Certification of a functionality in a quantum network stage

Lipinska, Victoria; Thinh, Le Phuc; Ribeiro, Jérémy; Wehner, Stephanie

DOI
10.1088/2058-9565/ab8c51

Publication date
2020

Document Version
Final published version

Published in
Quantum Science and Technology

Quantum Science and Technology

PAPER • **OPEN ACCESS**

Certification of a functionality in a quantum network stage

To cite this article: Victoria Lipinska *et al* 2020 *Quantum Sci. Technol.* **5** 035008

Quantum Science and Technology

OPEN ACCESS

RECEIVED
25 October 2019

REVISED
24 February 2020

ACCEPTED FOR PUBLICATION
23 April 2020

PUBLISHED
28 May 2020

PAPER

Certification of a functionality in a quantum network stage

Victoria Lipinska[1,2,4], **Lê Phuc Thinh**[1,3], **Jérémy Ribeiro**[1,2] **and Stephanie Wehner**[1,2]

[1] QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands
[2] Kavli Institute of Nanoscience, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands
[3] Institut für Theoretische Physik, Leibniz Universität Hannover, Appelstr. 2, D-30167 Hannover, Germany
[4] The author to whom any correspondence should be addressed.

E-mail: v.lipinska@tudelft.nl

Keywords: quantum network, quantum internet, certification, quantum communication, teleportation, interactive proof, estimation

Abstract

We consider testing the ability of quantum network nodes to execute multi-round quantum protocols. Specifically, we examine protocols in which the nodes are capable of performing quantum gates, storing qubits and exchanging said qubits over the network a certain number of times. We propose a simple ping-pong test, which provides a certificate for the capability of the nodes to run certain multi-round protocols. We first show that in the noise-free regime the only way the nodes can pass the test is if they do indeed possess the desired capabilities. We then proceed to consider the case where operations are noisy, and provide an initial analysis showing how our test can be used to estimate parameters that allow us to draw conclusions about the actual performance of such protocols on the tested nodes. Finally, we investigate the tightness of this analysis using example cases in a numerical simulation.

1. Introduction

Quantum communication allows us to solve tasks that are impossible to achieve using classical communication alone. The most well known example of such a task is quantum key distribution (QKD) [1, 2], but many more application protocols are already known (see e.g. [3]). Such application protocols run on the end nodes of a quantum network. These may range from simple photonic devices capable of preparing and measuring qubits, to sophisticated quantum processors. Recently, stages of development for a quantum internet were identified [3], where each stage is distinguished by a specific functionality that is offered to a user wishing to execute quantum network applications. Higher stages bring an increase of functionality—and thus a richer set of possible application protocols—at the expense of increased experimental difficulty.

Given such stages of development, one can ask whether there exists an efficient test to certify that a network offers the capabilities of a specific stage, and with what quality parameters. Here, we will examine this question with a focus on a specific set of protocols in the stage called a *quantum memory network* [3]:

> "For any two end nodes A and B the network allows the execution entanglement generation and the following additional tasks in any order: (i) preparation of a single-qubit ancilla state $|\psi\rangle$ by end node A or B, (ii) measurements of any subset of the qubits at node A or B, (iii) application of an arbitrary unitary gate G at node A or B. (iv) Storage of the qubits for a minimum time $k \cdot (\ell_z + \tau)$, where τ is defined as the time that is required to generate one Einstein–Podolsky–Rosen (EPR) pair and send a classical message from node A to B maximized over all pairs of nodes, ℓ_z is the time that it takes for the execution of a depth z quantum circuit at the end node."

Note that to realize useful application protocols, the storage time τ needs to be understood as the communication time in the network. In particular, the nodes that are far apart must exhibit longer storage capabilities to achieve this stage of development. Moreover, the stage is only attained if *any* two nodes in the

network can realize the functionality, even those that are farthest apart. Therefore, time τ can be thought of as the maximum time which takes any two nodes to communicate.

To certify that a quantum network achieves a functionality defined by this stage of development, we will consider a set of protocols which pass a qubit state $|\psi\rangle$ a number k of times between the nodes A and B, apply the gates and measure at the end. We will choose the testing nodes A and B to be farthest apart in the network.

Many existing tests are known that can be used to estimate whether the operations above can each be performed individually with high accuracy. Examples include quantum state [4] and process tomography [5], gate set tomography [6, 7], randomized benchmarking [8–10] or capacity estimation to verify the quality of qubit transmission [11]. The concept of self-testing even allows such estimates to be made with only partial trust in the devices (so called device-independent setting) [12, 13]. Having estimated the quality of each individual operation with metrics such as the diamond distance, it is straightforward to derive an overall estimate on how well protocols in this stage may be executed [3]. Yet, running many individual tests is rather inefficient, and one may wonder whether there might exist an integrated test that instills confidence that we are capable of performing protocols up to a certain number of rounds using the quantum memory network.

Another approach to testing quantum devices comes from the literature of (interactive) proof systems where a verifier interacts with one or more provers, who are trying to convince the verifier that a certain assertion is true, or indeed that they possess certain capabilities. A well known example of such work is the question whether a classical polynomially bounded verifier can convince herself that (two non-communicating) provers holding a quantum computer do indeed have full quantum computing capabilities [14]. Restricting to only a single prover, there exists also a verification protocol under complexity theoretic assumptions [15]. This line of research is not concerned with the quality of specific operations, but rather aims to obtain a certificate of the provers' general abilities to solve certain tasks. Such tests are appealing as they measure general aptitude—for example in the domain of quantum computation the ability to execute quantum algorithms—but do not typically make specific statements such as the actual number of physical qubits involved. Consequently, such tests usually require large amount of resources to be executed.

2. Results

Here we take a first step towards finding effective tests to certify that a network has reached the quantum memory stage of development (see definition 1). We propose a test which can be interpreted from two different angles. First, we interpret it as a prover-verifier type protocol inspired by interactive proof literature, to certify that the network has certain capabilities. Second, we interpret it as a tomography-type protocol where we estimate certain properties of operations.

- **Ping-pong test**. We formulate our test in a bipartite scenario where nodes A and B exchange quantum registers according to a defined set of rules. We call our test the ping-pong game as it is executed by passing qubits back and forth between two nodes. Additionally, the nodes apply gates specified by a gate set G. An important parameter of our test is the number of times k that the nodes pass (ping-pong) the state around.
- **Prover-verifier view**. Our protocol can be viewed as a simple game that the provers (the nodes) play against the verifier with the objective of convincing the verifier that they are capable of executing any protocol in the quantum memory stage, which has a specific form. In particular, we show that the provers win the k-round ping-pong game with probability one if and only if they are capable of executing perfectly any protocol of the following form: for any possible starting state $|\psi\rangle$, each node is capable of executing one possible gate $G \in \mathsf{G}$, before sending the resulting state to the other node. The nodes continue in this form for k rounds, before measuring at the end. Moreover, in the case when the winning probability is strictly less than one, we certify that the nodes sent information about the state at least a certain number $m < k$ of times.
- **Estimation view**. In the estimation view we take on a different perspective with the objective to estimate the quality of the operations performed by the nodes, as opposed to certifying their capabilities. We use the statistics of the ping-pong test to assess a measure of the overall quality of the network. We then compare this to the quality one would expect from combining the estimates of the individual devices used in the network. What is more, we estimate the performance of k-round protocols based on our ping-pong test. In order to evaluate the accuracy of our analytical results, we compare our analytical estimate with numerical estimates for a specific example of a k-round protocol influenced by noise.

This paper is organized as follows. In section 3 we define the k-round protocols and introduce our test. Then, inspired by the interactive proof literature, in section 4 we view our test in the prover-verifier setting. In section 5 we view our test in the context of estimation.

3. Ping-pong test

3.1. Assumptions

IID. Protocol 1 (see section 3.3) implements n executions of a ping-pong procedure, each of them containing at most k rounds. In section 4 (prover-verifier view) we assume that the execution of each of these ping-pong procedures is independent of the others and identical. In particular, this means that the provers' strategy will be the same in every execution of the ping-pong procedure, i.e. their strategy is independent and identically distributed (IID) across executions. However, within one execution, the provers' strategy can involve arbitrary correlation across rounds. Furthermore, in section 5 (estimation view), we assume that every round of the ping-pong procedure is independent of the others, although does not have to be identical.

EPR pairs. The main objective in the quantum memory network stage is using quantum memory in the presence of local gates. Therefore, for simplicity, we assume that any pair of nodes can generate a perfect EPR pair between them. This assumption is strictly speaking not necessary, but merely serves as an aid in understanding our test. In section 5.5 we show how to remove this assumption and how the noise associated with an EPR pair can be absorbed into the noise of the quantum memory.

State preparation and measurement. For the same reasons as above, we also assume that any node can perfectly prepare a local qubit state and perfectly measure at the end of a protocol. In section 5.5 we also discuss how to relax this assumption.

Hilbert space dimension. For the sake of clarity, throughout the rest of the manuscript we will assume that protocols run on a single qubit. We remark that the results we present generalize for any number Q of qubits (for details see appendix G).

Device stability. In the estimation view section 5 (in particular in theorem 6) we assume that after the devices were tested with the ping-pong test, their behavior does not change. That is, the devices used during the test and in a k-round protocol are identical. Note that this can be understood as a consequence of the above IID assumption for the estimation view.

3.2. k-round protocols

We start with formally describing k-round protocols. A bipartite k-round protocol between any two nodes A and B consists of the following consecutive operations:

(a) Local preparation PREP of a perfect qubit state $|\psi\rangle$ by node A.

(b) Sending deterministically the local qubit from node A to node B and vice versa, using a quantum channel $\mathcal{E}_{A\to B}$. Note that the time t_{send} it takes to send a qubit (or a classical bit) from node A to B is upper-bounded by the distance between them and the transmission speed for the qubit carrier. For example, for optical qubits the transmission speed can be understood as the speed of photons in a fiber [3].

(c) Storing the local qubit by nodes A or B, denoted by M_A and M_B respectively. Storage of the qubit takes time t_M.

(d) Applying an arbitrary local operation by a node on the local qubit. We describe this operation by a gate $G_A \in \mathsf{G}$ and $G_B \in \mathsf{G}$, where G is an arbitrary set of gates, for example the single-qubit Clifford gates. Executing a circuit of depth z takes time ℓ_z.

(e) Perfect local measurement of the local qubit at the end of the protocol. The measurements are specified by operators Π_A and Π_B for nodes A and B respectively.

Steps (b)–(d) are performed in rounds $j = 1, \ldots, k$ a total number of k times. We call k the depth of the protocol. Each round takes time $\Delta t = t_{\text{send}} + t_M + \ell_z$, so that $t_{j+1} - t_j = \Delta t$, for all j. Without loss of generality we assume here that the protocols always start at node A. Note that the parity of j indicates at which node the single qubit is located, i.e., for odd j the qubit is held (sent) by A and for even j—by B. Therefore, we denote the local operations performed by A or B at a jth round by simply putting M_j, G_j. In

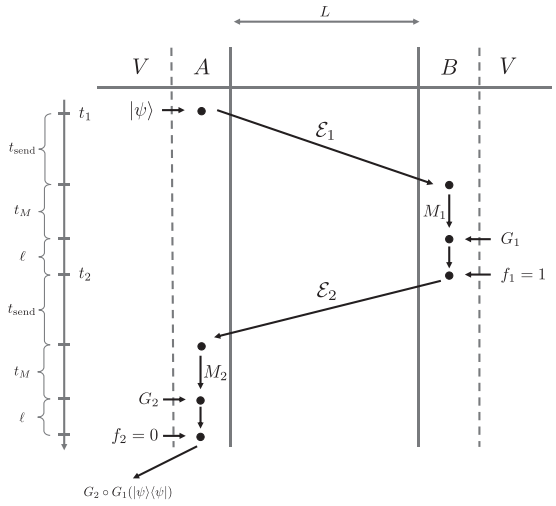

Figure 1. A schematic illustrating a single execution of depth $\kappa = 2$ of the ping-pong test, test 1.

particular, in this notation $\mathcal{E}_j$ means that a qubit is sent by A and received by B for odd j ($\mathcal{E}_j \equiv \mathcal{E}_{A_j \to B_j}$), and vice-versa for even j.

Definition 1 (k-round protocols). We define a k-round protocol as a map of the form $\Pi \circ \mathcal{P}^k \circ \text{Prep}$, where:

- PREP is a preparation of a local qubit $|\psi\rangle$ (step (a)).
- $\mathcal{P}^k$ is a map describing k rounds of local operations—memories M_j and gates G_j, as well as sending a qubit between A and B (steps (b)–(d)),

$$\mathcal{P}^k = \bigcirc_{j=1}^{k} G_j \circ M_j \circ \mathcal{E}_j. \tag{1}$$

- Π is a local measurement of all the local qubits (step (e)). Note that depending on the parity of k the measurement is performed either on A's or B's side.

3.3. Test

In this section we describe our ping-pong test. The test is a simple instance of a k-round protocol as in definition 1. As we will see in next sections, passing the test will allow us to draw conclusion about the whole class of k-round protocols.

Since our test will be later on viewed from two different angles, we introduce a node V which will interact with the nodes A and B. In the prover-verifier view, section 4, the node V will act as a verifier. Whereas, in the estimation view, section 5, the nodes A and B can take up the role of V. We choose the testing nodes A and B to be farthest apart in the network. For those nodes it is the hardest to fulfill the test, since they must account for the longest communication delays.

3.3.1. General ping-pong test

In our test, the task of the nodes is to send ('ping-pong') an unknown state an unknown number of times and at every ping-pong *round* apply a quantum operation given by V, see figure 1. Additionally, at every round V gives the nodes a challenge denoted by f—either to output the quantum state or continue the ping-pong. At the end of each *execution* of the test, $i = 1, \ldots, n$, the nodes output a state. V measures this output and produces a single classical bit v^i: 1 means 'accept' and 0 means 'reject', see test 1. As stated before, we assume that the nodes' operations are independent and identical across executions i of the test. This implies that v^i are independent and identically distributed (IID) random variables. We define a winning rate in such a game as the ratio of wins to the total number of executions:

$$R = \frac{1}{n}\sum_{i=1}^{n} v^i. \tag{2}$$

Test 1. General ping-pong test (k, G, $\mathcal{X}$).

Fix maximum depth k, gate set G and set of states $\mathcal{X}$. Fix a total number of executions n.

for $i = 1, \ldots, n$ **do**
  V chooses depth κ uniformly at random and constructs a challenge string $\vec{f}_\kappa = 1 \cdots 110$ of length κ
  V samples independently κ gates from the set G and creates a sequence $\vec{g}_\kappa = G_1 \cdots G_\kappa$
  V samples a state $|\psi\rangle \in \mathcal{X}$ and distributes it to A ▷ $t_1 = 0$
  for $j = 1, \ldots, \kappa$ **do**
    if j odd **then**
      A sends $|\psi\rangle$ to B using $\mathcal{E}_j$ ▷ t_j
      B stores the received state in memory M_j ▷ $t_j + t_{\text{send}}$
      V gives a classical description of G_j to B ▷ $t_j + t_{\text{send}} + t_M$
      B applies G_j to the state in the memory
      V distributes a challenge bit $f_j \in \{0, 1\}$ to B according to the string $\vec{f}_\kappa$ ▷ $t_j + t_{\text{send}} + t_M + \ell$
      if $f_j = 1$ **then**
        $j = j + 1$
        continue
      else
        B outputs his state
        V measures $\{\Pi_\kappa^{✓} = \bigcirc_{j=1}^{\kappa} G_j(|\psi\rangle\langle\psi|), \Pi_\kappa^{✗} = \mathbb{1} - \bigcirc_{j=1}^{\kappa} G_j(|\psi\rangle\langle\psi|)\}$
        V decides on the value v^i ('0' accept, '1' reject)
        break
    else if j even **then**
      B sends $|\psi\rangle$ to A using $\mathcal{E}_j$ ▷ t_j
      A stores the received state in memory M_j ▷ $t_j + t_{\text{send}}$
      V gives a classical description of G_j to A ▷ $t_j + t_{\text{send}} + t_M$
      A applies G_j to the state in the memory
      V distributes a challenge bit $f_j \in \{0, 1\}$ to A according to the string $\vec{f}_\kappa$ ▷ $t_j + t_{\text{send}} + t_M + \ell$
      if $f_j = 1$ **then**
        $j = j + 1$
        continue
      else
        A outputs her state
        V measures $\{\Pi_\kappa^{✓} = \bigcirc_{j=1}^{\kappa} G_j(|\psi\rangle\langle\psi|), \Pi_\kappa^{✗} = \mathbb{1} - \bigcirc_{j=1}^{\kappa} G_j(|\psi\rangle\langle\psi|)\}$
        V decides on the value v^i ('0' accept, '1' reject)
        break

The ping-pong test of depth κ for a sequence of chosen gates $\vec{g}_\kappa = G_1, \cdots, G_\kappa$ can be associated with the following operator

$$\mathcal{S}_\kappa = \bigcirc_{j=1}^{\kappa} G_j \circ M_j \circ \mathcal{E}_j. \tag{3}$$

In a single execution of test 1, the test can succeed with a certain probability. For all executions i, we define such probability, conditioned on a specific input state $|\psi\rangle$, a fixed depth κ and a fixed sequence of gates $\vec{g}_\kappa$ as

$$p_{✓|\psi,\vec{g}_\kappa,\kappa} = \text{Tr}[\mathcal{S}_\kappa(|\psi\rangle\langle\psi|) \cdot \Pi_\kappa^{✓}] \tag{4}$$

and similarly the probability of failure, $p_{✗|\psi,\vec{g}_\kappa,\kappa} = \text{Tr}\left[\mathcal{S}_\kappa(|\psi\rangle\langle\psi|) \cdot \Pi_\kappa^{✗}\right]$. Note that $p_{✓|\psi,\vec{g}_\kappa,\kappa}$ does not depend on the execution i, since we assume that executions are IID. Here $\{\Pi_\kappa^{✓}, \Pi_\kappa^{✗}\}$ denotes the measurement performed by V at the end of each execution i. We fix the figure of merit to be the average probability $P_✓$ that the nodes succeed ($v_i = 1$) in the test.

Definition 2 (Average probability of success for test 1). The probability of success in the general ping-pong test, test 2, averaged over depths κ, strings of gates $\vec{g}_\kappa$ of length κ, and states $|\psi\rangle \in \mathcal{X}$ is defined as

$$\begin{aligned} P_✓ &= \frac{1}{n}\sum_i \frac{1}{k}\sum_\kappa \frac{1}{|\mathcal{X}|}\sum_\psi \frac{1}{|\mathsf{G}|^\kappa}\sum_{\vec{c}_\kappa} p_{✓|\psi,\vec{g}_\kappa,\kappa} \\ &= \frac{1}{k}\sum_\kappa \frac{1}{|\mathcal{X}|}\sum_\psi \frac{1}{|\mathsf{G}|^\kappa}\sum_{\vec{c}_\kappa} p_{✓|\psi,\vec{g}_\kappa,\kappa}, \end{aligned} \tag{5}$$

where the last equality holds due to the IID assumption. Here k is the maximum depth of the test, $\mathcal{X}$ is the chosen set of states and G is the chosen set of gates.

