial ingredient for self-testing in the presence of dishonest parties. It is worth mentioning that different definitions of genuine multipartite nonlocality have been introduced [29,30], where the decomposition in (6) is restricted to nonsignaling or time-ordered distributions with one-way signaling. In particular, in [30] it is shown that Svetlichny's original definition of genuine multipartite nonlocality is inconsistent with a general operational framework for nonlocality. Recently, the term genuine multipartite nonlocality has been used to denote correlations that cannot be created in a network with independent bipartite sources (or k partite with $k < N$) using only local operations and shared randomness [31,32]. Nevertheless, Svetlichny's strong definition of genuine multipartite nonlocality is appropriate in our scenario because we consider a setup where the dishonest parties may collude and perform a joint strategy, which is fairly captured by a signaling probability distribution. The strong form of nonlocality witnessed by the Svetlichny inequality was also shown to have potential application for device-independent secret sharing [33,34].

State certification in quantum networks.—We now introduce a protocol for device-independent entanglement certification in a network with dishonest parties.

Our first result is a qualitative statement about the entanglement properties of the distributed state.

Protocol 1.

One of the parties is denoted the Verifier. Without loss of generality we assume the Verifier to be party A_1.

1. Repeat several times:
   - 1.1 The source distributes a state to the N parties.
   - 1.2 For each $i \in \{1, \ldots, N\}$, the Verifier selects a random input $x_i \in \{0, 1\}$. The Verifier keeps their corresponding input x_1 and sends x_i to party A_i using a private channel.
   - 1.3 Upon receiving input x_i, party A_i produces output a_i and sends it to the Verifier using a private channel.
2. The Verifier computes the value s_N for the Svetlichny inequality S_N^+, from the observed distribution of inputs and outputs.

Theorem 2.—If an honest Verifier observes a violation of the Svetlichny inequality, $s_N > 2^{N-1}$, then Protocol 1 certifies genuine multipartite entanglement among the honest parties and the set of unknown dishonest parties.

Proof.—By Proposition 1, the violation of an N-partite Svetlichny inequality implies that the $k-1$ honest parties and the set of dishonest parties violate a k-partite Svetlichny inequality in the standard k-partite Bell scenario. Moreover, by (6), a violation of a k-partite inequality in the standard Bell scenario witnesses genuine k-partite entanglement. ∎

With the self-testing result of Theorem 1, we can go beyond a qualitative detection of genuine multipartite entanglement and infer the shape of the distributed state. We recall that, in a scenario with dishonest parties, the best one can do is to certify the state up to a joint operation on the dishonest systems (see [14]).

Theorem 3.—If the Verifier is honest and the maximal violation of the Svetlichny inequality is observed, Protocol 1 certifies the N-partite GHZ state up to local isometries on the honest parties and a global isometry on the dishonest parties.

To prove Theorem 3, we use the self-testing result of Theorem 1 and the freedom of operations on the dishonest parties to reach the target N-partite state. Details are presented in the Supplemental Material, Sec. C [20]. Theorem 3 resembles the certification guarantees as first defined in [14]. The difference here is that, in the device-independent scenario, the state is certified up to local isometries in the honest parties.

The self-testing properties of the Svetlichny inequalities can also provide robust guarantees about the distributed state. We will now derive bounds on the device-independent fidelity of the shared state as a function of the observed violation. For that, we define the following figure of merit for the network scenario:

$$F_{\mathrm{DI}}^{\mathcal{D}}(s_N) = \inf_{\tilde{\rho} \in \mathcal{S}(s_N^{\mathcal{D}})} \max_{\substack{\Lambda_{\mathcal{D}}, \Lambda_i \\ i \in \mathcal{H}}} F(\otimes_{i \in \mathcal{H}} \Lambda_i \otimes \Lambda_{\mathcal{D}}(\tilde{\rho}), \Phi^N), \quad (10)$$

where $\Phi^N = |\Phi^N\rangle\langle\Phi^N|$ and $|\Phi^N\rangle = (1/\sqrt{2})(|0\ldots0\rangle + |1\ldots1\rangle)$ is the N-partite GHZ state, Λ_i denote local channels on the system of the honest parties, $i \in \mathcal{H}$, $\Lambda_{\mathcal{D}}$ is a joint quantum channel on the systems of the dishonest parties $\mathcal{D}$, and $\mathcal{S}(s_N^{\mathcal{D}})$ is the set of quantum states that achieves a value of at least s_N for an N-partite Svetlichny inequality when the parties in $\mathcal{D}$ can apply a joint strategy. The fidelity is defined as $F(\rho, \sigma) = (\mathrm{Tr}|\sqrt{\rho}\sqrt{\sigma}|)^2$.

