Verification of graph states in an untrusted network

Anupama Unnikrishnan[1] and Damian Markham[2,3]

[1]*Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom*
[2]*LIP6, CNRS, Sorbonne Université, 4 Place Jussieu, 75005 Paris, France*
[3]*JFLI, CNRS National Institute of Informatics, University of Tokyo, 113-0033 Tokyo, Japan*

Graph states are a large class of multipartite entangled quantum states that form the basis of schemes for quantum computation, communication, error correction, metrology, and more. In this work, we consider verification of graph states generated by an untrusted source and shared between a network of possibly dishonest parties. This has implications in certifying the application of graph states for various distributed tasks. We present a protocol which is globally efficient for a large family of useful graph states, including cluster states, GHZ states, cycle graph states, and more. For general graph states, efficiency with respect to the security parameter is maintained, though there is a cost increase with the size of the graph state. The protocols are practical, requiring only multiple copies of the graph state, local measurements, and classical communication.

The usefulness of graph states extends across the field of quantum information, with their inherent multipartite entanglement leading them to be promising candidates for a variety of tasks. As quantum states that correspond to mathematical graphs, where vertices represent qubits and edges preparation entanglement, graph states may possess varied entanglement that render them ideal for applications ranging from quantum computation [1–3] and error correction [4,5] to cryptography [6,7], metrology [8–10], and more [11–13].

As such, the verification of these resource states is a natural problem, and has been the topic of much investigation, under different assumptions of trust and particular questions of interest [14]. For example, in tomography, one wishes to find the density matrix of the state, while trusting measuring devices and that the state is not correlated across preparations, i.e., that it is independent and identically distributed (i.i.d.) [15]. With entanglement witnesses, on the other hand, we have the same trust settings but are interested only in demonstrating entanglement [16]. In cryptographic settings, one is often interested in the case where measurement devices are trusted, but the sources of the states are not, and in fact not even that they are i.i.d. [17–21]. Going further, in self-testing and device-independent approaches, one does not trust the source or the measurement devices [22]. These techniques have had applications across quantum information for verification of delegated quantum computation [17–20], simulation [23], sampling, and network tasks [17,24].

In all these examples, however, all of the participating parties behave in an honest way; it is the source or their devices which are not trusted. One may also be interested in a stronger type of scenario, where a graph state is distributed over a network of parties each holding a share of the state, but where, crucially, not all the parties behave in an honest way. This is an important cryptographic scenario, which has applications, for example, in the task of secure multiparty quantum computation [25,26], involving a set of possibly dishonest parties who wish to compute some function of their inputs. The first efforts to verify states in this scenario were for GHZ states [27–29]. This has already found application, for example, in anonymous transmission of quantum messages [7]. The ubiquity of graph states for quantum information naturally suggests the interest in generalizing such an approach to all graph states.

In this work, we present a way of verifying graph states across a network with untrusted parties. Our protocol is globally efficient in the number of copies required for families of graph states, including many graph states of interest. These include the complete graph state (locally equivalent to the GHZ state), one- and two-dimensional cluster states, and cyclic graph states, which are resource states for quantum metrology [8,10], universal quantum computation [1,30], and error correction [4,5], respectively. For an arbitrary graph state, our protocol maintains efficiency with respect to the security parameter (i.e., how sure we are that the state is good), but requires a number of copies of the graph state that grow exponentially with the size of the graph state. This cost arises since, in general, we lack certain symmetries which allow for efficiency. For small or fixed-size networks requiring fixed-size graph states, this cost may not be too burdensome, as there the security parameter efficiency dominates.

For ease of presentation, we break our work down into two protocols. The first follows very closely to [20], extending its use to dishonest networks, but requires an assumption on one party (the Verifier) to act honestly. Building on this, the second protocol is more involved, but removes this assumption. In this way, all parties are equally treated with no assumption of their honest behavior, and we refer to this as the symmetric protocol.

I. COMMUNICATION SCENARIO

Our network consists of n parties, split into sets of honest and dishonest parties, which we will denote by H and D, respectively. An untrusted source is asked to produce the n-qubit graph states requested by the parties, but may provide any states they wish, including entangled across copies and with possible registers reserved by the source for later use. The parties are only required to apply local operations and measurements, and communicate classically. While the honest parties follow the protocol, the dishonest parties might not, and can work together and do anything to their part of the state, as well as collaborate with the source to disrupt the protocol. Note that the honest parties do not need to know the identity of other honest parties, whereas the dishonest parties are assumed to have all the information about who is honest and dishonest. Each pair of parties must share a private classical channel. For the symmetric version of the protocol, we also require a trusted common random source.

II. PROTOCOL

Before we begin, let us give a brief description of stabilizers. The n-qubit graph state $|\mathcal{G}\rangle$ associated to a graph $\mathcal{G}$ can be uniquely specified by its stabilizer group S as follows. To each qubit $i \in \{1, \ldots, n\}$, we associate a *stabilizer generator* $K_i = X_i \prod_{e \in N(i)} Z_e$, where $N(i)$ is the set of neighboring vertices to i in the graph and X_i and Z_i are the Pauli operators acting on qubit i. The full *stabilizer group* S is generated by taking all 2^n products of the stabilizer generators. The graph state $|\mathcal{G}\rangle$ is the unique $+1$ eigenstate of every stabilizer $S_j \in S$.

An intuitive way to test a particular graph state is then to check that all stabilizer measurements give a $+1$ outcome. If all parties are honest, this can only happen if the source has sent them the ideal graph state (since it is the unique $+1$ eigenstate). By asking for many copies and randomly choosing which stabilizer to measure after the source has sent each copy, the parties can prevent the source from creating some other state that would pass an individual stabilizer measurement but not the full set. In fact, this is the essential idea behind many of the verification protocols for graph states, with details differing depending on trust, security statements, and efficiency [17–21,31–33]. Here, we extend this approach to account for any number of dishonest parties, who may work together and coordinate with the dishonest source.

To achieve this goal, we will use and adapt the verification protocol from [20]. Our Protocol I is almost identical to that of [20], although the security proof requires completely new elements at the state level to deal with dishonest parties. At this stage, however, the protocol still requires one party, the Verifier, to behave honestly. We then adapt it to build a new protocol to deal with the possibility of dishonest Verifiers, which we call the symmetric scenario (i.e., all parties are treated equally), in Protocol II.

The presence of dishonest parties affects the efficiency of the protocol. While the protocol in [20] only requires measuring the stabilizer generators, in order to extend this to any graph state with any number of dishonest parties, the parties must measure the full set of stabilizers, which leads to the requirement of exponentially many copies with graph size.

Protocol 1 VERIFICATION OF GRAPH STATE

Input: The parties choose values of $N_{\text{test}}, N_{\text{total}}$. Let $\mathcal{S}$ be the set of test measurements, and $\mathsf{J} = |\mathcal{S}|$.

1: An untrusted source generates N_{total} copies of the graph state, and sends the shares to the parties.

2: The parties repeat the following for $j = 1, \ldots, \mathsf{J}$:
(a) The Verifier chooses N_{test} copies from the remaining $N_{\text{total}} - (j-1)N_{\text{test}}$ copies independently and uniformly at random.
(b) For each copy, the Verifier instructs each party to perform the measurement corresponding to their part of the stabilizer $\mathcal{S}_j$.
(c) For each copy, the parties send their measurement outcome to the Verifier, who calculates the total measurement outcome. The copy passes the test if the total measurement outcome is $+1$. Let $N_{\text{pass},j}$ be the number of copies that pass the stabilizer test for $\mathcal{S}_j$.

3: The Verifier uniformly randomly chooses a single copy from the remaining $\mathsf{N} \equiv N_{\text{total}} - \mathsf{J}N_{\text{test}}$ copies that were not used for the tests in the previous steps. The chosen single copy is called the target copy. The others are discarded.

4: If $N_{\text{pass}} \equiv \sum_{j=1}^{\mathsf{J}} N_{\text{pass},j} \geqslant \mathsf{J}N_{\text{test}} - \frac{N_{\text{test}}}{2\mathsf{J}}$, the parties use the target copy for their application; otherwise, the target copy is discarded.

This scaling is due to the power of our adversarial model. We will show afterwards how to reduce this requirement if we have more information about the dishonest parties, or for specific families of graph states of interest.

Protocol 2 SYMMETRIC PROTOCOL FOR VERIFICATION OF GRAPH STATE

Input: The parties choose values of $N_{\text{test}}, N_{\text{total}}, \lambda$. Let $\mathcal{S}$ be the set of test measurements, and $\mathsf{J} = |\mathcal{S}|$.

1: An untrusted source generates N_{total} copies of the graph state, and sends the shares to the parties.

2: The parties repeat the following for $j = 1, \ldots, \mathsf{J}$:
(a) The CRS chooses λN_{test} copies from the remaining $N_{\text{total}} - (j-1)\lambda N_{\text{test}}$ copies independently and uniformly at random. These are split into λ sets of N_{test} copies, again at random by the CRS. For each set of N_{test} copies, the CRS chooses a random party to be the Verifier.
(b) For each copy, the corresponding Verifier instructs each party to perform the measurement corresponding to their part of the stabilizer $\mathcal{S}_j$.
(c) For each copy, the parties send their measurement outcome to the Verifier, who calculates the total measurement outcome. The copy passes the test if the total measurement outcome is $+1$. Let $N_{\text{pass},j}$ be the number of copies that pass the stabilizer test for $\mathcal{S}_j$.

3: The CRS uniformly randomly chooses a single copy from the remaining $\mathsf{N} \equiv N_{\text{total}} - \lambda \mathsf{J}N_{\text{test}}$ copies that were not used for the tests in the previous steps. The chosen single copy is called the target copy. The others are discarded.

4: If $N_{\text{pass}} \equiv \sum_{j=1}^{\mathsf{J}} N_{\text{pass},j} \geqslant \lambda \mathsf{J}N_{\text{test}} - \frac{N_{\text{test}}}{2\mathsf{J}}$, the parties use the target copy for their application; otherwise, the target copy is discarded.

III. SECURITY ANALYSIS

We first consider the case of an arbitrary n-qubit graph state, denoted by $|\mathcal{G}\rangle$, and assume an honest Verifier. The parties perform Protocol I, measuring the full set of $\mathsf{J} = 2^n$ stabilizers (i.e., we take the set of test measurements $\mathcal{S}$ to be the full stabilizer group S), to test whether the state they receive in each round, $|\Psi\rangle$, is the ideal graph state $|\mathcal{G}\rangle$, even in the presence of dishonest parties.

In a network with dishonest parties who may collaborate with the source of the state, we may take the state $|\Psi\rangle$ to be pure, as the dishonest parties can purify it by adding a reference system. Further, in such a network, we can only make statements on the fidelity up to local operations on the dishonest part. By Uhlmann's theorem [34], this refers to the fidelity between the reduced states of the honest parties.

Let us then take $\rho_H^{|\mathcal{G}\rangle}$ to be the reduced state of the honest parties in the ideal case (i.e., when they share $|\mathcal{G}\rangle$), and ρ_H^{avg} to be the reduced state of the honest parties of the averaged state of the target copy (over all random selections from the remaining N copies). We prove the security of our protocol in the following theorem for the case of an honest Verifier.

Theorem 1. Assuming an honest Verifier, if we set $N_{\text{total}} = 2 \times 2^n N_{\text{test}}$, $N_{\text{test}} = \lceil m2^{4n} \ln 2^n \rceil$, and $\mathcal{S}$ as the full set of stabilizers, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol I satisfies

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}}\right) \geqslant 1 - \frac{2\sqrt{c}}{2^n} - 2 \times 2^n \left(1 - \frac{N_{\text{pass}}}{2^n N_{\text{test}}}\right) \quad (1)$$

is at least $1 - (2^n)^{1 - \frac{2cm}{3}}$, where m, c are positive constants chosen such that $\frac{3}{2m} < c < \frac{(2^n - 1)^2}{4}$.

Proof sketch. Our proof has three main stages. In the first stage, we show that if all stabilizer tests pass perfectly, the state in each round of the protocol must be $|\Psi\rangle = U_D|\mathcal{G}\rangle$, where U_D is a unitary on the dishonest part of the state. This is the main part of our proof. To do this, we demonstrate that, for the Schmidt decomposition of the state corresponding to the partition (H, D), the Schmidt basis of the honest parties is the same for the actual and ideal states. We illustrate this by writing the unknown actual state as

$$|\Psi\rangle = \sum_{\bar{z}} \alpha_{\bar{z}} |\bar{z}\rangle_H \otimes |\psi_{\bar{z}}\rangle_D, \quad (2)$$

$$|\Psi\rangle = \sum_{\bar{x}} \beta_{\bar{x}} |\mathcal{H}_{(\bar{x})}\rangle_H \otimes |\phi_{\bar{x}}\rangle_D, \quad (3)$$

where $\bar{z}, \bar{x}$ are classical $|H|$-bit strings, $\alpha_{\bar{z}}, \beta_{\bar{x}}$ are unknown complex coefficients, and $\{|\bar{z}\rangle\}, \{|\mathcal{H}_{(\bar{x})}\rangle\}$ form complete bases for the honest side, where $|\mathcal{H}_{(\bar{x})}\rangle$ is the state corresponding to the honest subgraph with σ_Z's applied on vertices according to $\bar{x}$ (that is, σ_Z applied to the qubit of party i iff $x_i = 1$), and $|\psi_{\bar{z}}\rangle, |\phi_{\bar{x}}\rangle$ are the corresponding states on the dishonest side. We identify, purely from the fact that all stabilizer generator tests pass perfectly, which elements in $\{|\psi_{\bar{z}}\rangle\}$ and $\{|\phi_{\bar{x}}\rangle\}$ are orthogonal to each other. Passing the full set of stabilizer tests allows us to see which $\beta_{\bar{x}}$ must be zero; this tells us which terms of $|\bar{z}\rangle$ must correspond to the same $\alpha_{\bar{z}}, |\psi_{\bar{z}}\rangle$. We then show that each unique $\alpha_{\bar{z}} = \pm \frac{1}{\sqrt{2^{|H|}}}$. Substituting this information in Eq. (2), we see that the honest Schmidt basis

of $|\Psi\rangle$ must be equal to the honest Schmidt basis of $|\mathcal{G}\rangle$. Thus, the only state $|\Psi\rangle$ that can pass every stabilizer test perfectly is such that $\rho_H^{|\Psi\rangle} = \rho_H^{|\mathcal{G}\rangle}$ (or, equivalently, $|\Psi\rangle = U_D|\mathcal{G}\rangle$).

In the second stage, we employ the Serfling bound to find that, after the 2^n test measurements, the fraction of states out of the remaining untested copies that would pass all tests perfectly is at least $1 - \frac{2\sqrt{c}}{2^n} - 2 \times 2^n (1 - \frac{N_{\text{pass}}}{2^n N_{\text{test}}})$, with probability at least $1 - (2^n)^{1 - \frac{2cm}{3}}$. This follows straightforwardly using the method of [20], but with 2^n test measurements corresponding to the full set of stabilizers.

In the final stage, we translate this statement to the reduced state of the honest parties of the target copy, which gives our final result.

The full proof is given in Appendix A. ∎

IV. EFFICIENT EXAMPLES

For certain graph states or sets of dishonest parties, we can reduce the resources required for verification; in fact, we see that simply by measuring the stabilizer generators, the desired statement can be made about the fidelity of the unknown state. Then, the parties can instead run Protocol I with a simplified set of test measurements (where $\mathsf{J} = n$). Such examples are given in the following theorem, whose graph states are shown in Fig. 1.

Theorem 2. If $|\mathcal{G}\rangle$ is either

A. a complete graph state with dishonest parties anywhere in the network, or

B. a pentagon graph state with either one, three, or four dishonest parties anywhere in the network, or two dishonest parties who are adjacent, or

C. a cycle graph state with either one, $n - 2$, or $n - 1$ dishonest parties anywhere in the network, or any other number of dishonest parties who are adjacent, or

D. a 1D cluster state with either one or $n - 1$ dishonest parties anywhere in the network, or any other number of adjacent honest or dishonest parties, or

E. a 2D cluster state with either one or $n - 1$ dishonest parties anywhere in the network, or any other set of adjacent dishonest parties that forms a square or rectangle anywhere in the network,

and we set $N_{\text{total}} = 2n N_{\text{test}}$, $N_{\text{test}} = \lceil mn^4 \ln n \rceil$, and $\mathcal{S}$ as the set of stabilizer generators, assuming an honest Verifier, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol I satisfies

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}\right) \geqslant 1 - \frac{2\sqrt{c}}{n} - 2n\left(1 - \frac{N_{pass}}{n N_{test}}\right) \quad (4)$$

is at least $1 - n^{1 - \frac{2cm}{3}}$, where m, c are positive constants chosen such that $\frac{3}{2m} < c < \frac{(n-1)^2}{4}$.

Proof sketch. First, we see that, for the examples A-E in Theorem 2, testing the stabiliser generators is sufficient to identify the terms that are zero in Equation (3). Then, we follow the remainder of the proof of Theorem 1, but with n test measurements corresponding to the generator tests, and extend our results to the target copy in the final step. The full details are given in Appendix II. ∎
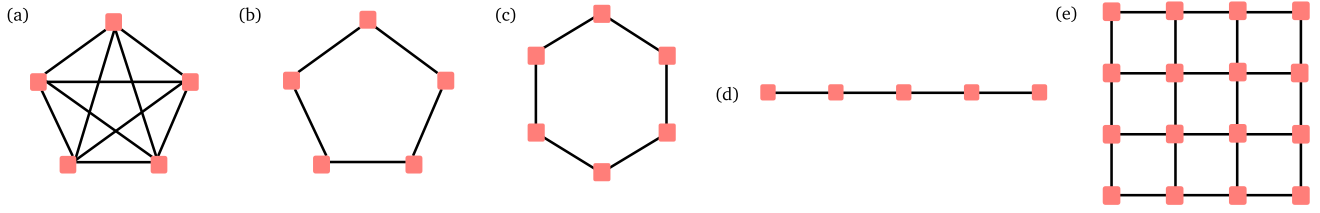
FIG. 1. Examples of a (a) complete graph, (b) pentagon graph, (c) cycle graph, (d) 1D cluster state, and (e) 2D cluster state. For quantum states that correspond to these types of graphs, one can perform efficient verification using Protocol I, possibly with some information regarding the dishonest parties, as shown in Theorem 2.

Noting that the GHZ state is locally equivalent to the complete graph state, example A offers an alternative to the verification protocol in [27].

V. SYMMETRIC PROTOCOL

Up to now, we have assumed that the party acting as the Verifier is honest. We will now remove this assumption. To do so, we increase the number of tested copies from N_{test} tests per stabilizer to λN_{test}, and make use of a trusted common random source (CRS) that provides the parties with shared randomness (following [27]). The CRS is used to replace the Verifier's choices and to pick which party acts as the Verifier. In this way, the honest parties are protected against a dishonest Verifier who may attempt to cheat. While using a CRS is an additional resource, it is natural that it is also required, as any protocol able to verify an entangled state can use this state to generate a CRS (for example, by sharing a GHZ state and measuring in the computational basis). A CRS can be created, for example, if a third or more of the network is honest, using [35].

Such a symmetric protocol is given in Protocol II, with the following adapted theorem, whose proof is given in Appendix C.