3.3.2. Teleportation-based ping-pong test

In the case when $\mathcal{X}$ is the set of all single-qubit states, the average probability of success gives us an estimate on the average fidelity of the test, see section 5. This would require sampling from $\mathcal{X}$ according to the Haar

Test 2. Teleportation-based ping-pong test $(k, \mathsf{Cliff}, \mathsf{X})$.

Fix maximum depth k, fix the gate set to Clifford set Cliff and the set of states to the set of six Pauli states X. Fix the total number of executions n.

for $i = 1, \ldots, n$ **do**
  V chooses depth κ and constructs a challenge string $\vec{f}_\kappa = 1 \cdots 110$ of length κ
  V samples independently and uniformly at random κ gates from the set Cliff and creates a sequence $\vec{c}_\kappa = C_1 \cdots C_\kappa$
  V samples independently and uniformly at random a state $|\psi\rangle \in \mathsf{X}$ and distributes it to A ▷ $t_1 = 0$
  for $j = 1, \ldots, \kappa$ **do**
    if j odd **then**
      A sends $|\psi\rangle$ to B using deterministic teleportation ▷ t_j
      B stores half of his teleportation EPR pair in memory $M_j^{\mathcal{T}}$ for time τ
      V gives a classical description of C_j to B ▷ $t_j + \tau$
      B applies C_j to the state in the memory
      V distributes a challenge bit $f_j \in \{0, 1\}$ to B according to the string $\vec{f}_\kappa$ ▷ $t_j + \tau + \ell$
      if $f_j = 1$ **then**
        Set $B = A$ and $A = B$
        continue
      else
        B outputs his state
        V measures $\{\Pi_\kappa^{\checkmark} = \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|), \Pi_\kappa^{\times} = \mathbb{1} - \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)\}$
        V decides on the value v^i ('0' reject, '1' accept)
        break
    else if j even **then**
      B sends $|\psi\rangle$ to A using deterministic teleportation ▷ t_j
      A stores half of her teleportation EPR pair in memory $M_j^{\mathcal{T}}$ for time τ
      V gives a classical description of C_j to A ▷ $t_j + \tau$
      A applies C_j to the state in the memory
      V distributes a challenge bit $f_j \in \{0, 1\}$ to A according to the string $\vec{f}_\kappa$ ▷ $t_j + \tau + \ell$
      if $f_j = 1$ **then**
        continue
      else
        A outputs her state
        V measures $\{\Pi_\kappa^{\checkmark} = \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|), \Pi_\kappa^{\times} = \mathbb{1} - \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)\}$
        V decides on the value v^i ('0' reject, '1' accept)
        break

measure in the test. However, the same can be achieved more efficiently, by using sampling from the finite set of the six Pauli states X. The reason for this is that X has a property of a 2-design, meaning that discrete uniform averaging over states (polynomials of degree 2) in X, reproduces the Haar average over the full state space. A similar observation holds for Haar sampling from a set of gates G in the case when G is a full unitary group. Then, it is enough to consider sampling from the Clifford group of single-qubit gates Cliff to reproduce the average probability of success. Note that this allows us to estimate the average fidelity of the test, even in the case when one is not able to implement the full unitary group. Lastly, we remark that any set of states and unitary gates with 2-design properties can be used in place of the Pauli states and Clifford gates. For more details on 2-design properties of the above sets see appendix D.

Therefore, we consider a more efficient version of the ping-pong test, test 2. Motivated by the above and the fact that for a quantum network quantum channels between the nodes are realized by quantum teleportation, we choose:

(a) The set of states is the set of six Pauli eigenstates, $|\psi\rangle \in \mathsf{X}$ with a uniform probability distribution $\frac{1}{|\mathsf{X}|} = \frac{1}{6}$;
(b) The set of gates is the Clifford set for a single qubit, $C_j \in \mathsf{Cliff}$ with a uniform probability distribution $\frac{1}{|\mathsf{Cliff}|}$;
(c) Sending a qubit from node A to B is done with perfect deterministic teleportation.

We describe the teleportation-based ping-pong test with a triple $(k, \mathsf{Cliff}, \mathsf{X})$. Note that in this case the quantum channel at round j, $\mathcal{E}_j$, is equivalent to applying a quantum memory $M_j^{\mathcal{T}}$ to a half of the EPR pair by one of the provers. We can put $\tau = t_M + t_{\text{send}}$, which is the time required to generate one maximally entangled state and send over a classical message from node A to B. Hence, a teleportation-based ping-pong test of depth κ for a sequence of chosen Clifford gates $\vec{c}_\kappa = C_1, \cdots, C_\kappa$ can be associated with the following operator

$$\mathcal{T}_\kappa = \bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathcal{T}}. \tag{6}$$

For detailed mathematical description of the test, we refer the reader to appendix B.

By using definition 2 with the set of Pauli states X and the set of Clifford gates Cliff, the average probability of success for the teleportation-based ping-pong, test 2, is

$$P_\checkmark = \frac{1}{k}\sum_\kappa \frac{1}{|\mathsf{X}|}\sum_\psi \frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}. \tag{7}$$

Note that in test 2 the sampling of depths, gates and states is done uniformly at random. Using the definition of the expected value and the IID assumption ($\forall i,j\, \mathbb{E}[v_i] = \mathbb{E}[v_j]$), we can write that the winning rate has the expected value $\mathbb{E}[R] = \frac{1}{k}\sum_\kappa \frac{1}{|\mathsf{X}|}\sum_\psi \frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} \cdot\ 1 + p_{\text{✗}|\psi,\vec{c}_\kappa,\kappa}\cdot 0$..

Lemma 1. *The expected value of the winning rate R in test 2, equation (2), is equal to the average probability of success $P_\checkmark$,*

$$\mathbb{E}[R] = P_\checkmark. \tag{8}$$

Corollary 1 (Finite statistics). *The probability that the winning rate R differs from the average probability of success $P_\checkmark$ by more than ϵ is exponentially small in ϵ,*

$$\Pr\left[|R - P_\checkmark| \leqslant \epsilon\right] \geqslant 1 - 2\mathrm{e}^{-2n\epsilon^2}. \tag{9}$$

Furthermore, let us set $\delta = 2\mathrm{e}^{-2n\epsilon^2}$. If one fixes confidence δ and accuracy ϵ, then the minimum number of rounds n necessary to attain these parameters is given by $n \geqslant \frac{\ln(2\delta^{-1})}{2\epsilon^2}$.

4. Prover-verifier view

In this section we interpret our test, test 2 in the prover-verifier view. Specifically, we view our test as an interactive game played between a verifier V (trusted third party), and two provers (the nodes A and B) [16]. An interactive game is a situation where provers exchange a fixed-sized quantum register with the verifier n times. The verifier is honest and wants to verify a certain statement, operating according to a defined set of rules. However, potentially dishonest provers optimize towards a strategy that causes a verifier to output 1 (accept). We further assume assume a standard scenario, where the provers agree on their strategy prior to the beginning of the test and they do not communicate to readjust it during the execution, see definition 4. In contrast to the interactive proof literature, in our framework we consider finitely many test executions and therefore, we can also make non-asymptotic statistical statements.

In this view, performing test 2 allows us to certify that the provers have capabilities to perform k-round protocols. Indeed, if the provers follow the test then they can convince the verifier that they do so and achieve a high average probability of success. On the other hand, if the provers do not follow the test they cannot achieve a high probability of success and the verifier detects this behavior with high probability. Formally, we require that the test satisfies:

- *Completeness*—if the provers are able to execute protocols that are certified by the test then they succeed in a game against the verifier, i.e. achieve a winning rate above a certain winning threshold t, $R > t$, see equation (2);
- *Soundness*—if the provers are not able to execute protocols certified by the test, then they can only achieve a winning rate $R \leqslant t$.

4.1. Sending channel

Let us now introduce a framework that formalizes what we mean by a round of a quantum communication. Whereas numerous schemes to describe local operations exist [4–10] it is not clear how to certify a round of quantum communication. To achieve this, we will assume that the provers are not honest, and might therefore employ an arbitrary strategy leading to a high probability of success. In particular, they might even try to not use a communication channel at all in some rounds of the protocol. As a consequence, we have to specify what we mean by a round of communication.

For sending classical bits one typically considers the following scenario: A chooses a random bit $b_{A_0} \in_R \{0,1\}$ at time t_0 and wishes to send it to B. We then say that the nodes used a classical channel

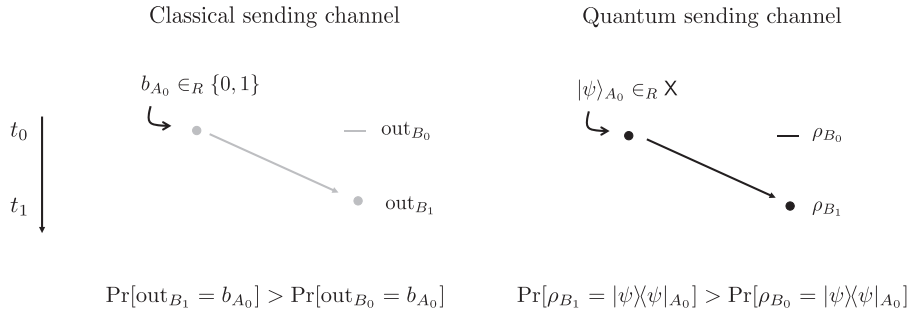

Figure 2. Informal representation of a sending channel in a classical and quantum case.

$\mathcal{E}_{\text{cl}} : A \to B$ if the probability at time t_1 that B's bit is the same as A's, is equal to 1, $\Pr[b_{B_1} = b_{A_0}] = 1$. In analogy, we could say that quantum communication through a quantum channel $\mathcal{E} : A_0 \to B_1$ occurred if at time t_0 a quantum state $|\psi\rangle_{A_0}$ was input on node A and at time t_1 it appeared on node B with probability 1, $\Pr[\rho_{B_1} = |\psi\rangle\langle\psi|_{A_0}] = 1$.

Note that in the classical case, we can prove that the channel was used to send information about the bit only for one round, by giving a uniformly random bit to A and ask B to guess it. Indeed if B guesses it with probability higher than $1/2$ then some information must have traveled from A to B. Given a single bit as an input, one cannot generalize that to many rounds with a 'ping-pong' type of protocol like test 2. This is due to the fact that before A sends information to B in the first round, she can keep a copy of the bit. However, this issue can be avoided in a quantum setting due to the no-cloning theorem [17]. Indeed, if A gets a random unknown state and B is able to output the exact same state (with probability 1), then not only did all the (quantum) information about the state traveled from A to B, but also A could not have kept any information about the state to herself (see theorem 2).

While the above definition provides a good intuition of what is going on, it becomes impractical when states do not have a unit probability of being transmitted through a channel (which in relation to our test means $t < 1$). In such a scenario, classically, we can say that the nodes used a classical channel $\mathcal{E}_{\text{cl}} : A_0 \to B_1$ if the probability of correctly identifying A's input bit on B's side increased in time, $\Pr[\text{out}_{B_1} = b_{A_0}] > \Pr[\text{out}_{B_0} = b_{A_0}]$. This implies that some information about the bit must have been transferred from A to B, see figure 2. Our definition of quantum communication is, therefore, a generalization of the above to the quantum case. We say that quantum communication $\mathcal{E} : A_0 \to B_1$ occurred if the probability of correctly outputting A's input quantum state on B's side increased in time, see definition 3.

In words, we say that a sending channel was used by the nodes if the fidelity averaged over all states, and optimized over all operations Γ that the nodes can locally do, increased from instant t_0 to t_1. Note that the above definition implies that any communication, quantum or classical, which increases fidelity of the state is considered a sending channel. As an example consider the following strategy. Node A receives an unknown state from the verifier, measures it in the standard basis and sends the measurement outcome to B. Without loss of generality, let this measurement outcome be 0. Before receiving A's measurement outcome, B has average probability $\frac{1}{2}$ of correctly passing verifier's test. However, after receiving A's measurement outcome, B can locally prepare $|0\rangle$ state which increases the average probability of correctly identifying verifier's state to $\frac{2}{3}$. Therefore, there exists a purely classical strategy which satisfies our definition. As a consequence, we say that whenever the nodes do not use a sending channel $\mathcal{E}$, no communication (quantum or classical) occurred between them.

Definition 3 (Sending channel). A channel $\mathcal{E}_{A_0 \to B_1}$ is a sending channel if there exists a CPTP map $\Omega_{A_0 \to A_0 B_0}$ such that $\forall |\psi\rangle_{A_0}$ it creates a state $\rho^{\psi}_{A_0 B_0} = \Omega(|\psi\rangle\langle\psi|_{A_0})$ and

$$\sup_{\Gamma_{B_0 B_1}} \int \mathrm{d}\psi \, \text{Tr}\left[\Gamma_{B_0 B_1}\left(\rho^{\psi}_{B_0 B_1}\right) \cdot |\psi\rangle\langle\psi|_{A_0}\right] > \sup_{\Gamma_{B_0}} \int \mathrm{d}\psi \, \text{Tr}\left[\Gamma_{B_0}\left(\rho^{\psi}_{A_0 B_0}\right) \cdot |\psi\rangle\langle\psi|_{A_0}\right], \tag{10}$$

where $\rho^{\psi}_{B_0 B_1} = \mathcal{E}_{A_0 \to B_1}(\rho^{\psi}_{A_0 B_0})$, Γ is a CPTP map which traces out additional registers of A and B and outputs a qubit state. In particular, if

$$\sup_{\Gamma_{B_0B_1}} \int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{B_0B_1}\left(\rho^{\psi}_{B_0B_1}\right)\cdot|\psi\rangle\langle\psi|_{A_0}\right] = 1 \quad \text{and} \quad \sup_{\Gamma_{B_0}} \int \mathrm{d}\psi \,\mathrm{Tr}\left[\Gamma_{B_0}\left(\rho^{\psi}_{A_0B_0}\right)\cdot|\psi\rangle\langle\psi|_{A_0}\right] = \frac{1}{2} \tag{11}$$

then we talk about an *exact sending* channel.

Definition 4 (m-cheating). Provers A and B are m-cheating if their cheating strategy uses a sending channel $\mathcal{E}$ between them at most m times. We assume that the provers choose a strategy—in which round they use a sending channel and in which they do not—prior to the beginning of the test.

4.2. Exact completeness and soundness

To investigate the power of test 2 in verifying capabilities of the network, we first consider an instructive case when $P_{\checkmark} = 1$. If the nodes are able to perfectly execute the test then they succeed with a unit probability, trivially satisfying the completeness, see theorem 1. On the other hand, if we demand that the nodes always succeed in the game, we can ask the question whether the nodes have the ability to perfectly execute protocols that have the form of test 2, i.e., whether the test is sound. We answer this question positively in theorem 2 below.

Theorem 1 (Exact completeness). *If the provers are honest and they are able to perfectly execute test 2 then they succeed $P_{\checkmark} = 1$.*

Theorem 2 (Exact soundness). *If the provers win the test with $P_{\checkmark} = 1$ then they must be able to perfectly execute test 2 and they use an exact sending channel $\mathcal{E}$ between them k times.*

Idea of the proof. To prove the theorem, we argue that $P_{\checkmark} = 1$ implies that the probability of winning $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$ for all states, all Clifford gates and all depths should be 1 (in particular, this implies that the provers are able to apply the required Clifford gates on the input state). Therefore, the average fidelity at every depth κ should be 1. That is, if at step $\kappa - 1$ A has fidelity 1 it means that the state on A is pure, and by a purifying argument, B's average fidelity at step $\kappa - 1$ must be $1/2$. At step κ B has fidelity 1, which means that whatever channel A and B have used between step $\kappa - 1$ and κ, it must be an exact sending channel (see definition 3). For more details see appendix E.1. □

Note that in practice we are only able to observe the winning rate R and, due to the finite statistics of our test, we cannot certify $P_{\checkmark} = 1$.

4.3. Completeness and soundness

Therefore, let us explore the implications of test 2, given that the winning rate $R > t$ is observed. If the provers are honest and their devices are sufficiently good, their winning rate should be larger than threshold t with high probability. More specifically, let memories and gates at every round j be described in terms of the average fidelity. Assume that the quality of memory and gates is the same at every round j, i.e. for all j, the average fidelity $\bar{\mu} = \int \mathrm{d}\psi \mathrm{Tr}[C_j \circ M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot C_j(|\psi\rangle\langle\psi|)]$. Below we show that for honest provers, a certain fidelity of operations implies a bound on the winning rate. In order to satisfy both completeness and soundness we choose the winning threshold $t > \frac{5}{6}$, since the test 2 does not lead to any conclusion in the case when $t \leqslant \frac{5}{6}$, see theorem 4. Let $h_k(\bar{\mu}) = \frac{\bar{\mu}(\bar{\mu}^k - 1)}{k(\bar{\mu} - 1)}$.

Theorem 3 (Completeness). *If provers are honest and their individual operations satisfy $\bar{\mu} \geqslant h_k^{-1}(t) + \epsilon$, then the winning rate R in test 2 is bounded by $R \geqslant t$ with probability at least $1 - \mathrm{e}^{-n\epsilon^2}$, where $t \in (\frac{5}{6}, 1]$ is a winning threshold and ϵ is given by equation (9).*

Idea of the proof. Using 2-design properties of the set of states X and the set of gates Cliff, we show that in the regime where fidelity $\bar{\mu}$ is the same for every round j, we can express the average probability of success as a sum of powers of $\bar{\mu}$. That is, $P_{\checkmark} = \frac{1}{k}\sum_{\kappa=1}^{k} \bar{\mu}^{\kappa} = \frac{\bar{\mu}(\bar{\mu}^k - 1)}{k(\bar{\mu} - 1)} = h_k(\bar{\mu})$, see appendix E.2 for details. Since we want the winning rate R to be higher than the threshold t, we invert the function h_k to obtain a bound on the fidelity of the devices $\bar{\mu}$. We plot the inverse $h_k^{-1}(t)$ in figure 3 for $t \in (\frac{5}{6}, 1]$. □

Moreover, we can ask whether the converse of the above statement is true, i.e. whether a certain winning rate $R > t$ implies something about test 2. When the provers are honest, we can reverse the completeness statement obtaining a bound on the quality of their devices. If the provers are dishonest (m-cheating) then

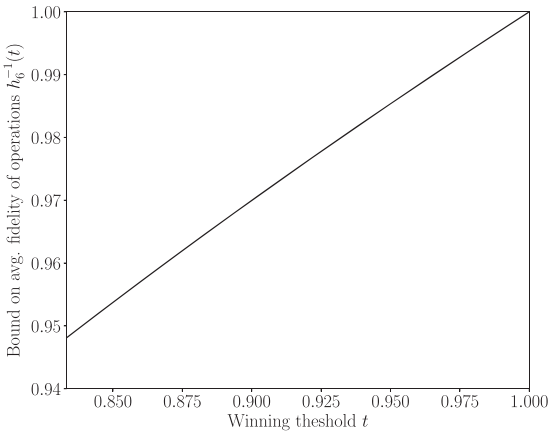

Figure 3. The average fidelity of individual operations $\bar{\mu}$ as a function of the winning threshold t (see theorem 3 completeness). The plot shows the inverse of the function h_k, i.e. $h_k^{-1}(t)$ for $k = 6$ and relevant values of t.

they do not have to exactly follow the test. However, in this case we will show that the winning rate R allows us to certify that the provers used a sending channel (definition 3) a certain number of times.