Equation (10) generalizes the concept of *extractability* introduced in [35] to the dishonest parties' scenario. Bounds on the fidelity as a function of the Bell violation in the standard Bell scenario can be derived using the self-testing from operator inequalities (STOPI) method introduced in [35] (see also [36]). The STOPI method consists of fixing channels $\{\Lambda_i\}_i$ and evaluating an operator inequality which is a function of the chosen channels, the Bell operator in question, and two free parameters, which we denote f_k and μ_k for the case of the k-partite Svetlichny inequality (see the Supplemental Material, Sec. D [20] for details). Any solution of this operator inequality provides a lower bound on the extractability of the k-partite Svetlichny inequality,

$$F_{\mathrm{DI}}(s_k) \geq f_k s_k - \mu_k, \quad (11)$$

where $F_{\mathrm{DI}}(s_k)$ correspond to (10) for $|\mathcal{D}| \leq 1$. We drop the superscript $\mathcal{D}$ to highlight that (11) refers to the standard Bell scenario with k noncollaborating parties.

In the following theorem, we show that bounds for the standard Bell scenario, (11), can be used to bound our quantity of interest, $F_{\mathrm{DI}}^{\mathcal{D}}(s_N)$.

Theorem 4.—If an honest Verifier observes a violation s_N in Protocol 1, then the following fidelity can be certified:

$$F_{\mathrm{DI}}^{|\mathcal{D}|=N-k+1} \geq f_k \frac{s_N}{2^{N-k}} - \mu_k, \quad (12)$$

where f_k and μ_k are coefficients that bound extractability for the k-partite Svetlichny inequalities in the standard Bell scenario, as defined in (11).

The proof follows from a chain of inequalities that lower bound $F_{\mathrm{DI}}^{|\mathcal{D}|=N-k+1}$ and is presented in the Supplemental Material, Sec. C [20].

Using the STOPI method [35,36], we determine f_k and μ_k for $k = 2, 3, 4$. The numerical methods, as well as analytical conjectures for f_k and μ_k are presented in the Supplemental Material, Sec. D [20]. Figure 1 illustrates the bounds for a network with four parties. We observe that the bounds for different sizes of $\mathcal{D}$ are not ordered. Intuitively, one could expect the certified fidelity to become better as the number of dishonest parties increases, since the protocol is effectively certifying a smaller GHZ state. This counterintuitive behavior can be an artifact of the employed lower bounds, where tightness may be lost in the application of Theorem 4 and the specific channels used to

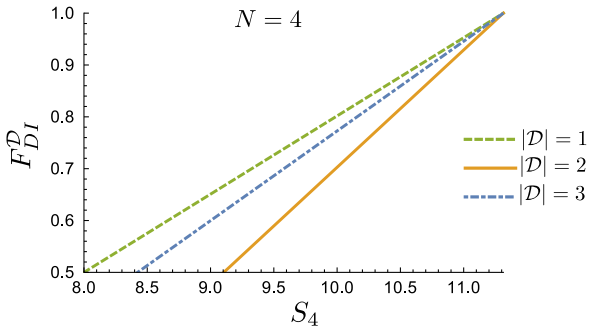

FIG. 1. Bounds on the fidelity as a function of the violation of a four-partite Svetlichny inequality. The curves represent scenarios with a different number of dishonest parties.

determine f_k and μ_k. Another possibility is that this is an intrinsic feature of $F_{\mathrm{DI}}^{\mathcal{D}}$, because as $\mathcal{D}$ increases the infimum is taken over a larger set of states (those achieving the given violation with more dishonest parties), but the maximum is also taken over a larger set of operations (with fewer honest parties constrained to act locally). New and tighter bounds, or a better understanding of the capabilities of the dishonest parties, may shed light on the behavior of the fidelity in the presence of dishonest parties. We leave it as an open question for future investigation.

Self-testing with cooperating clusters.—The previous results can be extended to the scenario where several subgroups of parties may collude. We denote it a network with cooperating clusters; see Fig. 2. This scenario is motivated by a network where specific sets of parties are more likely to collaborate with each other.

