








**Measurement-device-independent verification of quantum states**Xin-Yu Xu <sup>1,2</sup> Yi-Zheng Zhen <sup>1,2</sup> Qing Zhou <sup>1,2</sup> Shu-Ming Hu <sup>1,2</sup> Jun-Hao Wei <sup>1,2</sup> Nuo-Ya Yang <sup>1,2</sup>  
Li Li<sup>1,2,3,\*</sup> Nai-Le Liu<sup>1,2,3,†</sup> and Kai Chen <sup>1,2,3,‡</sup><sup>1</sup>*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*<sup>2</sup>*CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*<sup>3</sup>*Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

(Received 18 August 2023; revised 29 March 2024; accepted 3 April 2024; published 6 May 2024)

Efficient and reliable verification of quantum states is central to quantum information processing applications. If using well-characterized measurement devices, effective methods have been developed for quantum state verification (QSV). In reality, however, measurement devices are generally imperfect or untrusted, which limits significantly the application of standard QSV protocols. Here, we propose the measurement-device-independent QSV (MDI-QSV) scheme for practice. With the help of trusted quantum inputs, we have developed a systematic approach to design MDI-QSV strategies for an arbitrary pure target state. We find that the number of required measurements has an optimal scaling with required accuracy and confidence level, similar to the standard QSV where trusted measurement devices are available. Our results offer a sample-efficient and realistic method for quantum state verification with virtues of a measurement-device-independent manner, and are within reach of current technology.

DOI: [10.1103/PhysRevA.109.052607](https://doi.org/10.1103/PhysRevA.109.052607)**I. INTRODUCTION**

Quantum states serve as an essential resource [1] for quantum information processing, including quantum communication [2–4], quantum sensing [5], quantum simulation [6], and quantum computation [7,8]. Certification and characterization of quantum states is thus a crucial prerequisite for realizing tailored quantum information processing applications. In a quantum certification task, different techniques have multifaceted complexity, depending on the information gained as well as the assumption made [9]. For example, tomographic reconstruction of a quantum state [10] is generally a time-consuming and computationally difficult task, while entanglement detection [11,12] sometimes consumes less resources [13], even with few copies required in some cases [14,15]. A comprehensive and good review on various quantum certification and benchmarking techniques is provided in detail in Ref. [16].

In many practical cases, one aims at gaining confidence that the device outputs a particular state within a certain accuracy, using as few experimental rounds as possible. This is, in fact, a quantum state verification (QSV) problem [17–19]. In recent years, QSV has received much interest, with various methods proposed by using advanced statistical methods and the framework of hypothesis testing [20,21]. To be feasible for a real-world verifier, a QSV strategy usually involves

only local measurements [19], and classical communication can also be adopted [22–24]. Efficient protocols have been designed for many typical states, such as the Greenberger-Horne-Zeilinger (GHZ) states, stabilizer states, and Dicke states [25–27]. Moreover, when it comes to an adversarial scenario where the states are not independently distributed, a general framework has been established to construct efficient verification protocols [28,29].

Nevertheless, most QSV protocols require that all measurement devices are perfectly characterized. In reality, however, the measurement devices can be imperfect due to noise, or even untrusted due to attacks from a potential adversary. The adoption of such malicious devices may mislead the verifier in QSV. This necessitates our idea of extension of QSV by enjoying benefits of measurement-device-independent (MDI) approaches [30]. In Ref. [31], a systematic device-independent QSV approach based on self-testing [32,33] is introduced. There are also investigations of QSV in an untrusted quantum network [34,35]. Meanwhile, in the MDI scenario, trusted quantum inputs have been shown to enhance the entanglement detection [36,37] or assist novel self-testing protocols [38]. These naturally raise the question of how to design the QSV strategy to verify a target state efficiently in the MDI scenario. However, in general, the formulation of QSV in the MDI scenario, despite its significance, is still missing.

In this article, we propose an MDI-QSV scheme for verifying an arbitrary pure target state using trusted quantum inputs, with the help of a semiquantum nonlocal game [39]. Moreover, we provide a general construction of MDI-QSV strategy. By investigating the sample efficiency of the strategies, it is

\*eidos@ustc.edu.cn

†nlliu@ustc.edu.cn

‡kaichen@ustc.edu.cn

observed that the number of required measurements scales optimally with the required confidence level and accuracy. As examples, we apply the case of maximally entangled states with prime local dimension as well as the multiqubit stabilizer states, demonstrating the versatile feasibility and scalability of the scheme.

## II. EXTENDING QSV TO THE MDI SCENARIO

In the MDI scenario, due to the untrusted measurements, the verifier is not able to verify whether a source generates exactly a target state; nevertheless, they can test whether the generated state  $\sigma$  is equivalent to a target state  $\rho_\psi = |\psi\rangle\langle\psi|$  up to some local isometry  $\Phi$  [40], i.e.,  $\rho_\psi = \Phi(\sigma)$ . Before providing the main result, we introduce the notion of *extractability* [41,42], which quantifies the closeness between two arbitrary quantum states up to a local-isometric transformation. The extractability of a target state  $\rho_\psi$  from a produced state  $\sigma$  is defined as

$$F_e(\sigma \rightarrow \rho_\psi) = \max_{\Phi} \text{Tr}[\rho_\psi \Phi(\sigma)], \quad (1)$$

where the maximum is taken over all local isometries  $\Phi$ .

Consider that a source generate quantum states  $\{\sigma_1, \sigma_2, \dots, \sigma_N\}$ , which are supposed to all be  $\rho_\psi$ . The verifiers first make two hypothesis, including the null hypothesis  $H_0 : F_e(\sigma_j \rightarrow \rho_\psi) \leq 1 - \varepsilon$  for all  $j$ , and the alternative hypothesis  $H_1 : \text{there exists local isometry } \Phi \text{ such that } \Phi(\sigma_j) = \rho_\psi \text{ for all } j$ . Then, they need to decide which is the case with worst-case failure probability  $\delta$ .

## III. MDI-QSV PROTOCOLS AND STRATEGIES

For all single-qudit pure states, the MDI-QSV is a trivial task, because they are local-isometrically equivalent to each other. The MDI-QSV becomes really nontrivial when the target state is bipartite or multipartite while the verifiers remain local. Here, we consider firstly the bipartite case. We demonstrate that MDI-QSV of any pure bipartite state is not only feasible, but also can be done efficiently. These results are naturally generalized to the multipartite case, which will be discussed later in Appendix B.

An MDI-QSV *protocol* in the bipartite case is processed as follows. Suppose that two remote verifiers, Alice and Bob, aim to verify whether a source distributes a bipartite state local-isometrically equivalent to the target state  $\rho_\psi$ . Before the test begins, Alice and Bob specify an input set  $\mathcal{J} = \{(p_i, \tau_i^{A'}, \omega_i^{B'})\}_i$ , where  $p_i$  is a probability satisfying  $\sum_i p_i = 1$  and  $\tau_i^{A'}, \omega_i^{B'}$  are Alice's and Bob's local trusted quantum states, respectively. At the  $j$ th round of the test (see Fig. 1), after receiving the distributed state  $\sigma_j^{AB}$ , Alice randomly picks  $i$  according to probability  $p_i$  and communicates  $i$  with Bob. They adopt local trusted sources to prepare  $\tau_i^{A'}$  and  $\omega_i^{B'}$  and consequently measure their local states jointly with untrusted measurement devices, which yield outcomes  $a$  and  $b$ , respectively. For each event associated with the tuple of input and output  $(a, b, i)$ , Alice and Bob further assign a binary-outcome payoff function  $f(a, b, i) \in \{0, 1\}$ , where 0 stands for "pass" and 1 stands for "fail." Finally, after all  $N$  rounds, Alice and Bob conclude whether the distributed state is local-

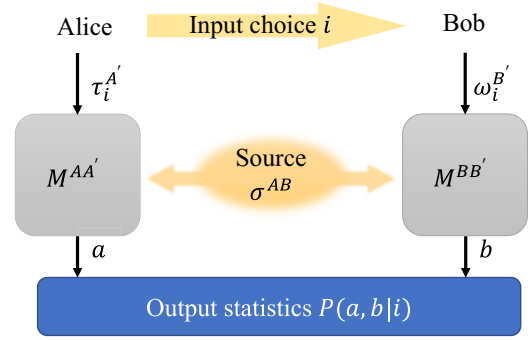


FIG. 1. An experimental round of the MDI-QSV. Alice and Bob perform untrusted joint measurements  $M^{AA'}, M^{BB'}$  on the distributed state  $\sigma^{AB}$  and trusted quantum inputs  $\tau_i^{A'}, \omega_i^{B'}$ .

isometrically equivalent to the target state according to the statistics of pass and fail events.

We denote  $\mathcal{S} = \{\mathcal{J}, f\}$  as the MDI-QSV *strategy*. Let  $P(a, b|i)$  be the probability of obtaining outcomes  $a, b$  given input  $i$ . Here, we further assume that the source generates quantum states identically and independently, i.e.,  $\sigma_j^{AB} = \sigma^{AB}$  for all  $j$ . Consequently, the probability that the strategy  $\mathcal{S}$  yields a fail outcome at an experimental round is

$$Q_{\mathcal{S}}(\sigma) = \sum_{a,b,i} p_i f(a, b, i) P(a, b|i). \quad (2)$$

Suppose that a state is at least  $\varepsilon$  far away from  $\rho_\psi$  up to local isometry. Then, the probability that this state leads to a pass outcome is upper bounded by  $1 - Q_{\mathcal{S}}^\varepsilon$ , where  $Q_{\mathcal{S}}^\varepsilon$  is determined by the optimization problem

$$Q_{\mathcal{S}}^\varepsilon = \min_{\sigma, M} Q_{\mathcal{S}}(\sigma), \quad \text{s.t. } F_e(\sigma \rightarrow \rho_\psi) \leq 1 - \varepsilon. \quad (3)$$

Meanwhile, any state that is local-isometrically equivalent to the target state has the highest probability  $1 - Q_{\mathcal{S}}^{\min}$  to pass the test if proper joint measurements are performed, with  $Q_{\mathcal{S}}^{\min} = \min_M Q_{\mathcal{S}}(\rho_\psi)$ , where the minimum is taken over arbitrary local measurements  $M$ .

By executing the strategy  $\mathcal{S}$ , the verifiers can perform MDI-QSV according to the following decision: After  $N$  rounds of the test, if the number of fail events does not exceed a certain threshold  $N_0$  ( $N_0 < N Q_{\mathcal{S}}^\varepsilon$ ), Alice and Bob conclude that the source distributes quantum states satisfying  $F_e(\sigma \rightarrow \rho_\psi) > 1 - \varepsilon$ , that is, reject  $H_0$ . To achieve a confidence level  $1 - \delta$  in this decision, the required number of measurements is

$$N \geq N_{\mathcal{S}}(\varepsilon, \delta) = \frac{1}{D[\frac{N_0}{N} \| Q_{\mathcal{S}}^\varepsilon]} \ln \delta^{-1}, \quad (4)$$

with  $D[x||y] = x \ln(x/y) + (1-x) \ln[(1-x)/(1-y)]$ . Equation (A11) gives the *sample efficiency* of  $\mathcal{S}$ . The proof follows directly from the Chernoff bound [43,44] (see Appendix A 2 for details).

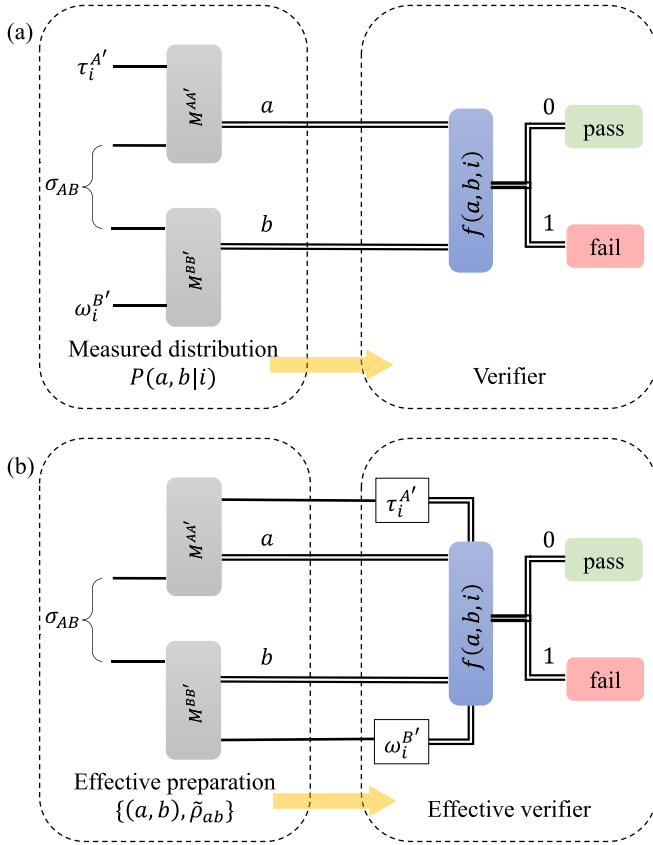


FIG. 2. The circuit representation of an MDI-QSV strategy (a) and an equivalent prepare-and-measure scenario (b). In the equivalent process, the uncharacterized state and measurement are grouped into an effective source sending conditional states  $\{(a, b), \tilde{\rho}_{ab}\}$ , while the trusted quantum input serves as an effective measurement for verifying these conditional states.

