ARTICLE OPEN

Robust and efficient verification of graph states in blind measurement-based quantum computation

Zihao Li[1,2,3], Huangjun Zhu[1,2,3]✉ and Masahito Hayashi[4,5,6]✉

Blind quantum computation (BQC) is a secure quantum computation method that protects the privacy of clients. Measurement-based quantum computation (MBQC) is a promising approach for realizing BQC. To obtain reliable results in blind MBQC, it is crucial to verify whether the resource graph states are accurately prepared in the adversarial scenario. However, previous verification protocols for this task are too resource-consuming or noise-susceptible to be applied in practice. Here, we propose a robust and efficient protocol for verifying arbitrary graph states with any prime local dimension in the adversarial scenario, which leads to a robust and efficient protocol for verifying the resource state in blind MBQC. Our protocol requires only local Pauli measurements and is thus easy to realize with current technologies. Nevertheless, it can achieve optimal scaling behaviors with respect to the system size and the target precision as quantified by the infidelity and significance level, which has never been achieved before. Notably, our protocol can exponentially enhance the scaling behavior with the significance level.

npj Quantum Information (2023)9:115 ; https://doi.org/10.1038/s41534-023-00783-9

INTRODUCTION

Quantum computation offers the promise of exponential speedups over classical computation on a number of important problems[1–3]. However, it is very challenging to realize practical quantum computation in the near future, especially for clients with limited quantum computational power. Blind quantum computation (BQC)[4] is an effective method that enables such a client to delegate his (her) computation to a server, which is capable of performing quantum computation, without leaking any information about the computation task. So far, various protocols of BQC have been proposed in theory[5–8] and demonstrated in experiments[9–12]. Many of these protocols build on the model of measurement-based quantum computation (MBQC)[13–15], in which graph states are used as resources and local projective measurements on qudits are used to drive the computation.

To realize BQC successfully, it is crucial to protect the privacy of the client and verify the correctness of the computation results. The latter task, known as verification of BQC, has been studied in various models as explained in the Methods section, among which MBQC in the receive-and-measure setting is particularly convenient[16–21]. However, it is extremely challenging to construct robust and efficient verification protocols, especially for noisy, intermediate-scale quantum (NISQ) devices[3,22,23]. Actually, this problem lies at the heart of the active research field of quantum characterization, verification, and validation (QCVV)[24–29].

In this work, we focus on the problem of verifying the resource graph states in the following adversarial scenario[16,30,31], which is crucial to the verification of blind MBQC in the receive-and-measure setting[6,16–21]: Alice is a client (verifier) who can only perform single-qudit projective measurements with a trusted measurement device, and Bob is a server (prover) who can prepare arbitrary quantum states. In order to perform MBQC, Alice delegates the preparation of the n-qudit graph state $|G\rangle \in \mathcal{H}$ to Bob, who then prepares a quantum state ρ on the whole space $\mathcal{H}^{\otimes(N+1)}$ and sends it to Alice qudit by qudit. If Bob is honest, then he is supposed to prepare $N+1$ copies of $|G\rangle$; while if he is malicious, then he can mess up the computation of Alice by generating an arbitrary correlated or even entangled state ρ. To obtain reliable computation results, Alice needs to verify the resource state prepared by Bob with suitable tests on N systems, where each test is a binary measurement on a single-copy system. If the test results satisfy certain conditions, then the conditional reduced state on the remaining system is close to the target state $|G\rangle$ and can be used for MBQC; otherwise, the state is rejected. Since there is no communication from Alice to Bob after the preparation of the state ρ, the information-theoretic blindness is guaranteed by the no-signaling principle[6].

The assumption that the client can perform reliable local projective measurements can be justified as follows. First, the measurement devices are controlled by Alice in her laboratory and are not affected by the adversary. So it is reasonable to assume that the measurement devices are trustworthy. Second, in practice, Alice can calibrate and verify her measurement devices before performing blind MBQC, and the resource costs of these operations are independent of the complexity of the quantum computation and the qudit number of the resource graph state. If high-quality measurements can be certified after calibration and verification, then Alice can safely use them to verify the graph state and perform blind MBQC.

As pointed out above, the verification of the resource graph state in the adversarial scenario[16,30,31] is a crucial and challenging part in the verification of blind MBQC. A valid verification protocol in the adversarial scenario has to meet the basic requirements of completeness and soundness[16,20,31]. The completeness means Alice does not reject the ideal graph state $|G\rangle$. Intuitively, the verification protocol is sound if Alice does not mistakenly accept any bad state that is far from the ideal state $|G\rangle$. Concretely, the soundness means the following: once accepting, Alice needs to

[1] State Key Laboratory of Surface Physics and Department of Physics, Fudan University, Shanghai 200433, China. [2] Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China. [3] Center for Field Theory and Particle Physics, Fudan University, Shanghai 200433, China. [4] School of Data Science, The Chinese University of Hong Kong, Longgang District, Shenzhen 518172, China. [5] International Quantum Academy (SIQA), Futian District, Shenzhen 518048, China. [6] Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan. ✉email: zhuhuangjun@fudan.edu.cn; hmasahito@cuhk.edu.cn

Table 1. Comparison of various protocols for verifying the resource states of blind MBQC in the adversarial scenario.

Protocol	This paper	Ref. [31]	Ref. [33]	Ref. [17]	Ref. [16]	Refs. [18,20,21,32]
Is the scaling optimal in n?	Yes	Yes	No	Yes	Yes	No
Is the scaling optimal in ϵ?	Yes	Yes	Yes	Yes	Yes	The choice of ϵ is restricted
Is the scaling optimal in δ?	Yes	Yes	Yes	No	No	The choice of δ is restricted
Is it robust to noise?	Yes	No	No	Yes*	No	No

Here n is the qubit (qudit) number of the resource graph state; ϵ and δ denote the target infidelity and significance level, respectively. The optimal scaling behaviors of the test number N in n, ϵ, and δ are $O(1)$, $O(\epsilon^{-1})$, and $O(\ln\delta^{-1})$, respectively. By 'robust to noise' we mean the verifier Alice can accept with a high probability if the state prepared has a sufficiently high fidelity. The robustness achieved in ref. [17] is different from the current definition. The scaling behaviors with respect to ϵ and δ are not clear for protocols in refs. [18,20,21,32]. See Supplementary Note 3 for details.

ensure with a high confidence level $1-\delta$ that the reduced state for MBQC has a sufficiently high fidelity (at least $1-\epsilon$) with $|G\rangle$. Here $0<\delta\leq 1$ is called the significance level and the threshold $0<\epsilon<1$ is called the target infidelity. The two parameters specify the target verification precision. The efficiency of a protocol is characterized by the number N of tests needed to achieve a given precision. Under the requirements of completeness and soundness, the optimal scaling behaviors of N with respect to ϵ, δ, and the qudit number n of $|G\rangle$ are $O(\epsilon^{-1})$, $O(\ln\delta^{-1})$, and $O(1)$, respectively, as explained in the Results section. However, it is highly nontrivial to construct efficient verification protocols in the adversarial scenario. Although various protocols have been proposed[16,18,20,21,31–33], most protocols known so far are too resource consuming. Even without considering noise robustness, only the protocol of refs. [30,31] achieves the optimal scaling behaviors with n, ϵ, and δ (see Table 1).

Moreover, most protocols are not robust to experimental noise: the state prepared by Bob may be rejected with a high probability even if it has a small deviation from the ideal resource state. However, in practice, it is extremely difficult to prepare quantum states with genuine multipartite entanglement perfectly. So it is unrealistic to ask honest Bob to generate the perfect resource state. On the other hand, if the deviation from the ideal state is small enough, then it is still useful for MBQC[20,32]. Therefore, a practical and robust protocol should accept nearly ideal states with a sufficiently high probability; otherwise, Alice needs to repeat the verification protocol many times to perform MBQC, which substantially increases the sample complexity. Unfortunately, no protocol known in the literature can achieve this goal.

Recently, a fault-tolerant protocol was proposed for verifying MBQC based on two-colorable graph states[17]. With this protocol, Alice can detect whether or not the given state belongs to a set of error-correctable states; then she can perform fault-tolerant MBQC on the accepted state. Although this protocol is noise-resilient to some extent, it is not very efficient (see Table 1), and is difficult to realize in the current era of NISQ devices[3,22,23] because too many physical qubits are required to encode the logical qubits. In addition, this protocol is robust only to certain correctable errors since it is based on a given error-correcting code. If the actual error is not correctable, then the probability of acceptance will decrease exponentially with the number of tests, which substantially increases the actual sample complexity.

In this work, we propose a robust and efficient protocol for verifying general qudit graph states with a prime local dimension in the adversarial scenario, which plays a crucial role in robust and efficient verification of blind MBQC. Our protocol is appealing to practical applications because it only requires stabilizer tests based on local Pauli measurements, which are easy to implement with current technologies. It is robust against arbitrary types of noise in state preparation, as long as the fidelity is sufficiently high. Moreover, our protocol can achieve optimal scaling behaviors with respect to the system size and target precision ϵ, δ, and the sample cost is comparable to the counterpart in the nonadversarial scenario as clarified in the Methods section. As far as we know, such a high efficiency has never been achieved before when robustness is taken into account. In addition to qudit graph states, our protocol can also be applied to verifying many other important quantum states in the adversarial scenario, as explained in the Discussion section. Furthermore, many technical results developed in the course of our work are also useful for studying random sampling without replacement, as discussed in the companion paper[34] (cf. the Methods section).

RESULTS

Qudit graph states

To establish our results, first, we review the definition of qudit graph states as a preliminary, where the local dimension d is a prime. Mathematically, a graph $G=(V,E,m_E)$ is characterized by a set of n vertices $V=\{1,2,\ldots,n\}$ and a set of edges E together with multiplicities specified by $m_E=(m_e)_{e\in E}$, where $m_e\in\mathbb{Z}_d$ and $\mathbb{Z}_d$ is the ring of integers modulo d, which is also a field given that d is a prime. Two distinct vertices i, j of G are adjacent if they are connected by an edge. The generalized Pauli operators X and Z for a qudit read

$$Z|j\rangle=\omega^j|j\rangle,\quad X|j\rangle=|j+1\rangle,\quad \omega=\mathrm{e}^{2\pi i/d},\tag{1}$$

where $j\in\mathbb{Z}_d$.