Theorem 3. If we set $N_{\text{total}} = (\lambda + 1)\lambda \mathsf{J} N_{\text{test}}$ and $N_{\text{test}} = \lceil m \mathsf{J}^4 \ln \mathsf{J} \rceil$, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol II satisfies

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}\right) \geqslant 1 - \left(\frac{1}{\lambda} - \frac{1}{\lambda^2}\right)$$
$$- \left(1 + \frac{1}{\lambda}\right)\left[\frac{\sqrt{c}}{\mathsf{J}} + \lambda \mathsf{J} - \frac{N_{\text{pass}}}{N_{\text{test}}}\right] \quad (5)$$

is at least $[1 - \sum_{x=0}^{\lambda} (1 - \frac{|H|}{n})^x (\frac{|H|}{n} \mathsf{J}^{-\frac{2cm}{3}})^{\lambda-x}]^{\mathsf{J}}$, where m, c are positive constants chosen such that the fidelity and probability expressions are greater than zero.

Replacing J by $\mathsf{J} = 2^n$ for a general graph state, and $\mathsf{J} = n$ for the special cases in Theorem 2, we recover symmetric versions of Theorems 1 and 2. The extra parameter λ allows the parties to further tailor the protocol to achieve their desired bounds, while taking into account their experimental limitations.

VI. DISCUSSION

In this work, we have shown how to verify any graph state shared between a network of parties who may or may not be trusted. Our protocols are easily implementable: performing a verified version of some task using graph states simply requires additional copies of the graph state. Indeed, recent experiments verifying the GHZ state [28] and secret sharing graph states [24] for trusted parties would need minimal changes to carry out our protocol, while giving increased security. The results here naturally extend to qudit graphs, as in [20].

We briefly consider the robustness and comparative efficiency of our protocols. In terms of robustness, we are interested in how the fidelity statements and probability of accept change when noise is introduced [20,36]. Our protocols follow the robustness properties of [20], in particular, the scaling of the accept probability with the number of tests (see Appendix D). Unsurprisingly, the additional tests required for the general case diminish robustness, whereas if only the generators need to be tested, such as for the examples in Theorem 2, we recover the linear scaling of [20]. Moving to the symmetric case (Theorem 3) does not greatly affect the robustness.

With respect to efficiency, we can compare with the case where all parties are trusted, studied in depth in [21,32,33]. In particular, these works also give lower bounds on the number of copies of a graph state needed to certify a given fidelity with a given probability of accept. Since our scenario is more paranoid (theirs corresponds to all parties being honest), these works give lower bounds for our protocols too. For the families of interest in Theorem 2, we achieve the same efficiency as [20]. For general graph states, where we cannot make use of symmetries, we suffer from an exponential overhead with the size of the graph state, but for a fixed-size graph we maintain efficiency with respect to the security (fidelity and probability). It is likely that further optimizations can be made for efficiency, either by adapting the protocol or different proof techniques [21,32,33,36,37], though it is not clear the same lower bounds will hold.

The efficient examples from Theorem 2 suggest several applications. Cluster states are universal for quantum computation [1,30] and can be used in a distributed setting, meaning their verification can be applied for secure multiparty computation [25,26]. The complete graph state, or locally equivalent GHZ state, is the optimal resource for quantum metrology [8,10], where verification would have applications for distributed or delegated sensing [38–41] in untrusted networks. The cycle graph state is both the most efficient state for error correction and a resource for secret sharing [42], again, with applications for further security in untrusted networks [24].

APPENDIX A: PROOF OF THEOREM 1

Using Protocol I, a network of parties, out of which any number may be dishonest, can verify any shared graph state. We now prove the following theorem to illustrate the security of this protocol, assuming for now that the Verifier is an honest party.

Theorem 1. Assuming an honest Verifier, if we set $N_{\text{total}} = 2 \times 2^n N_{\text{test}}$, $N_{\text{test}} = \lceil m2^{4n} \ln 2^n \rceil$, and $\mathcal{S}$ as the full set of stabilizers, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol I satisfies

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}\right) \geqslant 1 - \frac{2\sqrt{c}}{2^n} - 2 \times 2^n \left(1 - \frac{N_{\text{pass}}}{2^n N_{\text{test}}}\right) \quad \text{(A1)}$$

is at least $1 - (2^n)^{1 - \frac{2cm}{3}}$, where m, c are positive constants chosen such that $\frac{3}{2m} < c < \frac{(2^n - 1)^2}{4}$.

Proof. Our proof proceeds in stages. We will start by proving that if all stabilizer tests pass perfectly, then the state must be the ideal graph state, up to local unitaries on the dishonest parts of the state. This means that in order to pass perfectly, the source must create entanglement between the honest and dishonest parties. This is given in the following lemma.

Lemma 1. The only state that can pass all stabilizer tests perfectly in each round is $|\Psi\rangle = U_D |\mathcal{G}\rangle$, where U_D is a unitary on the dishonest part of the state.

Proof. Let s be the Schmidt rank of the graph state $|\mathcal{G}\rangle$ corresponding to the partition (H, D) into honest and dishonest vertices, $|\mathcal{H}\rangle$ be the state corresponding to the honest subgraph, and $E_{\mathcal{H}}$ be the set of edges within the honest subgraph.

Let $bn(x)$ be a function that converts a decimal number x into its binary representation, and let us define classical $|H|$-bit strings $\bar{\mathbf{z}}, \bar{\mathbf{x}} \in \{bn(0), \dots, bn(2^{|H|} - 1)\}$, where $|H|$ is the number of honest parties in the network. We will use z_a to refer to the ath element of $\bar{\mathbf{z}}$.

We will start by writing the Schmidt decomposition of the ideal state for the partition (H, D) from [11]. Some terms in $\{\bar{\mathbf{z}}\}$ may be grouped together as they have the same dishonest part, as given by

$$|\mathcal{G}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{z}}} (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} |\bar{\mathbf{z}}\rangle_H \otimes \prod_{a \in H} \left(\prod_{b \in N(a)} \sigma_Z^{(b)} \right)^{z_a}$$
$$\times |\mathcal{G} - \mathcal{H}\rangle_D \quad \text{(A2)}$$

$$= \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{z}}} (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} |\bar{\mathbf{z}}\rangle_H \otimes |\mathcal{G} - \mathcal{H}_{(f(\bar{\mathbf{z}}))}\rangle_D, \quad \text{(A3)}$$

where $f(\bar{\mathbf{z}})$ depends on $\bigoplus_{i \in N(d)} z_i$, $\forall d \in D$, and $\mathcal{G} - \mathcal{H}$ is the dishonest subgraph. Then, $|\mathcal{G} - \mathcal{H}_{(f(\bar{\mathbf{z}}))}\rangle$ is the state corresponding to the dishonest subgraph with σ_Z's applied to some

vertices depending on $\bar{\mathbf{z}}$. This means that for terms where $\bigoplus_{i \in N(d)} z_i$ is the same for all $d \in D$, the corresponding dishonest part $|\mathcal{G} - \mathcal{H}_{(f(\bar{\mathbf{z}}))}\rangle$ is the same, and so the $|\bar{\mathbf{z}}\rangle$s of these are grouped together.

Let $|\mathcal{H}_{(\bar{\mathbf{x}})}\rangle$ be the state corresponding to the honest subgraph with σ_Z's applied according to $\bar{\mathbf{x}}$ (for example, $|\mathcal{H}_{(001)}\rangle$ corresponds to a three-qubit graph with σ_Z applied to the third qubit). The set $\{|\mathcal{H}_{(\bar{\mathbf{x}})}\rangle\}$ for all $\bar{\mathbf{x}}$ forms a complete basis (the graph state basis), as does the set $\{|\bar{\mathbf{z}}\rangle\}$. The unknown state in any round of Protocol I can then be written using the following decomposition:

honest computational basis: $|\Psi\rangle = \sum_{\bar{\mathbf{z}}} \alpha_{\bar{\mathbf{z}}} |\bar{\mathbf{z}}\rangle_H \otimes |\psi_{\bar{\mathbf{z}}}\rangle_D$,

$\quad$ (A4)

honest subgraph basis: $|\Psi\rangle = \sum_{\bar{\mathbf{x}}} \beta_{\bar{\mathbf{x}}} |\mathcal{H}_{(\bar{\mathbf{x}})}\rangle_H \otimes |\phi_{\bar{\mathbf{x}}}\rangle_D$, (A5)

where $\alpha_{\bar{\mathbf{z}}}, \beta_{\bar{\mathbf{x}}}$ are complex coefficients, and both sets $\{|\psi_{\bar{\mathbf{z}}}\rangle\}, \{|\phi_{\bar{\mathbf{x}}}\rangle\}$ are the corresponding states on the dishonest side. So far, we have assumed nothing about the portion of the state in control of the dishonest parties since no matter what the source supplies, the dishonest parties may do anything to their part to cheat in the protocol.

In Protocol I, the test measurements are the elements $\mathcal{S}_{j \in \{1, \dots, 2^n\}}$ belonging to the full stabilizer group. These measurements are generated by the stabilizer generators $K_{i \in \{1, \dots, n\}}$ of each qubit i. Thus, the full stabilizer group $\mathcal{S}$ is given by

$$\mathcal{S} = \left\langle \left\{ K_i = X_i \prod_{e \in N(i)} Z_e \right\}_{i=1}^n \right\rangle. \quad \text{(A6)}$$

We want to determine the form of the state given that all the test measurements pass perfectly. Let us now group the test measurements into two sets, such that group 1 contains only $\mathbb{1}, Z$ for the honest part, and group 2 contains everything else.

We first consider the measurements in group 1. This set contains the stabilizer generators corresponding to the dishonest qubits, i.e., $K_{i \in D}$. For each dishonest qubit, the honest part of the corresponding stabilizer generator measurement will be composed of Z measurements on the honest qubits that are in the neighborhood of the dishonest qubit, and $\mathbb{1}$ on those that are not. We can then write the set of stabilizer generators belonging to group 1 as

$$\left\{ \forall d \in D, \left[\bigotimes_{i \in N(d)} Z_i \bigotimes_{i \notin N(d)} \mathbb{1}_i \right]_H \otimes (M'_d)_D \right\}, \quad \text{(A7)}$$

where $(M'_d)_D$ is the measurement on the dishonest part, the form of which does not matter here. Let $\bar{\mathbf{z}}, \bar{\mathbf{z}}'$ be two strings in the computational basis expansion of $|\Psi\rangle$. If $\bigoplus_{i \in N(d)} z_i \neq \bigoplus_{i \in N(d)} z_i'$, then each honest measurement $\bigotimes_{i \in N(d)} Z_i \bigotimes_{i \notin N(d)} \mathbb{1}_i$ will give different outcomes for $\bar{\mathbf{z}}, \bar{\mathbf{z}}'$ since the outcome of the Z measurement on all $i \in N(d)$ depends on the parity of the string (how many 1's). So, to pass perfectly, $(M'_d)_D$ must also give different outcomes. In order to do this, the dishonest parties must be able to guess the honest parties' outcome perfectly, which means that they must be able to perfectly discriminate between the corresponding $|\psi_{\bar{\mathbf{z}}}\rangle, |\psi_{\bar{\mathbf{z}}'}\rangle$; this tells them the outcome they should get in order to pass the test.

This means that we must have $\langle \psi_{\bar{z}} | \psi_{\bar{z}'} \rangle = 0$. In general, we can write this as

$$\forall \, \bar{z}, \bar{z}', \text{ if } \exists \, d \in D \text{ such that } \bigoplus_{i \in N(d)} z_i \neq \bigoplus_{i \in N(d)} z_i',$$

$$\text{then } \langle \psi_{\bar{z}} | \psi_{\bar{z}'} \rangle = 0. \tag{A8}$$

We will now see that if the measurements in group 2 pass perfectly, we get certain $\beta_{\bar{x}} = 0$, and for all $\beta_{\bar{x}} \neq 0$, the corresponding $|\phi_{\bar{x}}\rangle$'s will be orthogonal to each other.

To prove orthogonality, note that the set of stabilizer generators in group 2 contains all the stabilizer measurements with X in the honest part (the stabilizer generator corresponding to each qubit in the honest set). So, the honest part of the measurements in the group is of the form $\{X_1 M_2 M_3 \ldots M_n, M_1 X_2 M_3 \ldots M_n, M_1 M_2 X_3 \ldots M_n, \ldots, M_1 \ldots X_n\}$, where the honest measurement $M_{i \in \{1,\ldots,n\}}$ is either $\mathbb{1}$ or Z. Since no two states in the $|\mathcal{H}_{(\bar{x})}\rangle$ basis will give the same outcome for every one of these measurements, in order to pass perfectly, the dishonest parties must be able to discriminate between all corresponding $|\phi_{\bar{x}}\rangle$ to perfectly guess the honest outcome. We can write this as

$$\forall \, \bar{x} \neq \bar{x}', \ \langle \phi_{\bar{x}} | \phi_{\bar{x}'} \rangle = 0. \tag{A9}$$

To determine which $\beta_{\bar{x}} = 0$, we will use the measurements with dishonest part $M_D' = (\mathbb{1} \ldots \mathbb{1})'$. Let $A \subset H$ be a set containing vertices in H such that all $d \in D$ have an even number of neighbors in A. (Note that there may be multiple such sets A.) Now, let K_i be the stabilizer generator of qubit i of $|\mathcal{G}\rangle$, and k_i be the stabilizer generator of qubit i of $|\mathcal{H}\rangle$. We can then write a subset of the group 2 measurements as

$$\prod_{i \in A} K_i = \prod_{i \in A} (k_i)_H \otimes \mathbb{1}_D'. \tag{A10}$$

When the dishonest parties are asked to measure $\mathbb{1}$, they must always give outcome $+1$. So, in order to pass perfectly, the honest part must also give $+1$ outcome. In the expansion of

the state in Eq. (A5), if for any set A, we do not have an even number of σ_Z's on the qubits $i \in A$ in the honest subgraph, then the honest measurement will not give outcome $+1$. Since the positions of the σ_Z's are determined by the string $\bar{x}$, passing the group 2 measurements perfectly tells us that

$$\text{if } \exists A \text{ s.t. } \bigoplus_{i \in A} x_i = 1, \text{ then } \beta_{\bar{x}} = 0. \tag{A11}$$

In this way, we are left with s nonzero $\beta_{\bar{x}}$'s. We can write the set A as

$$A = \left\{ i \in H \mid \exists \, \bar{z}, \bar{z}' \text{ such that } \forall \, d \in D, \bigoplus_{i \in N(d)} z_i = \bigoplus_{i \in N(d)} z_i', \right.$$

$$\left. \text{and } z_i \oplus z_i' = 1 \right\}. \tag{A12}$$

Writing $i \in A$ using Eq. (A12), the condition on $\beta_{\bar{x}}$ in Eq. (A11) can be written as

$$\text{if } \exists \, \bar{z}, \bar{z}' \text{ such that } \forall \, d \in D, \bigoplus_{i \in N(d)} z_i = \bigoplus_{i \in N(d)} z_i',$$

$$\text{then } \beta_{\bar{x}} = 0 \text{ if } \bigoplus_{i \in H} (z_i \oplus z_i') \wedge x_i = 1. \tag{A13}$$

We will now relate the two expressions we have for the honest parts of the state. The graph state basis can be expressed in terms of the computational basis by

$$|\mathcal{H}_{(\bar{x})}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{z}} (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} (-1)^{\bigoplus_i x_i \wedge z_i} |\bar{z}\rangle. \tag{A14}$$

Substituting in Eq. (A5) and grouping, we get

$$|\Psi\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{x}} \beta_{\bar{x}} \sum_{\bar{z}} (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} (-1)^{\bigoplus_i x_i \wedge z_i} |\bar{z}\rangle_H |\phi_{\bar{x}}\rangle_D$$

$$= \sum_{\bar{z}} (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} |\bar{z}\rangle_H \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{x}} \beta_{\bar{x}} (-1)^{\bigoplus_i x_i \wedge z_i} |\phi_{\bar{x}}\rangle_D. \tag{A15}$$

Comparing the above expression with Eq. (A4) in terms of the coefficients of each $|\bar{z}\rangle$,

$$\alpha_{\bar{z}} |\psi_{\bar{z}}\rangle = (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{x}} \beta_{\bar{x}} (-1)^{\bigoplus_i x_i \wedge z_i} |\phi_{\bar{x}}\rangle, \ \forall \, \bar{z}$$

$$(-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} \alpha_{\bar{z}} |\psi_{\bar{z}}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{x}} \beta_{\bar{x}} (-1)^{\bigoplus_i x_i \wedge z_i} |\phi_{\bar{x}}\rangle, \ \forall \, \bar{z}. \tag{A16}$$

On the other hand, expressing the computational basis in terms of the graph state basis gives

$$|\bar{z}\rangle = \frac{1}{\sqrt{2^{|H|}}} (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} \sum_{\bar{x}} (-1)^{\bigoplus_i x_i \wedge z_i} |\mathcal{H}_{(\bar{x})}\rangle. \tag{A17}$$

Substituting in Eq. (A4) and grouping, we get

$$|\Psi\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{z}} \alpha_{\bar{z}} (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} \sum_{\bar{x}} (-1)^{\bigoplus_i x_i \wedge z_i} |\mathcal{H}_{(\bar{x})}\rangle_H |\psi_{\bar{z}}\rangle_D$$

$$= \sum_{\bar{x}} |\mathcal{H}_{(\bar{x})}\rangle_H \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{z}} (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} (-1)^{\bigoplus_i x_i \wedge z_i}$$

$$\times \alpha_{\bar{z}} |\psi_{\bar{z}}\rangle_D. \tag{A18}$$

Comparing the above expression with Eq. (A5) in terms of the coefficients of $|\mathcal{H}_{(\bar{x})}\rangle$,

$$\beta_{\bar{x}} |\phi_{\bar{x}}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{z}} (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} (-1)^{\bigoplus_i x_i \wedge z_i} \alpha_{\bar{z}} |\psi_{\bar{z}}\rangle, \ \forall \, \bar{x}. \tag{A19}$$

Note that for certain $\bar{x}$, $\beta_{\bar{x}} = 0$. In Eq. (A16), some terms will then be zero. In Eq. (A19), the whole left-hand side will then be zero. If any of the expressions are equal to zero, we can use them to show that the terms are grouped as in the Schmidt decomposition of $|\mathcal{G}\rangle$ in Eq. (A3), which will allow us to simplify Eqs. (A19) and (A4). If none of the expressions are equal to zero, we will see that the same simplification applies. This is encapsulated in Lemma 1.1.

Lemma 1.1. Equations (A19) and (A4) can be written as

$$\beta_{\overline{\mathbf{v}}} |\phi_{\overline{\mathbf{v}}}\rangle = \frac{\sqrt{2^{|H|}}}{s} \sum_{\overline{\mathbf{w}}} (-1)^{\overset{\oplus}{i} v_i \wedge w_i} \alpha_{\overline{\mathbf{w}}} |\psi_{\overline{\mathbf{w}}}\rangle, \ \forall \ \overline{\mathbf{v}} \qquad (A20)$$

$$|\Psi\rangle = \sum_{\overline{\mathbf{z}}} (-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\overline{\mathbf{w}}} |\overline{\mathbf{z}}\rangle_H \otimes |\psi_{\overline{\mathbf{w}}}\rangle_D, \qquad (A21)$$

where $\overline{\mathbf{w}}, \overline{\mathbf{v}} \in \{bn(0), \dots, bn(s-1)\}$.

