npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Optimal verification of the Bell state and Greenberger–Horne–Zeilinger states in untrusted quantum networks

Yun-Guang Han[1,2,3], Zihao Li[1,2,3], Yukun Wang[4] and Huangjun Zhu[1,2,3]✉

Bipartite and multipartite entangled states are basic ingredients for constructing quantum networks and their accurate verification is crucial to the functioning of the networks, especially for untrusted networks. Here we propose a simple approach for verifying the Bell state in an untrusted network in which one party is not honest. Only local projective measurements are required for the honest party. It turns out each verification protocol is tied to a probability distribution on the Bloch sphere and its performance has an intuitive geometric meaning. This geometric picture enables us to construct the optimal and simplest verification protocols, which are also very useful to detecting entanglement in the untrusted network. Moreover, we show that our verification protocols can achieve almost the same sample efficiencies as protocols tailored to standard quantum state verification. Furthermore, we establish an intimate connection between the verification of Greenberger–Horne–Zeilinger states and the verification of the Bell state. By virtue of this connection we construct the optimal protocol for verifying Greenberger–Horne–Zeilinger states and for detecting genuine multipartite entanglement.

npj Quantum Information (2021)7:164 ; https://doi.org/10.1038/s41534-021-00499-8

INTRODUCTION

Entanglement is the characteristic of quantum mechanics and key resource in quantum information processing[1–3]. As typical examples of bipartite and multipartite entangled states, the Bell state and Greenberger–Horne–Zeilinger (GHZ) states[4,5] play crucial roles in numerous quantum information processing tasks and in foundational studies, such as quantum teleportation[6–8], quantum key distribution[9,10], quantum random number generation[11], and nonlocality tests[12,13]. Furthermore, as a special example of graph states[14], GHZ states are useful to constructing quantum networks[15,16] designed for distributed quantum information processing, such as quantum secret sharing[17,18], quantum conference key agreement[19], and distribution[20].

To guarantee the proper functioning of a quantum network, it is essential to verify the entangled state deployed in the network accurately and efficiently, especially for untrusted networks[21–29]. This scenario has wide applications in quantum information processing, such as one-sided device-independent (DI) quantum key distribution[30], anonymous communication[31,32], and verifiable quantum secure modulo summation[33]. Meanwhile, this problem is tied to the foundational studies on quantum steering in the asymmetric scenario[3,34–36] and the uncertainty principle in the presence of quantum memory[37,38].

Unfortunately, not much is known about quantum verification in untrusted networks despite its significance. This is because not all parties in the networks are honest, and the verification problem gets much more complicated in the presence of dishonest parties. In particular, traditional tomographic approaches are not applicable in the network setting even if their low efficiency is tolerable. Also, most alternative approaches, including direct fidelity estimation[39] and quantum state verification (QSV)[40–45], are not applicable, although QSV can address the adversarial scenario in which the source is not trustworthy[43–45]. DI QSV[46] based on self-testing[22,47–52] can be applied in the network setting in principle, but is too resource consuming and too demanding with current technologies. For the Bell state and GHZ states, optimal verification protocols are known when all parties are honest[42,53–58]. In the network setting, however, only suboptimal protocols are known in the literature[23–26,29].

In this paper, we propose a simple approach for verifying the Bell state over an untrusted network in the semi-device-independent (SDI) scenario in which one party is not honest. Only local projective measurements are required for the honest party. In addition, we establish a simple connection between verification protocols of the Bell state and probability distributions on the Bloch sphere and reveal an intuitive geometric interpretation of the performance of each verification protocol. By virtue of this geometric picture, we construct the optimal and simplest protocols for verifying the Bell state, which can also be applied to detecting entanglement in the untrusted network. Moreover, we determine the sample efficiencies of our SDI verification protocols in addition to the guessing probabilities.

Furthermore, we establish an intimate connection between the verification of GHZ states and the verification of the Bell state. Thanks to this connection, efficient protocols for verifying GHZ states can easily be constructed from the counterparts for the Bell state. Notably, this connection enables us to construct the optimal protocol for verifying GHZ states and for detecting genuine multipartite entanglement (GME). To put our work in perspective, we also provide a detailed comparison between SDI QSV considered in this work and standard QSV as well as DI QSV based on self-testing. For the Bell state and GHZ states, SDI verification can achieve almost the same sample efficiency as standard QSV; by contrast, the sample efficiency in the DI scenario

[1]State Key Laboratory of Surface Physics and Department of Physics, Fudan University, Shanghai 200433, China. [2]Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China. [3]Center for Field Theory and Particle Physics, Fudan University, Shanghai 200433, China. [4]Department of Computer Science and Technology, China University of Petroleum, Beijing 102249, China. ✉email: zhuhuangjun@fudan.edu.cn

is in general quadratically worse in the infidelity unless there exists a suitable Bell inequality for which the quantum bound coincides with the algebraic bound.

RESULTS

Verification of the Bell state

Suppose two distant parties, Alice and Bob, want to create the Bell state $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ as follows: Bob first prepares $|\Phi\rangle$ in his lab and then sends one particle of the entangled pair to Alice using a quantum channel. To verify this state Alice can perform a random projective measurement from a set of accessible measurements and then ask Bob to guess the measurement outcome given the measurement chosen. Each projective measurement is specified by a unit vector $\boldsymbol{r}$ on the Bloch sphere, which specifies the two outcomes $P_\pm = (\mathbb{I} \pm \boldsymbol{r} \cdot \boldsymbol{\sigma})/2$, where $\boldsymbol{\sigma}$ is the vector composed of the three Pauli matrices. If Bob is honest and prepares the target state $|\Phi\rangle$, then his reduced states corresponding to the two outcomes P_+ and P_- have mutually orthogonal supports, so he can guess the measurement outcome with certainty by performing a suitable projective measurement.