Given a graph $G=(V,E,m_E)$ with n vertices, we can construct an n-qudit graph state $|G\rangle\in\mathcal{H}$ as follows[33,35]: first, prepare the state $|+\rangle:=\sum_{j\in\mathbb{Z}_d}|j\rangle/\sqrt{d}$ for each vertex; then, for each edge $e\in E$, apply m_e times the generalized controlled-Z operation CZ_e on the vertices of e, where $\mathrm{CZ}_e=\sum_{k\in\mathbb{Z}_d}|k\rangle\langle k|_i\otimes Z_j^k$ if $e=(i,j)$. The resulting graph state has the form

$$|G\rangle=\left(\prod_{e\in E}\mathrm{CZ}_e^{m_e}\right)|+\rangle^{\otimes n}.\tag{2}$$

This graph state is also uniquely determined by its stabilizer group S generated by the n commuting operators $S_i:=X_i\bigotimes_{j\in V_i}Z_j^{m_{(i,j)}}$ for $i=1,2,\ldots,n$, where V_i is the set of vertices adjacent to vertex i. Each stabilizer operator in S can be written as

$$g_{\mathbf{k}}=\prod_{i=1}^{n}S_i^{k_i}=\bigotimes_{i=1}^{n}(g_{\mathbf{k}})_i,\tag{3}$$

where $\mathbf{k}:=(k_1,\ldots,k_n)\in\mathbb{Z}_d^n$, and $(g_{\mathbf{k}})_i$ denotes the local generalized Pauli operator for the ith qudit.

Strategy for testing qudit graph states

Recently, a homogeneous strategy[30,31] for testing qubit stabilizer states based on stabilizer tests was proposed in ref. [36] and generalized to the qudit case with a prime local dimension in Sec. X E of ref. [31]. Here we use a variant strategy for testing qudit graph states, which serves as an important subroutine of our verification protocol. Let S be the stabilizer group of $|G\rangle\in\mathcal{H}$ and

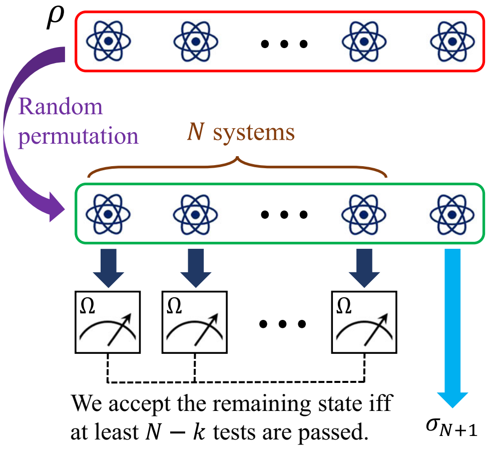

Fig. 1 Schematic view of our verification protocol. Here the state ρ generated by Bob might be arbitrarily correlated or entangled on the whole space $\mathcal{H}^{\otimes(N+1)}$. To verify the target state, Alice first randomly permutes all $N+1$ systems, and then uses a strategy Ω to test each of the first N systems. Finally, she accepts the reduced state σ_{N+1} on the remaining system iff at least $N-k$ tests are passed.

$\mathcal{D}(\mathcal{H})$ be the set of all density operators on $\mathcal{H}$. For any operator $g_{\mathbf{k}} \in S$, the corresponding stabilizer test is constructed as follows: party i measures the local generalized Pauli operator $(g_{\mathbf{k}})_i$ for $i=1$, 2, …, n, and records the outcome by an integer $o_i \in \mathbb{Z}_d$, which corresponds to the eigenvalue ω^{o_i} of $(g_{\mathbf{k}})_i$; then the test is passed if and only if the outcomes satisfy $\sum_i o_i = 0 \bmod d$. By construction, the test can be represented by a two-outcome measurement $\{P_{\mathbf{k}}, \mathbb{I}-P_{\mathbf{k}}\}$. Here $\mathbb{I}$ is the identity operator on $\mathcal{H}$;

$$P_{\mathbf{k}} = \frac{1}{d}\sum_{j\in\mathbb{Z}_d} g_{\mathbf{k}}^j \tag{4}$$

is the projector onto the eigenspace of $g_{\mathbf{k}}$ with eigenvalue 1 and corresponds to passing the test, while $\mathbb{I}-P_{\mathbf{k}}$ corresponds to the failure. It is easy to check that $P_{\mathbf{k}}|G\rangle = |G\rangle$, which means $|G\rangle$ can always pass the test. The stabilizer test corresponding to the operator $\mathbb{I}\in S$ is called the 'trivial test' since all states can pass the test with certainty.

To construct a verification strategy for $|G\rangle$, we perform all distinct tests $P_{\mathbf{k}}$ for $\mathbf{k}\in\mathbb{Z}_d^n$ randomly each with probability d^{-n}. The resulting strategy is characterized by a two-outcome measurement $\{\tilde{\Omega}, \mathbb{I}-\tilde{\Omega}\}$, which is determined by the verification operator

$$\tilde{\Omega} = \frac{1}{d^n}\sum_{\mathbf{k}\in\mathbb{Z}_d^n} P_{\mathbf{k}} = |G\rangle\langle G| + \frac{1}{d}(\mathbb{I}-|G\rangle\langle G|). \tag{5}$$

For $1/d \le \lambda < 1$, if one performs $\tilde{\Omega}$ and the trivial test with probabilities $p=\frac{d(1-\lambda)}{d-1}$ and $1-p$, respectively, then another strategy can be constructed as[30,31]

$$\Omega = p\tilde{\Omega} + (1-p)\mathbb{I} = |G\rangle\langle G| + \lambda(\mathbb{I}-|G\rangle\langle G|). \tag{6}$$

We denote by $\nu := 1-\lambda$ the spectral gap of Ω from the largest eigenvalue. This strategy plays a key role in our verification protocol introduced in the next subsection.

As shown in Supplementary Note 6A, the second equality in Eq. (5) holds whenever d is a prime, but may fail if d is not a prime. In the latter case, our strategy is no longer homogeneous in general, and many results in this work may not hold since they are based on homogeneous strategies. This is why we restrict our attention to the case of prime local dimensions.

Verification of graph states in blind MBQC

Suppose Alice intends to perform quantum computation with single-qudit projective measurements on the n-qudit graph state $|G\rangle$ generated by Bob. As shown in Fig. 1, our protocol for verifying $|G\rangle$ in the adversarial scenario runs as follows.

1. Bob produces a state ρ on the whole space $\mathcal{H}^{\otimes(N+1)}$ with $N\ge 1$ and sends it to Alice.
2. After receiving the state, Alice randomly permutes the $N+1$ systems of ρ (due to this procedure, we can assume that ρ is permutation invariant without loss of generality) and applies the strategy Ω defined in Eq. (6) to the first N systems.
3. Alice chooses an integer $0\le k\le N-1$, called the number of allowed failures. If at most k failures are observed among the N tests, Alice accepts the reduced state σ_{N+1} on the remaining system and uses it for MBQC; otherwise, she rejects it.

With this verification protocol, Alice aims to achieve three goals: completeness, soundness, and robustness. Recall that $|G\rangle$ can always pass each test, so the completeness is automatically guaranteed. The soundness is characterized by the target infidelity ϵ and significance level δ as explained in the introduction. For verification protocols working in the nonadversarial scenario, where the source only produces independent states with no correlation or entanglement among different runs, the optimal scaling behaviors of the test number N with respect to ϵ, δ, and n are $O(\epsilon^{-1})$, $O(\ln\delta^{-1})$, and $O(1)$, respectively[31,36]. The adversarial scenario studied in this work has a weaker assumption on the source[31,36], so the scaling behaviors in ϵ, δ, and n cannot be better. Although the condition of soundness looks quite simple, it is highly nontrivial to determine the degree of soundness. Even in the special case $k=0$, this problem was resolved only very recently after quite a lengthy analysis[30,31]. Unfortunately, the robustness of this protocol is poor in this special case, as we shall see later. So we need to tackle this challenge in the general case.

Most previous works did not consider the problem of robustness at all, because it is already very difficult to detect the bad case without considering robustness. To characterize the robustness of a protocol, we need to consider the case in which honest Bob prepares an independent and identically distributed (i.i.d.) quantum state, that is, ρ is a tensor power of the form $\rho=\tau^{\otimes(N+1)}$ with $\tau\in\mathcal{D}(\mathcal{H})$. Due to inevitable noise, τ may not equal the ideal state $|G\rangle\langle G|$. Nevertheless, if the infidelity $\epsilon_\tau := 1-\langle G|\tau|G\rangle$ is smaller than the target infidelity, that is, $\epsilon_\tau<\epsilon$, then τ is still useful for quantum computing. For a robust verification protocol, such a state should be accepted with a high probability.

In the i.i.d. case, the probability that Alice accepts τ reads

$$p_{N,k}^{\mathrm{iid}}(\tau) = B_{N,k}(1-\mathrm{tr}(\Omega\tau)) = B_{N,k}(\nu\epsilon_\tau), \tag{7}$$

where N is the number of tests, k is the number of allowed failures, and $B_{N,k}(p) := \sum_{j=0}^{k}\binom{N}{j}p^j(1-p)^{N-j}$ is the binomial cumulative distribution function. To construct a robust verification protocol, it is preferable to choose a large value of k, so that $p_{N,k}^{\mathrm{iid}}(\tau)$ is sufficiently high. Unfortunately, most previous verification protocols can reach a meaningful conclusion only when $k=0$[16,18,30,31,33], in which case the probability

$$p_{N,k=0}^{\mathrm{iid}}(\tau) = (1-\nu\epsilon_\tau)^N \tag{8}$$

decreases exponentially with the test number N, which is not satisfactory. These protocols need a large number of tests to guarantee soundness, so it is difficult to get accepted even if Bob is honest. Hence, previous protocols with the choice $k=0$ are not robust to noise in state preparation. Since the acceptance probability is small, Alice needs to repeat the verification protocol many times to ensure that she accepts the state τ at least once, which substantially increases the actual sample cost.

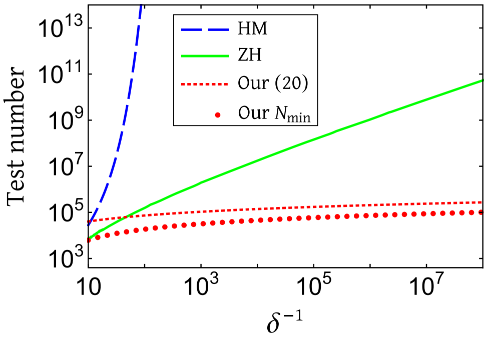

Fig. 2 Number of tests required to verify a general qudit graph state in the adversarial scenario within infidelity $\epsilon = 0.01$, significance level δ, and robustness $r = 1/2$. The red dots correspond to $N_{\rm min}(\epsilon,\delta,\lambda,r)$ in Eq. (18) with $\lambda = 1/2$, and the red dashed curve corresponds to the RHS of Eq. (20), which is an upper bound for $N_{\rm min}(\epsilon,\delta,\lambda,r)$. The blue dashed curve corresponds to the HM protocol[16], and the green solid curve corresponds to the ZH protocol[31] with $\lambda = 1/2$. The performances of the TMMMF protocol[20] and TM protocol[32] are not shown because the numbers of tests required are too large (see Supplementary Note 3).

