Blindly verifying partially unknown entanglement

Ming-Xing Luo, Shao-Ming Fei, Jing-Ling Chen
mxluo@swjtu.edu.cn (M.-X.L.)
feishm@cnu.edu.cn (S.-M.F.)
chenjl@nankai.edu.cn (J.-L.C.)

Highlights
A model of entanglement set verification is proposed and analyzed.
Nonlinear entanglement witnesses for specific entanglement sets are constructed.
Blind quantum verification scheme is built.

Luo et al., iScience 25, 103972
March 18, 2022 © 2022 The Author(s).
https://doi.org/10.1016/j.isci.2022.103972
Blindly verifying partially unknown entanglement

Ming-Xing Luo,1,5,6,* Shao-Ming Fei,2,4,* and Jing-Ling Chen3,*

SUMMARY
Quantum entanglement has shown distinguished features beyond any classical state. Many methods have been presented to verify unknown entanglement with the complete information about the density matrices by quantum state tomography. In this work, we aim to identify unknown entanglement with only partial information of the state space. The witness consists of a generalized Greenberger-Horne-Zeilinger-like paradox expressed by Pauli observables, and a nonlinear entanglement witness expressed by density matrix elements. First, we verify unknown bipartite entanglement and study the robustness of entanglement witnesses against the white noise. Second, we generalize such verification to partially unknown multipartite entangled states, including the Greenberger-Horne-Zeilinger-type and W-type states. Third, we give a quantum-information application related to the quantum zero-knowledge proof. It further provides a useful method in blindly verifying universal quantum computation resources. These results may be interesting in entanglement theories, quantum communication, and quantum networks.

INTRODUCTION
Quantum entanglement cannot be decomposed into a statistical mixture of various product states (Einstein et al., 1935). It is the most surprising nonclassical property of composite quantum systems (Horodecki et al., 2009) that Schrödinger has singled out as “the characteristic trait of quantum mechanics” (Schrödinger, 1935). How to verify a given entanglement has become a fundamental problem in both quantum mechanics and quantum information processing. In 1964, Bell firstly proved that the statistics generated by some proper local quantum measurements on a two-qubit entanglement cannot be generated by any local-hidden variable model (Bell, 1964). The so-called Bell inequality provides an experimental method for verifying the intrinsic nonlocality of entanglement. Subsequently, this method has been extended for various entangled states (Clauser et al., 1969; Gisin, 1991; Greenberger et al., 1989; Brunner et al., 2014; Gühne and Tóth, 2009), except for special mixed states (Werner, 1989). Another method is from the Hahn-Banach Theorem (Lewenstein et al., 2000; Horodecki et al., 2009), which can separate each entanglement from a specific convex set consisting of all the separable states (Horodecki et al., 2009) by exploring the state-dependent witness function. This provides a universal method for witnessing all the entangled states (Horodecki et al., 2009; Amico et al., 2008). In Bell experiments, such as experimentally observing the maximal violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality for a two-qubit state, initially one needs to know the explicit density matrix of the examined quantum state, so as to choose optimal measurements. Otherwise, selecting random measurement settings, he could only observe the probabilistic violations of the CHSH inequality (Laing et al., 2010). So far, the traditional Bell experiments (Bell, 1964; Clauser et al., 1969; Gisin, 1991) and entanglement witnesses (Lewenstein et al., 2000; Horodecki et al., 2009) require essentially the state tomography to learn its density matrix \( \rho \in \mathcal{B}(\mathcal{H}) \) (Lu et al., 2016), when people come to verify an unknown entangled source, as shown in Figure 1A. This situation seems to rule out the possibility for entanglement verification without complete information of its density matrix. It is interesting to consider that, what happens for an unknown entanglement with partial knowledge?

Specifically, suppose a given source is restricted to be an entanglement ensemble. One possibility is that the device provider gives only its state subspace \( \mathcal{S} \subset \mathcal{B}(\mathcal{H}) \), but not a specific density matrix. One example is known as an arbitrary bipartite state in the known subspace \( \mathcal{S} \subset \mathcal{B}(\mathcal{H}) \) spanned by the known basis \{\{(00),(01),(11)\}\} (see Figure 1B), but not a specific Einstein-Podolsky-Rosen (EPR) state (Einstein et al., 1935). This can be further regarded as a blind quantum communication model inspired by the device provider gives only its state subspace \( \mathcal{S} \subset \mathcal{B}(\mathcal{H}) \), but not a specific density matrix. It is interesting to consider that, what happens for an unknown entanglement with partial knowledge? In Bell experiments, such as experimentally observing the maximal violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality for a two-qubit state, initially one needs to know the explicit density matrix of the examined quantum state, so as to choose optimal measurements. Otherwise, selecting random measurement settings, he could only observe the probabilistic violations of the CHSH inequality (Laing et al., 2010). So far, the traditional Bell experiments (Bell, 1964; Clauser et al., 1969; Gisin, 1991) and entanglement witnesses (Lewenstein et al., 2000; Horodecki et al., 2009) require essentially the state tomography to learn its density matrix \( \rho \in \mathcal{B}(\mathcal{H}) \) (Lu et al., 2016), when people come to verify an unknown entangled source, as shown in Figure 1A. This situation seems to rule out the possibility for entanglement verification without complete information of its density matrix. It is interesting to consider that, what happens for an unknown entanglement with partial knowledge?

Specifically, suppose a given source is restricted to be an entanglement ensemble. One possibility is that the device provider gives only its state subspace \( \mathcal{S} \subset \mathcal{B}(\mathcal{H}) \), but not a specific density matrix. One example is known as an arbitrary bipartite state in the known subspace \( \mathcal{S} \subset \mathcal{B}(\mathcal{H}) \) spanned by the known basis \{\{(00),(01),(11)\}\} (see Figure 1B), but not a specific Einstein-Podolsky-Rosen (EPR) state (Einstein et al., 1935). This can be further regarded as a blind quantum communication model inspired by...
the blind quantum computation (Broadbent et al., 2009), in which the EPR state passes through a specific blind channel, such as some random unitary operations (see Figure 1C). A natural problem is whether such relaxed assumptions allow verifying entanglement ensembles without the state tomography. This also intrigues an interesting problem of entanglement locking (Horodecki et al., 2005).

The purpose of this paper is to verify unknown entanglement with partial information of the state space. To reach this aim, we shall propose a nonlinear entanglement witness (NEW), which consists of a generalized Greenberger-Horne-Zeilinger-like (GHZ-like) paradox expressed by Pauli observables, and a nonlinear inequality expressed by density matrix elements. First, we verify an unknown bipartite entanglement, and also discuss the robustness of entanglement witnesses. Second, we generalize the verification of unknown entanglement to multipartite entangled states, such as the GHZ-type states and the cluster states. Third, we provide a quantum-information application related to the quantum zero-knowledge proof. Our result provides a general method for verifying universal unknown quantum computation resources (Raussendorf and Briegel, 2001). It is also robust against white noises and allows for experiments with recent techniques.

RESULTS

Entanglement ensemble model

A pure finite-dimensional quantum state is represented by a normalized vector $|\psi\rangle$ in Hilbert space $\mathcal{H}$. An ensemble of pure states $\{|\psi_i\rangle\}$ is represented by using density matrix $\rho = \sum_p |\psi_i\rangle\langle\psi_i|$ on Hilbert space $\mathcal{H}$, where $\{p_i\}$ is a probability distribution. An bipartite state $\rho_{AB}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ is an entanglement (Horodecki et al., 2009) if it cannot be decomposed into the following form

$$\rho_{AB} = \sum_i p_i \rho_i^{(A)} \otimes \rho_i^{(B)}$$ (Equation 1)

where $\rho_i^{(A)}$ are single-particle states and $\{p_i\}$ is a probability distribution.

As for the entanglement ensemble model, in this work, we consider an n-particle state in the density operator space $\mathcal{B}(\otimes_{1}^n \mathcal{H}_A)$ associated with the Hilbert space $\otimes_{1}^n \mathcal{H}_A$. The additional information may be learned from the device provider. The traditional entanglement witnesses (Brunner et al., 2014; Gühne and Tóth, 2009; Horodecki et al., 2009) require complete information of its density matrix $\rho$ by using the

Figure 1. Schematic verification of partially unknown entanglement

(A) Traditional methods. The state tomography is firstly performed to learn the density matrix $\rho \in \mathcal{B}(\mathcal{H})$, which is further used for constructing Bell experiment or entanglement witness. Here, $\mathcal{B}(\mathcal{H})$ denotes the density operator space on Hilbert space $\mathcal{H}$.

(B) Proposed method without the state tomography. The given entanglement is supposed to be in a special subspace $S \subset \mathcal{B}(\mathcal{H})$ spanned by known basis such as $\{|00\rangle|00\rangle, |00\rangle|11\rangle, |11\rangle|00\rangle, |11\rangle|11\rangle\}$, but without the knowledge of the mixture, that is, the probability in the pure state decomposition of the density matrix.

(C) Entanglement in a blind quantum communication model. A known entanglement $\rho_{in}$ passes through one blind quantum channel $\mathcal{E}(\cdot)$ such as random unitary operations, that is, the output unknown state is given by $\rho = \mathcal{E}(\rho_{in})$. 

The purpose of this paper is to verify unknown entanglement with partial information of the state space. To reach this aim, we shall propose a nonlinear entanglement witness (NEW), which consists of a generalized Greenberger-Horne-Zeilinger-like (GHZ-like) paradox expressed by Pauli observables, and a nonlinear inequality expressed by density matrix elements. First, we verify an unknown bipartite entanglement, and also discuss the robustness of entanglement witnesses. Second, we generalize the verification of unknown entanglement to multipartite entangled states, such as the GHZ-type states and the cluster states. Third, we provide a quantum-information application related to the quantum zero-knowledge proof. Our result provides a general method for verifying universal unknown quantum computation resources (Raussendorf and Briegel, 2001). It is also robust against white noises and allows for experiments with recent techniques.
The CHSH inequality (Clauser et al., 1969) is inapplicable because of the unknown parameter $m$. Thus the main goal here is to separate one entanglement set $S$ from all the separable states. Interestingly, $S$ may be not convex and thus rule out the standard construction of linear entanglement witness (Horodecki et al., 2009) or linear Bell inequalities (Brunner et al., 2014). It is also different from self-testing entangled subspaces consisting of all entangled pure states with the state tomography (Baccari et al., 2020). Therefore, how to verify the entanglement set $S$ will show insights in fundamental problems of entanglement theory.

**Verifying partially unknown bipartite entanglement**

Let us consider the simplest case of a two-qubit system on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. A generalized bipartite entangled pure state shared by Alice and Bob reads

$$|\Phi(\theta)\rangle_{AB} = \cos \theta |00\rangle + \sin \theta |11\rangle,$$

(Equation 2)

where $\theta \in (0, \pi/2)$, and $|\Phi(\pi/4)\rangle$ is the EPR state (Einstein et al., 1935). We now consider the following scenario: both parties only know the shared state has the following form:

$$\rho_{AB} = \mathbb{E}(|\Phi(\theta)\rangle\langle\Phi(\theta)|),$$

(Equation 3)

where $\mathbb{E}(\cdot)$ is a blind quantum channel defined by $\mathbb{E}(\rho) = \sum_{i} p_i (U_i \otimes V_i)\rho (U_i^\dagger \otimes V_i^\dagger)$, $\rho$ is the input state, $\{|p_i\rangle\}$ is an unknown probability distribution, and $U_i$ and $V_i$ are any local phase transformations, e.g., $U_i = e^{i\theta_i}|0\rangle \langle 0| + e^{i\phi_i}|1\rangle \langle 1|$, and $V_i = e^{i\theta_i'}|0\rangle \langle 0| + e^{i\phi_i'}|1\rangle \langle 1|$, with unknown parameters $\theta_i, \theta_i', \phi_i, \phi_i' \in (0, \pi)$. In general, $\mathbb{E}(\cdot)$ can be defined through some positive-operator-value measurements (POVM), i.e., $\mathbb{E}(\rho) = \sum_{i} M_i \otimes 1$.