If Bob is not honest and tries to prepare a different state ρ instead of $|\Phi\rangle$, then his guessing probability—the probability of successful guess—would be limited. In this case, Alice cannot distinguish two states that can be turned into each other by local operations of Bob; nevertheless, she can verify whether the state prepared is indeed $|\Phi\rangle$ up to these local operations. Let $\rho_\pm = \mathrm{tr}_A(\rho P_\pm)$ be the unnormalized reduced states of Bob. To guess the measurement outcome of Alice, Bob can perform a two-outcome POVM $\{E_+, E_-\}$ to distinguish ρ_+ and ρ_-. By the Helstrom theorem[59], the maximum guessing probability $\gamma(\rho, \boldsymbol{r})$ over all POVMs (or projective measurements) is given by the formula $\gamma(\rho, \boldsymbol{r}) = (1 + ||\rho_+ - \rho_-||_1)/2$.

Recall that a general two-qubit state has the form

$$\rho = \frac{1}{4}\left(\mathbb{I} + \boldsymbol{a} \cdot \boldsymbol{\sigma} \otimes \mathbb{I} + \mathbb{I} \otimes \boldsymbol{b} \cdot \boldsymbol{\sigma} + \sum_{j,k} T_{jk} \sigma_j \otimes \sigma_k\right), \tag{1}$$

where σ_j, σ_k are Pauli matrices (also denoted by X, Y, Z), $\boldsymbol{a}$ and $\boldsymbol{b}$ are the Bloch vectors of the two reduced states, and T is the correlation matrix. If ρ is pure, then we can deduce (cf. Supplementary Note 1),

$$\gamma(\rho, \boldsymbol{r}) = \frac{1}{2}(1 + ||T^{\mathrm{T}} \boldsymbol{r}||) = \frac{1}{2}\left(1 + ||\sqrt{TT^{\mathrm{T}}}\, \boldsymbol{r}||\right). \tag{2}$$

To understand the geometric meaning of $\gamma(\rho, \boldsymbol{r})$, note that the set of vectors $\{\sqrt{TT^{\mathrm{T}}}\, \boldsymbol{r} : |\boldsymbol{r}| = 1\}$ forms a rotational ellipsoid, which is called the *correlation ellipsoid* and denoted by $\mathscr{E}_\rho$ (cf. the steering ellipsoid[60,61]), as illustrated in Fig. 1. The semi-major axis $\boldsymbol{v}$ and semi-minor axis of $\mathscr{E}_\rho$ have length 1 and C, respectively, where C is the concurrence of ρ[1,62]. In addition, the radius $||\sqrt{TT^{\mathrm{T}}}\, \boldsymbol{r}||$ is determined by C and the angle between $\boldsymbol{r}$ and the semi-major axis as follows,

$$||\sqrt{TT^{\mathrm{T}}}\, \boldsymbol{r}|| = ||T^{\mathrm{T}} \boldsymbol{r}|| = \sqrt{C^2 + (1 - C^2)(\boldsymbol{r} \cdot \boldsymbol{v})^2}. \tag{3}$$

A verification strategy of Alice is determined by a probability distribution μ on the Bloch sphere, which specifies the probability of performing each projective measurement. Given the strategy μ and the state ρ, the maximum average guessing probability of Bob reads

$$\gamma(\rho, \mu) := \int \mathrm{d}\mu(\boldsymbol{r}) \gamma(\rho, \boldsymbol{r}) = \frac{1}{2} + \frac{1}{2} \int \mathrm{d}\mu(\boldsymbol{r}) ||T^{\mathrm{T}} \boldsymbol{r}||, \tag{4}$$

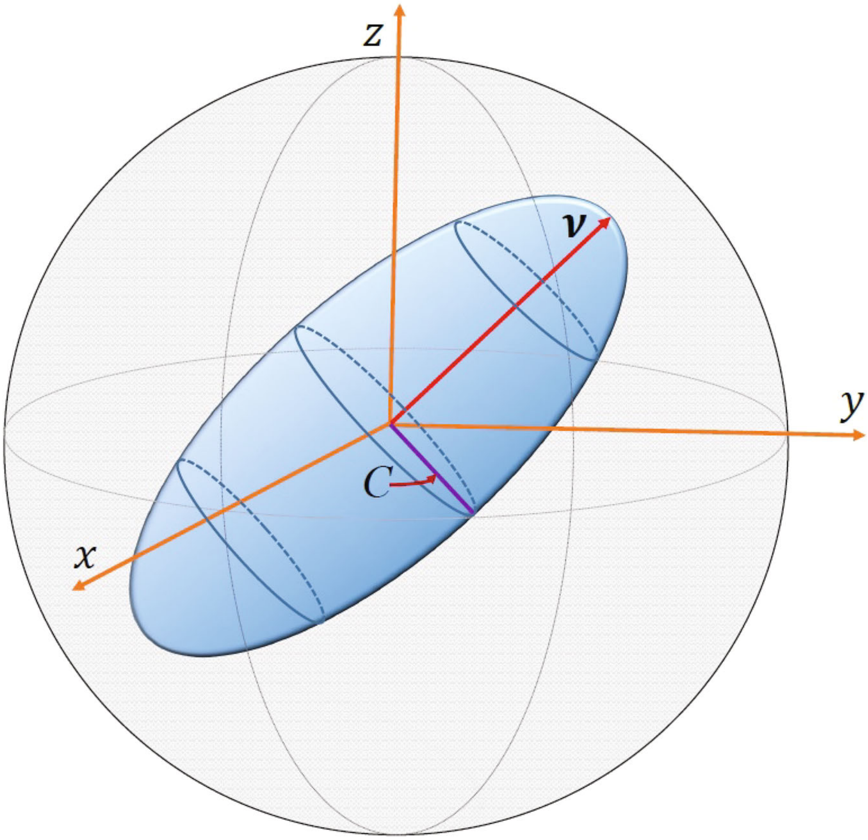

Fig. 1 Geometric illustration of the *XYZ* protocol in the Bloch sphere. For a given concurrence C, the guessing probability is maximized when the semi-major axis $\boldsymbol{v}$ of the correlation ellipsoid parallels one of the eight intelligent directions.

where the bias is a weighted average of radii of the correlation ellipsoid. Denote by $\gamma_2(C,\mu)$ the maximum guessing probability over all pure states with concurrence at most C. Note that maximizing $\gamma(\rho,\mu)$ for a given concurrence amounts to choosing a proper orientation of the correlation ellipsoid so as to maximize the weighted average of radii, as illustrated in Fig. 1. This intuition leads to the following theorem as proved in Supplementary Note 1.