#### IV. MDI-QSV STRATEGIES AND THE SAMPLE EFFICIENCY

Particularly, if the target state can pass the test with certainty in an MDI-QSV strategy  $\mathcal{S}$ , i.e.,  $Q_{\mathcal{S}}^{\min} = 0$ , then the threshold  $N_0$  can be taken as zero, such that Alice and Bob can terminate the verification as long as a single fail event is observed, and conclude that the distributed state is not the target state. We call  $\mathcal{S}$  an *no-false-negative* (NFN) MDI-QSV strategy, because the distributed state can never pass the test with certainty if it is not equivalent to the target state up to local isometry. From Eq. (A11), it can be seen that the sample efficiency of the NFN MDI-QSV strategy  $N_{\mathcal{S}}(\varepsilon, \delta)$  scales optimally with  $\varepsilon$  as  $N_{\mathcal{S}}(\varepsilon, \delta) \approx (Q_{\mathcal{S}}^{\varepsilon})^{-1} \ln \delta^{-1}$ . Therefore, the NFN strategy is actually favorable to the verifiers.

An intuitive construction of MDI-QSV strategies exists by considering an equivalent virtual prepare-and-measure process. Without loss of generality, the target state is imposed to be a pure state  $|\psi^{AB}\rangle$  with  $d \times d$  dimension. As shown in Fig. 2, in the effective process, all the uncharacterized devices are grouped into an effective source, which outputs the conditional states  $\{\tilde{\rho}_{ab} = \mathcal{E}_a^{A \rightarrow A'} \otimes \mathcal{E}_b^{B \rightarrow B'}(\sigma_{AB})\}_{a,b=0}^{d^2-1}$ , with  $\mathcal{E}_a^{A \rightarrow A'}(\rho^A) = \text{Tr}_A[(\rho^A \otimes \mathbb{1}^{A'})M_a^{AA'}]$  and  $\mathcal{E}_b^{B \rightarrow B'}(\rho^B) = \text{Tr}_B[(\rho^B \otimes \mathbb{1}^{B'})M_b^{BB'}]$ . Meanwhile, the trusted quantum inputs

can serve as effective measurements controlled by the function  $f(a, b, i)$ . Then, the failure probability in Eq. (2) is reformulated as  $Q_{\mathcal{S}} = \sum_{ab} \text{Tr}(\tilde{\rho}_{ab}\tilde{\Omega}_{ab})$ , where

$$\tilde{\Omega}_{ab} = \sum_i p_i f(a, b, i) \tau_i^{A'} \otimes \omega_i^{B'}. \quad (5)$$

This leads to a natural idea in designing MDI-QSV strategies, that is, transferring the MDI-QSV of the state  $\sigma$  into the standard QSV of states  $\tilde{\rho}_{ab}$  with a set of effective strategies  $\tilde{\Omega}_{ab}$ , in which the quantum input serves as trusted local measurements.

With this idea, we propose a general construction of NFN MDI-QSV strategies. Denote  $\{U_{a(b)}\}_{a(b)=0}^{d^2-1}$  as the set of Heisenberg-Weyl operators [45], and  $\rho_{ab} = (U_a \otimes U_b)(\rho_{\psi}^{AB})^T(U_a \otimes U_b)^\dagger$ .

*Proposition 1.* For any target state  $|\psi^{AB}\rangle$  with  $d \times d$  dimension, one can construct an NFN MDI-QSV strategy  $\mathcal{S}_{\psi}^D = \{J_{\psi}, f_{J_{\psi}}\}$ , where

$$J_{\psi} = \left\{ \left( \frac{c_j}{d^4}, U_a \phi_j^{A'} U_a^\dagger \otimes U_b \phi_j^{B'} U_b^\dagger \right) \right\}_{a,b,j} := \{(p_i, \tau_i^{A'} \otimes \omega_i^{B'})\}, \quad (6)$$

and

$$f_{J_{\psi}}(a, b, i) = \begin{cases} 1, & \text{if } \text{Tr}[(\tau_i \otimes \omega_i)\rho_{ab}] = 0, \\ 0, & \text{otherwise.} \end{cases} \quad (7)$$

Here, the  $\{(c_j, \phi_j^{A'}, \phi_j^{B'})\}$  satisfies  $\sum_j c_j \phi_j^{A'} \otimes \phi_j^{B'} = [\mathbb{1}_{d^2} - (\rho_{\psi}^{AB})^T]/(d^2 - 1)$ .

For the proof of this proposition and a detailed discussion on the construction of MDI-QSV strategies, please refer to Appendix A.

Proposition 1 shows clearly that every pure bipartite state can be verified in an MDI manner. Nevertheless, one may note that the NFN strategy from Proposition 1 is not unique with respect to a fixed target state, due to the fact that the decomposition of  $[\mathbb{1}_{d^2} - (\rho_{\psi}^{AB})^T]/(d^2 - 1)$  into separable states is not unique. Different decompositions lead to different MDI-QSV strategies. Although the sample efficiency of these strategies always scales as  $O(\varepsilon^{-1} \ln \delta^{-1})$ , the prefactors can be quite different from each other with different sample efficiency. This is characterized explicitly in the following proposition:

*Proposition 2.* To achieve a confidence level  $1 - \delta$  in deciding whether  $F_e(\sigma \rightarrow \rho_{\psi}) \leq 1 - \varepsilon$  using the strategy  $\mathcal{S}_{\psi}^D$ , the required number of measurements is

$$N \geq N_{\mathcal{S}_{\psi}^D}(\varepsilon, \delta) = \frac{\ln \delta^{-1}}{\ln(1 - d^2 \bar{q} \varepsilon)^{-1}} \approx \frac{1}{d^2 \bar{q} \varepsilon} \ln \delta^{-1}. \quad (8)$$

Here, the  $\bar{q}$  is the minimum nonzero eigenvalue of  $\tilde{\Omega}_{00}$  defined in Eq. (5), bounded by

$$\frac{c}{d^4(d^2 - 1)} \leq \bar{q} \leq \frac{1}{d^4(d^2 - 1)} \sum_{a,b,i} p_i f_{J_{\psi}}(a, b, i) \leq \frac{1}{d(d+1)}, \quad (9)$$

with  $c = d^2$  if  $|\psi^{AB}\rangle$  is maximally entangled, and  $c = d$  otherwise.

A detailed proof is provided in Appendix A 5. In Appendix A 5, we have shown that  $Q_{\mathcal{S}_\psi^D}^\varepsilon = d^2 \bar{q} \varepsilon$  for the NFN strategy  $\mathcal{S}_\psi^D$ , and have derived the lower and upper bounds of the strategy-dependent parameter  $\bar{q}$ .

Here, three remarks are in order. Firstly, in practice, one can hardly expect to receive a pass at every round in experimental verification of quantum states [46–48], due to the imperfections in practical experiments. This prevents the verifiers from verifying exactly the target state. In this practical situation, one can instead verify whether the extractability of the distributed-to-target state exceeds some thresholds  $1 - \varepsilon_1$ . The verifiers can use the same strategy  $\mathcal{S}_\psi^D$ , but set the threshold  $N_0$  as  $N_0 = d^2 \bar{q} \varepsilon_1$ , rather than  $N_0 = 0$  [31], where  $\varepsilon_1$  depends on the magnitude of noise. Given the required confidence level  $1 - \delta$ , around  $N \geq (d^2 \bar{q} D[\varepsilon_1 \|\varepsilon])^{-1} \ln \delta^{-1} \approx (1 + \varepsilon_1/\varepsilon)(d^2 \bar{q} \varepsilon)^{-1} \ln \delta^{-1}$  measurements are required in the noisy case. Additionally, in Appendix A 8 b, we also discuss the modification of MDI-QSV when only partial Bell state measurements (BSMs) are available.

Secondly, for any fixed target state, by maximizing the factor  $\bar{q}$  over all possible decompositions of  $[\mathbb{1}_{d^2} - (\rho_\psi^{AB})^T]/(d^2 - 1)$ , one obtains an MDI-QSV strategy as efficiently as possible. Even with the worst choice among the possible MDI-QSV strategies constructed from Proposition 1, the required number of measurements is no more than  $d^2(d^2 - 1)c^{-1}\varepsilon^{-1} \ln \delta^{-1}$ , which achieves the same optimal scaling  $O(\varepsilon^{-1} \ln \delta^{-1})$  as the standard QSV, and is affordable in experiments.

Finally, it can be observed from Proposition 2 that at least  $(d + 1)/d\varepsilon^{-1} \ln \delta^{-1}$  experimental round is required in the MDI-QSV of any state. This lower bound is tight, and can be achieved by some strategy designed from Proposition 1. An example is the MDI-QSV of maximally entangle states with prime local dimension.

## V. APPLICATION 1: OPTIMAL MDI-QSV OF MAXIMALLY ENTANGLE STATES WITH PRIME LOCAL DIMENSION

For the maximally entangle states with prime local dimension, Proposition 1 can be employed to design an optimal MDI-QSV strategy, whose sample efficiency is  $N(\varepsilon, \delta) \approx (d + 1)/d\varepsilon^{-1} \ln \delta^{-1}$ . Here, the optimality is proved by showing that this strategy has the same sample efficiency as the optimal two-way adaptive QSV strategy [22] of the target state. The detailed construction and some further discussion on the optimality of the MDI-QSV strategy is provided in Appendix A. Taking the qubit case as an instance for illustration, the optimal MDI-QSV strategy of  $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$  is as follows: Alice and Bob first randomly choose a common Pauli basis  $X$ ,  $Y$ , or  $Z$ . Then, they randomly choose one eigenstate under this basis as their input, respectively. The resulting input set is shown in Table I. After performing the joint measurements on the input states and shared state, they calculate the payoff with the function specified by Eq. (7) to verify the shared state.

## VI. APPLICATION 2: MDI-QSV IN MULTIPARTITE CASE

So far we have formulated the MDI-QSV in the bipartite case. In Appendix B, a further extension of the above results

TABLE I. Input set to achieve optimal MDI-QSV strategy for Bell state  $|\phi^+\rangle$ . There are 12 possible input states which are selected randomly by the verifiers. Here,  $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$  and  $|\pm i\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$ . By applying BSMs to the input states and their share of the state  $\sigma^{AB}$ , respectively, Alice and Bob can accomplish the MDI-QSV of  $|\phi^+\rangle$  efficiently solely based on the output statistics.

Input state		Input probability
Alice	Bob	
$ 0\rangle/ 1\rangle$	$ 0\rangle/ 1\rangle$	1/12
$ +\rangle/ -\rangle$	$ +\rangle/ -\rangle$	1/12
$ +i\rangle/ -i\rangle$	$ +i\rangle/ -i\rangle$	1/12

into the multipartite case is provided. Particularly, the MDI-QSV for one of the most typical class of states, the  $n$ -qubit stabilizer states [49]  $|G_n\rangle$ , is introduced as an example. It is observed that the constructed MDI-QSV strategy only requires  $N_{\mathcal{S}_{\sigma_n}}(\varepsilon, \delta) \approx \frac{2^n - 1}{2^{n-1}} \varepsilon^{-1} \ln \delta^{-1}$  measurements in verifying the target state. For growing qubit number  $n$ , the number of required measurements is bounded from above by  $2\varepsilon^{-1} \ln \delta^{-1}$  independently on the system size. This implies that the stabilizer state can be verified efficiently in an MDI manner with the help of local quantum inputs, and requires at most twice as many measurements as the optimal strategy using trusted measurement devices.

An explicit example is the MDI-QSV of the three-qubit GHZ state  $|GHZ_3\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$ . The input set is selected according to Table II. At some round of the test, denote the input state as  $\tau_i^1 \otimes \tau_i^2 \otimes \tau_i^3$  and the measurement output as  $(a, b, c)$ . The payoff function  $f(a, b, c, i)$  is 1 if  $\text{Tr}[(\tau_i^1 \otimes \tau_i^2 \otimes \tau_i^3)(\sigma_a \otimes \sigma_b \otimes \sigma_c)]|GHZ_3\rangle\langle GHZ_3|(\sigma_a \otimes \sigma_b \otimes \sigma_c) = 0$ , and  $f(a, b, c, i) = 0$  otherwise. Here,  $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$  are the Pauli matrices. This achieves an efficient MDI-QSV strategy of the three-qubit GHZ state.

## VII. CONCLUSION

In summary, we have shown that any pure target state can be efficiently verified in an MDI manner. More explicitly, we have provided a systematic construction of no-false-negative MDI-QSV strategies for an arbitrary target state. It is demonstrated that the sample efficiency of MDI-QSV enjoys the same optimal scaling as the standard QSV. Compared with quantum state tomography, Bell test, or fidelity estimation

TABLE II. Input set of MDI-QSV strategy for three-qubit GHZ state.

Input state			Input probability
Alice	Bob	Charlie	
$ 0\rangle/ 1\rangle$	$ 0\rangle/ 1\rangle$	$ 0\rangle/ 1\rangle$	3/56
$ +\rangle/ -\rangle$	$ +\rangle/ -\rangle$	$ +\rangle/ -\rangle$	1/56
$ +i\rangle/ -i\rangle$	$ +i\rangle/ -i\rangle$	$ +\rangle/ -\rangle$	1/56
$ +i\rangle/ -i\rangle$	$ +\rangle/ -\rangle$	$ +i\rangle/ -i\rangle$	1/56
$ +\rangle/ -\rangle$	$ +i\rangle/ -i\rangle$	$ +i\rangle/ -i\rangle$	1/56



protocols, quadratically fewer total measurements are required in MDI-QSV to verify the target state within a given accuracy. As for the maximally entangled states with prime local dimension and the multiqubit stabilizer states, we show that the construction leads to optimal or nearly optimal MDI-QSV strategies. The sample-efficient character of MDI-QSV highlights its potential as a powerful tool for practical verification and validation of quantum devices. Additionally, for a practical case that the generated states may not be independent identically distributed, we remark that the MDI-QSV for nonindependent sources can still work by employing the techniques developed in Refs. [28,29].