Theorem 4 (Soundness). *If the provers are m-cheating then the winning rate in test 2 is bounded by $R \leqslant \frac{1}{k}\left(m + \frac{5}{6}(k-m)\right) + \epsilon$, with probability exponentially close to 1, i.e. at least $1 - e^{-n\epsilon^2}$, where $\epsilon \in (0, 1)$.*

Idea of the proof. In the case when the provers are m-cheating they can agree on a cheating strategy which uses a quantum channel $\mathcal{E}$ between them at most m times, see definition 4. To prove soundness in this case we look at the average probability of winning for A and B at time steps $\kappa - 1$ and κ. In appendix E.2 we argue that whenever the provers use the channel $\mathcal{E}$, this probability is bounded by 1. On the other hand, whenever they do not use the channel and no communication occurred, we argue that the average probability of winning at both time steps is bounded by $\frac{5}{6}$ which is the bound provided by the approximate cloning theorem [18]. Since the nodes use the channel $\mathcal{E}$ at least m times, their overall average probability of winning $P_{\checkmark}$ is bounded by $\frac{1}{k}\left(m + \frac{5}{6}(k-m)\right)$. □

The above theorem implies that in the situation when we do not trust the nodes, the higher m we would like to certify, the higher the winning threshold should be. Indeed, for $P_{\checkmark} \geqslant t$ we obtain $m \geqslant k(6t-5)$. If we now set $t = 1 - \eta$, for some small η, then $m \geqslant k - 6k\eta$. For $m \sim k$, one should set at least $\eta = \mathcal{O}(k^{-1})$.

Remark. Note that in theorem 2 we are able to fully certify the action of the provers, even if they are not trusted. In particular, we know that they have perfectly sent the state to each other k times. On the other hand, theorem 4 only certifies the use of some quantum or classical channel regardless of its quality. In particular, in the limit where $P_{\checkmark} = 1$, theorem 4 show that $m = k$ sending channels have been used, but we cannot explicitly certify the quality of the channel. However, the exact soundness statement, theorem 2, suggests that even in the imperfect case, the test should be able to certify the quality of each individual operation used by the provers.

5. Estimation view

In this section we interpret our test in the context of estimation in order to obtain measures of confidence in the nodes' ability to perform the test. We assume that the nodes A and B are honest and follow the protocol. Specifically, we use the winning rate R in the teleportation-based ping-pong test, as a figure of merit to estimate the quality of the network. We then provide a consistency check which allows us to compare this to the quality one would expect from combining the individual devices. Furthermore, we use the statistics of the test to estimate the performance of k-round protocols.

Throughout this section we will use a tilde to denote noisy counterparts of operations, for example $\tilde{\mathcal{T}}_\kappa$ will denote a noisy realization of the κ-round teleportation-based ping-pong test $\mathcal{T}_\kappa$, test 2.

5.1. Preliminaries

In this section we introduce mathematical tools which will be useful for (i) checking whether the test is consistent when the honest nodes use devices of a certain quality, section 5.2, and (ii) drawing conclusions about the performance of k-round protocols, sections 5.3 and 5.4.

We describe the quality of individual devices with a noise model. Specifically, we assume that the individual operations used in the test, i.e. memories M_j and gates C_j, have been tested individually for each round j, to obtain an estimate on their performance. More formally, let the quality of a noisy gate $\tilde{C}_j$ at round j, be described with the average fidelity, $\bar{F}(\tilde{C}_j) = \int \mathrm{d}\psi \mathrm{Tr}\left[\tilde{C}_j(|\psi\rangle\langle\psi|) \cdot C_j(|\psi\rangle\langle\psi|)\right]$, for all $j = 1, \ldots, k$. Furthermore, let the average fidelity have an empirical estimate r_{C_j}, which is known with certain precision [19], such that

$$\Pr\left[|r_{C_j} - \bar{F}(\tilde{C}_j)| \leqslant \epsilon_{C_j}\right] \geqslant 1 - \delta_{C_j}, \tag{12}$$

where $\delta_{C_j} = 2\mathrm{e}^{-2n_{C_j}\epsilon_{C_j}^2}$. Here n_{C_j} is the number of repetitions with which the estimate r_{C_j} was obtained. Similarly, for $\tilde{M}_j^{\mathcal{T}}$ a noisy quantum memory at round j, average fidelity is $\bar{F}(\tilde{M}_j^{\mathcal{T}}) = \int \mathrm{d}\psi \mathrm{Tr}\left[\tilde{M}_j^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|)\right]$. This average fidelity has an empirical estimate $r_{M_j^{\mathcal{T}}}$ and a precision bound

$$\Pr\left[|r_{M_j^{\mathcal{T}}} - \bar{F}(\tilde{M}_j^{\mathcal{T}})| \leqslant \epsilon_{M_j^{\mathcal{T}}}\right] \geqslant 1 - \delta_{M_j^{\mathcal{T}}}, \tag{13}$$

where $\delta_{M_j^{\mathcal{T}}} = 2\mathrm{e}^{-2n_{M_j^{\mathcal{T}}}\epsilon_{M_j^{\mathcal{T}}}^2}$. Furthermore, we assume that the nodes can locally and perfectly prepare and measure a quantum state.

The teleportation-based ping-pong test, test 2, is performed the total of n times. Note that one can easily record which executions i were performed for depths κ, states ψ and strings of Clifford gates $\vec{c}_\kappa$. Then, in analogy to equation (2), we can define the winning rate for a *fixed* depth κ and string $\vec{c}_\kappa$,

$$R_{\vec{c}_\kappa,\kappa} = \frac{1}{n_{\vec{c}_\kappa,\kappa}} \sum_i v^i_{\vec{c}_\kappa,\kappa}, \tag{14}$$

where $n_{\vec{c}_\kappa,\kappa}$ is a total number of executions for fixed κ and $\vec{c}_\kappa$, and $v^i_{\vec{c}_\kappa,\kappa}$ is a corresponding random variable assuming values 0 and 1 for 'lose' and 'win' events respectively. Analogously, we can record which executions correspond to a fixed depth κ only. We define

$$R_\kappa = \frac{1}{n_\kappa} \sum_i v^i_\kappa \tag{15}$$

as the winning rate for a fixed κ. Here n_κ is a total number of executions for depth κ and v^i_κ is a corresponding random variable recording the wins in the test.

Now we will relate the above winning rates to the measures of quality of the test. Intuitively, the higher the winning rate the better the test performs and the less noise is present in the setup. In the remaining part of this section we make that statement rigorous.

Lemma 2. *Let the average fidelity of a noisy realization of test 2, $\tilde{\mathcal{T}}_\kappa$, for a fixed depth κ and a fixed string of Clifford gates $\vec{c}_\kappa$ be defined as $\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa) = \int \mathrm{d}\psi \mathrm{Tr}[\tilde{\mathcal{T}}_\kappa(|\psi\rangle\langle\psi|) \cdot \Pi^{✓}_\kappa]$, where $\mathcal{T}_\kappa$ is defined as in equation (6). The expected value of the winning rate $R_{\vec{c}_\kappa,\kappa}$ over the set of states X, is equal to the average fidelity of the test $\tilde{\mathcal{T}}_\kappa$,*

$$\mathbb{E}\left[R_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}} = \bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa). \tag{16}$$

Idea of the proof. The first step of the proof is to notice that the expected value of the variable $v^i_{\vec{c}_\kappa,\kappa}$ is the probability of success in a single round averaged over all the states in X,

$$\mathbb{E}\left[v^i_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}} = \frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}}\left(p_{✓|\psi,\vec{c}_\kappa,\kappa}\cdot 1 + p_{✗|\psi,\vec{c}_\kappa,\kappa}\cdot 0\right) = \frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}}\mathrm{Tr}\left[\tilde{\mathcal{T}}_\kappa(|\psi\rangle\langle\psi|)\cdot\Pi^{✓}_\kappa\right] \tag{17}$$

The second step is based on relating the above quantity to the average fidelity. Here the key idea is to observe that the expression under the trace contains only polynomials of degree 2 in $|\psi\rangle\langle\psi|$. Therefore one can use the 2-design properties of the set X to equate the discrete averaging over the six Pauli states to the continuous Haar averaging over the whole state space in average fidelity. The details of the proof can be found in appendix F.1.

The above lemma has a simple useful corollary, namely, that the average fidelity and the winning rate $R_{\vec{c}_\kappa,\kappa}$ can be related through the Hoeffding inequality,

$$\Pr\left[|R_{\vec{c}_\kappa,\kappa} - \bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa)| \geqslant \epsilon_{\vec{c}_\kappa,\kappa}\right] \geqslant 1 - 2\mathrm{e}^{-2n_{\vec{c}_\kappa,\kappa}\epsilon^2_{\vec{c}_\kappa,\kappa}}. \tag{18}$$

Before we make a similar connection for the rate R_κ, let us define a useful quantity.

Definition 5 (Double-averaged fidelity). Let $\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa)$ be the average fidelity of a the teleportation-based ping-pong test, test 2, defined for a fixed depth κ and a fixed sting of Clifford gates $\vec{c}_\kappa$. We define the quantity

$$\bar{\bar{F}}_\kappa(\tilde{\mathcal{T}}_\kappa) := \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_\kappa \bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa). \tag{19}$$

as double-averaged fidelity. The averaging for every gate C_j is taken according to the Haar measure.

Lemma 3. *The expected value of the winning rate R_κ in test 2, for a fixed depth κ, taken over the set of states* X *and set of Clifford gates, is equal to the double-averaged fidelity of the test $\tilde{\mathcal{T}}_\kappa$,*

$$\mathbb{E}[R_\kappa]_{\mathsf{X},\mathsf{Cliff}} = \bar{\bar{F}}_\kappa(\tilde{\mathcal{T}}_\kappa). \tag{20}$$

The intuition behind the above lemma is that discrete averaging in $\mathbb{E}[R_\kappa]_{\mathsf{X},\mathsf{Cliff}}$ over the Clifford gates is equal to the continuous averaging in the definition of $\bar{\bar{F}}_\kappa(\tilde{\mathcal{T}}_\kappa)$. This statement follows from the unitary 2-design properties of the Clifford set, see appendix F.2 for details.

Finally, the probability that the empirical data R_κ differs from double-averaged fidelity by more than ϵ_κ is bounded by the Hoeffding inequality,

$$\Pr\left[|R_\kappa - \bar{\bar{F}}_\kappa(\tilde{\mathcal{T}}_\kappa)| \leqslant \epsilon_\kappa\right] \geqslant 1 - 2\mathrm{e}^{-2n_\kappa\epsilon^2_\kappa}. \tag{21}$$

5.2. Consistency check

In the following we demonstrate how to use the winning rates defined above to check for consistency, i.e. that devices with certain fidelities were used *together* in test 2. Specifically, we provide a relation between the quality of the test in terms of $R_{\vec{c}_\kappa,\kappa}$ and what one may expect given individual devices with estimates of average fidelities $r_{M_j^\mathcal{T}}$ and r_{C_j}. Not satisfying this consistency-check relation implies that there is an internal contradiction in the reported values of individual average fidelities and observed rate $R_{\vec{c}_\kappa,\kappa}$.

Theorem 5 (Consistencycheck). *Let $r_{M_j^\mathcal{T}}$ and r_{C_j}, $j = 1,\ldots,k$, be empirical estimates of the average fidelity of all individual memories and gates respectively. Moreover let $R_{\vec{c}_\kappa,\kappa}$ be an empirical estimate of the average fidelity of the teleportation-based ping-pong test, test 2, for a fixed depth κ and a fixed string of Clifford gates $\vec{c}_\kappa$. Devices with estimates $r_{M_j^\mathcal{T}}$ and r_{C_j} were used together in the test $\tilde{\mathcal{T}}_\kappa$ if the following inequality is satisfied* [20],

$$R_{\vec{c}_\kappa,\kappa} \geqslant \frac{2\cos^2\left(\sum_{j=1}^{\kappa}\operatorname{acos}\sqrt{\frac{3r_{M_j^\mathcal{T}}-1}{2}} + \operatorname{acos}\sqrt{\frac{3r_{C_j}-1}{2}}\right) + 1}{3} - \epsilon_{\vec{c}_\kappa,\kappa} \tag{22}$$

The bound holds for any 2κ quantum channels such that $\sum_{j=1}^{\kappa}\operatorname{acos}\sqrt{\frac{3r_{M_j^\mathcal{T}}-1}{2}} + \operatorname{acos}\sqrt{\frac{3r_{C_j}-1}{2}} \leqslant \frac{\pi}{2}$, and $\epsilon_{\vec{c}_\kappa,\kappa}$ is given by equation (18).

Recall that the individual estimates are known with certain confidence. That means that the above consistency check will be satisfied with a certain probability. We state it formally in the corollary below.

Corollary 2. *Given the estimates of average fidelities for memories $r_{M_j^\mathcal{T}}$ and gates r_{C_j} are known with confidence $\epsilon_{M_j^\mathcal{T}}$ and ϵ_{C_j} respectively, the bound from theorem 5 is satisfied by noisy devices with probability at least* $1 - 2\sum_{j=1}^{\kappa}\left(\mathrm{e}^{-2n_{C_j}\epsilon^2_{C_j}} + e^{-2n_{M_j^\mathcal{T}}\epsilon^2_{M_j^\mathcal{T}}}\right)$.

Idea of the proof. The probability that the bound (22) is satisfied is equal to the unity, minus the probability that at least one of the bounds for individual devices is not satisfied. By properties of probability one arrives at the statement above, see appendix F.3 for details. □

5.3. Performance of *k*-round protocols

In this section we investigate the implications of test 2 for the performance of more general k-round protocols $\tilde{\mathcal{P}}^k$, see definition 1. We show that their performance can be bounded using the winning rate R_κ (section 5.1) in the teleportation-based ping-pong test.

To explore the performance of protocols $\tilde{\mathcal{P}}^k$ we consider the diamond distance [21], $\|\Pi \circ \tilde{\mathcal{P}}^k \circ \mathrm{Prep} - \Pi \circ \mathcal{P}^k \circ \mathrm{Prep}\|_\diamond$. However, since Prep and Π are perfect by assumption, the above diamond distance is upper-bounded by $\|\tilde{\mathcal{P}}^k - \mathcal{P}^k\|_\diamond$, which we fix to be the figure of merit in this section. It can be shown that the diamond distance is related to the average fidelity in the following way [22],

$$\|\tilde{\mathcal{P}}^k - \mathcal{P}^k\|_\diamond \leqslant 2\sqrt{6}\sqrt{\left(1 - \bar{F}_{k,\vec{g}_k}(\tilde{\mathcal{P}}^k)\right)}, \tag{23}$$

where $\bar{F}_{k,\vec{g}_k}(\tilde{\mathcal{P}}^k) = \int \mathrm{d}\psi\, \mathrm{Tr}\left[\tilde{\mathcal{P}}^k(|\psi\rangle\langle\psi|) \cdot \mathcal{P}^k(|\psi\rangle\langle\psi|)\right]$ is the average fidelity of a protocol $\tilde{\mathcal{P}}^k$ of a fixed depth k and for a fixed string of gates $\vec{g}_k$. Note that the average fidelity differs depending on the sequence of gates one chooses to apply. Therefore, to estimate the behavior of protocol $\tilde{\mathcal{P}}^k$ one would have to know fidelities $\bar{F}_{k,\vec{g}_k}(\tilde{\mathcal{P}}^k)$ for all possible gate sequences $G_1, \ldots, G_k$, which is unfeasible in practice. For this reason, it is much more convenient to use double-averaged fidelity to bound the performance of a protocol $\tilde{\mathcal{P}}^k$. We formalize this argument in the following theorem.

Theorem 6 (Performance of $k-$ round protocols). *The performance of single-qubit k-round protocols, definition 1, can be bounded in terms of an estimate for the double-averaged fidelity R_k of the k-round teleportation-based ping-pong test, test 2, in the following way*

$$\|\tilde{\mathcal{P}}^k - \mathcal{P}^k\|_\diamond \leqslant 2\sqrt{6}\sqrt{|\mathsf{Cliff}|^k\,(1 - R_k + \epsilon_k)} \tag{24}$$

where $|\mathsf{Cliff}|$ *is the size of the Clifford group for dimension* 2 *and* ϵ_k *is given by equation* (21). *The bound is satisfied with probability* $1 - \mathrm{e}^{-2n_\kappa\epsilon_\kappa^2}$.

Idea of the proof. To prove the theorem, one first needs to observe that the double-averaged fidelity, $\bar{\bar{F}}(\tilde{\mathcal{P}}^k)$, can be lower-bounded by $\bar{F}_{\vec{g}_k}(\tilde{\mathcal{P}}^k)$ minimized over all possible strings of gates $\vec{g}_\kappa$, see appendix F for details.

Moreover we have that $\bar{\bar{F}}_k(\tilde{\mathcal{P}}^k) = \bar{\bar{F}}_{\kappa=k}(\tilde{\mathcal{T}}^{\kappa=k})$. It follows from the fact that averaging over the Clifford group is equivalent to averaging over the entire unitary group, since the Clifford group forms a 2-design. Furthermore, the equality is possible, since we have put $M_j^{\mathcal{T}} \equiv M_j \circ \mathcal{E}_j$, and $M_j^{\mathcal{T}}$ encompasses operations associated with sending (in the test–teleporting) and storing the qubit. Combining the above with equations (20) and (23) yields the desired result. □

Finally, observe the above results can be straightforwardly generalized to bound the performance of protocols $\tilde{\mathcal{P}}^K$ for depth $K > k$. Since the teleportation-based ping-pong test is performed for all $1 \leqslant \kappa \leqslant k$, we can define a set S such that $\sum_{\kappa\in S}\kappa = K$. Then $\tilde{\mathcal{P}}^K = \bigcirc_{\kappa\in S}\tilde{\mathcal{P}}^\kappa$. Using the triangle inequality for the diamond distance, theorem 6 can be, therefore, rewritten as

$$\|\tilde{\mathcal{P}}^K - \mathcal{P}^K\|_\diamond \leqslant 2\sqrt{6}\sum_{\kappa\in S}\sqrt{|\mathsf{Cliff}|^\kappa\,(1 - R_\kappa + \epsilon_\kappa)}, \tag{25}$$

where ϵ_κ is given by equation (21).

5.4. Simulated results

To gain intuition on how the test performs in this section we consider a few numerical examples. First, we discuss the implications of the consistency check, theorem 5 and articulate the relation between the average fidelity of individual devices and the maximal depth of the test k. Second, we discuss the performance

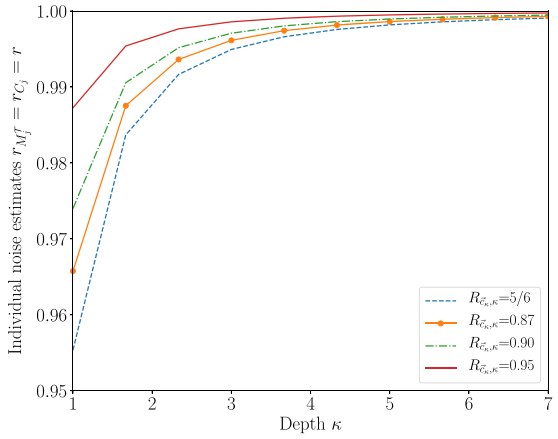

Figure 4. Minimum average fidelity r of individual operations (individual noise estimates) as a function of fixed depth κ for different winning rates $R_{\vec{c}_\kappa,\kappa}$. The plot shows the bound derived in equation (22).

of the test under common noise models, depolarizing and dephasing noise. Finally, we comment on bounding the noisy protocols $\tilde{\mathcal{P}}^k$ based on numerical results from the teleportation-based ping-pong test.