Theorem 1. *Suppose* $0 \le C \le 1$; *then*

$$\gamma_2(C,\mu) = \frac{1}{2}[1 + g(C,\mu)], \tag{5}$$

$$g(C,\mu) := \max_{\boldsymbol{v}} \int \mathrm{d}\mu(\boldsymbol{r})\sqrt{C^2 + (1-C^2)(\boldsymbol{r}\cdot\boldsymbol{v})^2}, \tag{6}$$

where the maximization in Eq. (6) is over all unit vectors.

Any unit vector $\boldsymbol{v}$ that maximizes the integration in Eq. (6) is called an *intelligent direction*. For a given concurrence, the guessing probability is maximized when the major axis of the correlation ellipsoid parallels an intelligent direction. When $C = 1$, the correlation ellipsoid is a sphere, in which case Theorem 1 yields $g(C,\mu) = 1$ and $\gamma_2(C,\mu) = 1$. When $C = 0$, the correlation ellipsoid reduces to a line segment, in which case we can deduce

$$g^*(\mu) := g(0,\mu) = \max_{\boldsymbol{v}} \int \mathrm{d}\mu(\boldsymbol{r})|\boldsymbol{r}\cdot\boldsymbol{v}|, \tag{7}$$

$$\gamma_2^*(\mu) := \gamma_2(0,\mu) = \frac{1}{2} + \frac{1}{2}\max_{\boldsymbol{v}} \int \mathrm{d}\mu(\boldsymbol{r})|\boldsymbol{r}\cdot\boldsymbol{v}|. \tag{8}$$

Notably, entanglement can be certified in the shared system when the guessing probability surpasses the threshold $\gamma_2^*(\mu)$. The relation between the guessing probability and concurrence for various verification protocols is illustrated in Fig. 2.

Alternative strategies of the adversary

So far we have assumed that the state ρ prepared by Bob is a two-qubit pure state and $\rho_A := \mathrm{tr}_B(\rho)$ is supported in the local support of the target Bell state, that is, the subspace spanned by $|0\rangle$ and $|1\rangle$. Can Bob gain any advantage if ρ_A is not supported in this subspace? The answer turns out to be negative. Now Alice can first perform the projective measurement $\{P_A, \mathbb{I} - P_A\}$ with $P_A = |0\rangle\langle 0| + |1\rangle\langle 1|$ and then apply a verification protocol as before if she obtains the first outcome and reject otherwise. The maximum guessing probability $\gamma(C,\mu)$ of Bob for any pure state with $C(\rho) \le C$ is the same as before as shown in the following lemma and proved in Supplementary Note 3.

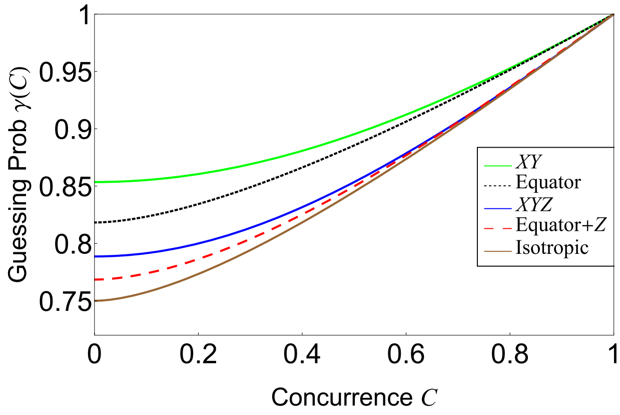

Fig. 2 The guessing probability $\gamma(C) = \gamma_2(C)$ as a function of the concurrence C for various verification protocols of the Bell state. Here the XY protocol and isotropic protocol are introduced in the main text, while other protocols are proposed in the Supplementary Material.

Lemma 1. $\gamma(C,\mu) = \gamma_2(C,\mu)$ *for* $0 \le C \le 1$.

Note that $\gamma(C,\mu) = 1$ when $C \ge 1$, in which case Bob can prepare the target Bell state. So we can focus on the case $0 \le C \le 1$. Define $\gamma^*(\mu) := \gamma(0,\mu)$, then $\gamma^*(\mu) = \gamma_2^*(\mu)$ thanks to Lemma 1, so the threshold for entanglement detection remains the same as before; cf. Eq. (8). In conjunction with the convexity of $\gamma_2(C,\mu)$ in C (cf. Lemma S1 in Supplementary Note 2), Lemma 1 implies that

$$\gamma(C,\mu) = \gamma_2(C,\mu) \le \gamma^*(\mu)(1-C) + C, \quad 0 \le C \le 1, \tag{9}$$

which offers the best linear upper bound for $\gamma(C,\mu)$. When the distribution μ is clear from the context, $\gamma^*(\mu)$ is abbreviated as γ^* for simplicity.

Above results can be extended to mixed states, although our main interest are pure states. Let $\hat{\gamma}(C,\mu)$ be the maximum guessing probability of Bob over all states with concurrence at most C. Define $\hat{\gamma}_2(C,\mu)$ in a similar way, but assuming that ρ_A is supported in the support of P_A. By the following theorem proved in Supplementary Note 4, $\hat{\gamma}(C,\mu)$ and $\hat{\gamma}_2(C,\mu)$ are weighted averages of $\gamma^*(\mu)$ and $\gamma(1,\mu) = 1$.