Proof. We will prove this in a series of steps. First, we show that the $|\psi_{\overline{\mathbf{z}}}\rangle$'s are equal for the $|\overline{\mathbf{z}}\rangle$ terms that are grouped together in the Schmidt decomposition of $|\mathcal{G}\rangle$ in Eq. (A3), and that their corresponding $\alpha_{\overline{\mathbf{z}}}$'s are equal up to ± 1. For any strings $\overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $\forall \ d \in D, \ \underset{i\in N(d)}{\oplus} z_i = \underset{i\in N(d)}{\oplus} z_i'$, we have using Eq. (A16)

$$(-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle - (-1)^{\overset{\oplus}{(k,l)\in E_H} z_k' \wedge z_l'} \alpha_{\overline{\mathbf{z}}'} |\psi_{\overline{\mathbf{z}}'}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\overline{\mathbf{x}}} \beta_{\overline{\mathbf{x}}} \left[(-1)^{\overset{\oplus}{i} x_i \wedge z_i} - (-1)^{\overset{\oplus}{i} x_i \wedge z_i'} \right] |\phi_{\overline{\mathbf{x}}}\rangle. \qquad (A22)$$

From Eq. (A13), we know that for such strings $\overline{\mathbf{z}}, \overline{\mathbf{z}}'$, if $\underset{i}{\oplus}(z_i \oplus z_i') \wedge x_i = 1$, then $\beta_{\overline{\mathbf{x}}} = 0$. Otherwise, for the terms where $\beta_{\overline{\mathbf{x}}} \neq 0$, we have

$$0 = \underset{i}{\oplus}(z_i \oplus z_i') \wedge x_i = \underset{i}{\oplus}[(x_i \wedge z_i) \oplus (x_i \wedge z_i')] = [\underset{i}{\oplus}(x_i \wedge z_i)] \oplus [\underset{i}{\oplus}(x_i \wedge z_i')], \qquad (A23)$$

which gives $\underset{i}{\oplus} x_i \wedge z_i = \underset{i}{\oplus} x_i \wedge z_i'$, and subsequently

$$(-1)^{\overset{\oplus}{i} x_i \wedge z_i} = (-1)^{\overset{\oplus}{i} x_i \wedge z_i'}. \qquad (A24)$$

Substituting in Eq. (A22), we get that $\forall \ \overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $\forall \ d \in D, \ \underset{i\in N(d)}{\oplus} z_i = \underset{i\in N(d)}{\oplus} z_i'$,

$$(-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle = (-1)^{\overset{\oplus}{(k,l)\in E_H} z_k' \wedge z_l'} \alpha_{\overline{\mathbf{z}}'} |\psi_{\overline{\mathbf{z}}'}\rangle. \qquad (A25)$$

Next, we will simplify the expression for $\beta_{\overline{\mathbf{x}}} |\phi_{\overline{\mathbf{x}}}\rangle$ by substituting Eqs. (A25) and (A24) in (A19) to get

$$\beta_{\overline{\mathbf{x}}} |\phi_{\overline{\mathbf{x}}}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\overline{\mathbf{z}}} (-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} (-1)^{\overset{\oplus}{i} x_i \wedge z_i} \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle, \ \forall \ \overline{\mathbf{x}} \text{ such that } \beta_{\overline{\mathbf{x}}} \neq 0$$

$$= \frac{1}{\sqrt{2^{|H|}}} \left[\sum_{\substack{\overline{\mathbf{z}} \text{ s. t.} \\ \underset{i\in N(d_1)}{\oplus} z_i = 0 \wedge \dots \\ \wedge \underset{i\in N(d_{|D|})}{\oplus} z_i = 0}} (-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} (-1)^{\overset{\oplus}{i} x_i \wedge z_i} \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle + \dots + \sum_{\substack{\overline{\mathbf{z}} \text{ s. t.} \\ \underset{i\in N(d_1)}{\oplus} z_i = 1 \wedge \dots \\ \wedge \underset{i\in N(d_{|D|})}{\oplus} z_i = 1}} (-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} (-1)^{\overset{\oplus}{i} x_i \wedge z_i} \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle \right]. \qquad (A26)$$

There are s nonzero expressions for $\beta_{\overline{\mathbf{x}}} |\phi_{\overline{\mathbf{x}}}\rangle$ since there are s nonzero $\beta_{\overline{\mathbf{x}}}$'s. There are also s sum terms on the right-hand side of the above expression. There are a total of $2^{|H|}$ terms of $\alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle$, grouped together if $\forall \ d \in D, \ \underset{i\in N(d)}{\oplus} z_i$ is the same. This means that, within each of the s sum terms, there are $\frac{2^{|H|}}{s}$ terms. From Eq. (A25), we know that $(-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\overline{\mathbf{z}}} |\psi_{\overline{\mathbf{z}}}\rangle$ is the same for each of these terms. Further, we know from Eq. (A24) that $(-1)^{\overset{\oplus}{i} x_i \wedge z_i}$ is the same for each of these terms (since $\beta_{\overline{\mathbf{x}}} \neq 0$). Then, we can write our expression using s terms (corresponding to each sum term in the above expression).

In this way, we are left with terms depending on s unique variables that can take any value 0 or 1, instead of $2^{|H|}$ variables that can only take certain values. Defining new variables $\overline{\mathbf{w}}, \overline{\mathbf{v}} \in \{bn(0), \dots, bn(s-1)\}$, we can write the above as

$$\beta_{\overline{\mathbf{v}}} |\phi_{\overline{\mathbf{v}}}\rangle = \frac{1}{\sqrt{2^{|H|}}} \frac{2^{|H|}}{s} \sum_{\overline{\mathbf{w}}} (-1)^{\overset{\oplus}{i} v_i \wedge w_i} \alpha_{\overline{\mathbf{w}}} |\psi_{\overline{\mathbf{w}}}\rangle = \frac{\sqrt{2^{|H|}}}{s} \sum_{\overline{\mathbf{w}}} (-1)^{\overset{\oplus}{i} v_i \wedge w_i} \alpha_{\overline{\mathbf{w}}} |\psi_{\overline{\mathbf{w}}}\rangle, \ \forall \ \overline{\mathbf{v}}. \qquad (A27)$$

Note that $\forall \ \overline{\mathbf{w}} \neq \overline{\mathbf{w}}'$, $\langle \psi_{\overline{\mathbf{w}}} | \psi_{\overline{\mathbf{w}}'} \rangle = 0$, from Eq. (A8) and the fact that any two states with different $\overline{\mathbf{w}}$ have different $\underset{i\in N(d)}{\oplus} z_i$ for some $d \in D$. As before, $\forall \ \overline{\mathbf{v}} \neq \overline{\mathbf{v}}'$, $\langle \phi_{\overline{\mathbf{v}}} | \phi_{\overline{\mathbf{v}}'} \rangle = 0$, from Eq. (A9). This means that now, instead of having $2^{|H|}$ variables $\overline{\mathbf{z}}, \overline{\mathbf{x}} \in \{bn(0), \dots, bn(2^{|H|} - 1)\}$, we have s variables $\overline{\mathbf{w}}, \overline{\mathbf{v}} \in \{bn(0), \dots, bn(s-1)\}$.

Finally, we simplify the computational basis expression for $|\Psi\rangle$ in Eq. (A4). The terms should now be grouped as in Eq. (A3), with s terms, as

$$|\Psi\rangle = \sum_{\overline{\mathbf{z}}} \alpha_{\overline{\mathbf{z}}} |\overline{\mathbf{z}}\rangle_H \otimes |\psi_{\overline{\mathbf{z}}}\rangle_D = \sum_{\overline{\mathbf{z}}} (-1)^{\overset{\oplus}{(k,l)\in E_H} z_k \wedge z_l} \alpha_{\overline{\mathbf{w}}} |\overline{\mathbf{z}}\rangle_H \otimes |\psi_{\overline{\mathbf{w}}}\rangle_D, \qquad (A28)$$

where $\overline{\mathbf{w}} = f(\overline{\mathbf{z}})$ depends on $\underset{i\in N(d)}{\oplus} z_i, \forall \ d \in D$. If none of the expressions are equal to zero, we have $s = 2^{|H|}$, and so we can simply rename $\overline{\mathbf{z}}$ as $\overline{\mathbf{w}}$, as they take values from the same set $\{bn(0), \dots, bn(s-1)\}$. ∎

Our next aim is to determine the value of $\alpha_{\overline{\mathbf{w}}}$. From the normalization condition $\langle \Psi | | \Psi \rangle = 1$, we have

$$\sum_{\overline{\mathbf{w}}} \frac{2^{|H|}}{s} |\alpha_{\overline{\mathbf{w}}}|^2 = 1 \Rightarrow \sum_{\overline{\mathbf{w}}} |\alpha_{\overline{\mathbf{w}}}|^2 = \frac{s}{2^{|H|}} \tag{A29}$$

since there are $\frac{2^{|H|}}{s}$ terms of $|\overline{\mathbf{z}}\rangle$ corresponding to each $\overline{\mathbf{w}}$, as we saw before.

To get the orthogonality conditions, we take the overlap of each nonzero expression for $\beta_{\overline{\mathbf{v}}} |\phi_{\overline{\mathbf{v}}}\rangle$ with another nonzero expression for $\beta_{\overline{\mathbf{v}}'} |\phi_{\overline{\mathbf{v}}'}\rangle$ to get $(s-1)$ equations for all $\overline{\mathbf{v}} \neq \overline{\mathbf{v}}'$ given by

$$\beta_{\overline{\mathbf{v}}}^{\dagger} \beta_{\overline{\mathbf{v}}'} \langle \phi_{\overline{\mathbf{v}}} | | \phi_{\overline{\mathbf{v}}'} \rangle = 0 = \frac{2^{|H|}}{s^2} \left[\sum_{\overline{\mathbf{w}}} (-1)^{\oplus_i v_i \wedge w_i} (-1)^{\oplus_i v_i' \wedge w_i} |\alpha_{\overline{\mathbf{w}}}|^2 \langle \psi_{\overline{\mathbf{w}}} | | \psi_{\overline{\mathbf{w}}} \rangle \right], \tag{A30}$$

which we can write as

$$\sum_{\overline{\mathbf{w}}} (-1)^{\oplus_i p_i \wedge w_i} |\alpha_{\overline{\mathbf{w}}}|^2 = 0, \quad \forall \, \overline{\mathbf{p}} \in \{bn(1), \dots, bn(s-1)\}. \tag{A31}$$

(Note that since the overlap is taken with two different expressions, $\overline{\mathbf{p}}$ can never be $0 \dots 0$.)

We will now solve the s equations for s variables (from the normalization and orthogonality conditions) using the matrix method, formulating the system of equations as $\mathcal{A}u = b$. The matrix $\mathcal{A}$ is of size $s \times s$, while u, b are of size $s \times 1$. u is a column vector containing each $|\alpha_{\overline{\mathbf{w}}}|^2$, and b is a column vector giving the normalization and orthogonality conditions. $\mathcal{A}$ has 1's in its first row and column, and the other elements are ± 1. The 1's on the first row are from the normalization condition. The 1's on the first column occur because for $\overline{\mathbf{w}} = 0 \dots 0$, the exponent of (-1) will always be 0 (since the AND of anything with $0 \dots 0$ gives $0 \dots 0$), and so the sign of $|\alpha_{\overline{\mathbf{w}}}|^2$ is always $+1$. We then have

$$\mathcal{A} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \pm 1 & \cdots & \pm 1 \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \pm 1 & \cdots & \pm 1 \end{bmatrix}, \quad u = \begin{bmatrix} |\alpha_{00\dots00}|^2 \\ |\alpha_{00\dots01}|^2 \\ \cdots \\ |\alpha_{11\dots11}|^2 \end{bmatrix}, \quad b = \frac{s}{2^{|H|}} \begin{bmatrix} 1 \\ 0 \\ \cdots \\ 0 \end{bmatrix}. \tag{A32}$$

The values of $|\alpha_{\overline{\mathbf{w}}}|^2$ are then determined by

$$\begin{bmatrix} |\alpha_{00\dots00}|^2 \\ |\alpha_{00\dots01}|^2 \\ \cdots \\ |\alpha_{11\dots11}|^2 \end{bmatrix} = \mathcal{A}^{-1} \frac{s}{2^{|H|}} \begin{bmatrix} 1 \\ 0 \\ \cdots \\ 0 \end{bmatrix} = \frac{s}{2^{|H|}} \begin{bmatrix} \mathcal{A}_{1,1}^{-1} \\ \mathcal{A}_{2,1}^{-1} \\ \cdots \\ \mathcal{A}_{s,1}^{-1} \end{bmatrix}. \tag{A33}$$

Thus, the solution to the set of equations is equal to $\frac{s}{2^{|H|}}$ times the first column of $\mathcal{A}^{-1}$. Using Eqs. (A29) and (A31), let us now write more precisely what the elements of $\mathcal{A}$ are:

$$\mathcal{A} = \begin{bmatrix} (-1)^{\oplus 00\dots00 \wedge 00\dots00} & (-1)^{\oplus 00\dots00 \wedge 00\dots01} & \cdots & (-1)^{\oplus 00\dots00 \wedge 11\dots11} \\ (-1)^{\oplus 00\dots01 \wedge 00\dots00} & (-1)^{\oplus 00\dots01 \wedge 00\dots01} & \cdots & (-1)^{\oplus 00\dots01 \wedge 11\dots11} \\ \cdots & \cdots & \cdots & \cdots \\ (-1)^{\oplus 11\dots11 \wedge 00\dots00} & (-1)^{\oplus 11\dots11 \wedge 00\dots01} & \cdots & (-1)^{\oplus 11\dots11 \wedge 11\dots11} \end{bmatrix}, \tag{A34}$$

where by $\oplus \mathsf{a} \wedge \mathsf{b}$ we mean computing the AND operation of the strings a, b, and then XORing all the resulting bits (or, in other words, finding the parity of the AND of the strings a, b).

Let us take $\overline{\mathbf{p}}_i$, $\overline{\mathbf{w}}_j$ to be the ith and jth strings in the set $\{bn(0), \dots, bn(s-1)\}$, where $i, j \in \{1, \dots, s\}$. (For example, if $i = 2$, $j = 3$, we have $\overline{\mathbf{p}}_2 = 00\dots01$, $\overline{\mathbf{w}}_3 = 00\dots10$.) Then, taking i to denote the row and j to denote the column, $\mathcal{A}$ is given by

$$\mathcal{A} = \begin{bmatrix} (-1)^{\oplus \overline{\mathbf{p}}_1 \wedge \overline{\mathbf{w}}_1} & (-1)^{\oplus \overline{\mathbf{p}}_1 \wedge \overline{\mathbf{w}}_2} & \cdots & (-1)^{\oplus \overline{\mathbf{p}}_1 \wedge \overline{\mathbf{w}}_s} \\ (-1)^{\oplus \overline{\mathbf{p}}_2 \wedge \overline{\mathbf{w}}_1} & (-1)^{\oplus \overline{\mathbf{p}}_2 \wedge \overline{\mathbf{w}}_2} & \cdots & (-1)^{\oplus \overline{\mathbf{p}}_2 \wedge \overline{\mathbf{w}}_s} \\ \cdots & \cdots & \cdots & \cdots \\ (-1)^{\oplus \overline{\mathbf{p}}_s \wedge \overline{\mathbf{w}}_1} & (-1)^{\oplus \overline{\mathbf{p}}_s \wedge \overline{\mathbf{w}}_2} & \cdots & (-1)^{\oplus \overline{\mathbf{p}}_s \wedge \overline{\mathbf{w}}_s} \end{bmatrix}. \tag{A35}$$

In general, the (i, j)th element of $\mathcal{A}$ is given by

$$\mathcal{A}_{i,j} = (-1)^{\oplus \overline{\mathbf{p}}_i \wedge \overline{\mathbf{w}}_j}. \tag{A36}$$

Note that since $\overline{\mathbf{p}}_i = \overline{\mathbf{w}}_i \, \forall \, i$, we have $\mathcal{A}_{i,j} = (-1)^{\oplus \overline{\mathbf{p}}_i \wedge \overline{\mathbf{w}}_j} = (-1)^{\oplus \overline{\mathbf{w}}_i \wedge \overline{\mathbf{p}}_j} = (-1)^{\oplus \overline{\mathbf{p}}_j \wedge \overline{\mathbf{w}}_i} = \mathcal{A}_{j,i}$, and so $\mathcal{A}$ is symmetric. We will now show that the inverse of the matrix $\mathcal{A}$ is given by $\mathcal{A}^{-1} = \frac{1}{s} \mathcal{A}$. To prove this, we just have to show that $\mathcal{A}\mathcal{A}^{-1} = \mathbb{1}$. Denoting $\mathcal{A}\mathcal{A} = \mathcal{M}$, we have

$$\mathcal{A}\mathcal{A}^{-1} = \mathcal{A} \frac{1}{s} \mathcal{A} = \frac{1}{s} \mathcal{A}\mathcal{A} = \frac{1}{s} \mathcal{M}. \tag{A37}$$

The (i, j)th element of $\mathcal{M}$ is given by

$$\mathcal{M}_{i,j} = \sum_{k=1}^{s} (-1)^{\oplus \overline{\mathbf{p}}_i \wedge \overline{\mathbf{w}}_k}(-1)^{\oplus \overline{\mathbf{p}}_k \wedge \overline{\mathbf{w}}_j} = \sum_{k=1}^{s} (-1)^{\oplus \overline{\mathbf{p}}_i \wedge \overline{\mathbf{w}}_k}(-1)^{\oplus \overline{\mathbf{p}}_j \wedge \overline{\mathbf{w}}_k} = \sum_{k=1}^{s} (-1)^{\oplus (\overline{\mathbf{p}}_i \oplus \overline{\mathbf{p}}_j) \wedge \overline{\mathbf{w}}_k}. \tag{A38}$$

When $i = j$, we have $\overline{\mathbf{p}}_i \oplus \overline{\mathbf{p}}_j = 00\ldots00$, and so for every $\overline{\mathbf{w}}_k$, we always have $(-1)^0$. Thus, we have $\mathcal{M}_{i,i} = \sum_{k=1}^{s} 1 = s$. When $i \neq j$, the AND operation is performed on the same string $\overline{\mathbf{p}}_i \oplus \overline{\mathbf{p}}_j$ and $\overline{\mathbf{w}}_k$, $\forall\, k$. In this case, $\overline{\mathbf{p}}_i \oplus \overline{\mathbf{p}}_j \in \{bn(1), \ldots, bn(s-1)\}$, as their sum can only be $00\ldots00$ if $i = j$. Thus, if we sum over the AND of this string with each possible $\overline{\mathbf{w}} \in \{00\ldots00, \ldots, 11\ldots11\}$, we get an equal number of $+1$'s and -1's. So, this sum is equal to 0. We can therefore say

$$\mathcal{M}_{i,j} = \delta_i^j s, \tag{A39}$$

which means $\mathcal{M} = s\mathbb{1}$. Substituting in Eq. (A37), we find $\mathcal{A}\mathcal{A}^{-1} = \mathbb{1}$. Thus, $\mathcal{A}^{-1} = \frac{1}{s}\mathcal{A}$, which we substitute in Eq. (A33) to get

$$\begin{bmatrix} |\alpha_{0\ldots0}|^2 \\ |\alpha_{0\ldots1}|^2 \\ \cdots \\ |\alpha_{1\ldots1}|^2 \end{bmatrix} = \frac{s}{2^{|H|}} \begin{bmatrix} \mathcal{A}_{1,1}^{-1} \\ \mathcal{A}_{2,1}^{-1} \\ \cdots \\ \mathcal{A}_{s,1}^{-1} \end{bmatrix} = \frac{1}{s} \times \frac{s}{2^{|H|}} \begin{bmatrix} \mathcal{A}_{1,1} \\ \mathcal{A}_{2,1} \\ \cdots \\ \mathcal{A}_{s,1} \end{bmatrix} = \frac{1}{s} \times \frac{s}{2^{|H|}} \begin{bmatrix} 1 \\ 1 \\ \cdots \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2^{|H|}} \\ \frac{1}{2^{|H|}} \\ \cdots \\ \frac{1}{2^{|H|}} \end{bmatrix}. \tag{A40}$$

