Robust self-testing of multipartite Greenberger-Horne-Zeilinger-state measurements in quantum networks

Qing Zhou,[1,2] Xin-Yu Xu,[1,2] Shuai Zhao,[1,2] Yi-Zheng Zhen,[1,2] Li Li,[1,2,3,*]
Nai-Le Liu,[1,2,3,†] and Kai Chen[1,2,3,‡]

[1] *Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China*

[2] *CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*

[3] *Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

(Received 24 May 2022; accepted 12 September 2022; published 11 October 2022)

Self-testing is an examination for characterizing unknown quantum devices based on correlations of observed statistics in a black-box scenario. With development of large-scale quantum networks, the requirement for self-testing multipartite entangled measurements has become very demanding. We develop here a general procedure for self-testing arbitrary generalized Greenberger-Horne-Zeilinger-state (GHZ-state) measurements which applies to any number of parties. Moreover, it turns out that the existing result for the three-qubit GHZ-state measurement is recovered as a special case. Our results will motivate operational certification of quantum devices related to device-independent quantum information tasks for various scenarios in complicated quantum networks.

DOI: 10.1103/PhysRevA.106.042608

I. INTRODUCTION

The rapid development of quantum communication in recent years has created an exigent requirement for devising certification methods to guarantee the correctness of quantum information tasks. To rule out any potential attacks by a malicious third party, such certification methods must be device independent. As the first device-independent tool, the Bell nonlocality has been extensively studied in recent decades [1]. It has brought great breakthroughs in quantum physics. Recently, as the strongest form of certification for quantum devices, self-testing has been developed [2], which is also based on the Bell nonlocality. Such a certification method can characterize target objects (quantum states, measurements) fully only up to local isometries. Moreover, as the self-testing is a black-box test, it can be considered a device-independent certification under the assumption that quantum systems are able to be prepared many times in an independent, identically distributed (IID) manner.

Since the pioneering work of Mayers and Yao [3], self-testing has attracted lots of attention. It can be used to certify entangled pure states and measurements [4–23]. To date, a wide range of entangled quantum states have been proved to be self-testable, such as the elegant results for all pure bipartite entangled states [24], three-qubit W states [25], and graph states [26]. It has also been shown that all pure multipartite Greenberger-Horne-Zeilinger (GHZ) states and Dicke states can be self-tested [27]. Moreover, a self-testing method for quantum channels has also been developed [28]. In addition, there have been many applications of self-testing, such as quantum key distribution [29], randomness expansion [30], detection for entanglement [31], certification of genuinely entangled subspaces [32,33], coarse-grained self-testing of a many-body singlet [34], and verification of quantum computations [35,36]. Recently, a device-independent quantum state verification protocol under a more stringent concept of device independence that drops the IID assumption was studied in Ref. [37] based on self-testing methods.

In this work, we focus on self-testing entangled measurements in quantum networks. Self-testing entangled quantum measurements has great potential for developing practical quantum networks, which were preliminarily studied in Refs. [38,39]. Consider a simple network connected by three nodes (Alice, Bob, and Charlie), where two observers, Alice and Bob, share entangled states with a central node, Charlie. If one wants to efficiently perform some quantum information processing tasks in such a network (e.g., the entanglement distribution between remote parties Alice and Bob), a self-testable entangled measurement on Charlie is essential. In Ref. [38], the authors presented a self-testing method for the Bell-state measurement (BSM) and three-qubit GHZ-state measurement (GSM). Furthermore, a more robust self-testing scheme for BSM was also proposed in Ref. [39]. However, there has not been a detailed characterization for self-testing multipartite ($N > 3$) entangled measurements directly.

By generalizing the idea of Ref. [38], we present herein a self-testing method for an N-qubit generalized GSM whose eigenstates are N-qubit generalized GHZ states. To verify whether a measurement is generalized GSM or not, one

[*] eidos@ustc.edu.cn

[†] nlliu@ustc.edu.cn

[‡] kaichen@ustc.edu.cn

©2022 American Physical Society

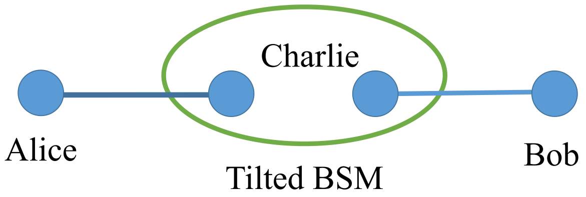

FIG. 1. An entanglement-swapping scenario: Charlie shares a maximally entangled two-qubit state with each of the other two observers (Alice and Bob). If Charlie performs tilted BSM and obtains outcome b, then Alice and Bob will be projected into $|\mathrm{Bell}_\theta^b\rangle$; that is, Alice and Bob can observe the maximal violation of the specific tilted CHSH inequality with $\mathrm{CHSH}_b^\alpha = \sqrt{8+2\alpha^2}$.

should first confirm all of its measurement eigenstates are really generalized GHZ states. Thus, the first step to self-test a generalized GSM is self-testing all of its measurement eigenstates, and the problem of self-testing a generalized GSM can be converted to the problem of self-testing states. Motivated by the method for self-testing multipartite entangled states in Ref. [27], we have developed further a general method for self-testing a multipartite generalized GSM in a star network, and the method is operational from an experimental point of view. We also show that one can self-test more entangled measurements using our developed method straightforwardly.

This paper is organized as follows. In Sec. II, we provide a preparation review of the tilted Clauser-Horne-Shimony-Holt (CHSH) scenario which constitutes an important ingredient of our self-testing method. In Sec. III, the self-testing method for a multipartite generalized GSM is presented. In Sec. IV, a noise-robust self-testing scheme of a three-qubit GSM is presented, with the help of semidefinite-program (SDP) method. Finally, we conclude our results and discuss potential future works in Sec. V.

II. PRELIMINARIES

Before studying the self-testing of multipartite generalized GSM, let us introduce an entanglement-swapping scenario in detail (see Fig. 1). It is shown that after Charlie performs an entangled measurement, the remaining state of Alice and Bob will be projected into the eigenstate of Charlie's measurement. Such a procedure presents direct insight into the relation between the entangled measurement and its measurement eigenstates, which is a fundamental idea for self-testing multipartite generalized GSM. Like in Appendix C in Ref. [38], we consider the tilted BSM here. To certify the tilted BSM, the tilted CHSH inequality is necessary [40]. Let us consider a task: Alice and Bob share a two-qubit state, and they want to know whether the shared state is entangled or not. They perform local measurements (dichotomic observables) separately. The tilted CHSH inequality is given by

$$\alpha\langle A_0\rangle + \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leqslant 2+\alpha, \quad (1)$$

where the maximal value of quantum violation is $\sqrt{8+2\alpha^2}, \alpha \in [0,2)$, with A_i and B_i being observables with outcomes $\{-1,+1\}$ measured locally by Alice and Bob. Here, we omit the notation $\otimes$ between systems A and B and write $A_0 \otimes I$ as A_0 for short. After performing local measurements, if Alice and Bob obtain the maximal violation of the tilted CHSH inequality, the state shared by them is certainly a partially entangled two-qubit state (tilted Bell state). For the detailed case, the four tilted Bell states $|\mathrm{Bell}_\theta^b\rangle$, $b = 0, 1, 2, 3$, are

$$|\mathrm{Bell}_\theta^b\rangle = (-1)^{2k_1+k_2}\cos\theta|k_1k_2\rangle + \sin\theta|\bar{k}_1\bar{k}_2\rangle,$$

where $b = 2k_1 + k_2$, $k_i \in \{0,1\}$, and $\bar{k}_i = 1 - k_i$, $i \in \{1,2\}$, $\theta \in (0, \frac{\pi}{4}]$. Let μ satisfy $\tan\mu = \sin 2\theta$ and σ_Z, σ_X be Pauli matrices. If one fixes the measurement settings of Alice and Bob as $A_0 = \sigma_Z$, $A_1 = \sigma_X$, $B_0 = \cos\mu\sigma_Z + \sin\mu\sigma_X$, and $B_1 = \cos\mu\sigma_Z - \sin\mu\sigma_X$, the output statistics obtained with these measurements will maximally violate some tilted CHSH inequalities. The maximal violation is $\mathrm{CHSH}_b^\alpha = \langle\mathrm{Bell}_\theta^b|W_b^\alpha|\mathrm{Bell}_\theta^b\rangle = \sqrt{8+2\alpha^2}$, with $\alpha = 2\cos 2\theta/\sqrt{1+\sin^2 2\theta}$, where

$$\begin{aligned}
W_0^\alpha &= \alpha A_0 + A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1,\\
W_1^\alpha &= \alpha A_0 - A_0B_0 - A_0B_1 - A_1B_0 + A_1B_1,\\
W_2^\alpha &= -\alpha A_0 - A_0B_0 - A_0B_1 + A_1B_0 - A_1B_1,\\
W_3^\alpha &= -\alpha A_0 + A_0B_0 + A_0B_1 - A_1B_0 + A_1B_1.
\end{aligned}$$

Here, W_b^α is a Bell operator acting on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ of Alice and Bob. It is easy to show that the eigenvalue $\sqrt{8+2\alpha^2}$ of the Bell operator W_b^α is nondegenerate with the associated eigenvector $|\mathrm{Bell}_\theta^b\rangle$. Hence, if the maximal violation of CHSH_b^α is $\sqrt{8+2\alpha^2}$, the shared state will be $|\mathrm{Bell}_\theta^b\rangle$. One can discriminate the four tilted Bell states by the maximal violations of four tilted Bell inequalities with fixed measurement settings. Furthermore, other tilted Bell states that are local unitary (constructed by σ_Z, σ_X) equivalent to the above four tilted Bell states can also be discriminated. For example, the state $|\Phi\rangle = \cos\theta|00\rangle - \sin\theta|11\rangle = \sigma_{Z_A}|\mathrm{Bell}_\theta^0\rangle$ can maximally violate the tilted CHSH inequality with $\mathrm{CHSH}_\theta = \langle\sigma_{Z_A}W_0^\alpha\sigma_{Z_A}^\dagger\rangle = \alpha\langle A_0\rangle + \langle A_0B_0 + A_0B_1 - A_1B_0 + A_1B_1\rangle$ and fixed measurements given above.