$\rho(M_i \otimes 1)$, with $M_i = \sqrt{p_i}|00\rangle \langle 00| + \sqrt{1-p_i}|11\rangle \langle 11|$, $\sum_i M_i^\dagger M_i = 1$, and $\sum_i p_i = 1$. The entanglement involved in the state $\rho_{AB}$ is named as the EPR-type entanglement. The density matrix $\rho_{AB}$ is rewritten into

$$\rho_{AB} = \rho_{00,00}|00\rangle \langle 00| + \rho_{11,11}|11\rangle \langle 11| + \rho_{00,11}|00\rangle \langle 11| + \rho_{11,00}|11\rangle \langle 00|,$$

(Equation 4)

where $\rho_{ij,kl}$'s are the matrix elements satisfying $\rho_{00,00} + \rho_{11,11} = 1$ and $\rho_{00,11} = \rho_{11,00}$. Thus our goal is to verify the entanglement set

$$S_{epr} := \{\mathbb{E}(|\Phi(\theta)\rangle\langle\Phi(\theta)|), \forall |\Phi(\theta)\rangle, \mathbb{E}(\cdot)\}$$

(Equation 5)

which is spanned by the known basis $\{|00\rangle, |01\rangle, |11\rangle, |10\rangle\}$ as in Equation (4). Notably, the CHSH inequality (Clauser et al., 1969) is inapplicable because of the unknown parameter $\theta$'s in Equation (3), which forbids two parties to find suitable observables. Meanwhile, $S_{epr}$ is not convex. For instance, for the given state $\rho = |\Phi(\theta)\rangle\langle\Phi(\theta)|$, $U_0 = 1 = |00\rangle \langle 00| + |11\rangle \langle 11|$, and $U_1 = |00\rangle \langle 00| - |11\rangle \langle 11|$, then one easily has $\rho_{AB} = \sum_{i,j=0,1} \rho_{ij,kl} |U_i \otimes V_j\rangle \langle U_i^\dagger \otimes V_j^\dagger| = \cos^2 \theta |00\rangle \langle 00| + \sin^2 \theta |11\rangle \langle 11|$, which is a separable state. This fact excludes the well-known method of linear entanglement witnesses (Horodecki et al., 2009).

For solving the problem, we have the following Theorem 1.

**Theorem 1.** The entanglement set $S_{epr}$ is verifiable.

**Proof.**—First, let us present a generalized GHZ-like paradox for quantum entanglement, which is given by

$$\langle \sigma_x \otimes \sigma_x \rangle = 1,$$

$$\langle \sigma_x \otimes \sigma_y \rangle = 0,$$

$$\langle \sigma_y \otimes \sigma_z \rangle = 0,$$

$$\langle \sigma_z \otimes \sigma_x E_{se} \rangle \neq 0,$$

(Equation 6)

where "ES" represents "entangled states", $\sigma_x$ and $\sigma_z$ are Pauli matrices, and $\langle \sigma_x \otimes \sigma_i \rangle$ is defined by $\langle \sigma_x \otimes \sigma_i \rangle = Tr[\rho (\sigma_x \otimes \sigma_i)]$. In Equation (6), whose left-hand side contains four operators $\{E_1 = \sigma_x \otimes \sigma_z, E_2 = \sigma_x \otimes \sigma_z, E_3 = \sigma_x \otimes \sigma_z, E_4 = \sigma_x \otimes \sigma_z\}$. For a standard GHZ paradox (Greenberger et al., 1989), the global observable $E$'s are required to satisfy a very strict condition: they are mutually commutative, i.e., $[E_i, E_j] = 0$ for any $i \neq j$, and moreover the examined entanglement is the common eigenstate of $(E_1, E_2, E_3, E_4)$. In Ref. (Wiseman et al., 2007), quantum nonlocality has been classified into three distinct
types: quantum entanglement, EPR steering, and Bell nonlocality. Among which, as quantum entanglement is the weakest type of quantum nonlocality, we develop the paradox (6) without the above strict conditions for witnessing entanglement.

Let us denote the supposedly definite real values of \( v_{1,z} \) and \( v_{2,z} \) for Alice, and \( v_{1,x} \) and \( v_{2,x} \) for Bob, with \( v_{1,z}, v_{1,x}, v_{2,z}, v_{2,x} \in [1, -1] \) beyond the integers in the standard GHZ paradox (Greenberger et al., 1989). This can be regarded as a restricted hidden variable model. Then similar to the analysis of GHZ paradox, classically we have from Equation (6) that \( v_{1,z} v_{2,z} = 1, v_{1,z} v_{2,x} = 0, v_{1,x} v_{2,x} = 0, \) and \( v_{1,x} v_{2,z} \neq 0 \). But, the product of the first three relations gives \( v_{1,z} v_{2,z} v_{1,x} v_{2,x} = v_{1,z} v_{2,x} = 0 \), which conflicts with the fourth relation.

The proof of witnessing entanglement set \( S_{epr} \) depends on the following nonlinear inequality

\[
2 \sqrt{\rho_{00,11} \rho_{11,00} + \rho_{00,00} + \rho_{11,11}} - 1 \leq 0 \tag{Equation 7}
\]

Which holds for any biseparable states (see Lemma 1 in Method details). From the inequality (7), \( \rho \) in Equation (4) is entangled if and only if \( \rho_{00,11} \neq 0 \), in other words, it is separable state if and only if \( \rho_{00,11} = \rho_{11,00} = 0 \).

Next we come to prove that any separable state would violate one statement in the paradox (6). For any separable state \( \rho_{epr} \) without the decomposition in Equation (4), it violates the first statement in the paradox (6). Otherwise, from Equation (6) any \( \rho_{epr} \) with \( \rho_{00,11} = \rho_{11,00} = 0 \) violates the fourth relation in the paradox (6). This has completed the proof.

The paradox (6) and the nonlinear inequality (7) together have provided a nonlinear entanglement witness to successfully verify the bipartite entangled states in a blind manner. In experiment, the inequality (7) is verified according to the paradox (6). Interestingly, different from the standard linear entanglement witness (Horodecki et al., 2009) for any entanglement derived from the Hahn-Banach Theorem, the inequality (7) implies a nonlinear entanglement witness for verifying the non-convex set \( S_{epr} \). Although the present method is constructive for specific sets, it might intrigue general interests beyond the Hahn-Banach Theorem.

Robustness of entanglement witnesses

The generalized GHZ-like paradox (7) of verifying unknown entangled sources is adaptable against white noise. Consider a bipartite noisy Werner state (Werner, 1989) as

\[
\rho_v = v \rho_{AB} + \frac{1 - v}{4} I_4, \tag{Equation 8}
\]

where \( \rho_{AB} \) is given in Equation (4), \( I_4 \) is the identity operator of rank 4, and \( v \in [0, 1] \) is the visibility. From Equations (6) and (7), the entanglement of \( \rho_v \) is witnessed if it satisfies the following modified entanglement witness (see Method details)

\[
\{ (\sigma_x \otimes \sigma_x)_{\rho_v} = 0, \quad (\sigma_y \otimes \sigma_y)_{\rho_v} = 0, \quad 4(\sigma_z \otimes \sigma_z)_{\rho_v} - (\sigma_x \otimes \sigma_x)_{\rho_v} > 1 \} \tag{Equation 9}
\]

The visibilities of white noise, denoted by \( v^* \), are shown in Figure 2. There is an evident gap between two curves, indicating the present entanglement witness is more efficient than the CHSH inequality (Clauser et al., 1969) even with known density matrix.

Verifying partially unknown multipartite entanglement

The stabilizer formalism presents a novel way for describing quantum mechanics by using the concepts from group theory, such as the Pauli group (Dehaene and Moor, 2003). This inspires a way for witnessing partially unknown multipartite entanglement using its stabilizer. Specially, for a given \( n \)-partite entanglement ensemble \( \{|\Psi(\omega)\rangle\} \) depending on some parameter \( \omega \in \mathbb{R} \) on Hilbert space \( \otimes_{i=1}^n \mathcal{H}_A \), a generalized GHZ-like paradox for quantum entanglement is built as

\[
\langle g_j | \Psi(\omega) \rangle = \pm 1, \quad (j = 1, \ldots, N), \quad \langle w | \Psi(\omega) \rangle \neq 0, \tag{Equation 10}
\]

\[
\langle g_j | \Psi(\omega) \rangle = \pm 1, \quad (j = 1, \ldots, N), \quad \langle w | \Psi(\omega) \rangle \neq 0, \tag{Equation 10}
\]
Theorem 2 (see Method details). The entanglement set $S_{\text{sep}}$ (Svetlichny, 1987), and $\{g_{1}, \ldots, g_{N}\}$ are simultaneous stabilizers of $|\Psi(\alpha)\rangle$’s. Specially, $w$ may be defined by

$$w \left\{ \pm |\Psi(\alpha)\rangle\langle\Psi(\alpha)| + \sum_{j} q_{j} |\Phi_{j}\rangle\langle\Phi_{j}| \right\},$$  \hspace{1cm} \text{(Equation 11)}$$

where $\{|\Psi(\alpha)\rangle, |\Phi_{j}\rangle, \forall j\}$ is an orthogonal basis of specific Hilbert space. The witness operator $w$ may be separable for special $q_j$’s.

One example is an $m$-partite entanglement given by

$$\rho_{A_{1}\cdots A_{m}} = \mathcal{E}(|\Psi(\theta)\rangle\langle\Psi(\theta)|)$$  \hspace{1cm} \text{(Equation 12)}$$

On Hilbert space $\bigotimes_{j=1}^{n} \mathcal{H}_{A_{j}}$, where $|\Psi(\theta)\rangle$ is a generalized GHZ state (Greenberger et al., 1989) defined by

$$|\Psi(\theta)\rangle = \cos \theta |0\rangle^{\otimes n} + \sin \theta |1\rangle^{\otimes n}$$  \hspace{1cm} \text{(Equation 13)}$$

with $\theta \in (0, \pi)$ and $\mathcal{E}(\cdot)$ is a blind quantum channel defined by $\mathcal{E}(q) = \sum_{a_{1}, \ldots, a_{n} = 1}^{3} E_{a_{1}, \ldots, a_{n}} |U_{j}^{k}(j)\rangle\langle U_{j}^{k}(j)|$, $U_{j}^{k} = e^{i \theta_{k}} |0\rangle_{j} + e^{i \phi_{k}} |1\rangle_{j}$ with unknown parameters $\theta_{k}, \phi_{k} \in (0, \pi)$, and $\{p_{a_{j}}\}$ is unknown probability distribution. This is regarded as the multipartite GHZ-type entanglement. A generalized GHZ-like paradox for the entanglement (12) is given by

$$\begin{align*}
\langle \sigma_{j}^{0} \otimes \sigma_{j}^{0} \rangle_{p} &= 1, \\
\langle \sigma_{j}^{0} \otimes \sigma_{j}^{0} \rangle_{p} &= 1, \\
\langle \sigma_{j}^{0} \otimes \sigma_{j}^{0} \rangle_{p} &= 0, \\
\langle \sigma_{j}^{0} \otimes \sigma_{j}^{0} \rangle_{p} &= 0, \\
\langle \sigma_{j}^{0} \otimes \sigma_{j}^{0} \rangle_{p} &= 0, \\
\langle \sigma_{j}^{0} \otimes \sigma_{j}^{0} \rangle_{p} &= 0, \quad (j = 1, \ldots, n - 1), \\
\langle \otimes_{k=1}^{n} \sigma_{j}^{0} \rangle_{p} &= 0,
\end{align*}$$  \hspace{1cm} \text{(Equation 14)}$$

where $\sigma_{j}^{0}$ denotes the Pauli matrix acting on the $j$-th party. This paradox reduces to the bipartite paradox (6) when $n = 2$. For the $n$-qubit scenarios, denote $S_{\text{ghz}} = \{\mathcal{E}(|\Psi(\theta)\rangle\langle\Psi(\theta)|), \forall |\Psi(\theta)\rangle, \mathcal{E}(\cdot)\}$. We have the following Theorem 2 (see Method details).

Theorem 2. The entanglement set $S_{\text{ghz}}$ is verifiable.