Assume a test of maximum depth $k = 2$, where we teleport a single qubit state at most two times between A and B. Moreover, for simplicity say that A and B have access to memories and gates of equal fidelities, $r_{M_j^T} = r_{C_j} = r$. Observe that the higher depth of the test κ, i.e. the more devices one is testing, the higher individual fidelities should be, see figure 4. Finally, note that the bound used for consistency check (22) was derived for a generic noise model and it was shown to be tight [20]. This means that if one does not have any additional knowledge about the noise present in the devices then the results presented here cannot be further improved.

Let us now look at two specific noise models. Namely, let us model memories and gates to be (i) single-qubit depolarizing channels, i.e. $\mathcal{D}(\rho) = p\rho + (1-p)\mathbb{1}/2$ and (ii) single-qubit dephasing channels, i.e. $\mathcal{F}(\rho) = q\rho + (1-q)(Z\rho Z^\dagger)/2$, where Z is the Pauli Z gate. Again, in these two cases let us fix the average fidelity estimate of individual devices r. Figure 5 presents the simulated behavior of the test as a function of individual estimates r in the two cases. Observe that the test performs according to intuitive expectations—if the noise is modeled as dephasing, the average fidelity of the test is higher than in the case of depolarizing noise, since the dephasing channel subjects any input state only to the Z component of the Pauli noise, whereas depolarizing channel to all X, Y and Z components. Therefore, we expect 'more' noise when the state is subjected to the depolarizing noise.

Although in our network model we assume that the state preparation is perfect, it is interesting to see the behavior of the test once imperfect states are used. Figure 5 shows a result of simulation of the test when the initial state is submitted to a small dephasing noise, such that fidelity of the input state is 0.9. Note that if one has access to the average fidelity estimate of the noisy channel acting on the initial state, then one can use it in the consistency check (22), simply treating the noise of the state as an additional channel in the protocol.

Let us also comment on the bound from theorem 6. Already for a single qubit one obtains a constant prefactor of $2\sqrt{d(d+1)} \approx 4.9$. In addition to that, bound (24) contains a factor associated with the size of the Clifford group—for a single qubit $|\mathsf{Cliff}| = 24$. If one considers protocols of maximum depth $k = 2$ then to obtain a non-trivial bound on the behavior of protocols in the class, the estimate of double-averaged fidelity must be of order $R_\kappa = 1\text{–}10^{-5}$. This puts a very high precision requirement on double-averaged fidelity and, consequently, on individual devices.

As an example consider the quantum gambling (QG) protocol [23]. In the protocol, A chooses one of the states $\{|0_z\rangle, |0_x\rangle\}$ and sends it to B. After receiving the state B stores the state and communicates classically his guess on the state sent by A. A upon receiving the classical message from B, communicates back whether B won or lost. After this round of communication B measures the state either in Z basis or X basis. Let the protocol be described with a map $\mathcal{P}_{\mathrm{QG}}$ which consists of local operations on the state (except measurement and state preparation, as before). Then $\mathcal{P}_{\mathrm{QG}}$ consists of $k = 2$ rounds of communication during which B has to store the state. Assume that in the protocol quantum memory is modeled as a depolarizing channel with fidelity $1\text{–}10^{-5}$. Then explicit evaluation of the diamond distance $\|\tilde{\mathcal{P}}_{\mathrm{QG}} - \mathcal{P}_{\mathrm{QG}}\|_\diamond$

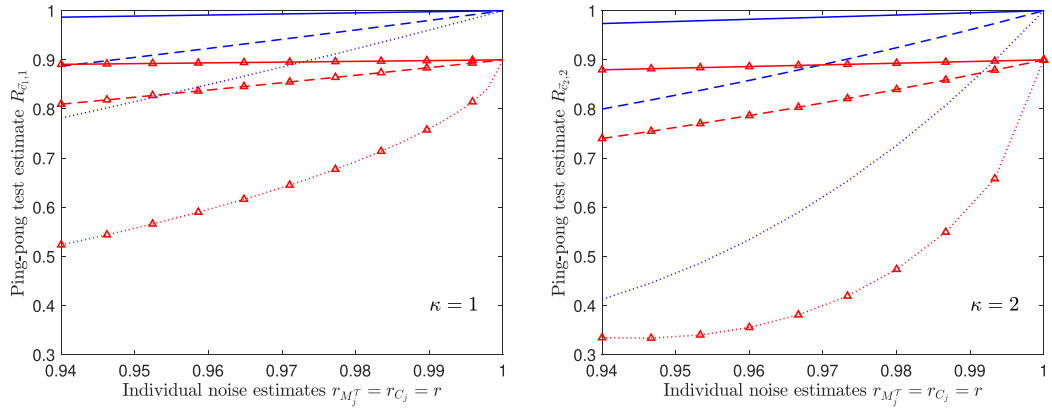

Figure 5. Average fidelity of the test as a function of the average fidelity of individual devices r, left plot for $\kappa = 1$, right plot for $\kappa = 2$. Solid lines represent simulation of the test with the dephasing channel $\mathcal{D}$, dashed lines the simulation of the test with the depolarizing channel $\mathcal{F}$, and dotted lines the value of the bound (22). No markers (blue color) correspond to the case where the input state is perfect, whereas the triangle markers (red color) to the case where the input state is dephased to initial fidelity 0.9.

yields value $6 \cdot 10^{-5}$. On the other hand if one uses a two-round test to bound the behavior of the protocol, without explicit *a priori* knowledge about the noise model of the memories then the bound from theorem 6 has the value 0.7436. However, note that in the quantum gambling protocol one does not perform any gates. Using this explicit knowledge about the protocol one could in principle tailor a ping-pong teleportation-based test without any gates. In this case, there would be no need to average over gates and therefore, the bound from theorem 6 would not carry the $|\mathsf{Cliff}|^k$ term. Consequently, the bound could be improved to value 0.0310.

5.5. More noise

In our network model we have assumed that state preparation, measurement, sending qubits as well as preparing an EPR pair can be done perfectly. In particular, this implies that in our test teleportation is carried out perfectly. However, the test can still be performed without major changes if one wishes to take into account noisy teleportation.

We consider two main noise sources arising in teleportation—noise coming from performing imperfect Bell measurement and recovery operation, and noise originating from creation of an EPR pair. In appendix C.1 we show that in a single round j of our test both of these noise types can be absorbed into the noise coming from the memory $\tilde{M}_j^T$, for all j. For the former noise source we assume a noise model where the imperfections follow the Bell measurement but precede recovery operation. For the latter noise source, we assume that noise is local for each half of the EPR pair and that it can be modeled as mixed-unitary noise. That is, each half of the EPR pair is subjected to $N(\cdot) = \sum_l p_l U_l^\dagger(\cdot)U_l$, where U_l is a unitary operation, and p_l is a probability. Then all the teleportation noise can be included in the noise of the memory and we can carry out the test as described above, i.e. by sending qubits via perfect teleportation.

Similarly to the analysis outlined in the previous paragraph, we can treat the noise of the state preparation as if it arose in the teleportation. Indeed, one can absorb the noise in the initial state similarly to the analysis in appendix C.1. Note that in figure 5 we indicate what one might expect from the test if the initial state is noisy. As for the noise in the final measurement, if we consider that the noisy measurement is described by a noise map N followed by a perfect measurement, then N can be treated as another noisy memory applied to the state before measuring. In this case, the analysis carried out in lemma 7 of appendix D still holds.

Finally, we remark that our test can be extended onto multi-qubit settings, where the number of qubits in the k-round protocol is Q. For a detailed description we refer the reader to appendix G.

6. Conclusions and outlook

In this work we considered the problem of certifying that a quantum network achieves the ability to perform a subset of protocols within a certain stage of development, i.e. a stage called quantum memory

network. We designed the first testing protocol, which certifies that nodes have the capability to control and send qubits around the network k times. We provided completeness and soundness statements for our protocol and expressed them in the interactive proof language. Moreover, in an honest implementation, we demonstrated that passing our test allows us to estimate statistical quantities about the devices used in the test and conclude about the performance of other k-round protocols in a quantum network.

An important question is how our estimate of performance for the class of multi-round protocols can be improved. Note that in our simple analysis we bound a very general class of protocols using a single test—we bound the behavior of any unitary gate in terms of behavior of a small subset of gates. Therefore, it is not surprising that there must exist a trade-off between universality of the protocols and the precision of estimating their performance. One improvement could result from designing tests for a more specific (and therefore smaller) class of protocols. Alternatively, tailoring tests using additional knowledge of the underlying noise in a quantum network could improve the bound on the performance of k-round protocols.

Furthermore, as mentioned before, our test does not certify that any universal gate can be implemented. Due to the mathematical structures of unitary designs that we used, we can only make a statement about implementability of the gates from the Clifford set or any gate set with 2-design properties. It is, therefore, an open problem how to test a quantum memory in the presence of the set powerful enough to generate any unitary operation. Such a universal set is, for example, a Clifford set extended with a T gate [24, 25].

In the following we present technical details of our work. We first provide mathematical preliminaries necessary for our further considerations in appendix A. Then, in appendix B we give a detailed mathematical description of the general ping-pong test, test 1, and the teleportation-based ping-pong test, test 2. In appendix C we justify why in the teleportation-based ping-pong test, it is possible to absorb the (possibly noisy) teleportation channel into a memory $M_j^{\mathcal{T}}$. Next, we discuss 2-design properties of sets of Pauli states and Clifford gates in appendix D. In appendix E we prove completeness and soundness statements of our test 2. Then, in appendix F we give proofs of statements discussed in the estimation view of our test. Finally, we discuss how to extend our results to Q-qubit protocols in appendix G.

Acknowledgments

We thank J Helsen, and G Murta for inspiring discussions and useful comments on this work. We also thank B Dirkse, T Coopmans, M Steudtner and K Goodenough for feedback on the manuscript. This work was supported by STW Netherlands, NWO VIDI grant, ERC Starting grant and NWO Zwaartekracht QSC.

Appendix A. Preliminaries

Communication between nodes of a quantum network can be described by quantum channels. A quantum channel can be described by a completely positive trace-preserving (CPTP) linear map $\Lambda : \mathbb{D}(\mathcal{H}) \to \mathbb{D}(\mathcal{H})$, where $\mathbb{D}(\mathcal{H})$ denotes the space of density operators acting on Hilbert space $\mathcal{H}$. In a realistic setup, quantum channels are not perfect (or ideal) and instead of applying a perfect channel Λ one applies its noisy counterpart $\tilde{\Lambda}$. If the perfect Λ is unitary, then without loss of generality, a noisy channel $\tilde{\Lambda}$ can be written as a noise map N followed by a perfect channel Λ, i.e. $\tilde{\Lambda} = \Lambda \circ N$. A sequence of n operations can be represented as a composition of n maps, $\tilde{\Lambda}_n \circ \cdots \circ \tilde{\Lambda}_1$.

One can quantify the difference between a noisy channel and its perfect implementation using the average fidelity.

Definition 6 (Average fidelity). The average fidelity of the channel $\tilde{\Lambda}$ (to Λ) is defined as

$$\bar{F}(\tilde{\Lambda}) = \int \mathrm{d}\psi \, \mathrm{Tr}\left[\tilde{\Lambda}(|\psi\rangle\langle\psi|)\, \Lambda(|\psi\rangle\langle\psi|)\right], \tag{A1}$$

where $\mathrm{d}\psi$ is the Haar measure on pure states.

Average fidelity is a quantity which can be accessed empirically and as such it is widely used as a parameter estimating the quality of a quantum channel. One cannot hope, however, to empirically average

over the continuum of all pure states. Realistically, to access average fidelity one can use the properties of so called *quantum state designs*. Intuitively, a quantum design is a probability distribution over pure states, which replicates the properties of the Haar averaging over the entire space of pure states.

Definition 7 (Projective t-design). A projective t-design is a distribution $\{q_\psi, \psi\}$ over some finite set of states such that

$$\sum_\psi q_\psi \, |\psi\rangle\langle\psi|^{\otimes t} = \int \mathrm{d}\psi \; |\psi\rangle\langle\psi|^{\otimes t}. \tag{A2}$$

An example of a projective 2-design for qubits is given by a set of six Pauli eigenstates, X chosen with equal probability $\frac{1}{6}$. A similar definition can be used when talking about averaging over the unitary group $U(d)$ of dimension d, see [26] for details.

Definition 8 (Unitary 2-design). A set $U(d)$ of unitary matrices is 2-design if for any quantum channel Λ holds that [27]

$$\frac{1}{|\mathcal{Y}|}\sum_{U_l\in\mathcal{Y}} U_l^\dagger \Lambda(U_l \rho U_l^\dagger) U_l = \int \mathrm{d}U \; U^\dagger \Lambda(U\rho U^\dagger) U \tag{A3}$$

where $\mathrm{d}U$ denotes the Haar measure on $U(d)$. An example of a 2-design for a unitary group $U(d)$ is the Clifford group $\mathsf{Cliff}(d)$ with uniform probability of each element.

Another useful figure of merit for channels is the diamond distance [21].

Definition 9 (Diamond distance). The diamond distance between two operators, $\tilde{\Lambda}$ and Λ, is defined through a distance measure on the space of density operators, maximized over all density operators ρ,

$$\|\tilde{\Lambda} - \Lambda\|_\diamond = \sup_\rho \|\tilde{\Lambda}\otimes \mathbb{1}(\rho) - \Lambda \otimes \mathbb{1}(\rho)\|_1, \tag{A4}$$

where $\|\cdot\|_1$ is the trace distance. The operational meaning behind the diamond distance definition is that it quantifies the worst-case distinguishability of any two quantum channels when one is given access to entanglement with an auxiliary system.

From the properties of the diamond distance it follows that,

$$\|\tilde{\Lambda}_N \circ \cdots \circ \tilde{\Lambda}_1 - \Lambda_N \circ \cdots \circ \Lambda_1\|_\diamond \leqslant \sum_{j=1}^N \|\tilde{\Lambda}_j - \Lambda_j\|_\diamond. \tag{A5}$$

Note that such a relation cannot be easily found for average fidelity, since, unlike the diamond distance, fidelity is not a metric.

Although the diamond distance offers a convenient theoretical description, it is not as practical as average fidelity. But, since average fidelity and diamond distance both estimate the quality of a quantum channel, there exists a relation between the two. Indeed, it can be shown CIT that

$$\|\tilde{\Lambda} - \Lambda\|_\diamond \leqslant 2\sqrt{d(d+1)}\sqrt{1 - \bar{F}(\tilde{\Lambda})}, \tag{A6}$$

where d is the dimension of the underlying quantum system.

While performing an experiment, for example estimating the average fidelity, one gathers empirical data. To compare the data with theoretical expectation one can use the Hoeffding's inequality [19]. It states that the probability of the empirical mean and its expectation differing by more than ϵ is exponentially small in n.

Lemma 4 (Hoeffding's inequality). *If $v_1, \ldots, v_n$ are independent random variables, $0 \leqslant v_i \leqslant 1$, with empirical mean defined as*

$$R = \frac{v}{n} = \frac{\sum_{i=1}^n v_i}{n}, \tag{A7}$$

then an upper bound on the probability that the mean of random variables deviates from its expected value is given by

$$\Pr[|R - \mathbb{E}[R]| \geqslant \epsilon] \leqslant 2e^{-2n\epsilon^2}. \tag{A8}$$

Lemma 5 (Choi isomorphism). *For a map $\Omega : \mathcal{H}_{S_1} \to \mathcal{H}_{S_2}$ the following identity holds:*

$$\mathrm{Tr}[|\psi\rangle\langle\psi|_{S_2}\, \Omega_{S_1\to S_2}(|\psi\rangle\langle\psi|_{S_1})] = |S_1|\mathrm{Tr}\left[|\psi\rangle\langle\psi|_{S_2} \otimes |\psi\rangle\langle\psi|_{S_1'}\, \omega^{\Gamma}_{S_2S_1'}\right], \tag{A9}$$

where $\omega^{\Gamma}_{S_2S_1'}$ is a Choi state associated with the map $\Omega_{S_1\to S_2}$ of the form $\omega^{\Gamma}_{S_2S_1'} = \Omega_{S_1\to S_2} \otimes \mathbb{1}_{S_1'}(\Phi)$, with $\Phi = \sum_{i,j} |ii\rangle\langle jj| / |S_1'|$ being the maximally entangled state. Γ denotes partial transposition of ω on the system S_1', and $|S_1|$ ($|S_1'|$) is a size of Hilbert space $\mathcal{H}_{S_1}$ ($\mathcal{H}_{S_1'}$).

Appendix B. The test—detailed description

In this section we provide a mathematical detailed description of our tests. First we consider a general case of the ping-pong test, test 1. Then we discuss the specific case of the teleportation-based ping-pong test, test 2.

B.1. General ping-pong test

We describe a general test test 1 as a CPTP map which we will denote $\mathcal{S}_\kappa$. We first consider all the registers available to the nodes. We call κ the *depth* of the test and assume that κ is a natural number upper-bounded by given k. The time for performing one round $j = 1, \ldots, \kappa$ of the protocol is equal for all the rounds, i.e. $\Delta t = t_{j+1} - t_j = t_{\mathrm{send}} + t_M + \ell$.

We will describe a *round* where node A initiates sending of the state, which implies that j is odd. However, this description is fully symmetric and for even j it is enough to interchange registers of A with registers of B. A sends the qubit $|\psi\rangle\langle\psi|_{A_j^{\mathrm{in}}}$ to node B using channel $\mathcal{E}_{A_j^{\mathrm{in}}\to B_j}$ which takes time upper-bounded by t_{send}. After time $t_{\mathrm{send}} + t_M$ the verifier chooses a gate according to distribution p_{G} and gives its classical description $|g_j\rangle\langle g_j|_{G_j}$ to B. B applies the quantum gate that corresponds to the description and that we describe with a CPTP map $G_{G_jB_j\to G_j}$. This takes time ℓ. After this, at time $t_{\mathrm{send}} + t_M + \ell$ the verifier distributes a challenge bit $|f_j\rangle\langle f_j|_{F_j}$ chosen uniformly at random (0 means 'teleport back', 1 means 'output'). Depending on the challenge, B applies $\mathrm{IN}_{F_jB_j^{\mathrm{EPR}}\to B_{j+1}^{\mathrm{in}}}$ for $f_j = 0$ and $\mathrm{OUT}_{F_jB_j\to B_j^{\mathrm{out}}}$ for $f_j = 1$.

Definition 10 (Honest round j). Round j of a general test, where provers are honest, can be described as

$$\hat{\Lambda}_{A_j^{\mathrm{in}}F_jG_j\to B_{j+1}^{\mathrm{in}}} = \mathrm{IN}_{F_jB_j^{\mathrm{EPR}}\to B_{j+1}^{\mathrm{in}}} \circ G_{G_jB_j\to B_j} \circ M_{B_j\to B_j} \circ \mathcal{E}_{A_j^{\mathrm{in}}\to B_j} \tag{B1}$$

whenever the challenge bit is 0, or

$$\hat{\Lambda}_{A_j^{\mathrm{in}}F_jG_j\to B_j^{\mathrm{out}}} = \mathrm{OUT}_{F_jB_j\to B_j^{\mathrm{out}}} \circ G_{G_jB_j\to B_j} \circ M_{B_j\to B_j} \circ \mathcal{E}_{A_j^{\mathrm{in}}\to B_j} \tag{B2}$$

whenever the challenge bit is 1.