In the entanglement-swapping scenario [41] shown in Fig. 1, let Charlie perform a tilted BSM with outcomes b. Then, the remaining state will be projected into one of the four tilted Bell states $|\mathrm{Bell}_\theta^b\rangle$ conditioned on the outcomes b. Conversely, if one finds that Alice and Bob share tilted Bell states $|\mathrm{Bell}_\theta^b\rangle$ for $b \in \{0,1,2,3\}$, Charlie's performed measurement is a tilted BSM. When it comes to the self-testing scenario, the target for self-testing will be equivalent to one of the four tilted Bell states or a tilted BSM, up to a local isometry. Physically, a local isometry performed on a state can be considered a local unitary operator after adding local ancillas (e.g., $|0\cdots0\rangle$) [2]. Motivated by this idea, we will develop a procedure for self-testing a multipartite generalized GSM.

III. SELF-TESTING A MULTIPARTITE GENERALIZED GSM

As shown in Ref. [42], any completely positive and trace-preserving (CPTP) map can be implemented by tracing out

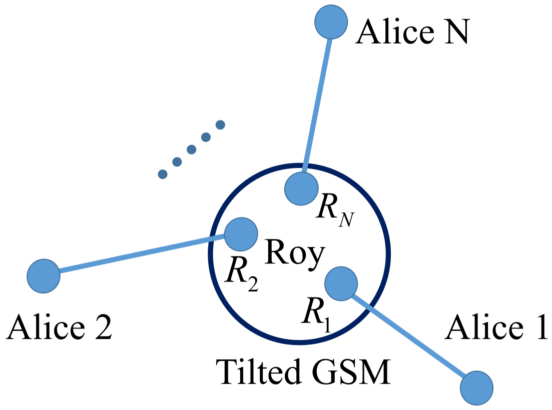

FIG. 2. Roy shares a Bell state with each of the other N observers (Alice 1, Alice 2, …, Alice N). If Roy performs multipartite generalized GSM, then the state shared by Alice 1, Alice 2, …, Alice N will be projected into $|\mathrm{GHZ}_\theta^r\rangle$. Conversely, if Alice 1, Alice 2, …, Alice N observe that it is projected into $|\mathrm{GHZ}_\theta^r\rangle$ for all r, the measurement performed by Roy is equivalent to the generalized GSM.

degrees of freedom that do not involve effective information after applying a local isometry. Therefore, one can directly generalize the definition in [2,16,38] to present the self-testing of multipartite measurements via simulation: denote an ideal d-outcome measurement for Roy acting on $\mathcal{H}_{R'_1}\otimes\mathcal{H}_{R'_2}\otimes\cdots\otimes\mathcal{H}_{R'_N}$ as $\mathcal{P}'=\{P'^r_{R'_1R'_2\cdots R'_N}\}_{r=1}^d$ and a real measurement acting on $\mathcal{H}_{R_1}\otimes\mathcal{H}_{R_2}\otimes\cdots\otimes\mathcal{H}_{R_N}$ as $\mathcal{P}=\{P^r_{R_1R_2\cdots R_N}\}_{r=1}^d$. If there exist completely positive and unital maps $\Lambda_{R_j}:\mathcal{L}(\mathcal{H}_{R_j})\rightarrow\mathcal{L}(\mathcal{H}_{A'_j})$ for $j\in\{1,2,\ldots,N\}$, such that

$$\Lambda_{R_1}\otimes\Lambda_{R_2}\otimes\cdots\otimes\Lambda_{R_N}\left(P^r_{R_1R_2\cdots R_N}\right)=P'^r_{R'_1R'_2\cdots R'_N}\qquad(2)$$

for all r, we say $\mathcal{P}$ is capable of simulating $\mathcal{P}'$. In the above definition, we adopt the assumption that the different physical sources are independent in a quantum network. The construction of a quantum network as shown in Fig. 2 guarantees the well-defined N partition for Roy's measurement device, i.e., $\mathcal{H}_R=\mathcal{H}_{R_1}\otimes\mathcal{H}_{R_2}\otimes\cdots\otimes\mathcal{H}_{R_N}$.

The idea of our self-testing method relies on the task of entanglement swapping as shown in Fig. 2. There are N initially uncorrelated parties Alice 1 (A_1), Alice 2 (A_2), …, Alice N (A_N). They are independently entangled with an additional party, Roy. Specifically, A_i and Roy share a Bell state $|\mathrm{Bell}^0_{\pi/4}\rangle_{A_iR_i}\in\mathcal{H}_{A_i}\otimes\mathcal{H}_{R_i}$, $i\in\{1,2,\ldots,N\}$. To distribute entanglement among $A_1,A_2,\ldots,A_N$ in such a quantum star network, Roy performs the generalized GSM and obtains outcomes $r=(k_1k_2\cdots k_N)$ with $k_1,k_2,\ldots,k_N\in\{0,1\}$. For simplicity, we denote the outcomes as $r\in\{0,1,\ldots,2^N-1\}$. Then, the states shared by $A_1,A_2,\ldots,A_N$ are projected to one of the 2^N generalized GHZ states $|\mathrm{GHZ}_\theta^r\rangle$ based on the outcome r. The generalized GHZ states are measurement eigenstates of the generalized GSM given by

$$|\mathrm{GHZ}_\theta^r\rangle=(-1)^r\cos\theta|k_1k_2\cdots k_N\rangle+\sin\theta|\bar{k}_1\bar{k}_2\cdots\bar{k}_N\rangle,$$

where $r=\sum_{i=1}^N k_i2^{N-i}$, $\bar{k}_i=1-k_i$, and $k_i\in\{0,1\}$, $i\in\{1,\ldots,N\}$. The generalized GSM can be denoted as $\mathrm{GSM}_\theta=\{\mathrm{GHZ}_\theta^r\}_{r=0}^{2^N-1}$, with $\mathrm{GHZ}_\theta^r=|\mathrm{GHZ}_\theta^r\rangle\langle\mathrm{GHZ}_\theta^r|$. If $A_1,A_2,\ldots,A_N$ obtain Roy's outcomes r, they can apply a certain local unitary operation on their qubits, so that they share a certain generalized GHZ state. With the above operations, we have implemented the distribution of entanglement among N remote parties.

The self-testing procedure is similar to the task of entanglement swapping without assumptions on the dimensions, initial states, and operators. From now on, for any observable Q acting on Hilbert spaces $\mathcal{H}$, by adding a prime, we denote Q' as the observable acting on two-dimensional Hilbert spaces $\mathcal{H}'$. Let us start with presenting the self-testing method for N-partite generalized GHZ states given in Ref. [27].

Lemma 1. (Refer to Ref. [27].) Suppose an N-partite state $|\psi\rangle$ and a pair of binary observables $A_{0,i}$ and $A_{1,i}$ for the ith party, with $i=1,\ldots,N$. For an observable D, let $P_D^a=[I+(-1)^aD]/2$, $a\in\{0,1\}$. Let μ satisfy $\tan\mu=\sin 2\theta$, $Z_i=A_{0,i}$, and $X_i=A_{1,i}$ for $i=1,\ldots,N-1$. Then, let Z_N^* be $(A_{0,N}+A_{1,N})/(2\cos\mu)$ with zero eigenvalues replaced by 1 and X_N^* be $(A_{0,N}-A_{1,N})/(2\sin\mu)$ with zero eigenvalues replaced by 1. Define $Z_N=Z_N^*|Z_N^*|^{-1}$ and $X_N=X_N^*|X_N^*|^{-1}$. If the relations

$$\langle\psi|P^0_{A_{0,i}}|\psi\rangle=\langle\psi|P^0_{A_{0,i}}P^0_{A_{0,j}}|\psi\rangle=c_\theta^2\;\;\forall\, i,j\in\{1,\ldots,N-1\},$$

$$\left\langle\psi|\prod_{i=1}^{N-2}P^{a_i}_{A_{1,i}}|\psi\right\rangle=\frac{1}{2^{N-2}}\;\;\forall\, a_i\in\{0,1\},$$

$$\left\langle\psi\left|\left(\prod_{i=1}^{N-2}P^{a_i}_{A_{1,i}}\right)W\right|\psi\right\rangle=\frac{\sqrt{8+2\alpha^2}}{2^{N-2}}\forall\, a_i\in\{0,1\},$$

where

$$\begin{aligned}W=&\alpha A_{0,N-1}\otimes I_N+A_{0,N-1}A_{0,N}+A_{0,N-1}A_{1,N}\\&+(-1)^{\sum_{i=1}^{N-2}a_i}(A_{1,N-1}A_{0,N}-A_{1,N-1}A_{1,N}),\end{aligned}$$

$\alpha = 2\cos 2\theta/\sqrt{1+\sin^2 2\theta}$ and $c_\theta = \cos\theta$, $\theta \in (0, \pi/4]$, are satisfied, there exists a local isometry Φ such that

$$\Phi(|\psi\rangle) = |\text{junk}\rangle|\text{GHZ}_\theta^0\rangle.$$

Hence, the correlations that satisfy the above relations self-test the state $|\text{GHZ}_\theta^0\rangle = \cos\theta|0\rangle^{\otimes N} + \sin\theta|1\rangle^{\otimes N}$.

The junk state in Lemma 1 can be any state and can be removed by tracing out the $A_1A_2\cdots A_N$ space. Here, Z_N and X_N act on $|\psi\rangle$ in the same way as $(A_{0,N}+A_{1,N})/(2\cos\mu)$ and $(A_{0,N}-A_{1,N})/(2\sin\mu)$, respectively [2]. For details, the ideal measurements achieving these correlations in Lemma 1 are $A'_{0,i} = \sigma_Z$ and $A'_{1,i} = \sigma_X$ for $i = 1, \ldots, N-1$, $A'_{0,N} = \cos\mu\sigma_Z + \sin\mu\sigma_X$, and $A'_{1,N} = \cos\mu\sigma_Z - \sin\mu\sigma_X$.

Remarkably, for different $r \in \{0, 1, \ldots, 2^N-1\}$, the $|\text{GHZ}_\theta^r\rangle$ can all be self-tested by correlations in Lemma 1 with different measurement settings up to local isometries. In other words, one can obtain a local isometry such that $\Phi^r(|\psi^r\rangle) = |\text{junk}\rangle|\text{GHZ}_\theta^r\rangle$ for each r. As the isometry Φ^r can always be constructed by local operations which do not depend on r, one can always construct a single isometry such that $\Phi(|\psi^r\rangle) = |\text{junk}\rangle|\text{GHZ}_\theta^r\rangle$. A detailed description will be given in Lemma 2.