This gives each $\alpha_{\overline{\mathbf{w}}} = \pm\frac{1}{\sqrt{2^{|H|}}}$. Let us substitute the value of $\alpha_{\overline{\mathbf{w}}}$ in Eq. (A28). We get

$$|\Psi\rangle = \pm\frac{1}{\sqrt{2^{|H|}}} \sum_{\overline{\mathbf{z}}} (-1)^{\underset{(k,l)\in E_H}{\oplus} z_k \wedge z_l} |\overline{\mathbf{z}}\rangle_H \otimes |\psi_{\overline{\mathbf{w}}}\rangle_D = \pm\frac{1}{\sqrt{2^{|H|}}} \sum_{\overline{\mathbf{z}}} (-1)^{\underset{(k,l)\in E_H}{\oplus} z_k \wedge z_l} |\overline{\mathbf{z}}\rangle_H \otimes |\psi_{(f(\overline{\mathbf{z}}))}\rangle_D. \tag{A41}$$

Finally, $\rho_H^{|\Psi\rangle}$ only depends on the honest Schmidt basis. Comparing the above expression with Eq. (A3) shows that the honest Schmidt basis of the actual state $|\Psi\rangle$ is equal to the honest Schmidt basis of the ideal state $|\mathcal{G}\rangle$, giving $\rho_H^{|\Psi\rangle} = \rho_H^{|\mathcal{G}\rangle}$. If $|\Psi\rangle$ is a purification of $\rho_H^{|\Psi\rangle}$, and $|\mathcal{G}\rangle$ is a purification of $\rho_H^{|\mathcal{G}\rangle}$, then due to the unitary equivalence of purifications, we must have $|\Psi\rangle = U_D |\mathcal{G}\rangle$ if all the test measurements pass perfectly. This concludes the proof of Lemma 1. ∎

The above Lemma 1 tells us that only the state $U_D |\mathcal{G}\rangle$ (the ideal state up to local unitaries on the dishonest side), or equivalently $\rho_H^{|\mathcal{G}\rangle}$, always passes the stabilizer test $\mathcal{S}_j$ in any round j. For simplicity of presentation later on, we now analyze the case where the number of stabilizers that need to be measured to have the analogous statement of Lemma 1 is J. We fix N_{total} such that $\mathsf{N} \equiv N_{\text{total}} - \mathsf{J}N_{\text{test}} = \mathsf{J}N_{\text{test}}$ is the total number of remaining copies, out of which one is chosen to be the target copy. Let k be the number of copies out of the remaining N copies that are $\rho_H^{|\mathcal{G}\rangle}$. Now, using the Serfling bound, we will find a bound on $\frac{\mathsf{k}}{\mathsf{N}}$ in the following lemma, which is an adaptation of the method of Takeuchi *et al.* [20] to our scenario of verifying general graph states with any number of dishonest parties.

Lemma 2 (adapted from [20]). The probability that the fraction of states that would pass all stabilizer tests out of the remaining copies in Protocol I is given by

$$\frac{\mathsf{k}}{\mathsf{N}} \geqslant 1 - \frac{2\sqrt{c}}{\mathsf{J}} - 2\mathsf{J}\left(1 - \frac{N_{\text{pass}}}{\mathsf{J}N_{\text{test}}}\right) \tag{A42}$$

is at least $1 - \mathsf{J}^{1-\frac{2cm}{3}}$.

Proof. Consider a set of binary random variables $Y = \{Y_1, \ldots, Y_{\mathcal{T}}\}$ where $Y_t \in \{0, 1\}$. Let us set the value of $Y_t = 0$ if the stabilizer test passes on copy t, and otherwise $Y_t = 1$. Then, by Serfling's bound [43], where $\mathcal{T} = \mathcal{L} + \mathcal{R}$, for any $0 < \nu < 1$,

$$\Pr\left[\sum_{t \in \overline{\Pi}} Y_t \leqslant \frac{\mathcal{L}}{\mathcal{R}}\sum_{t \in \Pi} Y_t + \mathcal{L}\nu\right] \geqslant 1 - \exp\left[-\frac{2\nu^2 \mathcal{L}\mathcal{R}^2}{(\mathcal{L} + \mathcal{R})(\mathcal{R} + 1)}\right], \tag{A43}$$

where Π is a set of $\mathcal{R}$ samples chosen independently and uniformly randomly from Y without replacement, and $\overline{\Pi}$ is the complementary set of Π. The expression inside the probability bracket is then an upper bound on the number of copies out of the remaining that would fail the stabilizer test, given a number of copies that pass.

Now, let us consider the stabilizer measurement $\mathcal{S}_{j\in\{1,\ldots,\mathsf{J}\}}$. We take $\mathcal{L} = N_{\text{total}} - jN_{\text{test}}$, and $\mathcal{R} = N_{\text{test}}$. Let us then set $\nu = \frac{\sqrt{c}}{\mathsf{J}^2}$, which is chosen in this way to maximize both the fidelity and probability in our resulting expression (this implies $0 < \sqrt{c} < \mathsf{J}^2$). Let $\Pi^{(j)}$ be the set of copies on which each $\mathcal{S}_j$ was measured, and $\overline{\Pi}^{(j)}$ be the set of remaining copies after measuring $\mathcal{S}_j$. Finally, we denote the probability expression on the right-hand side of Eq. (A43) for the stabilizer test in round j as q_j. Then, after the stabilizer test for $\mathcal{S}_j$ is performed, we have

$$\Pr\left[\sum_{t \in \overline{\Pi}^{(j)}} Y_t \leqslant \frac{N_{\text{total}} - jN_{\text{test}}}{N_{\text{test}}}\sum_{t \in \Pi^{(j)}} Y_t + (N_{\text{total}} - jN_{\text{test}})\nu\right] \geqslant q_j. \tag{A44}$$

In other words, with probability at least q_j, the maximum number of copies that would fail the stabilizer test of $\mathcal{S}_j$ out of the remaining is given by $\frac{N_{\text{total}} - jN_{\text{test}}}{N_{\text{test}}} \sum_{t \in \Pi^{(j)}} Y_t + (N_{\text{total}} - jN_{\text{test}})\nu$. Then, the minimum number of copies that would pass the $\mathcal{S}_j$ test is given by the total number of remaining copies minus this maximum number of failed copies. Thus, after all stabilizer tests are performed, we can lower bound the number of remaining copies which would pass all of the stabilizer tests by summing over all j's corresponding to all stabilizers $\mathcal{S}_j$. Recalling that we denote the number of "good" remaining copies by k, we then have

$$
\begin{aligned}
\mathsf{k} &\geqslant (N_{\text{total}} - \mathsf{J}N_{\text{test}}) - \sum_{j=1}^{\mathsf{J}} \left[\frac{N_{\text{total}} - jN_{\text{test}}}{N_{\text{test}}} \sum_{t \in \Pi^{(j)}} Y_t + (N_{\text{total}} - jN_{\text{test}})\nu \right] \\
&= 2\mathsf{J}N_{\text{test}} - \mathsf{J}N_{\text{test}} - \frac{N_{\text{total}}}{N_{\text{test}}} \sum_{j=1}^{\mathsf{J}} \sum_{t \in \Pi^{(j)}} Y_t + \sum_{j=1}^{\mathsf{J}} j \sum_{t \in \Pi^{(j)}} Y_t - \nu\mathsf{J}N_{\text{total}} + \sum_{j=1}^{\mathsf{J}} jN_{\text{test}}\nu \\
&\geqslant \mathsf{J}N_{\text{test}} - \nu\mathsf{J}N_{\text{total}} - \frac{N_{\text{total}}}{N_{\text{test}}} \sum_{j=1}^{\mathsf{J}} \sum_{t \in \Pi^{(j)}} Y_t \\
&\geqslant \mathsf{J}N_{\text{test}} - \nu\mathsf{J}N_{\text{total}} - \frac{N_{\text{total}}}{N_{\text{test}}} (\mathsf{J}N_{\text{test}} - N_{\text{pass}}) \\
&= \mathsf{J}N_{\text{test}} - \nu\mathsf{J} \times 2 \times \mathsf{J}N_{\text{test}} - \frac{2\mathsf{J}N_{\text{test}}}{N_{\text{test}}} (\mathsf{J}N_{\text{test}} - N_{\text{pass}}) \\
&= \left(\mathsf{J} - 2\sqrt{c} - 2\mathsf{J}^2 + 2\mathsf{J}\frac{N_{\text{pass}}}{N_{\text{test}}} \right) N_{\text{test}},
\end{aligned}
\tag{A45}
$$

which gives the fraction of "good" remaining copies $\frac{\mathsf{k}}{\mathsf{N}}$ as

$$
\begin{aligned}
\frac{\mathsf{k}}{\mathsf{N}} &\geqslant \frac{\left(\mathsf{J} - 2\sqrt{c} - 2\mathsf{J}^2 + 2\mathsf{J}\frac{N_{\text{pass}}}{N_{\text{test}}} \right) N_{\text{test}}}{N_{\text{total}} - \mathsf{J}N_{\text{test}}} \\
&= \frac{\mathsf{J} - 2\sqrt{c} - 2\mathsf{J}^2 + 2\mathsf{J}\frac{N_{\text{pass}}}{N_{\text{test}}}}{\mathsf{J}} \\
&= 1 - \frac{2\sqrt{c}}{\mathsf{J}} - 2\mathsf{J}\left(1 - \frac{N_{\text{pass}}}{\mathsf{J}N_{\text{test}}} \right).
\end{aligned}
\tag{A46}
$$

From Eq. (A43), we then get for q_j, the probability corresponding to the test $\mathcal{S}_j$,

$$
\begin{aligned}
q_j &= 1 - \exp\left[-\frac{2\nu^2(N_{\text{total}} - jN_{\text{test}})N_{\text{test}}^2}{(N_{\text{total}} - jN_{\text{test}} + N_{\text{test}})(N_{\text{test}} + 1)} \right] \\
&= 1 - \exp\left[-2\nu^2 N_{\text{test}} \frac{1}{\frac{N_{\text{total}} - jN_{\text{test}} + N_{\text{test}}}{N_{\text{total}} - jN_{\text{test}}} \times \frac{N_{\text{test}} + 1}{N_{\text{test}}}} \right] \\
&= 1 - \exp\left[-2\nu^2 N_{\text{test}} \frac{1}{1 + \frac{1}{2\mathsf{J} - j}} \frac{1}{1 + \frac{1}{N_{\text{test}}}} \right].
\end{aligned}
\tag{A47}
$$

Now, let us compute the total probability corresponding to the full set of J stabilizer tests. Taking $N_{\text{test}} = m\mathsf{J}^4 \ln \mathsf{J}$ and using $\mathsf{J} \geqslant 2 \Rightarrow \frac{1}{1 + \frac{1}{\mathsf{J}}} \geqslant \frac{2}{3}$, and $N_{\text{test}} \geqslant 1 \Rightarrow \frac{1}{1 + \frac{1}{N_{\text{test}}}} \geqslant \frac{1}{2}$, we get the total probability corresponding to J stabilizer tests as

$$
\begin{aligned}
\prod_{j=1}^{\mathsf{J}} q_j &\geqslant q_{\mathsf{J}}^{\mathsf{J}} = \left[1 - \exp\left(-2\nu^2 N_{\text{test}} \frac{1}{1 + \frac{1}{2\mathsf{J} - \mathsf{J}}} \frac{1}{1 + \frac{1}{N_{\text{test}}}} \right) \right]^{\mathsf{J}} \\
&\geqslant \left[1 - \exp\left(-\frac{2\nu^2 N_{\text{test}}}{3} \right) \right]^{\mathsf{J}}
\end{aligned}
$$

$$
\begin{aligned}
&\geqslant \left[1 - \exp\left(-\frac{2\nu^2 m\mathsf{J}^4}{3} \ln \mathsf{J} \right) \right]^{\mathsf{J}} \\
&= \left[1 - \mathsf{J}^{-\frac{2cm}{3}} \right]^{\mathsf{J}} \\
&\geqslant 1 - \mathsf{J}^{1 - \frac{2cm}{3}}.
\end{aligned}
\tag{A48}
$$

Thus, the event that the fraction of "good" copies that pass all the stabilizer tests $\mathcal{S}_j$ is lower bounded by $\frac{\mathsf{k}}{\mathsf{N}} \geqslant 1 - \frac{2\sqrt{c}}{\mathsf{J}} - 2\mathsf{J}(1 - \frac{N_{\text{pass}}}{\mathsf{J}N_{\text{test}}})$ occurs with probability greater than or equal to $1 - \mathsf{J}^{1 - \frac{2cm}{3}}$. ∎

In the final step of the protocol, one copy is chosen, out of the remaining $\mathsf{N} \equiv N_{\text{total}} - \mathsf{J}N_{\text{test}}$ copies, to be the target copy. Let us now finish the proof by proving Lemma 3, relating the above analysis to the averaged state of this target copy.

Lemma 3. The probability that the fidelity of the averaged state of the target copy in Protocol I satisfies

$$
F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}} \right) \geqslant \frac{\mathsf{k}}{\mathsf{N}}
\tag{A49}
$$

is at least $1 - \mathsf{J}^{1 - \frac{2cm}{3}}$.

Proof. Now, ρ_H^{avg} is the reduced state of the honest parties of the averaged state, where the average is taken over all uniformly random selections of the target copy from the total number of remaining copies N, and given by

$$
\rho_H^{\text{avg}} = \frac{1}{\mathsf{N}} \sum_{i=1}^{\mathsf{N}} \rho_H^i.
\tag{A50}
$$

Here, ρ_H^i denotes the reduced state of the honest parties in each round (for each one of the remaining copies). We now want to find the fidelity $F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}})$ between this averaged

state and the ideal state (in terms of the honest reduced states). From the concavity of fidelity,

$$F\left(\rho, \sum_i p_i \sigma_i\right) \geqslant \sum_i p_i F(\rho, \sigma_i). \qquad (A51)$$

We can use this to get

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}\right) = F\left(\rho_H^{|\mathcal{G}\rangle}, \frac{1}{\mathsf{N}} \sum_{i=1}^{\mathsf{N}} \rho_H^i\right) \geqslant \frac{1}{\mathsf{N}} \sum_{i=1}^{\mathsf{N}} F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^i\right). \qquad (A52)$$

Now, we know that for a number k of the remaining states, we have $\rho_H^i = \rho_H^{|\mathcal{G}\rangle}$ with probability at least $1 - \mathsf{J}^{1-\frac{2cm}{3}}$. Assuming the worst case scenario that the rest of the states, each denoted by ρ_H^{unknown}, have zero fidelity with the ideal state, we get

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}\right) \geqslant \frac{1}{\mathsf{N}}\left[\mathsf{k}F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{|\mathcal{G}\rangle}\right) + (\mathsf{N} - \mathsf{k})F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{unknown}}\right)\right]$$

$$\geqslant \frac{1}{\mathsf{N}}[\mathsf{k} \times 1 + (\mathsf{N} - \mathsf{k}) \times 054]$$

$$= \frac{\mathsf{k}}{\mathsf{N}}. \qquad (A53)$$

∎

Our final result then tells us that, with the appropriate choice of $N_{\text{total}}, N_{\text{test}}$, the parties can ensure that with probability at least $1 - \mathsf{J}^{1-\frac{2cm}{3}}$, the fidelity of the averaged state of the target copy satisfies

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}\right) \geqslant 1 - \frac{2\sqrt{c}}{\mathsf{J}} - 2\mathsf{J}\left(1 - \frac{N_{\text{pass}}}{\mathsf{J}N_{\text{test}}}\right). \qquad (A54)$$

Note that in order to ensure that the probability and fidelity are greater than zero, the choice of the constants m, c must be such that $\frac{3}{2m} < c < \frac{(\mathsf{J}-1)^2}{4}$. Setting $\mathsf{J} = 2^n$, this concludes the proof of Theorem 1. ∎

APPENDIX B: PROOF OF THEOREM 2

We now give some examples of types of graph states that are useful for specific purposes, and prove the following theorem to show how we can reduce the resources required to verify them (in the presence of dishonest parties) in each case.

Theorem 2. If $|\mathcal{G}\rangle$ is either

A. a complete graph state with dishonest parties anywhere in the network, or

B. a pentagon graph state with either one, three or four dishonest parties anywhere in the network, or two dishonest parties who are adjacent, or

C. a cycle graph state with either one, $n - 2$ or $n - 1$ dishonest parties anywhere in the network, or any other number of dishonest parties who are adjacent, or

D. a 1D cluster state with either one or $n - 1$ dishonest parties anywhere in the network, or any other number of adjacent honest and dishonest parties, or

E. a 2D cluster state with either one or $n - 1$ dishonest parties anywhere in the network, or any other set of adjacent dishonest parties that forms a square or rectangle anywhere in the network,

and we set $N_{\text{total}} = 2nN_{\text{test}}$, $N_{\text{test}} = \lceil mn^4 \ln n \rceil$, and $\mathcal{S}$ as the set of stabilizer generators, assuming an honest Verifier, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol I satisfies

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}\right) \geqslant 1 - \frac{2\sqrt{c}}{n} - 2n\left(1 - \frac{N_{\text{pass}}}{nN_{\text{test}}}\right) \qquad (B1)$$

is at least $1 - n^{1-\frac{2cm}{3}}$, where m, c are positive constants chosen such that $\frac{3}{2m} < c < \frac{(n-1)^2}{4}$.

For clarity, we will treat each example separately. To prove such a statement, we start by inspecting the proof of Theorem 1, to understand how the information about passing the stabilizer tests is used. In Lemma 1, this is first used to identify which elements of $\{|\psi_{\bar{\mathbf{z}}}\rangle\}, \{|\phi_{\bar{\mathbf{x}}}\rangle\}$ are orthogonal; however, as we see in Eqs. (A8) and (A9), this follows from passing purely the set of stabilizer generator measurements. It then remains to show that the conditions on which $\beta_{\bar{\mathbf{x}}}$'s are zero, given in Eq. (A11), may also be deduced from only passing the stabilizer generator tests. [We point out that if the set A is empty, which can be checked by examining the graph for the partition (H, D), then from passing the full set of stabilizer measurements, we cannot set any $\beta_{\bar{\mathbf{x}}}$ to be zero, and so we can trivially see that only the stabilizer generator measurements are required.] If this is true, it is possible for the parties to protect themselves against dishonest action even by running Protocol I with this simpler set of test measurements.

Recall that once we know which $\beta_{\bar{\mathbf{x}}}$'s must be zero, we can determine which terms have the same $\alpha_{\bar{\mathbf{z}}}, |\psi_{\bar{\mathbf{z}}}\rangle$, allowing us to group the $|\bar{\mathbf{z}}\rangle$ terms in Eq. (A4) in the same way as in the Schmidt decomposition of the ideal graph state, leading to the conclusion that $|\Psi\rangle = U_D|\mathcal{G}\rangle$. Thus, once we have derived the conditions for $\beta_{\bar{\mathbf{x}}}$ to be zero, we can simply continue with the remainder of the proof of Lemma 1. Inserting $\mathsf{J} = n$ into Lemmas 2 and 3, we obtain the desired results.