When $\epsilon_\tau = \frac{\epsilon}{2}$ for example, the number of repetitions required is at least $\Theta\left(\exp\left[\frac{1}{4\delta}\right]\right)$ for the HM protocol in ref. [16] and $\Theta\left(\frac{1}{\sqrt{\delta}}\right)$ for the ZH protocol in refs. [30,31] (see Supplementary Note 3 for details). As a consequence, the total number of required tests is at least $\Theta\left(\frac{1}{\delta}\exp\left[\frac{1}{4\delta}\right]\right)$ for the HM protocol and $\Theta\left(\frac{\ln\delta^{-1}}{\sqrt{\delta}}\right)$ for the ZH protocol, as illustrated in Fig. 2. Therefore, although some protocols known in the literature are reasonably efficient in detecting the bad case, they are not useful in verifying the resource state of blind MBQC in a realistic scenario.

Guaranteed infidelity

Suppose ρ is permutation invariant. Then the probability that Alice accepts ρ reads

$$p_k(\rho) = \sum_{i=0}^{k}\binom{N}{i}\mathrm{tr}\left(\left[\Omega^{\otimes(N-i)}\otimes\overline{\Omega}^{\otimes i}\otimes\mathbb{I}\right]\rho\right), \tag{9}$$

where $\overline{\Omega} := \mathbb{I}-\Omega$. Denote by σ_{N+1} the reduced state on the remaining system when at most k failures are observed among the N tests. The fidelity between σ_{N+1} and the ideal state $|G\rangle$ reads $F_k(\rho) = f_k(\rho)/p_k(\rho)$ [assuming $p_k(\rho) > 0$], where

$$f_k(\rho) = \sum_{i=0}^{k}\binom{N}{i}\mathrm{tr}\left(\left[\Omega^{\otimes(N-i)}\otimes\overline{\Omega}^{\otimes i}\otimes|G\rangle\langle G|\right]\rho\right). \tag{10}$$

The actual verification precision can be characterized by the following figure of merit with $0 < \delta \le 1$,

$$\bar{\epsilon}_\lambda(k,N,\delta) := 1 - \min_{\rho}\{F_k(\rho)\,|\,p_k(\rho)\ge\delta\}, \tag{11}$$

where λ is determined by Eq. (6), and the minimization is taken over permutation-invariant states ρ on $\mathcal{H}^{\otimes(N+1)}$.

If Alice accepts the state prepared by Bob, then she can guarantee (with significance level δ) that the reduced state σ_{N+1} has infidelity at most $\bar{\epsilon}_\lambda(k,N,\delta)$ with the ideal state $|G\rangle$. Consequently, according to the relation between the fidelity and trace norm, Alice can ensure the condition[16]

$$|\mathrm{tr}(E\sigma_{N+1}) - \langle G|E|G\rangle| \le \sqrt{\bar{\epsilon}_\lambda(k,N,\delta)} \tag{12}$$

for any POVM element $0 \le E \le \mathbb{I}$; that is, the deviation of any measurement outcome probability from the ideal value is not larger than $\sqrt{\bar{\epsilon}_\lambda(k,N,\delta)}$.

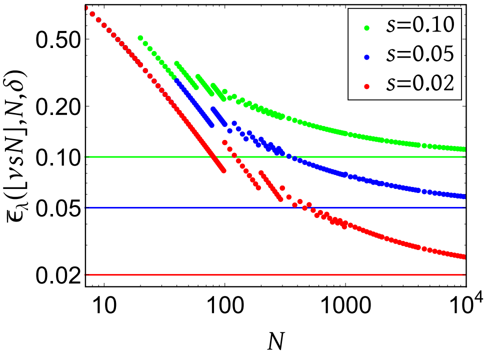

Fig. 3 Variations of $\bar{\epsilon}_\lambda(\lfloor \nu sN\rfloor, N, \delta)$ with the number N of tests and error rate s [by Eq. (6) in Supplementary Note 1]. Here $\lambda = 1/2$ and significance level $\delta = 0.05$. Each horizontal line represents an error rate. As the test number N increases, $\bar{\epsilon}_\lambda(\lfloor \nu sN\rfloor, N, \delta)$ approaches s.

In view of the above discussions, the computation of $\bar{\epsilon}_\lambda(k,N,\delta)$ given in Eq. (11) is of central importance to analyzing the soundness of our protocol. Thanks to the analysis presented in the Methods section, this quantum optimization problem can actually be reduced to a classical sampling problem studied in the companion paper[34]. Using the results derived in ref. [34], we can deduce many useful properties of $\bar{\epsilon}_\lambda(k,N,\delta)$ as well as its analytical formula, which are presented in Supplementary Note 1. Here it suffices to clarify the monotonicity properties of $\bar{\epsilon}_\lambda(k,N,\delta)$ as stated in Proposition 1 below, which follows from Proposition 6.5 in ref. [34]. Let $\mathbb{Z}^{\ge j}$ be the set of integers larger than or equal to j.

Proposition 1. Suppose $0 \le \lambda < 1$, $0 < \delta \le 1$, $k \in \mathbb{Z}^{\ge 0}$, and $N \in \mathbb{Z}^{\ge k+1}$. Then $\bar{\epsilon}_\lambda(k,N,\delta)$ is nonincreasing in δ and N, but nondecreasing in k.

Verification with a fixed error rate

If the number k of allowed failures is sublinear in N, that is, $k = o(N)$, then the acceptance probability $p^{\rm iid}_{N,k}(\tau)$ in Eq. (7) for the i.i.d. case approaches 0 as the number of tests N increases, which is not satisfactory. To achieve robust verification, here we set the number k to be proportional to the number of tests, that is, $k = \lfloor \nu sN\rfloor$, where $0 \le s < 1$ is the error rate, and $\nu = 1-\lambda$ is the spectral gap of the strategy Ω. In this case, when Bob prepares i.i.d. states $\tau \in \mathcal{D}(\mathcal{H})$ with $\epsilon_\tau < s$, the acceptance probability $p^{\rm iid}_{N,k}(\tau)$ approaches one as N increases. In addition, we can deduce the following theorem, which is proved in Supplementary Note 6B.

Theorem 1. Suppose $0 < s$, $\lambda < 1$, $0 < \delta \le 1/4$, and $N \in \mathbb{Z}^{\ge 1}$. Then

$$s - \frac{1}{\nu N} < \bar{\epsilon}_\lambda(\lfloor \nu sN\rfloor, N, \delta) \le s + \frac{1}{\nu\lambda}\sqrt{\frac{s\ln\delta^{-1}}{N} + \frac{\ln\delta^{-1}}{2\nu^2\lambda N} + \frac{2}{\lambda N}}. \tag{13}$$

Theorem 1 implies that $\bar{\epsilon}_\lambda(\lfloor \nu sN\rfloor, N, \delta)$ converges to the error rate s when the number N of tests gets large, as illustrated in Fig. 3. To achieve a given infidelity ϵ and significance level δ, which means $\bar{\epsilon}_\lambda(\lfloor \nu sN\rfloor, N, \delta) \le \epsilon$, it suffices to set $s < \epsilon$ and choose a sufficiently large N. By virtue of Theorem 1 we can derive the following theorem as proved in Supplementary Note 6C.

Theorem 2. Suppose $0 < \lambda < 1$, $0 \le s < \epsilon < 1$, and $0 < \delta \le 1/2$. If the number N of tests satisfies

$$N \ge \frac{\epsilon}{[\lambda\nu(\epsilon - s)]^2}\left(\ln\delta^{-1} + 4\lambda\nu^2\right), \tag{14}$$

then $\bar{\epsilon}_\lambda(\lfloor \nu sN\rfloor, N, \delta) \le \epsilon$.

Notably, if the ratio s/ϵ is a constant, then the sample cost is only $O(\epsilon^{-1}\ln\delta^{-1})$. The scaling behaviors in ϵ and δ are the same as the counterparts in the nonadversarial scenario, and are thus optimal.

The number of allowed failures

Next, we consider the case in which the number N of tests is given. To construct a concrete verification protocol, we need to specify the number k of allowed failures such that the conditions of soundness and robustness are satisfied simultaneously. According to Proposition 1, a small k is preferred to guarantee soundness, while a larger k is preferred to guarantee robustness. To construct a robust and efficient verification protocol, we need to find a good balance between the two conflicting requirements. The following proposition provides a suitable interval for the number k of allowed failures that can guarantee soundness; see Supplementary Note 6E for a proof.

Proposition 2. Suppose $0<\lambda$, $\epsilon<1$, $0<\delta\leq 1/4$, and $N,k\in\mathbb{Z}^{\geq 0}$. If $\nu\epsilon N\leq k\leq N-1$, then $\bar{\epsilon}_\lambda(k,N,\delta)>\epsilon$. If $k\leq l(\lambda, N, \epsilon, \delta)$, then $\bar{\epsilon}_\lambda(k,N,\delta)\leq\epsilon$. Here

$$l(\lambda,N,\epsilon,\delta):=\left\lfloor \nu\epsilon N-\frac{\sqrt{N\epsilon\ln\delta^{-1}}}{\lambda}-\frac{\ln\delta^{-1}}{2\lambda\nu}-\frac{2\nu}{\lambda}\right\rfloor. \tag{15}$$

Next, we turn to the condition of robustness. When honest Bob prepares i.i.d. quantum states $\tau\in\mathcal{D}(\mathcal{H})$ with infidelity $0<\epsilon_\tau<\epsilon$, the probability that Alice accepts τ is $p^{\rm iid}_{N,k}(\tau)$ given in Eq. (7), which is strictly increasing in k according to Lemma S4 in Supplementary Note 2. Suppose we set $k=l(\lambda, N, \epsilon, \delta)$. As the number of tests N increases, the acceptance probability has the following asymptotic behavior if $0<\epsilon_\tau<\epsilon$ (see Supplementary Note 6F for a proof),

$$p^{\rm iid}_{N,l}(\tau)=1-\exp\left[-D(\nu\epsilon\|\nu\epsilon_\tau)N+O(\sqrt{N})\right], \tag{16}$$

where $D(p\|q):=p\ln\frac{p}{q}+(1-p)\ln\frac{1-p}{1-q}$ is the relative entropy between two binary probability vectors $(p, 1-p)$ and $(q, 1-q)$, and l is a shorthand for $l(\lambda, N, \epsilon, \delta)$. Therefore, the probability of acceptance is arbitrarily close to one as long as N is sufficiently large, as illustrated in Fig. 4. Hence, our verification protocol is able to reach any degree of robustness.

Sample complexity of robust verification

Now we consider the resource cost required by our protocol to reach given verification precision and robustness. Let ρ be the state on $\mathcal{H}^{\otimes(N+1)}$ prepared by Bob and σ_{N+1} be the reduced state after Alice performs suitable tests and accepts the state ρ. To verify the target state within infidelity ϵ, significance level δ, and robustness r (with $0\leq r<1$) entails the following two conditions.