The results follow from the symmetries of the Svetlichny inequalities. Indeed, in a scenario with k disjoint clusters, a violation of an N-partite Svetlichny inequality also implies the violation of a k-partite Svetlichny inequality where each party represents one cluster. Therefore it is straightforward to see that the self-testing and entanglement certification results derived in the previous section also extend to the cluster scenario. For more details see the Supplemental Material, Sec. E [20].

Discussion.—We investigated the task of device-independent state certification in a network with dishonest parties. We introduced the concept of self-testing with dishonest parties and proved self-testing of the GHZ state and Pauli measurements based on the N-partite Svetlichny inequalities.

The Svetlichny inequalities, with their ability to witness strong multipartite nonlocality, as defined in (6), seem to be a crucial ingredient for our results. Indeed, we conjecture that witnessing genuine multipartite nonlocality in the sense originally defined by Svetlichny is necessary for self-testing and device-independent entanglement certification with dishonest parties.

We applied the self-testing results to design a protocol to certify the GHZ state in a network with dishonest parties.

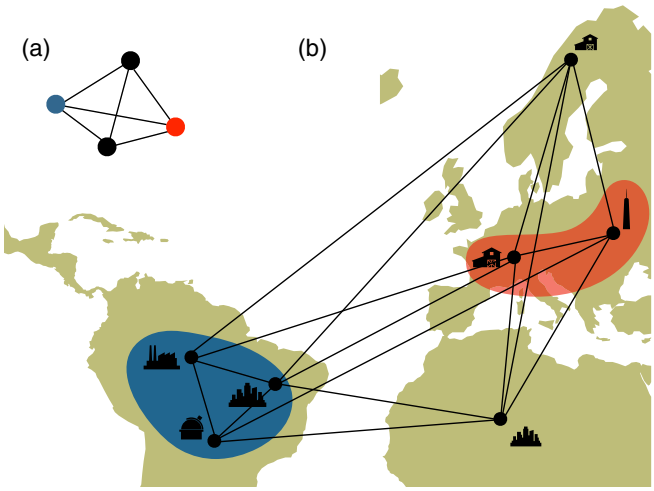

FIG. 2. (a) Effective network for self-testing, where each cluster is treated as a single party. (b) Corresponding pictorial representation of a network with cooperating clusters. Shaded blue and red regions indicate nodes that are likely to collude.

Our protocol witnesses genuine multipartite entanglement among the honest parties and the set of dishonest parties and also allows us to bound the fidelity of the distributed state with an N-partite GHZ state. Our results are proved under the IID assumption, i.e., that the state distributed by the source and the strategies of the parties are the same in every round of the protocol. An interesting outlook is to investigate how to drop this assumption in order to consider a fully adversarial scenario.

The results derived in this work have a direct application to relaxing the trusted source assumption for network protocols based on the GHZ state, similarly to what was done in [15]. It is interesting to ask whether we can extend the results to self-test other classes of multipartite states in the presence of dishonest parties. In particular, a protocol to certify the W state [37] can lift the anonymous transmission protocol of [38] to the untrusted source scenario.

We thank Hermann Kampermann for helpful comments, Tim Coopmans for sharing his master thesis with details on the results of [36], Boris Bourdoncle for giving us the inspiration to improve Fig. 2, and Ivan Šupić for feedback on an earlier version of this manuscript. G. M. is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy—Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) EXC 2004/1–390534769. F. B. acknowledges financial support from the Alexander von Humboldt Foundation.

*These authors contributed equally to this work.
†glaucia.murta@hhu.de
‡flavio.baccari@mpq.mpg.de

[1] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, Experimental quantum conference key agreement, Sci. Adv. **7**, eabe0395 (2021).

[2] F. Hahn, J. de Jong, and A. Pappa, Anonymous quantum conference key agreement, PRX Quantum **1**, 020325 (2020).

[3] F. Grasselli, G. Murta, J. de Jong, F. Hahn, D. Bruß, H. Kampermann, and A. Pappa, Secure anonymous conferencing in quantum networks, PRX Quantum **3**, 040306 (2022).

[4] C. Thalacker, F. Hahn, J. de Jong, A. Pappa, and S. Barz, Anonymous and secret communication in quantum networks, New J. Phys. **23**, 083026 (2021).

[5] L. Rückle, J. Budde, J. de Jong, F. Hahn, A. Pappa, and S. Barz, Experimental anonymous conference key agreement using linear cluster states, arXiv:2207.09487.

[6] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Going beyond Bell's theorem, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Springer, Dordrecht, 1989), Vol. 37.