In the following, we adapt our general proof in this way to cater to the specificities of complete graphs, cycle graphs, and cluster states, with particular characteristics of the dishonest set of parties. Armed with this information, we will show that our parties can verify each graph state in an efficient way.

1. Complete graph states

Complete graph states, where every vertex is connected to every other vertex, are locally equivalent to GHZ states. As we have seen, such states are central to schemes for quantum anonymous transmission [7,44], as well as secret sharing [45], metrology [8], and many other applications. A verification test for GHZ states was already proposed and analyzed in [27]; however, we now approach this goal using the Serfling bound method. This section also serves to provide a comprehensive example of how our protocol and analysis work for this particular graph state, and so we will go through all steps of the proof.

Due to the symmetry of complete graphs (Fig. 2), we will see that we can protect against any number of dishonest parties anywhere in the network by only measuring the stabilizer generators. Recall that we denote the stabilizer generator corresponding to the ith qubit as K_i. Let the parties now run
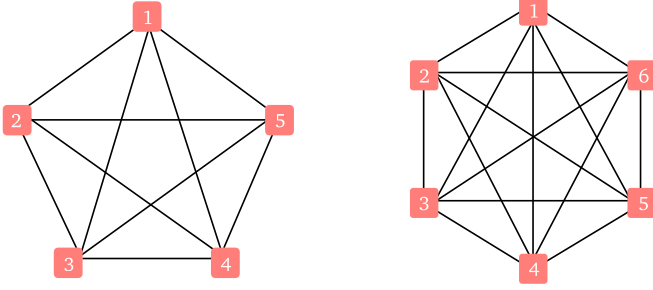
FIG. 2. Five- and six-qubit complete graph states.

Protocol I with $\mathcal{S}$ as the set of generators; our result is given in the following theorem.

Theorem 2A. If $|\mathcal{G}\rangle$ is a complete graph state, and we set $N_{\text{total}} = 2nN_{\text{test}}$, $N_{\text{test}} = \lceil mn^4 \ln n \rceil$, and $\mathcal{S}$ as the set of stabilizer generators, the probability that the fidelity of the

averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol I satisfies

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}}\right) \geqslant 1 - \frac{2\sqrt{c}}{n} - 2n\left(1 - \frac{N_{\text{pass}}}{nN_{\text{test}}}\right) \quad \text{(B2)}$$

is at least $1 - n^{1 - \frac{2cm}{3}}$, where m, c are positive constants chosen such that $\frac{3}{2m} < c < \frac{(n-1)^2}{4}$.

Proof. As before, we prove this in stages, now for the specific case of complete graph states.

Lemma 4. The only state that can pass all stabilizer generator tests perfectly in each round is $|\Psi\rangle = U_D|\mathcal{G}\rangle$, where U_D is a unitary on the dishonest part of the state.

Proof. Complete graph states are of Schmidt rank 2, i.e., there are always exactly two terms in their Schmidt decomposition. The Schmidt decomposition of a complete graph state with respect to any partition (H, D) is

$$|\mathcal{G}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{z}}} (-1)^{\bigoplus_{(k,l) \in E_H} z_k \wedge z_l} |\bar{\mathbf{z}}\rangle_H \otimes \prod_{a \in H} \left(\prod_{b \in N(a)} \sigma_Z^{(b)}\right)^{z_a} |\mathcal{G} - \mathcal{H}\rangle_D$$

$$= \frac{1}{\sqrt{2^{|H|}}} \left[\left(\sum_{\Delta(\bar{\mathbf{z}})=0(\text{mod }4)} |\bar{\mathbf{z}}\rangle - \sum_{\Delta(\bar{\mathbf{z}})=2(\text{mod }4)} |\bar{\mathbf{z}}\rangle\right)_H \otimes |\mathcal{G} - \mathcal{H}_{(00...00)}\rangle_D \right.$$

$$\left. + \left(\sum_{\Delta(\bar{\mathbf{z}})=1(\text{mod }4)} |\bar{\mathbf{z}}\rangle - \sum_{\Delta(\bar{\mathbf{z}})=3(\text{mod }4)} |\bar{\mathbf{z}}\rangle\right)_H \otimes |\mathcal{G} - \mathcal{H}_{(11...11)}\rangle_D\right], \quad \text{(B3)}$$

where $|\mathcal{G} - \mathcal{H}_{(00...00)}\rangle$ is the dishonest subgraph with no σ_Z's on any vertices, and $|\mathcal{G} - \mathcal{H}_{(11...11)}\rangle$ is the dishonest subgraph with σ_Zs on all vertices. Thus, the reduced state of the honest parties of this ideal state is given by

$$\rho_H^{|\mathcal{G}\rangle} = \frac{1}{2^{|H|}} \left[\left(\sum_{\Delta(\bar{\mathbf{z}})=0(\text{mod }4)} |\bar{\mathbf{z}}\rangle - \sum_{\Delta(\bar{\mathbf{z}})=2(\text{mod }4)} |\bar{\mathbf{z}}\rangle\right)\left(\sum_{\Delta(\bar{\mathbf{z}})=0(\text{mod }4)} \langle\bar{\mathbf{z}}| - \sum_{\Delta(\bar{\mathbf{z}})=2(\text{mod }4)} \langle\bar{\mathbf{z}}|\right) \right.$$

$$\left. + \left(\sum_{\Delta(\bar{\mathbf{z}})=1(\text{mod }4)} |\bar{\mathbf{z}}\rangle - \sum_{\Delta(\bar{\mathbf{z}})=3(\text{mod }4)} |\bar{\mathbf{z}}\rangle\right)\left(\sum_{\Delta(\bar{\mathbf{z}})=1(\text{mod }4)} \langle\bar{\mathbf{z}}| - \sum_{\Delta(\bar{\mathbf{z}})=3(\text{mod }4)} \langle\bar{\mathbf{z}}|\right)\right]. \quad \text{(B4)}$$

From Eqs. (A4) and (A5), we know that our state can be written in general as $|\Psi\rangle = \sum_{\bar{\mathbf{z}}} \alpha_{\bar{\mathbf{z}}}|\bar{\mathbf{z}}\rangle_H \otimes |\psi_{\bar{\mathbf{z}}}\rangle_D$ and $|\Psi\rangle = \sum_{\bar{\mathbf{x}}} \beta_{\bar{\mathbf{x}}}|\mathcal{H}_{(\bar{\mathbf{x}})}\rangle_H \otimes |\phi_{\bar{\mathbf{x}}}\rangle_D$. Let us now write the test measurements, which are the stabilizer generators here. Since, for the complete graph, each vertex shares an edge with every other vertex, the stabilizer generators are given by

$$K_i = X_i \prod_{e \in V} Z_e, \quad \text{(B5)}$$

where V is the set of vertices in the graph. We will again group the test measurements into group 1, where the honest measurement only consists of Z's, and group 2, which contains the remaining measurements. In order to pass perfectly, the overall outcome of each measurement must be $+1$.

Let us first consider the group 1 measurements. Any $|\bar{\mathbf{z}}\rangle$ that has an even number of 1's (parity of $\bar{\mathbf{z}}$ is 0) will give outcome $+1$ for the honest measurement $Z \dots Z$, and so the dishonest measurement must give outcome $+1$ in order to pass the test. Any $|\bar{\mathbf{z}}\rangle$ that has an odd number of 1's

(parity of $\bar{\mathbf{z}}$ is 1) will give outcome -1 for $Z \dots Z$, and so the dishonest measurement must give outcome -1. So, in order to pass perfectly, the dishonest parties must be able to discriminate perfectly between the states $|\psi_{\Delta(\bar{\mathbf{z}})=0(\text{mod }2)}\rangle$ and $|\psi_{\Delta(\bar{\mathbf{z}})=1(\text{mod }2)}\rangle$, where $\Delta(\bar{\mathbf{z}})$ is the Hamming weight of $\bar{\mathbf{z}}$ (number of 1's in the string). This means that for all $\bar{\mathbf{z}}$, we have $\langle\psi_{\Delta(\bar{\mathbf{z}})=0(\text{mod }2)}||\psi_{\Delta(\bar{\mathbf{z}})=1(\text{mod }2)}\rangle = 0$. (Note that this can be seen from the general proof, which tells us in this case that $\forall \bar{\mathbf{z}}, \bar{\mathbf{z}}'$ such that $\bigoplus_i z_i \neq \bigoplus_i z_i'$, we have $\langle\psi_{\bar{\mathbf{z}}}||\psi_{\bar{\mathbf{z}}'}\rangle = 0$.)

Now, let us see what happens if the group 2 measurements pass perfectly. This group will have all measurements $XZ \dots Z, ZXZ \dots Z, \dots, Z \dots ZX$ in the honest part, and the dishonest part of each will be $(Z \dots Z)'$ (so the same dishonest part for each). To pass perfectly, the dishonest parties must be able to always give the correct outcome; however, they only know that the measurement they must do is $(Z \dots Z)'$, and this does not tell them whether the honest parties are measuring $XZ \dots Z, ZXZ \dots Z, \dots, Z \dots ZX$. In order for the dishonest parties to always output the correct outcome for all of these

measurements (to make the overall outcome $+1$), the only terms that can appear in Eq. (A5) are the honest subgraph ($|\mathcal{H}_{(00\ldots00)}\rangle$), and the honest subgraph with σ_Z's on all the vertices ($|\mathcal{H}_{(11\ldots11)}\rangle$). So, passing the group 2 measurements tells us that $\beta_{\overline{\mathbf{x}}} = 0$ for $\overline{\mathbf{x}} \notin \{00\ldots00, 11\ldots11\}$. (Note that this is the same conclusion that can be derived from measuring the full set of stabilizers in the general proof. Every pair of honest vertices forms a possible set A here, and we have $\beta_{\overline{\mathbf{x}}} = 0$ if $\exists A$ such that $\bigoplus_{i \in A} x_i = 1$. The only remaining strings are then those $\overline{\mathbf{x}}$ that have all elements equal to one another.)

We can then write the state in Eq. (A5) as

$$|\Psi\rangle = \beta_{00\ldots00}|\mathcal{H}_{(00\ldots00)}\rangle_H|\phi_{00\ldots00}\rangle_D$$
$$+ \beta_{11\ldots11}|\mathcal{H}_{(11\ldots11)}\rangle_H|\phi_{11\ldots11}\rangle_D. \tag{B6}$$

Since measuring $(Z\ldots Z)'$ on $|\phi_{00\ldots00}\rangle$ must give outcome $+1$, and on $|\phi_{11\ldots11}\rangle$ it must give outcome -1 (in order to always get the total outcome to be $+1$), the dishonest parties must be able to perfectly discriminate between these two states, and so we must have $\langle\phi_{00\ldots00}||\phi_{11\ldots11}\rangle = 0$. Then, following the steps in the general proof, we get

$$\beta_{\overline{\mathbf{x}}}|\phi_{\overline{\mathbf{x}}}\rangle = \frac{1}{\sqrt{2^{|H|}}}\left[\sum_{\overline{\mathbf{z}}}(-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l}(-1)^{\bigoplus_i x_i \wedge z_i}\alpha_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}}\rangle_D\right], \quad \forall \, \overline{\mathbf{x}} \text{ such that } \beta_{\overline{\mathbf{x}}} \neq 0 \tag{B7}$$

$$0 = \frac{1}{\sqrt{2^{|H|}}}\left[\sum_{\overline{\mathbf{z}}}(-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l}(-1)^{\bigoplus_i x_i \wedge z_i}\alpha_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}}\rangle_D\right], \quad \forall \, \overline{\mathbf{x}} \text{ such that } \beta_{\overline{\mathbf{x}}} = 0. \tag{B8}$$

The solution of Eq. (B8), as adapted for complete graphs from the general proof, is $\forall \, \overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $\Delta(\overline{\mathbf{z}}) \bmod 2 = \Delta(\overline{\mathbf{z}}') \bmod 2$, we have

$$(-1)^{\bigoplus_{(k,l)\in E_H} z_k \wedge z_l}\alpha_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}}\rangle = (-1)^{\bigoplus_{(k,l)\in E_H} z_k' \wedge z_l'}\alpha_{\overline{\mathbf{z}}'}|\psi_{\overline{\mathbf{z}}'}\rangle. \tag{B9}$$

Recall that for complete graphs, all the honest vertices are connected to each other. Using this, we can simplify the exponent $\bigoplus_{(k,l)\in E_H} z_k \wedge z_l$. Each $(z_k \wedge z_l)$ will give 1 only if both z_k, z_l are 1. So, we can rephrase this using the Hamming weight $\Delta(\overline{\mathbf{z}})$, which tells us how many 1's are in the string $\overline{\mathbf{z}}$. Then, finding how many pairs $(z_k \wedge z_l)$ give 1 is equivalent to calculating $^{\Delta(\overline{\mathbf{z}})}C_2$.

Let us first take $\overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $\Delta(\overline{\mathbf{z}}), \Delta(\overline{\mathbf{z}}') = 0 \pmod 2$. We see that $(-1)^{\Delta(\overline{\mathbf{z}})}C_2 = (-1)^{\Delta(\overline{\mathbf{z}}')}C_2$ for $\Delta(\overline{\mathbf{z}}) \bmod 4 = \Delta(\overline{\mathbf{z}}') \bmod 4$. Similarly, if we take $\overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $\Delta(\overline{\mathbf{z}}), \Delta(\overline{\mathbf{z}}') = 1 \pmod 2$, we again find that $(-1)^{\Delta(\overline{\mathbf{z}})}C_2 = (-1)^{\Delta(\overline{\mathbf{z}}')}C_2$ for $\Delta(\overline{\mathbf{z}}) \bmod 4 = \Delta(\overline{\mathbf{z}}')$ mod 4. Thus, we have

$$\forall \, \overline{\mathbf{z}}, \overline{\mathbf{z}}' \text{ such that } \Delta(\overline{\mathbf{z}}) = 0 \pmod 4, \ \Delta(\overline{\mathbf{z}}') = 2 \pmod 4, \ \alpha_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}}\rangle = -\alpha_{\overline{\mathbf{z}}'}|\psi_{\overline{\mathbf{z}}'}\rangle,$$
$$\forall \, \overline{\mathbf{z}}, \overline{\mathbf{z}}' \text{ such that } \Delta(\overline{\mathbf{z}}) = 1 \pmod 4, \ \Delta(\overline{\mathbf{z}}') = 3 \pmod 4, \ \alpha_{\overline{\mathbf{z}}}|\psi_{\overline{\mathbf{z}}}\rangle = -\alpha_{\overline{\mathbf{z}}'}|\psi_{\overline{\mathbf{z}}'}\rangle. \tag{B10}$$

We can now write our state as

$$|\Psi\rangle = \sum_{\overline{\mathbf{z}}}\alpha_{\overline{\mathbf{z}}}|\overline{\mathbf{z}}\rangle_H \otimes |\psi_{\overline{\mathbf{z}}}\rangle_D$$

$$= \alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\bmod 2)}\left[\sum_{\Delta(\overline{\mathbf{z}})=0(\bmod 4)}|\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=2(\bmod 4)}|\overline{\mathbf{z}}\rangle\right]_H \otimes |\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\bmod 2)}\rangle_D$$

$$+ \alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\bmod 2)}\left[\sum_{\Delta(\overline{\mathbf{z}})=1(\bmod 4)}|\overline{\mathbf{z}}\rangle - \sum_{\Delta(\overline{\mathbf{z}})=3(\bmod 4)}|\overline{\mathbf{z}}\rangle\right]_H \otimes |\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\bmod 2)}\rangle_D. \tag{B11}$$

Then, our expressions for $\beta_{\overline{\mathbf{x}}}|\phi_{\overline{\mathbf{x}}}\rangle$ can be written using Eq. (A27) as

$$\beta_{00\ldots00}|\phi_{00\ldots00}\rangle = \frac{\sqrt{2^{|H|}}}{2}[\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\bmod 2)}|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\bmod 2)}\rangle + \alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\bmod 2)}|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\bmod 2)}\rangle],$$

$$\beta_{11\ldots11}|\phi_{11\ldots11}\rangle = \frac{\sqrt{2^{|H|}}}{2}[\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\bmod 2)}|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\bmod 2)}\rangle - \alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\bmod 2)}|\psi_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\bmod 2)}\rangle]. \tag{B12}$$

Now, recall that $\langle\phi_{00\ldots00}||\phi_{11\ldots11}\rangle = 0$, and $\langle\psi_{\Delta(\overline{\mathbf{z}})=0(\bmod 2)}||\psi_{\Delta(\overline{\mathbf{z}})=1(\bmod 2)}\rangle = 0$. Using these orthogonality conditions and taking the inner product of the two expressions above, we get

$$|\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=0(\bmod 2)}|^2 - |\alpha_{\overline{\mathbf{z}},\Delta(\overline{\mathbf{z}})=1(\bmod 2)}|^2 = 0. \tag{B13}$$

By normalization, we have

$$|\alpha_{\bar{\mathbf{z}}, \Delta(\bar{\mathbf{z}})=0(\text{mod }2)}|^2 + |\alpha_{\bar{\mathbf{z}}, \Delta(\bar{\mathbf{z}})=1(\text{mod }2)}|^2 = \frac{2}{2^{|H|}}. \tag{B14}$$

Solving these, we find that $\alpha_{\bar{\mathbf{z}}, \Delta(\bar{\mathbf{z}})=0(\text{mod }2)}, \alpha_{\bar{\mathbf{z}}, \Delta(\bar{\mathbf{z}})=1(\text{mod }2)} = \pm\frac{1}{\sqrt{2^{|H|}}}$. Substituting this in Eq. (B11) gives the state as

$$|\Psi\rangle = \pm\frac{1}{\sqrt{2^{|H|}}}\Bigg[\Bigg(\sum_{\Delta(\bar{\mathbf{z}})=0(\text{mod }4)}|\bar{\mathbf{z}}\rangle - \sum_{\Delta(\bar{\mathbf{z}})=2(\text{mod }4)}|\bar{\mathbf{z}}\rangle\Bigg)_H \otimes |\psi_{\bar{\mathbf{z}}, \Delta(\bar{\mathbf{z}})=0(\text{mod }2)}\rangle_D$$
$$\pm\Bigg(\sum_{\Delta(\bar{\mathbf{z}})=1(\text{mod }4)}|\bar{\mathbf{z}}\rangle - \sum_{\Delta(\bar{\mathbf{z}})=3(\text{mod }4)}|\bar{\mathbf{z}}\rangle\Bigg)_H \otimes |\psi_{\bar{\mathbf{z}}, \Delta(\bar{\mathbf{z}})=1(\text{mod }2)}\rangle_D\Bigg], \tag{B15}$$

which gives

$$\rho_H^{|\Psi\rangle} = \frac{1}{2^{|H|}}\Bigg[\Bigg(\sum_{\Delta(\bar{\mathbf{z}})=0(\text{mod }4)}|\bar{\mathbf{z}}\rangle - \sum_{\Delta(\bar{\mathbf{z}})=2(\text{mod }4)}|\bar{\mathbf{z}}\rangle\Bigg)\Bigg(\sum_{\Delta(\bar{\mathbf{z}})=0(\text{mod }4)}\langle\bar{\mathbf{z}}| - \sum_{\Delta(\bar{\mathbf{z}})=2(\text{mod }4)}\langle\bar{\mathbf{z}}|\Bigg)$$
$$+\Bigg(\sum_{\Delta(\bar{\mathbf{z}})=1(\text{mod }4)}|\bar{\mathbf{z}}\rangle - \sum_{\Delta(\bar{\mathbf{z}})=3(\text{mod }4)}|\bar{\mathbf{z}}\rangle\Bigg)\Bigg(\sum_{\Delta(\bar{\mathbf{z}})=1(\text{mod }4)}\langle\bar{\mathbf{z}}| - \sum_{\Delta(\bar{\mathbf{z}})=3(\text{mod }4)}\langle\bar{\mathbf{z}}|\Bigg)\Bigg]$$
$$= \rho_H^{|\mathcal{G}\rangle}. \tag{B16}$$

Thus, $|\Psi\rangle = U_D|\mathcal{G}\rangle$.