With the development of quantum information technology and entering the noisy intermediate-scale quantum (NISQ) era, the reliable and efficient verification of quantum devices' functioning properly is becoming increasingly important. We anticipate that these results facilitate development of versatile relevant researches, such as entanglement detection, fidelity estimation [50,51], and quantum channel verification with low sample complexity in an MDI fashion. Additionally, such a pass or fail test is not sufficient to verify a mixed target state, while the experimentalists may also be targeting to produce a mixed state in certain tasks. It is interesting to consider the modification of MDI-QSV by combining the methods developed for quantum state discrimination when the target state is mixed.

### ACKNOWLEDGMENTS

This work has been supported by the National Natural Science Foundation of China (Grants No. 62375252, No. 62031024, No. 11874346, and No. 12174375), the National Key R&D Program of China (Grant No. 2019YFA0308700), the Anhui Initiative in Quantum Information Technologies (Grant No. AHY060200), the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0301100), the Anhui Provincial Natural Science Foundation (Grant No. 2308085MA26), and the Fundamental Research Funds for the Central Universities.

### APPENDIX A: MDI-QSV OF BIPARTITE STATE

In this section, we provide in detail the construction of the MDI-QSV strategy and its sample efficiency. By starting with an intuitive construction of MDI-QSV strategy, we show how the construction can be improved to obtain better or even optimal MDI-QSV strategies.

#### 1. An equivalent process

To start with, we briefly recall the MDI-QSV scenario in the bipartite case, where two remote parties, Alice and Bob, aim to verify whether the distributed states are the target state  $|\psi^{AB}\rangle$  without imposing trust on their measurement devices. Without loss of generality, the target state is imposed to be a  $d \times d$  dimensional pure state  $|\psi^{AB}\rangle = \sum_{i=0}^{d-1} \sqrt{\lambda_i} |ii\rangle$  ( $0 < \lambda_i < 1$ ). To this end, they employ an MDI-QSV strategy denoted by  $\mathcal{S} = \{\mathcal{J}, f\}$ , with  $\mathcal{J} = \{p_i, \tau_i \otimes \omega_i\}$  being the input set and  $f$  being a binary outcome payoff function. This process can be described by quantum circuit as in Fig. 3. In each

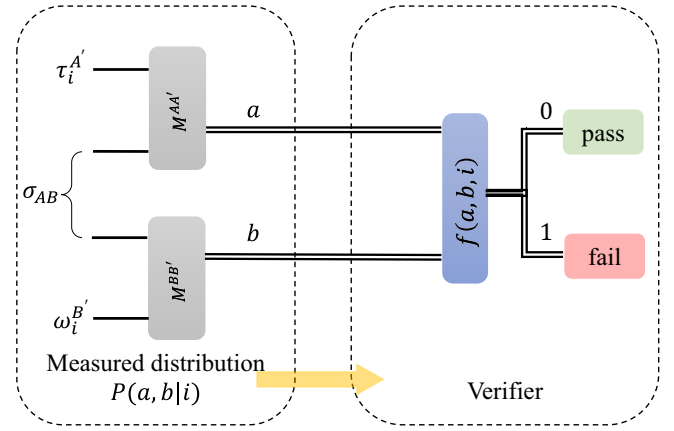


FIG. 3. The circuit representation of an MDI-QSV strategy.

round, the distributed state has an average failure probability given by

$$Q_S(\sigma^{AB}) = \sum_{a,b,i} p_i f(a, b, i) P(a, b|i), \quad (\text{A1})$$

with

$$P(a, b|i) = \text{Tr}[(M_a^{AA'} \otimes M_b^{BB'})(\tau_i^{A'} \otimes \sigma^{AB} \otimes \omega_i^{B'})], \quad (\text{A2})$$

where  $M^{AA'}$ ,  $M^{BB'}$  are untrusted joint measurements. In the following, we omit the superscript  $A(A')$ ,  $B(B')$  for simplicity if there is no ambiguity.

As mentioned in the main text, the MDI-QSV can be transformed into an equivalent virtual prepare-and-measure process. In this process, the average failure probability in Eq. (A1) is reformulated into the summation

$$Q_S(\sigma) = \sum_{a,b} \text{Tr}(\tilde{\Omega}_{ab} \tilde{\rho}_{ab}), \quad (\text{A3})$$

with  $\tilde{\rho}_{ab}$  being a set of unnormalized conditional states

$$\tilde{\rho}_{ab} = \text{Tr}_{AB}[(M_a^{AA'} \otimes M_b^{BB'})(\mathbb{1}^{A'} \otimes \sigma^{AB} \otimes \mathbb{1}^{B'})], \quad (\text{A4})$$

and

$$\tilde{\Omega}_{ab} = \sum_i p_i f(a, b, i) \tau_i \otimes \omega_i, \quad (\text{A5})$$

from Eq. (A1). Here, the  $\mathbb{1}^{A(B')}$  is the identity operator on subsystem  $A'(B')$ . Note that the operator  $\tilde{\Omega}_{ab}$  only involves trusted terms. Intuitively, we may obtain a valid MDI-QSV strategy as long as  $\tilde{\Omega}_{ab}$  is capable of verifying certain target states for all  $a, b$ . In principle, the target state of  $\tilde{\Omega}_{ab}$  should be decided by  $\rho_\psi = |\psi\rangle\langle\psi|$  undergoing the same operation with the distributed state  $\sigma$ , i.e.,  $\text{Tr}_{AB}[(M_a^{AA'} \otimes M_b^{BB'})(\mathbb{1}^{A'} \otimes \rho_\psi^{AB} \otimes \mathbb{1}^{B'})]$  denoting as  $\tilde{\rho}_{ab}^0$ . We remark that Alice and Bob have no information on the joint measurements. They just assume that  $M^{AA'}$ ,  $M^{BB'}$  are some prespecified measurements in designing the MDI-QSV strategy.

Here, we focus on the particular case where the measurements are supposed to be BSMs. First, the BSM is more experimentally mature and favorable, and this choice helps to simplify the derivation of sample efficiency of the resulting strategy. More importantly, the Bell state measurements help to distinguish better the target state and any other states. To

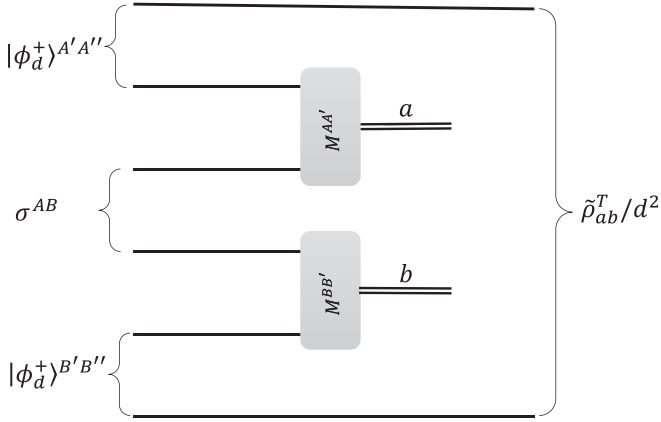


FIG. 4. With the help of two maximally entangled states on Alice and Bob's side, respectively, the source  $\sigma^{AB}$  and joint measurements  $M^{AA'}$ ,  $M^{BB'}$  can be employed to prepare the conditional states  $\{\tilde{\rho}_{ab}^T\}$  in reality, up to a normalization  $1/d^2$ .

illustrate this, note that in the MDI-QSV scenario, the extractability of the shared state to the target state can only be decided via the set of conditional states  $\{\tilde{\rho}_{ab}\}$  because the measurement devices are untrusted. Therefore, the task is in fact verifying that the ensemble  $\{\tilde{\rho}_{ab}\}$  is equivalent to the target ensemble  $\{\tilde{\rho}_{ab}^0\}$ . Meanwhile, the virtual preparation of ensemble  $\{\tilde{\rho}_{ab}\}$  can be implemented physically with the help of two locally maximally entangled states, up to a normalization  $1/d^2$  and a transposition as shown in Fig. 4, i.e.,

$$\begin{aligned} \mathcal{E}_{ab}(\sigma^{AB}) &= \text{Tr}_{AA'BB'} [(\mathbb{1}^{A''} \otimes M_a^{AA'} \otimes M_b^{BB'} \otimes \mathbb{1}^{B''}) \\ &\quad \cdot (|\phi_d^+\rangle^{A''A'} \langle \phi_d^+| \otimes \sigma^{AB} \otimes |\phi_d^+\rangle^{B''B'} \langle \phi_d^+|)]. \\ &= \tilde{\rho}_{ab}^T/d^2. \end{aligned} \quad (\text{A6})$$

By employing the relative entropy as a figure of merit, the relation

$$\begin{aligned} \frac{1}{d^2} \sum_{a,b} D(\tilde{\rho}_{ab}, \tilde{\rho}_{ab}^0) &= \sum_{a,b} D[\mathcal{E}_{ab}(\sigma^{AB}), \mathcal{E}_{ab}(\rho_\psi^{AB})] \\ &\leq D(\sigma^{AB}, \rho_\psi^{AB}) \end{aligned} \quad (\text{A7})$$

holds, where the inequality comes from the fact that the relative entropy does not increase under a completely positive and trace-preserving (CPTP) map (Theorem 5 of Ref. [52]). In Eq. (A7), the equality is achieved if and only if the joint measurements are BSMs, indicating the advantage of BSM in MDI-QSV over any other joint measurements in the MDI-QSV task.

## 2. Sample efficiency of an MDI-QSV strategy

Given a state that is at least  $\varepsilon$  far away from the target state up to local isometry, the maximal probability for this state to give a “pass” outcome in a trial is  $1 - Q_S^\varepsilon$ , where

$$Q_S^\varepsilon = \min_{\sigma, M} Q_S(\sigma), \quad \text{s.t. } F_e(\sigma \rightarrow \rho_\psi) \leq 1 - \varepsilon. \quad (\text{A8})$$

To distinguish such state from the target state, the verifiers need to set a threshold  $N_0 < NQ_S^\varepsilon$ . After  $N$  rounds of the

test, if the number of “fail” events exceeds  $N_0$ , Alice and Bob conclude that the distributed states are not local-isometrically equivalent to the target state. Otherwise, they are convinced that the source distributes quantum states satisfying  $F_e(\sigma \rightarrow \rho_\psi) > 1 - \varepsilon$ .

*Lemma 1.* The probability that a state satisfying  $F_e(\sigma \rightarrow \rho_\psi) \leq 1 - \varepsilon$  is  $1 - \delta$  mistakenly pass the test is upper bounded by

$$\delta \leq \exp \left\{ -ND \left[ \frac{N_0}{N} \middle\| Q_S^\varepsilon \right] \right\}. \quad (\text{A9})$$

Here,  $D[x||y]$  is defined as  $D[x||y] = x \ln(x/y) + (1-x) \ln[(1-x)/(1-y)]$ . In other words, the confidence in concluding that the distributed states satisfying  $F_e(\sigma \rightarrow \rho_\psi) > 1 - \varepsilon$  is  $1 - \delta$ .

*Proof.* The proof follows directly from the Chernoff bound [43,44]. For any distributed state  $\sigma$  satisfying  $F_e(\sigma \rightarrow \rho_\psi) \leq 1 - \varepsilon$ , the probability that the number of fail events is less than  $N_0$  after  $N$  rounds is

$$\begin{aligned} \delta &= \text{Prob}\{N_{\text{fail}} \leq N_0 | N, \sigma\} \leq e^{-ND \left[ \frac{N_0}{N} \middle\| Q_S(\sigma) \right]} \\ &\leq e^{-ND \left[ \frac{N_0}{N} \middle\| Q_S^\varepsilon \right]}, \end{aligned} \quad (\text{A10})$$

where the second inequality is from the property of  $D[x||y]$  and the fact that  $N_0/N \leq Q_S^\varepsilon \leq Q_S(\sigma)$ .

This lemma shows that the MDI-QSV strategy  $\mathcal{S}$  can exclude all states satisfying  $F_e(\sigma \rightarrow \rho_\psi) \leq 1 - \varepsilon$  for any  $\varepsilon > 0$  with a confidence  $1 - \delta$ , as long as the protocol is executed over a sufficient number of rounds. Here, the  $\varepsilon$  reflects the accuracy in the verification, and a smaller  $\varepsilon$  means that a state is closer to the target state (up to local isometry), such that more measurements are required to distinguish it from  $\rho_\psi$ . More explicitly, given some fixed accuracy  $1 - \varepsilon$  and confidence level  $1 - \delta$ , the required number of measurements is

$$N \geq N_S(\varepsilon, \delta) = \frac{1}{D \left[ \frac{N_0}{N} \middle\| Q_S^\varepsilon \right]} \ln \delta^{-1}, \quad (\text{A11})$$

which gives the *sample efficiency* of  $\mathcal{S}$ .

## 3. An intuitive construction of MDI-QSV strategy

With the above discussion, there exists an intuitive construction of MDI-QSV. For each state  $\tilde{\rho}_{ab}^0$  in the target ensemble, one can design a standard QSV strategy  $\Omega_{ab}$  that contains only rank-1 projectors to verify  $\tilde{\rho}_{ab}^0$ . More explicitly, this can be achieved as follows.