Another example is to verify a $W$-type entanglement set $S_{w} = \{\mathcal{E}(|\Phi\rangle\langle\Phi|), \forall |\Phi\rangle, \mathcal{E}(\cdot)\}$ (see Method details), where $|\Phi\rangle = a_{0}|001\rangle + a_{1}|010\rangle + a_{2}|100\rangle + a_{3}|111\rangle$ (Dur et al., 2000) on Hilbert space $\mathcal{H}_{A} \otimes \mathcal{H}_{B} \otimes \mathcal{H}_{C}$, $a_{j}$ are real parameters satisfying $\sum_{j=0}^{3} a_{j}^{2} = 1$, and $\mathcal{E}(\cdot)$ is defined in Equation (12).
In the following, let us discuss two applications.

Verifying partially unknown universal computation resources
The one-way quantum computer (Raussendorf and Briegel, 2001) is realized by measuring individual qubits of a highly entangled multiparticle state in a temporal sequence. The involved cluster state provides a universal resource for quantum computation. One easy way to generate cluster states is from quantum networks (den Nest et al., 2006; Wei et al., 2011) by using local two-qubit controlled-phase operations:

$$CP(q) = |00\rangle_D + |01\rangle_D + e^{i\phi} |10\rangle_D + |11\rangle_D.$$  

Specially, consider a connected quantum network $N_q$ consisting of $\cdots, A_i, \cdots$, where each party shares the entanglement (2) or (13) with others. The connectedness means that for any pair of $A_i$ and $A_j$ there is a chain subnetwork $N_{ij}$ consisting of $A_i, A_{i1}, \cdots, A_{is}, A_j$ satisfying any adjacent two parties share some entangled states. These multipartite entangled states can be in whole verified by using Bell inequalities (Guhne et al., 2005; Luo, 2021a, 2021b), entanglement witness (Jungnitsch et al., 2011), or GHZ-type paradoxes (Scarani et al., 2005; Tang et al., 2013; Liu et al., 2021). Instead, the goal here is to witness partially unknown cluster states generated by entangled states (2) and (13) under blind channels. Let the set $S_{cl}$ consist of all cluster states generated from quantum network $N_q$ in the state $\rho_G$, that is, $S_{cl} = \{E(C(\rho_G), \xi(\cdot))\}$, where $\xi(\cdot)$ is defined in Equation (12), and $C(\cdot)$ is a blind unitary transformation defined by $\Theta_{ic}\, CP(\theta)$ with unknown $\theta \in (0, \pi)$. The set $S_{cl}$ is unique because $\xi(\cdot)$ and $C(\cdot)$ are commutative. We have the following Theorem 3 (see Method details).

**Theorem 3**  
The entanglement set $S_{cl}$ is verifiable.

For the EPR-type state (3) or GHZ-type state (12), the controlling and controlled qubits in the two-qubit operation $CP(\theta) = |00\rangle_D + |01\rangle_D + |10\rangle_D + |11\rangle_D$ can be swapped. The symmetry allows for reshaping $N_q$ in Figure 3A into a star-shaped network, as Figure 3B, in which all $CP(\theta)$’s are performed by the center party. The new network is easy for proving the universality of generated entangled states (Wei et al., 2011). Thus Theorem three provides a blind witness of universal quantum computation resources without the state tomography beyond previous results (Guhne et al., 2005; Jungnitsch et al., 2011; Scarani et al., 2005; Tang et al., 2013; Liu et al., 2021).

Zero-knowledge proof of partially unknown quantum entangled source
Classical zero-knowledge proof provides an interesting protocol to prove special hard problems without leaking its information (Goldwasser et al., 1989; Goldreich and Oren, 1994). It is of a cryptographic primitive in secure multiparty computation. The quantum versions take use of entangled states. So far, most results have focused on extensions of classical tasks (Watrous, 2002) or entangled provers (Ito and Vidick, 2012; Ji, 2017; Grilo et al., 2019); however, our proposed method proves a quantum information task, that is, verifying an entanglement (3) (for example) without leaking knowledge of mixture probability distribution.
The verifier challenges with a random bit series $k_i$ and sends the qubit series $B_1, \cdots, B_N$ to the verifier. (ii) The verifier complies with $a_1, \cdots, a_N \in \{ \pm 1 \}$, where $a_i$ denotes the outcome on qubit $A_i$ by performing Pauli measurement $\sigma_k \oplus q_k = \sigma_k$ and $q_k := q_k$. (iii) The verifier performs the measurement on qubit $B_1$ with Pauli observable $\sigma_k \in \{ \sigma_x, \sigma_y, \sigma_z \}$ under the uniform distribution. The proof is true if all the joint statistics of $(\sigma_k \otimes \sigma_{k'})_{A_iB_i}$ satisfy the paradox (6) under the assumptions of ideal Pauli measurement devices. Otherwise, it is false. The verifier can only access the partial particle, which implies a difficult problem for the verifier to complete the task without the help of a prover. The completeness is followed from Theorem 1, that is, the prover can convince the verifier’s result. A malicious prover, who prepares another entanglement beyond the one in Equation (3) or separable state, cannot convince the verifier’s verification because he cannot forge measurement outcomes of challenges before the random measurements $\sigma_{a_1}, \cdots, \sigma_{a_N}$. This yields soundness. Besides, a malicious verifier can only learn the decomposition (4) of its density matrix, which leaks no useful information of $(\rho_j)$ and parameters $\theta$’s. This follows the zero-knowledge. A more rigid analysis requires formal cryptographic models beyond the scope of this paper. The protocol may be extended for multiparty by using the GHZ-type entanglement (12). Those examples may inspire interesting applications in cryptography.

**DISCUSSION**

In this paper, we have investigated unknown entangled states with limited information of its state subspace. We proposed a generalized GHZ-like paradox for verifying an entanglement set consisting of unknown bipartite entangled states using only Pauli observables. This allows a blind entanglement verification assisted by a nonlinear entanglement witness in a device-independent manner. We further verified an entanglement set consisting of unknown multipartite entangled states such as multipartite GHZ-type entanglement and cluster states from quantum networks. This provides a useful method for verifying universal quantum computation resources blindly. The present results should be interesting in entanglement theory, Bell theory, and quantum communication.

The well-known Bell theory and entanglement witness are designed for detecting given entanglement. Our method is designed for unknown entanglement without the state tomography. This intrinsically a new problem of verifying specific sets consisting of entangled states. It may be regarded as entanglement verification in adversary scenarios where the given entanglement passes through a blind channel of black-box device controlled by adversaries. The present result holds for special sources in generalized EPR states or multipartite GHZ states. It can be extended to high-dimensional EPR-type or GHZ-type entangled states (see Method details). This motivates a general problem for other entangled sources (Dicke, 1954; Luo, 2021a, 2021b) or entangled subspaces (Baccari et al., 2020). Another interesting problem is to find new applications specially in cryptography with specific entanglement sets. In addition, it is unknown what kind of information is necessary for verifying a general set consisting of all entangled states. This might intrigue new entanglement models.

**Limitations of the study**

This paper is aimed to verify the entangled ensemble. The main limitation of the proposed method is from the simultaneous stabilizers. This requires all the involved states being in a specific subspace. Another is the nonconvexity of the involved subspace, which requires in principle nonlinear entanglement witnesses, or a set of linear witnesses.

**STAR METHODS**

Detailed methods are provided in the online version of this paper and include the following:

- **KEY RESOURCES TABLE**
- **RESOURCE AVAILABILITY**
  - Lead contact
  - Materials availability
  - Data and code availability
- **METHOD DETAILS**
  - Proof of Lemma 1
  - Robustness of bipartite entanglement witness
Proof of Theorem 2
Witnessing unknown entanglement set $S_{ghz}$
Verifying the nonlocality
Robustness against white noise
Nonlocality verified by violating the Svetlichny inequality
Verifying unknown W-type entanglement
Proof of Theorem 3
Verifying high-dimensional unknown GHZ-type entanglement
Bipartite entanglement
Multipartite entanglement

ACKNOWLEDGMENTS
This work is supported by the National Natural Science Foundation of China (Grants Nos. 62172341, 61303039, 12171044, 12075159, 11875167, and 12075001), Beijing Natural Science Foundation (Grant No. Z190005), Academy for Multidisciplinary Studies, Capital Normal University, Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology (Grant Nos. SIQSE202001, SIQSE202105), and the Academician Innovation Platform of Hainan Province.

AUTHOR CONTRIBUTIONS
M.X. conceived the study. M.X., S.M., and J.L. wrote the manuscript. All authors reviewed and critically revised the manuscript.

DECLARATION OF INTERESTS
The authors declare no competing interests.

Received: December 2, 2021
Revised: February 6, 2022
Accepted: February 17, 2022
Published: March 18, 2022

REFERENCES
Amico, L., Fazio, R., Osterloh, A., and Vedral, V. (2008). Entanglement in many-body systems. Rev. Mod. Phys. 80, 517–576. https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.80.517.
Baccari, F., Augusiak, R., Supic, I., and Acín, A. (2020). Device-independent certification of genuinely entangled subspaces. Phys. Rev. Lett. 125, 260507. https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.125.260507.
Bell, J.S. (1964). On the Einstein-Podolsky-Rosen paradox. Phys. I, 195. https://journals.aps.org/pp/10.1103/PhysicaPhysicaEpsicoe1.195.
Broadbent, A., Fitzsimons, J., and Kashefi, E. (2009). Universal blind quantum computation. In Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer (IEEE Computer society), pp. 517–527.
Brune, N., Cavalcanti, D., Pironio, S., Scarani, V., and Wehner, S. (2014). Bell nonlocality. Rev. Mod. Phys. 86, 419. https://link.aps.org/doi/10.1103/RevModPhys.86.419.
Clauser, J.F., Horne, M.A., Shimony, A., and Holt, R.A. (1969). Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. 23, 880–884. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.23.880.
Dehaene, J., and Moor, B.D. (2003). Normal forms and entanglement measures for multipartite quantum states. Phys. Rev. A. 68, 062318. https://journals.aps.org/pra/abstract/10.1103/PhysRevA.68.062318.
Dicke, R.H. (1954). Coherence in spontaneous radiation processes. Phys. Rev. 93, 99–110. https://link.aps.org/doi/10.1103/PhysRev.93.99.
Dur, W., Vidal, G., and Cirac, J.I. (2000). Three qubits can be entangled in two inequivalent ways. Phys. Rev. A. 62, 062314. https://link.aps.org/doi/10.1103/PhysRevA.62.062314.
Einstein, A., Podolsky, B., and Rosen, N. (1935). Can quantum mechanical description of physical reality be considered complete? Phys. Rev. 47, 777–780. https://journals.aps.org/pr/abstract/10.1103/PhysRev.47.777.
Gisin, N. (1991). Bell’s inequality holds for all nonproduct states. Phys. Lett. A. 154, 201. https://www.sciencedirect.com/science/article/abs/pii/0375960190908051.
Goldreich, O., and Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. J. Crypt. 7, 1–32. https://doi.org/10.1007/BF00195907.
Goldwasser, S., Micali, S., and Rackoff, C. (1989). The knowledge complexity of interactive proofs. SIAM J. Comput. 18, 186–208. https://epubs.siam.org/doi/abs/10.1137/0218012.
Greenberger, D.M., Horne, M.A., and Zeilinger, A. (1989). Going beyond Bell’s theorem. In Bell’s Theorem, Quantum Theory and Conceptions of the Universe, M. Kafatos, ed. (Kluwer), pp. 69–72.
Grilo, A.B., Slokstra, W., and Yuen, H. (2019). Perfect zero knowledge for quantum multiprover interactive proofs. In 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS), p. 611.
Gühne, O., and Seevinck, M. (2010). Separability criteria for genuine multiparticle entanglement. New J. Phys. 12, 053002. https://iopscience.iop.org/article/10.1088/1367-2630/12/5/053002/meta.
Gühne, O., and Tóth, G. (2009). Entanglement detection. Phys. Rep. 474, 1–75. https://www.sciencedirect.com/science/article/abs/pii/S0370157309000623.
Gühne, O., Tóth, G., Hyllus, P., and Briegel, H.J. (2005). Bell inequalities for graph states. Phys.
STAR METHODS

KEY RESOURCES TABLE

| REAGENT or RESOURCE | SOURCE | IDENTIFIER |
|---------------------|--------|------------|
| Other               |        | N/A        |
| EPR steering        | Einstein et al. (1935) | N/A |
| Entanglement        | Horodecki et al. (2009) | N/A |
| Bell nonlocality    | Bell (1964) | N/A |
| GHZ paradox         | Greenberger et al. (1989) | N/A |
| Entangled subspace  | Baccari et al. (2020) | N/A |
| Entanglement set    | This paper | N/A |

RESOURCE AVAILABILITY

Lead contact
Further information and requests for resources should be directed to the lead contact Ming-Xing Luo (mmlxuo@swjtu.edu.cn).