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

[8] C. Crépeau, D. Gottesman, and A. Smith, Secure multiparty quantum computation, in *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing*, STOC '02 (Association for Computing Machinery, New York, NY, USA, 2002), pp. 643–652, 10.1145/509907.510000.

[9] M. Christandl and S. Wehner, Quantum anonymous transmissions, in *International Conference on the Theory and Application of Cryptology and Information Security* (Springer, New York, 2005), pp. 217–235, 10.1007/11593447_12.

[10] O. Gühne and G. Tóth, Entanglement detection, Phys. Rep. **474**, 1 (2009).

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

[12] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Device-Independent Witnesses of Genuine Multipartite Entanglement, Phys. Rev. Lett. **106**, 250404 (2011).

[13] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, Quantum **4**, 337 (2020).

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

[15] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, Anonymity for Practical Quantum Networks, Phys. Rev. Lett. **122**, 240501 (2019).

[16] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. G. Rarity, and M. S. Tame, Experimental verification of multipartite entanglement in quantum networks, Nat. Commun. **7**, 13251 (2016).

[17] A. Unnikrishnan and D. Markham, Verification of graph states in an untrusted network, Phys. Rev. A **105**, 052420 (2022).

[18] G. Svetlichny, Distinguishing three-body from two-body nonseparability by a Bell-type inequality, Phys. Rev. D **35**, 3066 (1987).

[19] M. Seevinck and G. Svetlichny, Bell-Type Inequalities for Partial Separability in n-Particle Systems and Quantum Mechanical Violations, Phys. Rev. Lett. **89**, 060401 (2002).

[20] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.131.140201 for self-testing with dishonest parties and device-independent entanglement certification in quantum communication networks.

[21] F. Bernards and O. Gühne, Bell inequalities for nonlocality depth, Phys. Rev. A **107**, 022412 (2023).

[22] S. Sami, I. Chakrabarty, and A. Chaturvedi, Complementarity of genuine multipartite Bell nonlocality, Phys. Rev. A **96**, 022121 (2017).

[23] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 (1969).

[24] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Nest, and H.-J. Briegel, Entanglement in graph states and its applications, arXiv:quant-ph/0602096.

[25] F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín, Scalable Bell Inequalities for Qubit Graph States and Robust Self-Testing, Phys. Rev. Lett. **124**, 020402 (2020).

[26] N. D. Mermin, Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct States, Phys. Rev. Lett. **65**, 1838 (1990).

[27] M. Ardehali, Bell inequalities with a magnitude of violation that grows exponentially with the number of particles, Phys. Rev. A **46**, 5375 (1992).

[28] A. V. Belinskiĭ and D. N. Klyshko, Interference of light and Bell's theorem, Phys. Usp. **36**, 653 (1993).

[29] J.-D. Bancal, J. Barrett, N. Gisin, and S. Pironio, Definitions of multipartite nonlocality, Phys. Rev. A **88**, 014102 (2013).

[30] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués, Operational Framework for Nonlocality, Phys. Rev. Lett. **109**, 070401 (2012).

[31] X. Coiteux-Roy, E. Wolfe, and M.-O. Renou, No Bipartite-Nonlocal Causal Theory Can Explain Nature's Correlations, Phys. Rev. Lett. **127**, 200401 (2021).

[32] X. Coiteux-Roy, E. Wolfe, and M.-O. Renou, Any physical theory of nature must be boundlessly multipartite nonlocal, Phys. Rev. A **104**, 052207 (2021).

[33] M. G. M. Moreno, S. Brito, R. V. Nery, and R. Chaves, Device-independent secret sharing and a stronger form of Bell nonlocality, Phys. Rev. A **101**, 052339 (2020).

[34] Y. Xiang, Multipartite quantum cryptography based on the violation of Svetlichny's inequality, Eur. Phys. J. D **77**, 31 (2023).

[35] J. Kaniewski, Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities, Phys. Rev. Lett. **117**, 070402 (2016).

[36] T. Coopmans, J. Kaniewski, and C. Schaffner, Robust self-testing of two-qubit states, Phys. Rev. A **99**, 052123 (2019).

[37] W. Dür, G. Vidal, and J. I. Cirac, Three qubits can be entangled in two inequivalent ways, Phys. Rev. A **62**, 062314 (2000).

[38] V. Lipinska, G. Murta, and S. Wehner, Anonymous transmission in a noisy quantum network using the W state, Phys. Rev. A **98**, 052320 (2018).