(1) For any  $a, b$ , design an observable  $\Omega_{ab}$  such that  $\tilde{\rho}_{ab}^0$  is its eigenstate with minimum eigenvalue, and thus can be used as a strategy in verifying  $\tilde{\rho}_{ab}^0$ . Note that the operator  $O_{ab}$  needs to admit a decomposition into a linear combination of pure product states, or equivalently,  $O_{ab}$  can be regarded as a separable state, according to Eq. (A5).

(2) Specify  $d^4$  input sets  $\mathcal{J}_{ab} = \{p_{ab}^i, \tau_{ab}^i \otimes \omega_{ab}^i\}_i$ , where  $\sum_i p_{ab}^i \tau_{ab}^i \otimes \omega_{ab}^i = O_{ab}$  and  $\sum_i p_{ab}^i = 1$ .

(3) In each round, Alice and Bob randomly choose one from the  $d^4$  input set, namely,  $\mathcal{J}_{a_0b_0}$ , and prepare input states according to  $\mathcal{J}_{a_0b_0}$ . After performing joint measurements on their prepared states and the distributed state, Alice and Bob obtain their outcome  $(a, b)$ . The payoff function is 1 if and

only if  $a = a_0$  and  $b = b_0$ , i.e., the effective strategy must match the conditional state.

When the joint measurements are supposed to be BSMs, the target ensemble is

$$\{|\psi_{ab}\rangle\langle\psi_{ab}| = (U_a \otimes U_b)(\rho_{\psi}^{AB})^T(U_a \otimes U_b)^\dagger\}_{a,b}. \quad (\text{A12})$$

Here,  $\{U_j\}$  are the set of Heisenberg-Weyl operators

$$U_j = X_d^k Z_d^l, \quad (\text{A13})$$

with  $k = \lfloor j/d \rfloor$ ,  $l = j \bmod d$  and the  $X_d = \sum_{m=0}^{d-1} |m\rangle\langle m+1|$ ,  $Z_d = \sum_{m=0}^{d-1} e^{i2m\pi/d} |m\rangle\langle m|$  being the generalized Pauli operators. In the following, we denote  $|\psi_{ab}\rangle\langle\psi_{ab}|$  as  $\rho_{ab}$  in short for brevity.

Therefore, the remaining problem in this construction is to design standard QSV strategies  $O_{ab}$  for  $|\psi_{ab}\rangle$ , which involves only rank-1 local projectors. For this task, we have the following result:

**Lemma 2.** (Optimal QSV strategy using rank-1 local projectors) Consider a  $d \times d$ -dimensional target state  $|\psi\rangle$ . The optimal standard QSV protocol implementable with rank-1 projectors is  $\Omega_\psi = \frac{1}{d^2-1}(\mathbb{1}_{d^2} - \rho_\psi)$ , whose spectral gap is  $\frac{1}{d^2-1}$ .

*Proof.* An optimal QSV involving only rank-1 local projectors should be as follows: In each round, the verifier randomly draws a rank-1 local projector  $P_j^A \otimes P_j^B$  from some set  $\mathcal{M}$  with probability  $p_j$ . By performing the binary outcome measurement  $\{P_j^A \otimes P_j^B, \mathbb{1}_{d^2} - P_j^A \otimes P_j^B\}$ , the verifier labels the outcomes as fail and pass, respectively. Remarkably, one always has  $\langle\psi|P_j^A \otimes P_j^B|\psi\rangle < 1$  if considering the nontrivial case where the target state is entangled, since  $P_j^A \otimes P_j^B$  is nothing but a pure product state. Therefore, to guarantee that the target state  $|\psi\rangle = \sum_{i=0}^{d-1} \lambda_i |ii\rangle$  always passes the test, the verifier has to label “fail” to the events detected by  $P_j^A \otimes P_j^B$  and imposes the constraint  $P_j^A \otimes P_j^B |\psi\rangle = 0$ . Then, the QSV strategy can be expressed as  $\Omega = \sum_j p_j P_j^A \otimes P_j^B$  with  $p_j \geq 0$  and  $\Omega|\psi\rangle = 0$ .

Denote all the  $d^2$  eigenvalues of  $\Omega$  in increasing order as  $\{0, e_1, e_2, \dots, e_{d^2-1}\}$ . An optimal strategy should have the largest possible spectral gap [19], which is just the second smallest eigenvalue  $e_1$  of  $\Omega$ . By observing that  $\sum_{k=1}^{d^2-1} e_k = \text{Tr}(\Omega) = 1$ , it is known that  $e_1$  has an upper bound  $1/(d^2-1)$ , which is achieved if  $e_1 = e_2 = \dots = e_{d^2-1}$ . Therefore, the strategy  $\Omega_\psi = (\mathbb{1}_{d^2} - \rho_\psi)/(d^2-1)$  is optimal for  $\psi$  as long as it exists.

Now we proceed to prove that  $\Omega_\psi$  is always implementable with rank-1 local projectors. That is,  $\Omega_{|\psi\rangle}$  is separable, and admits a decomposition of the form  $\sum_j p_j P_j^A \otimes P_j^B$ . To show this, one can perform a partial transpose on  $\Omega_{|\psi\rangle}$ ,

$$\begin{aligned} \Omega_{|\psi\rangle}^{TA} &= \frac{1}{d^2-1} \sum_{i<j} (\lambda_j^2 |ii\rangle\langle ii| + \lambda_i^2 |jj\rangle\langle jj| + |ij\rangle\langle ij| \\ &\quad + |ji\rangle\langle ji| - \lambda_i \lambda_j |ij\rangle\langle ji| - \lambda_j \lambda_i |ji\rangle\langle ij|). \end{aligned} \quad (\text{A14})$$

It is observed that the  $\Omega_{|\psi\rangle}^{TA}$  is a summation of some  $4 \times 4$  submatrices  $B_{ij}(i < j)$ , i.e.,  $\Omega_{|\psi\rangle}^{TA} = \sum_{i<j} B_{ij}$ , with  $B_{ij}$  supported

on the subspace  $\{|ii\rangle, |ij\rangle, |ji\rangle, |jj\rangle\}$  as

$$B_{ij} = \frac{1}{d^2-1} \begin{pmatrix} \lambda_j^2 & 0 & 0 & 0 \\ 0 & 1 & -\lambda_i \lambda_j & 0 \\ 0 & -\lambda_i \lambda_j & 1 & 0 \\ 0 & 0 & 0 & \lambda_i^2 \end{pmatrix}. \quad (\text{A15})$$

From the positive partial transpose criterion [53] which is necessary and sufficient for solving the separability problem in this four-dimensional subspace [54], one knows that all the  $B_{ij}$  can be seen as unnormalized separable states. Therefore,  $\Omega_{|\psi\rangle}^{TA}$  is separable and the initial observable  $\Omega_{|\psi\rangle}$  is also separable. This finishes the proof.

Additionally, we remark that the decomposition of  $\frac{1}{d^2-1}(\mathbb{1}_{d^2} - \rho_\psi)$  is not unique, and contains at least  $d^2$  terms. In general cases, an alternative decomposition is of the form

$$\begin{aligned} \mathbb{1}_{d^2} - \rho_\psi &= \sum_{k<l} \left[ (1 - \lambda_k^2) |kl\rangle\langle kl| + (1 - \lambda_l^2) |lk\rangle\langle lk| \right. \\ &\quad \left. + \frac{1}{2} \sum_{j=1}^4 \rho_{kl}^j \otimes \rho_{kl}^{j'} \right], \end{aligned} \quad (\text{A16})$$

with the components  $\rho_{kl}^j \otimes \rho_{kl}^{j'}$  defined by

$$\begin{aligned} \rho_{kl}^1 \otimes \rho_{kl}^{1'} &= |+\rangle_{kl} \langle +|_{kl} \otimes (\lambda_l |k\rangle - \lambda_k |l\rangle)(\lambda_l \langle k| - \lambda_k \langle l|) \\ \rho_{kl}^2 \otimes \rho_{kl}^{2'} &= |-\rangle_{kl} \langle -|_{kl} \otimes (\lambda_l |k\rangle + \lambda_k |l\rangle)(\lambda_l \langle k| + \lambda_k \langle l|) \\ \rho_{kl}^3 \otimes \rho_{kl}^{3'} &= |i\rangle_{kl} \langle i|_{kl} \otimes (\lambda_l |k\rangle + i\lambda_k |l\rangle)(\lambda_l \langle k| + i\lambda_k \langle l|) \\ \rho_{kl}^4 \otimes \rho_{kl}^{4'} &= |-i\rangle_{kl} \langle -i|_{kl} \otimes (\lambda_l |k\rangle - i\lambda_k |l\rangle)(\lambda_l \langle k| - i\lambda_k \langle l|), \end{aligned} \quad (\text{A17})$$

where  $|\pm\rangle_{kl} = (|k\rangle \pm |l\rangle)/\sqrt{2}$ , and  $|\pm i\rangle_{kl} = (|k\rangle \pm i|l\rangle)/\sqrt{2}$ . ■

Up to now, we have finished the construction of the MDI-QSV strategy, denoted as  $\mathcal{S}_\psi^0$ . A satisfying nature of  $\mathcal{S}_\psi^0$  is that the target state can always pass the test as long as proper joint measurements (i.e., BSMs in this situation) are performed. This makes its sample efficiency scale optimally with the verification accuracy as  $O(\varepsilon^{-1})$ . Such strategies are called *no-false-negative* (NFN) in the main text.

However, a prefactor  $1/d^4$  will appear in the sample efficiency due to the above construction of  $\tilde{\Omega}_{ab}$ , which limits the performance of  $\mathcal{S}_\psi^0$ . This limitation in fact comes from the mismatching between  $(a_0, b_0)$  and  $(a, b)$ . To be specific,  $(a_0, b_0)$  labels the choice of effective strategy, and  $(a, b)$  labels the state to be verified in the equivalent process. Due to the casual order between the input and output in the actual MDI-QSV protocol, the strategy has to be decided before the target state is known, which leads to this mismatch. Hence, the natural questions are, can we optimize the strategy  $\mathcal{S}_\psi^0$  to overcome this drawback, and how well does an optimal MDI-QSV strategy perform? To answer these questions, it is sufficient to consider the NFN MDI-QSV strategies, whose properties are investigated in the next section.

#### 4. No-false-negative MDI-QSV strategies

Because of the observation in Sec. A 1, we still consider the case where the target ensemble is obtained from BSMs. For this kind of NFN MDI-QSV strategy, there are two observations.

Firstly, only the events with nonzero payoff, i.e.,  $f(a, b, i) = 1$ , contribute in an NFN MDI-QSV strategy (namely, the *valid events*). An intuition is that, with a fixed input set, more valid events will lead to a more powerful strategy.

*Lemma 3.* For an NFN MDI-QSV strategy  $S^D$  of  $|\psi\rangle$  whose input set is  $\mathcal{J}$ , the optimal payoff function  $f_{\mathcal{J},\psi}$  is given by

$$f_{\mathcal{J},\psi}(a, b, i) = \begin{cases} 1, & \text{if } \text{Tr}[(\tau_i \otimes \omega_i)\rho_{ab}] = 0 \\ 0, & \text{other cases} \end{cases}. \quad (\text{A18})$$

*Proof.* Firstly, if the shared state is just the target state and the joint measurement is perfect BSM, Alice and Bob will obtain pass in every round during the verification. Hence, the strategy  $S^D = \{\mathcal{J}, f_{\mathcal{J},\psi}\}$  is a valid NFN MDI-QSV strategy.

Meanwhile, the equality  $\text{Tr}[(\tau_i \otimes \omega_i)\rho_{ab}] = 0$  is a necessary condition for any NFN MDI-QSV strategy. This constraint guarantees that the target state can always pass the test. For any other strategy  $S^{D'} = \{\mathcal{J}, f'\}$ ,  $Q_{S^{D'}}(\sigma^{AB}) \geq Q_{S^D}(\sigma^{AB})$  holds for any distributed state  $\sigma^{AB}$ . Therefore,  $S^D$  requires fewer measurements to verify the shared state compared with  $S^{D'}$ . ■

Besides the optimization on the input function, a symmetrization on the input set also helps to further improve the performance of an MDI-QSV strategy.

*Lemma 4.* For an MDI-QSV strategy  $S^D = \{\mathcal{J}, f_{\mathcal{J},\psi}\}$  of  $|\psi\rangle$  where the input set is denoted as  $\mathcal{J} = \{p_i, \tau_i \otimes \omega_i\}$ , one can obtain a symmetrized input set by the local unitaries  $\{U_a \otimes U_b\}_{a,b=0}^{d^2-1}$ , that is,

$$\mathcal{J}^{\text{sym}} = \cup_{a,b} \frac{1}{d^4} \mathcal{J}_{ab}, \quad (\text{A19})$$

where

$$\mathcal{J}_{ab}/d^4 = \{p_i/d^4, (U_a \otimes U_b)^\dagger \tau_i \otimes \omega_i (U_a \otimes U_b)\}. \quad (\text{A20})$$

Then, the strategy specified by  $S^{D'} = \{\mathcal{J}^{\text{sym}}, f_{\mathcal{J}^{\text{sym}},\psi}\}$  is at least as efficient as the original strategy  $S^D$ .

This result is a direct consequence of the observation that the target ensemble  $\{\rho_{ab}\}_{a,b=0}^{d^2-1}$  is invariant under the local unitaries  $\{U_a \otimes U_b\}_{a,b=0}^{d^2-1}$ .

These two lemmas tell us how one can improve the performance of an NFN MDI-QSV strategy by modifying its input set and payoff function.