Materials availability
This study did not generate new materials.

Data and code availability
This study has no data and code available.

METHOD DETAILS

Proof of Lemma 1

Lemma 1. For any two-qubit state \( \rho \) on Hilbert space \( \mathcal{H}_A \otimes \mathcal{H}_B \), the following inequality holds
\[
2\sqrt{\rho_{00,11} \rho_{11,00} + \rho_{00,00} + \rho_{11,11}} - 1 \leq 0, \quad \text{(Equation 15)}
\]
if and only if \( \rho_{AB} \) is separable, where \( \rho_{ij,kl} \) denote density matrix components of \( \rho_{AB} \), that is, \( \rho_{AB} = \sum_{i,j,k,l} \rho_{ij,kl} |i\rangle \langle j| |k\rangle \langle l| \).

Proof. Let us consider an arbitrary separable two-qubit pure state \( |\Phi\rangle_{AB} = |\psi_1\rangle_A |\psi_2\rangle_B \) on Hilbert space \( \mathcal{H}_A \otimes \mathcal{H}_B \) with \( |\psi_j\rangle = \cos \theta_j |0\rangle + \sin \theta_j |1\rangle, \theta_j \in (0, \pi), j = 1, 2 \). It follows that \( \rho_{00,11} = \cos \theta_1 \sin \theta_1 \cos \theta_2 \sin \theta_2 \), and \( \rho_{01,01} = \rho_{10,10} = (\cos \theta_1 \sin \theta_1 \cos \theta_2 \sin \theta_2)^2 \). From the Hermitian symmetry of the density matrix \( \rho \), it implies
\[
2|\rho_{00,11}| = 2\sqrt{\rho_{01,01} \rho_{10,10}} \leq \rho_{01,01} + \rho_{10,10}, \quad \text{(Equation 16)}
\]
where the last inequality is due to the Cauchy-Schwarz inequality of \( 2\sqrt{xy} \leq x^2 + y^2 \).

Consider an arbitrary mixed separable state on Hilbert space \( \mathcal{H}_A \otimes \mathcal{H}_B \) given by
\[
\rho_{AB} = \sum_i p_i |\Phi_i\rangle_{AB} \langle \Phi_i| = \sum_{i,j,k,l} \rho_{ij,kl} |i\rangle \langle j| |k\rangle \langle l| , \quad \text{(Equation 17)}
\]
where \( |\Phi_i\rangle_{AB} \) are separable pure states defined by \( \rho_{ij,kl}^{(i)} = |\Phi_i\rangle \langle \Phi_i| \), and \( \{p_i\} \) is a probability distribution. From Equation (17) we get
\[
2\sqrt{\rho_{00,11} \rho_{11,00}} = 2|\rho_{00,11}| = 2\sum_i p_i |\rho_{00,11}^{(i)}| \leq 2\sum_i p_i |\rho_{00,11}^{(i)}| \leq \sum_i p_i \left( \rho_{01,01}^{(i)} + \rho_{10,10}^{(i)} \right), \quad \text{(Equation 18)}
\]
\begin{align}
01_{01} + 10_{10} \\
01_{00} - 11_{11}. 
\end{align}

(Equation 20)  

(Equation 21)  

The inequality (18) is followed from the convexity of function \( f(x) = |x| \). The inequality (19) is followed from the inequality (16). The equality (20) is from Equation (17). Equation (21) follows the trace equality of \( \text{Tr}_p = 1 \). Thus we have successfully proved the inequality (15).  

Robustness of bipartite entanglement witness

Consider a bipartite state with white noise on Hilbert space \( \mathcal{H}_A \otimes \mathcal{H}_B \) is given by

\begin{equation}
\rho_v = v \rho_{AB} + \frac{1 - v}{4},
\end{equation}

where \( v \) is the rank-4 identity operator on Hilbert space \( \mathcal{H}_A \otimes \mathcal{H}_B \) and \( v \in [0, 1] \). For the noisy state \( \rho_v \), the density matrix is given by

\[
\rho_v = \begin{pmatrix}
\frac{1 - v}{4} + v \rho_{00,00} & 0 & 0 & v \rho_{00,11} \\
0 & \frac{1 - v}{4} & 0 & 0 \\
0 & 0 & \frac{1 - v}{4} & 0 \\
v \rho_{00,11} & 0 & 0 & \frac{1 - v}{4} + v \rho_{11,11}
\end{pmatrix},
\]

where \( \rho_{00,00} \) and \( \rho_{11,11} \) satisfies \( \rho_{00,00} \cdot \rho_{11,11} \geq 0 \) and \( \rho_{00,00} + \rho_{11,11} = 1 \), and \( \rho_{00,11} \geq 0 \) (for simplicity, let us take \( \rho_{00,11} \) as a real number). From Lemma 1, \( \rho_v \) is a bipartite entanglement if \( v \) satisfies the following inequality

\begin{equation}
\frac{1}{v} > \frac{1}{1 + 4 \rho_{00,11}}.
\end{equation}

(Equation 23)  

For two observables \( \sigma_z \otimes \sigma_z \) and \( \sigma_x \otimes \sigma_x \), from Eq. (Robustness of bipartite entanglement witness) it is easy to prove that \( \rho_v \) satisfies

\begin{align}
\langle \sigma_z \otimes \sigma_z \rangle_{\rho_v} &= 0, \\
\langle \sigma_x \otimes \sigma_x \rangle_{\rho_v} &= 0.
\end{align}

(Equation 24)  

(Equation 25)  

Similarly, for two observables \( \sigma_z \otimes \sigma_x \) and \( \sigma_x \otimes \sigma_z \), from Eq. (Robustness of bipartite entanglement witness) it follows that

\begin{align}
\langle \sigma_z \otimes \sigma_x \rangle_{\rho_v} &= v, \\
\langle \sigma_x \otimes \sigma_z \rangle_{\rho_v} &= 2v \rho_{00,11}.
\end{align}

(Equation 26)  

(Equation 27)  

So, combining Equations 24–27 and the inequality (23), \( \rho_v \) is entangled if it satisfies the following statements as

\begin{align}
\langle \sigma_z \otimes \sigma_z \rangle_{\rho_v} &= 0, \\
\langle \sigma_x \otimes \sigma_x \rangle_{\rho_v} &= 0, \\
2 \langle \sigma_z \otimes \sigma_x \rangle_{\rho_v} + \langle \sigma_z \otimes \sigma_z \rangle_{\rho_v} &> 1.
\end{align}

(Equation 28)  

This has completed the proof.

Proof of Theorem 2

In this section we prove Theorem 2. The first subsection is for witnessing the unknown entanglement by using present generalized GHZ-type paradox (13) in the main text. The second subsection is for verifying the nonlocality. The third subsection is for the robustness against white noise while the last section is for verifying noisy state using the Svetlichny inequality.

Witnessing unknown entanglement set \( S_{ghz} \)

Similar to Lemma 1, we prove the following Lemma.

Lemma 2. For any \( n \)-qubit biseparable state \( \rho \) on Hilbert space \( \bigotimes_{j=1}^{n} \mathcal{H}_a_j \), the following inequality holds
\[2 \sqrt{\rho_{00}^{(i)} - \rho_{01}^{(i)} \rho_{10}^{(i)} - \rho_{11}^{(i)} + \rho_{11}^{(i)}} - 1 \leq 0, \quad \text{Equation (29)}\]

where \(\rho_n\) and \(\mathcal{T}_n\) denote respectively n-bit series 0⋯0 and 1⋯1, and \(\rho_{ij}^{(i)}\) are density matrix components defined by \(\rho_{ij}^{(i)} = \sum_{k=1}^{n} \rho_{kn,jk}^{(i)} |k\rangle \langle k|\).

**Proof of Lemma 2.** The proof is similar to Lemma 1 and a recent method (Gühne and Seevinck, 2010). Consider an arbitrary biseparable pure state (Svetlichny, 1987) on Hilbert space \(\mathcal{H}_{A_i}^{\otimes n}\) given by

\[|\Psi\rangle_{A_i \cdots A_n} = |\Psi_1\rangle\]

(Equation 30)

where \(|\Psi_1\rangle_{A_1 \cdots A_n} = \sum_{k=1}^{n} \alpha_{ki} |j_i\rangle |j_{i+1}\rangle \cdots |j_n\rangle\) is a \(s\)-qubit pure state on Hilbert space \(\mathcal{H}_{A_i}^{\otimes n}\)

and \(|\Psi_2\rangle_{A_1 \cdots A_n} = \sum_{j=1}^{n} \beta_{j1} |j_1\rangle |j_2\rangle \cdots |j_n\rangle\) and \(|\Psi_2\rangle_{A_1 \cdots A_n} = \sum_{j=1}^{n} \beta_{j1} |j_1\rangle |j_2\rangle \cdots |j_n\rangle\) is an \(n\)-qubit pure state on Hilbert space \(\mathcal{H}_{A_i}^{\otimes n}\). It follows that

\[|\rho_{\overline{0}_n: 1}_n| = |\alpha_0 - \alpha_0 \beta \beta \beta \beta - \alpha_0| = \sqrt{|\rho_{00}^{(i)} - \rho_{01}^{(i)} \rho_{10}^{(i)} - \rho_{11}^{(i)} + \rho_{11}^{(i)}|}

(Equation 31)

This implies that

\[2|\rho_{\overline{0}_n: 1}_n| = 2 \sqrt{|\rho_{00}^{(i)} - \rho_{01}^{(i)} \rho_{10}^{(i)} - \rho_{11}^{(i)} + \rho_{11}^{(i)}|} \leq |\rho_{00}^{(i)} - \rho_{01}^{(i)} \rho_{10}^{(i)} - \rho_{11}^{(i)} + \rho_{11}^{(i)}| \leq 1 - |\rho_{\overline{0}_n: 1}_n|.

(Equation 32)

Here, the inequality (32) is followed from the Cauchy-Schwarz inequality of \(2|ab| \leq a^2 + b^2\), and the inequality (32) has used the inequality of \(|\rho_{00}^{(i)} - \rho_{01}^{(i)} \rho_{10}^{(i)} - \rho_{11}^{(i)} + \rho_{11}^{(i)}| \leq 1 - |\rho_{\overline{0}_n: 1}_n|\).