Now, let us first introduce some notations. For an observable O' acting on Hilbert space $\mathcal{H}' = \otimes_{i=1}^N \mathcal{H}_{A'_i}$, let $\widetilde{O'}^r = U'^{r\dagger} O' U'^r$, where $U'^r = \otimes_{i=1}^N U'^r_{A'_i}$ acts on $\mathcal{H}'$. Here, $\mathcal{H}_{A'_i}$, $i \in \{1, 2, \ldots, N\}$, are two dimensional Hilbert spaces. The unitary operator U'^r satisfies the equation $U'^r|\text{GHZ}_\theta^r\rangle = |\text{GHZ}_\theta^0\rangle$ and is constructed by the product of the identity matrix I' and Pauli matrices X' and Z'. Then, one can define $\widetilde{O}^r = U^{r\dagger} O U^r$ by replacing I', X', and Z' in $\widetilde{O'}^r$ with I, X, and Z. With the above special unitary transformation, one can obtain Lemma 2.

Lemma 2. Let $|\psi\rangle$ be an N-partite state, and let $A_{0,i}$ and $A_{1,i}$ be a pair of binary observables for the ith party for $i = 1, \ldots, N$. Suppose that, for all $r \in \{0, 1, \ldots, 2^N-1\}$, the following relations are satisfied:

$$\begin{aligned}\langle\psi|\widetilde{P^0_{A_{0,i}}}^r|\psi\rangle &= \langle\psi|\widetilde{P^0_{A_{0,i}}}^r\widetilde{P^0_{A_{0,j}}}^r|\psi\rangle \\ &= c_\theta^2 \quad \forall\, i, j \in \{1, \ldots, N-1\}, \qquad (3)\end{aligned}$$

$$\left\langle\psi\left|\prod_{i=1}^{N-2}\widetilde{P^{a_i}_{A_{1,i}}}^r\right|\psi\right\rangle = \frac{1}{2^{N-2}} \quad \forall\, a_i \in \{0, 1\}, \qquad (4)$$

$$\left\langle\psi\left|\left(\prod_{i=1}^{N-2}\widetilde{P^{a_i}_{A_{1,i}}}^r\right)\widetilde{W^\alpha_{\vec{a}}}^r\right|\psi\right\rangle = \frac{\sqrt{8+2\alpha^2}}{2^{N-2}} \quad \forall\, a_i \in \{0, 1\}, \qquad (5)$$

where $\vec{a} = a_1\cdots a_{N-2}$ and

$$\begin{aligned}\widetilde{W^\alpha_{\vec{a}}}^0 = W^\alpha_{\vec{a}} &= \alpha A_{0,N-1}\otimes I_N + A_{0,N-1}A_{0,N} + A_{0,N-1}A_{1,N} \\ &\quad + (-1)^{\Sigma_{i=1}^{N-2}a_i}(A_{1,N-1}A_{0,N} - A_{1,N-1}A_{1,N}).\end{aligned}$$

The detailed forms for $\widetilde{P^0_{A_{0,i}}}^r$ and $\widetilde{P^{a_i}_{A_{1,i}}}^r$ are easy to calculate, and the details for $\widetilde{W^\alpha_{\vec{a}}}^r$ as an example are provided in Appendix B. The measurements here are the same as shown in Lemma 1. Then, there exists a single local isometry such that $\Phi(|\psi^r\rangle) = |\text{junk}\rangle|\text{GHZ}_\theta^r\rangle$ for all r.

Proof. For $r = 0$, the correlations in Lemma 2 are the same as in Lemma 1. Hence, these correlations self-test state $|\text{GHZ}_\theta^0\rangle$. Denote $|\psi\rangle$ in the self-testing procedure as $|\psi^0\rangle$. From Lemma 1, there exists a local isometry Φ such that $\Phi(|\psi^0\rangle) = |\text{junk}\rangle|\text{GHZ}_\theta^0\rangle$. Meanwhile, $X_f^2 = Z_f^2 = I$, and X_f and Z_f anticommute over the support of the state $|\psi^0\rangle$ for all $f \in \{A_1, A_2, \ldots, A_N\}$ [27]. Then, one can construct this isometry using ancillary qubits $|0\rangle^{\otimes N}$ and SWAP gates $\{S_{X_f,Z_f}\}$ as

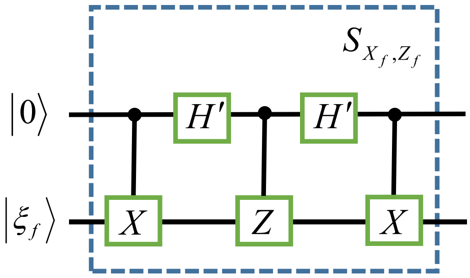

FIG. 3. A SWAP gate is constructed by unitary X, Z, and H', where H' is the Hadamard gate, and X and Z anticommute over the support of the state $|\xi_f\rangle \in \mathcal{H}$. The $|0\rangle$ is in the qubit Hilbert space $\mathcal{H}'$.

$$\Phi(|\psi^0\rangle) = \big(\otimes_{i=1}^N S_{X_{A_i},Z_{A_i}}\big)|0\rangle^{\otimes N}|\psi^0\rangle = |\text{junk}\rangle|\text{GHZ}_\theta^0\rangle. \qquad (6)$$

The detailed form of a SWAP gate is shown in Fig. 3. From Lemma 1 in Ref. [38], one knows that $S_{X_f,Z_f}\cdot X\cdot|0\rangle|\xi_f\rangle = X'\cdot S_{X_f,Z_f}\cdot|0\rangle|\xi_f\rangle$ and $S_{X_f,Z_f}\cdot Z\cdot|0\rangle|\xi_f\rangle = Z'\cdot S_{X_f,Z_f}\cdot|0\rangle|\xi_f\rangle$. Let $S_{A_1A_2\cdots A_N} = (\otimes_{i=1}^N S_{X_{A_i},Z_{A_i}})$. As U^r is constructed by I, X, and Z, one has

$$\begin{aligned}\Phi(U^{r\dagger}|\psi^0\rangle) &= S_{A_1A_2\cdots A_N}|0\rangle^{\otimes N}U^{r\dagger}|\psi^0\rangle \\ &= U'^{r\dagger}S_{A_1A_2\cdots A_N}|0\rangle^{\otimes N}|\psi^0\rangle \\ &= U'^{r\dagger}\Phi(|\psi^0\rangle) = |\text{junk}\rangle\otimes U'^{r\dagger}|\text{GHZ}_\theta^0\rangle \\ &= |\text{junk}\rangle\otimes|\text{GHZ}_\theta^r\rangle.\end{aligned}$$

Here, $U^{r\dagger}|\psi^0\rangle = |\psi\rangle$. One has $\Phi(|\psi\rangle) = |\text{junk}\rangle|\text{GHZ}_\theta^r\rangle$. Therefore, the correlations that satisfy the relations in Lemma 2 self-test state $|\text{GHZ}_\theta^r\rangle$. $|\psi\rangle$ can be denoted as $|\psi^r\rangle$. Thus, one has $\Phi(|\psi^r\rangle) = |\text{junk}\rangle|\text{GHZ}_\theta^r\rangle$. ■

From Lemma 2, the self-testing method with fixed measurements can be used to distinguish special entangled pure states. Here, let $\{|\text{GHZ}_\theta^r\rangle\}_{r=0}^{2^N-1}$ be reference states and $|\text{GHZ}_\theta^0\rangle$ be a standard reference state. For example, there is a set of states $\{|\psi^s\rangle\}_{s=0}^{2^N-1}$ shared by $A_1, A_2, \ldots, A_N$. If one shared state $|\psi^{s_1}\rangle$ satisfies the correlations in Lemma 2 with $r = 0$, one can specify the shared state $|\psi^{s_1}\rangle$ as state $|\psi^0\rangle$ according to the standard reference state $|\text{GHZ}_\theta^0\rangle$. Then, for another shared state $|\psi^{s_2}\rangle$ with $s_2 \in \{0, 1, 2, \ldots, s_1-1, s_1+1, \ldots, 2^N-1\}$, if it satisfies correlations in Lemma 2 for one r with $r \in \{1, 2, \ldots, 2^N-1\}$, e.g., $r = 3$, then, one resets s_2 as $s_2 = 3$. In other words, the state $|\psi^{s_2}\rangle$ can be rewritten as $|\psi^3\rangle$, and these correlations have self-tested the $|\text{GHZ}_\theta^3\rangle$. Therefore, the states $|\psi^{s_1}\rangle$ and $|\psi^{s_2}\rangle$ are actually different. Now, the main result of the paper is as follows.

Theorem 1. Let $A_1, A_2, \ldots, A_N$ share a pair of quantum states with Roy as $\tau_{A_1R_1A_2R_2\cdots A_NR_N} = \tau_{A_1R_1}\otimes\tau_{A_2R_2}\otimes\cdots\otimes\tau_{A_NR_N}$, and let $\mathcal{R} = \{R^r_{R_1R_2\cdots R_N}\}_{r=0}^{2^N-1}$ be a 2^N-outcome measurement acting on $\mathcal{H}_{R_1}\otimes\mathcal{H}_{R_2}\otimes\cdots\otimes\mathcal{H}_{R_N}$. For $A_1, A_2, \ldots, A_N$, if there exist measurements such that the observed correlations conditioned on outcome r of Roy's measurement satisfy the relations in Lemma 2, then there exist completely positive and unital maps $\Lambda_{R_i}: \mathcal{L}(\mathcal{H}_{R_i}) \rightarrow \mathcal{L}(\mathcal{H}_{A_i'})$, $i \in \{1, 2, \dots, N\}$, for $\dim(\mathcal{H}_{A_i'}) = 2$ such that

$$\Lambda_{R_1} \otimes \Lambda_{R_2} \otimes \cdots \otimes \Lambda_{R_N}\left(R^r_{R_1R_2\cdots R_N}\right) = \mathrm{GHZ}^r_\theta \tag{7}$$

for $r \in \{0, 1, 2, \dots, 2^N - 1\}$.