Note that challenge bits form a string of length κ, $f_1 \ldots f_\kappa$, in registers $F_1 \ldots F_\kappa$, consisting of $\kappa - 1$ ones and a single zero bit on κ-th position. We denote such a string by $\vec{f}$, i.e. $\vec{f}_\kappa = \underbrace{1\cdots 10}_{\kappa}$. For simplicity we will use a short notation for multiple registers, e.g. $F_{[1,\kappa]} \equiv F_1 \ldots F_\kappa$. Similarly, we will denote by $\vec{g}_\kappa$ a sequence of κ gates chosen by the verifier, each of the gates chosen at the time step defined above. By $G_{[1,\kappa]} \equiv G_1 \cdots G_k$ we denote k registers for the choice of a gate.

Definition 11 The ping-pong testing protocol of depth κ for a state $|\psi\rangle\langle\psi| \in \mathcal{X}$, a sequence of gates $\vec{g}_\kappa \in \mathcal{G}^\kappa$ and a string of challenges $\vec{f}_\kappa = 1\cdots 10$ is defined as a CPTP map $\mathcal{S}_\kappa$ such that

$$\mathcal{S}_\kappa \equiv \mathcal{S}_{A_1^{\text{in}} F_{[1,\kappa]} G_{[1,\kappa]} \to B_\kappa^{\text{out}}} \left(|\psi\rangle\langle\psi|_{A_1^{\text{in}}} \otimes \left|\vec{f}_\kappa\right\rangle\left\langle\vec{f}_\kappa\right|_{F_{[1,\kappa]}} \otimes |\vec{g}_\kappa\rangle\langle\vec{g}_\kappa|_{G_{[1,\kappa]}} \right) \tag{B3}$$

$$= \hat{\Lambda}_{A_j^{\text{in}} F_j G_j \to B_j^{\text{out}}} \circ \bigcirc_{j=1}^{\kappa-1} \hat{\Lambda}_{A_j^{\text{in}} F_j G_j \to B_{j+1}^{\text{in}}} \left(|\psi\rangle\langle\psi|_{A_1^{\text{in}}} \otimes \left|\vec{f}_\kappa\right\rangle\left\langle\vec{f}_\kappa\right|_{F_{[1,\kappa]}} \otimes |\vec{g}_\kappa\rangle\langle\vec{g}_\kappa|_{G_{[1,\kappa]}} \right) \tag{B4}$$

B.2. Teleportation-based test

We now describe a single round j of the test when the quantum communication is performed with teleportation, $\mathcal{T}_\kappa$ (see test 2). Let node A initiate the teleportation, i.e. j is odd. A round j starts with placing the state to be teleported $|\psi\rangle\langle\psi|_{A_j^{\text{in}}}$ in an input register of A, A_j^{in}. Nodes generate an EPR pair between each other, $\Phi^+_{A_j^{\text{EPR}} B_j^{\text{EPR}}}$. A, using the generated pair, teleports the state $|\psi\rangle\langle\psi|_{A_j^{\text{in}}}$ to B by performing a Bell state measurement and sending a classical message $m \in M$. This action is described by a CPTP map $\mathcal{B}_{A_j^{\text{in}} A_j^{\text{EPR}} \to M}$. At the same time B applies quantum memory to his half of the EPR pair while waiting for the classical message from A to arrive, which takes time t_M. We describe the action of the memory with a CPTP map $M_{B_j^{\text{EPR}} \to B_j^{\text{EPR}}}$. Upon receiving classical message B now applies a recovery map $\mathcal{R}_{M B_j^{\text{EPR}} \to B_j^{\text{EPR}}}$ to recover the state which A teleported. Then, B applies a random gate chosen by the verifier from the set of Clifford gates $\mathsf{Cliff}(2)$. This choice is announced by the verifier with a classical register $|c_j\rangle\langle c_j|_{C_j}$. B then applies the gate to his recovered state, which we describe with a CPTP map $C_{C_j B_j^{\text{EPR}} \to B_j^{\text{EPR}}}$. This operation takes time ℓ.

Now, at time $t_M + \ell$ the verifier announces a flag in register F_j with the challenge bit, 0: teleport back, 1: output. The choice of the challenge is uniform and random. Depending on the challenge, B applies $\text{IN}_{F_j B_j^{\text{EPR}} \to B_{j+1}^{\text{in}}}$ for $f_j = 0$ and $\text{OUT}_{F_j B_j^{\text{EPR}} \to B_j^{\text{out}}}$ for $f_j = 1$. The whole round j takes time $\Delta t = t_M + \ell$.

Definition 12 (Round j of the teleportation-based test). We define a jth round of teleportation as a sequence of following maps

$$\Lambda_{A_j^{\text{in}} A_j^{\text{EPR}} B_j^{\text{EPR}} F_j C_j \to B_{j+1}^{\text{in}}} = \text{IN}_{F_j B_j^{\text{EPR}} \to B_{j+1}^{\text{in}}} \circ C_{C_j B_j^{\text{EPR}} \to B_j^{\text{EPR}}} \circ \mathcal{R}_{M B_j^{\text{EPR}} \to B_j^{\text{EPR}}} \circ M_{B_j^{\text{EPR}} \to B_j^{\text{EPR}}} \circ \mathcal{B}_{A_j^{\text{in}} A_j^{\text{EPR}} \to M} \tag{B5}$$

whenever the challenge bit is 0, or

$$\Lambda_{A_j^{\text{in}} A_j^{\text{EPR}} B_j^{\text{EPR}} F_j C_j \to B_j^{\text{out}}} = \text{OUT}_{F_j B_j^{\text{EPR}} \to B_j^{\text{out}}} \circ C_{C_j B_j^{\text{EPR}} \to B_j^{\text{EPR}}} \circ \mathcal{R}_{M B_j^{\text{EPR}} \to B_j^{\text{EPR}}} \circ M_{B_j^{\text{EPR}} \to B_j^{\text{EPR}}} \circ \mathcal{B}_{A_j^{\text{in}} A_j^{\text{EPR}} \to M} \tag{B6}$$

whenever the challenge bit is 1.

Note that, for simplicity, in the main text we denote $M_j^{\mathcal{T}} = \mathcal{R}_{M B_j^{\text{EPR}} \to B_j^{\text{EPR}}} \circ M_{B_j^{\text{EPR}} \to B_j^{\text{EPR}}} \circ \mathcal{B}_{A_j^{\text{in}} A_j^{\text{EPR}} \to M}$.

Having defined a single round of a protocol we describe the ping-pong teleportation protocol of depth κ. Such a protocol is simply a κ-round teleportation, where first $\kappa - 1$ maps have form (B5) and the last map outputs the state and so has the form (B6).

Definition 13. The teleportation-based ping-pong testing protocol of depth κ for a state $|\psi\rangle\langle\psi| \in \mathsf{X}$, a sequence of gates $\vec{c}_\kappa \in \mathsf{Cliff}^\kappa$ and a string of challenges $\vec{f}_\kappa = 1 \cdots 10$ is defined as a CPTP map $\mathcal{T}_\kappa$ such that

$$\mathcal{T}_\kappa \equiv \mathcal{T}_{A_1^{\text{in}} A_{[1,\kappa]}^{\text{EPR}} B_{[1,\kappa]}^{\text{EPR}} F_{[1,\kappa]} C_{[1,\kappa]} \to B_\kappa^{\text{out}}} = \Lambda_{A_\kappa^{\text{in}} A_\kappa^{\text{EPR}} B_\kappa^{\text{EPR}} F_\kappa C_\kappa \to B_\kappa^{\text{out}}} \circ \bigcirc_{j=1}^{\kappa-1} \Lambda_{A_j^{\text{in}} A_j^{\text{EPR}} B_j^{\text{EPR}} F_j C_j \to B_{j+1}^{\text{in}}} \tag{B7}$$

applied to the input state

$$|\psi\rangle\langle\psi|_{A_1^{\text{in}}} \otimes \bigotimes_{j=1}^{\kappa} \Phi^+_{A_j^{\text{EPR}} B_j^{\text{EPR}}} \otimes \left|\vec{f}_\kappa\right\rangle\left\langle\vec{f}_\kappa\right|_{F_{[1,\kappa]}} \otimes |\vec{c}_\kappa\rangle\langle\vec{c}_\kappa|_{C_{[1,\kappa]}} \tag{B8}$$

where Λ's are defined as in definition 12.

B.3. Measurements

Upon receiving requested state from either A or B, V must check its consistency with the distributed state, as well as confirm applying desired gates. This can be achieved by projecting outcomes onto the state $C_\kappa \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{B_\kappa^{\text{out}}}$, which is the original state rotated with κ Clifford channels.

Definition 14 (POVM elements for the node V). Measurements performed by V in the teleportation-based ping-pong test can be described by POVM elements,

$$\Pi^{\kappa}_{\checkmark} = C_\kappa \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{B^{\text{out}}_\kappa} \tag{B9}$$

$$\Pi^{\kappa}_{\text{✗}} = \mathbb{1} - C_\kappa \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{B^{\text{out}}_\kappa} \tag{B10}$$

for all $\kappa = 1, \ldots, k$. κ denotes here the output register of the κ-th party, depending on the parity either A or B.

B.4. Renaming teleportation channel

Now that we have formalized the testing protocol in detail, we will justify using notation for a teleportation channel used in the main text. That is, we will show that a teleportation channel with noisy memory acting on $|\psi\rangle\langle\otimes|\,\Phi^+$ can be viewed as a channel $M_j^{\mathcal{T}}$ acting only on $|\psi\rangle\langle\psi|$.

Recall definition 12. In a single round j of the protocol A performs a Bell measurement on the state $|\psi\rangle\langle\psi|_{A_j^{\text{in}}}$ and her part of EPR pair. This action is described described by an operator $\mathcal{B}_{A_j^{\text{in}}A_j^{\text{EPR}}\to M}$, acting on two registers on A's side and producing a classical message $m \in M$ which is then sent to B. The initial state $|\psi\rangle\langle\psi|_{A_j^{\text{in}}} \otimes \Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}$ becomes

$$\begin{aligned}\mathcal{B}_{A_j^{\text{in}}A_j^{\text{EPR}}\to M}(|\psi\rangle\langle\psi|_{A_j^{\text{in}}} \otimes \Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}) &= \text{Tr}_{A_j^{\text{in}}A_j^{\text{EPR}}}\left[\sum_{m\in M} p_m \Psi'_{A_j^{\text{in}}A_j^{\text{EPR}},m} \otimes (U_m|\psi\rangle\langle\psi|\,U_m^\dagger)_{B_j^{\text{EPR}}} \otimes |m\rangle\langle m|_M,\right] \\ &= \sum_{m\in M} p_m (U_m|\psi\rangle\langle\psi|\,U_m^\dagger)_{B_1^{\text{EPR}}} \otimes |m\rangle\langle m|_M\end{aligned} \tag{B11}$$

where $\Psi'_{A_j^{\text{in}}A_j^{\text{EPR}},m}$ is one of four Bell states resulting from the Bell measurement, $p_m \geqslant 0$, $\sum_m p_m = 1$ is a probability of an outcome m occurring. $(U_m|\psi\rangle\langle\psi|\,U_m^\dagger)_{B_j^{\text{EPR}}}$ is a state on B's register after the Bell measurement. Note that this is simply a unitary applied to the initial state. $|m\rangle\langle m|$ is a classical message register, which A sends to B in order for him to correct the state. Next, B applies a memory $M_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}}$ to his share of the state:

$$M_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}} \circ \mathcal{B}_{A_j^{\text{in}}A_j^{\text{EPR}}\to M}(|\psi\rangle\langle\psi|_{A_j^{\text{in}}} \otimes \Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}) = M_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}} \sum_{m\in M} p_m (U_m|\psi\rangle\langle\psi|\,U_m^\dagger)_{B_j^{\text{EPR}}} \otimes |m\rangle\langle m|_M \tag{B12}$$

$$= \sum_{m\in M} p_m M_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}}(U_m|\psi\rangle\langle\psi|\,U_m^\dagger)_{B_j^{\text{EPR}}} \otimes |m\rangle\langle m|_M \tag{B13}$$

Upon receiving a classical message m B undoes the unitary operations to recover the teleported state. This operation is described by a map $\mathcal{R}_{MB_j^{\text{EPR}}\to B_j^{\text{EPR}}}(\cdot) = \text{Tr}_M[\sum_m U_m(\cdot)U_m^\dagger \otimes |m\rangle\langle m|_M]$,

$$\begin{aligned}&\mathcal{R}_{MB_j^{\text{EPR}}\to B_j^{\text{EPR}}} \circ M_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}} \circ \mathcal{B}_{A_j^{\text{in}}A_j^{\text{EPR}}\to M}(|\psi\rangle\langle\psi|_{A_j^{\text{in}}} \otimes \Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}) \\ &= \text{Tr}_M\left[\sum_{m\in M} p_m U_m^\dagger M_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}}(U_m|\psi\rangle\langle\psi|\,U_m^\dagger)_{B_j^{\text{EPR}}} U_m \otimes |m\rangle\langle m|_M\right] \\ &= \sum_{m\in M} p_m U_m^\dagger M_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}}(U_m|\psi\rangle\langle\psi|\,U_m^\dagger)_{B_j^{\text{EPR}}} U_m \\ &= \sum_{m\in M} p_m \mathcal{U}_m^\dagger \circ M_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}} \circ \mathcal{U}_m(|\psi\rangle\langle\psi|) =: M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|)\end{aligned} \tag{B14}$$

Then, the test of depth κ can be described as in the main text

$$\mathcal{T}^\kappa = \mathcal{T}_{A_1^{\text{in}}A_{[1,\kappa]}^{\text{EPR}}B_{[1,\kappa]}^{\text{EPR}}F_{[1,\kappa]}C_{[1,\kappa]}\to B_\kappa^{\text{out}}}\left(|\psi\rangle\langle\psi|_{A_1^{\text{in}}} \otimes \bigotimes_{j=1}^{\kappa} \Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}} \otimes \left|\vec{f}_\kappa\right\rangle\left\langle\vec{f}_\kappa\right|_{F_{[1,k]}} \otimes |\vec{c}_\kappa\rangle\langle\vec{c}_\kappa|_{C_{[1,k]}}\right) \tag{B15}$$

$$\equiv \bigcirc_{j=1}^{\kappa}\Lambda_j = \bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathcal{T}}\left(|\psi\rangle\langle\psi|\right) \tag{B16}$$

Appendix C. Teleportation and quantum memory

C.1. Absorbing teleportation noise into the memory

As it is often done in the estimation literature for quantum computing, see e.g. [8–10], we will model teleportation as a perfect operation followed (or preceded) by noise. This will allow us to consider teleportation as a perfect operation i.e. with perfect Bell measurement and recovery operation as well as perfect EPR pair, and absorb all the associated noise into the quantum memory.

C.1.1. Noisy operations. Assume a Bell state measurement is followed by a local noise, $\mathcal{B}_{A_j^{\text{in}}A_j^{\text{EPR}}\to M} \equiv N^{\mathcal{B}} \circ \mathcal{B}_{A_j^{\text{in}}A_j^{\text{EPR}}\to M}$. Assume further that the recovery operation is also noisy, but in this case the map is preceded by the noise, $\mathcal{R}_{MB_j^{\text{EPR}}\to B_j^{\text{EPR}}} \equiv \mathcal{R}_{MB_j^{\text{EPR}}\to B_j^{\text{EPR}}} \circ N^{\mathcal{R}}$. Looking at definition 12 it is now clear that one can redefine $M'_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}} = N^{\mathcal{R}} \circ M_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}} \circ N^{\mathcal{B}}$ and use M' as a new memory channel.

C.1.2. Noisy EPR pair. The situation is similar for a noisy EPR pair. Assume an EPR pair is affected by local noise, i.e. teleportation occurs on a state $N_{A_j^{\text{EPR}}} \otimes N_{B_j^{\text{EPR}}}\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right)$. Here the maps N are mixed-unitary channels, i.e. have the form $N(\cdot) = \sum_l p_l U_l(\cdot)U_l^\dagger$, with p_l being a probability and U_l a unitary. Note that this is not the most general type of noise, however the most common ones (e.g. depolarizing, dephasing) can be modeled this way. Moreover, note that for an EPR pair it holds that

$$U_{A_j^{\text{EPR}}} \otimes U_{B_j^{\text{EPR}}}\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right) = \mathrm{id}_{A_j^{\text{EPR}}} \otimes U_{B_j^{\text{EPR}}} U^T_{A_j^{\text{EPR}}}\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right). \tag{C1}$$

Therefore, using an explicit form of maps N and the above statement, we can write,

$$N_{A_j^{\text{EPR}}} \otimes N_{B_j^{\text{EPR}}}\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right) = \sum_{l,l'} p_{l,l'} U_{A_j^{\text{EPR}}} \otimes U_{B_j^{\text{EPR}}}\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right) \tag{C2}$$

$$= \sum_{l,l'} p_{l,l'} \mathrm{id}_{A_j^{\text{EPR}}} \otimes U_{B_j^{\text{EPR}}} U^T_{A_j^{\text{EPR}}}\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right) \tag{C3}$$

$$=: \mathrm{id}_{A_j^{\text{EPR}}} \otimes N'_{B_j^{\text{EPR}}}\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right) \tag{C4}$$

In particular, this means that noise acting on the EPR pair, which has the mixed-unitary form, can be absorbed into the memory map,

$$M'_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}} \circ \mathcal{B}_{A_j^{\text{in}}A_j^{\text{EPR}}\to M} \circ \left(N_{A_j^{\text{EPR}}} \otimes N_{B_j^{\text{EPR}}}\right)\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right) \tag{C5}$$

$$= M'_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}} \circ \mathcal{B}_{A_j^{\text{in}}A_j^{\text{EPR}}\to M} \circ \left(\mathrm{id}_{A_j^{\text{EPR}}} \otimes N'_{B_j^{\text{EPR}}}\right)\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right) \tag{C6}$$

$$= M'_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}} \circ N'_{B_j^{\text{EPR}}} \circ \mathcal{B}_{A_j^{\text{in}}A_j^{\text{EPR}}\to M}\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right) \tag{C7}$$

$$\equiv M''_{B_j^{\text{EPR}}\to B_j^{\text{EPR}}} \circ \mathcal{B}_{A_j^{\text{in}}A_j^{\text{EPR}}\to M}\left(\Phi^+_{A_j^{\text{EPR}}B_j^{\text{EPR}}}\right) \tag{C8}$$

Appendix D. 2-designs

In this appendix we show that for the ping-pong test, the average of the probability $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$ over the six Pauli states is equal to its average over the whole state space according to the Haar measure. To do so, we use the fact that the uniform distribution over set X is a 2-design [26] and $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$ contains a polynomial of degree 2 in $|\psi\rangle$. Next, we prove a similar statement when averaging over the Clifford group.