Similarly, we can prove the inequality (32) for any mixed biseparable state in Equation (30) in terms of each bipartition of \(\{A_1, \cdots, A_n\}\). In what follows, consider a biseparable mixed state \(\rho_{bs}\) on Hilbert space \(\mathcal{H}_{A_i}^{\otimes n}\) as

\[\rho_{bs} = \sum_i \rho_i |\Psi_i\rangle_{A_i \cdots A_n} \langle \Psi_i| = \sum_{k=1}^{n} \sum_{j=1}^{n} \rho_{kn,jk}^{(i)} |j_1\rangle \langle k_1| \cdots |j_n\rangle \langle k_n|\]

(Equation 33)

where \(|\Psi_i\rangle_{A_i \cdots A_n}\) are biseparable pure states defined in Equation (30) with density matrices \(|\Psi_i\rangle_{A_i \cdots A_n} \langle \Psi_i| = \sum_{k=1}^{n} \rho_{kn,jk}^{(i)} |j_1\rangle \langle k_1| \cdots |j_n\rangle \langle k_n|\). From the inequality (32), it follows that

\[2 \sqrt{\rho_{00}^{(i)} - \rho_{01}^{(i)} \rho_{10}^{(i)} - \rho_{11}^{(i)} + \rho_{11}^{(i)}|} = 2 \sqrt{\rho_{00}^{(i)} - \rho_{01}^{(i)} \rho_{10}^{(i)} - \rho_{11}^{(i)} + \rho_{11}^{(i)}|}

(Equation 34)

\[\leq 2 \sum_i \rho_i |\rho_{00}^{(i)} - \rho_{01}^{(i)} \rho_{10}^{(i)} - \rho_{11}^{(i)} + \rho_{11}^{(i)}|\]

\[\leq \sum_i \rho_i \left| 1 - \rho_{00}^{(i)} - \rho_{01}^{(i)} - \rho_{10}^{(i)} - \rho_{11}^{(i)} \right|\]

(Equation 35)

\[= \sum_i \rho_i \left( 1 - \rho_{00}^{(i)} - \rho_{01}^{(i)} - \rho_{10}^{(i)} - \rho_{11}^{(i)} \right)\]

(Equation 36)

\[= 1 - \rho_{00}^{(i)} - \rho_{01}^{(i)} - \rho_{10}^{(i)} - \rho_{11}^{(i)}\]

(Equation 37)

Here, the inequality (34) is followed from the convexity of the function \(f(x) = |x|\). The inequality (35) is from the inequality (32). The inequality (36) is obtained from the equality \(1 - \rho_{00}^{(i)} - \rho_{01}^{(i)} - \rho_{10}^{(i)} - \rho_{11}^{(i)} \leq 1\). The equality (37) is from Equation (33). This has proved the inequality (29).
Now, continue to prove Theorem 2. The generalized GHZ-type entangled state reads
\[ \rho_{A_1\ldots A_n} = \mathcal{E}(\rho(\theta))(\rho(\theta)), \]

(Equation 38)
where \(|\Phi(\theta)\rangle\) is a generalized GHZ state given by
\[ |\Phi(\theta)\rangle_{A_1\ldots A_n} = \cos \theta |0\rangle^{\otimes n} + \sin \theta |1\rangle^{\otimes n}, \]
with \(\theta \in (0, \pi)\) and \(\mathcal{E}(\cdot)\) is local phase transformation defined by
\[ \mathcal{E}(\rho) = \sum_{j=1}^{n} \rho_j \otimes \rho_{A_1\ldots A_n}(U_j) \]
with unknown parameters \(\theta_j, \phi_j \in (0, \pi)\), and any unknown probability distribution \(\{p_j\}\). With these notions, the entanglement set \(S_{\text{ghz}}\) is given by
\[ S_{\text{ghz}} = \{\rho, \forall |\Phi(\theta)\rangle, \mathcal{E}(\cdot)\} \]
(Equation 40)
The goal is to witness the entanglement set \(S_{\text{ghz}}\) by using the generalized GHZ-like paradox (13) in the main text and Lemma 2.

We firstly prove that any entanglement \(\rho \in S_{\text{ghz}}\) satisfies the paradox (13). In fact, it is forward to check any entangled state in Equation (38) satisfies the first three equalities of the paradox (14) from the fact that \(|\Phi(\theta)\rangle_{A_1\ldots A_n}\) in Equation (39) satisfies these equalities for any \(\theta \in (0, \pi)\).

For any state \(\rho_{A_1\ldots A_n} \in S_{\text{ghz}}\), it is rewritten into
\[ \rho_{A_1\ldots A_n} = \rho_{A_1\ldots F_{j=1}^{n} A_n} \rightarrow |\overline{0}_n\rangle \langle 0_n| + \rho_{A_1\ldots T_{j=1}^{n} A_n} \rightarrow |\overline{1}_n\rangle \langle 1_n| \]
+ \rho_{A_1\ldots T_{j=1}^{n} A_n} \rightarrow |\overline{1}_n\rangle \langle 0_n| + \rho_{A_1\ldots T_{j=1}^{n} A_n} \rightarrow |\overline{0}_n\rangle \langle 1_n| \]
(Equation 41)
where \(\{\rho_{A_1\ldots F_{j=1}^{n} A_n} \rightarrow |\overline{0}_n\rangle \langle 0_n|, \rho_{A_1\ldots T_{j=1}^{n} A_n} \rightarrow |\overline{1}_n\rangle \langle 1_n|\}\) is a probability distribution, and \(\rho_{A_1\ldots F_{j=1}^{n} A_n} \rightarrow \rho_{A_1\ldots T_{j=1}^{n} A_n} \rightarrow \beta_{A_n} |\overline{1}_n\rangle \langle 0_n|\). From Lemma 2, \(\rho\) is an n-partite entanglement in the biseparable model (Svetlichny, 1987) if \(\beta_{A_n} \neq 0\). Otherwise, \(\rho\) is a biseparable state with the following decomposition
\[ \rho = \rho_{A_1\ldots F_{j=1}^{n} A_n} \rightarrow |\overline{0}_n\rangle \langle 0_n| + \rho_{A_1\ldots T_{j=1}^{n} A_n} \rightarrow |\overline{1}_n\rangle \langle 1_n| = \sum_{i=1}^{2^n} \rho_i |\Phi(\theta)_i\rangle \langle \Phi(\theta)_i| + |\Phi(\theta)_i\rangle \langle \Phi(\theta)_i| \]
(Equation 42)
where \(\{\Phi(\theta)_i\}, \Phi(\theta)^{-1}\}\) are orthogonal states for any \(\theta\). This further implies that the inequality (29) is sufficient and necessary for witnessing the entanglement set \(S_{\text{ghz}}\). Hence, any state in \(S_{\text{ghz}}\) is an n-partite entanglement if and only if the paradox (13) holds.

In the following, we prove any biseparable state violates one statement in the paradox (13). In fact, consider an n-qubit biseparable pure state \(|\psi\rangle_{A_1\ldots A_n} = |\psi\rangle_{A_1\ldots A_n}\rangle_{A_1\ldots A_n}\) on Hilbert space \(\mathcal{H}_{A_1\ldots A_n}\). From all the equalities of the paradox (13), \(\psi\) is represented by the state \(|0\rangle^{\otimes n} \text{or} |1\rangle^{\otimes n}\) while \(|\psi\rangle\) is represented by the state \(|0\rangle^{\otimes n} |0\rangle^{\otimes n-1} |1\rangle^{\otimes n-2}\). Otherwise, \(\psi\) will violate one statement in the paradox (13). Generally, consider a general n-qubit mixed biseparable state \(\rho_{bs}\) on Hilbert space \(\mathcal{H}_{A_1\ldots A_n}\) given by
\[ \rho_{bs} = \sum_{\rho_{bs}} \rho_{bs}^{(1)} \otimes \rho_{bs}^{(2)} \]
(Equation 43)
where \(\rho_{bs}^{(1)}, \rho_{bs}^{(2)}\) denote pure states of the systems in the set \(I\) of \(\{A_1, \ldots, A_n\}\). \(\rho_{bs}^{(1)}\) denote pure states of the systems in the complement set \(I\) of \(\{A_1, \ldots, A_n\} - \{I\}\) a probability distribution. So, \(\rho_{bs}\) can only be a diagonal state given by
\[ \rho_{bs} = \rho_{bs}^{(1)} |\overline{0}_n\rangle \langle 0_n| + \rho_{bs}^{(2)} |\overline{1}_n\rangle \langle 1_n| \]
(Equation 44)
if all the equalities in the paradox (13) hold. This implies \(\rho_{bs}^{(1)} \otimes \rho_{bs}^{(2)} = 0\), that is, \(\rho_{bs}\) violates the last inequality of the paradox (13). So, any biseparable state violates at least one equality or the last inequality of the paradox (13).

Verifying the nonlocality
We verify the nonlocality by using the generalized GHZ-type paradox (13). Denote the supposedly definite real values of \(X_j\) and \(Y_{j}\) for the \(j\)-th party, with \(X_j, Y_{j} \in \{-1, 1\}\) beyond the integers in the standard GHZ paradox (Greenberger et al., 1989), \(j = 1, \ldots, n\). Similar to the analysis of the GHZ paradox, classically we have from the first two statements in Equation (13) that...
Moreover, combining with the third to sixth statements in Equation (13), we get
\[ \forall i \neq j : \rho_{ij} = 0, \quad (j = 1, \cdots, n). \]  
(Equation 46)
This contradicts to the last relation of \(\prod_{i=1}^{n} \forall_i \neq 0\) in Equation (13). This completes the proof.

**Robustness against white noise**
Consider an unknown \(n\)-partite entangled state with white noise on Hilbert space \(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \cdots \otimes \mathcal{H}_N\) as
\[ \psi = \rho_{\text{A}} \otimes \rho_{\text{B}} \otimes \cdots \otimes \rho_{\text{N}}, \]
where \(\rho_{\text{A}}\) is a rank-2 \(\rho\) square identity matrix, \(\rho\) is defined in Equation (38), and \(\forall \rho \geq 0\). Its density matrix is given by
\[ \rho_v = \frac{1}{2^n} \left[ \left( 1 - v + \rho \right) |0\rangle\langle 0| + \left( 1 - v + \rho \right) |1\rangle\langle 1| \right] + \rho \sum_{j=1}^{n} |j\rangle\langle j|, \]
(Equation 48)
where \(\rho = \sum_i \rho_i \otimes \rho_i \otimes \cdots \otimes \rho_i = 0\), \(\rho_i = 1\), \(\rho_i = 1\), \(\rho = 0\) from the definition in Equation (38). \(\sum_j |j\rangle\langle j|\) is an n-bit series. From Lemma 2, the noisy state \(\psi\) is an \(n\)-partite entanglement in the biseparable model (Svetlichny, 1987) if \(v \geq 1\) satisfies the following inequality
\[ v \geq 1 + 4\rho \sum_{j=1}^{n} |j\rangle\langle j|. \]  
(Equation 49)

For \(2n\) separable observables \(\{a_1^{(3)} \otimes a_3^{(n)}, a_2^{(3)} \otimes a_3^{(n)}, a_3^{(3)} \otimes a_3^{(n)}, a_1^{(3)} \otimes a_1^{(n)}, a_2^{(3)} \otimes a_2^{(n)}, a_3^{(3)} \otimes a_3^{(n)} \}, i = 1, \cdots, n - 1\), from Equation (48) it is easy to prove that
\[ \sum_{j=1}^{n} |j\rangle\langle j| , \sum_{j=1}^{n} \left( |j\rangle\langle j| + 1 \right) = n. \]  
(Equation 50)
\[ \sum_{j=1}^{n} |j\rangle\langle j| , \sum_{j=1}^{n} \left( |j\rangle\langle j| + 1 \right) = n. \]  
(Equation 51)
\[ \sum_{j=1}^{n} |j\rangle\langle j| , \sum_{j=1}^{n} \left( |j\rangle\langle j| + 1 \right) = n. \]  
(Equation 52)
Similarly, for \(n + 1\) observables \(a_1^{(3)} \otimes a_3^{(n)}, a_2^{(3)} \otimes a_3^{(n)}, a_3^{(3)} \otimes a_3^{(n)}\), \(i = 1, \cdots, n - 1\) and \(a_1^{(3)} \otimes \cdots \otimes a_3^{(n)}\), from Equation (48) it follows that
\[ \sum_{j=1}^{n} |j\rangle\langle j| , \sum_{j=1}^{n} \left( |j\rangle\langle j| + 1 \right) = n. \]  
(Equation 53)
\[ \sum_{j=1}^{n} |j\rangle\langle j| , \sum_{j=1}^{n} \left( |j\rangle\langle j| + 1 \right) = n. \]  
(Equation 54)
\[ \sum_{j=1}^{n} |j\rangle\langle j| , \sum_{j=1}^{n} \left( |j\rangle\langle j| + 1 \right) = n. \]  
(Equation 55)
\[ \sum_{j=1}^{n} |j\rangle\langle j| , \sum_{j=1}^{n} \left( |j\rangle\langle j| + 1 \right) = n. \]  
(Equation 56)
So, from Equations 50–56 and the inequality (49), \(\psi\) is \(n\)-partite entangled (Svetlichny, 1987) if it satisfies the following statements
\[ \sum_{j=1}^{n} |j\rangle\langle j| , \sum_{j=1}^{n} \left( |j\rangle\langle j| + 1 \right) = n. \]  
(Equation 57)

\[ v \geq 1 + 4\rho \sum_{j=1}^{n} |j\rangle\langle j|. \]  
(Equation 49)