#### 5. Proof of the propositions in the main text

The construction of MDI-QSV strategy in Propositions 1 in the main text follows directly from the above results. Indeed, when the optimizations in Lemmas 3 and 4 are applied to the above constructed strategy  $S_\psi^0$  in Sec. A 3, one ends up with the strategy  $S_\psi^D = \{\mathcal{J}_\psi, f_{\mathcal{J}_\psi}\}$  proposed in Propositions 1 in three steps:

(1) Decompose the  $[\mathbb{1}_{d^2} - (\rho_\psi^{AB})^T]/(d^2 - 1)$  into separable states, i.e.,  $\sum_j c_j \phi_j^{A'} \otimes \phi_j^{B'} = [\mathbb{1}_{d^2} - (\rho_\psi^{AB})^T]/(d^2 - 1)$ .

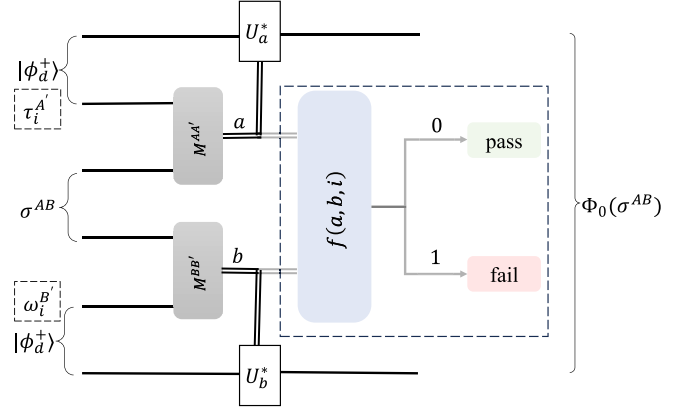


FIG. 5. If  $\sigma^{AB}$  always pass the test, one can extract the target state by replacing the verification setups (the parts in dashed boxes) with locally maximally entangled states and unitary operations on the ancilla qudits.

(2) Symmetrize the set  $\{(c_j, \phi_j^{A'}, \phi_j^{B'})\}$  with all Heisenberg-Weyl operators, which gives the input set

$$\mathcal{J}_\psi = \left\{ \left( \frac{c_j}{d^4}, U_a \phi_j^{A'} U_a^\dagger \otimes U_b \phi_j^{B'} U_b^\dagger \right)_{a,b,j} \right\} := \{(p_i, \tau_i^{A'} \otimes \omega_i^{B'})\}, \quad (\text{A21})$$

(3) The optimized payoff function for this input set is given according to Eq. (A18).

Now we proceed to prove the Propositions 2, i.e., quantitatively investigate the number of required measurements by  $S_\psi^D$ . In the main text, it is shown that its sample efficiency is decided by the following optimization problem:

$$\begin{aligned} Q_{S_\psi^D}^\varepsilon &= \min_{\sigma, M} Q_{S_\psi^D}(\sigma) \\ \text{s.t. } F_e(\sigma \rightarrow \rho_\psi) &\leq 1 - \varepsilon, \end{aligned} \quad (\text{A22})$$

where  $F_e(\sigma \rightarrow \rho_\psi)$  is the extractability [41,42] from  $\sigma$  to target state  $|\psi\rangle$ . Here, the extractability is defined as

$$F_e(\sigma \rightarrow \rho_\psi) = \max_{\Phi} \text{Tr}[\rho_\psi \Phi(\sigma)], \quad (\text{A23})$$

with the maximum taken over all local isometries  $\Phi$ .

Since the  $Q_{S_\psi^D}^\varepsilon$  is nonincreasing with  $\varepsilon$ , the functional relationship between  $Q_{S_\psi^D}^\varepsilon$  and  $\varepsilon$  can also be decided by

$$\begin{aligned} 1 - \varepsilon_{Q_0} &= \min_{\sigma} \left( \max_{\Phi} \text{Tr}[\rho_\psi \Phi(\sigma)] \right) \\ \text{s.t. } Q_{S_\psi^D}(\sigma) &= Q_0, \end{aligned} \quad (\text{A24})$$

That is, when the distributed state  $\sigma$  passes the test at every round with probability  $1 - Q_0$ , the solution  $1 - \varepsilon_{Q_0}$  is the minimal possible extractability of  $\sigma$ .

We first derive a lower bound of the minimal extractability  $1 - \varepsilon_{Q_0}$  by using a fixed local isometry. In an ideal case where the  $\sigma$  always passes the test, the circuit in Fig. 4 just outputs the conditional states  $\{\rho_{ab}^T = (U_a \otimes U_b)^* \rho_\psi (U_a \otimes U_b)^T\}$ , which can be transformed into the target state after applying  $(U_a \otimes U_b)^T$ . Here,  $(\cdot)^*$  is the complex conjugate of an operator. By definition, this provides a satisfying choice of local isometry  $\Phi_0$  as in Fig. 5, which has been frequently used in the self-testing of the quantum state [32,33,38]. Formally, the



local isometry  $\Phi_0$  is defined as

$$\Phi_0(\sigma^{AB}) = \sum_{a,b} (U_a^{A''} \otimes U_b^{B''})^T \text{Tr}_{AA'BB'} [(\mathbb{1}^{A''} \otimes M_a^{AA'} \otimes M_b^{BB'} \otimes \mathbb{1}^{B''}) \cdot (|\phi_d^+\rangle^{A'A'} \langle \phi_d^+| \otimes \sigma^{AB} \otimes |\phi_d^+\rangle^{B'B'} \langle \phi_d^+|)] (U_a^{A''} \otimes U_b^{B''})^*, \quad (\text{A25})$$

which can be written in short as

$$\Phi_0(\sigma^{AB}) = \frac{1}{d^2} \sum_{a,b} (U_a \otimes U_b)^T \tilde{\rho}_{ab}^T (U_a \otimes U_b)^*, \quad (\text{A26})$$

according to Eq. (A6). The fidelity between the target state and the extracted state  $\Phi_0(\sigma^{AB})$  is

$$1 - \varepsilon_{Q_0} \geq F_e^l = \frac{1}{d^2} \sum_{ab} \text{Tr}(\rho_{ab} \tilde{\rho}_{ab}) := \frac{1}{d^2} \sum_{ab} \tilde{f}_{ab}. \quad (\text{A27})$$

Denote  $\tilde{\Omega}_{ab,\psi}$  as the effective QSV strategy induced by  $\mathcal{S}_\psi^D$  according to Eq. (A5), and  $q_{ab}$  its minimum nonzero eigenvalue, then the construction leads to

$$\tilde{\Omega}_{ab,\psi} \geq q_{ab}(\mathbb{1}_{d^2} - \rho_{ab}) \geq \frac{1}{d^4(d^2 - 1)}(\mathbb{1}_{d^2} - \rho_{ab}) \quad (\text{A28})$$

for all  $a, b$ . The second inequality comes from the fact that the  $\mathcal{S}_\psi^D$  always outperform the original strategy  $\mathcal{S}_0$  proposed in Sec. A3. Meanwhile, the conditional states  $\tilde{\rho}_{ab}$  are unnormalized, and satisfy

$$\text{Tr}(\tilde{\rho}_{ab}) := c_{ab}, \quad \sum_{ab} c_{ab} = d^2 \quad (\text{A29})$$

due to the completeness of the measurements  $M^{AA'}$  and  $M^{BB'}$ . Then, the average failure probability  $Q_{\mathcal{S}_\psi^D}$  satisfies

$$\begin{aligned} Q_0 &= Q_{\mathcal{S}_\psi^D}(\sigma^{AB}) \\ &\geq \sum_{ab} q_{ab} \text{Tr}[(\mathbb{1}_{d^2} - \rho_{ab}) \tilde{\rho}_{ab}] \\ &= \sum_{ab} q_{ab} (c_{ab} - \tilde{f}_{ab}). \end{aligned} \quad (\text{A30})$$

Additionally, as the input set has been symmetrized, these effective strategies  $\tilde{\Omega}_{ab,\psi}$  are equivalent up to local unitary, such that  $q_{ab} = \bar{q}$  for all  $a, b$ . Then, the optimization problem becomes

$$\begin{aligned} F_e^l &= \min \sum_{ab} \tilde{f}_{ab}/d^2 \\ \text{s.t. } &\bar{q} \sum_{ab} (c_{ab} - \tilde{f}_{ab}) \leq Q_0, \\ &\sum_{ab} c_{ab} = d^2, \\ &\forall a, b, \quad 0 \leq \tilde{f}_{ab} \leq c_{ab} \leq 1, \\ &\bar{q} \geq \frac{1}{d^4(d^2 - 1)}, \end{aligned} \quad (\text{A31})$$

whose solution can be obtained directly as  $F_e^l = 1 - Q_0/(d^2\bar{q})$ , that is,  $\varepsilon_{Q_0} \leq Q_0/(d^2\bar{q})$ .

Meanwhile, we provide an upper bound of this worst-case extractability  $1 - \varepsilon_{Q_0}$ , by specifying the shared states and joint measurements. Let  $R(\rho)$  be the robustness of entanglement [55], and  $\rho(\varepsilon)$  be the state that minimizes  $R(\rho)$  among all the

states with infidelity  $\varepsilon$  to  $|\psi^{AB}\rangle$ , i.e.,

$$r(\varepsilon) = \min_{\rho} R(\rho)$$

$$\rho(\varepsilon) = \arg \min_{\rho} R(\rho)$$

$$\text{s.t. } F(\rho, \rho_\psi^{AB}) = 1 - \varepsilon. \quad (\text{A32})$$

Because one can always mix  $\rho(\varepsilon)$  with some separable states to increase the infidelity  $\varepsilon$  and decrease the robustness of entanglement,  $r(\varepsilon)$  decreases monotonically with the infidelity  $\varepsilon$ , until  $r(\varepsilon) = 0$  [ $\rho(\varepsilon)$  is separable]. Given the state  $\rho(\varepsilon)$  and perfect BSM, it is straightforward to check that  $Q_{\mathcal{S}_\psi^D}[\rho(\varepsilon)] = d^2\bar{q}\varepsilon$ . Then, it remains to calculate the extractability from  $\rho(\varepsilon)$  to the target state. If  $r(\varepsilon) > 0$ , there exist optimal local operations to transform  $\rho(\varepsilon)$  into some other state  $\rho'(\varepsilon)$  to maximize the fidelity to the target state. However, as the local operations cannot increase the robustness of entanglement, the relation  $r(\varepsilon) \geq R[\rho'(\varepsilon)]$  always holds. From the monotonicity of  $r(\varepsilon)$  and the definition in Eq. (A32), it can be observed that  $F[\rho'(\varepsilon), \rho_\psi^{AB}] \leq 1 - \varepsilon$ . In other words, when  $r(\varepsilon) > 0$ , there always exists a state with infidelity  $1 - \varepsilon$  such that its infidelity to the target state can never be increased under local strategies, while if  $r(\varepsilon) = 0$  [ $\rho(\varepsilon)$  is separable], the extractability is just  $\lambda_0^2$ , with  $\lambda_0$  being the largest Schmidt coefficient of  $|\psi^{AB}\rangle$ . This can be achieved by replacing  $\rho(\varepsilon)$  with the separable state having the largest overlap with the target state. Therefore, once  $Q_{\mathcal{S}_\psi^D}(\sigma^{AB}) = Q_0$  is given, the worst-case extractability  $F_e(\sigma^{AB} \rightarrow \rho_\psi^{AB})$  is upper bounded by

$$F_e^u(\sigma^{AB} \rightarrow \rho_\psi^{AB}) \leq \begin{cases} 1 - Q_0/(d^2\bar{q}), & \text{if } Q_0 < d^2\bar{q}(1 - \lambda_0^2) \\ \lambda_0^2, & \text{if } Q_0 \geq d^2\bar{q}(1 - \lambda_0^2) \end{cases}. \quad (\text{A33})$$

Consequently, when considering the nontrivial case  $Q_0 < d^2\bar{q}(1 - \lambda_0^2)$ , the upper bound and lower bound coincide, indicating that the exact value of the worst-case extractability in Eq. (A24) is exactly  $\varepsilon_{Q_0} = Q_0/(d^2\bar{q})$ . The solution of the initial problem in Eq. (A22) is thus  $Q_{\mathcal{S}_\psi^D}^\varepsilon = d^2\bar{q}\varepsilon$ . By employing Lemma 1, the sample efficiency of  $\mathcal{S}_\psi^D$  is

$$N_{\varepsilon,\delta}(\mathcal{S}_\psi^D) \geq \frac{\ln \delta^{-1}}{\ln(1 - d^2\bar{q}\varepsilon)^{-1}} \approx \frac{1}{d^2\bar{q}\varepsilon} \ln \delta^{-1}. \quad (\text{A34})$$

This is just the first result of Proposition 2 in the main text.

Next, we proceed to figure out the behavior of this strategy-dependent parameter  $\bar{q}$ . By taking trace on the effective QSV strategy  $\tilde{\Omega}_{ab,\psi}$ , one has

$$\text{Tr}(\tilde{\Omega}_{ab,\psi}) \geq \bar{q}(d^2 - 1) \quad (\text{A35})$$

from Eq. (A28), and

$$\text{Tr}(\tilde{\Omega}_{ab,\psi}) = \sum_i p_i f_{\mathcal{J}_\psi}(a, b, i) \quad (\text{A36})$$

by the definition of  $\tilde{\Omega}_{ab,\psi}$ . After substituting this into Eq. (A35) and summing over all  $a, b$ , one arrives at

$$\bar{q} \leq \frac{1}{d^4(d^2-1)} \sum_{a,b,i} p_i f(a, b, i). \quad (\text{A37})$$

Here and after, we denote the payoff function  $f_{j_\psi}$  as  $f$  in short for simplicity if there is no ambiguity.