A detailed proof is shown in Appendix A. Here, we present a brief description. Let the $\tau^r_{A_1A_2\cdots A_N} = |\psi^r\rangle\langle\psi^r|$ acting on $\otimes_{i=1}^N \mathcal{H}_i$ be the state shared by $A_1, A_2, \dots, A_N$ conditioned on outcome r. From Lemma 2, there exists a single isometry such that $\Phi(|\psi^r\rangle) = |\mathrm{junk}\rangle|\mathrm{GHZ}^r_\theta\rangle$. By tracing out the subsystems $\mathcal{H}_1, \dots, \mathcal{H}_N$, one can construct a single set of SWAP channels $\Gamma_{A_i}: \mathcal{L}(\mathcal{H}_{A_i}) \rightarrow \mathcal{L}(\mathcal{H}_{A_i'})$, $i \in \{1, 2, \dots, N\}$, such that

$$\left(\otimes_{i=1}^N \Gamma_{A_i}\right)\left(\tau^r_{A_1A_2\dots A_N}\right) = |\mathrm{GHZ}^r_\theta\rangle\langle\mathrm{GHZ}^r_\theta|$$

for all r. With the help of a Choi-Jamiołkowski map [38], one can construct completely positive and unital maps $\otimes_{i=1}^N \Lambda_{R_i}$, which are associated with the above SWAP channels, such that

$$\left(\otimes_{i=1}^N \Lambda_{R_i}\right)\left(R^r_{R_1R_2\cdots R_N}\right) = \left(\otimes_{i=1}^N \Gamma_{A_i}\right)\left(\tau^r_{A_1A_2\cdots A_N}\right) = \mathrm{GHZ}^r_\theta.$$

The 2^N equations given by Eq. (7) imply that a real measurement $\mathcal{R} = \{R^r_{R_1\cdots R_N}\}_{r=0}^{2^N-1}$ is capable of simulating an ideal generalized GSM, $\{\mathrm{GHZ}^r_\theta\}_{r=0}^{2^N-1}$; that is, Theorem 1 self-tests the generalized GSM. The method presents a unified form of the theorem for the multipartite case without resorting to different Bell inequalities. Following our procedure, one needs to check only whether the remaining two parties (A_N and A_{N-1}) maximally violate the tilted CHSH Bell inequality after performing local measurements on the other $N-2$ parties of state $|\psi^r\rangle_{A_1\cdots A_N}$, where the measurement settings are fixed by Lemma 2. Therefore, this approach is physically operational from an experimental point of view. Moreover, one can recover the case of a three-qubit GSM [38] when $\alpha = 0, \theta = \pi/4$, and $N = 3$.

Remarkably, for any self-testing method of generalized GHZ states, if the ideal measurements in the self-testing procedure are constructed using the linear combination of Pauli matrices, it can be adopted to self-test the generalized GSM. Such a property can be a rule to construct the self-testing method for generalized GSMs in the qubit case.

IV. ROBUST SELF-TESTING OF THE GSM

The ideal self-testing method is an excellent tool to certify quantum information tasks. However, due to the imperfection of quantum devices, accurate correlations in the above theorem may not be satisfied. Hence, a robust version of self-testing is necessary from an experimental point of view. Here, we focus on investigating the feasibility for robust self-testing of an arbitrary multipartite GSM. For convenience, we study a robust self-testing scheme for a three-qubit GSM, where $N = 3$, $\alpha = 0$, and $\theta = \pi/4$. The method for studying robustness of other N parties is similar.

Before presenting the robustness of the GSM, let us first study the robust self-testing of the GHZ state with the SDP method. One can rewrite A_1, A_2, and A_3 as A, B, and C and let $A_{i,1} = A_i, A_{i,2} = B$, and $A_{i,3} = C_i$, $i \in \{0, 1\}$. Let the state shared by A, B, and C with outcome $r = 0$ be $\tau^0_{ABC} = |\psi^0\rangle\langle\psi^0|$. In a general way, one can adopt the fidelity $F = \langle\mathrm{GHZ}|\sigma^0_{A'B'C'}|GHZ\rangle$ to capture the distance of the unknown state from the target state [43], where $|\mathrm{GHZ}\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}}$ and $\sigma^0_{A'B'C'} = \Gamma_A \otimes \Gamma_B \otimes \Gamma_C(\tau^0_{ABC})$. The maps Γ_f, $f \in \{A, B, C\}$, are defined in Fig. 3 as $\Gamma_f(|\xi\rangle_f\langle\xi|) = Tr_{\mathcal{H}_f}(S_{X_f,Z_f}|0\rangle\langle 0| \otimes |\xi\rangle_f\langle\xi|S^\dagger_{X_f,Z_f})$, with $f \in \{A, B, C\}$. Here, the assumption that X and Z are anticommutative in the definition of Γ has been removed. The state $\sigma^0_{A'B'C'}$ can be written as

$$\sigma^0_{A'B'C'} = \mathrm{Tr}_{ABC}(S_{ABC}|000\rangle_{A'B'C'}\langle 000| \otimes \tau^0_{ABC}S^\dagger_{ABC}). \tag{8}$$

From the definition of fidelity, one has

$$\begin{aligned} F &= \langle\mathrm{GHZ}|\sigma^0_{A'B'C'}|\mathrm{GHZ}\rangle \\ &= \frac{1}{128}\mathrm{Tr}_{ABC}\{8(1+Z_A)(1+Z_B)(1+Z_C)\tau^0_{ABC} \\ &\quad + 8(1-Z_A)(1-Z_B)(1-Z_C)\tau^0_{ABC} \\ &\quad + [\Pi_{f\in\{A,B,C\}}(1+Z_f)X_f(1-Z_f)]\tau^0_{ABC} \\ &\quad + [\Pi_{f\in\{A,B,C\}}(1-Z_f)X_f(1+Z_f)]\tau^0_{ABC}\}, \end{aligned} \tag{9}$$

where the fidelity can be expressed as a linear function of the expectation values. Suppose the channel has white noise (weight ε); one can transform the problem of robustness into the problem of finding a lower bound on the fidelity. It can be solved with the SDP [25,43–45]:

$$\begin{aligned} &\min \quad F = \langle\mathrm{GHZ}|\sigma^0_{A'B'C'}|\mathrm{GHZ}\rangle, \\ &\text{such that} \quad M \geqslant 0, \\ &\langle\psi|P^0_{A_0}|\psi\rangle = \langle\psi|P^0_{B_0}|\psi\rangle = \tfrac{1}{2}, \\ &\langle\psi|P^0_{A_0}P^0_{B_0}|\psi\rangle = \frac{1-\varepsilon}{2} + \frac{\varepsilon}{4}, \\ &\langle\psi|P^a_{A_1}|\psi\rangle = \tfrac{1}{2} \ \text{ for } a \in \{0, 1\}, \\ &\langle\psi|P^a_{A_1}[\alpha B_0 + B_0C_0 + B_0C_1 + (-1)^a(B_1C_0 - B_1C_1)]|\psi\rangle \\ &\quad = \sqrt{2}(1-\varepsilon), \ a \in \{0, 1\} \end{aligned} \tag{10}$$

where M is a moment matrix defined as $M_{ij} = \mathrm{Tr}(\tau^0_{ABC}D_i^\dagger D_j)$ with the set $\{D_1 = I, D_2 = Z_A, D_3 = X_A \cdots\}$ [46]. For an ideal case, the fidelity is 1 when error $\varepsilon = 0$. For other ε up to 0.1225, the relations between the minimal fidelity and error are shown in Fig. 4. Without loss of generality, one can define the relation between the minimal fidelity and ε as a function $G(\varepsilon^0)$, which will be used to study the robustness of the GSM. Here, ε has been rewritten as ε^0.

To define the quality of the real measurement $\mathcal{R}$ as a simulation of the ideal GSM $\mathcal{P}$, where $\mathcal{R} = \{R^r_{R_1R_2R_3}\}_0^7$ and $\mathcal{P} = \{\mathrm{GHZ}^r\}_0^7$, we directly extend the definition in Ref. [38] to three parties as

$$\mathcal{Q}(\mathcal{R}, \mathcal{P}) = \frac{1}{8} \times \max_{\Lambda_{R_1}\Lambda_{R_2}\Lambda_{R_3}} \sum_{r=0}^{7} \langle(\Lambda_{R_1} \otimes \Lambda_{R_2} \otimes \Lambda_{R_3})\left(R^r_{R_1R_2R_3}\right), \mathrm{GHZ}^r\rangle. \tag{11}$$

Here, we omit the subscript of $\mathrm{GHZ}^r_{\frac{\pi}{4}}$ and use GHZ^r, and Λ_{R_1}, Λ_{R_2}, and Λ_{R_3} are unital CPTP maps with Λ_{R_1} :

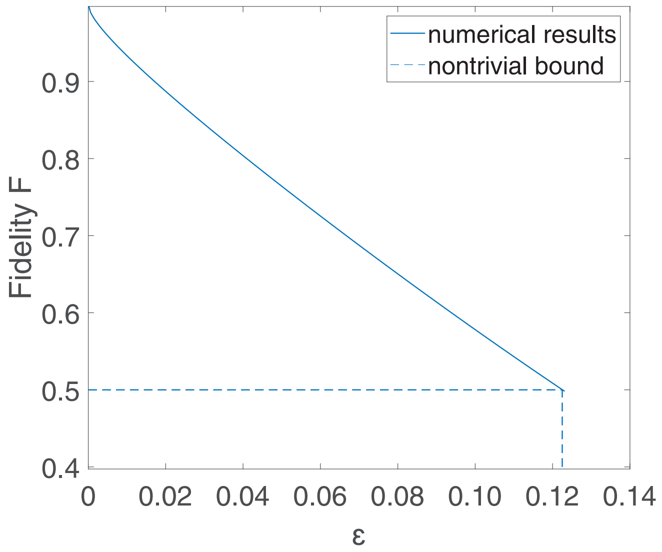

FIG. 4. The lower bound on the fidelity F between the GHZ state and the unknown state $\sigma^0_{A'B'C'}$ for different levels of white noise ε. When the fidelity is above the nontrivial bound of 0.5 (i.e., $\varepsilon \leqslant 12.25\%$), the unknown state is close to a GHZ state.