Theorem 2. *Suppose* $0 \le C \le 1$; *then*

$$\begin{aligned}\hat{\gamma}(C,\mu) &= \hat{\gamma}_2(C,\mu) = (1-C)\gamma^*(\mu) + C \\ &= \tfrac{1+C}{2} + \tfrac{1-C}{2}\max_{\boldsymbol{v}} \textstyle\int \mathrm{d}\mu(\boldsymbol{r})|\boldsymbol{r}\cdot\boldsymbol{v}|.\end{aligned} \tag{10}$$

Fidelity as the figure of merit

Next, we consider the fidelity as the figure of merit, which is more natural for QSV. Here we assume that Bob controls the whole system except that of Alice, so we can assume that the state ρ prepared by Bob is pure. Define the reduced fidelity

$$F_B(\rho) := \max_{U_B} \langle\Phi|(\mathbb{I}_A \otimes U_B)\rho(\mathbb{I}_A \otimes U_B)^\dagger|\Phi\rangle, \tag{11}$$

where the maximization is taken over all local unitary transformations on $\mathcal{H}_B$. Denote by $\gamma^{\mathrm{F}}(F,\mu)$ the maximum guessing probability over all pure states with $F_B(\rho) \le F$. Define $\gamma_2^{\mathrm{F}}(F,\mu)$ in a similar way, but assuming that ρ_A is supported in the support of P_A. It is known that $F_B(\rho) = [1 + C(\rho)]/2 \ge 1/2$ for any two-qubit pure state ρ satisfying $P_A\rho_A = \rho_A$[63]. So $\gamma_2^{\mathrm{F}}(F,\mu)$ is defined only for $1/2 \le F \le 1$, although $\gamma^{\mathrm{F}}(F,\mu)$ is defined for $0 \le F \le 1$.

The following theorem proved in Supplementary Note 5 clarifies the relations between $\gamma^{\mathrm{F}}(F,\mu)$, $\gamma_2^{\mathrm{F}}(F,\mu)$, and $\gamma_2(C,\mu)$. The guessing probabilities $\gamma^{\mathrm{F}}(F,\mu)$ for various verification protocols are illustrated in Fig. 3.

Theorem 3. *Suppose* $1/2 \le F \le 1$; *then*

$$\gamma_2^{\mathrm{F}}(F,\mu) = \gamma_2(2F-1,\mu) \le 1 - 2(1-\gamma^*)(1-F). \tag{12}$$

Suppose $0 \le F \le 1$; *then*

$$\gamma^{\mathrm{F}}(F,\mu) = \begin{cases} 2\gamma^* F & 0 \le F < 1/2, \\ \gamma_2(2F-1,\mu) & 1/2 \le F \le 1, \end{cases} \tag{13}$$

$$\gamma^{\mathrm{F}}(F,\mu) \le 1 - 2(1-\gamma^*)(1-F). \tag{14}$$

Equation (14) offers the best linear upper bound for $\gamma^{\mathrm{F}}(F,\mu)$ when $1/2 \le F \le 1$ and demonstrates the robustness of the verification protocol. Theorems 1 to 3 corroborate the significance of the threshold γ^* in verifying the Bell state and entanglement in the SDI scenario. Moreover, the threshold γ^* determines the sample efficiency, as we shall see shortly. Therefore, γ^* can be regarded as the most important figure of merit for characterizing the performance of a verification protocol.

Simplest and optimal verification protocols

Here we propose several concrete verification protocols, including the simplest and optimal protocols. The main results are summarized in Table 1 and illustrated in Fig. 2; more details can be found in Supplementary Note 9.

In the simplest verification protocol, Alice can perform two projective measurements $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ with probabilities p_1 and p_2, respectively. Here the maximum guessing probability $\gamma(C,\mu)$ only depends on the angle between $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ in addition to the probabilities p_1 and p_2. Moreover, $\gamma(C,\mu)$ is minimized when $\boldsymbol{r}_1\cdot\boldsymbol{r}_2=0$ and $p_1=p_2=1/2$, in which case we have

$$g(C,\mu)=\sqrt{\frac{1+C^2}{2}},\quad \gamma(C,\mu)=\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1+C^2}{2}}, \tag{15}$$

and the guessing probability threshold is $\gamma^*=(2+\sqrt{2})/4$. When $\boldsymbol{r}_1=(1,0,0)^{\mathrm{T}}$ and $\boldsymbol{r}_2=(0,1,0)^{\mathrm{T}}$ for example, we get the *XY* protocol. Previously, ref. [23] proposed an equivalent protocol, but neither derived the exact formula for the guessing probability nor proved the optimality of the *XY* protocol among all two-setting protocols.

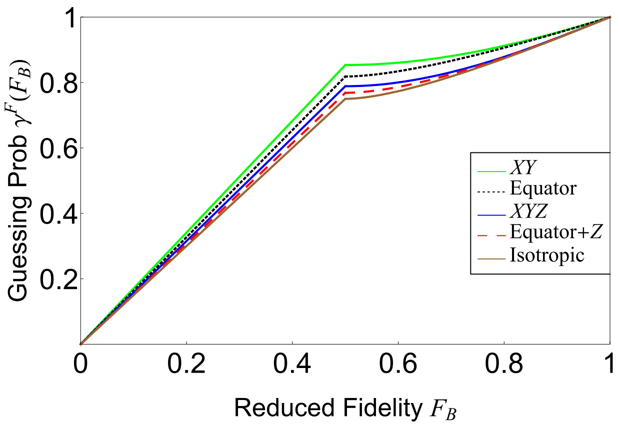

Fig. 3 Relation between the guessing probability $\gamma^F(F_B)$ and the reduced fidelity F_B for various verification protocols of the Bell state. Here the *XY* protocol and isotropic protocol are introduced in the main text, while other protocols are proposed in the Supplementary Material.

To determine the optimal protocol, we need to minimize $g(C,\mu)$ over μ. By Theorem 1, $g(C,\mu)$ is convex in μ, so $g(C,\mu)$ is minimized when μ is the uniform distribution on the Bloch sphere, which yields the isotropic protocol with

$$g(C,\mu)=\frac{1}{2}+\frac{C^2\operatorname{arcsinh}\left(\frac{\sqrt{1-C^2}}{C}\right)}{2\sqrt{1-C^2}}, \tag{16}$$

$$\gamma(C,\mu)=\frac{3}{4}+\frac{C^2\operatorname{arcsinh}\left(\frac{\sqrt{1-C^2}}{C}\right)}{4\sqrt{1-C^2}}, \tag{17}$$

and the guessing probability threshold is $\gamma^*=3/4$.