Notably, even for the same target state, different decomposition of  $\frac{1}{d^2-1}(\mathbb{1}_{d^2} - \rho_\psi^{AB})$  leads to different input sets and finally different efficiency of the resulting strategy. As shown in Eq. (A37), the sample efficiency is directly related to the number of valid events. To design a more efficient MDI-QSV strategy, one is expected to find an input set whose weighted average of valid events  $\sum_{a,b,i} p_i f(a, b, i)$  is as large as possible. The weighted average of valid events is upper bounded as follows:

*Lemma 5.* In any NFN MDI-QSV strategy, there exist at most  $d^3(d-1)$  pairs  $(a, b)$  such that the payoff  $f(a, b, i)$  is 1 for each possible quantum input  $\tau_i \otimes \omega_i$ .

*Proof.* Given that the label  $b$  has been fixed as  $b = 0$ , that is,  $U_b = \mathbb{1}_d$ , we have

$$\sum_{a=0}^{d^2-1} (U_a \otimes \mathbb{1}_d)^\dagger \tau_i \otimes \omega_i (U_a \otimes \mathbb{1}_d) = d \mathbb{1}_d \otimes \omega_i. \quad (\text{A38})$$

Meanwhile, consider the following summation on the subset  $\{a | f(a, 0, i) = 1\}$ :

$$\sum_{\{a | f(a, 0, i) = 1\}} (U_a \otimes \mathbb{1}_d)^\dagger \tau_i \otimes \omega_i (U_a \otimes \mathbb{1}_d) := O^A \otimes \omega_i. \quad (\text{A39})$$

Due to the NFN character of the MDI-QSV strategy considered here, we have the constraint

$$\text{Tr}[(O^A \otimes \omega_i)(\rho_\psi^{AB})^T] = 0. \quad (\text{A40})$$

Define  $\rho^A = \frac{\text{Tr}_B[\omega_i^B(\rho_\psi^{AB})^T]}{\text{Tr}[\omega_i^B(\rho_\psi^{AB})^T]}$ , then the above constraint indicates that

$$O^A \leq \lambda_{\max}(O^A)(\mathbb{1}_d - \rho^A), \quad (\text{A41})$$

with  $\lambda_{\max}(O^A)$  being the maximal eigenvalue of  $O^A$ . By comparing Eqs. (A38) and (A41), it is observed that  $O^A \leq d(\mathbb{1}_d - \rho^A)$ . Therefore, the size of the set  $\{a | f(a, 0, i) = 1\}$  satisfies

$$|\{a | f(a, 0, \tau_i \otimes \omega_i) = 1\}| = \text{Tr}(O^A) \leq d(d-1). \quad (\text{A42})$$

Similarly, the same result holds for all  $d^2$  choices of label  $b$ , and there exist no more than  $d^3(d-1)$  pairs  $(a, b)$  satisfying  $f(a, b, i) = 1$ . This finishes the proof. ■

With this lemma, one arrives at  $\bar{q} \leq 1/[d(d+1)]$  from Eq. (A37). As for the lower bound of  $\bar{q}$ , we remark that the target state  $|\psi\rangle$  is invariant under  $(Z_d \otimes Z_d^\dagger)^k$  for  $k = 0, 1, \dots, d$ . If some input  $\tau_i \otimes \omega_i$  satisfying  $f(0, 0, i) = 1$ , then the construction guarantees that  $f(a, b, i) = 1$  as long as  $U_a \otimes U_b = (Z_d \otimes Z_d^\dagger)^k$  for some  $k$ . Therefore, the relation  $\sum_{a,b} f(a, b, i) \geq d$  holds for this input, and similarly for all the other inputs. This imposes a lower bound on  $\bar{q}$  as  $\bar{q} \geq 1/[d^3(d^2-1)]$ . Particularly, the maximally entangled state has  $d^2$  stabilizers in all, and it will lead to a lower bound  $\bar{q} \geq 1/[d^2(d^2-1)]$  for such state.

Consequently, the upper and lower bound on  $\bar{q}$  is given as in Proposition 2 of the main text, namely,

$$\frac{c}{d^4(d^2-1)} \leq \bar{q} \leq \frac{1}{d^4(d^2-1)} \sum_{a,b,i} p_i f(a, b, i) \leq \frac{1}{d(d+1)}, \quad (\text{A43})$$

with  $c = d^2$  if  $\rho_\psi^{AB}$  is maximally entangled, and  $c = d$  otherwise. This finishes the proof of Proposition 2.

## 6. MDI-QSV and two-way adaptive QSV strategy

In this section, we discuss the problem of how well an MDI-QSV strategy can perform. Here, an intuition is that the untrusted measurement devices will never lead to a better performance than QSV with trusted measurements, even with the help of trusted local quantum inputs. This is expressed more rigorously and proved as follows:

*Lemma 6.* For a given target state, the sample efficiency of any MDI-QSV strategy cannot be better than the optimal two-way adaptive QSV strategy [22], in which trusted local measurements and one-round two-way classical communication is required.

*Proof.* For the proof, we first make a reformulation on the failure probability in one round  $Q_S$  as

$$Q_S(\sigma^{AB}) = \text{Tr}(\Omega_{\text{eff}} \sigma^{AB}), \quad (\text{A44})$$

where

$$\begin{aligned} \Omega_{\text{eff}} &= \sum_i p_i \sum_{a,b} f(a, b, i) \\ &\quad \text{Tr}_{AB}[(M_a^{AA'} \otimes M_b^{BB'})(\tau_i^{A'} \otimes \mathbb{1}^{AB} \otimes \omega_i^{B'})] \\ &:= \sum_i p_i \sum_{a,b} f(a, b, i) E_{a|i} \otimes E'_{b|i}, \end{aligned} \quad (\text{A45})$$

with  $E_{a|i} = \text{Tr}_A[M_a^{AA'}(\tau_i^{A'} \otimes \mathbb{1}^A)]$  and similar for  $E'_{b|i}$ . Moreover,  $\{E_{a|i}\}$ ,  $\{E'_{b|i}\}$  satisfy  $\sum_a E_{a|i} = \mathbb{1}_d$  and  $\sum_b E'_{b|i} = \mathbb{1}_d$  due to the completeness of the measurements  $\{M_a^{AA'}\}$ ,  $\{M_b^{BB'}\}$ . Therefore, one can regard  $\{E_{a|i}\}$ ,  $\{E'_{b|i}\}$  as untrusted positive operator valued measurements (POVMs) on Alice's and Bob's side, respectively. Meanwhile, the payoff function  $f(a, b, i)$  is regarded as a function requiring two-way classical communication to be decided. In this way, an MDI-QSV strategy  $S$  is regarded effectively as a two-way adaptive QSV strategy introduced in Ref. [22], while the difference is that here the effective POVMs are untrusted.

Consequently, for any MDI-QSV strategy, there exists a two-way adaptive QSV strategy having the same efficiency for the same target state. That is, the performance of MDI-QSV is upper bounded by an optimal two-way adaptive QSV strategy. This finishes the proof. ■

Besides imposing an upper bound on the sample efficiency of the MDI-QSV strategy, Lemma 6, can also be used as a criterion for an MDI-QSV strategy to be optimal. That is, for a given target state, an MDI-QSV strategy is optimal if it performs as good as the optimal two-way adaptive QSV strategy. In the next section, we show by example that such strategies do exist, by applying our construction of  $S_\psi^D$  to maximally entangled states with prime local dimension.

### 7. Optimal MDI-QSV of maximally entangled states with prime local dimension

For prime local dimension  $d$ , it is known that the eigenbases of  $\{Z_d, X_d, X_d Z_d, X_d Z_d^2, \dots, X_d Z_d^{d-1}\}$  form a complete set of mutually unbiased bases (MUBs). Given that  $|\phi_d^+\rangle$  are maximally entangled states with prime local dimension  $d$ , the following equation holds:

$$\mathbb{1}_{d^2} + d|\phi_d^+\rangle\langle\phi_d^+| = \sum_{|e\rangle} |e\rangle\langle e| \otimes |e^*\rangle\langle e^*|, \quad (\text{A46})$$

where the summation is taken over all eigenstates of the set of operators  $\{Z_d, X_d, X_d Z_d, X_d Z_d^2, \dots, X_d Z_d^{d-1}\}$ , and  $|e^*\rangle$  is the conjugate of  $|e\rangle$ . Then, a decomposition of  $\mathbb{1}_{d^2} - |\phi_d^+\rangle\langle\phi_d^+|$  in constructing the MDI-QSV strategy for  $|\phi_d^+\rangle$  can be taken as

$$\begin{aligned} \mathbb{1}_{d^2} - |\phi_d^+\rangle\langle\phi_d^+| &= \frac{d+1}{d}\mathbb{1}_{d^2} - \frac{1}{d} \left( \sum_{|e\rangle} |e\rangle\langle e| \otimes |e^*\rangle\langle e^*| \right) \\ &= \frac{1}{d} \left[ (d+1)\mathbb{1}_{d^2} - \sum_{|e\rangle} |e\rangle\langle e| \otimes |e^*\rangle\langle e^*| \right]. \end{aligned} \quad (\text{A47})$$

Moreover, if a vector  $|e\rangle$  belongs to the basis  $X^x Z^y$  ( $x, y \in \{0, 1, \dots, d-1\}$ ), i.e.,  $X_d^x Z_d^y |e\rangle \propto |e\rangle$ , then the state  $U_a |e\rangle$  remains a vector belonging to the basis  $X_d^x Z_d^y$ , which can be observed by  $X_d^x Z_d^y U_a |e\rangle \propto U_a X_d^x Z_d^y |e\rangle \propto U_a |e\rangle$ .

With the above decomposition, one can check that the construction in Proposition 1 of the main text leads to an input set that can be implemented in two steps. Firstly, Alice randomly chooses one basis from the set  $\{Z_d, X_d, X_d Z_d, X_d Z_d^2, \dots, X_d Z_d^{d-1}\}$ , and Bob's basis is chosen to be conjugate to the basis of Alice. Secondly, Alice and Bob randomly choose one state vector in their own basis as their input state, respectively. After obtaining the outcomes of the joint measurements on the input states and shared state, they calculate the payoff with the function specified by Eq. (A18) to verify the shared state.

As for the sample efficiency, it can be derived that  $\bar{q} = \frac{1}{d(d+1)}$  for this strategy. Hence, the number of required measurements is  $N(\varepsilon, \delta) \approx \frac{d+1}{d\varepsilon} \ln \delta^{-1}$ , which coincides with the best standard QSV strategy for this class of state.

### 8. MDI-QSV of two-qubit pure states

Consider a two-qubit pure state  $|\psi(\theta)\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$  [ $\theta \in (0, \pi/2)$ ]. By employing the decomposition proposed in Eq. (A16), an MDI-QSV strategy  $\mathcal{S}_{\psi(\theta)}$  can be designed using Proposition 1. Define two sets of states  $\{|\phi_i\rangle\}_{i=1}^4$  and  $\{|\varphi_i\rangle_{i=1}^4\}$ , where

$$\begin{aligned} |\phi\rangle_1 &= \cos\theta|0\rangle - \sin\theta|1\rangle, & |\phi\rangle_2 &= \cos\theta|0\rangle + \sin\theta|1\rangle, \\ |\phi\rangle_3 &= \sin\theta|0\rangle - \cos\theta|1\rangle, & |\phi\rangle_4 &= \sin\theta|0\rangle + \cos\theta|1\rangle, \\ |\varphi\rangle_1 &= \cos\theta|0\rangle - i\sin\theta|1\rangle, & |\varphi\rangle_2 &= \cos\theta|0\rangle + i\sin\theta|1\rangle, \\ |\varphi\rangle_3 &= \sin\theta|0\rangle - i\cos\theta|1\rangle, & |\varphi\rangle_4 &= \sin\theta|0\rangle + i\cos\theta|1\rangle. \end{aligned} \quad (\text{A48})$$

TABLE III. Input set of the MDI-QSV strategy  $\mathcal{S}_{\psi(\theta)}$  for  $|\psi(\theta)\rangle$ .

Input state		Input probability
Alice	Bob	
$ 0\rangle/ 1\rangle$	$ 0\rangle/ 1\rangle$	1/12
$ +\rangle/ -\rangle$	$\{ \phi_i\rangle\}_{i=1}^4$	1/24
$ +\rangle/ -i\rangle$	$\{ \varphi_i\rangle_{i=1}^4\}$	1/24

The input set of this strategy is given in Table III. Then, combined with the payoff function defined via Eq. (A18), it is found that the parameter  $\bar{q}$  is

$$\bar{q} = \begin{cases} 1/6, & \theta = \pi/4 \\ 1/12, & \theta \neq \pi/4 \end{cases}. \quad (\text{A49})$$

Therefore, the sample efficiency of this class of strategies is  $3/2\varepsilon^{-1} \ln \delta^{-1}$  for Bell states and  $3\varepsilon^{-1} \ln \delta^{-1}$  for any other pure entangled states.

#### a. Optimality of the proposed strategy

It has been pointed out that  $[\mathbb{1}_4 - |\psi(\theta)\rangle\langle\psi(\theta)|]/3$  admits many possible decompositions into the summation of product states. As we will show, the one proposed in Eq. (A16) is the optimal choice for constructing the MDI-QSV strategy in the two-qubit case.