Inserting $\mathsf{J} = n$ into Lemmas 2 and 3 concludes the proof. ∎

2. Pentagon graph state

The five-qubit cycle graph state, in the shape of a pentagon, is known to be useful for secret sharing [6], as well as being the smallest quantum error-correcting code that tolerates an arbitrary error on a single qubit [46]. Let us now consider all possible sets of dishonest parties sharing such a graph (Fig. 3), and see how we can reduce the resources required. We will

FIG. 3. Sets of honest (H) and dishonest (D) parties for the pentagon graph state considered in Theorem 2B.

show that in certain cases, by purely measuring the stabilizer generators, we can determine that if all tests pass perfectly, the state $|\Psi\rangle = U_D|\mathcal{G}\rangle$; this means that the parties can run the simpler version of Protocol I (with $\mathcal{S}$ as the set of generators). We summarize the result in Theorem 2B.

Theorem 2B. If $|\mathcal{G}\rangle$ is a pentagon graph state with either one, three, or four dishonest parties anywhere in the network, or two dishonest parties who are adjacent, and we set $N_{\text{total}} = 2nN_{\text{test}}$, $N_{\text{test}} = \lceil mn^4 \ln n \rceil$, and $\mathcal{S}$ as the set of stabilizer generators, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol I satisfies
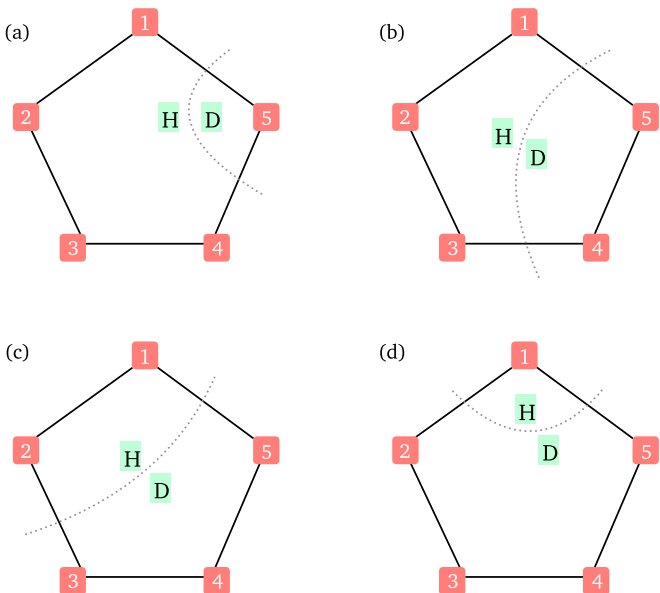
$$F\big(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}}\big) \geqslant 1 - \frac{2\sqrt{c}}{n} - 2n\left(1 - \frac{N_{\text{pass}}}{nN_{\text{test}}}\right) \tag{B17}$$

is at least $1 - n^{1-\frac{2cm}{3}}$, where m, c are positive constants chosen such that $\frac{3}{2m} < c < \frac{(n-1)^2}{4}$.

Proof. We will tackle this proof taking all possible sets of dishonest parties separately. For the sets of dishonest parties specified in the statement of Theorem 2B, we will show certain steps in proving that by passing all stabilizer generator tests, our state must be $|\Psi\rangle = U_D|\mathcal{G}\rangle$. Then, as long as the honest parties know that the set of dishonest parties belongs to this "allowed set," they may simply measure the stabilizer generators instead of the full stabilizer group.

a. One dishonest party

We will start with a scenario where one party in the network is dishonest. Without loss of generality, let us assume party 5 is dishonest, as shown in Fig. 3(a). Then, we can write the Schmidt decomposition of the ideal state $|\mathcal{G}\rangle$ with respect

to the partition (H, D) as

$$|\mathcal{G}\rangle = \frac{1}{\sqrt{2^4}} \sum_{\overline{\mathbf{z}}} (-1)^{(z_1 \wedge z_2) \oplus (z_2 \wedge z_3) \oplus (z_3 \wedge z_4)} |\overline{\mathbf{z}}\rangle_H \otimes \left(\sigma_Z^{(5)}\right)^{z_1} \left(\sigma_Z^{(5)}\right)^{z_4} |\mathcal{G} - \mathcal{H}\rangle_D$$

$$= \frac{1}{4} [(|0000\rangle + |1001\rangle + |0010\rangle - |1011\rangle + |0100\rangle - |1101\rangle - |0110\rangle - |1111\rangle)_H \otimes |\mathcal{G} - \mathcal{H}_{(0)}\rangle_D$$

$$+ (|0001\rangle + |1000\rangle - |0011\rangle + |1010\rangle + |0101\rangle - |1100\rangle + |0111\rangle + |1110\rangle)_H \otimes |\mathcal{G} - \mathcal{H}_{(1)}\rangle_D]. \quad (B18)$$

(Note that, as expected, the dishonest part of the state $|\mathcal{G} - \mathcal{H}\rangle$ is the same for honest parts with the same value of $\underset{i \in N(d)}{\oplus} z_i = z_1 \oplus z_4$.)

As usual, we start by writing our state in the honest computational and subgraph bases as in Eqs. (A4) and (A5). Now, the test measurements, or the stabilizer generators in this case, are given by $\{XZ\mathbb{1}\mathbb{1}Z', ZXZ\mathbb{1}\mathbb{1}', \mathbb{1}ZXZ\mathbb{1}', \mathbb{1}\mathbb{1}ZXZ', Z\mathbb{1}\mathbb{1}ZX'\}$. We group them into group 1 measurements $\{Z\mathbb{1}\mathbb{1}ZX'\}$ and group 2 measurements $\{XZ\mathbb{1}\mathbb{1}Z', ZXZ\mathbb{1}\mathbb{1}', \mathbb{1}ZXZ\mathbb{1}', \mathbb{1}\mathbb{1}ZXZ'\}$. From the group 1 measurement passing perfectly, we see that $\forall \overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $z_1 \oplus z_4 \neq z_1' \oplus z_4'$, we must have $\langle \psi_{\overline{\mathbf{z}}} | | \psi_{\overline{\mathbf{z}}'} \rangle = 0$. [Note that this matches Eq. (A8).] From the group 2 measurements passing perfectly, we know that $\forall \overline{\mathbf{x}}, \overline{\mathbf{x}}'$, we have $\langle \phi_{\overline{\mathbf{x}}} | | \phi_{\overline{\mathbf{x}}'} \rangle = 0$.

We will now see how to set certain $\beta_{\overline{\mathbf{x}}} = 0$ from just the stabilizer generators alone. The measurements $ZXZ\mathbb{1}\mathbb{1}', \mathbb{1}ZXZ\mathbb{1}'$ must give outcome $+1$ to pass the test. Since the dishonest party asked to measure $\mathbb{1}'$ will always output $+1$, the honest measurements $ZXZ\mathbb{1}, \mathbb{1}ZXZ$ must also give outcome $+1$. Further, the measurements $XZ\mathbb{1}\mathbb{1}Z', \mathbb{1}\mathbb{1}ZXZ'$ give outcome $+1$. Since the dishonest party asked to measure Z' does not know whether the honest parties are measuring $XZ\mathbb{1}\mathbb{1}$ or $\mathbb{1}\mathbb{1}ZX$, yet still manages to make the test pass perfectly, this means that the honest part of the state must give the same outcome for these two measurements. With these conditions, we have $\beta_{\overline{\mathbf{x}}} = 0 \ \forall \overline{\mathbf{x}} \notin \{0000, 1001\}$. (Note that we get the same result from the full stabilizer group: the possible sets A are $\{1, 4\}, \{2\}, \{3\}, \{2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{1, 2, 3, 4\}$ and so $\beta_{\overline{\mathbf{x}}} = 0$ if $x_1 \oplus x_4 = 1, x_2 = 1$, or $x_3 = 1$.)

Following the remaining steps of the general proof, we then get

$$|\Psi\rangle = \pm \frac{1}{\sqrt{2^4}} [(|0000\rangle + |1001\rangle + |0010\rangle - |1011\rangle + |0100\rangle - |1101\rangle - |0110\rangle - |1111\rangle)_H \otimes |\phi_{0000}\rangle_D$$

$$\pm (|0001\rangle + |1000\rangle - |0011\rangle + |1010\rangle + |0101\rangle - |1100\rangle + |0111\rangle + |1110\rangle)_H \otimes |\phi_{1001}\rangle_D], \quad (B19)$$

which gives $|\Psi\rangle = U_D |\mathcal{G}\rangle$.

b. Two dishonest parties

Let us start by considering parties 1, 2, and 3 as honest and parties 4 and 5 as dishonest, pictured in Fig. 3(b). We will vary the dishonest parties later and see how this affects the results, but for now let us consider the two dishonest parties to be adjacent to one another. The Schmidt decomposition of the ideal graph state for this partition is given by

$$|\mathcal{G}\rangle = \frac{1}{\sqrt{2^3}} \sum_{\overline{\mathbf{z}}} (-1)^{(z_1 \wedge z_2) \oplus (z_2 \wedge z_3)} |\overline{\mathbf{z}}\rangle_H \otimes (\sigma_Z^{(5)})^{z_1} (\sigma_Z^{(4)})^{z_3} |\mathcal{G} - \mathcal{H}\rangle_D$$

$$= \frac{1}{2\sqrt{2}} [(|000\rangle + |010\rangle)_H \otimes |\mathcal{G} - \mathcal{H}_{(00)}\rangle_D + (|001\rangle - |011\rangle)_H \otimes |\mathcal{G} - \mathcal{H}_{(10)}\rangle_D$$

$$+ (|100\rangle - |110\rangle)_H \otimes |\mathcal{G} - \mathcal{H}_{(01)}\rangle_D + (|101\rangle + |111\rangle)_H \otimes |\mathcal{G} - \mathcal{H}_{(11)}\rangle_D]. \quad (B20)$$

(It is easy to see that for states with the same $\underset{i \in N(d)}{\oplus} z_i$, $\forall d \in D$, which here refers to states with the same value of z_1 and z_3, the corresponding dishonest part $|\mathcal{G} - \mathcal{H}\rangle$ is the same.)

Let us now see whether we can make the desired statement by purely considering the stabilizer generators $\{XZ\mathbb{1}(\mathbb{1}Z)', ZXZ(\mathbb{1}\mathbb{1})', \mathbb{1}ZX(Z\mathbb{1})', \mathbb{1}\mathbb{1}Z(XZ)', Z\mathbb{1}\mathbb{1}(ZX)'\}$. We group them, as usual, into group 1 given by $\{\mathbb{1}\mathbb{1}Z(XZ)', Z\mathbb{1}\mathbb{1}(ZX)'\}$, and group 2 given by $\{XZ\mathbb{1}(\mathbb{1}Z)', ZXZ(\mathbb{1}\mathbb{1})', \mathbb{1}ZX(Z\mathbb{1})'\}$. By the measurements in group 1 passing perfectly, we see that $\forall \overline{\mathbf{z}}, \overline{\mathbf{z}}'$ such that $z_1 \neq z_1'$ or $z_3 \neq z_3'$, we have $\langle \psi_{\overline{\mathbf{z}}} | | \psi_{\overline{\mathbf{z}}'} \rangle = 0$, which can also be seen from Eq. (A8). By the measurements in group 2 passing perfectly, we have $\forall \overline{\mathbf{x}}, \overline{\mathbf{x}}', \langle \phi_{\overline{\mathbf{x}}} | | \phi_{\overline{\mathbf{x}}'} \rangle = 0$.

Now, group 2 contains the measurement $ZXZ(\mathbb{1}\mathbb{1})'$. In order to get outcome $+1$ here, the only terms of the honest subgraph that can appear in Eq. (A5) are those that give $+1$ when measuring ZXZ. Thus, the group 2 measurements passing perfectly tells us that $\beta_{\overline{\mathbf{x}}} = 0 \ \forall \overline{\mathbf{x}} \notin \{000, 001, 100, 101\}$. (Note that by using the full set of stabilizer measurements, we do not get more information than this, as the only possible set $A = \{2\}$ and so we know that if $x_2 = 1$, then $\beta_{\overline{\mathbf{x}}} = 0$.) Continuing with the steps of the general proof, we obtain $|\Psi\rangle = U_D |\mathcal{G}\rangle$.

By inspecting the stabilizer generators, we see that such an analysis holds whenever the two dishonest parties are adjacent, as there will always be a measurement $(\mathbb{1}\mathbb{1})'$ that forces the corresponding honest outcome to be $+1$. Thus, in this case, it suffices to measure the stabilizer generators. If the two

dishonest parties are not adjacent, however, there will not be such a measurement $(\mathbb{1}\mathbb{1})'$, and so the parties must measure the full set of stabilizers.

c. Three dishonest parties

Let us now assume parties 1 and 2 are honest, while parties 3, 4, and 5 are dishonest, as in Fig. 3(c), to start with. The Schmidt decomposition is given by

$$
|\mathcal{G}\rangle = \frac{1}{\sqrt{2^2}} \sum_{\bar{\mathbf{z}}} (-1)^{z_1 \wedge z_2} |\bar{\mathbf{z}}\rangle_H \otimes (\sigma_Z^{(5)})^{z_1} (\sigma_Z^{(3)})^{z_2} |\mathcal{G} - \mathcal{H}\rangle_D
$$

$$
= \frac{1}{2} [|00\rangle_H \otimes |\mathcal{G} - \mathcal{H}_{(000)}\rangle_D + |01\rangle_H \otimes |\mathcal{G} - \mathcal{H}_{(100)}\rangle_D
$$

$$
+ |10\rangle_H \otimes |\mathcal{G} - \mathcal{H}_{(001)}\rangle_D - |11\rangle_H \otimes |\mathcal{G} - \mathcal{H}_{(101)}\rangle_D].
$$
(B21)

(Here, as in the general proof, we see that both z_1 and z_2 must be the same in order for the corresponding $|\mathcal{G} - \mathcal{H}\rangle$ to be the same.)

As we see here, there is no grouping of $|\bar{\mathbf{z}}\rangle$ terms, and so there will be no $\beta_{\bar{\mathbf{x}}} = 0$. The group 1 measurements are then $\{\mathbb{1}Z(XZ\mathbb{1})', \mathbb{1}\mathbb{1}(ZXZ)', Z\mathbb{1}(\mathbb{1}ZX)'\}$, and the group 2 measurements are $\{XZ(\mathbb{1}\mathbb{1}Z)', ZX(Z\mathbb{1}\mathbb{1})'\}$. We see that if $z_1 \neq z_1'$ or $z_2 \neq z_2'$, the respective states are orthogonal. This implies that $\langle \psi_{\bar{\mathbf{z}}} || \psi_{\bar{\mathbf{z}}'} \rangle = 0 \ \forall \ \bar{\mathbf{z}}, \bar{\mathbf{z}}'$. We also have $\forall \ \bar{\mathbf{x}}, \bar{\mathbf{x}}', \langle \phi_{\bar{\mathbf{x}}} || \phi_{\bar{\mathbf{x}}'} \rangle = 0$. From passing the group 2 measurements, we cannot set any $\beta_{\bar{\mathbf{x}}} = 0$ (using the full stabilizer set, we see that A is the empty set). Then, we simply follow the steps of the general proof to get $|\Psi\rangle = U_D|\mathcal{G}\rangle$. This reasoning holds for any two parties being dishonest, no matter whether they are adjacent, and so, for this case, the parties only need to measure the stabilizer generators.

d. Four dishonest parties

In this scenario where only one party is honest, the analysis is again simple. Without loss of generality, let us assume only party 1 is honest, as shown in Fig. 3(d). First, let us write the Schmidt decomposition for this partition (H, D) as

$$
|\mathcal{G}\rangle = \frac{1}{\sqrt{2^1}} \sum_{\bar{\mathbf{z}}} |\bar{\mathbf{z}}\rangle_H \otimes (\sigma_Z^{(2)} \sigma_Z^{(5)})^{z_1} |\mathcal{G} - \mathcal{H}\rangle_D
$$

$$
= \frac{1}{\sqrt{2}} [|0\rangle_H \otimes |\mathcal{G} - \mathcal{H}_{(0000)}\rangle_D + |1\rangle_H \otimes |\mathcal{G} - \mathcal{H}_{(1001)}\rangle_D].
$$
(B22)

(Note that, as in the general proof, if $\bigoplus_{i \in N(d)} z_i = z_1$ is the same, the corresponding $|\mathcal{G} - \mathcal{H}\rangle$ is the same.)

Now, the set of measurements is given by the stabilizer generators again, which we will separate into group 1 containing $\{Z(XZ\mathbb{1}\mathbb{1})', \mathbb{1}(ZXZ\mathbb{1})', \mathbb{1}(\mathbb{1}ZXZ)', Z(\mathbb{1}\mathbb{1}ZX)'\}$, and group 2 containing $\{X(Z\mathbb{1}\mathbb{1}Z)'\}$. Group 1 passing perfectly gives $\langle \psi_0 || \psi_1 \rangle = 0$ since $|0\rangle_H, |1\rangle_H$ will give different outcomes for Z, and so the dishonest parties must be able to perfectly discriminate between their corresponding parts of the state in order to pass perfectly [we reach the same conclusion using Eq. (A8)]. Similarly, group 2 passing perfectly gives $\langle \phi_0 || \phi_1 \rangle = 0$ since $|+\rangle_H, |-\rangle_H$ give different outcomes
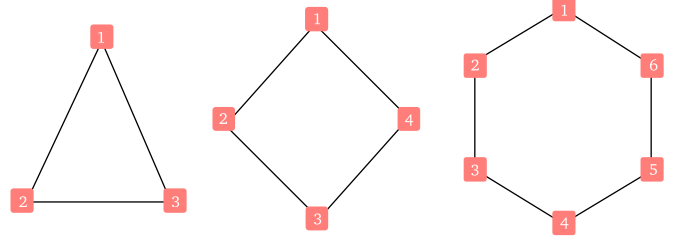

FIG. 4. Three-, four-, and six-qubit cycle (ring) graph states.

for X. When there is only one honest party, we cannot set any $\beta_{\bar{\mathbf{x}}} = 0$ from passing perfectly (the set A is the empty set, so this gives the same result as measuring the full stabilizer set). We then proceed with the proof to get $|\Psi\rangle = U_D|\mathcal{G}\rangle$.

Thus, for any number of adjacent dishonest parties, passing the stabilizer generator tests of Protocol I allows us to conclude that the state in each round is $|\Psi\rangle = U_D|\mathcal{G}\rangle$. Inserting $\mathsf{J} = n$ into Lemmas 2 and 3 concludes the proof. ∎

3. Cycle graph states

With the example of the pentagon graph state in the previous subsection, we notice some features which can be extended to general n-qubit cycle (or ring) graph states (Fig. 4), used in various applications such as quantum error correction [4] and quantum walks [47]. In Theorem 2C, we give some cases for the cycle graph state where it suffices to measure only stabilizer generators in Protocol I. We will outline the reasoning behind this, although it can be seen explicitly in the pentagon graph state example.