**Nonlocality verified by violating the Svetlichny inequality**
Another method for verifying the multipartite nonlocality of noisy state is using the Svetlichny inequality (Svetlichny, 1987) with the known density matrix. Take a tripartite GHZ-type state in Equation (48) as an example. For simplicity, we can restrict measurement along directions lying in the x-y plane of Pauli sphere,
so that two observables $A_i$ and $A_i'$ of the $i$-th party are specified by the azimuthal angles $\varphi_i$ and $\varphi_i'$, respectively, for $i = 1, 2, 3$. For the noisy state in Equation (47) with $n = 3$, it follows that

\[
\begin{align*}
\langle A_iA_iA_i \rangle_{\rho} &= 2\nu_{000,111}\cos(\varphi_i + \varphi_2 + \varphi_3), \\
\langle A_iA_i'A_i' \rangle_{\rho} &= 2\nu_{000,111}\cos(\varphi_i + \varphi_2 + \varphi_3), \\
\langle A_iA_i'A_i' \rangle_{\rho} &= 2\nu_{000,111}\cos(\varphi_i + \varphi_2 + \varphi_3), \\
\langle A_i'A_iA_i' \rangle_{\rho} &= 2\nu_{000,111}\cos(\varphi_i' + \varphi_2 + \varphi_3), \\
\langle A_i'A_i'A_i' \rangle_{\rho} &= 2\nu_{000,111}\cos(\varphi_i' + \varphi_2 + \varphi_3), \\
\langle A_i'A_i'A_i' \rangle_{\rho} &= 2\nu_{000,111}\cos(\varphi_i' + \varphi_2 + \varphi_3), \\
\langle A_i'A_i'A_i' \rangle_{\rho} &= 2\nu_{000,111}\cos(\varphi_i' + \varphi_2 + \varphi_3).
\end{align*}
\] (Equation 58)

From Equation (58), we get

\[
\|SV\|_v = \langle A_1A_2A_3 \rangle + \langle A_1A_2A_3' \rangle + \langle A_1A_2'A_3 \rangle - \langle A_1A_2'A_3' \rangle - \langle A_1A_2A_3 \rangle - \langle A_1A_2'A_3 \rangle
\] (Equation 59)

\[
= 8\sqrt{2}\nu_{000,111},
\]

where $\varphi_1 + \varphi_2 + \varphi_3 = \frac{\pi}{2}$ and $\varphi_i' = \varphi_i + \frac{\pi}{2}$. The noise visibility is given by

\[
1 \geq v' > \frac{1}{2\nu_{000,111}}
\] (Equation 60)

for a known state $\rho$, as shown in Figure 4. It should be interesting to explore other Bell-type inequalities with greater noise visibility.

![Figure 4. (Color online) Visibility of white noise for $\rho$, in Equation (47)](image)

Here, $n = 3$. The blue line denotes the witnessed visibility given in Equation (49) with unknown density matrix. The red line denotes the verified visibility given in Equation (60) by using the Svetlichny inequality (Svetlichny, 1987) with known density matrix.

**Verifying unknown W-type entanglement**

Our goal here is for verifying unknown W-type entanglement. Consider a three-qubit system W-type entangled state (Dur et al., 2000) on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ given by

\[
|\Psi\rangle_{ABC} = a_0|001\rangle + a_1|010\rangle + a_2|100\rangle + a_3|111\rangle,
\] (Equation 61)

where $a_i$'s are real parameters satisfying $\sum_{i=0}^{3} |a_i|^2 = 1$. Suppose $|\Psi\rangle_{ABC}$ is shared by three parties, Alice, Bob, and Charlie who only know the shared state being the following form:

\[
\rho_{ABC} = \mathcal{E}(|\Psi\rangle\langle\Psi|),
\] (Equation 62)

where $\mathcal{E}(\cdot)$ is a local channel defined by

\[
\mathcal{E}(\rho) = \sum_j \rho (U_j \otimes V_j \otimes Y_j) \mathcal{E}(U'_j \otimes V'_j \otimes Y'_j),
\] (Equation 63)
according to local unknown phase rotations $U_i, V_i$ and $Y_j$ defined in Equation (11) in the main text, and $\{p_j\}$ is an unknown probability distribution. The entanglement involved in the state $\rho_{ABC}$ is named as the W-type entanglement.

Under the local channel $\mathcal{E}(\cdot)$, the density matrix $\rho_{ABC}$ in Equation (62) can be rewritten into the following form

$$\rho_{ABC} = \sum_{h+j+k=1,3} \rho_{h,j,k}|h,j,k\rangle\langle h,j,k|$$

(Equation 64)

where $\rho_{h,j,k}$ satisfy that $\{\rho_{h,j,k}\}$, being a probability distribution and $\rho_{h,j,k} = \rho_{k,j,h}$. Our goal in what follows is to verify the entanglement set

$$S_w := \{\mathcal{E}(\langle \psi | \phi \rangle), \langle \psi | \psi \rangle, \mathcal{E}(\cdot)\}$$

(Equation 65)

which is spanned by the basis $\{|h,j,k\rangle|v_j + j_2 + k_1 + k_2 + k_3 = 1, 3\}$.

The entanglement set $S_w$ is not convex because the separable state $\rho_{ABC} = \sum_{d-1} \rho_{h,j,k}\{|h,j,k\rangle\langle h,j,k|}$ has the decomposition in Equation (64). This rules out the linear entanglement witnesses (Horodecki et al., 2009). Similar to Theorem 2, we have the following Theorem 2'.

**Theorem 2'.** The entanglement set $S_w$ is verifiable if

$$\sqrt{\rho_{011.111}^2 + \rho_{010.100}^2 + \rho_{001.111}^2 + \rho_{010.100}^2 + \rho_{100.111}^2 + \rho_{100.111}^2} > \frac{1}{4}$$

(Equation 66)

**Proof.** Similar to the generalized GHZ-like paradox (13) in the main text, we present a paradox for W states $\rho \in S_w$ as

$$\langle \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \rangle_{\rho} = -1, \langle \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \rangle_{\rho} = 0, \langle \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \rangle_{\rho} = 0, \langle \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \rangle_{\rho} = 0, \langle \sigma_1^{(1)} \otimes \sigma_2^{(2)} \rangle_{\rho}^{\text{ES}} \neq 0, \langle \sigma_1^{(1)} \otimes \sigma_2^{(2)} \rangle_{\rho}^{\text{ES}} \neq 0.$$

(Equation 67)

The proof of the nonlocality with definite real values of both parties is similar to its for Theorem 2. Specially, denote the supposedly definite real values of $v_{1_2}$ and $v_{1_3}$ for Alice, $v_{2_2}$ and $v_{2_3}$ for Bob, and $v_{3_2}$ and $v_{3_3}$ for Charlie, with $v_{1_2}, v_{1_3} \in (1, -1)$. From the first statement in Equation (67) we have $v_{1_2} v_{2_2} v_{2_3} = 1$ while implies $v_{2_2} \neq 0$. Combined with the second to fourth statements in Equation (67), it follows that $v_{2_3} = 0$ for any $j$. This conflicts with the last relation.

Next, we prove any biseparable state would violate one statement in the paradox (67). For any biseparable state $\rho_{bs}$ on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, it violates the first statement in the paradox (67) if it does not has the decomposition (64). Otherwise, $\rho_{bs}$ has the decomposition (64). From Equation (67), we have

$$\langle \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \rangle_{\rho_{bs}} = -1, \langle \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \rangle_{\rho_{bs}} = 0, \langle \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \rangle_{\rho_{bs}} = 0, \langle \sigma_1 \otimes \sigma_2 \otimes \sigma_3 \rangle_{\rho_{bs}} = 0, \langle \sigma_1^{(1)} \otimes \sigma_2^{(2)} \rangle_{\rho_{bs}} = 2 \sqrt{\rho_{011.111}^2 + \rho_{111.000}^2 + 2 \sqrt{\rho_{111.100}^2 + \rho_{000.010}^2}}$$

(Equation 68)

$$\langle \sigma_1^{(1)} \otimes \sigma_2^{(2)} \rangle_{\rho_{bs}} = 2 \sqrt{\rho_{011.111}^2 + \rho_{111.000}^2 + 2 \sqrt{\rho_{111.100}^2 + \rho_{000.010}^2}}$$

It will violate the inequality (66), that is, for any bisasurable state we have

$$\sqrt{\rho_{011.111}^2 + \rho_{111.000}^2 + 2 \sqrt{\rho_{111.100}^2 + \rho_{000.010}^2}} \leq \frac{1}{4}$$

(Equation 69)

Hence, this has completed the proof.
Now, before ending the proof we prove the inequality (69). Consider an arbitrary biseparable pure state on Hilbert space \( H_A \otimes H_B \otimes H_C \) as
\[
|\Phi\rangle_{ABC} = |\psi_1\rangle_A |\psi_2\rangle_B |\psi_3\rangle_C \tag{Equation 70}
\]
where \(|\psi_1\rangle = a_0|0\rangle + a_1|1\rangle\) and \(|\psi_2\rangle = \sum_{i,j=0,1} b_{ij}|ij\rangle\), with \(\sum_{i,j=0,1}^1 a_{ij}^2 = 1\) and \(|\psi_3\rangle = \sum_{i,j=0,1} b_{ij}^2 = 1\). Similar to proof of Lemma 2, we can prove that
\[
2\sqrt{p_{001,111}p_{111,000}} \leq p_{011,011} + p_{101,101} \tag{Equation 71}
\]
\[
2\sqrt{p_{001,010}p_{100,010}} \leq p_{001,010} + p_{100,010} \tag{Equation 72}
\]
Moreover, from the positive semidefinite density matrix \(p\), all the principal minors are positive semidefinite. Combining with the Cauchy-Schmidt inequality, we get
\[
2\sqrt{p_{001,010}p_{100,010}} \leq \sqrt{p_{001,001}p_{100,010}} \tag{Equation 73}
\]
and
\[
2\sqrt{p_{100,111}p_{111,100}} \leq \sqrt{p_{100,100}p_{111,111}} \tag{Equation 74}
\]
From the inequalities (71)-(74), we get
\[
\sqrt{p_{001,111}p_{111,000}} + \sqrt{p_{010,100}p_{010,010}} + \sqrt{p_{001,010}p_{100,010}} + \sqrt{p_{100,111}p_{111,100}} \leq \sum_{i,j,k=0,1} p_{ijkl} = 1 \tag{Equation 75}
\]
For other two biseparable states, we can similarly prove the inequality (75). Moreover, for any mixed biseparable states \(p_{ijkl} = \sum_i |\Phi_i\rangle \langle \Phi_i|\) with product states \(|\Phi_i\rangle\), from the concavity of function \(f(x) = \sqrt{x}\) it follows that
\[
\sqrt{p_{001,111}p_{111,000}} + \sqrt{p_{010,100}p_{010,010}} + \sqrt{p_{001,010}p_{100,010}} + \sqrt{p_{100,111}p_{111,100}} \leq \sum_i \sqrt{\rho_{ij,kl}^{(i)}} + \sqrt{\rho_{ijkl}^{(i)}} \tag{Equation 76}
\]
from the inequality (75), where \(\rho_{ijkl}^{(i)}\) are density matrix elements defined by \(|\Phi_i\rangle \langle \Phi_i| = \sum_i \rho_{ijkl}^{(i)} |ij\rangle \langle kj|\). This has proved the inequality (66).