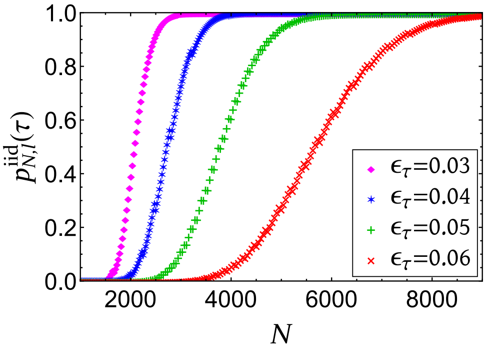

Fig. 4 The probability $p^{\rm iid}_{N,l(\lambda,N,\epsilon,\delta)}(\tau)$ that Alice accepts i.i.d. quantum states $\tau\in\mathcal{D}(\mathcal{H})$. Here $\lambda=1/2$, infidelity $\epsilon=0.1$, and significance level $\delta=0.01$; ϵ_τ is the infidelity between τ and the target state $|G\rangle$; and $l(\lambda, N, \epsilon, \delta)$ is the number of allowed failures defined in Eq. (15).

1. (Soundness) If the infidelity of σ_{N+1} with the target state is larger than ϵ, then the probability that Alice accepts ρ is less than δ.
2. (Robustness) If $\rho=\tau^{\otimes(N+1)}$ with $\tau\in\mathcal{D}(\mathcal{H})$ and $\epsilon_\tau\leq r\epsilon$, then the probability that Alice accepts ρ is at least $1-\delta$.

The tensor power ρ in Condition 2 can be replaced by the tensor product of $N+1$ independent quantum states $\tau_1,\tau_2,\ldots,\tau_{N+1}\in\mathcal{D}(\mathcal{H})$ that have infidelities at most $r\epsilon$. All our conclusions do not change under this modification.

To achieve the conditions of soundness and robustness, we need to choose the test number N and the number k of allowed failures properly. To determine the resource cost, we define $N_{\rm min}(\epsilon,\delta,\lambda,r)$ as the minimum number of tests required for robust verification, that is, the minimum positive integer N such that there exists an integer $0\leq k\leq N-1$ which together with N achieves the above two conditions. Note that the conditions of soundness and robustness can be expressed as

$$\bar{\epsilon}_\lambda(k,N,\delta)\leq\epsilon,\qquad B_{N,k}(\nu r\epsilon)\geq 1-\delta. \tag{17}$$

So $N_{\rm min}(\epsilon,\delta,\lambda,r)$ can be expressed as

$$N_{\rm min}(\epsilon,\delta,\lambda,r):=\min_{N,k}\left\{N\,|\,k\in\mathbb{Z}^{\geq 0},N\in\mathbb{Z}^{\geq k+1},\bar{\epsilon}_\lambda(k,N,\delta)\leq\epsilon,B_{N,k}(\nu r\epsilon)\geq 1-\delta\right\}. \tag{18}$$

Algorithm 1. Minimum test number for robust verification

```
Input: $\lambda$, $\epsilon$, $\delta\in(0, 1)$ and $r\in[0, 1)$.
Output: $k_{\rm min}(\epsilon,\delta,\lambda,r)$ and $N_{\rm min}(\epsilon,\delta,\lambda,r)$.
if $r=0$ then
    $k_{\rm min}\leftarrow 0$
else
    for $k=0, 1, 2, \ldots$ do
        Find the largest integer $M$ such that $B_{M,k}(\nu r\epsilon)\geq 1-\delta$.
        if $M\geq k+1$ and $\bar{\epsilon}_\lambda(k,M,\delta)\leq\epsilon$, then
            stop
        end if
    end for
    $k_{\rm min}\leftarrow k$
end if
Find the smallest integer $N$ that satisfies $N\geq k_{\rm min}+1$ and
    $\bar{\epsilon}_\lambda(k_{\rm min},N,\delta)\leq\epsilon$.
$N_{\rm min}\leftarrow N$
return $k_{\rm min}$ and $N_{\rm min}$.
```

Next, we propose a simple algorithm, Algorithm 1, for computing $N_{\rm min}(\epsilon,\delta,\lambda,r)$, which is very useful for practical applications. In addition to $N_{\rm min}(\epsilon,\delta,\lambda,r)$, this algorithm determines the corresponding number of allowed failures, which is denoted by $k_{\rm min}(\epsilon,\delta,\lambda,r)$. In Supplementary Note 7C we explain why Algorithm 1 works. Algorithm 1 is particularly useful for studying the variations of $N_{\rm min}(\epsilon,\delta,\lambda,r)$ with the four parameters ϵ, δ, λ, r as illustrated in Fig. 5. When δ and r are fixed, $N_{\rm min}(\epsilon,\delta,\lambda,r)$ is inversely proportional to ϵ; when ϵ, r are fixed and δ approaches 0, $N_{\rm min}(\epsilon,\delta,\lambda,r)$ is proportional to $\ln\delta^{-1}$. In addition, Fig. 5d indicates that a strategy Ω with small or large λ is not very efficient for robust verification, while any choice satisfying $0.3\leq\lambda\leq 0.5$ is nearly optimal.

The following theorem provides an informative upper bound for $N_{\rm min}(\epsilon,\delta,\lambda,r)$ and clarifies the sample complexity of robust verification; see Supplementary Note 6D for a proof.

Theorem 3. Suppose $0<\lambda$, $\epsilon<1$, $0<\delta\leq 1/2$, and $0\leq r<1$. Then the conditions of soundness and robustness in Eq. (17) hold as

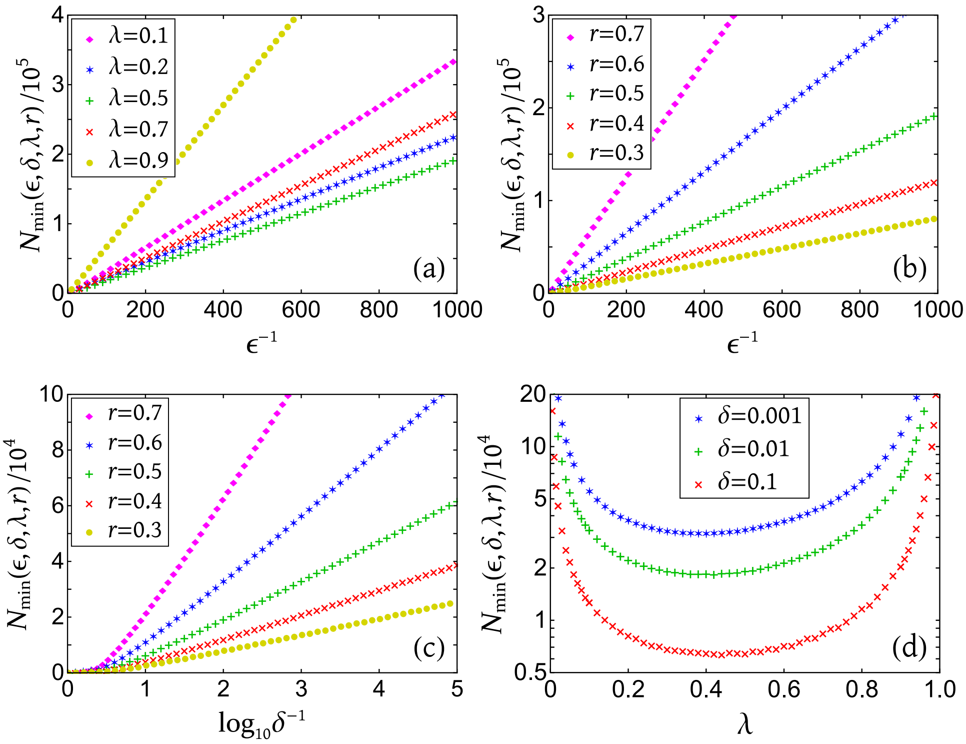

Fig. 5 Minimum number of tests required for robust verification (by Algorithm 1). **a** Variations of $N_{\min}(\epsilon,\delta,\lambda,r)$ with ϵ^{-1} and λ, where robustness $r=1/2$ and significance level $\delta=0.01$. **b** Variations of $N_{\min}(\epsilon,\delta,\lambda,r)$ with ϵ^{-1} and r, where $\delta=0.01$ and $\lambda=1/2$. **c** Variations of $N_{\min}(\epsilon,\delta,\lambda,r)$ with $\log_{10}\delta^{-1}$ and r, where $\lambda=1/2$ and infidelity $\epsilon=0.01$. **d** Variations of $N_{\min}(\epsilon,\delta,\lambda,r)$ with λ and δ, where $\epsilon=0.01$ and $r=1/2$.

long as

$$k=\left\lfloor\left(\frac{\lambda\sqrt{2\nu}+r}{\lambda\sqrt{2\nu}+1}\right)\nu\epsilon N\right\rfloor, \tag{19}$$

$$N\geq\left\lceil\left[\frac{\lambda\sqrt{2\nu}+1}{\lambda\nu(1-r)}\right]^2\frac{\ln\delta^{-1}+4\lambda\nu^2}{\epsilon}\right\rceil. \tag{20}$$

For given λ and r, the minimum number of tests is only $O(\epsilon^{-1}\ln\delta^{-1})$, which is independent of the qudit number n of $|G\rangle$ and achieves the optimal scaling behaviors with respect to the infidelity ϵ and significance level δ. The coefficient is large when λ is close to 0 or 1, while it is around the minimum for any value of λ in the interval [0.3, 0.5]. Numerical calculation based on Algorithm 1 shows that the upper bound for $N_{\min}(\epsilon,\delta,\lambda,r)$ provided in Theorem 3 is a bit conservative, especially when r is small. In other words, the actual sample cost is smaller than what can be proved rigorously. Nevertheless, the bound is quite informative about the general trends. If we choose $r=\lambda=1/2$ for example, then Theorem 3 implies that

$$N_{\min}(\epsilon,\delta,\lambda,r)\leq\lceil 144\,\epsilon^{-1}(\ln\delta^{-1}+0.5)\rceil, \tag{21}$$

while numerical calculation yields $N_{\min}(\epsilon,\delta,\lambda,r)\leq 67\,\epsilon^{-1}\ln\delta^{-1}$. Compared with previous works[16,30,31], our protocol improves the scaling behavior with respect to the significance level δ exponentially and even doubly exponentially, as illustrated in Fig. 2.

DISCUSSION

Verification of resource graph states in the adversarial scenario is a crucial step in the verification of blind MBQC. We have proposed a highly robust and efficient protocol for achieving this task, which applies to any qudit graph state with a prime local dimension. To implement this protocol, it suffices to perform simple stabilizer tests based on local Pauli measurements, which is quite appealing to NISQ devices. For any given degree of robustness, to verify the target graph state within infidelity ϵ and significance level δ, only $O(\epsilon^{-1}\ln\delta^{-1})$ tests are required, which achieve the optimal sample complexity with respect to the system size, infidelity, and significance level. Compared with previous protocols, our protocol can reduce the sample cost dramatically in a realistic scenario; notably, the scaling behavior in the significance level can be improved exponentially.