$\mathcal{L}(\mathcal{H}_{R_1}) \to \mathcal{L}(\mathcal{H}_{A'})$, $\Lambda_{R_2}: \mathcal{L}(\mathcal{H}_{R_2}) \to \mathcal{L}(\mathcal{H}_{B'})$, and $\Lambda_{R_3}: \mathcal{L}(\mathcal{H}_{R_3}) \to \mathcal{L}(\mathcal{H}_{C'})$. For two matrices L_1 and L_2, the symbol $\langle\cdot,\cdot\rangle$ is defined as

$$\langle L_1, L_2\rangle = Tr(L_1 L_2^\dagger).$$

Now, the robust version of the self-testing method is presented as follows.

Theorem 2. Let A, B, and C share a pair of quantum states with Roy as $\tau_{AR_1BR_2CR_3} = \tau_{AR_1} \otimes \tau_{BR_2} \otimes \tau_{CR_3}$, and let $\mathcal{R} = \{R^r_{R_1R_2R_3}\}_{r=0}^7$ be an eight-outcome measurement acting on $\mathcal{H}_{R_1} \otimes \mathcal{H}_{R_2} \otimes \mathcal{H}_{R_3}$. Let p_r be the probability of Roy observing the outcome r. Define the function $G(\varepsilon^r)$ as the lower bound on the fidelity between $\Gamma_A \otimes \Gamma_B \otimes \Gamma_C(\tau^r_{ABC})$ and GHZ^r under noise ε^r. For A, B, and C, suppose there exist measurements such that the observed correlations conditioned on outcomes r satisfy the relations in Lemma 2 with error ε^r and $G(\varepsilon^r) > 0.5$. Define $q = \Sigma_r p_r G(\varepsilon^r)$; then one has

$$\mathcal{Q}(\mathcal{R},\mathcal{P}) \geqslant \frac{1}{2[1+2\sqrt{q(1-q)}]^2} \times \min_{u\in[0,2\sqrt{q(1-q)}]} \left(\frac{2q-1}{\sqrt{(1-u^2)}} + \frac{1}{(1+u)}\right). \tag{12}$$

A detailed proof is given in Appendix C. One can always let every ε^r be $\max\{\varepsilon^r\}_{r=0}^7$ and denote it as ε. Then, one has $q = G(\varepsilon)$, which can be obtained with the numerical method of the SDP problem. The relation between the quality of the unknown real measurement and the noise $\varepsilon = \max\{\varepsilon^r\}_{r=0}^7$ is shown in Fig. 5. Along with the numerical results, we have shown the robust self-testing scheme for the three-qubit GSM in Theorem 2, where the noise tolerance can be up to 0.28%. Although the noise tolerance is not satisfactory, Theorem 2 demonstrates that the self-testing scheme of the three-qubit GSM is robust.

In fact, from the definition of the quality $\mathcal{Q}(\mathcal{R},\mathcal{P})$, the maximization in right hand side of Eq. (11) should go through all possible unital CPTP maps Λ_{R_1}, Λ_{R_2}, and Λ_{R_3} and then choose the maximal value. However, our result is currently based on the Choi map, which is only one choice of these CPTP maps. Thus, we do not acquire the optimal robustness bound. Additionally, the improvement of robustness under the Choi map is difficult, as the relaxation of some inequalities shown in Appendix C is not tight. Therefore, a better robustness can be expected if one optimizes these questions. Moreover, the above procedure for robust self-testing for a three-qubit GSM can be directly generalized to an arbitrary multipartite GSM. However, the maximal noise tolerance will decrease quickly as the number of N increases.

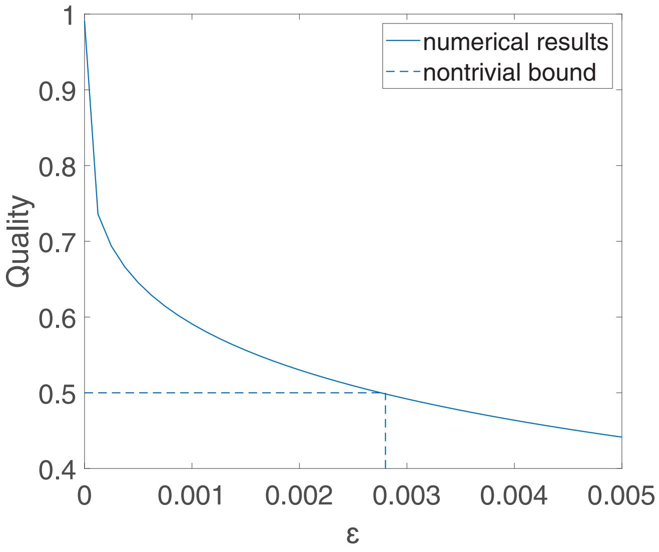

FIG. 5. The lower bound on the quality of the unknown real measurement is numerically estimated as a function of the weight of white noise ε. When the weight of white noise $\varepsilon \lesssim 0.28\%$ (i.e., the quality is above the nontrivial bound of 0.5), the presented procedure guarantees the unknown measurement is close to a three-qubit GHZ-state measurement.

V. CONCLUSION

In a quantum network, it is extremely vital to certify multipartite entangled measurements. Here, we have presented a self-testing method for the important class of generalized GHZ-state measurements. The procedure is operational for an arbitrary number of parties from an experimental point of views, which does not resort to N-partite Bell inequalities. One needs to check only whether the remaining two states maximally violate the tilted CHSH inequality after measuring the other $N-2$ parties. In addition, we have provided a proof for the robustness of the self-testing procedure with the help of the semidefinite program, where a noise tolerance up to 0.28% is observed. It is known that improving the robustness of the self-testing scheme to enable implementations of experiments with the current technique is an extremely challenging task, even in two-qubit states. For instance, the noise tolerance for self-testing a singlet in Ref. [6] is only on the level of 10^{-4}. Therefore, our result is enough to show that the self-testing scheme for the GHZ-state measurement is robust. For a quantum network connected by bipartite entangled states, one can always verify the entangled measurements in central nodes using our self-testing scheme. The results provide insightful understanding and pave the way to the construction of large-scale quantum networks.

For future works, it would be very beneficial to develop further practical methods to promote noise tolerance for self-testing multipartite entangled measurements and to drop the IID assumption, which would enable implementations of experiments on self-testing quantum networks in a device-independent manner. It is expected that our approach can also be straightforwardly extended to high-dimensional entangled measurements, like the self-testing method for high-dimensional entangled states [27].

ACKNOWLEDGMENTS

We sincerely thank Xin-Hui Li for insightful discussions about the technology of semidefinite programs. This work has been supported by the National Natural Science Foundation of China (Grants No. 62031024, No. 11874346, No. 12174375, and No. 12005091), the National Key R&D Program of China (Grant No. 2019YFA0308700), the Anhui Initiative in Quantum Information Technologies (Grant No. AHY060200), and the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0301100).

APPENDIX A: PROOF OF THEOREM 1

As shown in Theorem 1, if the observed correlations conditioned on the outcome of Roy's measurement satisfy the relations in Lemma 2, the measurement performed by Roy is a generalized GHZ-state measurement. Now, let us present a detailed proof of it.

Proof. Let p_r be the probability of Roy observing the outcome r and $\tau^r_{A_1A_2\cdots A_N} = |\psi^r\rangle_{A_1A_2\cdots A_N}\langle\psi^r|$ be the state shared among $A_1\cdots A_N$ conditioned on the outcome $r \in \{0,\dots,2^N-1\}$, i.e., $p_r\tau^r_{A_1\cdots A_N} = \mathrm{Tr}_{R_1R_2\cdots R_N}[(I_{A_1A_2\cdots A_N} \otimes R^r_{R_1R_2\cdots R_N})(\otimes^N_{i=1}\tau_{A_iR_i})]$. One can always choose $p_r = \frac{1}{2^N}$. From the definition of the SWAP gate in Fig. 3, one can construct SWAP channels as

$$\Gamma_f(|\xi\rangle_f\langle\xi|) = \mathrm{Tr}_{\mathcal{H}_f}(S_{X_f,Z_f}|0\rangle\langle 0| \otimes |\xi\rangle_f\langle\xi|S^\dagger_{X_f,Z_f}),$$

where $f \in \{A_1, A_2, \dots A_N\}$. Define

$$\begin{aligned}\sigma_{A_i'R_i} &\equiv \Gamma_{A_i}(\tau_{A_iR_i}),\, i \in \{1,2,\dots,N\},\\ \sigma^r_{A_1'A_2'\cdots A_N'} &\equiv \left(\otimes^N_{i=1}\Gamma_{A_i}\right)\left(\tau^r_{A_1A_2\cdots A_N}\right)\\ &= \left(\frac{1}{p_r}\right)\mathrm{Tr}_{R_1R_2\cdots R_N}\left[R^r_{R_1R_2\cdots R_N}\left(\otimes^N_{i=1}\sigma_{A_i'R_i}\right)\right]\\ &= (2^N)\mathrm{Tr}_{R_1R_2\cdots R_N}\left[R^r_{R_1R_2\cdots R_N}(\otimes^N_{i=1}\sigma_{A_i'R_i})\right].\end{aligned}\tag{A1}$$

Then, one has

$$\begin{aligned}&(\Gamma_{A_1}\otimes\Gamma_{A_2}\otimes\cdots\otimes\Gamma_{A_N})\left(\tau^r_{A_1A_2\cdots A_N}\right)\\ &\quad= \mathrm{Tr}_{A_1A_2\cdots A_N}\left(S_{A_1A_2\cdots A_N}|0\rangle^{\otimes N}_{A_1'\cdots A_N'}\langle 0|^{\otimes N}\otimes\tau^r_{A_1A_2\cdots A_N}S^\dagger_{A_1A_2\cdots A_N}\right)\\ &\quad= \mathrm{Tr}_{A_1A_2\cdots A_N}(S_{A_1A_2\cdots A_N}|0\rangle^{\otimes N}_{A_1'\cdots A_N'}|\psi\rangle^r\langle 0|^{\otimes N}\langle\psi^r|S^\dagger_{A_1A_2\cdots A_N})\\ &\quad= \mathrm{Tr}_{A_1A_2\cdots A_N}\left(|\mathrm{junk}\rangle_{A_1A_2\cdots A_N}\langle\mathrm{junk}|\otimes|\mathrm{GHZ}^r_\theta\rangle\langle\mathrm{GHZ}^r_\theta|\right)\\ &\quad= |\mathrm{GHZ}^r_\theta\rangle\langle\mathrm{GHZ}^r_\theta|.\end{aligned}\tag{A2}$$