Suppose that a product state  $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$  appears in the decomposition of  $[\mathbb{1}_4 - |\psi(\theta)\rangle\langle\psi(\theta)|]/3$ , such that the equation

$$\langle\psi(\theta)|(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = 0 \quad (\text{A50})$$

holds. As discussed in Sec. A5 before Lemma 5, the sample efficiency is directly related to the number of valid events. That is, the number of pairs  $(a, b)$  satisfying

$$\langle\psi(\theta)|U_a \otimes U_b(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = 0 \quad (\text{A51})$$

should be as large as possible, and here the set  $\{U_a\}$  is just the Pauli matrices  $\{I, X, Y, Z\}$  in the qubit case. When  $|\psi(\theta)\rangle$  is not maximally entangled ( $\theta \neq \pi/4$ ), it is direct to check that Eq. (A51) holds if and only if  $U_a \otimes U_b$  can be decomposed into  $(U_{a_1} \otimes U_{b_1})(U_{a_2} \otimes U_{b_2})$  such that

$$U_{a_1} \otimes U_{b_1} |\psi(\theta)\rangle = e^{i\xi} |\psi(\theta)\rangle \quad (\text{A52})$$

and

$$\begin{aligned} U_{a_2} \otimes U_{b_2} (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \\ = e^{i\xi'} (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \end{aligned} \quad (\text{A53})$$

are satisfied for some  $\xi$  and  $\xi'$ . The first constraint is satisfied when  $U_{a_1} \otimes U_{b_1}$  is  $I \otimes I$  or  $Z \otimes Z$ , independent of the explicit  $\theta$ , while the second constraint becomes state dependent. Ignoring the trivial case  $U_{a_2} \otimes U_{b_2} = I \otimes I$ , we can suppose that  $U_{a_2} \in \{X, Y, Z\}$  without loss of generality. Then, the constraint in Eq. (A53) holds only if  $\alpha_1|0\rangle + \beta_1|1\rangle$  is the eigenstate of  $U_{a_2}$ . Once the  $\alpha_1|0\rangle + \beta_1|1\rangle$  is given,  $\alpha_2|0\rangle + \beta_2|1\rangle$  is uniquely determined by the orthogonality requirement in Eq. (A50), and it is observed that  $U_{b_2}$  has to be  $I$  to meet the constraint (A53). Consequently, this leads to an

optimal decomposition of  $[\mathbb{1}_4 - |\psi(\theta)\rangle\langle\psi(\theta)|]/3$  to construct an MDI-QSV strategy for a two-qubit pure entangled state using Proposition 1, which is just the decomposition given in Eq. (A16).

As our discussion here has a prerequisite that the target ensemble  $\{\rho_{ab}^0\}$  is generated from BSMs, the above analysis is sufficient to show that  $\mathcal{S}_{\psi(\theta)}$  is optimal under this prerequisite, while it remains open whether other joint measurements can induce more efficient MDI-QSV strategies.

### b. Modification of MDI-QSV with partial Bell state measurements

In practice, the parties may be only accessible to partial Bell state measurements. A typical case is the linear optics schemes, where only two out of the four Bell states can be recognized. Note that the two recognized Bell states can be modulated by changing the local basis of BSM. So, we can take them as  $\{(|00\rangle + |11\rangle)/\sqrt{2}, (|01\rangle + |10\rangle)/\sqrt{2}\}$  without loss of generality. The measurement outcome of such partial Bell state measurements is denoted as  $\{0, 1, \star\}$ , respectively, where  $\star$  means that the BSM fails at this round. To guarantee the target state can always pass the test, one has to label the entire event as “pass” if at least one BSM fails. Therefore, the target ensemble that is nontrivial in the modified scenario reduces to

$$\{(U_a \otimes U_b)|\psi(\theta)\rangle\langle\psi(\theta)|(U_a \otimes U_b)^\dagger\}_{U_a, U_b=I, X}. \quad (\text{A54})$$

However, the same ensemble can also be generated by the maximally entangled state  $(|00\rangle + |11\rangle)/\sqrt{2}$ , if the joint measurements used by Alice and Bob are partial BSM and

$$\{|\psi(\theta)\rangle\langle\psi(\theta)|, |\phi(\theta)\rangle\langle\phi(\theta)|, \star\}, \quad (\text{A55})$$

respectively, with  $|\phi(\theta)\rangle = \sin\theta|01\rangle + \cos\theta|10\rangle$ . This prevents Alice and Bob from verifying the target state in an MDI manner.

An intuitive way to get around this problem is postselection. That is, Alice and Bob just conclude that the shared state can be prepared into  $|\psi(\theta)\rangle$  by the local isometry  $\Phi_0$  in Fig. 5 when the measurement outcomes  $(a, b)$  satisfy  $a, b \neq \star$ . However, such a statement may not be satisfactory, because such postselection can exclude many useful states. Let  $\theta = \pi/4$  and the verifiers can observe that all the  $n$  rounds of test give the pass outcome. They can only verify that  $n/4$  pairs of Bell state can be extracted in this postselection process. This leads to a waste of useful resources.

As another solution to tackle with the problem caused by the partial BSM, one may introduce an extra assumption that the underlying Hilbert space dimension of the shared state is known, which is justified in many practical cases. Then, the verifiers can apply trusted random rotations  $U_i \otimes U_j$  before the partial joint measurement ( $U_i = I, X, Y, Z$ ). Denote the unknown partial joint measurement as  $\{P_1, P_2, \star\}$ . Then, the overall system implements the following POVMs:

$$\{(U_i \otimes U_j)P_1(U_i \otimes U_j)^\dagger/16, (U_i \otimes U_j)P_2(U_i \otimes U_j)^\dagger/16, \star\}_{i,j}, \quad (\text{A56})$$

which is, however, complete up to normalization, as  $\sum_{i,j}(U_i \otimes U_j)P_1(U_i \otimes U_j) \propto \mathbb{1}_4$  is satisfied for any projector  $P_1$ . By employing this overall POVM in MDI-QSV, the results in Propositions 1 and 2 become viable again for

constructing an MDI-QSV strategy and calculating the sample efficiency. Consequently, one can verify  $|\psi(\theta)\rangle$  using around  $12\varepsilon^{-1} \ln \delta^{-1}$  copies of shared states if  $\theta \neq \pi/4$ , and  $6\varepsilon^{-1} \ln \delta^{-1}$  copies if  $\theta = \pi/4$ , which is exactly four times compared to the above strategy  $\mathcal{S}_{\psi(\theta)}$ .

Notably, with the dimension of shared state given and trusted local rotations available, the modified strategy is applicable as long as at least one Bell state can be recognized. And, the inefficiency directly depends on the proportion of success of all the joint measurements. This result also admits a straightforward generalization to higher dimensions.

## APPENDIX B: MDI-QSV IN MULTIPARTITE CASE

In a general case, where  $n$  remote parties aim at verifying the shared state in an MDI manner with the help of trusted local quantum inputs  $\tau_i^1 \otimes \tau_i^2 \cdots \otimes \tau_i^n$ , our results in the bipartite case admit a natural generalization.

As for MDI-QSV strategies construction, we can still design an NFN one for some  $n$ -partite  $d$ -level pure target state  $\rho_{\psi_{n,d}} = |\psi_{n,d}\rangle\langle\psi_{n,d}|$  in three steps, following a similar line as in the bipartite case:

(1) Construct a standard QSV strategy  $\Omega_{\psi_{n,d}}$  with only rank-1 projective local measurements for  $\rho_{\psi_{n,d}}^T$ , which specifies an input set  $\mathcal{J}_{\psi_{n,d}}$ . To guarantee the resulting MDI-QSV strategy has no false negative, it is further required that  $\text{Tr}(\Omega_{\psi_{n,d}} \rho_{\psi_{n,d}}^T) = 0$ .

(2) Symmetrize the input set with the set of operators  $\{\otimes_{k=1}^n U_{a_k}\}$ , which results in

$$\begin{aligned} \mathcal{J}_{\psi_{n,d}}^{\text{sym}} &= \cup_{a_1, \dots, a_n} (\otimes_{k=1}^n U_{a_k})^\dagger \mathcal{J}_{\psi_{n,d}} / d^n (\otimes_{k=1}^n U_{a_k}) \\ &:= \{p_i, \tau_i^1 \otimes \tau_i^2 \cdots \otimes \tau_i^n\}. \end{aligned} \quad (\text{B1})$$

(3) For every input state  $\tau_i^1 \otimes \tau_i^2 \cdots \otimes \tau_i^n$  in  $\mathcal{J}_{\psi_{n,d}}^{\text{sym}}$ , the payoff function is given by

$$f_{\mathcal{J}_{\psi_{n,d}}^{\text{sym}}}(\vec{a}, i) = \begin{cases} 1, & \text{if } \text{Tr}[(\tau_i^1 \otimes \tau_i^2 \cdots \otimes \tau_i^n) \rho_{\vec{a}}] = 0. \\ 0, & \text{other cases} \end{cases}. \quad (\text{B2})$$

Here,  $\vec{a} = (a_1, a_2, \dots, a_n) \in \{0, 1, \dots, d^2 - 1\}^{\otimes n}$  is the vector denoting the outcome of each verifier, and

$$\rho_{\vec{a}} = |\psi_{\vec{a}}\rangle\langle\psi_{\vec{a}}| = (\otimes_{i=1}^n U_{a_i}) \rho_{\psi_{n,d}}^T (\otimes_{i=1}^n U_{a_i})^\dagger. \quad (\text{B3})$$

Note that the QSV strategy in the first step is not specified to be  $\frac{1}{d^n-1}(\mathbb{1}_{d^n} - \rho_{\psi_{n,d}}^T)$  as in the bipartite case. In fact, it remains open whether  $\frac{1}{d^n-1}(\mathbb{1}_{d^n} - \rho_{\psi_{n,d}}^T)$  is fully separable for all  $|\psi_{n,d}\rangle$ , so as to be implementable with local quantum inputs.

As for the sample efficiency of this class of MDI-QSV strategies, a similar discussion to the bipartite case gives that the required number of measurements in the multipartite case is

$$N \geq N_{\mathcal{S}_{\psi_{n,d}}}(\varepsilon, \delta) \approx \frac{1}{d^n \bar{q}_{n,d} \varepsilon} \ln \delta^{-1}, \quad (\text{B4})$$

with  $\bar{q}_{n,d}$  being the minimum nonzero eigenvalue of

$$\tilde{\Omega}_{\vec{a}, \psi_{n,d}} = \sum_i p_i f_{\mathcal{J}_{\psi_{n,d}}^{\text{sym}}}(\vec{a}, i) \tau_i^1 \otimes \tau_i^2 \cdots \otimes \tau_i^n. \quad (\text{B5})$$



### 1. MDI-QSV of single-qudit pure state

A special case is  $n = 1$ , i.e., the MDI-QSV for a single qudit, which is a trivial task to some extent as mentioned in the main text. In fact, as all the single-qudit pure states are equivalent to each other under local unitary operation, the single-qudit MDI-QSV is in fact verifying whether the shared state is pure. In this case, the above results are still valid, and it suffices to consider the MDI-QSV of  $|0\rangle$  in the  $d$ -dimensional Hilbert space.

Following the above three steps, a simple MDI-QSV strategy can be designed. First, the optimal QSV strategy for  $|0\rangle$  is nothing but  $(\mathbb{1}_d - |0\rangle\langle 0|)/(d-1)$ , which specifies a set of inputs as  $\{1/(d-1), |i\rangle\langle i|\}_{i=1}^{d-1}$ . After symmetrizing this set with the Heisenberg-Weyl operators  $\{U_a\}_{a=0}^{d^2-1}$ , the input set finally becomes  $\{1/d, |i\rangle\langle i|\}_{i=0}^{d^2-1}$ . That is, the verifier just needs to randomly choose a state from the computational basis as the input at each round. Finally, the payoff function is defined by Eq. (B2) as

$$f(a, i) = \begin{cases} 1, & \text{if } \text{Tr}[U_a(|i\rangle\langle i|)U_a^\dagger|0\rangle\langle 0|] = 0 \\ 0, & \text{other cases} \end{cases}. \quad (\text{B6})$$

According to Eqs. (B4) and (B5), one has  $\bar{q} = 1/d$ , and the sample efficiency of the MDI-QSV of the single-qudit pure state is  $\varepsilon^{-1} \ln \delta^{-1}$  for this strategy. This is the same as the optimal standard QSV strategy for  $|0\rangle$ , by performing the projective measurement  $\{|0\rangle\langle 0|, \mathbb{1}_d - |0\rangle\langle 0|\}$ .

### 2. MDI-QSV of stabilizer states

As another example, we consider the MDI-QSV of stabilizer states, which is a class of important multipartite entangled states in quantum communication and computation tasks. Let  $|G_n\rangle$  be an  $n$ -qubit stabilizer state, and  $\{S_i\}_{i=1}^{2^n}$  be the set of all  $2^n$  stabilizers of the target state  $|G_n\rangle$ , such that

$$|G_n\rangle\langle G_n| = \frac{1}{2^n} \sum_{i=1}^{2^n} S_i. \quad (\text{B7})$$

Without loss of generality, it is assumed that all the  $S_i$  are tensor products of the Pauli operators  $X, Y, Z$ , and the identity operator  $I$ . Then, one has

$$\mathbb{1}_{2^n} - (|G_n\rangle\langle G_n|)^T = \frac{1}{2^n} \sum_{i=1}^{2^n} (\mathbb{1}_{2^n} - S_i^T). \quad (\text{B8})$$

As  $(\mathbb{1}_{2^n} - S_i^T)$  is fully separable,  $\Omega_{G_n} = \frac{1}{2^n-1}[\mathbb{1}_{2^n} - (|G_n\rangle\langle G_n|)^T]$  admits a decomposition into fully separable states. Following a similar line as the proof of Lemma 2, it is known that  $\Omega_{G_n}$  is the optimal standard QSV strategy of  $(|G_n\rangle\langle G_n|)^T$  involving only fully separable projectors. Denote  $\mathcal{B}_i$  as the fully separable basis specified by  $S_i^T$  and  $\mathcal{B}_i^-$  as the subset spanning the negative eigenspace of  $S_i^T$ . It is observed that the  $\cup_i \mathcal{B}_i^-$  provide a decomposition of  $\Omega_{G_n}$ . Moreover, let

TABLE IV. Input set of MDI-QSV strategy for three-qubit GHZ state.