So far we have focused on the verification of resource graph states with trustworthy and ideal local projective measurements. According to Eq. (12), if the blind MBQC is performed with ideal measurements after Alice accepts the state prepared by Bob, then the precision of the computation results is guaranteed by the precision of the graph state. However, in practice, it is unrealistic to assume that the measurement devices are perfect. So we need additional operations to guarantee the precision of the computation results when verifying blind MBQC in the receive-and-measure setting. As mentioned in the introduction, the client can calibrate her measurement devices before performing blind MBQC with a small overhead. In addition, we can convert the noise in measurements to noise in state preparation. To apply this method, we need the assumption that any measurement used in MBQC and graph state verification can be expressed as a composition of a measurement-independent noise process and the noiseless measurement. The detail of this conversion method is presented in Supplementary Note 4. When the noise process depends on the specific measurement, the situation is more complicated, and further study is required to deal with such noise.

After obtaining a reliable resource graph state accepted by the verification protocol, Alice can use it to perform MBQC. In this procedure, she needs to adaptively select local projective measurements to drive the computation. Nevertheless, these operations can be completed by using a classical computer, and the classical computation complexity scales linearly with the size of the original quantum computation[13]. Therefore, the most challenging part in the verification of blind MBQC is the verification of the resource graph state, which is the focus of this work.

In the above discussion, we assume that the measurement devices are controlled by the client and are trustworthy. It is also desirable to construct robust and efficient protocols for verifying blind MBQC when the measurement devices are not trustworthy. To this end, a device-independent (DI) verification protocol was proposed in ref. [37]. However, this protocol has a quantum communication complexity of the order $O(\tilde{n}^c)$, where $\tilde{n}$ is the size of the delegated quantum computation and $c > 2048$, which is too prohibitive for any practical implementation. By combining the CHSH inequality and stabilizer tests applied to a qubit graph state, ref. [19] proposed a protocol for self-testing MBQC in the receive-and-measure setting. This protocol requires $O(n^4 \log n)$ samples with n being the qubit number of the resource graph state, which is much more efficient than previous protocols, but is still far from the optimal scaling achieved in this work. In addition, it does not consider the problem of robustness. To further reduce the overhead and improve the robustness, it might be helpful to combine our approach with DI quantum state certification (DI QSC) developed recently[38]. See Supplementary Note 5 for details.

In addition to graph states, our protocol can also be used to verify many other pure quantum states in the adversarial scenario, where the state preparation is controlled by a potentially malicious adversary Bob, who can produce an arbitrary correlated or entangled state ρ on the whole system $\mathcal{H}^{\otimes(N+1)}$. Let $|\Psi\rangle \in \mathcal{H}$ be the target pure state to be verified. Then a verification strategy Ω for $|\Psi\rangle$ is called homogeneous[30,31] if it has the form

$$\Omega = |\Psi\rangle\langle\Psi| + \lambda(\mathbb{I} - |\Psi\rangle\langle\Psi|), \qquad 0 \le \lambda < 1. \tag{22}$$

Efficient homogeneous strategies based on local projective measurements have been constructed for many important quantum states[31,36,39–46].

If a homogeneous strategy Ω given in Eq. (22) can be constructed, then the target state $|\Psi\rangle$ can be verified in the adversarial scenario by virtue of our protocol: Alice first randomly permutes all systems of ρ and applies the strategy Ω to the first N systems, then she accepts the remaining unmeasured system if at most k failures are observed among these tests. Most results (including Theorems 1, 2, 3, Algorithm 1, and Propositions 1, 2) in this paper are still applicable if the target graph state $|G\rangle$ is replaced by $|\Psi\rangle$. Therefore, our verification protocol is of interest not only to blind MBQC, but also to many other tasks in quantum information processing that entail high security. More results on quantum state verification (QSV) in the adversarial scenario are presented in Supplementary Note 7.

Up to now, we have focused on robust QSV in the adversarial scenario, in which the prepared state ρ can be arbitrarily correlated or entangled, which is pertinent to blind MBQC. On the other hand, robust QSV in the i.i.d. scenario is also important to many applications. Although this scenario is much simpler than the adversarial scenario, the sample complexity of robust QSV has not been clarified before. In the Methods section and Supplementary Note 8 we will discuss this issue in detail and clarify the sample complexity of robust QSV in the i.i.d. scenario in comparison with the adversarial scenario. Not surprisingly, most of our results on the adversarial scenario have analog for the i.i.d. scenario.

METHODS

Protocols for realizing verifiable BQC

To put our work into context, here we briefly review existing protocols for realizing verifiable BQC, which can be broadly divided into four classes[24]. Many protocols in the four classes build on the model of MBQC due to its convenience and flexibility.

The first class of protocols works in the multi-prover setting[8,37,47,48]. These protocols can achieve a classical client (verifier), but a trade-off is the requirement of multiple non-communicating servers (provers) that share entanglement with each other, which is very difficult to realize in practice.

The second and third classes of protocols need only a single server, but assume that the client has limited quantum computational power. The second class of protocols works in the prepare-and-send setting[10,49–51], in which the client has a trusted preparation device and the ability to send single-qudit quantum states to the server. This class includes the protocol based on quantum authentication[49], protocol based on repeating indistinguishable runs of tests and computations[50], and protocol based on trap qubits[51], which has been demonstrated experimentally[10]. The third class of protocols works in the receive-and-measure setting[16–18,20,21,37], in which the client receives quantum states from the server and has the ability to perform reliable local projective measurements. This class includes the protocol based on CHSH games[37], protocols based on QSV in the adversarial scenario[16–18,20,21], and our protocol. Notably, the above three classes of protocols are all information-theoretically secure[24].

Recently, the fourth class of protocols based on computational assumptions has been developed[52–55], which elegantly enables a classical client to hide and verify the quantum computation of a single server. However, these schemes are no longer information-theoretically secure, and their overheads are too prohibitive for any sort of practical implementation in the near future.

Simplifying the calculation of $\bar{\epsilon}_\lambda(k, N, \delta)$

Here we show how to simplify the calculation of the guaranteed infidelity $\bar{\epsilon}_\lambda(k, N, \delta)$ given in Eq. (11) by virtue of results derived in the companion paper[34].

Recall that Ω is a homogeneous strategy for the target state $|G\rangle \in \mathcal{H}$ as shown in Eq. (6). It has the following spectral decomposition,

$$\Omega = |G\rangle\langle G| + \lambda(\mathbb{I} - |G\rangle\langle G|) = \Pi_1 + \lambda\sum_{j=2}^{D}\Pi_j, \tag{23}$$

where D is the dimension of $\mathcal{H}$, and Π_j are mutually orthogonal rank-1 projectors with $\Pi_1 = |G\rangle\langle G|$. In addition, ρ is a permutation-invariant state on $\mathcal{H}^{\otimes(N+1)}$. Note that $p_k(\rho)$ defined in Eq. (9) and $f_k(\rho)$ defined in Eq. (10) only depend on the diagonal elements of ρ in the product basis constructed from the eigenbasis of Ω (as determined by Π_j). Hence, we may assume that ρ is diagonal in this basis without loss of generality. In other words, ρ can be expressed as a mixture of tensor products of Π_j. For $i = 1, 2, \ldots, N+1$, we can associate the ith system of ρ with a {0, 1}-valued variable Y_i: we define $Y_i = 0$ (1) if the state on the ith system is Π_1 ($\Pi_{j\neq1}$). Since the state ρ is permutation invariant, the variables $Y_1, \ldots, Y_{N+1}$ are subject to a permutation-invariant joint distribution $P_{Y_1,\ldots,Y_{N+1}}$ on $[N+1] := \{1, 2, \ldots, N+1\}$. Conversely, for any permutation-invariant joint distribution on $[N+1]$, we can always find a diagonal state ρ, whose corresponding variables $Y_1, \ldots, Y_{N+1}$ are subject to this distribution.

Next, we define a {0, 1}-valued random variable U_i to express the test outcome on the ith system, where 0 corresponds to passing the test and 1 corresponds to failure. If $Y_i = 0$, which means the state on the ith system is Π_1, then the ith system must pass the test; if $Y_i = 1$, which means the state on the ith system is $\Pi_{j\neq1}$, then the ith system passes the test with probability λ, and fails with

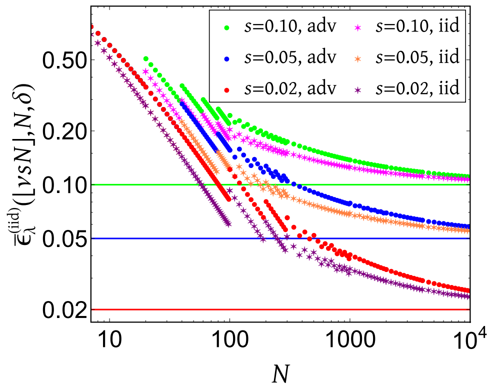

Fig. 6 Guaranteed infidelities in the i.i.d. scenario and adversarial scenario. Here $\lambda = 1/2$ and $\delta = 0.05$; the green, blue, and red dots represent $\bar{\epsilon}_\lambda(\lfloor \nu sN \rfloor, N, \delta)$ [by Eq. (6) in Supplementary Note 1] for the adversarial scenario, while the magenta, orange, and purple stars represent $\bar{\epsilon}_\lambda^{\mathrm{iid}}(\lfloor \nu sN \rfloor, N, \delta)$ [by Eq. (29)] for the i.i.d. scenario; each horizontal line represents an error rate s.

probability $1-\lambda$. So we have the following conditional distribution:

$$\begin{aligned} &P_{U_i|Y_i}(0|0) = 1, \qquad &P_{U_i|Y_i}(1|0) = 0, \\ &P_{U_i|Y_i}(0|1) = \lambda, \qquad &P_{U_i|Y_i}(1|1) = 1-\lambda. \end{aligned} \tag{24}$$

Note that U_i is determined by the random variable Y_i and the parameter λ in Eq. (6). Let K be the random variable that counts the number of 1, that is, the number of failures, among U_1, U_2, …, U_N. Then the probability that Alice accepts is

$$p_k(\rho) = \Pr(K \le k), \tag{25}$$

given that Alice accepts if at most k failures are observed among the N tests. This probability only depends on the joint distribution $P_{Y_1,\ldots,Y_{N+1}}$. If at most k failures are observed, then the fidelity of the state on the $(N+1)$th system can be expressed as the conditional probability

$$F_k(\rho) = \Pr(Y_{N+1} = 0 | K \le k), \tag{26}$$

which also only depends on $P_{Y_1,\ldots,Y_{N+1}}$. Hence, the guaranteed infidelity defined in Eq. (11) can be expressed as

$$\begin{aligned} \bar{\epsilon}_\lambda(k, N, \delta) &= 1 - \min\{\Pr(Y_{N+1} = 0 | K \le k) \,|\, \Pr(K \le k) \ge \delta\} \\ &= \max\{\Pr(Y_{N+1} = 1 | K \le k) \,|\, \Pr(K \le k) \ge \delta\}, \end{aligned} \tag{27}$$

where the optimization is taken over all permutation-invariant joint distributions $P_{Y_1,\ldots,Y_{N+1}}$.