Theorem 2C. If $|\mathcal{G}\rangle$ is a cycle graph state with either one, $n - 2$, or $n - 1$ dishonest parties anywhere in the network, or any other number of dishonest parties who are adjacent, and we set $N_{\text{total}} = 2nN_{\text{test}}$, $N_{\text{test}} = \lceil mn^4 \ln n \rceil$, and $\mathcal{S}$ as the set of stabilizer generators in Protocol I, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol I satisfies

$$
F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}}\right) \geqslant 1 - \frac{2\sqrt{c}}{n} - 2n\left(1 - \frac{N_{\text{pass}}}{nN_{\text{test}}}\right) \quad \text{(B23)}
$$

is at least $1 - n^{1 - \frac{2cm}{3}}$, where m, c are positive constants chosen such that $\frac{3}{2m} < c < \frac{(n-1)^2}{4}$.

Proof sketch. Whenever there are $n - 1$ or $n - 2$ dishonest parties in the network, the Schmidt decomposition is given by

$$
|\mathcal{G}\rangle = \frac{1}{\sqrt{2^{|H|}}} \sum_{\bar{\mathbf{z}}} |\bar{\mathbf{z}}\rangle_H \otimes |\mathcal{G} - \mathcal{H}_{(\bar{\mathbf{z}})}\rangle_D, \quad \text{(B24)}
$$

where each $|\bar{\mathbf{z}}\rangle$ corresponds to a different dishonest part $|\mathcal{G} - \mathcal{H}\rangle$. This means that there is no grouping of $|\bar{\mathbf{z}}\rangle$ terms, and so the group 2 measurements do not tell us that any $\beta_{\bar{\mathbf{x}}} = 0$, as we saw in the previous example. Thus, in this case the parties can simply measure the stabilizer generators (the full stabilizer group would give no additional information, as the set A is empty).

Let us now consider the case of one dishonest party. The dishonest measurements of $\mathbb{1}'$, corresponding to the generators of qubits $i \notin N(d)$, ensure that if $x_{i \notin N(d)} = 1$, then $\beta_{\bar{\mathbf{x}}} = 0$. Further, the two dishonest measurements of Z', corresponding

FIG. 5. Five-qubit path graph state, or 1D cluster state.

to the generators of the two qubits $i \in N(d)$, ensure that if $x_{i \in N(d)}$ are not the same (in order to give the same honest outcome), then $\beta_{\overline{\mathbf{x}}} = 0$. This means that the only terms in the honest subgraph are $|\mathcal{H}_{(00...00)}\rangle$ and $|\mathcal{H}_{(10...01)}\rangle$, which allows us to arrive at our result from just the stabilizer generators. [Note that using the full stabilizer group, Eq. (A11) would imply that if $\bigoplus_{i \in N(d)} x_i = 1$, or $x_{i \notin N(d)} = 1$, then $\beta_{\overline{\mathbf{x}}} = 0$, which gives the same result.]

Finally, for any other number of honest or dishonest parties, if the dishonest parties are adjacent then there will be measurements $(\mathbb{1} ... \mathbb{1})'$ in the set of stabilizer generators, corresponding to the generators of honest vertices that are not connected to any of the dishonest vertices [for qubits $i \notin N(D)$]. Since the dishonest part must give outcome $+1$ for this measurement, the honest part must also give outcome $+1$ in order to pass perfectly, any terms where $x_{i \notin N(D)} = 1$ must have $\beta_{\overline{\mathbf{x}}} = 0$. (Note that using the full stabilizer group, the possible sets A are all combinations of honest vertices that are not connected to any dishonest vertex, which gives the same result.) Thus, we can conclude that $|\Psi\rangle = U_D|\mathcal{G}\rangle$ from only measuring the stabilizer generators.

Inserting $\mathsf{J} = n$ into Lemmas 2 and 3 concludes the proof. ∎

In fact, there are additional examples that do not fall into these categories, but where it suffices to measure the stabilizer generators only. For example, consider the six-qubit cycle graph state with $D = \{2, 3, 6\}$, the seven-qubit cycle graph state with $D = \{2, 3, 4, 7\}$, or the eight-qubit cycle graph state with $D = \{2, 3, 6, 7\}$. There are no $\beta_{\overline{\mathbf{x}}} = 0$ in the Schmidt decomposition for these cases, which means that by passing the stabilizer generator measurements in Protocol I perfectly, we can determine that $|\Psi\rangle = U_D|\mathcal{G}\rangle$.

4. Cluster states

Cluster states correspond to lattices of dimension D, and have been shown to be a central resource in MBQC [1,30]. For verification of such states in an untrusted network, we will now give some examples of scenarios where we can reduce the number of test measurements to purely the stabilizer generators (thus allowing the parties to run the simpler verification scheme in Protocol I) with a smaller set of test measurements. Again, these are not the only possible sets of dishonest parties in a cluster state network that allow such a simplification; there may be many more examples.

Linear, or one-dimensional, cluster states (also known as path graph states) correspond to qubits connected in a line (Fig. 5). In Theorem 2D, we give some cases where it is sufficient to measure the stabilizer generators.

Theorem 2D. If $|\mathcal{G}\rangle$ is a 1D cluster state with either one or $n-1$ dishonest parties anywhere in the network, or any other number of adjacent honest or dishonest parties, and we set $N_{\text{total}} = 2nN_{\text{test}}$, $N_{\text{test}} = \lceil mn^4 \ln n \rceil$, and $\mathcal{S}$ is the set of stabilizer generators, the probability that the fidelity of the averaged state of the target copy (over all possible choices of

the tested copies and target copy) in Protocol I satisfies

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}}\right) \geqslant 1 - \frac{2\sqrt{c}}{n} - 2n\left(1 - \frac{N_{\text{pass}}}{nN_{\text{test}}}\right) \qquad \text{(B25)}$$

is at least $1 - n^{1-\frac{2cm}{3}}$, where m, c are positive constants chosen such that $\frac{3}{2m} < c < \frac{(n-1)^2}{4}$.

Proof. The stabilizer generators of an n-qubit 1D cluster state are given by $\{XZ\mathbb{1} ... \mathbb{1}, ZXZ\mathbb{1} ... \mathbb{1}, ..., \mathbb{1} ... \mathbb{1}ZX\}$. As we noted for cycle graphs, if there are $n - 1$ dishonest parties in the network, it suffices to measure only stabilizer generators, as passing the group 2 measurements perfectly does not tell us to set any $\beta_{\overline{\mathbf{x}}} = 0$.

If there is one dishonest party at either end of the line, we see that to get overall outcome $+1$, the honest part of the stabilizer generator measurements corresponding to every honest vertex $i \notin N(d)$ must give outcome $+1$. This means that if $x_{i \notin N(d)} = 1$, we must have $\beta_{\overline{\mathbf{x}}} = 0$. [Note that from the full stabilizer group, we see that all possible sets A contain only honest vertices $i \notin N(d)$, and so we come to the same conclusion.] If the dishonest party is not at the end of the line, but at a vertex connected to two other (honest) vertices, we again must have that if $x_{i \notin N(d)} = 1$ then $\beta_{\overline{\mathbf{x}}} = 0$ and, further, the honest part of the stabiliser generators for $i \in N(d)$ must give the same outcome (as they have the same dishonest part). This means that if x_i does not have the same value for both $i \in N(d)$, then $\beta_{\overline{\mathbf{x}}} = 0$. [Note that this gives the same result as using the full stabilizer group, as the set A may consist of any combination of honest vertices $i \notin N(d)$ as well as both honest vertices $i \in N(d)$.]

Further, for any other number of dishonest parties, if it is known that the honest parties are all adjacent to each other, or the dishonest parties are all adjacent to each other, then the parties could measure only the stabilizer generators. In such a setting, there will be $(\mathbb{1} ... \mathbb{1})'$ measurements in the stabilizer generators [corresponding to $i \notin N(D)$] that allow us to set $\beta_{\overline{\mathbf{x}}} = 0$ if $x_{i \notin N(D)} = 1$. [Note that from the full stabilizer group, all possible sets A will consist of $i \notin N(D)$, and so this gives the same result.] This corresponds to the first $|H|$ qubits of the line belonging to the honest parties, and the remaining $|D|$ qubits belonging to the dishonest parties (or vice versa).

Inserting $\mathsf{J} = n$ into Lemmas 2 and 3 concludes the proof. ∎

Additional examples of path graph states where it is sufficient to measure only the stabilizer generators include, for the five-qubit path graph, the sets $D = \{1, 2, 5\}$, or $D = \{1, 3, 5\}$, where there are no $\beta_{\overline{\mathbf{x}}} = 0$ in the Schmidt decomposition, and so measuring the stabilizer generators suffices.

Two-dimensional cluster states have the underlying structure of a $t \times t$ square grid, where the total number of qubits in the lattice is $n = t \times t$. In Theorem 2E, we give certain sets of dishonest parties for which it is possible to verify such states with the resource-efficient Protocol I requiring only generator tests. This is a useful result for verification in the MBQC paradigm.

Theorem 2E. If $|\mathcal{G}\rangle$ is a 2D cluster state with either one or $n-1$ dishonest parties anywhere in the network, or any other set of adjacent dishonest parties that forms a square or rectangle anywhere in the network, and we set $N_{\text{total}} = 2nN_{\text{test}}$, $N_{\text{test}} = \lceil mn^4 \ln n \rceil$, and $\mathcal{S}$ as the set of stabilizer generators, the
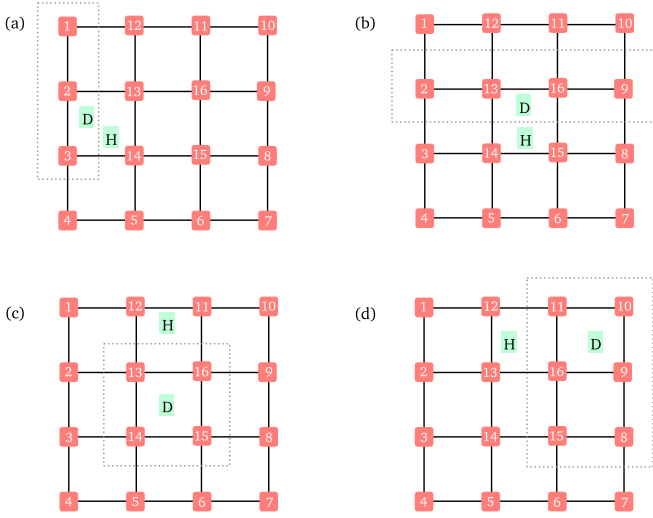
FIG. 6. Sets of honest (H) and dishonest (D) parties for the 4×4 cluster state considered in Theorem 2E.

probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol I satisfies

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}}\right) \geqslant 1 - \frac{2\sqrt{c}}{n} - 2n\left(1 - \frac{N_{\text{pass}}}{nN_{\text{test}}}\right) \quad \text{(B26)}$$

is at least $1 - n^{1 - \frac{2cm}{3}}$, where m, c are positive constants chosen such that $\frac{3}{2m} < c < \frac{(n-1)^2}{4}$.

Proof. Similarly to what we have seen in previous examples, if there is one honest party, or one dishonest party, it is enough to measure only the stabilizer generators. We will now show that, for any number of dishonest parties in a 2D cluster state, if they form a square or rectangle in the lattice, it is possible to do the verification using only the generators.

Consider the example of a 4×4 (or 16-qubit) cluster state, with example sets of honest and dishonest parties as shown in Fig. 6. Let us start with the parties 1, 2, and 3 being dishonest, while the remaining are honest, as in Fig. 6(a). If we write the set of stabilizer generators, we find that the generators corresponding to qubits 5, 6, 7, 8, 9, 10, 11, 15, and 16 will have dishonest part $(\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1})'$, as they are not connected to the dishonest set. This means that the corresponding honest measurements on the state $|\Psi\rangle$ must give outcome $+1$. Recall that the generator of qubit i contains the measurement X_i, which tells us that if $x_i = 1$ for $i \in \{5, 6, 7, 8, 9, 10, 11, 15, 16\}$ (or, equivalently, if $x_{i \notin N(D)} = 1$), then $\beta_{\overline{\mathbf{x}}} = 0$. Further, the dishonest part of the measurement will be the same for generators of qubits 4 and 14 (since they are both connected to dishonest qubit 3). This means that in order to pass these test measurements, the corresponding honest part of the measurements must give the same outcome, and so we must have that if $x_4 \neq x_{14}$, then $\beta_{\overline{\mathbf{x}}} = 0$. [Note that from the full stabilizer group, we have all possible sets A containing $i \notin N(D)$ as well as both $i = 4, 14$ which are evenly connected to all $d \in D$. This gives the same conclusions as previously, and so it is clear that only measuring the generators is necessary.]

Now, consider the example shown in Fig. 6(b), where parties 2, 13, 16, and 9 are dishonest, while the remaining

are honest. Again, writing the set of stabilizer generators, we find that the generators corresponding to qubits 4, 5, 6 and 7 have dishonest part $(\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1})'$, which tells us that if $x_i = 1$ for $i \in \{4, 5, 6, 7\}$, then $\beta_{\overline{\mathbf{x}}} = 0$. Further, the generators of qubits 1 and 3, 12 and 14, 11 and 15, and 8 and 10 have the same dishonest part, and so we must have that if either $x_1 \neq x_3$, $x_{12} \neq x_{14}$, $x_{11} \neq x_{15}$, or $x_8 \neq x_{10}$, then $\beta_{\overline{\mathbf{x}}} = 0$. [Note that from the full stabilizer group, the set A consists of all combinations of $i \notin N(D)$, as well as combinations of the pairs of vertices (1, 3), (12, 14), (11, 15), (8, 10) which are evenly connected to all $d \in D$, leading to the same result.]

Let us now move on to the example shown in Fig. 6(c), where parties 13, 14, 15, and 16 are dishonest, and the remaining are honest. The generators of qubits 1, 4, 7, and 10 have dishonest part $(\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1})'$, which means that if $x_i = 1$ for $i \in \{1, 4, 7, 10\}$, then $\beta_{\overline{\mathbf{x}}} = 0$. Further, the generators of qubits 1 and 12, 9 and 11, 3 and 5, and 6 and 8 have the same dishonest part, which means that, additionally, if either $x_1 \neq x_{12}$, $x_9 \neq x_{11}$, $x_3 \neq x_5$, or $x_6 \neq x_8$, then $\beta_{\overline{\mathbf{x}}} = 0$. [Note that from the full stabilizer group, we come to the same conclusions, as the set A contains all combinations of $i \notin N(D)$ as well as the pairs (1, 12), (9, 11), (3, 5), (6, 8).]

As another example, consider the dishonest set to comprise of parties 8, 9, 10, 11, 15, and 16, as shown in Fig. 6(d). From the generators whose dishonest part is $(\mathbb{1} \ldots \mathbb{1})'$, we must have that if $x_i = 1$ for $i \in \{1, 2, 3, 4, 5\}$, then $\beta_{\overline{\mathbf{x}}} = 0$. Further, from the generators whose dishonest part is the same, we have that if $x_6 \neq x_{14}$, then $\beta_{\overline{\mathbf{x}}} = 0$. [Note that from the full stabilizer group, we see that the set A can contain all combinations of $i \notin N(D)$ along with the pair (6, 14).]

Such an analysis easily extends to all cases where the dishonest parties lie in a square or rectangular section of the lattice; for example, where $D = \{8, 9, 10, 11, 12, 13, 14, 15, 16\}$ or $D = \{5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$.

We finish the proof by invoking Lemmas 2 and 3, taking $\mathsf{J} = n$. ∎

Note that there are many other sets of dishonest parties for the 2D cluster state for which passing only the stabilizer generator measurements perfectly implies $|\Psi\rangle = U_D|\mathcal{G}\rangle$; as before, here we are only giving some examples of cases where such a simplification is allowed.

APPENDIX C: PROOF OF THEOREM 3

In Protocol II, we outlined a symmetric protocol for verification of any graph state with a randomly chosen party playing the role of the Verifier. We will now prove its security in the following theorem.

Theorem 3. If we set $N_{\text{total}} = (\lambda + 1)\lambda \mathsf{J} N_{\text{test}}$ and $N_{\text{test}} = \lceil m\mathsf{J}^4 \ln \mathsf{J} \rceil$, the probability that the fidelity of the averaged state of the target copy (over all possible choices of the tested copies and target copy) in Protocol II satisfies

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}}\right) \geqslant 1 - \left(\frac{1}{\lambda} - \frac{1}{\lambda^2}\right)$$
$$- \left(1 + \frac{1}{\lambda}\right)\left[\frac{\sqrt{c}}{\mathsf{J}} + \lambda \mathsf{J} - \frac{N_{\text{pass}}}{N_{\text{test}}}\right] \quad \text{(C1)}$$

is at least $[1 - \sum_{x=0}^{\lambda} (1 - \frac{|H|}{n})^x (\frac{|H|}{n} \mathsf{J}^{-\frac{2cm}{3}})^{\lambda-x}]^{\mathsf{J}}$, where m, c are positive constants chosen such that the fidelity and probability expressions are greater than zero.

Proof. Recall that by Serfling's bound, we have

$$\Pr\left[\sum_{t \in \overline{\Pi}} Y_t \leqslant \frac{\mathcal{L}}{\mathcal{R}} \sum_{t \in \Pi} Y_t + \mathcal{L}\nu\right]$$

$$\geqslant 1 - \exp\left[-\frac{2\nu^2 \mathcal{L}\mathcal{R}^2}{(\mathcal{L} + \mathcal{R})(\mathcal{R} + 1)}\right]. \quad \text{(C2)}$$

In step 2 of Protocol II, each $\mathcal{S}_j$ is tested in λ sets of N_{test} copies, with a Verifier chosen at random for each set of N_{test} copies. Now consider the case where we measure the lth set of N_{test} copies for the stabilizer $\mathcal{S}_j$. This corresponds to taking $\mathcal{L} = N_{\text{total}} - [(j-1)\lambda + l]N_{\text{test}}$ and $\mathcal{R} = N_{\text{test}}$. Let $\Pi^{(j,l)}$ be the lth set of copies on which each S_j is measured, and $\overline{\Pi}^{(j,l)}$ be the set of remaining copies after measuring. Applying Serfling's bound and assuming an honest Verifier, we get

$$\Pr\left[\sum_{t \in \overline{\Pi}^{(j,l)}} Y_t \leqslant \frac{N_{\text{total}} - [(j-1)\lambda + l]N_{\text{test}}}{N_{\text{test}}} \sum_{t \in \Pi^{(j,l)}} Y_t + \{N_{\text{total}} - [(j-1)\lambda + l]N_{\text{test}}\}\nu\right] \geqslant q_j^l. \quad \text{(C3)}$$

The number of remaining copies after all tests is $\mathsf{N} = N_{\text{total}} - \lambda \mathsf{J} N_{\text{test}} = \lambda^2 \mathsf{J} N_{\text{test}}$. To bound k, which is the number of "good" copies in the remaining, we must determine the number of "bad" copies for each stabilizer measurement $\mathcal{S}_j$. Recall that for each λN_{test} copies that we test with stabilizer $\mathcal{S}_j$, the CRS randomly chooses a different Verifier to test each set of N_{test} copies.