**Proof of Theorem 3**

Consider an \(n\)-partite quantum network \(N\) shared by \(n\) parties \(A_1, \ldots, A_n\). The total state of \(N\) is given by
\[
p_{ijkl} = \otimes_{j=1}^m p_{ijkl} \otimes_{k=1}^n p_{ijkl} \tag{Equation 77}
\]
where \(p_j\) are generalized EPR entangled states defined in Equation (1) in the main text and \(q_k\) are multipartite GHZ entangled states defined in Equation (12) in the main text. Denote the triple \((A_j, \theta_j, (k_j, s_j))\) as the specification of a local controlled-phase
\[
CP(\theta_j) = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + e^{i\theta}|11\rangle\langle 11| \tag{Equation 78}
\]
performed by \(A_j\) on two qubits from entangled states \(p_{ijkl}\) and \(q_k\). Let \(\mathcal{G} = \{(A_j, \theta_j, (k_j, s_j)), \forall j\}\) be the set of all specifications for generating a cluster state.

Define cluster-type entanglement set \(S_{ij}\) as
\[
S_{ij} = \{E \in \mathcal{C}(p_{ijkl}), \forall p_{ijkl}, E(\cdot), \mathcal{C}(\cdot)\} \tag{Equation 79}
\]
where \(\mathcal{E}(\cdot)\) is a blind quantum channel consisting of local phase rotations on each qubit, e.g., \(\mathcal{E}(p) = \otimes_{j=1}^m \mathcal{E}_j(\theta_j) \otimes_{k=1}^n \mathcal{E}_k(q_k)|ij\rangle \langle kj|\) with \(\mathcal{E}_j(\cdot)\) defined in Equation (2) (in the main text) and \(\mathcal{E}_k(\cdot)\) defined in Equation (11)
We firstly prove two lemmas.

**Lemma 3.** Consider any unknown m-partite entanglement \( \rho_{A_1 \cdots A_m} \) in Equation (11) shared by \( n \) parties \( A_1, \cdots, A_n \). Then any two parties \( A_i \) and \( A_j \) can share one unknown bipartite entanglement in Equation (2) assisted by other’s local operations and classical communication (LOCC).

**Proof of Lemma 3.** Consider any unknown multipartite GHZ-type \( \rho_{A_1 \cdots A_m} \) given in Equation (11). For any two parties \( A_i \) and \( A_j \), suppose other parties perform local projection measurement under the basis \( \{ | \pm \rangle = \frac{1}{\sqrt{2}} (|0angle \pm |1\rangle) \} \) and send out measurement outcomes \( a_k \in \{1, \cdots, n\} \setminus \{i, j\} \). The resultant conditional on outcomes \( a_k \)’s is given by

\[
\rho_{A_i A_j} = p_{\pm} |00\rangle \langle 00| + p_{\pm} |11\rangle \langle 11| + (-1)^{a_k} p_{\pm} |00\rangle \langle 01| + (-1)^{a_k} p_{\pm} |11\rangle \langle 10|
\]

(Equation 80)

which can be locally transformed into

\[
\rho_{A_i A_j} = p_{\pm} |00\rangle \langle 00| + p_{\pm} |11\rangle \langle 11| + \sum_{a_k} (-1)^{a_k} p_{\pm} |00\rangle \langle 11| + \sum_{a_k} (-1)^{a_k} p_{\pm} |11\rangle \langle 00|
\]

(Equation 81)

after one party performs a local rotation \( |0\rangle \langle 0| + (-1)^{a_k} |1\rangle \langle 1| \) on its shared qubit. From Lemmas 1 and 2, \( \rho_{A_i A_j} \) is an entanglement in Equation (2) if and only if \( \rho_{A_1 \cdots A_m} \) is an entanglement (i.e., \( p_{\pm} |00\rangle \langle 00| + p_{\pm} |11\rangle \langle 11| \neq 0 \)). This has completed the proof.

**Lemma 4.** Consider a chain quantum network consisting of any two unknown entangled states \( \rho_{AB} \) and \( \rho_{CD} \) in Equation (2), where Alice has qubit A, Bob has two qubits B and C while Charlie has qubit D. Then Alice and Charlie can share one unknown entanglement in Equation (2) assisted by Bob’s LOCC.

**Proof of Lemma 4.** Consider a chain quantum network consisting of any two unknown states \( \rho_{AB} = \sum_{j,k} \rho_{ij,j} |j\rangle \langle k| \) and \( \rho_{CD} = \sum_{j,k} \rho_{ik,j} |j\rangle \langle k| \) in Equation (2). Suppose Charlie performs joint measurement on two qubits B and C under the Bell basis \( \{|\phi_\pm\rangle = \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle), |\psi_\pm\rangle = \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle) \} \). It follows the resultant as

\[
\rho_{AD} = \frac{1}{p_{00, 00} p_{00, 00} + p_{11, 11} p_{11, 11}} \left( p_{00, 00} p_{00, 00} |00\rangle \langle 00| + p_{00, 11} p_{00, 11} |00\rangle \langle 11| + p_{11, 00} p_{11, 00} |11\rangle \langle 00| + p_{11, 11} p_{11, 11} |11\rangle \langle 11| \right)
\]

(Equation 82)

for the measurement outcomes \( |\phi_\pm\rangle \). Both above states can be locally transformed into

\[
\rho_{AD} = \frac{1}{p_{00, 00} p_{00, 00} + p_{11, 11} p_{11, 11}} \left( p_{00, 00} p_{00, 00} |00\rangle \langle 00| + p_{00, 11} p_{00, 11} |00\rangle \langle 11| + p_{11, 00} p_{11, 00} |11\rangle \langle 00| + p_{11, 11} p_{11, 11} |11\rangle \langle 11| \right)
\]

(Equation 83)

after one party performs a local rotation \( \sigma_z \) on its shared qubit for the measurement outcome \( |\phi_\pm\rangle \). Similarly, for the measurement outcomes \( |\psi_\pm\rangle \), the resultant is given by

\[
\rho_{AD} = \frac{1}{p_{11, 11} p_{00, 00} + p_{00, 00} p_{11, 11}} \left( p_{11, 11} p_{00, 00} |01\rangle \langle 01| + p_{11, 00} p_{11, 00} |01\rangle \langle 10| + p_{00, 11} p_{00, 11} |10\rangle \langle 01| + p_{00, 00} p_{00, 00} |10\rangle \langle 10| \right)
\]

(Equation 84)

which can be locally transformed into

\[
\rho_{AD} = \frac{1}{p_{11, 11} p_{00, 00} + p_{00, 00} p_{11, 11}} \left( p_{11, 11} p_{00, 00} |01\rangle \langle 01| + p_{11, 00} p_{11, 00} |01\rangle \langle 10| + p_{00, 11} p_{00, 11} |10\rangle \langle 01| + p_{00, 00} p_{00, 00} |10\rangle \langle 10| \right)
\]

(Equation 85)
with a local phase shift conditional on measurement outcome. So, from Lemmas 1 and 2, both states in Equations (83) and (85) are entangled states in Equation (2) if and only if $\rho_{AB}$ and $\rho_{CD}$ are entangled (i.e., $\rho_{0011}, \rho_{1100}, \rho_{0011}, \rho_{1100} \neq 0$). This has completed the proof. □

**Proof of Theorem 3.** Note $C(\cdot)$ does not change the entanglement of the joint state $\mathcal{E}(\rho_j)$ because it consists of all the local unitary operations. From the equality of $\mathcal{E}^{\ast}(\rho_j) = \mathcal{E}(\mathcal{C}(\rho_j))$, it is sufficient to verify all the states $\mathcal{E}(\rho_j)$. Moreover, from the assumption of connectedness the joint state $\rho_j$ is entangled in the biseparable model (Svetlichny, 1987) if the associated quantum network $\mathcal{N}_q$ is connected. This can be verified by using the recent method (Luo, 2021a, 2021b) combined with Lemmas 3 and 4, that is, each pair can share one bipartite entangled state with the help of other parties’ local measurements and classical communication. From Equation (79), it only needs to verify all the entangled states $\mathcal{E}_j(\rho_j)$ and $\mathcal{E}_k(\rho_k)$.

The main idea is to combine the paradoxes (5) and (13) in the main text. Specially, for a given N-partite cluster state $\varrho_{\text{cl}} \in S_d$ on Hilbert space $\otimes_{j=1}^d \mathcal{H}_j$, it satisfies the following statements as

\[
\begin{align*}
\langle \sigma^{(j)} \otimes \sigma^{(j)} \rangle_{\varrho_{\text{cl}}} &= 1, (A_j, A_j) \in \{\rho_j, \forall s\} \cup \{\tau_j, \forall t\} \\
\langle \sigma^{(j)} \otimes \sigma^{(j)} \rangle_{\varrho_{\text{cl}}} &= 0, (A_j, A_j) \in \{\rho_j, \forall s\} \cup \{\tau_j, \forall t\} \\
\langle \sigma^{(j)} \otimes \sigma^{(j)} \rangle_{\varrho_{\text{cl}}} &= 0, (A_j, A_j) \in \{\rho_j, \forall s\} \cup \{\tau_j, \forall t\}
\end{align*}
\]

\[(\text{Equation 86)} \quad \text{(Equation 87)} \quad \text{(Equation 88)}
\]

where the statement for $(A_j, A_j) \in \{\rho_j, \forall s\} \cup \{\tau_j, \forall t\}$ in Equations 86–88 means both qubits $A_j$ and $A_j$ belong to one EPR-type entanglement (2) or one GHZ-type entanglement (12). The statement for $(A_j, A_j) \in \{\rho_j, \forall s\}$ in Equation (89) means both qubits $A_j$ and $A_j$ belong to one EPR-type entanglement (2). The statement of $\tau_j \in \{\tau_j, \forall t\}$ in Equation (90) means all the qubits $\tau_j$ belong to one multipartite GHZ-type entanglement (12).

Similar to the paradoxes (5) and (13), Equations 86–90 are used for verifying the entanglement for single EPR-type entanglement or GHZ-type entanglement in the cluster state $\varrho$. This completes the proof. □

**Verifying high-dimensional unknown GHZ-type entanglement**

Our goal in this section is to extend Theorems 1 and 2 for verifying high-dimensional unknown GHZ-type entanglement. Consider a d-dimensional Hilbert space $\mathcal{H}$ with computation basis $\{0, \ldots, |d - 1\rangle\}$, where $d \geq 2$. Denote $\omega = \exp(2\pi i / d)$ as the root of unity, that is, $\omega^d = 1$ and $\omega \neq 1$. Define $\Sigma_1$ be the shift operator (Weyl, 2014, Ch.III) (similar to Pauli operator $\sigma_j$) given by

\[\Sigma_1 = \sum_{j=0}^{d-1} j + 1 \mod d |j\rangle \langle j|\]

and $\Sigma_1$ be the clock operator (similar to Pauli operator $\sigma_j$) matrix given by

\[\Sigma_1 = \sum_{j=0}^{d-1} \omega^j |j\rangle \langle j|\]

\[(\text{Equation 91)} \quad \text{(Equation 92)}
\]

It is easy to check that

\[(\Sigma_1)^{d-1} = (\Sigma_2)^d = 1\]

with the identity operator 1 on $\mathcal{H}$. Both operators $\Sigma_1$ and $\Sigma_2$ are fundamental operations for quantum dynamics in high-dimensional spaces (Vourdas, 2004).