Equation (27) reduces the computation of $\bar{\epsilon}_\lambda(k, N, \delta)$ to the computation of a maximum conditional probability. The latter problem was studied in detail in our companion paper[34], in which $\bar{\epsilon}_\lambda(k, N, \delta)$ is called the upper confidence limit. Hence, all properties of $\bar{\epsilon}_\lambda(k, N, \delta)$ derived in ref. [34] also hold in the current context. Notably, several results in this paper are simple corollaries of the counterparts in ref. [34]. To be specific, Proposition 1 follows from Proposition 6.5 in ref. [34]; Theorem S1 in Supplementary Note 1 follows from Theorem 6.4 in ref. [34]; Lemma S6 in Supplementary Note 2 follows from Lemma 6.7 in ref. [34]; Lemma S7 in Supplementary Note 2 follows from Lemma 2.2 in ref. [34]; Proposition S7 in Supplementary Note 7 follows from Lemma 5.4 and Eq. (89) in ref. [34].

Although this paper and the companion paper[34] study essentially the same quantity $\bar{\epsilon}_\lambda(k, N, \delta)$, they have different focuses. In ref. [34], we mainly focus on asymptotic behaviors of $\bar{\epsilon}_\lambda(k, N, \delta)$ and its related quantities, which are of interest to the theory of statistical sampling and hypothesis testing. The main goal of ref. [34] is to show that the randomized test with parameter $\lambda > 0$ can substantially improve the significance level over the deterministic test with $\lambda = 0$. In this paper, by contrast, we focus on finite bounds for $\bar{\epsilon}_\lambda(k, N, \delta)$ and its related quantities, which are important to practical applications. In addition, the key result on robust verification, Theorem 3, has no analog in the companion paper. The main goal of this paper is to provide a robust and efficient protocol for verifying the resource graph state in blind MBQC and clarify the sample complexity. So the two papers are complementary to each other.

It is worth pointing out that the 'randomized test' considered in ref. [34] has a different meaning from the 'quantum test' in this paper because of different conventions in the two communities. The 'randomized test' in ref. [34] means the whole procedure that one observes the N variables U_1, U_2, …, U_N and makes a decision based on the number of failures observed; while a 'quantum test' in this paper means Alice performs a two-outcome measurement on one system of the state ρ, in which one outcome corresponds to passing the test, and the other outcome corresponds to a failure.

Robust and efficient verification of quantum states in the i.i.d. scenario

Up to now we have focused on QSV in the adversarial scenario, in which the server Bob can prepare an arbitrary state ρ on the whole space $\mathcal{H}^{\otimes(N+1)}$. In this section, we turn to the i.i.d. scenario, in which the prepared state is a tensor power of the form $\rho = \sigma^{\otimes(N+1)}$ with $\sigma \in \mathcal{D}(\mathcal{H})$. This verification problem was originally studied in refs. [39,40] and later more systematically in ref. [36]. So far, efficient verification strategies based on local operations and classical communication (LOCC) have been constructed for various classes of pure states, including bipartite pure states[42,43,56], stabilizer states (including graph states)[16,31,33,36,57], hypergraph states[33], weighted graph states[58], Dicke states[45,59], ground states of local Hamiltonians[60,61], and certain continuous-variable states[62], see refs. [28,29] for overviews. Verification protocols based on local collective measurements have also been constructed for Bell states[40,63]. However, most previous works did not consider the problem of robustness. Consequently, most protocols known so far are not robust, and the sample cost may increase substantially if robustness is taken into account, see Supplementary Note 8A for explanation. Only recently, several works considered the problem of robustness[29,64–67]; however, the degree of robustness of verification protocols has not been analyzed, and the sample complexity of robust verification has not been clarified, although this problem is apparently much simpler than the counterpart in the adversarial scenario.

In this section, we propose a general approach for constructing robust and efficient verification protocols in the i.i.d. scenario and clarify the sample complexity of robust verification. The results presented here can serve as a benchmark for understanding QSV in the adversarial scenario. To streamline the presentation, the proofs of these results [including Propositions 3–6 and Eq. (38)] are relegated to Supplementary Note 8.

Consider a quantum device that is expected to produce the target state $|\Psi\rangle \in \mathcal{H}$, but actually produces the states σ_1, σ_2, …, σ_N in N runs. In the i.i.d. scenario, all these states are identical to the state σ, and the goal of Alice is to verify whether σ is sufficiently close to the target state $|\Psi\rangle$. If a strategy Ω of the form in Eq. (22) can be constructed for $|\Psi\rangle$, then our verification protocol runs as follows: Alice applies the strategy Ω to each of the N states, and counts the number of failures. If at most k failures are observed among the N tests, then Alice accepts the states prepared; otherwise, she rejects. Here $0 \le k \le N-1$ is called the number of allowed failures. The completeness of this protocol is guaranteed because the target state $|\Psi\rangle$ can never be mistakenly rejected.

Most previous works did not consider the problem of robustness and can reach a meaningful conclusion only when

$k=0$[31,33,36,39–45], i.e., Alice accepts if all N tests are passed. However, the requirement of passing all tests is too demanding in a realistic scenario and leads to poor robustness, as clarified in Supplementary Note 8. To remedy this problem, several recent works considered modifications that allow some failures[29,64–67]. However, the robustness of such verification protocols has not been analyzed, and the sample complexity of robust verification has not been clarified.

Here we consider robust verification in which at most k failures are allowed. Then the probability of acceptance is given by

$$p^{\mathrm{iid}}_{N,k}(\sigma)=\sum_{j=0}^{k}\binom{N}{j}[1-\mathrm{tr}\,(\Omega\sigma)]^{j}\mathrm{tr}\,(\Omega\sigma)^{N-j}=B_{N,k}(1-\mathrm{tr}\,(\Omega\sigma))=B_{N,k}(\nu\epsilon_{\sigma}), \tag{28}$$

where $\epsilon_\sigma := 1-\langle\Psi|\sigma|\Psi\rangle$ is the infidelity between σ and the target state. Similar to Eq. (11), for $0<\delta\le 1$ we define the guaranteed infidelity in the i.i.d. scenario as

$$\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(k,N,\delta):=\max_{\sigma}\left\{\epsilon_\sigma \,|\, p^{\mathrm{iid}}_{N,k}(\sigma)\ge\delta\right\}=\max_{\epsilon}\{0\le\epsilon\le 1\,|\,B_{N,k}(\nu\epsilon)\ge\delta\}, \tag{29}$$

where the first maximization is taken over all states σ on $\mathcal{H}$, and the second equality follows from Eq. (28). By definition, if Alice accepts the state σ, then she can ensure (with significance level δ) that σ has infidelity at most $\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(k,N,\delta)$ with the target state (soundness). Hence, $\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(k,N,\delta)$ characterizes the verification precision in the i.i.d. scenario. Since the i.i.d. scenario has a stronger constraint than the full adversarial scenario, the guaranteed infidelity for the former scenario cannot be larger than that for the later scenario, that is,

$$\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(k,N,\delta)\le\bar{\epsilon}_{\lambda}(k,N,\delta), \tag{30}$$

as illustrated in Fig. 6.

The following proposition clarifies the monotonicities of $\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(k,N,\delta)$. It is the counterpart of Proposition 1.

Proposition 3. Suppose $0\le\lambda<1$, $0<\delta\le 1$, $k\in\mathbb{Z}^{\ge 0}$, and $N\in\mathbb{Z}^{\ge k+1}$. Then $\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(k,N,\delta)$ is strictly decreasing in δ and N, but strictly increasing in k.

Next, we consider the verification with a fixed error rate in the i.i.d. scenario. Concretely, we set the number of allowed failures k to be proportional to the number of tests, i.e., $k=\lfloor s\nu N\rfloor$, where $0\le s<1$ is the error rate, and $\nu=1-\lambda$ is the spectral gap of the strategy Ω. The following proposition provides informative bounds for $\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(\lfloor\nu sN\rfloor,N,\delta)$. It is the counterpart of Theorem 1.

Proposition 4. Suppose $0<s,\lambda<1$, $0<\delta\le 1/2$, and $N\in\mathbb{Z}^{\ge 1}$; then

$$s-\frac{1}{\nu N}<\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(\lfloor\nu sN\rfloor,N,\delta)\le s+\sqrt{\frac{2s\ln\delta^{-1}}{\nu N}}+\frac{2\ln\delta^{-1}}{\nu N}. \tag{31}$$

Similar to the behavior of $\bar{\epsilon}_{\lambda}(\lfloor\nu sN\rfloor,N,\delta)$, the guaranteed infidelity $\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(\lfloor\nu sN\rfloor,N,\delta)$ for the i.i.d. scenario converges to the error rate s as the number N gets large, as illustrated in Fig. 6. To achieve a given infidelity ϵ and significance level δ, which means $\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(\lfloor\nu sN\rfloor,N,\delta)\le\epsilon$, it suffices to set $s<\epsilon$ and choose a sufficiently large N. By virtue of Proposition 4 we can derive the following proposition, which is the counterpart of Theorem 2.

Proposition 5. Suppose $0\le\lambda<1$, $0\le s<\epsilon<1$, and $0<\delta<1$. If the number of tests N satisfies

$$N\ge\frac{\ln\delta^{-1}}{D(\nu s\|\nu\epsilon)}, \tag{32}$$

then $\bar{\epsilon}^{\mathrm{iid}}_{\lambda}(\lfloor\nu sN\rfloor,N,\delta)\le\epsilon$.

In the rest of this section, we turn to study the sample complexity of robust verification in the i.i.d. scenario. To verify the target state within infidelity ϵ, significance level δ, and robustness r (with $0\le r<1$) entails the following conditions,

1. (Soundness) If the device prepares i.i.d. states $\tau\in\mathcal{D}(\mathcal{H})$ with infidelity $\epsilon_\tau>\epsilon$, then the probability that Alice accepts τ is smaller than δ.
2. (Robustness) If the device prepares i.i.d. states $\tau\in\mathcal{D}(\mathcal{H})$ with infidelity $\epsilon_\tau\le r\epsilon$, then the probability that Alice accepts τ is at least $1-\delta$.

Here the condition of robustness is the same as the counterpart in the adversarial scenario, while the condition of soundness is different. In the adversarial scenario, once accepting, only the reduced state on the remaining unmeasured system can be used for application, so the condition of soundness only focuses on the fidelity of this state. In the i.i.d. scenario, by contrast, the prepared states are identical and independent, so the condition of soundness focuses on the fidelity of each state.