The third equality is from Lemma 2. From the definition of the state $\sigma^r_{A_1'A_2'\cdots A_N'}$, one has

$$\sigma^r_{A_1'A_2'\cdots A_N'} = \mathrm{GHZ}^r_\theta$$

for all $r \in \{0,1,\dots,2^N-1\}$. Let us first present the definition of the Choi-Jamiołkowski map [38]. If ρ_{AB} acts on $\mathcal{H}_A\otimes\mathcal{H}_B$, the Choi-Jamiołkowski map ($\Lambda_B : \mathcal{H}_B \to \mathcal{H}_A$) associated with it is defined by $\Lambda_B(\sigma_B) = \mathrm{Tr}_B[(I_A\otimes\sigma_B^T)\rho_{AB}]$ for all σ_B. Here, ρ_{AB} is the Choi state and can be un-normalized. Now, let $\Lambda_{R_i} : \mathcal{L}(\mathcal{H}_{R_i}) \to \mathcal{L}(\mathcal{H}_{A_i'})$ be the Choi-Jamiołkowski maps associated with the operators $2\sigma_{A_i'R_i}, i \in \{1,2,\dots,N\}$. By decomposing the operator $R^r_{R_1R_2\cdots R_N}$ as $R^r_{R_1R_2\cdots R_N} = \Sigma_l\bigotimes_k\omega^r_{k,l}$, where $\omega^r_{k,l}$ is the operator of $\mathcal{H}_{R_k}$, one has $\Lambda_{R_1}\otimes\Lambda_{R_2}\otimes\cdots\otimes\Lambda_{R_N}(R^r_{R_1R_2\cdots R_N}) = (2^N)\mathrm{Tr}_{R_1R_2\cdots R_N}[R^r_{R_1R_2\cdots R_N}(\otimes^N_{i=1}\sigma_{A_i'R_i})] = \sigma^r_{A_1'A_2'\cdots A_N'} = \mathrm{GHZ}^r_\theta$. Moreover, we will prove that these Choi maps $\Lambda_{R_i}, i \in \{1,2,\dots,N\}$, are unital maps. Let us first consider Λ_{R_1}, with the other cases being similar. By the definition of the Choi-Jamiołkowski map, one has

$$\begin{aligned}\Lambda_{R_1}(I_{R_1}) &= \mathrm{Tr}_{R_1}(2\sigma_{A_1'R_1})\\ &= 2\mathrm{Tr}_{R_1R_2\cdots R_NA_2'\cdots A_N'}\left(\otimes^N_{i=1}\sigma_{A_i'R_i}\right)\\ &= 2\Sigma^{2^N-1}_{r=0}\mathrm{Tr}_{R_1R_2\cdots R_NA_2'\cdots A_N'}\left[R^r_{R_1R_2R_3}\left(\otimes^N_{i=1}\sigma_{A_i'R_i}\right)\right]\\ &= \frac{1}{2^{N-1}}\Sigma^{2^N-1}_{r=0}\mathrm{Tr}_{A_2'\cdots A_N'}\left(\sigma^r_{A_1'A_2'\cdots A_N'}\right) = I_{A_1'},\end{aligned}$$

where we have used the fact that $\Sigma^{2^N-1}_{r=0}R^r_{R_1R_2\cdots R_N} = I$ and $\sigma^r_{A_1'A_2'\cdots A_N'} = \mathrm{GHZ}^r_\theta$.

Therefore, we have proven that the joint measurement performed by central node Roy is actually a generalized GHZ-state measurement under the conditions in Lemma 2. It should be noted that the proof of Lemma 1 still holds if one replaces $|\psi\rangle$ with a general ρ [27]. Thus, the proof of our Theorem 1 can also be repeated by starting from a general $\tau^r_{A_1A_2\cdots A_N}$.

APPENDIX B: THE DETAILED FORM OF $\widetilde{W^\alpha_{\vec{a}}}^r$ IN LEMMA 2

In Lemma 2, a new form of self-testing statement was presented. The notation $\widetilde{\cdot}^r$ in $\widetilde{O}^r$ means that local unitary transformations are performed on the observable O. Here, we will provide the details for $\widetilde{W^\alpha_{\vec{a}}}^r$, where $\vec{a} = a_1\cdots a_{N-2}$. For convenience, let $N = 3$. Rewrite A_1, A_2, and A_3 as A, B, and C, and let $A_{i,1} = A_i$, $A_{i,2} = B_i$, and $A_{i,3} = C_i$, $i \in \{0,1\}$. Now, $\vec{a}$ is a_1 and rewritten as $a \in \{0,1\}$. W^α_0 and W^α_1 can been obtained from Lemma 2 as $W^\alpha_0 = \alpha B_0\otimes I + B_0C_0 + B_0C_1 + B_1C_0 - B_1C_1$ and $W^\alpha_1 = \alpha B_0\otimes I + B_0C_0 + B_0C_1 - B_1C_0 + B_1C_1$. First, by adding a superscript in the formulas for W^α_0 and W^α_1, one has $W'^\alpha_0 = \alpha B_0' + W_0'$ and $W'^\alpha_1 = \alpha B_0' + W_1'$, where $W_0' = B_0'C_0' + B_0'C_1' + B_1'C_0' - B_1'C_1'$ and $W_1' = B_0'C_0' + B_0'C_1' - B_1'C_0' + B_1'C_1'$. From Lemma 1, one knows that $B_0' = Z', B_1' = X'$, $C_0' = \cos\mu Z' + \sin\mu X'$, and $C_1' = \cos\mu Z' - \sin\mu X'$, with $\tan\mu = \sin 2\theta$. The local unitary transformation performed on W'^α_a is $U'^r = U'^r_{A'}\otimes U'^r_{B'C'}$. As U'^r is the local unitary transformation between generalized GHZ states, one can always choose $U'^r_{B'C'} \in \{X'\otimes X', I'\otimes X', X'\otimes I', I'\otimes I'\}$. For the $r = 7$ case, one has $X'Z'\otimes X'\otimes X'|\mathrm{GHZ}^7_\theta\rangle = |\mathrm{GHZ}^0_\theta\rangle$, where $|\mathrm{GHZ}_\theta^7\rangle = \sin\theta|000\rangle - \cos\theta|111\rangle$ and $|\mathrm{GHZ}_\theta^0\rangle = \cos\theta|000\rangle + \sin\theta|111\rangle$. Here, $U'^7 = X'Z' \otimes X' \otimes X'$. Thus, $\widetilde{W_0'^{\alpha}}^{7} = U'^{7\dagger} W_0'^{\alpha} U'^7 = -\alpha B_0' + W_0'$ and $\widetilde{W_1'^{\alpha}}^{7} = U'^{7\dagger} W_1'^{\alpha} U'^7 = -\alpha B_0' + W_1'$. After calculating $\widetilde{W_a'^{\alpha}}^{r}$ for all $r \in \{0, 1, \dots, 7\}$ and $a \in \{0, 1\}$, the detailed formulas for $\widetilde{W_a'^{\alpha}}^{r}$ can be obtained. By replacing the symbols I', B_i', and C_i', $i \in \{0, 1\}$, in $\widetilde{W_a'^{\alpha}}^{r}$ with I, B_i, and C_i, $i \in \{0, 1\}$, one can obtain the detailed form of $\widetilde{W_a^{\alpha}}^{r}$.

In short, $\widetilde{W_{\vec{a}}^{\alpha}}^{r}$ is acquired by deleting the superscript prime of $\widetilde{W_{\vec{a}}'^{\alpha}}^{r}$. $\widetilde{W_{\vec{a}}'^{\alpha}}^{r}$ is obtained by performing local unitary transformations on $W_{\vec{a}}'^{\alpha}$. The local unitary transformation depends on the transformation between states $|\mathrm{GHZ}_\theta^r\rangle$ and $|\mathrm{GHZ}_\theta^0\rangle$. Therefore, one can easily write the detailed form of $\widetilde{W_{\vec{a}}^{\alpha}}^{r}$ in Lemma 2.

APPENDIX C: PROOF OF THEOREM 2

In this Appendix, we give a proof of Theorem 2 that shows the robust self-testing of the three-qubit GHZ-state measurement. If the observed correlations cannot perfectly satisfy the conditions in Lemma 2, one cannot adopt the ideal self-testing method presented in Theorem 1 directly. We should bound the quality of the unknown measurement under the certain white noise, i.e., study how close the unknown measurement performed by Roy is to the ideal three-qubit GHZ-state measurement. Before presenting the proof of Theorem 2, we first generalize the result of the semidefinite program in the main text as the following lemma.

Lemma 3. Let A_0, A_1, B_0, B_1, C_0, and C_1 be the pairs of observables for the three parties. If the correlations in Lemma 2 with error ε^r ($\theta = \pi/4$, $\alpha = 0$) satisfy the relations

$$\langle\psi|\widetilde{P_{A_0}^{0}}^{r}|\psi\rangle = \langle\psi|\widetilde{P_{B_0}^{0}}^{r}|\psi\rangle = \tfrac{1}{2}, \tag{C1}$$

$$\langle\psi|\widetilde{P_{A_0}^{0}}^{r}\widetilde{P_{B_0}^{0}}^{r}|\psi\rangle = \frac{(1-\varepsilon^r)}{2} + \frac{\varepsilon^r}{4}, \tag{C2}$$

$$\langle\psi|\widetilde{P_{A_1}^{\vec{a}}}^{r}|\psi\rangle = \tfrac{1}{2}, \quad a \in \{0, 1\}, \tag{C3}$$

$$\langle\psi|\widetilde{P_{A_1}^{\vec{a}}}^{r}\widetilde{W_a^{\alpha}}^{r}|\psi\rangle = \sqrt{2}(1-\varepsilon^r), \quad a \in \{0, 1\}, \tag{C4}$$

then there exist fixed CPTP maps Γ_A, Γ_B, and Γ_C as shown in Appendix A such that

$$F\big((\Gamma_A \otimes \Gamma_B \otimes \Gamma_C)(\tau_{ABC}^r), \mathrm{GHZ}_{A'B'C'}^r\big) \geqslant G(\varepsilon^r)$$

for all $r \in \{0, 1, \dots, 7\}$. The function $G(x)$ is defined in the main text as a function of the lower bound of the fidelity and white noise ε^r. It is a numerical solution from the SDP.