D.1. Pauli states

Lemma 6. *Averaging the probability of success for a single execution of test 2, $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$, over Pauli states is equal to averaging over all qubit states according to the Haar measure,*

$$\frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \int \mathrm{d}\psi\, p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}. \tag{D1}$$

Proof of lemma 2. We can write the left-hand side explicitly as,

$$\frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \frac{1}{|\mathsf{X}|}\sum_{\psi} \mathrm{Tr}\left[\mathcal{T}_\kappa(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}})\cdot \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)_{B_\kappa^{\mathrm{out}}}\right] \tag{D2}$$

where we explicitly write A and B's input and output registers. Let $X, Y \in \mathcal{L}(\mathcal{H})$ be linear operators over the Hilbert space. The inner product $\langle X\rangle Y := \mathrm{Tr}[X^\dagger Y]$ is invariant $\forall U : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$, i.e. $\langle U(X)\rangle U(Y) = \mathrm{Tr}[(U(X))^\dagger \cdot U(Y)] = \mathrm{Tr}[X^\dagger \cdot Y] = \langle X\rangle Y$. Note that $\bigcirc_{j=1}^{\kappa} C_j$ is a unitary channel and therefore, we can write,

$$\frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \frac{1}{|\mathsf{X}|}\sum_{\psi} \mathrm{Tr}\left[\left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1}\circ \mathcal{T}_\kappa(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}})\cdot \left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1}\circ \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)_{B_\kappa^{\mathrm{out}}}\right] \tag{D3}$$

$$= \frac{1}{|\mathsf{X}|}\sum_{\psi} \mathrm{Tr}\left[\left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1}\circ \mathcal{T}_\kappa(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}})\cdot |\psi\rangle\langle\psi|_{B_\kappa^{\mathrm{out}}}\right] \tag{D4}$$

Now, using Choi–Jamiolkowski theorem, see lemma 5, we can write

$$\frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \frac{1}{|\mathsf{X}|}\sum_{\psi} |A_1^{\mathrm{in}'}|\mathrm{Tr}\left[|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}}\otimes|\psi\rangle\langle\psi|_{B_\kappa^{\mathrm{out}}}\omega^{\Gamma}_{A_1^{\mathrm{in}'}B_\kappa^{\mathrm{out}}}\right] \tag{D5}$$

$\omega^{\Gamma}_{A_1^{\mathrm{in}'}B_\kappa^{\mathrm{out}}}$ is a Choi–Jamiolkowski state associated with the map $\left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1}\circ\tilde{\mathcal{T}}_\kappa$. It is now clear that averaging is taken over a polynomial of degree 2 under the trace and we can use properties of a 2-design. Therefore,

$$\frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \int \mathrm{d}\psi |A_1^{\mathrm{in}'}|\mathrm{Tr}\left[|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}}\otimes|\psi\rangle\langle\psi|_{B_\kappa^{\mathrm{out}}}\,\omega^{\Gamma}_{A_1^{\mathrm{in}'}B_\kappa^{\mathrm{out}}}\right] \tag{D6}$$

$$= \int \mathrm{d}\psi \mathrm{Tr}\left[\mathcal{T}_\kappa(|\psi\rangle\langle\psi|_{A_1^{\mathrm{in}}})\cdot \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)_{B_\kappa^{\mathrm{out}}}\right] \tag{D7}$$

$$= \int \mathrm{d}\psi\, p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} \tag{D8}$$

where we used Choi–Jamiolkowski isomorphism and properties of the trace again. We define $\bar{F}_{\vec{c}_\kappa,\kappa} = \int \mathrm{d}\psi\, p_{\checkmark|\psi,\vec{c}_\kappa,kt}$ as the average fidelity. □

D.2. Clifford gates

Now we will prove that averaging $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$ over the Clifford set reproduces averaging over the whole unitary set taken according to the Haar measure.

Lemma 7. *Averaging the probability of success for a single execution of test 2, $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$, over Pauli states and over Clifford gates is equal to averaging over all qubit states and all 2-qubit unitary gates according to the Haar measure,*

$$\frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}} \frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa} p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \int \mathrm{d}\psi \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_\kappa\, p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}. \tag{D9}$$

Proof. Just like in the previous lemma, let us first use cyclicity of the trace,

$$\text{LHS} = \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa}} \sum_{\vec{c}_\kappa} \mathrm{Tr}\left[\left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1} \circ \mathcal{T}_\kappa(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right] \tag{D10}$$

$$= \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa}} \sum_{\vec{c}_\kappa} \mathrm{Tr}\left[C_1^\dagger \circ \cdots \circ C_\kappa^\dagger \circ C_\kappa \circ M_\kappa^{\mathcal{T}} \circ C_{\kappa-1} \circ M_{\kappa-1}^{\mathcal{T}} \circ \cdots \circ C_1 \circ M_1^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right] \tag{D11}$$

$$= \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa-1}} \sum_{C_1,\cdots,C_{\kappa-1}\in\mathsf{Cliff}} \mathrm{Tr}\left[C_1^\dagger \circ \cdots \circ C_{\kappa-1}^\dagger \circ M_\kappa^{\mathcal{T}} \circ C_{\kappa-1} \circ M_{\kappa-1}^{\mathcal{T}} \circ \cdots \circ C_1 \times \circ M_1^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right] \tag{D12}$$

$$= \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa-1}} \sum_{C_1,\cdots,C_{\kappa-2}\in\mathsf{Cliff}} \mathrm{Tr}\left[C_1^\dagger \circ \cdots \circ C_{\kappa-2}^\dagger \left(\sum_{C_{\kappa-1}\in\mathsf{Cliff}} C_{\kappa-1}^\dagger \circ M_\kappa^{\mathcal{T}} \circ C_{\kappa-1}\right) \times \circ M_{\kappa-1}^{\mathcal{T}} \circ \cdots \circ C_1 \circ M_1^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right], \tag{D13}$$

where in the last step we pulled the summation over $\kappa - 1$ under the trace. Note that $\left(\sum_{C_{\kappa-1}} C_{\kappa-1}^\dagger \circ M_\kappa^{\mathcal{T}} \circ C_{\kappa-1}\right)$ is an unnormalized twirl over Cliff and therefore it commutes with all Clifford gates $C \in \mathsf{Cliff}$. By repeating pulling the summation under the trace, we can write,

$$\text{LHS} = \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa-1}} \sum_{C_1,\cdots,C_{\kappa-3}\in\mathsf{Cliff}} \mathrm{Tr}\left[C_1^\dagger \circ \cdots \circ C_{\kappa-3}^\dagger \left(\sum_{C_{\kappa-2}\in\mathsf{Cliff}} C_{\kappa-2}^\dagger \circ M_{\kappa-1}^{\mathcal{T}} \circ C_{\kappa-2}\right) \circ \left(\sum_{C_{\kappa-1}\in\mathsf{Cliff}} C_{\kappa-1}^\dagger \circ M_\kappa^{\mathcal{T}} \circ C_{\kappa-1}\right) \circ M_{\kappa-2}^{\mathcal{T}} \circ \cdots \circ C_1 \circ M_1^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right] \tag{D14}$$

$$= \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa-1}} \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa-1} \left(\sum_{C_j\in\mathsf{Cliff}} C_j^\dagger \circ M_{j+1}^{\mathcal{T}} \circ C_j\right) \circ M_1^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right]. \tag{D15}$$

Now we are left with a rather awkward map $M_1^{\mathcal{T}}$ which is not twirled. However, since the Haar measure is invariant under unitary transformations, for all $E \in \mathsf{Cliff}$ it holds that

$$\text{LHS} = \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa-1}} \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa-1} \left(\sum_{C_j\in\mathsf{Cliff}} C_j^\dagger \circ M_{j+1}^{\mathcal{T}} \circ C_j\right) \circ M_1^{\mathcal{T}} \circ E(|\psi\rangle\langle\psi|) \cdot E(|\psi\rangle\langle\psi|)\right] \tag{D16}$$

$$= \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa}} \sum_{E\in\mathsf{Cliff}} \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa-1} \left(\sum_{C_j\in\mathsf{Cliff}} C_j^\dagger \circ M_{j+1}^{\mathcal{T}} \circ C_j\right) \circ M_1^{\mathcal{T}} \circ E(|\psi\rangle\langle\psi|) \cdot E(|\psi\rangle\langle\psi|)\right] \tag{D17}$$

where in the last line we used the fact that the value of the expression does not depend on E. Now, using cyclicity of the trace and commutativity properties of E, we get

$$\text{LHS} = \int \mathrm{d}\psi \frac{1}{|\mathsf{Cliff}|^{\kappa}} \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa-1} \left(\sum_{C_j\in\mathsf{Cliff}} C_j^\dagger \circ M_{j+1}^{\mathcal{T}} \circ C_j\right) \circ \left(\sum_{E\in\mathsf{Cliff}} E^\dagger \circ M_1^{\mathcal{T}} \circ E\right)(|\psi\rangle\langle\psi|) \cdot (|\psi\rangle\langle\psi|)\right]. \tag{D18}$$

Now we can change discrete averaging to the continuous one by definition of the unitary 2-design, see definition 8 and [27]. We have

$$\text{LHS} = \int \mathrm{d}\psi\, \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa-1} \left(\int \mathrm{d}C_j\, C_j^\dagger \circ M_{j+1}^{\mathcal{T}} \circ C_j\right) \circ \left(\int \mathrm{d}E\, E^\dagger \circ M_1^{\mathcal{T}} \circ E\right)(|\psi\rangle\langle\psi|) \cdot (|\psi\rangle\langle\psi|)\right]. \tag{D19}$$

To get back to the expression for $p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$, we can invert the procedure we just applied, i.e.

$$\text{LHS} = \int \mathrm{d}\psi \int \mathrm{d}E \,\mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa-1}\left(\int \mathrm{d}C_j\, C_j^\dagger \circ M_{j+1}^{\mathcal{T}} \circ C_j\right) \circ \left(E^\dagger \circ M_1^{\mathcal{T}} \circ E\right)(|\psi\rangle\langle\psi|) \cdot (|\psi\rangle\langle\psi|)\right] \tag{D20}$$

$$= \int \mathrm{d}\psi \int \mathrm{d}E \,\mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa-1}\left(\int \mathrm{d}C_j\, C_j^\dagger \circ M_{j+1}^{\mathcal{T}} \circ C_j\right) \circ M_1^{\mathcal{T}} \circ E(|\psi\rangle\langle\psi|) \cdot E(|\psi\rangle\langle\psi|)\right] \tag{D21}$$

$$= \int \mathrm{d}\psi \int \mathrm{d}E \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_{\kappa-1}\,\mathrm{Tr}\left[C_1^\dagger \circ \cdots \circ C_{\kappa-1}^\dagger \circ M_\kappa^{\mathcal{T}} \circ C_{\kappa-1} \circ M_{\kappa-1}^{\mathcal{T}} \circ \cdots \circ C_1 \right.$$
$$\left. \circ M_1^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right] \tag{D22}$$

$$= \int \mathrm{d}\psi \int \mathrm{d}E \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_{\kappa-1}\,\mathrm{Tr}\left[C_1^\dagger \circ \cdots \circ C_{\kappa-1}^\dagger \circ E^\dagger \circ E \circ M_\kappa^{\mathcal{T}} \circ C_{\kappa-1} \circ M_{\kappa-1}^{\mathcal{T}} \circ \cdots \circ C_1 \right.$$
$$\left. \circ M_1^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right] \tag{D23}$$

If now we put $E = C_\kappa$ we obtain the desired result. We define $\bar{\bar{F}}_\kappa = \int \mathrm{d}\psi \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_\kappa\, p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}$ as double-averaged fidelity. □

Appendix E. Completeness and soundness

E.1. Exact completeness and soundness

To keep this section more compact, we use notation from the main text. That is we express test 2 as $\mathcal{T}_\kappa = \bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathcal{T}}$, see equation (6).

Proof of theorem 1. First, we prove that test 2 is exactly correct when the winning threshold $P_\checkmark = 1$. That is, for honest A and B and for any $1 \leqslant \kappa \leqslant k$ after κ rounds the state that the verifier obtains at output κ is $\bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|)$. To prove this, we need to make sure that for all the rounds preceding κ the state at outputs $j = 1, \ldots, \kappa$ are correct. The above can be proven by induction. For $\kappa = 1$ the verifier measures $C_1(|\psi\rangle\langle\psi|)$. On the other hand, $C_1 \circ M_1^{\mathcal{T}} = C_1(|\psi\rangle\langle\psi|)$, since the setup is perfect. Repeating this step inductively we get for all κ,

$$\bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|) = \bigcirc_{j=1}^{\kappa} C_j(|\psi\rangle\langle\psi|) \tag{E1}$$

Hence, $P_\checkmark = 1$. □

Before proving theorem 2 we formally prove a known fact related to no-cloning theorem [17].

Lemma 8. *Let $V_{A\to A'B}$ be an arbitrary isometry, and let for any qubit state $|\psi\rangle_A$, $|\Psi\rangle_{A'B} := V|\psi\rangle_A$. If for all $|\psi\rangle$, $\mathrm{Tr}_B(|\Psi\rangle\langle\Psi|_{A'B}) = |\psi\rangle\langle\psi|_{A'}$, then $|\Psi\rangle_{A'B} = |\psi\rangle_{A'} \otimes |\mathrm{junk}\rangle_B$, where $|\mathrm{junk}\rangle$ is a pure state independent of $|\psi\rangle$.*

Proof. If the above is true for all $|\psi\rangle$ it is in particular true for $|0\rangle$, namely, $V|0\rangle = |0\rangle \otimes |\sigma_0\rangle$. Similarly $V|1\rangle = |1\rangle \otimes |\sigma_1\rangle$. When now computing the action of V on the state $|+\rangle$, we have $V|+\rangle = \frac{|0\rangle\otimes|\sigma_0\rangle + |1\rangle\otimes|\sigma_1\rangle}{\sqrt{2}}$. But since $\mathrm{Tr}_B(V|+\rangle\langle V|^\dagger) = |+\rangle\langle+|$, we must have $|\sigma_0\rangle = |\sigma_1\rangle =: |\mathrm{junk}\rangle$ □

Corollary 3. *Let $\Omega_{A\to A'B}$ be an arbitrary CPTP map, and let for any qubit state $|\psi\rangle\langle\psi|_A$, $\rho_{A'B} := \Omega(|\psi\rangle\langle\psi|_A)$. If for all $|\psi\rangle$, $\mathrm{Tr}_B(\rho_{A'B}) = |\psi\rangle\langle\psi|_{A'}$, then $\rho_{A'B} = |\psi\rangle\langle\psi|_{A'} \otimes \mathrm{junk}_B$, where junk is a state independent of $|\psi\rangle\langle\psi|$.*

Proof. By Stinespring dilation $\exists V_{A\to A'BE}\ \Omega(\cdot) = \mathrm{Tr}_E(V(\cdot)V^\dagger)$. Since $\mathrm{Tr}_B(\rho_{A'B}) = |\psi\rangle\langle\psi|_{A'} = \mathrm{tr}_{BE}(V|\psi\rangle\langle\psi|V^\dagger)$ we must have by the above lemma that $V|\psi\rangle\langle\psi|V^\dagger = |\psi\rangle\langle\psi|_{A'} \otimes |\mathrm{junk}'\rangle\langle\mathrm{junk}'|_{BE}$, and therefore $\rho_{A'B} = |\psi\rangle\langle\psi|_{A'} \otimes \mathrm{Tr}_E(|\mathrm{junk}'\rangle\langle\mathrm{junk}'|_{BE}) = |\psi\rangle\langle\psi|_{A'} \otimes \mathrm{junk}_B$. □

Proof of theorem 2. Now we prove that test 2 is exactly sound. That is, if the average probability of success $P_\checkmark = 1$, then nodes A and B have the ability to correctly execute test 2. The intuition behind our proof is

that challenges given by the verifier impose a certain structure on the provers strategy. We first show that if the nodes win the test with probability 1, then their strategy must produce the correct state at each time step κ. Then, we argue that this implies that the nodes must have passed the state around, and therefore use a quantum channel between them exactly κ times.

Lemma 9. *Let $\mathcal{Q}_{\vec{c}_\kappa,\kappa}$ be an arbitrary strategy of the provers, which can depend on the information available throughout the protocol, i.e. depth κ and Clifford string $\vec{c}_\kappa$. If the average probability of success in test 2 is $P_\checkmark = 1$, then for all depths $\kappa = 1,\ldots,k$, all Clifford strings $\vec{c}_\kappa$ and all input states $\psi \in \mathsf{X}$, $\mathcal{Q}_{\vec{c}_\kappa,\kappa}$ outputs the correct state.*

Proof. This statement is essentially the inverse of the exact completeness statement. Let us explicitly write the average probability of success,

$$P_\checkmark = \frac{1}{k}\sum_\kappa \frac{1}{|\mathsf{X}|}\sum_{\psi\in\mathsf{X}} \frac{1}{|\mathsf{Cliff}|^\kappa} \sum_{\vec{c}_\kappa\in\mathsf{Cliff}^\kappa} \mathrm{Tr}\left[\mathcal{Q}_{\vec{c}_\kappa,\kappa}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^\kappa_\checkmark\right] = 1. \tag{E2}$$

This implies that for all states, gates and depths the trace must be equal to 1,

$$\forall\psi\in\mathsf{X},\ \forall\vec{c}_\kappa\in\mathsf{Cliff}^\kappa,\ \forall\kappa=1,\cdots,k:\quad \mathrm{Tr}\left[\mathcal{Q}_{\vec{c}_\kappa,\kappa}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^\kappa_\checkmark\right] = 1. \tag{E3}$$

Therefore,

$$\forall\psi\in\mathsf{X},\ \forall\vec{c}_\kappa\in\mathsf{Cliff}^\kappa,\ \forall\kappa=1,\cdots,k:\quad \mathcal{Q}_{\vec{c}_\kappa,\kappa}\left(|\psi\rangle\langle\psi|\right) = C_\kappa\circ\cdots\circ C_1(|\psi\rangle\langle\psi|) \tag{E4}$$

and the state at every κ must be exactly the one requested by the verifier. □

Lemma 10. *If the average probability of success in test 2 is $P_\checkmark = 1$, then for all depths $\kappa = 1,\ldots,k$, all Clifford strings $\vec{c}_\kappa$ and all input states $\psi\in\mathsf{X}$, $\mathcal{Q}_{\vec{c}_\kappa,\kappa}$ uses an exact sending channel κ times and apply an operation equivalent to the one described by $\vec{c}_\kappa$.*

Proof. In our test at every time step κ the provers must produce some state. Since at every time step a state has to be defined, $\mathcal{Q}_{\vec{c}_\kappa,\kappa}$ can be described by

$$\mathcal{Q}_{\vec{c}_\kappa,\kappa} = \bigcirc_{j=1}^{\kappa}\mathcal{E}_{\vec{c}_j,j} \tag{E5}$$