Given the total number N of tests and the number k of allowed failures, then the conditions of soundness and robustness can be expressed as

$$B_{N,k}(\nu\epsilon)\le\delta,\qquad B_{N,k}(\nu r\epsilon)\ge 1-\delta. \tag{33}$$

Let $N^{\mathrm{iid}}_{\min}(\epsilon,\delta,\lambda,r)$ be the minimum number of tests required for robust verification in the i.i.d. scenario. Then $N^{\mathrm{iid}}_{\min}(\epsilon,\delta,\lambda,r)$ is the minimum positive integer N such that Eq. (33) holds for some $0\le k\le N-1$, namely,

$$N^{\mathrm{iid}}_{\min}(\epsilon,\delta,\lambda,r):=\min_{N,k}\left\{N\,|\,k\in\mathbb{Z}^{\ge 0},N\in\mathbb{Z}^{\ge k+1},B_{N,k}(\nu\epsilon)\le\delta,B_{N,k}(\nu r\epsilon)\ge 1-\delta\right\}. \tag{34}$$

It is determined by $\nu\epsilon$, δ, r, and is the counterpart of $N_{\min}(\epsilon,\delta,\lambda,r)$ in the adversarial scenario.

Next, we propose a simple algorithm, Algorithm 2, for computing $N^{\mathrm{iid}}_{\min}(\epsilon,\delta,\lambda,r)$, which is very useful to practical applications. This algorithm is the counterpart of Algorithm 1 for computing $N_{\min}(\epsilon,\delta,\lambda,r)$. In addition to the number of tests, Algorithm 2 also determines the corresponding number of allowed failures, which is denoted by $k^{\mathrm{iid}}_{\min}(\epsilon,\delta,\lambda,r)$. In Supplementary Note 8F we explain why Algorithm 2 works.

Algorithm 2. Minimum test number for robust verification in the i.i.d. scenario

```
Input: $\lambda$, $\epsilon$, $\delta \in (0, 1)$ and $r \in [0, 1)$.
Output: $k^{\mathrm{iid}}_{\min}(\epsilon,\delta,\lambda,r)$ and $N^{\mathrm{iid}}_{\min}(\epsilon,\delta,\lambda,r)$.
if $r = 0$ then
    $k^{\mathrm{iid}}_{\min} \leftarrow 0$
else
    for $k = 0, 1, 2, \ldots$ do
        Find the largest integer $M$ such that $B_{M,k}(\nu r\epsilon) \ge 1-\delta$.
        if $M \ge k+1$ and $B_{M,k}(\nu\epsilon) \le \delta$ then
            stop
        end if
    end for
    $k^{\mathrm{iid}}_{\min} \leftarrow k$
end if
Find the smallest integer $N$ that satisfies $N \ge k^{\mathrm{iid}}_{\min}+1$ and
    $B_{N,k^{\mathrm{iid}}_{\min}}(\nu\epsilon) \le \delta$.
$N^{\mathrm{iid}}_{\min} \leftarrow N$
return $k^{\mathrm{iid}}_{\min}$ and $N^{\mathrm{iid}}_{\min}$.
```

Algorithm 2 is quite useful to studying the variations of $N^{\mathrm{iid}}_{\min}(\epsilon,\delta,\lambda,r)$ with λ, δ, ϵ, and r as illustrated in Fig. 7. When ϵ, r are fixed and δ approaches 0, $N^{\mathrm{iid}}_{\min}(\epsilon,\delta,\lambda,r)$ is proportional to $\ln\delta^{-1}$.

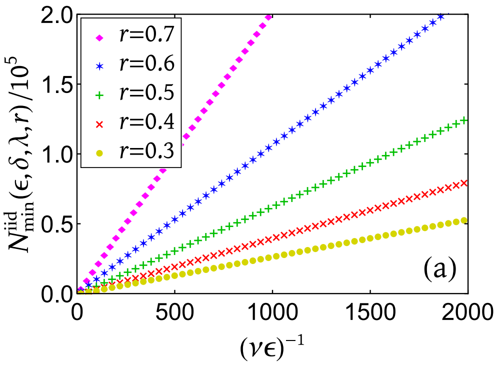

Fig. 7 Minimum number of tests required for robust verification in the i.i.d. scenario (by Algorithm 2). a Variations of $N_{\min}^{\mathrm{iid}}(\epsilon,\delta,\lambda,r)$ with $(\nu\epsilon)^{-1}$ and r, where $\delta = 0.01$. **b** Variations of $N_{\min}^{\mathrm{iid}}(\epsilon,\delta,\lambda,r)$ with $\log_{10}\delta^{-1}$ and r, where $\nu\epsilon = 0.005$.

When δ and r are fixed, $N_{\min}^{\mathrm{iid}}(\epsilon,\delta,\lambda,r)$ is inversely proportional to $\nu\epsilon$. This fact shows that strategies with larger spectral gaps are more efficient, in sharp contrast with the adversarial scenario.

At this point it is instructive to compare the minimum number of tests for robust verification in the adversarial scenario with the counterpart in the i.i.d. scenario. Numerical calculation shows that the ratio of $N_{\min}(\epsilon,\delta,\lambda,r)$ over $N_{\min}^{\mathrm{iid}}(\epsilon,\delta,\lambda,r)$ is decreasing in λ, as reflected in Fig. 8. For a typical value of λ, say $\lambda = 1/2$, this ratio is smaller than 2, so the sample complexity in the adversarial scenario is comparable to the counterpart in the i.i.d. scenario. When λ is small, one can construct another strategy with a larger λ by adding the trivial test [see Eq. (6)], which can achieve a higher efficiency in the adversarial scenario. Due to this reason, the ratio of $N_{\min}(\epsilon,\delta,\lambda,r)$ over $N_{\min}^{\mathrm{iid}}(\epsilon,\delta,\lambda,r)$ is not so important when $\lambda \leq 0.3$.

The following proposition provides a guideline for choosing appropriate parameters N and k for achieving a given verification precision and robustness.

Proposition 6. Suppose $0 < \delta,\ \epsilon,\ r < 1$ and $0 \leq \lambda < 1$. Then the conditions of soundness and robustness in Eq. (33) hold as long as $s \in (r\epsilon,\ \epsilon)$, $k = \lfloor \nu s N \rfloor$, and

$$N \geq \left\lceil \frac{\ln \delta^{-1}}{\min\{D(\nu s\|\nu r\epsilon), D(\nu s\|\nu\epsilon)\}} \right\rceil. \tag{35}$$

For $0 < p,\ r < 1$ we define functions

$$\zeta(r,p) := p\left[D\left(\frac{\ln\left(\frac{1-p}{1-rp}\right)}{\ln r + \ln\left(\frac{1-p}{1-rp}\right)}\middle\| p\right)\right]^{-1}, \tag{36}$$

$$\xi(r) := \lim_{p\to 0}\zeta(r,p) = \left[\frac{r-1}{\ln r}\ln\left(\frac{r-1}{\ln r}\right) + \left(1 - \frac{r-1}{\ln r}\right)\right]^{-1}. \tag{37}$$

By virtue of Proposition 6 we can derive the following informative bounds (for $0 < \delta,\ \epsilon,\ r < 1$),

$$N_{\min}^{\mathrm{iid}}(\epsilon,\delta,\lambda,r) \leq \left\lceil \frac{\ln\delta^{-1}}{\nu\epsilon}\zeta(r,\nu\epsilon)\right\rceil \leq \left\lceil \frac{\ln\delta^{-1}}{\nu\epsilon}\xi(r)\right\rceil. \tag{38}$$

These bounds become tighter when the significance level δ approaches 0, as shown in Supplementary Figure 4. The coefficient $\xi(r)$ in the second bound is plotted in Supplementary Figure 5. When $r = \lambda = 1/2$ for instance, the second upper bound in Eq. (38) implies that

$$N_{\min}^{\mathrm{iid}}(\epsilon,\delta,\lambda,r) \leq \left\lceil \frac{2\,\xi(1/2)\ln\delta^{-1}}{\epsilon}\right\rceil \leq \left\lceil \frac{46.5\ln\delta^{-1}}{\epsilon}\right\rceil, \tag{39}$$

while numerical calculation shows that $N_{\min}^{\mathrm{iid}}(\epsilon,\delta,\lambda,r)$ is smaller than $41\,\epsilon^{-1}\ln\delta^{-1}$ for $\delta \geq 10^{-10}$ and approaches $2\,\xi(1/2)\,\epsilon^{-1}\ln\delta^{-1}$ when $\delta,\ \epsilon \to 0$. Therefore, our protocol can enable robust and efficient verification of quantum states in the i.i.d. scenario.

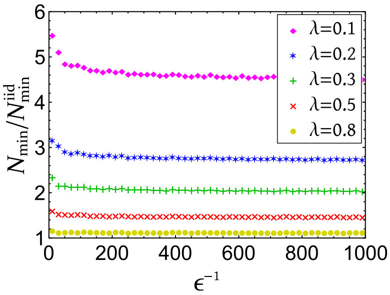

Fig. 8 The ratio of $N_{\min}(\epsilon,\delta,\lambda,r)$ over $N_{\min}^{\mathrm{iid}}(\epsilon,\delta,\lambda,r)$ with $\epsilon = \delta$ and $r = 1/2$. Here $N_{\min}(\epsilon,\delta,\lambda,r)$ and $N_{\min}^{\mathrm{iid}}(\epsilon,\delta,\lambda,r)$ are the minimum numbers of tests required for robust verification in the adversarial scenario and i.i.d. scenario, respectively.

Finally, it is instructive to clarify the relation between QSV in the i.i.d. scenario, nonadversarial scenario, and adversarial scenario. In the i.i.d. scenario, the assumptions on the source are the strongest, so QSV is the easiest, and the sample cost is the smallest. In the adversarial scenario, by contrast, the assumptions on the source are the weakest, so QSV is the most difficult, and the sample cost is the largest. For graph states with a prime local dimension, the sample cost in the adversarial scenario is comparable to the counterpart in the i.i.d. scenario thanks to our analysis above, which means the sample costs in all three scenarios are comparable.

DATA AVAILABILITY

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

CODE AVAILABILITY

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

Received: 16 March 2023; Accepted: 27 October 2023;
Published online: 14 November 2023

REFERENCES

1. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. *In*: 1994 IEEE 35th Annual Symposium on Foundations of Computer Science (FOCS) (1994), pp. 124–134.
2. Nielsen, M. A. & Chuang, I. L. Quantum computation and quantum information (Cambridge University Press, Cambridge, U.K., 2000).