Input state			Input probability
Alice	Bob	Charlie	
$ 0\rangle/ 1\rangle$	$ 0\rangle/ 1\rangle$	$ 0\rangle/ 1\rangle$	3/56
$ +\rangle/ -\rangle$	$ +\rangle/ -\rangle$	$ +\rangle/ -\rangle$	1/56
$ +i\rangle/ -i\rangle$	$ +i\rangle/ -i\rangle$	$ +\rangle/ -\rangle$	1/56
$ +i\rangle/ -i\rangle$	$ +\rangle/ -\rangle$	$ +i\rangle/ -i\rangle$	1/56
$ +\rangle/ -\rangle$	$ +i\rangle/ -i\rangle$	$ +i\rangle/ -i\rangle$	1/56

$|e_j^i\rangle$  be a state vector in the basis  $\mathcal{B}_i$ ; any local Pauli operators will just transform it into another vector  $|e_{j'}^i\rangle$  in the same basis  $\mathcal{B}_i$ , but cannot change it into another basis  $\mathcal{B}_{i'}$ .

Based on these observations, one can apply the above construction of the MDI-QSV strategy, starting from the QSV strategy  $\Omega_{G_n}$ . The final input set can be implemented in two steps: (1) The verifiers randomly specify a stabilizer  $S_i$ . The operator  $S_i^T$  defines a fully separable basis  $\mathcal{B}_i$ . (2) The verifiers communicate to randomly choose an eigenstate under this basis  $\mathcal{B}_i$ , and locally prepare this state as the input for this round. With this input set, and the payoff function determined again by Eq. (B2), one arrives at an MDI-QSV strategy the stabilizer state  $|G_n\rangle$ .

Additionally, we remark that the fully separable basis  $\mathcal{B}_i$  specified by  $S_i$  may not be unique, if  $S_i$  contains identity operator  $I$  at some qubits. In fact, the stabilizers  $S_j$  and  $S_{j'}$  can share a common fully separable basis if they locally commute to each other. In this way, if the set of all stabilizers can be grouped into  $m$  subsets such that the stabilizers in the same set are locally commutative with each other, it will be sufficient for the verifiers to take their input states from  $m$  different basis. This helps to reduce the experimental complexity.

For this class of strategies, the factor  $\bar{q}_{2,d}$  can be calculated by Eq. (B5) as  $\bar{q}_{2,d} = \frac{2^{n-1}}{2^n-1}$ . Therefore, the required number of measurements will be  $N_{S_{|G_n}}(\varepsilon, \delta) \approx \frac{2^n-1}{2^n-1\varepsilon} \ln \delta^{-1}$ , which is nearly optimal and is independent of system size. As an explicit instance, we consider the MDI-QSV of the three-qubit GHZ state  $|GHZ_3\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$  to illustrate the construction. The set of all its stabilizers  $\{ZZI, ZIZ, IZZ, XXX, YYX, YXY, XYY\}$ , except for  $III$ , is grouped into five subsets,

$$\{ZZI, ZIZ, IZZ\}, \{XXX\}, \{YYX\}, \{YXY\}, \{XYY\}, \quad (\text{B9})$$

such that the operators inside every subset are locally commutative with each other. Then, we obtain five fully separable bases define by  $\{ZZZ, XXX, YYX, YXY, XYY\}$ . By decomposing the operator  $(\mathbb{1}_8 - |GHZ_3\rangle\langle GHZ_3|)$  into fully separable states under these five bases as a set of input states, and applying local Pauli operators to symmetrize the obtained set, it can be checked that the input set is constructed as shown in Table IV. And, the payoff function is decided accordingly once the input set is determined.

[1] E. Chitambar and G. Gour, Quantum resource theories, *Rev. Mod. Phys.* **91**, 025001 (2019).

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state

- via dual classical and Einstein-Podolsky-Rosen channels, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [5] C. L. Degen, F. Reinhard, and P. Cappellaro, Quantum sensing, *Rev. Mod. Phys.* **89**, 035002 (2017).
- [6] R. P. Feynman, Simulating physics with computers, *Int. J. Theor. Phys.* **21**, 467 (1982).
- [7] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, Measurement-based quantum computation, *Nat. Phys.* **5**, 19 (2009).
- [8] J. Preskill, Quantum computing in the NISQ era and beyond, *Quantum* **2**, 79 (2018).
- [9] M. Kliesch and I. Roth, Theory of quantum system certification, *PRX Quantum* **2**, 010201 (2021).
- [10] M. Paris and J. Rehacek, *Quantum State Estimation* (Springer Science & Business Media, Berlin, 2004), Vol. 649.
- [11] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, *Rev. Mod. Phys.* **81**, 865 (2009).
- [12] O. Gühne and G. Tóth, Entanglement detection, *Phys. Rep.* **474**, 1 (2009).
- [13] N. Friis, G. Vitagliano, M. Malik, and M. Huber, Entanglement certification from theory to experiment, *Nat. Rev. Phys.* **1**, 72 (2019).
- [14] A. Dimić and B. Dakić, Single-copy entanglement detection, *npj Quantum Inf.* **4**, 11 (2018).
- [15] V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, and B. Dakić, Experimental few-copy multipartite entanglement detection, *Nat. Phys.* **15**, 935 (2019).
- [16] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Quantum certification and benchmarking, *Nat. Rev. Phys.* **2**, 382 (2020).
- [17] M. Hayashi, K. Matsumoto, and Y. Tsuda, A study of LOCC-detection of a maximally entangled state using hypothesis testing, *J. Phys. A: Math. Gen.* **39**, 14427 (2006).
- [18] M. Hayashi, Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing, *New J. Phys.* **11**, 043028 (2009).
- [19] S. Pallister, N. Linden, and A. Montanaro, Optimal verification of entangled states with local measurements, *Phys. Rev. Lett.* **120**, 170502 (2018).
- [20] X.-D. Yu, J. Shang, and O. Gühne, Statistical methods for quantum state verification and fidelity estimation, *Adv. Quantum Technol.* **5**, 2100126 (2022).
- [21] J. Morris, V. Saggio, A. Gočanin, and B. Dakić, Quantum verification and estimation with few copies, *Adv. Quantum Technol.* **5**, 2100118 (2022).
- [22] X.-D. Yu, J. Shang, and O. Gühne, Optimal verification of general bipartite pure states, *npj Quantum Inf.* **5**, 112 (2019).
- [23] K. Wang and M. Hayashi, Optimal verification of two-qubit pure states, *Phys. Rev. A* **100**, 032315 (2019).
- [24] Z. Li, Y.-G. Han, and H. Zhu, Efficient verification of bipartite pure states, *Phys. Rev. A* **100**, 032316 (2019).
- [25] Z. Li, Y.-G. Han, and H. Zhu, Optimal verification of Greenberger-Horne-Zeilinger states, *Phys. Rev. Appl.* **13**, 054002 (2020).
- [26] N. Dangniam, Y.-G. Han, and H. Zhu, Optimal verification of stabilizer states, *Phys. Rev. Res.* **2**, 043323 (2020).
- [27] Z. Li, Y.-G. Han, H.-F. Sun, J. Shang, and H. Zhu, Verification of phased Dicke states, *Phys. Rev. A* **103**, 022601 (2021).
- [28] H. Zhu and M. Hayashi, Efficient verification of pure quantum states in the adversarial scenario, *Phys. Rev. Lett.* **123**, 260504 (2019).
- [29] H. Zhu and M. Hayashi, General framework for verifying pure quantum states in the adversarial scenario, *Phys. Rev. A* **100**, 062335 (2019).
- [30] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [31] A. Gočanin, I. Šupić, and B. Dakić, Sample-efficient device-independent quantum state verification and certification, *PRX Quantum* **3**, 010317 (2022).
- [32] D. Mayers and A. Yao, Self testing quantum apparatus, *Quantum Inf. Comput.* **4**, 273 (2004).
- [33] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, *Quantum* **4**, 337 (2020).
- [34] Y.-G. Han, Z. Li, Y. Wang, and H. Zhu, Optimal verification of the Bell state and Greenberger-Horne-Zeilinger states in untrusted quantum networks, *npj Quantum Inf.* **7**, 164 (2021).
- [35] A. Unnikrishnan and D. Markham, Verification of graph states in an untrusted network, *Phys. Rev. A* **105**, 052420 (2022).
- [36] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, Measurement-device-independent entanglement witnesses for all entangled quantum states, *Phys. Rev. Lett.* **110**, 060405 (2013).
- [37] Z.-D. Li, Q. Zhao, R. Zhang, L.-Z. Liu, X.-F. Yin, X. Zhang, Y.-Y. Fei, K. Chen, N.-L. Liu, F. Xu, Y.-A. Chen, L. Li, and J.-W. Pan, Measurement-device-independent entanglement witness of tripartite entangled states and its applications, *Phys. Rev. Lett.* **124**, 160503 (2020).
- [38] I. Šupić, M. J. Hoban, L. D. Colomer, and A. Acín, Self-testing and certification using trusted quantum inputs, *New J. Phys.* **22**, 073006 (2020).
- [39] F. Buscemi, All entangled quantum states are nonlocal, *Phys. Rev. Lett.* **108**, 200401 (2012).
- [40] A local isometry  $\Phi$  on  $\sigma$  is realized by adding local ancillas and applying local unitaries. Taking the bipartite case as an example, a local isometry is formulated as
- $$\Phi(\sigma^{AB}) = (U^{AA'} \otimes U^{BB'})[|00\rangle^{A'B'} \langle 00| \otimes \sigma^{AB}](U^{AA'} \otimes U^{BB'})^\dagger,$$
- where the local ancilla is denoted by  $|00\rangle^{A'B'}$ . And, one says that the  $\sigma^{AB}$  is equivalent to target state  $|\psi\rangle$ , if there exists a local isometry such that
- $$\Phi(\sigma^{AB}) = \rho_\psi^{A'B'} \otimes \rho_{\text{junk}}^{AB},$$
- where  $\rho_{\text{junk}}^{AB}$  is some junk state. Here, we omit the junk state and simply write  $\Phi(\sigma) = \rho_\psi$  for convenience.
- [41] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, Device-independent state estimation based on Bell's inequalities, *Phys. Rev. A* **80**, 062327 (2009).
- [42] J. Kaniewski, Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities, *Phys. Rev. Lett.* **117**, 070402 (2016).

- [43] H. Chernoff, A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, *Ann. Math. Stat.* **23**, 493 (1952).
- [44] W. Hoeffding, Probability inequalities for sums of bounded random variables, *J. Am. Stat. Assoc.* **58**, 13 (1963).
- [45] In the  $d$ -dimensional case, the generalized Pauli “phase” and “shift” operators  $Z_d$  and  $X_d$  are defined as  $Z_d = \sum_{m=0}^{d-1} e^{i2m\pi/d} |m\rangle\langle m|$ ,  $X_d = \sum_{m=0}^{d-1} |m\rangle\langle m+1|$ . They generate the group of Heisenberg-Weyl operators  $\{U_j\}_{j=0}^{d^2-1}$ , with  $U_j = X_d^k Z_d^l$ , where  $k = \lfloor j/d \rfloor$ ,  $l = j \bmod d$ .
- [46] W.-H. Zhang, C. Zhang, Z. Chen, X.-X. Peng, X.-Y. Xu, P. Yin, S. Yu, X.-J. Ye, Y.-J. Han, J.-S. Xu, G. Chen, C.-F. Li, and G.-C. Guo, Experimental optimal verification of entangled states using local measurements, *Phys. Rev. Lett.* **125**, 030506 (2020).
- [47] X. Jiang, K. Wang, K. Qian, Z. Chen, Z. Chen, L. Lu, L. Xia, F. Song, S. Zhu, and X. Ma, Towards the standardization of quantum state verification using optimal strategies, *npj Quantum Inf.* **6**, 90 (2020).
- [48] W.-H. Zhang, X. Liu, P. Yin, X.-X. Peng, G.-C. Li, X.-Y. Xu, S. Yu, Z.-B. Hou, Y.-J. Han, J.-S. Xu *et al.*, Classical communication enhanced quantum state verification, *npj Quantum Inf.* **6**, 103 (2020).
- [49] D. Gottesman, Stabilizer codes and quantum error correction, Ph.D. thesis, California Institute of Technology, 1997.
- [50] O. Gühne, C.-Y. Lu, W.-B. Gao, and J.-W. Pan, Toolbox for entanglement detection and fidelity estimation, *Phys. Rev. A* **76**, 030305(R) (2007).
- [51] S. T. Flammia and Y.-K. Liu, Direct fidelity estimation from few Pauli measurements, *Phys. Rev. Lett.* **106**, 230501 (2011).
- [52] V. Vedral, The role of relative entropy in quantum information theory, *Rev. Mod. Phys.* **74**, 197 (2002).
- [53] P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, *Phys. Lett. A* **232**, 333 (1997).
- [54] M. Horodecki, P. Horodecki, and R. Horodecki, Separability of mixed states: Necessary and sufficient conditions, *Phys. Lett. A* **223**, 1 (1996).
- [55] G. Vidal and R. Tarrach, Robustness of entanglement, *Phys. Rev. A* **59**, 141 (1999).