Let us now assume that for each stabilizer test $\mathcal{S}_j$, at least one Verifier (out of λ) is honest, meaning that $\lambda - 1$ Verifiers are dishonest. For the $(\lambda - 1)N_{\text{test}}$ copies tested by a dishonest Verifier, we cannot conclude anything from our test since the Verifier can let any state could pass the test. So, for all $\mathcal{S}_j$ copies, we have a total of $(\lambda - 1)\mathsf{J}N_{\text{test}}$ copies that we will have to assume are bad. This means that we can lower bound k by

$$\mathsf{k} \geqslant (N_{\text{total}} - \lambda \mathsf{J} N_{\text{test}}) - (\lambda - 1)\mathsf{J}N_{\text{test}} - \sum_{j=1}^{\mathsf{J}}\left[\frac{N_{\text{total}} - [(j-1)\lambda]N_{\text{test}}}{N_{\text{test}}} \sum_{t \in \Pi^{(j,l)}} Y_t + \{N_{\text{total}} - [(j-1)\lambda]N_{\text{test}}\}\nu\right]$$

$$= N_{\text{total}} - (2\lambda - 1)\mathsf{J}N_{\text{test}} - \sum_{j=1}^{\mathsf{J}}\left[\frac{N_{\text{total}} - [(j-1)\lambda]N_{\text{test}}}{N_{\text{test}}} \sum_{t \in \Pi^{(j,l)}} Y_t + \{N_{\text{total}} - [(j-1)\lambda]N_{\text{test}}\}\nu\right]$$

$$= [(\lambda^2 + \lambda) - (2\lambda - 1)]\mathsf{J}N_{\text{test}} - \sum_{j=1}^{\mathsf{J}} \frac{N_{\text{total}}}{N_{\text{test}}} \sum_{t \in \Pi^{(j,l)}} Y_t + \sum_{j=1}^{\mathsf{J}} \frac{[(j-1)\lambda]N_{\text{test}}}{N_{\text{test}}} \sum_{t \in \Pi^{(j,l)}} Y_t - \sum_{j=1}^{\mathsf{J}} N_{\text{total}}\nu + \sum_{j=1}^{\mathsf{J}} [(j-1)\lambda]N_{\text{test}}\nu$$

$$\geqslant (\lambda^2 - \lambda + 1)\mathsf{J}N_{\text{test}} - \frac{N_{\text{total}}}{N_{\text{test}}} \sum_{j=1}^{\mathsf{J}} \sum_{t \in \Pi^{(j,l)}} Y_t - \sum_{j=1}^{\mathsf{J}} N_{\text{total}}\nu$$

$$= (\lambda^2 - \lambda + 1)\mathsf{J}N_{\text{test}} - \frac{N_{\text{total}}}{N_{\text{test}}}\left(\lambda \mathsf{J}N_{\text{test}} - N_{\text{pass}}\right) - \mathsf{J}N_{\text{total}}\nu$$

$$= (\lambda^2 - \lambda + 1)\mathsf{J}N_{\text{test}} - (\lambda^2 + \lambda)\mathsf{J}(\lambda \mathsf{J}N_{\text{test}} - N_{\text{pass}}) - (\lambda^2 + \lambda)\mathsf{J}^2\nu N_{\text{test}}$$

$$= \left[(\lambda^2 - \lambda + 1)\mathsf{J} - (\lambda^2 + \lambda)\lambda \mathsf{J}^2 + (\lambda^2 + \lambda)\mathsf{J}\frac{N_{\text{pass}}}{N_{\text{test}}} - (\lambda^2 + \lambda)\mathsf{J}^2\nu\right]N_{\text{test}}, \quad \text{(C4)}$$

which gives the fraction of "good" remaining copies as

$$\frac{\mathsf{k}}{\mathsf{N}} \geqslant \frac{\left[(\lambda^2 - \lambda + 1)\mathsf{J} - (\lambda^2 + \lambda)\lambda \mathsf{J}^2 + (\lambda^2 + \lambda)\mathsf{J}\frac{N_{\text{pass}}}{N_{\text{test}}} - (\lambda^2 + \lambda)\mathsf{J}^2\nu\right]N_{\text{test}}}{\lambda^2 \mathsf{J}N_{\text{test}}}$$

$$= 1 - \left(\frac{1}{\lambda} - \frac{1}{\lambda^2}\right) - \left(\frac{\lambda^3 + \lambda^2}{\lambda^2}\right)\mathsf{J} + \left(1 + \frac{1}{\lambda}\right)\frac{N_{\text{pass}}}{N_{\text{test}}} - \left(1 + \frac{1}{\lambda}\right)\mathsf{J}\nu$$

$$= 1 - \left(\frac{1}{\lambda} - \frac{1}{\lambda^2}\right) - \left(1 + \frac{1}{\lambda}\right)\left[\frac{\sqrt{c}}{\mathsf{J}} + \lambda \mathsf{J} - \frac{N_{\text{pass}}}{N_{\text{test}}}\right]. \quad \text{(C5)}$$

Recall that the fidelity $F(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{avg}) \geqslant \frac{\mathsf{k}}{\mathsf{N}}$, and so we have

$$F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}}\right) \geqslant 1 - \left(\frac{1}{\lambda} - \frac{1}{\lambda^2}\right) - \left(1 + \frac{1}{\lambda}\right)\left[\frac{\sqrt{c}}{\mathsf{J}} + \lambda \mathsf{J} - \frac{N_{\text{pass}}}{N_{\text{test}}}\right]. \quad \text{(C6)}$$

Let us now calculate q_j^l. We get

$$
\begin{aligned}
q_j^l &= 1 - \exp\left[-\frac{2\nu^2 \mathcal{L}\mathcal{R}^2}{(\mathcal{L}+\mathcal{R})(\mathcal{R}+1)} \right] \\
&= 1 - \exp\left[-2\nu^2 \frac{\{N_{\text{total}} - [(j-1)\lambda + l]N_{\text{test}}\}N_{\text{test}}^2}{\{N_{\text{total}} - [(j-1)\lambda + l]N_{\text{test}} + N_{\text{test}}\}(N_{\text{test}}+1)} \right] \\
&= 1 - \exp\left[-2\nu^2 N_{\text{test}} \frac{1}{\frac{N_{\text{total}} - [(j-1)\lambda + l]N_{\text{test}} + N_{\text{test}}}{N_{\text{total}} - [(j-1)\lambda + l]N_{\text{test}}}} \frac{1}{\frac{N_{\text{test}}+1}{N_{\text{test}}}} \right] \\
&= 1 - \exp\left[-2\nu^2 N_{\text{test}} \frac{1}{1 + \frac{N_{\text{test}}}{N_{\text{total}} - [(j-1)\lambda + l]N_{\text{test}}}} \frac{1}{1 + \frac{1}{N_{\text{test}}}} \right] \\
&= 1 - \exp\left[-2\nu^2 N_{\text{test}} \frac{1}{1 + \frac{1}{\lambda^2\mathsf{J} + \lambda\mathsf{J} - \lambda j + \lambda - l}} \frac{1}{1 + \frac{1}{N_{\text{test}}}} \right].
\end{aligned}
\tag{C7}
$$

Setting $j = \mathsf{J}$, $l = \lambda$, we get

$$
q_{\mathsf{J}} = 1 - \exp\left[-2\nu^2 N_{\text{test}} \frac{1}{1 + \frac{1}{\lambda^2\mathsf{J}}} \frac{1}{1 + \frac{1}{N_{\text{test}}}} \right]. \tag{C8}
$$

Noting that $\lambda \geqslant 1$, $\mathsf{J} \geqslant 2$, $N_{\text{test}} \geqslant 1$, we get the probability that there are k good copies out of the remaining to be at least

$$
q_{\mathsf{J}} \geqslant 1 - \exp\left[-\frac{2}{3}\nu^2 N_{test} \right] = 1 - \mathsf{J}^{-\frac{2cm}{3}}. \tag{C9}
$$

We now calculate the probability that the above occurs, i.e., that for each stabilizer test $\mathcal{S}_j$, one or more of the Verifiers are honest, and that when they are, the condition on the left-hand side of Eq. (C3) holds, leading to Eq. (C6). For a given $\mathcal{S}_j$, this probability is given by

$$
1 - \sum_{x=0}^{\lambda} \left(1 - \frac{|H|}{n}\right)^x \left(\frac{|H|}{n}\right)^{\lambda-x} \left(1 - q_j^{l_{\max}}\right)^{\lambda-x}, \tag{C10}
$$

where $q_j^{l_{\max}}$ is the maximum of q_j^l over all l. From Eq. (C7), we see that $q_j^l \geqslant q_{\mathsf{J}}$. Taking this for all $\mathcal{S}_j$, we get the probability that Eq. (C6) holds to be

$$
\begin{aligned}
&\prod_{j=1}^{\mathsf{J}} \left[1 - \sum_{x=0}^{\lambda} \left(1 - \frac{|H|}{n}\right)^x \left(\frac{|H|}{n}\right)^{\lambda-x} \left(1 - q_j^{l_{\max}}\right)^{\lambda-x} \right] \\
&\geqslant \left[1 - \sum_{x=0}^{\lambda} \left(1 - \frac{|H|}{n}\right)^x \left(\frac{|H|}{n}\right)^{\lambda-x} (1 - q_{\mathsf{J}})^{\lambda-x} \right]^{\mathsf{J}} \\
&\geqslant \left[1 - \sum_{x=0}^{\lambda} \left(1 - \frac{|H|}{n}\right)^x \left(\frac{|H|}{n}\mathsf{J}^{-\frac{2cm}{3}}\right)^{\lambda-x} \right]^{\mathsf{J}}. \tag{C11}
\end{aligned}
$$

∎

APPENDIX D: ROBUSTNESS

When considering the robustness of our protocols, one is interested in how the security and probability of accept depend on the noise that is introduced (e.g., as in [20,36]).

For example, if we satisfy the condition in step 4 of Protocols I and II, i.e., we have

$$
N_{\text{pass}} \equiv \sum_{j=1}^{\mathsf{J}} N_{\text{pass},j} \geqslant \lambda \mathsf{J} N_{\text{test}} - \frac{N_{\text{test}}}{2\mathsf{J}}, \tag{D1}
$$

then Theorems 1, 2, and 3 give fidelity

$$
F\left(\rho_H^{|\mathcal{G}\rangle}, \rho_H^{\text{avg}}\right) \geqslant 1 - \left(\frac{1}{\lambda} - \frac{1}{\lambda^2}\right) - \left(1 + \frac{1}{\lambda}\right)\left[\frac{2\sqrt{c}+1}{2\mathsf{J}}\right], \tag{D2}
$$

where we take $\lambda = 1$ for the cases in Theorems 1 and 2, $\mathsf{J} = 2^n$ for the general case (Theorems 1 and 3), and $\mathsf{J} = n$ when generator tests are enough (Theorems 2 and 3).

Following [20], let us take the example of the following noisy state being provided by the source

$$
\rho = \sigma^{\otimes N_{\text{total}}}, \tag{D3}
$$

where $\sigma = (1 - \epsilon)|G\rangle\langle G| + \epsilon\eta$, for some noise state η and noise parameter ϵ. Then, the probability of the state being used for an application (step 4) is bounded by

$$
p_{\text{app}} \geqslant \sum_{k=1}^{N_{\text{test}}/2\mathsf{J}} \binom{\lambda\mathsf{J}N_{\text{test}}}{k} (1 - \epsilon)^{\lambda\mathsf{J}N_{\text{test}}-k}\epsilon^k, \tag{D4}
$$

which goes to one with n when $\epsilon < O(\frac{1}{\lambda\mathsf{J}N_{\text{test}}})$. This has the same dependency on the number of tests as [20] when $\lambda = 1$. The cost of the symmetric version scales only linearly with λ; however, the cost with the number of parties for the general graph state is exponentially higher once more. Thus, for the general case the scheme loses out on robustness, but this is recovered for cases such as those in Theorem 2 where the generator tests suffice.

[1] M. A. Rosenberry and T. E. Chupp, A One-Way Quantum Computer, Phys. Rev. Lett. **86**, 22 (2001).

[2] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind quantum computation, Phys. Rev. A **96**, 012303 (2017).

[3] E. Kashefi and A. Pappa, Multiparty delegated quantum computing, Cryptography **1**, 12 (2017).

[4] D. Gottesman, Stabilizer codes and quantum error correction, Ph.D. thesis, California Institute of Technology, 1997.

[5] B. A. Bell, M. S. Tame, D. Markham, W. J. Wadsworth, and J. G. Rarity, Experimental demonstration of a graph state quantum error-correction code, Nat. Commun. **5**, 3658 (2014).

[6] D. Markham and B. C. Sanders, Graph states for quantum secret sharing, Phys. Rev. A **78**, 042309 (2008).

[7] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, Anonymity for Practical Quantum Networks, Phys. Rev. Lett. **122**, 240501 (2019).

[8] G. Tóth and I. Apellaniz, Quantum metrology from a quantum information science perspective, J. Phys. A: Math. Theor. **47**, 424006 (2014).

[9] N. Friis, D. Orsucci, M. Skotiniotis, P. Sekatski, V. Dunjko, H. J. Briegel, and W. Dür, Flexible resources for quantum metrology, New J. Phys. **19**, 063044 (2017).

[10] N. Shettell and D. Markham, Graph States as a Resource for Quantum Metrology, Phys. Rev. Lett. **124**, 110502 (2020).

[11] M. Hein, J. Eisert, and H. J. Briegel, Multiparty entanglement in graph states, Phys. Rev. A **69**, 062311 (2004).

[12] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. van den Nest, and H. J. Briegel, Entanglement in graph states and its applications, in *Proceedings of the International School of Physics "Enrico Fermi"*, Quantum Computers, Algorithms and Chaos, Vol. 162 (2006), arXiv:quant-ph/0602096.

[13] D. Markham, Quantum lego: Graph states for quantum computing and information processing, ERCIM News **112**, 19 (2018).

[14] 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).

[15] G. M. D'Ariano, M. G. Paris, and M. F. Sacchi, Quantum tomography, Adv. Imaging Electron Phys. **128**, 205 (2003).

[16] B. Jungnitsch, T. Moroder, and O. Gühne, Entanglement witnesses for graph states: General theory and examples, Phys. Rev. A **84**, 032310 (2011).

[17] D. Markham and A. Krause, A simple protocol for certifying graph states and applications in quantum networks, Cryptography **4**, 3 (2020).

[18] M. Hayashi and T. Morimae, Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing, Phys. Rev. Lett. **115**, 220502 (2015).

[19] Y. Takeuchi and T. Morimae, Verification of Many-Qubit States, Phys. Rev. X **8**, 021060 (2018).

[20] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, Resource-efficient verification of quantum computing using Serfling's bound, npj Quantum Inf. **5**, 27 (2019).

[21] H. Zhu and M. Hayashi, Efficient Verification of Pure Quantum States in the Adversarial Scenario, Phys. Rev. Lett. **123**, 260504 (2019).

[22] M. McKague, Self-testing graph states, in *Theory of Quantum Computation, Communication, and Cryptography, TQC 2011, Lecture Notes in Computer Science*, edited by D. Bacon, M. Martin-Delgado, and M. Roetteler (Springer, Berlin, 2011), Vol. 6745, pp. 104–120.

[23] J. Bermejo-Vega, D. Hangleiter, M. Schwarz, R. Raussendorf, and J. Eisert, Architectures for Quantum Simulation Showing a Quantum Speedup, Phys. Rev. X **8**, 021010 (2018).

[24] B. A. Bell, D. Markham, D. A. Herrera-Marti, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, Experimental demonstration of graph state quantum secret sharing, Nat. Commun. **5**, 5480 (2014).

[25] C. Crépeau, D. Gottesman, and A. Smith, Secure multi-party quantum computation, *Proceedings of the 34th Annual ACM Symposium on the Theory of Computing* (ACM, New York, 2002), pp. 643–652.

[26] M. Ben-Or, C. Crepeau, D. Gottesman, A. Smith, and A. Hassidim, Secure multiparty quantum computation with (only) a strict honest majority, *Proceedings of the 47th Annual IEEE Symposium on the Foundations of Computer Science* (IEEE, Piscataway, NJ, 2006), pp. 249–260.

[27] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, Multipartite Entanglement Verification Resistant against Dishonest Parties, Phys. Rev. Lett. **108**, 260502 (2012).

[28] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. Rarity, and M. S. Tame, Experimental verification of multipartite entanglement in quantum networks, Nat. Commun. **7**, 13251 (2016).

[29] R. Yehia, E. Diamanti, and I. Kerenidis, Composable security for multipartite entanglement verification, Phys. Rev. A **103**, 052609 (2021).

[30] R. Raussendorf, D. E. Browne, and H. J. Briegel, Measurement-based quantum computation on cluster states, Phys. Rev. A **68**, 022312 (2003).

[31] D. Markham and A. Marin, Practical sharing of quantum secrets over untrusted channels, in *International Conference on Information Theoretic Security* (Springer, Berlin, 2015), pp. 1–14.

[32] H. Zhu and M. Hayashi, Efficient verification of hypergraph states, Phys. Rev. Applied **12**, 054047 (2019).

[33] S. Pallister, N. Linden, and A. Montanaro, Optimal Verification of Entangled States with Local Measurements, Phys. Rev. Lett. **120**, 170502 (2018).

[34] A. Uhlmann, The 'transition probability' in the state space of a *-algebra, Rep. Math. Phys. **9**, 273 (1976).

[35] D. Chaum, C. Crépeau, and I. Damgard, Multiparty unconditionally secure protocols, in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing* (ACM, New York, 1988), pp. 11–19.

[36] A. Unnikrishnan and D. Markham, Authenticated teleportation and verification in a noisy network, Phys. Rev. A **102**, 042401 (2020).

[37] M. Hayashi and M. Hajdušek, Self-guaranteed measurement-based quantum computation, Phys. Rev. A **97**, 052308 (2018).

[38] Z. Huang, C. Macchiavello, and L. Maccone, Cryptographic quantum metrology, Phys. Rev. A **99**, 022314 (2019).

[39] P. Yin, Y. Takeuchi, W.-H. Zhang, Z.-Q. Yin, Y. Matsuzaki, X.-X. Peng, X.-Y. Xu, J.-S. Xu, J.-S. Tang, Z.-Q. Zhou, *et al.*, Experimental Demonstration of Secure Quantum Remote Sensing, Phys. Rev. Applied **14**, 014065 (2020).

[40] P. Komar, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, A quantum network of clocks, Nat. Phys. **10**, 582 (2014).

[41] N. Shettell, E. Kashefi, and D. Markham, A cryptographic approach to quantum metrology, Phys. Rev. A **105**, L010401 (2022).

[42] A. Marin and D. Markham, On the equivalence between sharing quantum and classical secrets, Phys. Rev. A **88**, 042332 (2013).

[43] R. J. Serfling, Probability inequalities for the sum in sampling without replacement, Ann. Statistics **2**, 39 (1974).

[44] M. Christandl and S. Wehner, Quantum anonymous transmissions, in *Advances in Cryptology-ASIACRYPT 2005, Lecture Notes in Computer Science*, edited by B. Roy (Springer, Berlin, 2005), Vol. 3788, pp. 217–235.

[45] M. Hillery, V. Buzek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[46] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Perfect Quantum Error Correcting Code, Phys. Rev. Lett. **77**, 198 (1996).

[47] D. Aharonov, A. Ambainis, J. Kempe, and U. Vazirani, Quantum walks on graphs, in *Proceedings of the 33rd Annual ACM Symposium on the Theory of Computing* (ACM, New York, 2001), pp. 50–59.