Protocols based on the Pauli Z measurement and measurements on the *xy*-plane are of special interest to the verification of GHZ states as we shall see shortly. Prominent examples include the *XYZ* protocol (cf. Fig. 1), equator protocol, equator + Z protocol, polygon protocol, and polygon + Z protocol (see Supplementary Note 9).

Sample efficiency

To construct a practical verification protocol, it is crucial to clarify the sample efficiency. Although this problem has been resolved in standard QSV[42–44], little is known about the sample efficiency in the DI and SDI scenarios[46]. Here we clarify the sample efficiency of our verification protocols in the SDI scenario. Consider a quantum device that is supposed to produce the target state $|\Phi\rangle\in\mathcal{H}$, but actually produces the states $\rho_1,\rho_2,\ldots,\rho_N$ in N runs. Our task is to verify whether these states are sufficiently close to the target state on average. Here the reduced fidelity is a natural choice for quantifying the closeness since Alice is ignorant to the local unitary transformations acting on Bob's system. To guarantee that the average reduced fidelity of the states $\rho_1,\rho_2,\ldots,\rho_N$ is larger than $1-\epsilon$ with significance level δ (confidence level $1-\delta$), the number of tests required is determined in Supplementary Note 6, with the result

$$N=\left\lceil\frac{\ln\delta}{\ln\left[1-2(1-\gamma^*)\epsilon\right]}\right\rceil\approx\frac{\ln\delta^{-1}}{2(1-\gamma^*)\epsilon}. \tag{18}$$

Note that the sample efficiency is determined by the threshold $\gamma^*=\gamma_2^*$ defined in Eq. (8).

The minimum threshold $\gamma^*=3/4$ is attained for the isotropic protocol, in which case $N\approx(2\ln\delta^{-1})/\epsilon$, which is comparable to the number $(3\ln\delta^{-1})/(2\epsilon)$ required in standard QSV[42,53]. So the Bell state can be verified in the SDI scenario almost as efficiently as in the standard QSV. Our protocol can achieve the optimal sample

Table 1. Concrete protocols for verifying the Bell state in an untrusted quantum network.

Protocol	Threshold γ^*	$\gamma(C)$ (pure state)	$\hat{\gamma}(C)$ (mixed state)	$\boldsymbol{v}(C=0)$
XY	$\frac{1}{2}+\frac{1}{2\sqrt{2}}\approx 0.854$	$\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1+C^2}{2}}$	$\frac{1}{4}[2+\sqrt{2}+(2-\sqrt{2})C]$	$\frac{1}{\sqrt{2}}(1,1,0)^{\mathrm{T}}$
XYZ	$\frac{1}{2}+\frac{1}{2\sqrt{3}}\approx 0.789$	$\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1+2C^2}{3}}$	$\frac{1}{6}[3+\sqrt{3}+(3-\sqrt{3})C]$	$\frac{1}{\sqrt{3}}(1,1,1)^{\mathrm{T}}$
Isotropic	$\frac{3}{4}=0.75$	$\frac{3}{4}+\frac{C^2\operatorname{arcsinh}\left(\frac{\sqrt{1-C^2}}{C}\right)}{4\sqrt{1-C^2}}$	$\frac{3+C}{4}$	any direction
Equator	$\frac{1}{2}+\frac{1}{\pi}\approx 0.818$	$\frac{1}{2}+\frac{1}{\pi}K(\sqrt{1-C^2})$	$\frac{1}{2\pi}[\pi+2+(\pi-2)C]$	any direction in the *xy*-plane
Polygon(3)	$\frac{5}{6}\approx 0.833$	$\frac{4+\sqrt{1+3C^2}}{6}$	$\frac{5+C}{6}$	any vertex direction
Equator $+Z$	$\frac{1}{2}+\frac{1}{\sqrt{4+\pi^2}}\approx 0.769$	–	$\frac{1+C}{2}+\frac{1-C}{\sqrt{4+\pi^2}}$	$\frac{1}{\sqrt{4+\pi^2}}(\pi,0,2)^{\mathrm{T}}$
Polygon(3)+Z	$\frac{1}{2}+\frac{1}{\sqrt{13}}\approx 0.777$	–	$\frac{1}{2}+\frac{1}{\sqrt{13}}+\left(\frac{1}{2}-\frac{1}{\sqrt{13}}\right)C$	$\frac{1}{\sqrt{13}}(3,0,2)^{\mathrm{T}}$

Here $\gamma(C)$ ($\hat{\gamma}(C)$) is the maximum guessing probability for pure (mixed) states with concurrence at most C, and $\boldsymbol{v}(C=0)$ is an intelligent direction for $C=0$. Entanglement can be certified when the guessing probability surpasses the threshold $\gamma^*=\gamma(0)=\hat{\gamma}(0)$. The *XY* protocol and isotropic protocol are the simplest and optimal verification protocols, respectively. All protocols listed, except for the isotropic protocol, can be generalized to GHZ states.

complexity because it is tied to a steering inequality whose quantum bound coincides with the algebraic bound. In contrast, the sample complexity in the DI scenario is quadratically worse in the scaling with $1/\epsilon$, that is, $N \propto (\ln\delta^{-1})/\epsilon^2$ [46] (cf. Supplementary Note 7).

Verification of the GHZ state

Next, consider the GHZ state $|G^n\rangle = (|0\rangle^{\otimes n} + |1\rangle^{\otimes n})/\sqrt{2}$ of n-qubits with $n \geq 3$. To verify this state, the n parties can randomly perform certain tests based on local projective measurements. In each test, the verifier (one of the parties) asks each party to perform a local projective measurement as specified by a unit vector on the Bloch sphere and return the measurement outcome. If all parties are honest, then only the target state $|G^n\rangle$ can pass all tests with certainty, so the GHZ state can be verified. In the presence of dishonest parties, let $\mathscr{D}$ be the set of dishonest parties, who know which parties are honest or dishonest and who may collude with each other; let $\mathscr{H}$ be the set of honest parties (including the verifier), who do not know which other parties are honest or dishonest. The goal is to verify $|G^n\rangle$ up to local unitary transformations on the joint Hilbert space of $\mathscr{D}$[23,24]. Assuming $|\mathscr{D}|, |\mathscr{H}| \geq 1$, then $|G^n\rangle$ may be regarded as a Bell state shared between $\mathscr{H}$ and $\mathscr{D}$. So the verification of the GHZ state is closely tied to the verification of the Bell state. Actually, there is no essential difference when $|\mathscr{H}| = 1$.