Proof. For $r = 0$, we gave the detailed process of the SDP to derive this result in Sec. IV. The CPTP maps are fixed for all $r \in \{0, 1, \dots, 7\}$. For different r, the observables in the above correlations are all equivalent to the $r = 0$ case, up to local unitary transformations. Thus, the lower bounds of the fidelity for different r have the same form; that is, they have the same function $G(x)$.

Now, we start to prove Theorem 2 for finding the lower bound on the quality of the unknown real measurement $\{R_{R_1R_2R_3}^r\}_{r=0}^7$. As $\mathrm{GHZ}_{A'B'C'}^r$ are pure states, from Eq. (A1), one has

$$\begin{aligned} p_r F\big((\Gamma_A \otimes \Gamma_B \otimes \Gamma_C)(\tau_{ABC}^r), \mathrm{GHZ}_{A'B'C'}^r\big) &= p_r\langle(\Gamma_A \otimes \Gamma_B \otimes \Gamma_C)(\tau_{ABC}^r), \mathrm{GHZ}_{A'B'C'}^r\rangle \\ &= \big\langle\sigma_{A'R_1} \otimes \sigma_{B'R_2} \otimes \sigma_{C'R_3}, \mathrm{GHZ}_{A'B'C'}^r \otimes R_{R_1R_2R_3}^r\big\rangle. \end{aligned}$$

From Lemma 3, we have

$$\big\langle\sigma_{A'R_1} \otimes \sigma_{B'R_2} \otimes \sigma_{C'R_3}, \mathrm{GHZ}_{A'B'C'}^r \otimes R_{R_1R_2R_3}^r\big\rangle \geqslant p_r G(\varepsilon^r). \tag{C5}$$

To derive the main result, one should construct unital CPTP maps $\Lambda_{R_1} : \mathcal{L}(\mathcal{H}_{R_1}) \to \mathcal{L}(\mathcal{H}_{A'})$, $\Lambda_{R_2} : \mathcal{L}(\mathcal{H}_{R_2}) \to \mathcal{L}(\mathcal{H}_{B'})$, and $\Lambda_{R_3} : \mathcal{L}(\mathcal{H}_{R_3}) \to \mathcal{L}(\mathcal{H}_{C'})$ and then find the lower bound on $\langle\Lambda_{R_1} \otimes \Lambda_{R_2} \otimes \Lambda_{R_3}(R_{R_1R_2R_3}^r), \mathrm{GHZ}_{A'B'C'}^r\rangle$. Let $\lambda_{A'R_1}$, $\lambda_{B'R_2}$, and $\lambda_{C'R_3}$ be the Choi states of the maps Λ_{R_1}, Λ_{R_2}, and Λ_{R_3}. One has

$$\begin{aligned} \big\langle\Lambda_{R_1} \otimes \Lambda_{R_2} \otimes \Lambda_{R_3}\big(R_{R_1R_2R_3}^r\big), \mathrm{GHZ}_{A'B'C'}^r\big\rangle &= \langle\mathrm{Tr}_{R_1R_2R_3}\big\{(\lambda_{A'R_1} \otimes \lambda_{B'R_2} \otimes \lambda_{C'R_3})\big[I_{A'B'C'} \\ &\quad \otimes \big(R_{R_1R_2R_3}^r\big)^T\big]\big\}, \mathrm{GHZ}_{A'B'C'}^r\rangle \\ &= \big\langle\lambda_{A'R_1} \otimes \lambda_{B'R_2} \otimes \lambda_{C'R_3}, \mathrm{GHZ}_{A'B'C'}^r \otimes \big(R_{R_1R_2R_3}^r\big)^T\big\rangle \\ &= \big\langle\lambda_{A'R_1}^T \otimes \lambda_{B'R_2}^T \otimes \lambda_{C'R_3}^T, \mathrm{GHZ}_{A'B'C'}^r \otimes R_{R_1R_2R_3}^r\big\rangle. \end{aligned} \tag{C6}$$

To utilize the relation in Eq. (C5) in the above equation, the Choi states should be constructed by $\sigma_{A'R_1}$, $\sigma_{B'R_2}$, and $\sigma_{C'R_3}$, respectively. One can bound the marginals $\sigma_{A'}$, $\sigma_{B'}$, and $\sigma_{C'}$ to guarantee the marginals of the constructed Choi states are proportional to I. From Eq. (A1), we have

$$\begin{aligned} F\big((\Gamma_A \otimes \Gamma_B \otimes \Gamma_C)(\tau_{ABC}^r), \mathrm{GHZ}_{A'B'C'}^r\big) &= F\big(\sigma_{A'B'C'}^r, \mathrm{GHZ}_{A'B'C'}^r\big) \\ &= \big\langle\sigma_{A'B'C'}^r, \mathrm{GHZ}_{A'B'C'}^r\big\rangle \\ &\geqslant G(\varepsilon^r). \end{aligned}$$

Here, we adopt the definition in the main text regarding the notation $\widetilde{\{\cdots\}}^{r}$ and define

$$\begin{aligned} \sigma_{A'B'C'}' &= \sum_{r=0}^{7} p_r\big(\widetilde{\sigma_{A'B'C'}^r}^{r}\big)^\dagger \\ &= \sum_{r=0}^{7} p_r\big(U_{A'}'^r \otimes U_{B'}'^r \otimes U_{C'}'^r\big)\sigma_{A'B'C'}^r\big(U_{A'}'^r \otimes U_{B'}'^r \otimes U_{C'}'^r\big)^\dagger. \end{aligned}$$

By calculation, one has

$$\begin{aligned} F\big(\sigma_{A'B'C'}', GHZ_{A'B'C'}^0\big) &= \big\langle\sigma_{A'B'C'}', \mathrm{GHZ}_{A'B'C'}^0\big\rangle \\ &= \sum_{r=0}^{7} p_r\big\langle\sigma_{A'B'C'}^r, \mathrm{GHZ}_{A'B'C'}^r\big\rangle \\ &\geqslant \sum_{r=0}^{7} p_r G(\varepsilon^r) = q. \end{aligned} \tag{C7}$$

Furthermore, the spectrum of $\sigma_{A'}$ is the same as $\sigma'_{A'}$ because

$$\begin{aligned}\sigma_{A'} &= \mathrm{Tr}_{R_1}\sigma_{A'R_1} = \mathrm{Tr}_{B'C'R_1R_2R_3}(\sigma_{A'R_1}\otimes\sigma_{B'R_2}\otimes\sigma_{C'R_3})\\ &= \Sigma_r \mathrm{Tr}_{B'C'R_1R_2R_3}\big[R^r_{R_1R_2R_3}(\sigma_{A'R_1}\otimes\sigma_{B'R_2}\otimes\sigma_{C'R_3})\big]\\ &= \Sigma_r p_r \mathrm{Tr}_{B'C'}\sigma^r_{A'B'C'} = \Sigma_r p_r \sigma^r_{A'} = \sigma'_{A'},\end{aligned}$$

where we use $\Sigma_{r=0}^{2^N-1}R^r_{R_1R_2R_3} = I$. Next, we will bound the spectrum of $\sigma'_{A'}$. One can always find a pure state $\sigma'_{A'B'C'}$ to achieve the upper and lower bounds. Without loss of generality, let $\sigma'_{A'B'C'} = \alpha|000\rangle + \beta|111\rangle$. From inequality (C7), $0.5 < q \leqslant 1$, and $\alpha^2+\beta^2=1$, one has $\frac{1-2\sqrt{q(1-q)}}{2} \leqslant \alpha^2 \leqslant \frac{1+2\sqrt{q(1-q)}}{2}$. Thus, $\mathrm{spectrum}(\sigma_{A'}) = \mathrm{spectrum}(\sigma'_{A'}) \in [\frac{1-2\sqrt{q(1-q)}}{2}, \frac{1+2\sqrt{q(1-q)}}{2}]$. One can write the spectrum of $\sigma_{A'}$ as

$$\mathrm{spectrum}(\sigma_{A'}) = \left\{\frac{1-\eta_{A'}}{2}, \frac{1+\eta_{A'}}{2}\right\},$$

where $0 \leqslant \eta_{A'} \leqslant 2\sqrt{q(1-q)} < 1$. The same bounds on $\eta_{B'}$ and $\eta_{C'}$ will be obtained in a similar way as

$$\mathrm{spectrum}(\sigma_{B'}) = \left\{\frac{1-\eta_{B'}}{2}, \frac{1+\eta_{B'}}{2}\right\}$$

and

$$\mathrm{spectrum}(\sigma_{C'}) = \left\{\frac{1-\eta_{C'}}{2}, \frac{1+\eta_{C'}}{2}\right\}.$$

Now, the detailed forms of the Choi states are

$$\begin{aligned}\lambda^T_{A'R_1} &= \big(\sigma_{A'}^{-1/2}\otimes I\big)\sigma_{A'R_1}\big(\sigma_{A'}^{-1/2}\otimes I\big),\\ \lambda^T_{B'R_2} &= \frac{2}{1+\eta_{B'}}\sigma_{B'R_2} + \sigma_{R_2}\otimes\left(I - \frac{2}{1+\eta_{B'}}\sigma_{B'}\right),\\ \lambda^T_{C'R_3} &= \frac{2}{1+\eta_{C'}}\sigma_{C'R_3} + \sigma_{R_3}\otimes\left(I - \frac{2}{1+\eta_{C'}}\sigma_{C'}\right),\end{aligned} \tag{C8}$$

where $\sigma_{A'} = \mathrm{Tr}_{R_1}\sigma_{A'R_1}$, $\sigma_{B'} = \mathrm{Tr}_{R_2}\sigma_{B'R_2}$, $\sigma_{C'} = \mathrm{Tr}_{R_3}\sigma_{C'R_3}$, $\sigma_{R_2} = \mathrm{Tr}_{B'}\sigma_{B'R_2}$, and $\sigma_{R_3} = \mathrm{Tr}_{C'}\sigma_{C'R_3}$. As $\mathrm{spectrum}(\sigma_{B'}) = \{\frac{1-\eta_{B'}}{2}, \frac{1+\eta_{B'}}{2}\}$ and $\mathrm{spectrum}(\sigma_{C'}) = \{\frac{1-\eta_{C'}}{2}, \frac{1+\eta_{C'}}{2}\}$ are bounded by $0 \leqslant \eta_{B'} \leqslant 2\sqrt{q(1-q)}$ and $0 \leqslant \eta_{C'} \leqslant 2\sqrt{q(1-q)}$, $\sigma_{R_3}\otimes(I - \frac{2}{1+\eta_{C'}}\sigma_{C'})$ and $\sigma_{R_2}\otimes(I - \frac{2}{1+\eta_{B'}}\sigma_{B'})$ are positive semidefinite. Thus, one has

$$\lambda^T_{A'R_1}\otimes\lambda^T_{B'R_2}\otimes\lambda^T_{C'R_3} \geqslant \lambda^T_{A'R_1}\otimes\frac{2}{1+\eta_{B'}}\sigma_{B'R_2}\otimes\frac{2}{1+\eta_{C'}}\sigma_{C'R_3}.$$