Let $\hat{\Gamma}_{A_{\kappa-1}}$ and $\hat{\Gamma}_{B_{\kappa-1},B_\kappa}$ denote CPTP maps which act on registers of A and B respectively, and output qubit states, and let $\Gamma_{A_{\kappa-1}}$ and $\Gamma_{B_{\kappa-1},B_\kappa}$ be $\mathrm{Tr}_{B_{\kappa-1},B_\kappa}[\hat{\Gamma}_{A_{\kappa-1}}(\cdot)]$ and $\mathrm{Tr}_{A_{\kappa-1}}[\hat{\Gamma}_{B_{\kappa-1},B_\kappa}(\cdot)]$ respectively. The above fact together with lemmas 6 and 10 implies that at time steps κ and $\kappa-1$

$$\int \mathrm{d}\psi \mathrm{Tr}\left[\mathcal{E}_{\vec{c}_\kappa,\kappa}\circ\mathcal{Q}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^\kappa_\checkmark\right] = 1 \Rightarrow \sup_{\Gamma_{B_{\kappa-1},B_\kappa}}\int \mathrm{d}\psi \mathrm{Tr}\left[\Gamma_{B_{\kappa-1},B_\kappa}\left(\mathcal{E}_{\vec{c}_\kappa,\kappa}\left(\rho^\psi_{\vec{c}_{\kappa-1},\kappa-1}\right)\right)\cdot\Pi^\kappa_\checkmark\right] = 1 \tag{E6}$$

$$\int \mathrm{d}\psi \mathrm{Tr}\left[\mathcal{Q}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^{\kappa-1}_\checkmark\right] = 1 \Rightarrow \sup_{\Gamma_{A_{\kappa-1}}}\int \mathrm{d}\psi \mathrm{Tr}\left[\Gamma_{A_{\kappa-1}}\left(\rho^\psi_{\vec{c}_{\kappa-1},\kappa-1}\right)\cdot\Pi^{\kappa-1}_\checkmark\right] = 1 \tag{E7}$$

Moreover, we have put $\rho^\psi_{\vec{c}_{\kappa-1},\kappa-1} := \mathcal{Q}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right)$ to denote a joint state of A and B at time step $\kappa-1$. Observe that for all κ, $\Pi^\kappa_\checkmark = C_\kappa\circ\cdots\circ C_1(|\psi\rangle\langle\psi|)$ projects onto a pure state. Therefore, for all κ, the states at output registers $\kappa-1$ for A, and κ for B, must be pure,

$$\Gamma_{B_{\kappa-1},B_\kappa}\left(\mathcal{E}_{\vec{c}_\kappa,\kappa}\left(\rho^\psi_{\vec{c}_{\kappa-1},\kappa-1}\right)\right) = C_\kappa\circ\cdots\circ C_1(|\psi\rangle\langle\psi|)_{B_\kappa} \tag{E8}$$

$$\Gamma_{A_{\kappa-1}}\left(\rho^\psi_{\vec{c}_{\kappa-1},\kappa-1}\right) = C_{\kappa-1}\circ\cdots\circ C_1(|\psi\rangle\langle\psi|)_{A_{\kappa-1}} \tag{E9}$$

Let $\sigma^\psi = (\hat{\Gamma}_{A_{\kappa-1}}\otimes\mathbb{1})(\rho^\psi_{\vec{c}_{\kappa-1},\kappa-1})$ be the joint state of A and B at time step $\kappa-1$, and after applying $\hat{\Gamma}_{A_{\kappa-1}}$ on A. Using equation (E9) we have that,

$$\mathrm{Tr}_{B_{\kappa-1}}(\sigma^{\psi}) = C_{\kappa-1} \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{A_{\kappa-1}}, \tag{E10}$$

which is a pure state on A, and therefore any extension of this state has tensor product form across A and B, in particular,

$$\sigma^{\psi} = C_{\kappa-1} \circ \cdots \circ C_1(|\psi\rangle\langle\psi|)_{A_{\kappa-1}} \otimes \sigma_{B_{\kappa-1}}, \tag{E11}$$

where $\sigma_{B_{\kappa-1}}$ is a state on B independent of ψ by corollary 3. Therefore the (maximum) average fidelity of the state on B's side is,

$$\sup_{\Gamma_{B_{\kappa-1}}} \int \mathrm{d}\psi \mathrm{Tr}\left[\Gamma_{B_{\kappa-1}}\left(\rho^{\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right) \cdot \Pi^{\kappa-1}_{\checkmark}\right] = \sup_{\Gamma_{B_{\kappa-1}}} \int \mathrm{d}\psi \mathrm{Tr}\left[\sigma_{B_{\kappa-1}} \cdot \Pi^{\kappa-1}_{\checkmark}\right] = \sup_{\Gamma_{B_{\kappa-1}}} \mathrm{Tr}\left[\sigma_{B_{\kappa-1}} \cdot \frac{\mathbb{1}}{2}\right] = \frac{1}{2} \tag{E12}$$

This, together with equation (E6), implies that $\mathcal{E}_{\vec{c}_\kappa,\kappa}$ is an exact sending channel at time step κ. Since the statement holds for all κ, the provers necessarily use the exact sending channel k times. □

E.2. Completeness and soundness

Proof of theorem 3. *Completeness.* As stated in the main text, we assume that the quality of operations is quantified by average fidelity and that at every round j the quality of operations is the same, i.e. for all j, $\bar{\mu} = \int \mathrm{d}\psi \mathrm{Tr}[C_j \circ M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot C_j(|\psi\rangle\langle\psi|)]$. In the following we bound the average probability of success $P_\checkmark$ in terms of $\bar{\mu}$. Let us write $P_\checkmark$ explicitly,

$$P_\checkmark = \frac{1}{k}\sum_{\kappa} \frac{1}{|\mathsf{X}|} \sum_{\psi} \frac{1}{|\mathsf{Cliff}|^{\kappa}} \sum_{\vec{c}_\kappa} \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot \Pi^{\checkmark}_{\kappa}\right] \tag{E13}$$

From lemma 7 we have that

$$P_\checkmark = \frac{1}{k}\sum_{\kappa} \int \mathrm{d}\psi \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_\kappa \mathrm{Tr}\left[\left(\bigcirc_{j=1}^{\kappa} C_j\right)^{-1} \circ \bigcirc_{j=1}^{\kappa} C_j \circ M_j^{\mathcal{T}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right], \tag{E14}$$

$$= \frac{1}{k}\sum_{\kappa} \int \mathrm{d}\psi \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa} \left(\int \mathrm{d}C_j\, C_j^{\dagger} \circ M_j^{\mathcal{T}} \circ C_j\right)(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right]. \tag{E15}$$

Observe that $(M_j^{\mathcal{T}})_{\mathrm{twirl}} = \int \mathrm{d}C_j\, C_j^{\dagger} \circ M_j^{\mathcal{T}} \circ C_j$ is a twirl of the operator $M_j^{\mathcal{T}}$ [28]. Furthermore, twirling any map is equivalent to the action of a depolarizing channel, i.e. $(M_j^{\mathcal{T}})_{\mathrm{twirl}}(\rho) = \mathcal{D}_j(\rho) = p\rho + (1-p)\mathbb{1}/2$, for some parameter p and any state ρ. Using properties of the depolarizing channel we can write,

$$P_\checkmark = \frac{1}{k}\sum_{\kappa} \int \mathrm{d}\psi \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa} (M_j^{\mathcal{T}})_{\mathrm{twirl}}(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right] \tag{E16}$$

$$= \frac{1}{k}\sum_{\kappa} \int \mathrm{d}\psi \mathrm{Tr}\left[\bigcirc_{j=1}^{\kappa} \mathcal{D}_j(|\psi\rangle\langle\psi|) \cdot |\psi\rangle\langle\psi|\right] \tag{E17}$$

$$= \frac{1}{k}\sum_{\kappa} \prod_{j=1}^{\kappa} \bar{F}\left(\mathcal{D}_j\right) \tag{E18}$$

$$= \frac{1}{k}\sum_{\kappa} \prod_{j=1}^{\kappa} \bar{F}\left((M_j^{\mathcal{T}})_{\mathrm{twirl}}\right) \tag{E19}$$

Additionally, the average fidelity of a twirled map is equal to the average fidelity of the same map without a twirl [28], therefore, $P_\checkmark = \frac{1}{k}\sum_{\kappa}\prod_{j=1}^{\kappa} \bar{F}\left(M_j^{\mathcal{T}}\right)$. By assumption, $\forall j\, \bar{F}\left(M_j^{\mathcal{T}}\right) = \bar{\mu}$, and

$$P_\checkmark = \frac{1}{k}\sum_{\kappa} \bar{\mu}^{\kappa} = \frac{1}{k}\frac{\bar{\mu}(\bar{\mu}^k - 1)}{k(\bar{\mu} - 1)} = h_k(\bar{\mu}). \tag{E20}$$

If we demand that $P_\checkmark \geqslant t$ then $\bar{\mu} \geqslant h_k^{-1}(t)$. □

Proof of theorem 4. *Soundness.* In the case when the nodes A and B are honest, the soundness statement is the converse of the completeness, see the proof above. Here we prove soundness of test 2 in the case when

the nodes are dishonest (m-cheating). Just like before, we will assume that output for a fixed κ happens at node B.

The idea behind this proof is that we bound the average probability of success of the provers when they use a quantum channel between them, and when they do not. More specifically, let $\rho_{A_{\kappa-1}^{\text{out}}}$ be a state available at A's output at time step $\kappa-1$ and $\rho_{B_\kappa}^{\text{out}}$ be a state available at B's at time step κ. We show that whenever the provers use the channel, the average fidelity between these two states is bounded by 1. However, whenever they do not use the channel, the average fidelity between these two states is at most as large as the average fidelity between the states at time step $\kappa-1$, i.e. $\rho_{A_{\kappa-1}^{\text{out}}}$ and $\rho_{B_{\kappa-1}^{\text{out}}}$. This average fidelity is intrinsically bounded by the approximate cloning theorem [18], and here takes value $\frac{5}{6}$. If the provers are m-cheating, they use the channel between at least m times. We prove that, as a consequence, their overall average probability of winning $P_\checkmark$ is upper-bounded by $\frac{1}{k}(m+\frac{5}{6}(k-m))$.

When the provers are m-cheating they adapt an arbitrary strategy $\mathcal{Q}^m_{\vec{c}_\kappa,\kappa}$ which depends on the maximum number of channel uses m between the nodes. It can also depend on all the information available throughout the protocol, i.e. the challenges and gates distributed by the verifier. We assume that the executions of the test are IID (independent and identically distributed) and the probability of winning a single execution $i=1,\ldots,n$ is expressed as

$$\forall\,\vec{c}_\kappa,\kappa,\psi \quad p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}=\mathrm{Tr}\left[\mathcal{Q}^m_{\vec{c}_\kappa,\kappa}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^\kappa_\checkmark\right]. \tag{E21}$$

The configuration of channel uses, i.e. at which time step the provers use the channel between them, does not need to be fixed. At each execution, the provers can choose a particular strategy $\mathcal{Q}^{m,\nu}$ which describes a configuration ν of channel uses between the nodes. We assume that the provers are *non-adaptive* and throughout an execution i their strategy does not change. Therefore, the fact whether the provers choose to send the state or not, is independent of the information available throughout the protocol. I.e. ν is independent of κ and $\vec{c}_\kappa$, and we have $q_\nu\geqslant 0$, $\sum_\nu q_\nu=1$, such that

$$\mathcal{Q}^m_{\vec{c}_\kappa,\kappa}=\sum_\nu q_\nu\mathcal{Q}^{m,\nu}_{\vec{c}_\kappa,\kappa}. \tag{E22}$$

Note that there are $\binom{k}{m}$ such strategies. Furthermore, let us define

$$p_{\checkmark|\nu,\psi,\vec{c}_\kappa,\kappa}:=\mathrm{Tr}\left[\mathcal{Q}^{m,\nu}_{\vec{c}_\kappa,\kappa}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^\kappa_\checkmark\right]. \tag{E23}$$

Let us rewrite the average probability of success, equation (7),

$$P_\checkmark=\frac{1}{2}\left(\frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_\psi\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}+\frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_\psi\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}\right). \tag{E24}$$

Now, we will move the summation in the second component of the sum over κ—instead of going through $(1,2,\ldots,k-1,k)$ we will set it to go $(k,1,2,\ldots,k-1)$,

$$P_\checkmark=\frac{1}{2}\left(\frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_\psi\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}+\frac{1}{k}\sum_{\kappa=k}^{k-1}\frac{1}{|\mathsf{X}|}\sum_\psi\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}\right). \tag{E25}$$

Let us define $p_{\checkmark|\psi,\vec{c}_0,0}:=1$ for round $\kappa=0$, which one can interpret as simply giving the state to node A and immediately requesting it back. Now since for $\kappa=k$ it holds that $p_{\checkmark|\psi,\vec{c}_k,k}\leqslant 1$, we have $p_{\checkmark|\psi,\vec{c}_k,k}\leqslant p_{\checkmark|\psi,\vec{c}_0,0}$. Therefore,

$$P_\checkmark\leqslant\frac{1}{2}\left(\frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_\psi\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}+\frac{1}{k}\sum_{\kappa=0}^{k-1}\frac{1}{|\mathsf{X}|}\sum_\psi\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}\right). \tag{E26}$$

Now we write the expression as a single summation,

$$P_{\checkmark} \leqslant \frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^{\kappa}}\sum_{\vec{c}_{\kappa}}\frac{p_{\checkmark|\psi,\vec{c}_{\kappa},\kappa}+p_{\checkmark|\psi,\vec{c}_{\kappa-1},\kappa-1}}{2} \tag{E27}$$

$$= \sum_{\nu} q_{\nu}\frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{X}|}\sum_{\psi}\frac{1}{|\mathsf{Cliff}|^{\kappa}}\sum_{\vec{c}_{\kappa}}\frac{1}{2}\left(p_{\checkmark|\nu,\psi,\vec{c}_{\kappa},\kappa}+p_{\checkmark|\nu,\psi,\vec{c}_{\kappa-1},\kappa-1}\right) \tag{E28}$$

$$= \sum_{\nu} q_{\nu}\frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{Cliff}|^{\kappa}}\sum_{\vec{c}_{\kappa}}\frac{1}{2}\left(\bar{F}_{\nu,\vec{c}_{\kappa},\kappa}+\bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1}\right) \tag{E29}$$

In line (E28) we used the linearity property of the trace, and in line (E29) we used 2-design properties of the set X (see argument in section 6) together with the fact that $\mathcal{Q}^{m,\nu}_{\vec{c}_{\kappa},\kappa}$ does not depend on the state.

In our test at every time step κ the provers must produce some state. Since at every time step a state has to be defined, $\mathcal{Q}^{m,\nu}_{\vec{c}_{\kappa},\kappa}$ can be described by

$$\mathcal{Q}^{m,\nu}_{\vec{c}_{\kappa},\kappa} = \bigcirc_{j=1}^{\kappa}\mathcal{E}^{m,\nu}_{\vec{c}_j,j} \tag{E30}$$

Now our goal is to bound the probability of winning $P_{\checkmark}$ if $\mathcal{Q}^{m,\nu}_{\vec{c}_{\kappa},\kappa}$ has exactly m sending channels $\mathcal{E}$, as defined in definition 3. We will consider two cases: when the channel $\mathcal{E}$ is a sending channel and when it is not.

(a) *$\mathcal{E}$ is a sending channel.* In this case the provers can output the correct state at both time steps, $\kappa-1$ and κ. Therefore, in this case we use the trivial bound that each of the fidelities is upper-bounded by 1, and

$$\frac{1}{2}\left(\bar{F}_{\nu,\vec{c}_{\kappa},\kappa}+\bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1}\right)\leqslant 1. \tag{E31}$$

(b) *$\mathcal{E}$ is not a sending channel.* Consider average fidelity expressions at time steps κ and $\kappa-1$ for the same execution i, and assume that κ is odd and output is requested at B's side. Each of the fidelities can be upper-bounded by its supremum,

$$\bar{F}_{\nu,\vec{c}_{\kappa},\kappa} = \int \mathrm{d}\psi \mathrm{Tr}\left[\mathcal{E}^{m,\nu}_{\vec{c}_{\kappa},\kappa}\circ\mathcal{Q}^{m,\nu}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^{\kappa}_{\checkmark}\right] \tag{E32}$$

$$\leqslant \sup_{\Gamma_{B_{\kappa-1},B_{\kappa}}}\int \mathrm{d}\psi \mathrm{Tr}\left[\Gamma_{B_{\kappa-1},B_{\kappa}}\left(\mathcal{E}^{m,\nu}_{\vec{c}_{\kappa},\kappa}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\right)\cdot\Pi^{\kappa}_{\checkmark}\right] \tag{E33}$$

and

$$\bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1} = \int \mathrm{d}\psi \mathrm{Tr}\left[\mathcal{Q}^{m,\nu}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right)\cdot\Pi^{\kappa-1}_{\checkmark}\right] \tag{E34}$$

$$\leqslant \sup_{\Gamma_{A_{\kappa-1}}}\int \mathrm{d}\psi \mathrm{Tr}\left[\Gamma_{A_{\kappa-1}}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\cdot\Pi^{\kappa-1}_{\checkmark}\right]. \tag{E35}$$

Here $\Gamma_{A_{\kappa-1}}$ and $\Gamma_{B_{\kappa-1},B_{\kappa}}$ denote CPTP maps which trace out additional registers of A and B and output a qubit state. Moreover, we have put $\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1} := \mathcal{Q}^{m,\nu}_{\vec{c}_{\kappa-1},\kappa-1}\left(|\psi\rangle\langle\psi|\right)$ to denote a joint state of A and B at time step $\kappa-1$.

According to definition 3 if the channel is not sending then we can bound

$$\sup_{\Gamma_{B_{\kappa-1},B_{\kappa}}}\int \mathrm{d}\psi \mathrm{Tr}\left[\Gamma_{B_{\kappa-1},B_{\kappa}}\left(\mathcal{E}^{m,\nu}_{\vec{c}_{\kappa},\kappa}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\right)\cdot\Pi^{\kappa-1}_{\checkmark}\right]\leqslant\sup_{\Gamma_{B_{\kappa-1}}}\int \mathrm{d}\psi \mathrm{Tr}\left[\Gamma_{B_{\kappa-1}}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\cdot\Pi^{\kappa}_{\checkmark}\right] \tag{E36}$$

and hence,

$$\frac{1}{2}\left(\bar{F}_{\nu,\vec{c}_{\kappa},\kappa}+\bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1}\right)\leqslant\frac{1}{2}\left(\sup_{\Gamma_{B_{\kappa-1}}}\int \mathrm{d}\psi \mathrm{Tr}\left[\Gamma_{B_{\kappa-1}}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\cdot\Pi^{\kappa-1}_{\checkmark}\right]\right.$$
$$\left.+\sup_{\Gamma_{A_{\kappa-1}}}\int \mathrm{d}\psi \mathrm{Tr}\left[\Gamma_{A_{\kappa-1}}\left(\rho^{m,\nu,\psi}_{\vec{c}_{\kappa-1},\kappa-1}\right)\cdot\Pi^{\kappa-1}_{\checkmark}\right]\right) \tag{E37}$$

The right-hand side of the above equation is bounded by $\frac{5}{6}$ due to the approximate cloning theorem [18]. Therefore, we have

$$\frac{1}{2}\left(\bar{F}_{\nu,\vec{c}_\kappa,\kappa}+\bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1}\right)\leqslant\frac{5}{6}. \tag{E38}$$

There are at most $k-m$ time steps $\kappa=1,\ldots,k$ such that the channel $\mathcal{E}$ is not sending. Therefore, using equations (E31) and (E38) we can write (E29)

$$P_{\checkmark}\leqslant\sum_\nu q_\nu\frac{1}{k}\sum_{\kappa=1}^{k}\frac{1}{|\mathsf{Cliff}|^\kappa}\sum_{\vec{c}_\kappa}\frac{\bar{F}_{\nu,\vec{c}_\kappa,\kappa}+\bar{F}_{\nu,\vec{c}_{\kappa-1},\kappa-1}}{2} \tag{E39}$$

$$\leqslant\sum_\nu q_\nu\frac{1}{k}\left(m\cdot 1+(k-m)\cdot\frac{5}{6}\right) \tag{E40}$$

$$=\frac{1}{k}\left(m+\frac{5}{6}(k-m)\right) \tag{E41}$$

where in the last line we used the fact that $\sum_\nu q_\nu=1$. □

Appendix F. Other proofs

In this appendix we present remaining proofs from section 5.3. First we prove two statements about expected value of the rate of wins and average fidelity. Then we calculate the probability that our consistency check is satisfied. Finally, we derive a bound on the performance of k-round protocols in terms of double-average fidelity.