However, a key distinction arises when $|\mathscr{H}| \geq 2$ because each member of $\mathscr{H}$ can only perform local projective measurements on his/her party. So the potential tests that the verifier can realize are restricted. Careful analysis in Supplementary Note 10 shows that only two types of tests for verifying the GHZ state $|G^n\rangle$ can be constructed from local projective measurements. In the first type, all parties perform Z measurements, and the test is passed if they obtain the same outcome. In this way the verifier can effectively realize the Z measurement on $V_{\mathscr{H}}$, where $V_{\mathscr{H}}$ is the two-dimensional subspace spanned by $\bigotimes_{j\in\mathscr{H}}|0\rangle_j$ and $\bigotimes_{j\in\mathscr{H}}|1\rangle_j$.

In the second type of tests, party j performs the $X(\phi_j)$ measurement with $\sum_j \phi_j = 0 \bmod 2\pi$, where $X(\phi_j) = \mathrm{e}^{-\mathrm{i}\phi_j}|0\rangle\langle 1| + \mathrm{e}^{\mathrm{i}\phi_j}|1\rangle\langle 0|$ corresponds to the Bloch vector $(\cos\phi_j, \sin\phi_j, 0)^{\mathrm{T}}$, and each ϕ_j is decided by the verifier. The test is passed if the number of outcomes -1 is even. Suppose $\phi_1, \phi_2, \ldots, \phi_n$ are chosen independently and uniformly at random from the interval $[0, 2\pi)$. Then $\phi_{\mathscr{H}} := \sum_{j\in\mathscr{H}} \phi_j \bmod 2\pi$ is uniformly distributed in $[0, 2\pi)$. Given $\phi \in [0, 2\pi)$, the average of $\bigotimes_{j\in\mathscr{H}} X(\phi_j)$ under the condition $\phi_{\mathscr{H}} = \phi$ reads

$$\left\langle \bigotimes_{j\in\mathscr{H}} X(\phi_j) \right\rangle_{\phi} = \mathrm{e}^{-\mathrm{i}\phi} \bigotimes_{j\in\mathscr{H}} (|0\rangle\langle 1|)_j + \mathrm{e}^{\mathrm{i}\phi} \bigotimes_{j\in\mathscr{H}} (|1\rangle\langle 0|)_j. \tag{19}$$

In this way, the verifier can effectively realize the $X(\phi)$ measurement on $V_{\mathscr{H}}$, where ϕ is completely random. A similar result holds when ϕ_j are chosen independently and uniformly at random from the discrete set $\{2k\pi/M\}_{k=0}^{M-1}$ with $M \geq 3$ being a positive integer.

By the above analysis, the verifier can effectively realize projective measurements along the z-axis or on the xy-plane when represented on the Bloch-sphere of $V_{\mathscr{H}}$, but not other projective measurements (assuming $|\mathscr{H}| \geq 2$). Each verification protocol of the GHZ state corresponds to a probability distribution μ on the Bloch sphere that is supported on the equator together with the north and south poles. Moreover, for all protocols in Table 1 except for the isotropic protocol (cf. Supplementary Notes 9 and 10), the guessing probabilities are the same as in the verification of the Bell state. To be specific, $\gamma(C, \mu)$ and $\gamma^{\mathrm{F}}(F, \mu)$ can be defined as before; Theorems 1, 3, and Lemma 1 still hold, except that now C refers to the bipartite concurrence between $\mathscr{H}$ and $\mathscr{D}$. Although variants of the XY protocol and equator protocol were proposed previously[23,24], such exact formulas for the guessing probabilities are not known in the literature. To optimize the performance, μ should be uniform on the equator, which leads to the equator $+\,Z$ protocol; the optimal probability p_Z for performing the Z measurement depends on C or F as before.

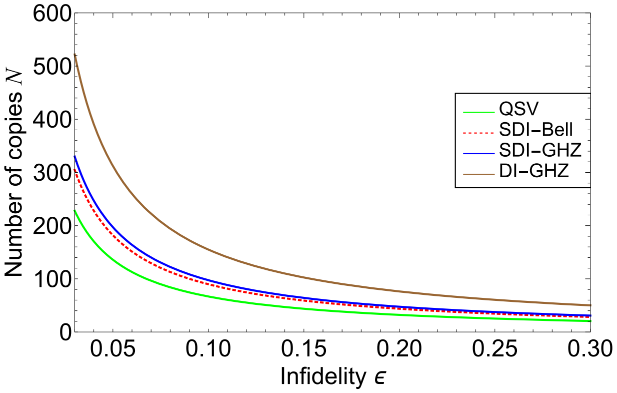

Fig. 4 Sample complexities for verifying the Bell state and GHZ states in three different scenarios. In standard QSV, the Bell state and GHZ states can be verified with the same sample complexity[42,57]. In the SDI scenario, the isotropic protocol is chosen for verifying the Bell state and the optimized equator $+\,Z$ protocol is chosen for verifying the GHZ states. In the DI scenario, the Mermin inequality is employed for verifying the three-qubit GHZ state[46,50]. Here the significance level is chosen to be $\delta = 0.01$.

A quantum state ρ is genuinely multipartite entangled (GME) if its fidelity with the GHZ state $\mathrm{tr}\,(\rho|G^n\rangle\langle G^n|)$ is larger than $1/2$[64]. The GME can be certified if the guessing probability surpasses the threshold $\gamma^{\mathrm{F}}(1/2) = \gamma^*$. This threshold is minimized at the special equator $+\,Z$ protocol with $p_Z = 4/(4+\pi^2) = 0.288$, in which case we have

$$\gamma^{\mathrm{F}}(1/2) = \gamma^* = \frac{1}{2} + \frac{1}{\sqrt{4+\pi^2}} \approx 0.769. \tag{20}$$

This threshold is only 2.5% higher than the optimal threshold 3/4 for certifying the entanglement of the Bell state based on the isotropic protocol.