From Lemma 3 in the Supplemental Material of Ref. [38], the inequality

$$\lambda^T_{A'R_1} \geqslant s(\eta_{A'})\sigma_{A'R_1} - t(\eta_{A'})\frac{I}{2}\otimes\sigma_{R_1} \tag{C9}$$

holds, where $s(x) = \frac{2}{\sqrt{1-x^2}}$, $t(x) = \frac{4}{\sqrt{1-x^2}} - \frac{4}{1+x}$, and $\sigma_{R_1} = Tr_{A'}\sigma_{A'R_1}$. Therefore, one has

$$\lambda^T_{A'R_1}\otimes\lambda^T_{B'R_2}\otimes\lambda^T_{C'R_3} \geqslant \left[s(\eta_{A'})\sigma_{A'R_1} - t(\eta_{A'})\frac{I}{2}\otimes\sigma_{R_1}\right]\otimes\frac{2}{1+\eta_{B'}}\sigma_{B'R_2}\otimes\frac{2}{1+\eta_{C'}}\sigma_{C'R_3}, \tag{C10}$$

where the inequality is from Eq. (C9) and positive semidefinite matrices $\frac{2}{1+\eta_{B'}}\sigma_{B'R_2}$ and $\frac{2}{1+\eta_{C'}}\sigma_{C'R_3}$. As

$$\begin{aligned}&\big\langle\sigma_{R_1}\otimes\sigma_{R_2}\otimes\sigma_{R_3}, R^r_{R_1R_2R_3}\big\rangle\\ &\quad= \mathrm{Tr}_{R_1R_2R_3}\big[(\sigma_{R_1}\otimes\sigma_{R_2}\otimes\sigma_{R_3})\cdot R^r_{R_1R_2R_3}\big]\\ &\quad= \mathrm{Tr}_{A'B'C'R_1R_2R_3}\big[(\sigma_{A'R_1}\otimes\sigma_{B'R_2}\otimes\sigma_{C'R_3})\cdot R^r_{R_1R_2R_3}\big]\\ &\quad= p_r\mathrm{Tr}_{A'B'C'}\sigma^r_{A'B'C'} = p_r,\end{aligned}$$

one has $\langle I\otimes\sigma_{R_1}\otimes I\otimes\sigma_{R_2}\otimes\sigma_{C'R_3}, \mathrm{GHZ}^r_{A'B'C'}\otimes R^r_{R_1R_2R_3}\rangle = \frac{1}{2}\langle\sigma_{R_1}\otimes\sigma_{R_2}\otimes\sigma_{R_3}, R^r_{R_1R_2R_3}\rangle = \frac{p_r}{2}$. Then, one arrives at

$$\begin{aligned}&\big\langle\lambda^T_{A'R_1}\otimes\lambda^T_{B'R_2}\otimes\lambda^T_{C'R_3}, \mathrm{GHZ}^r_{A'B'C'}\otimes R^r_{R_1R_2R_3}\big\rangle\\ &\quad\geqslant \frac{4s(\eta_{A'})p_rG(\varepsilon^r) - t(\eta_{A'})p_r}{(1+\eta_{B'})(1+\eta_{C'})}.\end{aligned}$$

The inequality is derived from the fact that the fidelity can only increase after tracing out the subsystem. Now, we can obtain

$$\begin{aligned}\mathcal{Q}(\mathcal{R},\mathcal{P}) &\geqslant \frac{1}{8}\sum_{r=0}^{7}\big\langle\lambda^T_{A'R_1}\otimes\lambda^T_{B'R_2}\\ &\quad\otimes\lambda^T_{C'R_3}, \mathrm{GHZ}^r_{A'B'C'}\otimes R^r_{R_1R_2R_3}\big\rangle\\ &\geqslant \frac{1}{8}\Big(\frac{4s(\eta_{A'})\sum_{r=0}^{7}p_rG(\varepsilon^r) - t(\eta_{A'})\sum_{r=0}^{7}p_r}{(1+\eta_{B'})(1+\eta_{C'})}\Big)\\ &= \frac{4s(\eta_{A'})q - t(\eta_{A'})}{8(1+\eta_{B'})(1+\eta_{C'})}.\end{aligned}$$

As $0.5 < q \leqslant 1$, the numerator is positive. Hence, one obtains the result

$$\begin{aligned}\mathcal{Q}(\mathcal{R},\mathcal{P}) &\geqslant \frac{1}{2(1+2\sqrt{q(1-q)})^2}\left(\frac{2q-1}{\sqrt{(1-\eta^2_{A'})}} + \frac{1}{(1+\eta_{A'})}\right)\\ &\geqslant \frac{1}{2[1+2\sqrt{q(1-q)}]^2}\\ &\quad\times\min_{u\in[0,2\sqrt{q(1-q)}]}\left(\frac{2q-1}{\sqrt{(1-u^2)}} + \frac{1}{(1+u)}\right).\end{aligned}$$

Here, we have presented a lower bound for the quality of the unknown joint measurement performed by Roy under certain white noise. The quality implies the ability of the unknown measurement to simulate the ideal three-qubit GHZ-state measurement. Thus, a robust self-testing statement for the three-qubit GHZ-state measurement has been shown.

[1] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).

[2] I. Šupić and J. Bowles, Quantum **4**, 337 (2020).

[3] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).

[4] T. H. Yang and M. Navascués, Phys. Rev. A **87**, 050102(R) (2013).

[5] A. Natarajan and T. Vidick, in *STOC 2017: Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing* (Association for Computing Machinery, New York, 2017), p. 1003.

[6] M. McKague, T. H. Yang, and V. Scarani, J. Phys. A **45**, 455304 (2012).

[7] C. Bamps and S. Pironio, Phys. Rev. A **91**, 052111 (2015).

[8] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, New J. Phys. **18**, 035013 (2016).

[9] I. Šupić, D. Cavalcanti, and J. Bowles, Quantum **5**, 418 (2021).

[10] S. Goswami, B. Bhattacharya, D. Das, S. Sasmal, C. Jebaratnam, and A. S. Majumdar, Phys. Rev. A **98**, 022311 (2018).

[11] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak, npj Quantum Inf. **7**, 151 (2021).

[12] K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L.-C. Kwek, Phys. Rev. Lett. **122**, 250403 (2019).

[13] X. Li, Y. Wang, Y. Han, S. Qin, F. Gao, and Q. Wen, IEEE J. Sel. Areas Commun. **38**, 589 (2020).

[14] A. Coladangelo, Phys. Rev. A **98**, 052115 (2018).

[15] T. Coopmans, J. Kaniewski, and C. Schaffner, Phys. Rev. A **99**, 052123 (2019).

[16] J. Kaniewski, Phys. Rev. A **95**, 062323 (2017).

[17] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Phys. Rev. A **98**, 062307 (2018).

[18] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, Phys. Rev. A **93**, 062121 (2016).

[19] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Phys. Rev. Lett. **113**, 040401 (2014).

[20] N. Miklin, J. J. Borkała, and M. Pawłowski, Phys. Rev. Res. **2**, 033014 (2020).

[21] C. Jebarathinam, J.-C. Hung, S.-L. Chen, and Y.-C. Liang, Phys. Rev. Res. **1**, 033073 (2019).

[22] N. Miklin and M. Oszmaniec, Quantum **5**, 424 (2021).

[23] K. Bharti, M. Ray, Z.-P. Xu, M. Hayashi, L.-C. Kwek, and A. Cabello, arXiv:2104.13035

[24] A. Coladangelo, K. T. Goh, and V. Scarani, Nat. Commun. **8**, 15485 (2017).

[25] X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, Phys. Rev. A **90**, 042339 (2014).

[26] M. McKague, in *Theory of Quantum Computation, Communication, and Cryptography* edited by D. Bacon, M. Martin-Delgado, and M. Roetteler (Springer Berlin Heidelberg, Berlin, Heidelberg, 2011), pp. 104–120.

[27] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, New J. Phys. **20**, 083041 (2018).

[28] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, Phys. Rev. Lett. **121**, 180505 (2018).

[29] M. McKague and M. Mosca, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by W. van Dam, V. M. Kendon, and S. Severini (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010), pp. 113–130.

[30] C. A. Miller and Y. Shi, J. Assoc. Comput. Mach. **63**, 1 (2016).

[31] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, Phys. Rev. Lett. **121**, 180503 (2018).

[32] F. Baccari, R. Augusiak, I. Šupić, and A. Acín, Phys. Rev. Lett. **125**, 260507 (2020).

[33] O. Makuta and R. Augusiak, New J. Phys. **23**, 043042 (2021).

[34] I. Frérot and A. Acín, Phys. Rev. Lett. **127**, 240401 (2021).

[35] A. Gheorghiu, P. Wallden, and E. Kashefi, New J. Phys. **19**, 023043 (2017).

[36] M. McKague, Theory Comput. **12**, 1 (2016).

[37] A. Gočanin, I. Šupić, and B. Dakić, PRX Quantum **3**, 010317 (2022).

[38] M. O. Renou, J. Kaniewski, and N. Brunner, Phys. Rev. Lett. **121**, 250507 (2018).

[39] J.-D. Bancal, N. Sangouard, and P. Sekatski, Phys. Rev. Lett. **121**, 250506 (2018).

[40] A. Acín, S. Massar, and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).

[41] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).

[42] M.-D. Choi, Linear Algebra Appl. **10**, 285 (1975).

[43] X. Li, Y. Cai, Y. Han, Q. Wen, and V. Scarani, Phys. Rev. A **98**, 052331 (2018).

[44] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, Phys. Rev. A **91**, 022115 (2015).

[45] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).

[46] M. Navascués, S. Pironio, and A. Acín, New J. Phys. **10**, 073013 (2008).