3. Preskill, J. Quantum computing in the NISQ era and beyond. *Quantum* **2**, 79 (2018).
4. Fitzsimons, J. F. Private quantum computation: an introduction to blind quantum computing and related protocols. *npj Quantum Inf.* **3**, 23 (2017).
5. Broadbent, A., Fitzsimons, J. F. & Kashefi, E. Universal blind quantum computation. *In:* 2009 IEEE 50th Annual Symposium on Foundations of Computer Science (FOCS), pp. 517–526 (2006).
6. Morimae, T. & Fujii, K. Blind quantum computation protocol in which Alice only makes measurements. *Phys. Rev. A* **87**, 050301(R) (2013).
7. Mantri, A., Pérez-Delgado, C. A. & Fitzsimons, J. F. Optimal blind quantum computation. *Phys. Rev. Lett.* **111**, 230502 (2013).
8. Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496**, 456 (2013).
9. Barz, S. et al. Demonstration of blind quantum computing. *Science* **335**, 303 (2012).
10. Barz, S., Fitzsimons, J. F., Kashefi, E. & Walther, P. Experimental verification of quantum computation. *Nat. Phys.* **9**, 727–731 (2013).
11. Greganti, C., Roehsner, M.-C., Barz, S., Morimae, T. & Walther, P. Demonstration of measurement-only blind quantum computing. *New J. Phys.* **18**, 013020 (2016).
12. Jiang, Y.-F. et al. Remote blind state preparation with weak coherent pulses in the field. *Phys. Rev. Lett.* **123**, 100503 (2019).
13. Raussendorf, R. & Briegel, H. J. A one-way quantum computer. *Phys. Rev. Lett.* **86**, 5188 (2001).
14. Raussendorf, R., Browne, D. E. & Briegel, H. J. Measurement-based quantum computation on cluster states. *Phys. Rev. A* **68**, 022312 (2003).
15. Briegel, H. J., Dür, W., Raussendorf, R. & Van den Nest, M. Measurement-based quantum computation. *Nat. Phys.* **5**, 19 (2009).
16. Hayashi, M. & Morimae, T. Verifiable measurement-only blind quantum computing with stabilizer testing. *Phys. Rev. Lett.* **115**, 220502 (2015).
17. Fujii, K. & Hayashi, M. Verifiable fault tolerance in measurement-based quantum computation. *Phys. Rev. A* **96**, 030301(R) (2017).
18. Morimae, T., Takeuchi, Y. & Hayashi, M. Verification of hypergraph states. *Phys. Rev. A* **96**, 062321 (2017).
19. Hayashi, M. & Hajdušek, M. Self-guaranteed measurement-based blind quantum computation. *Phys. Rev. A* **97**, 052308 (2018).
20. Takeuchi, Y., Mantri, A., Morimae, T., Mizutani, A. & Fitzsimons, J. F. Resource-efficient verification of quantum computing using Serfling's bound. *npj Quantum Inf.* **5**, 27 (2019).
21. Xu, Q., Tan, X., Huang, R. & Li, M. Verification of blind quantum computation with entanglement witnesses. *Phys. Rev. A* **104**, 042412 (2021).
22. Arute, F. et al. Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505 (2019).
23. Zhong, H.-S. et al. Quantum computational advantage using photons. *Science* **370**, 1460 (2020).
24. Gheorghiu, A., Kapourniotis, T. & Kashefi, E. Verification of quantum computation: an overview of existing approaches. *Theory Comput. Syst.* **63**, 715–808 (2019).
25. Šupić, I. & Bowles, J. Self-testing of quantum systems: a review. *Quantum* **4**, 337 (2020).
26. Eisert, J. et al. Quantum certification and benchmarking. *Nat. Rev. Phys.* **2**, 382–390 (2020).
27. Carrasco, J., Elben, A., Kokail, C., Kraus, B. & Zoller, P. Theoretical and experimental perspectives of quantum verification. *PRX Quantum* **2**, 010102 (2021).
28. Kliesch, M. & Roth, I. Theory of quantum system certification. *PRX Quantum* **2**, 010201 (2021).
29. Yu, X.-D., Shang, J. & Gühne, O. Statistical methods for quantum state verification and fidelity estimation. *Adv. Quantum Technol.* **5**, 2100126 (2022).
30. Zhu, H. & Hayashi, M. Efficient verification of pure quantum states in the adversarial scenario. *Phys. Rev. Lett.* **123**, 260504 (2019).
31. Zhu, H. & Hayashi, M. General framework for verifying pure quantum states in the adversarial scenario. *Phys. Rev. A* **100**, 062335 (2019).
32. Takeuchi, Y. & Morimae, T. Verification of Many-Qubit states. *Phys. Rev. X* **8**, 021060 (2018).
33. Zhu, H. & Hayashi, M. Efficient verification of hypergraph states. *Phys. Rev. Appl.* **12**, 054047 (2019).
34. Li, Z., Zhu, H. & Hayashi, M. Significance improvement by randomized test in random sampling without replacement. Preprint at https://arxiv.org/abs/2211.02399 (2022).
35. Keet, A., Fortescue, B., Markham, D. & Sanders, B. C. Quantum secret sharing with qudit graph states. *Phys. Rev. A* **82**, 062315 (2010).
36. Pallister, S., Linden, N. & Montanaro, A. Optimal verification of entangled states with local measurements. *Phys. Rev. Lett.* **120**, 170502 (2018).
37. Gheorghiu, A., Kashefi, E. & Wallden, P. Robustness and device independence of verifiable blind quantum computing. *New J. Phys.* **17**, 083040 (2015).
38. Gočanin, A., Šupić, I. & Dakić, B. Sample-efficient device-independent quantum state verification and certification. *PRX Quantum* **3**, 010317 (2022).
39. Hayashi, M., Matsumoto, K. & Tsuda, Y. A study of LOCC-detection of a maximally entangled state using hypothesis testing. *J. Phys. A: Math. Gen.* **39**, 14427 (2006).
40. Hayashi, M. Group theoretical study of LOCC-detection of maximally entangled state using hypothesis testing. *New J. Phys.* **11**, 043028 (2009).
41. Zhu, H. & Hayashi, M. Optimal verification and fidelity estimation of maximally entangled states. *Phys. Rev. A* **99**, 052346 (2019).
42. Li, Z., Han, Y.-G. & Zhu, H. Efficient verification of bipartite pure states. *Phys. Rev. A* **100**, 032316 (2019).
43. Wang, K. & Hayashi, M. Optimal verification of two-qubit pure states. *Phys. Rev. A* **100**, 032315 (2019).
44. Li, Z., Han, Y.-G. & Zhu, H. Optimal verification of greenberger-Horne-Zeilinger states. *Phys. Rev. Appl.* **13**, 054002 (2020).
45. Li, Z., Han, Y.-G., Sun, H.-F., Shang, J. & Zhu, H. Verification of phased Dicke states. *Phys. Rev. A* **103**, 022601 (2021).
46. Liu, Y.-C., Li, Y., Shang, J. & Zhang, X. Verification of arbitrary entangled states with homogeneous local measurements. *Adv. Quantum Technol.* **6**, 2300083 (2023).
47. Hajdušek, M., Pérez-Delgado, C. A. & Fitzsimons, J. F. Device-independent verifiable blind quantum computation. Preprint at https://arxiv.org/abs/1502.02563 (2015).
48. Coladangelo, A., Grilo, A. B., Jeffery, S. & Vidick, T. Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. *In:* Annual international conference on the theory and applications of cryptographic techniques, pp. 247–277, (Springer, 2019).
49. Aharonov, D., Ben-Or, M. & Eban, E. Interactive proofs for quantum computations. *In:* Innovations in computer science (ICS), pp. 453–469 (Tsinghua University Press, 2010).
50. Broadbent, A. How to verify a quantum computation. *Theory Comput.* **14**, 09 (2015).
51. Fitzsimons, J. F. & Kashefi, E. Unconditionally verifiable blind quantum computation. *Phys. Rev. A* **96**, 012303 (2017).
52. Mahadev, U. Classical verification of quantum computations. *In:* 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS), pp. 259–267 (2018).
53. Gheorghiu, A. & Vidick, T. Computationally-secure and composable remote state preparation. *In:* 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS), pp. 1024–1033 (2019).
54. Bartusek, J. et al. Succinct classical verification of quantum computation. *In:* Advances in Cryptology - CRYPTO 2022: 42nd Annual International Cryptology Conference, pp. 195–211 (Springer, 2022).
55. Zhang, J. Classical verification of quantum computations in linear time. *In*: 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS), pp. 46–57 (2022).
56. Yu, X.-D., Shang, J. & Gühne, O. Optimal verification of general bipartite pure states. *npj Quantum Inf.* **5**, 112 (2019).
57. Dangniam, N., Han, Y.-G. & Zhu, H. Optimal verification of stabilizer states. *Phys. Rev. Res.* **2**, 043323 (2020).
58. Hayashi, M. & Takeuchi, Y. Verifying commuting quantum computations via fidelity estimation of weighted graph states. *New J. Phys.* **21**, 093060 (2019).
59. Liu, Y.-C., Yu, X.-D., Shang, J., Zhu, H. & Zhang, X. Efficient verification of Dicke states. *Phys. Rev. Appl.* **12**, 044020 (2019).
60. Zhu, H., Li, Y. & Chen, T. Efficient verification of ground states of frustration-free Hamiltonians. Preprint at https://arxiv.org/abs/2206.15292 (2022).
61. Chen, T., Li, Y. & Zhu, H. Efficient verification of Affleck-Kennedy-Lieb-Tasaki states. *Phys. Rev. A* **107**, 022616 (2023).
62. Liu, Y.-C., Shang, J. & Zhang, X. Efficient verification of entangled continuous-variable quantum states with local measurements. *Phys. Rev. Res.* **3**, L042004 (2021).
63. Miguel-Ramiro, J., Riera-Sàbat, F. & Dür, W. Collective operations can exponentially enhance quantum state verification. *Phys. Rev. Lett.* **129**, 190504 (2022).
64. Zhang, W.-H. et al. Experimental optimal verification of entangled states using local measurements. *Phys. Rev. Lett.* **125**, 030506 (2020).
65. Zhang, W.-H. et al. Classical communication enhanced quantum state verification. *npj Quantum Inf.* **6**, 103 (2020).
66. Jiang, X. et al. Towards the standardization of quantum state verification using optimal strategies. *npj Quantum Inf.* **6**, 90 (2020).
67. Xia, L. et al. Experimental optimal verification of three-dimensional entanglement on a silicon chip. *New J. Phys.* **24**, 095002 (2022).

ACKNOWLEDGEMENTS

The work at Fudan is supported by the National Natural Science Foundation of China (Grants no. 92165109 and no. 11875110), the National Key Research and Development Program of China (Grant no. 2022YFA1404204), and Shanghai Municipal Science and

Technology Major Project (Grant no. 2019SHZDZX01). MH is supported in part by the National Natural Science Foundation of China (Grants no. 62171212 and no. 11875110) and Guangdong Provincial Key Laboratory (Grant no. 2019B121203002).

AUTHOR CONTRIBUTIONS

H.Z. and M.H. proposed this project. Z.L., H.Z., and M.H. derived the theoretical results. Z.L. performed numerical calculations and plotted the figures. Z.L., H.Z., and M.H. wrote the paper.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-023-00783-9.

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

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

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