The sample efficiency for verifying the GHZ state can be determined following a similar analysis applied to the Bell state. The formula in Eq. (18) still applies, except that the choice of verification protocols is restricted. Now the minimum of γ^* is achieved at a special equator $+\,Z$ protocol [cf. Eq. (20)]. So the GHZ state can be verified in the SDI scenario with almost the same efficiency as in the standard QSV[57], as illustrated in Fig. 4. In the DI scenario, by contrast, it is in general impossible to achieve such a high efficiency unless one can construct a Bell inequality for which the quantum bound coincides with the algebraic bound[46]. Notably, the three-qubit GHZ state can be verified with such a high efficiency by virtue of the Mermin inequality[46,50].

It should be pointed out that all our protocols for verifying GHZ states are applicable even in the presence of an arbitrary number of dishonest parties as long as the verifier is honest. Meanwhile, these protocols are useful for detecting GME. For some cryptographic tasks such as anonymous quantum communication, the security for all honest parties can be guaranteed at the same time with the assistance of a trusted common random source (CRS)[23]. In this case, the number of honest parties can affect the security parameter.

DISCUSSION

We proposed a simple and practical approach for verifying the Bell state in an untrusted quantum network in which one party is not honest. We also established a simple connection between verification protocols of the Bell state and probability distributions on the Bloch sphere together with an intuitive geometric picture. Based on this connection, we derived simple formulas for the guessing probability as functions of the concurrence and reduced fidelity. Meanwhile, we clarified the sample efficiency of each verification protocol and showed that the sample efficiency is determined by the threshold in the guessing probability. Moreover, we constructed the optimal and simplest protocols for verifying the Bell state, which are also very useful to detecting entanglement in the untrusted network.

Furthermore, we reduce the verification problem of GHZ states to the counterpart of the Bell state, which enables us to construct the optimal protocol for verifying GHZ states and for detecting GME. Our work shows that both Bell state and GHZ states can be verified in the SDI scenario with the same sample complexity as in standard QSV. By contrast, the sample complexity in the DI scenario is in general quadratically worse. This work is instrumental to verifying entangled states in untrusted quantum networks, which is crucial to guaranteeing the proper functioning of quantum networks. In addition, this work is of intrinsic interest to the foundational studies on quantum steering. In the future, it would be desirable to generalize our results to generic bipartite pure states, stabilizer states, and other quantum states.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon request.

CODE AVAILABILITY

The codes used for numerical analysis are available from the corresponding author upon request.

Received: 9 February 2021; Accepted: 20 October 2021;
Published online: 26 November 2021