**Bipartite entanglement**

Consider a two-qudit system $|\Phi\rangle_{AB}$ on Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are both d-dimensional spaces. A bipartite entangled pure state shared by Alice and Bob is given by

\[|\Phi\rangle_{AB} = \sum_{j=0}^{d-1} a_j |j\rangle |j\rangle\]

\[(\text{Equation 94)}
\]
where \( a_i \) are real parameters satisfying \( \sum_{i=0}^{d-1} a_i^2 = 1 \). Suppose that both parties only know the shared state has the following form:

\[
\rho_{AB} = \mathcal{E}(\Phi)(\Phi),
\]

(Equation 95)

where \( \mathcal{E}(\cdot) \) is a blind quantum channel defined by

\[
\mathcal{E}(\sigma) = \sum_j \rho_j (U_j \otimes V_j) \sigma (U_j^\dagger \otimes V_j^\dagger).
\]

(Equation 96)

with local phase transformations \( U_j \) and \( V_j \) given respectively by

\[
U_j = \sum_{k=0}^{d-1} e^{i\theta_k} |k\rangle |k\rangle,
\]

(Equation 97)

\[
V_j = \sum_{k=0}^{d-1} e^{i\phi_k} |k\rangle |k\rangle,
\]

with unknown parameters \( \theta_k, \phi_k \in (0, \pi) \), and \( \{\rho_j\} \) is an unknown probability distribution. In general, \( \mathcal{E}(\cdot) \) can be defined through semi-positive definite operators \( M_j \)'s as

\[
\mathcal{E}(\sigma) = \sum_j (M_j \otimes N_j) \sigma (M_j^\dagger \otimes N_j^\dagger)
\]

(Equation 98)

where \( M_j \) and \( N_j \) are Kraus operators defined respectively by

\[
M_j = \sum_s \sqrt{\epsilon_{js}} |s\rangle \langle |s\rangle, N_j = \sum_t \sqrt{\rho_{jt}} |t\rangle \langle |t\rangle
\]

which satisfy

\[
\sum_j M_j^\dagger M_j = \sum_j N_j^\dagger N_j = I,
\]

and \( \{\epsilon_{js}, \rho_{jt}\} \) are unknown probability distributions. Under the blind channel \( \mathcal{E}(\cdot) \), the density matrix \( \rho_{AB} \) in Equation (95) can be rewritten into the following form

\[
\rho_{AB} = \sum_{j=0}^{d-1} \rho_{j|i}\langle jj\rangle + \sum_{j\neq k} \rho_{jk|kk}\langle kk\rangle,
\]

(Equation 99)

where \( \rho_{j|i} \) ’s are the density matrix elements satisfying \( \{\rho_{j|i}\} \) is a probability distribution and \( \rho_{jk|kk} = \rho_{kk|jj}^* \).

Our goal in what follows is to verify the entanglement set

\[
S_2 : = \{\mathcal{E}(\Phi)(\Phi), \forall |\Phi\rangle, \mathcal{E}(\cdot)\}
\]

(Equation 100)

which is spanned by the basis \( \{|jj\rangle |kk\rangle, |jj\rangle |jj\rangle\} \).

It is easy to prove that \( S_2 \) is not convex because the separable state \( \rho_{AB} = \sum_{i=0}^{d-1} \rho_{ij|ij}\langle ij\rangle \) has the decomposition in Equation (99). This rules out the linear entanglement witnesses (Horodecki et al., 2009). Similar to Theorem 1, we have the following Theorem.

**Theorem 4.** The entanglement set \( S_2 \) is verifiable.

**Proof.** Similar to the generalized GHZ-like paradox (5) in the main text, we present a paradox for high-dimensional quantum entanglement by using \( \Sigma_1 \) in Equation (91) and \( \Sigma_2 \) in Equation (92) as

\[
\langle \Sigma_1 \otimes \Sigma_3 \rangle_\epsilon = 1, (k = 1, \ldots, d - 2),
\]

\[
\langle \Sigma_1 \otimes \Sigma_2 \rangle_\epsilon = 0,
\]

\[
\langle \Sigma_1 \otimes \Sigma_3 \rangle_\epsilon = 0,
\]

\[
\langle \Sigma_1 \otimes \Sigma_2 \rangle_\epsilon = 0.
\]

(Equation 101)

This can be proved by a forward evaluation. The proof of the nonlocality with definite real values of both parties is similar to its for Theorem 1.

The proof for witnessing the entanglement set \( S_2 \) depends on the following nonlinear inequality

\[
2 \sum_{0 \leq j \neq k \leq d-1} \sqrt{\rho_{kj|kl}} \rho_{kj|kl} + \sum_{j=0}^{d-1} \rho_{jj|jj} - 1 \leq 0
\]

(Equation 102)
for any bipartite separable state. The proof will be presented in the later. From the inequality (102), \( \rho \) in Equation (99) is entangled for \( p_{j+1,k} \neq 0 \) for any two integers \( j \neq k \). In other words, it is separable state if and only if \( p_{j+1,k} = 0 \) for any integers \( j \) and \( k \) with \( j \neq k \).

Next we come to prove that any separable state would violate one statement in the paradox (101). For any separable state \( \rho_s \), it violates the first statement in the paradox (101) if it does not has the decomposition in Equation (99). Otherwise, \( \rho_s \) has the decomposition in Equation (99). From Equation (101), we have

\[
\langle \Sigma_j \otimes \Sigma^{d-j}_k \rangle = \sum_{j=0}^{d-1} p_{j,k} = 1,
\]
\[
\langle \Sigma_j \otimes \Sigma_j \rangle_p = 0,
\]
\[
\langle \Sigma_1 \otimes \Sigma_j \rangle_p = 0,
\]
\[
\langle \Sigma_1 \otimes \Sigma_1 \rangle_p = \sum_{j=0}^{d-1} p_{j,j+1} + \sum_{j=0}^{d-1} p_{j+1,j+1}.
\]

(Equation 103)

It means that \( p_{j+1,k} = 0 \) for any integers \( j \) and \( k \) with \( j \neq k \). This violates the fourth statement in the paradox (101). Hence, this has completed the proof if we can prove the inequality (102).

**Proof of the inequality (102).** Similar to Lemma 1, consider an arbitrary separable two-qudit pure state on Hilbert space \( \mathcal{H}_A \otimes \mathcal{H}_B \) as

\[
|\Phi\rangle = |\varphi_1\rangle |\varphi_2\rangle
\]

(Equation 104)

With \( |\varphi_i\rangle = \sum_{j=0}^{d-1} a_j |\varphi_j\rangle \) and \( \sum_{j=0}^{d-1} a_j^2 = 1, i = 1, 2 \). It follows that

\[
|p_{j+1,j+1}|^2 = |a_1 a_2 a_{j+1} a_{j+1}|^2 = |j+1,j+1| a_{j+1} a_{j+1}^{-1}.
\]

(Equation 105)

This implies that

\[
2|p_{j+1,j+1}| \leq p_{j+1,j+1} + p_{j+1,j+1}^{-1},
\]

due to the Cauchy-Schwarz inequality of \( 2\sqrt{xy} \leq x^2 + y^2 \).

Consider an arbitrary mixed separable state on Hilbert space \( \mathcal{H}_A \otimes \mathcal{H}_B \) as

\[
\rho = \sum_i p_i |\Phi_i\rangle \langle \Phi_i| = \sum_{j,k} p_{j,k} |j,k\rangle \langle j,k| = \sum_{j,k} p_{j,k} \sum_{j,k} p_{j,k} |j,k\rangle \langle j,k|
\]

(Equation 107)

with separable pure states \( |\Phi_i\rangle \), where \( \{ p_i \} \) is a probability distribution, and \( \rho_{j,k} = |\Phi_i\rangle \langle \Phi_i| \). Similar to the inequalities (18)-(20), from Equation (106) we get

\[
2|p_{j+1,j+1}| = 2 \sum_i p_{i,j+1,j+1} \leq p_{j+1,j+1} + p_{j+1,j+1}^{-1}.
\]

(Equation 108)

Similarly, we can prove that

\[
2|p_{j,k}| \leq p_{j,k} + p_{j,k}^{-1}
\]

(Equation 109)

So, from the inequality (109) we have

\[
2 \sum_{0 \leq j \leq d-1} \sqrt{p_{j,k}} p_{j,k} = 2 \sum_{0 \leq j \leq d-1} |p_{j,k}| \leq \sum_{0 \leq j \leq d-1} (p_{j,k} + p_{j,k}) = 1 - \sum_{j=0}^{d-1} p_{j,j}
\]

(Equation 110)

This has completed the proof.

**Multipartite entanglement**

Consider an \( n \)-qudit system \( |\Psi\rangle_{A_1 \cdots A_n} \) on Hilbert space \( \mathcal{H}_A \otimes \mathcal{H}_A \), where \( \mathcal{H}_A \)’s are all \( d \)-dimensional spaces. A generalized n-partite entangled pure state shared by \( A_1, \cdots, A_n \) is given by
\[ |\Psi\rangle_{A_1\cdots A_n} = \sum_{j=0}^{d-1} \alpha_j |j\rangle \cdots |j\rangle, \quad \text{(Equation 111)} \]

where \(\alpha_j\)'s are real parameters satisfying \(\sum_{j=0}^{d-1} \alpha_j^2 = 1\). Suppose that all the parties only know the shared state has the following form:

\[ \rho_{A_1\cdots A_n} = \mathcal{E}(|\Psi\rangle\langle\Psi|), \quad \text{(Equation 112)} \]

where \(\mathcal{E}(\cdot)\) is a blind quantum channel defined similar to Equation (96) by using unknown local phase transformations for each party. Under the blind channel \(\mathcal{E}(\cdot)\), the density matrix \(\rho_{A_1\cdots A_n}\) in Equation (111) can be rewritten into the following form

\[ \rho_{A_1\cdots A_n} = \sum_{j=0}^{d-1} \rho_{j, j, \cdots, j} |j\rangle \langle j|_n + \sum_{j=0}^{d-1} \rho_{j, \cdots, j, \cdots, j} |j\rangle \langle j|_n |j\rangle \langle j|_n, \quad \text{(Equation 113)} \]

where \(|j\rangle\_n\) denotes \(n\) number of \(j\), i.e., \(|j\rangle\_n = j\cdots j\_n\), \(\rho_{j, \cdots, j, \cdots, j}\) are the density matrix elements satisfying \(\sum_{j=0}^{d-1} \rho_{j, j, \cdots, j} = 1\) (\(|j\rangle\_n\) is a probability distribution) and \(\rho_{j, \cdots, j, \cdots, j} = \rho_{k, \cdots, k, \cdots, k}\_n\). Our goal in what follows is to verify the entanglement set

\[ S_n : = \{\mathcal{E}(|\Psi\rangle\langle\Psi|), \forall |\Psi\rangle, \mathcal{E}(\cdot)\} \]

which is spanned by the basis \(|j\rangle\_n |j\rangle\_n |j\rangle\_n \rangle\_{\forall j, k}\).

Similar to Theorem 2, we have the following Theorem 5.

**Theorem 5**

The entanglement set \(S_n\) is verifiable.

The proof of Theorem 5 is based on two facts. One is from the generalized GHZ-like paradox given by

\[ \left( \left( \Sigma_3^{(i)} \right)^k \otimes \left( \Sigma_3^{(n)} \right) \right)^{d-k} = 1, \quad (k = 1, \cdots, d - 1), \]
\[ \left( \left( \Sigma_3^{(j)} \right)^k \otimes \left( \Sigma_3^{(j+1)} \right) \right)^{d-k} = 1, \]
\[ \left( \Sigma_3^{(i)} \otimes \Sigma_3^{(n)} \right) = 0, \]
\[ \left( \Sigma_3^{(j)} \otimes \Sigma_3^{(j+1)} \right) = 0, \]
\[ \left( \Sigma_3^{(j)} \otimes \Sigma_3^{(n)} \right) = 0, \]
\[ \left( \Sigma_3^{(j)} \otimes \Sigma_3^{(j+1)} \right) = 0, \quad (j = 1, \cdots, n - 1), \]
\[ \left( \Sigma_3^{(1)} \otimes \cdots \otimes \Sigma_3^{(n)} \right) \neq 0, \quad \text{(Equation 115)} \]

for all the entangled states in \(S_n\), while it will be violated by any biseparable state. Here, \(\Sigma_3^{(i)}\) denotes the local observable \(\Sigma_i\) performed by \(A_i\). The paradox (115) can be proved similar to its for the paradox (13). The other is from the nonlinear inequality given by

\[ 2 \sum_{0 \leq i + j + k \leq d - 1} \sqrt{\rho_{j, j, \cdots, j, i, i, \cdots, i, k, k, \cdots, k}} + \sum_{j=0}^{d-1} \rho_{j, j, \cdots, j} \leq 1, \quad \text{(Equation 116)} \]

which holds for any biseparable state. This can be proved similar to Lemma 2 and the inequality (102), where \(j = j_1 \cdots j_n\) and \(k = k_1 \cdots k_n, j_1, \cdots, j_n, k_1, \cdots, k_n \in \{0, \cdots, d - 1\}\).