REFERENCES

1. Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* **81**, 865–942 (2009).
2. Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).
3. Uola, R., Costa, A. C. S., Nguyen, H. C. & Gühne, O. Quantum steering. *Rev. Mod. Phys.* **92**, 015001 (2020).
4. Greenberger, D. M., Horne, M. A. & Zeilinger, A. *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, ed Kafatos, M. (Kluwer Academic, 1989).
5. Greenberger, D. M., Horne, M. A., Shimony, A. & Zeilinger, A. Bell's theorem without inequalities. *Am. J. Phys.* **58**, 1131–1143 (1990).
6. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
7. Bouwmeester, D. et al. Experimental quantum teleportation. *Nature* **390**, 575–579 (1997).
8. Zhao, Z. et al. Experimental demonstration of five-photon entanglement and open-destination teleportation. *Nature* **430**, 54–58 (2004).
9. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
10. Acín, A. et al. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
11. Acín, A. & Masanes, L. Certified randomness in quantum physics. *Nature* **540**, 213–219 (2016).
12. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).
13. Pan, J.-W., Bouwmeester, D., Daniell, M., Weinfurter, H. & Zeilinger, A. Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. *Nature* **403**, 515–519 (2000).
14. Hein, M., Eisert, J. & Briegel, H. J. Multiparty entanglement in graph states. *Phys. Rev. A* **69**, 062311 (2004).
15. Kimble, H. J. The quantum internet. *Nature* **453**, 1023–1030 (2008).
16. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: a vision for the road ahead. *Science* **362**, eaam9288 (2018).
17. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).
18. Bell, B. A. et al. Experimental demonstration of graph-state quantum secret sharing. *Nat. Commun.* **5**, 5480 (2014).
19. Zhao, S. et al. Phase-matching quantum cryptographic conferencing. *Phys. Rev. Appl.* **14**, 024010 (2020).
20. Fu, Y., Yin, H.-L., Chen, T.-Y. & Chen, Z.-B. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **114**, 090501 (2015).
21. Eisert, J. et al. Quantum certification and benchmarking. *Nat. Rev. Phys.* **2**, 382–390 (2020).
22. Šupić, I. & Bowles, J. Self-testing of quantum systems: a review. *Quantum* **4**, 337 (2020).
23. Pappa, A., Chailloux, A., Wehner, S., Diamanti, E. & Kerenidis, I. Multipartite entanglement verification resistant against dishonest parties. *Phys. Rev. Lett.* **108**, 260502 (2012).
24. McCutcheon, W. et al. Experimental verification of multipartite entanglement in quantum networks. *Nat. Commun.* **7**, 13251 (2016).
25. Šupić, I. & Hoban, M. J. Self-testing through EPR-steering. *New J. Phys.* **18**, 075006 (2016).
26. Gheorghiu, A., Wallden, P. & Kashefi, E. Rigidity of quantum steering and one-sided device-independent verifiable quantum computation. *New J. Phys.* **19**, 023043 (2017).
27. Lu, H. et al. Counting classical nodes in quantum networks. *Phys. Rev. Lett.* **124**, 180503 (2020).
28. Markham, D. & Krause, A. A simple protocol for certifying graph states and applications in quantum networks. *Cryptography* **4**, 3 (2020).
29. Unnikrishnan, A. & Markham, D. Verification of graph states in an untrusted network. Preprint at http://arxiv.org/abs/2007.13126 (2020).
30. Branciard, C., Cavalcanti, E. G., Walborn, S. P., Scarani, V. & Wiseman, H. M. One-sided device-independent quantum key distribution: security, feasibility, and the connection with steering. *Phys. Rev. A* **85**, 010301(R) (2012).
31. Unnikrishnan, A. et al. Anonymity for practical quantum networks. *Phys. Rev. Lett.* **122**, 240501 (2019).
32. Hahn, F., Jong, J. & Pappa, A. Anonymous quantum conference key agreement. *PRX Quantum* **1**, 020325 (2020).
33. Hayashi, M. & Koshiba, T. Verifiable quantum secure modulo summation. Preprint at http://arxiv.org/abs/1910.05976 (2019).
34. Wiseman, H. M., Jones, S. J. & Doherty, A. C. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.* **98**, 140402 (2007).
35. Saunders, D. J., Jones, S. J., Wiseman, H. M. & Pryde, G. J. Experimental EPR-steering using Bell-local states. *Nat. Phys.* **6**, 845–849 (2010).
36. Cavalcanti, D. et al. Detection of entanglement in asymmetric quantum networks and multipartite quantum steering. *Nat. Commun.* **6**, 7941 (2015).
37. Berta, M., Christandl, M., Colbeck, R., Renes, J. M. & Renner, R. The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **6**, 659–662 (2010).
38. Zhu, H. Zero uncertainty states in the presence of quantum memory. *npj Quantum Inf.* **7**, 47 (2021).
39. Flammia, S. T. & Liu, Y.-K. Direct fidelity estimation from few Pauli measurements. *Phys. Rev. Lett.* **106**, 230501 (2011).
40. Hayashi, M., Matsumoto, K. & Tsuda, Y. A study of LOCC-detection of a maximally entangled state using hypothesis testing. *J. Phys. A: Math. Gen.* **39**, 14427–14446 (2006).
41. Hayashi, M. Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing. *New J. Phys.* **11**, 043028 (2009).
42. Pallister, S., Linden, N. & Montanaro, A. Optimal verification of entangled states with local measurements. *Phys. Rev. Lett.* **120**, 170502 (2018).
43. Zhu, H. & Hayashi, M. Efficient Verification of Pure Quantum States in the Adversarial Scenario. *Phys. Rev. Lett.* **123**, 260504 (2019).
44. Zhu, H. & Hayashi, M. General framework for verifying pure quantum states in the adversarial scenario. *Phys. Rev. A* **100**, 062335 (2019).
45. Takeuchi, Y. & Morimae, T. Verification of many-qubit states. *Phys. Rev. X* **8**, 021060 (2018).
46. Dimić, A., Šupić, I. & Dakić, B. Sample-efficient device-independent quantum state verification and certification. Preprint at http://arxiv.org/abs/2105.05832 (2021).
47. Mayers, D. & Yao, A. Self testing quantum apparatus. *Quantum Inf. Comput.* **4**, 273 (2004).
48. McKague, M., Yang, T. H. & Scarani, V. Robust self-testing of the singlet. *J. Phys. A: Math. Theor.* **45**, 455304 (2012).
49. Yang, T. H., Vértesi, T., Bancal, J.-D., Scarani, V. & Navascués, M. Robust and versatile black-box certification of quantum devices. *Phys. Rev. Lett.* **113**, 040401 (2014).
50. Kaniewski, J. Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities. *Phys. Rev. Lett.* **117**, 070402 (2016).
51. Hayashi, M. & Hajdušek, M. Self-guaranteed measurement-based quantum computation. *Phys. Rev. A* **97**, 052308 (2018).
52. Metger, T. & Vidick, T. Self-testing of a single quantum device under computational assumptions. *Quantum* **5**, 544 (2021).
53. Zhu, H. & Hayashi, M. Optimal verification and fidelity estimation of maximally entangled states. *Phys. Rev. A* **99**, 052346 (2019).

54. Wang, K. & Hayashi, M. Optimal verification of two-qubit pure states. *Phys. Rev. A* **100**, 032315 (2019).
55. Li, Z., Han, Y.-G. & Zhu, H. Efficient verification of bipartite pure states. *Phys. Rev. A* **100**, 032316 (2019).
56. Yu, X.-D., Shang, J. & Gühne, O. Optimal verification of general bipartite pure states. *npj Quantum Inf.* **5**, 112 (2019).
57. Li, Z., Han, Y.-G. & Zhu, H. Optimal verification of Greenberger-Horne-Zeilinger states. *Phys. Rev. Appl.* **13**, 054002 (2020).
58. Dangniam, N., Han, Y.-G. & Zhu, H. Optimal verification of stabilizer states. *Phys. Rev. Res.* **2**, 043323 (2020).
59. Helstrom, C. W. *Quantum Detection and Estimation Theory* (Academic, 1976).
60. Jevtic, S., Pusey, M., Jennings, D. & Rudolph, T. Quantum steering ellipsoids. *Phys. Rev. Lett.* **113**, 020402 (2014).
61. Zhang, C. et al. Experimental validation of quantum steering ellipsoids and tests of volume monogamy relations. *Phys. Rev. Lett.* **122**, 070402 (2019).
62. Wootters, W. K. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.* **80**, 2245 (1998).
63. Verstraete, F. & Verschelde, H. Fidelity of mixed states of two qubits. *Phys. Rev. A* **66**, 022307 (2002).
64. Gühne, O. & Tóth, G. Entanglement detection. *Phys. Rep.* **474**, 1–75 (2009).

ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China (Grant No. 11875110 and No. 62101600) and Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01).

AUTHOR CONTRIBUTIONS

Y.G.H. and Y.W. initiated the project. Y.G.H., Z.L. and H.Z. did the theoretical analysis. H.Z. supervised the project. All authors discussed the results and contributed to the final manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-021-00499-8.

Correspondence and requests for materials should be addressed to Huangjun Zhu.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.