F.1. Proof of lemma 2

Here we prove that the expected value of rate $R_{\vec{c}_\kappa,\kappa}$, for specific depth κ and string of Clifford gates $\vec{c}_\kappa$, is equal to fidelity $\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa)$ averaged over the state space.

Proof of lemma 2. By definition, the expected value of $v^i_{\vec{c}_\kappa,\kappa}$ as,

$$\mathbb{E}\left[v^i_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}}=\frac{1}{|\mathsf{X}|}\sum_\psi\left(p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}\cdot 1+p_{\text{✗}|\psi,\vec{c}_\kappa,\kappa}\cdot 0\right)=\frac{1}{|\mathsf{X}|}\sum_\psi p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} \tag{F1}$$

From the 2-design properties of set X, lemma 6, we have that

$$\mathbb{E}\left[v^i_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}}=\int \mathrm{d}\psi\, p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}=\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa) \tag{F2}$$

By linearity property of expected value,

$$\mathbb{E}\left[\sum_i v^i_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}}=\sum_i\mathbb{E}\left[v^i_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}}=\sum_i\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa)=n_{\vec{c}_\kappa,\kappa}\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa). \tag{F3}$$

And therefore,

$$\mathbb{E}\left[R_{\vec{c}_\kappa,\kappa}\right]_{\mathsf{X}}=\mathbb{E}\left[\frac{\sum_i v^i_{\vec{c}_\kappa,\kappa}}{n_{\vec{c}_\kappa,\kappa}}\right]_{\mathsf{X}}=\bar{F}_{\vec{c}_\kappa,\kappa}(\tilde{\mathcal{T}}_\kappa) \tag{F4}$$

□

F.2. Proof of lemma 3

Here we present a proof that is analogous to the previous one, and shows that expected value of rate R_κ for a fixed depth κ, is equal to double-average fidelity.

Proof of lemma 3. By definition, the expected value $\mathbb{E}\left[v^i_\kappa\right]_{\mathsf{X},\mathsf{Cliff}}$ as

$$\mathbb{E}\left[v^i_\kappa\right]_{\mathsf{X},\mathsf{Cliff}}=\frac{1}{|\mathsf{Cliff}|^\kappa}\frac{1}{|\mathsf{X}|}\sum_{C_1,\ldots,C_\kappa\in\mathsf{Cliff}}\sum_{\psi\in\mathsf{X}}\left(p_{\checkmark|\psi,\vec{c}_\kappa,\kappa}\cdot 1+p_{\text{✗}|\psi,\vec{c}_\kappa,\kappa}\cdot 0\right) \tag{F5}$$

$$=\frac{1}{|\mathsf{Cliff}|^\kappa}\frac{1}{|\mathsf{X}|}\sum_{C_1,\cdots,C_\kappa\in\mathsf{Cliff}}\sum_{\psi\in\mathsf{X}}p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} \tag{F6}$$

By 2-design properties of the Clifford set, lemma 7, we have that

$$\mathbb{E}\left[v_\kappa^i\right]_{\mathsf{X,Cliff}} = \int \mathrm{d}\psi \int C_1 \cdots \int C_\kappa \, p_{\checkmark|\psi,\vec{c}_\kappa,\kappa} = \bar{\bar{F}}(\tilde{\mathcal{T}}_\kappa). \tag{F7}$$

Since $\mathbb{E}[R_\kappa]_{\mathsf{X,Cliff}} = \frac{\sum_i^{n_\kappa} \mathbb{E}\left[v_\kappa^i\right]_{\mathsf{X,Cliff}}}{n_\kappa}$, with n_κ being a total number of executions for a fixed κ, we have that $\mathbb{E}[R_\kappa]_{\mathsf{X,Cliff}} = \bar{\bar{F}}_\kappa(\tilde{\mathcal{T}}_\kappa)$. □

F.3. Proof of corollary 2

Next, we prove that the consistency check, theorem 5, is satisfied with a certain probability, determined by the estimates on the performance of individual devices.

Proof of corollary 2. The probability that the bound (22) is satisfied is equal to probability that all the individual bounds are satisfied, i.e. $\Pr\left[\left(\bigwedge_{j=1}^{\kappa}\left(|r_{M_j^{\mathcal{T}}} - \bar{F}(\tilde{M}_j^{\mathcal{T}})| > \epsilon_{M_j^{\mathcal{T}}} \wedge |r_{C_j} - \bar{F}(\tilde{C}_j)| > \epsilon_{C_j}\right)\right)\right]$. This is equal to

$$\Pr\left[\left(\bigwedge_{j=1}^{\kappa}\left(|r_{M_j^{\mathcal{T}}} - \bar{F}(\tilde{M}_j^{\mathcal{T}})| > \epsilon_{M_j^{\mathcal{T}}} \wedge |r_{C_j} - \bar{F}(\tilde{C}_j)| > \epsilon_{C_j}\right)\right)\right] \tag{F8}$$

$$= 1 - \Pr\left[\left(\bigvee_{j=1}^{\kappa}\left(|r_{M_j^{\mathcal{T}}} - \bar{F}(\tilde{M}_j^{\mathcal{T}})| \leqslant \epsilon_{M_j^{\mathcal{T}}} \vee |r_{C_j} - \bar{F}(\tilde{C}_j)| \leqslant \epsilon_{C_j}\right)\right)\right]. \tag{F9}$$

Since $\Pr[A \vee B] \leqslant \Pr[A] + \Pr[B]$, we can write that

$$\Pr\left[\left(\bigvee_{j=1}^{\kappa}\left(|r_{M_j^{\mathcal{T}}} - \bar{F}(\tilde{M}_j^{\mathcal{T}})| \leqslant \epsilon_{M_j^{\mathcal{T}}} \vee |r_{C_j} - \bar{F}(\tilde{C}_j)| \leqslant \epsilon_{C_j}\right)\right)\right] \tag{F10}$$

$$\leqslant \sum_{j=1}^{\kappa} \Pr\left[|r_{M_j^{\mathcal{T}}} - \bar{F}(\tilde{M}_j^{\mathcal{T}})| \leqslant \epsilon_{M_j^{\mathcal{T}}}\right] + \Pr\left[|r_{C_j} - \bar{F}(\tilde{C}_j)| \leqslant \epsilon_{C_j}\right] \tag{F11}$$

$$\leqslant 2\sum_{j=1}^{\kappa}\left(\mathrm{e}^{-2n_{C_j}\epsilon_{C_j}^2} + \mathrm{e}^{-2n_{M_j^{\mathcal{T}}}\epsilon_{M_j^{\mathcal{T}}}^2}\right) \tag{F12}$$

where in the last line we used Hoeffding inequality, equations (12) and (13). Hence, we can write that $\Pr\left[\left(\bigwedge_{j=1}^{\kappa}\left(|r_{M_j^{\mathcal{T}}} - \bar{F}(\tilde{M}_j^{\mathcal{T}})| > \epsilon_{M_j^{\mathcal{T}}} \wedge |r_{C_j} - \bar{F}(\tilde{C}_j)| > \epsilon_{C_j}\right)\right)\right] \geqslant 1 - 2\sum_{j=1}^{\kappa}\left(\mathrm{e}^{-2n_{C_j}\epsilon_{C_j}^2} + \mathrm{e}^{-2n_{M_j^{\mathcal{T}}}\epsilon_{M_j^{\mathcal{T}}}^2}\right)$. □

F.4. Proof of theorem 6

Here we prove our bound on the performance of k-round protocols in terms of winning rate R_κ in test 2. The core of this theorem is the following lemma, which relates the diamond distance between the ideal and real implementation of a k-round protocol, and the double-average fidelity.

Lemma 11. *The performance of a k-round protocol can be bounded by the double-averaged fidelity in the following way*

$$\|\tilde{\mathcal{P}}^k - \mathcal{P}^k\|_\diamond \leqslant 2\sqrt{d(d+1)|\mathsf{Cliff}|^k\left(1 - \bar{\bar{F}}(\tilde{\mathcal{P}}^k)\right)} \tag{F13}$$

where d is the dimension of the underlying Hilbert space, and $|\mathsf{Cliff}|$ *is a size of the Clifford group for dimension d.*

Proof of lemma 11. To prove the inequality from lemma 11 one needs to show dependence between $\bar{F}_{\vec{g}_k}(\tilde{\mathcal{P}}^k)$ and $\bar{\bar{F}}(\tilde{\mathcal{P}}^k)$. In particular, to preserve the direction of inequality we want that $\bar{F}_{\vec{g}_k}(\tilde{\mathcal{P}}^k) \geqslant \bar{\bar{F}}(\tilde{\mathcal{P}}^k)$. Firstly, we trivially have that

$$\bar{F}_{\vec{g}_k}(\tilde{\mathcal{P}}^k) \geqslant \min_{\vec{g}_k} \bar{F}_{\vec{g}_k}(\tilde{\mathcal{P}}^k) \tag{F14}$$

On the other hand,

$$\bar{\bar{F}}(\tilde{\mathcal{P}}^k) = \int \mathrm{d}G_1 \cdots \int \mathrm{d}G_k \bar{F}_{\vec{g}_k}(\tilde{\mathcal{P}}^k) \tag{F15}$$

$$= \int \mathrm{d}C_1 \cdots \int \mathrm{d}C_k \bar{F}_{\vec{c}_k}(\tilde{\mathcal{P}}^k) \tag{F16}$$

$$= \frac{1}{|\mathsf{Cliff}|^k} \sum_{\vec{c}_k \in \mathsf{Cliff}} \bar{F}_{\vec{c}_k}(\tilde{\mathcal{P}}^k) \tag{F17}$$

$$= \frac{1}{|\mathsf{Cliff}|^k} \left(\bar{F}_{\vec{c}_k^{\min}}(\tilde{\mathcal{P}}^k) + \sum_{\vec{c}_k \neq \vec{c}_k^{\min}} \underbrace{\bar{F}_{\vec{c}_k}(\tilde{\mathcal{P}}^k)}_{\leqslant 1} \right) \tag{F18}$$

$$\leqslant \frac{1}{|\mathsf{Cliff}|^k} \bar{F}_{\vec{c}_k^{\min}}(\tilde{\mathcal{P}}^k) + 1 - \frac{1}{|\mathsf{Cliff}|^k} = 1 - \frac{1}{|\mathsf{Cliff}|^k} \left(1 - \bar{F}_{\vec{c}_k^{\min}}(\tilde{\mathcal{P}}^k)\right), \tag{F19}$$

where in lines (F16) and (F17) we used lemma 7, and in line (F18) we separated the minimum element out of the summation and in line (F19) we bounded each element under the sum by 1.

Now let us relate the minimum over the Clifford group to a minimum over the whole unitary group. Note that the Clifford group rotated by any unitary $\mathcal{U}$ remains a Clifford group. Therefore, let us rotate every C_j by a constant $\mathcal{U}_j$, $j = 1, \ldots, k$, such that the minimum over the Clifford sets corresponds to the minimum over the whole unitary group. Let us write $\vec{u}_k = \mathcal{U}_1, \cdots, \mathcal{U}_k$,

$$\bar{F}_{\vec{u}_k \vec{c}_\kappa^{\min}}(\tilde{\mathcal{P}}^k) = \min_{\vec{g}_k} \bar{F}_{\vec{g}_k}(\tilde{\mathcal{P}}^k). \tag{F20}$$

We obtain

$$\bar{\bar{F}}(\tilde{\mathcal{P}}^k) \leqslant 1 - \frac{1}{|\mathsf{Cliff}|^k} \left(1 - \min_{\vec{g}_k} \bar{F}_{\vec{g}_k}(\tilde{\mathcal{P}}^k)\right) \tag{F21}$$

and so

$$\|\tilde{\mathcal{P}}^k - \mathcal{P}^k\|_\diamond \leqslant 2\sqrt{d(d+1)} \sqrt{|\mathsf{Cliff}|^k \left(1 - \bar{\bar{F}}(\tilde{\mathcal{P}}^k)\right)}. \tag{F22}$$

□

Now we will relate the double-average fidelity of a k-round protocol to the double-average fidelity of the test. Indeed, we will show that these quantities are equal.

Lemma 12. *Double-averaged fidelity of a k-round protocol $\tilde{\mathcal{P}}^k$ of depth k is equal to double averaged fidelity of the test $\tilde{\mathcal{T}}_\kappa$ of the same depth, $\kappa = k$,*

$$\bar{\bar{F}}(\tilde{\mathcal{P}}^k) = \bar{\bar{F}}(\tilde{\mathcal{T}}_\kappa) \tag{F23}$$

Proof. As stated in the main text, the proof of this lemma follows from noticing that the expression for double-averaged fidelity contains only polynomials of degree 2 in every Clifford gate C_j. Therefore, here averaging over the Clifford group is equivalent to averaging over the entire unitary group, since the Clifford group forms a 2-design. Furthermore, the equality is possible, since we have put $M_j^{\mathcal{T}} \equiv M_j \circ \mathcal{E}_j$, and $M_j^{\mathcal{T}}$ encompasses operations associated with sending and storing the qubit. □

The above two lemmas, combined with the Hoeffding bound on R_κ, equation (21) complete the proof theorem 6.

Appendix G. Q-qubit protocols

In this section we provide a description of a Q-qubit extension of our class of protocols. The structure of our description is exactly the same as the one from section 3.2 with the difference that all the operations are carried out on more than one qubit.

In a Q-qubit k-round protocol nodes have a total of Q qubits available. At each round $j = 1, \ldots, k$ of the protocol nodes A and B can send any subset of the local qubits to one another. We denote all of the sending operations in round j by $\mathcal{E}_j$. Moreover, the nodes can store local qubits in the quantum memory

and apply local gates. We denote these operations by $M_{A_j}^{(q_j)}$ and $G_{A_j}^{(q_j)}$ for node A, and $G_{B_j}^{(Q-q_j)}$ and $M_{B_j}^{(Q-q_j)}$ for node B. Here q_j and $Q-q_j$ denote the number of local qubits at A or B's side at round j, respectively, *after* the sending operation $\mathcal{E}_j$. Therefore, we describe a Q-qubit k-round protocol can with a map

$$\mathcal{P}^{k,(Q)} = \bigcirc_{j=1}^{k} \left[\left(G_{A_j}^{(q_j)} \circ M_{A_j}^{(q_j)} \right) \otimes \left(G_{B_j}^{(Q-q_j)} \circ M_{B_j}^{(Q-q_j)} \right) \circ \mathcal{E}_j \otimes \right. \tag{G1}$$

In the presence of noise, we assume the following noise model for Q-qubit k-round protocols:

- The noise on gates is independent of the applied gate;
- The noise from memories, gates and transmission channels acts individually on each qubit;
- For each round j, the qubits are submitted to the same kind of noise on node A and node B (noise can differ from round to round).

Formally, we assume the following

$$\begin{aligned} \tilde{M}_{A_j}^{(q_j)} &= \tilde{M}_j^{\otimes q_j}, \quad \tilde{M}_{B_j}^{(Q-q_j)} = \tilde{M}_j^{\otimes Q-q_j} \\ \tilde{G}_{A_j}^{(q_j)} &= G_{A_j}^{(q_j)} \circ N_j^{\otimes q_j}, \quad \tilde{G}_{B_j}^{(Q-q_j)} = G_{B_j}^{(q_j)} \circ N_j^{\otimes Q-q_j} \end{aligned} \tag{G2}$$

A bipartite Q-qubit, k-round protocol between any two nodes A and B consists of the following operations:

(a) Local preparation of Q perfect qubit states, $|\psi\rangle_A \in \mathbb{D}(\mathcal{H}_A^{\otimes q})$ and $|\psi\rangle_B \in \mathbb{D}(\mathcal{H}_B^{\otimes Q-q})$. Here the superscript denotes the number of qubits on A's or B's side.

(b) Sending any subset of local qubits from node A to node B and vice versa. We denote all exchanging of qubits in a round j by $\mathcal{E}_j$

(c) Storing all local qubits, $M_A^{(q)} = M_A^{\otimes q}$, where $M_A \in U(\mathcal{H}_A)$, and $M_B^{(Q-q)} = M_A^{\otimes Q-q}$, where $M_B \in U(\mathcal{H}_B)$. Again, the superscript denotes the number qubits on A or B's side. Storage can take up to kt_M, where t_M is time necessary for creating one EPR pair and communicating classically between two most distant nodes. A noisy memory is denoted by a tilde, $\tilde{M}_A^{(q)}$ and accordingly for B.

(d) Applying an arbitrary local operation by any node on any subset of local qubits. We describe this operation by a unitary gate $G_A^{(q)} \in U(\mathcal{H}_A^{\otimes q})$ and $G_B^{(Q-q)} \in U(\mathcal{H}_A^{\otimes Q-q})$. $\tilde{G}_A^{(q)} = G_A^{(q)} \circ N_A^{(q)}$ denotes the noisy counterpart, where $G_A^{(q)}$ is a perfect gate and $N_A^{(q)} = N_A^{\otimes q}$ is a noise map independent of the applied gate. Similarly for gates on B's side. Applying any gate takes a known finite time $\ell \ll t_M$.

(d) Local measurement of all local qubits at the end of the protocol, $\Pi_A^{(q)} \in \mathrm{Proj}(\mathcal{H}_A^{\otimes q})$ and $\Pi_B^{(Q-q)} \in \mathrm{Proj}(\mathcal{H}_B^{\otimes Q-q})$. As stated before, we assume that the measurement can be performed perfectly.

Steps (b)–(d) are performed in rounds $j = 1, \cdots, k_{\mathcal{P}}$ a total of k times. We denote memories and gates that are used by A and B at a jth round by $M_{A_j}^{(q_j)}$, $\tilde{G}_{A_j}^{(q_j)}$ and $M_{B_j}^{(Q-q_j)}$, $\tilde{G}_{B_j}^{(Q-q_j)}$ respectively. Such a protocol operates on a total number of Q qubits. Note that we model noise map as a product for each of Q qubits.

Definition 15 (k-round protocols). Let $\mathcal{H}^{\otimes Q}$ be the Hilbert space of a two-partite quantum network. We define a k-round protocol as a CPTP map of the form $\Pi^{(Q)} \circ \tilde{\mathcal{P}}^{k,(Q)} \circ \mathrm{Prep}^{(Q)}$, where:

- $\mathrm{Prep}^{(Q)}$ corresponds to preparation of Q local qubits $|\psi\rangle_A \in \mathbb{D}(\mathcal{H}_A^{\otimes q_1})$ and $|\psi\rangle_B \in \mathbb{D}(\mathcal{H}_B^{\otimes Q-q_1})$ (step (a)).
- $\tilde{\mathcal{P}}^{k,(Q)}$ is a map describing k rounds of local operations—memories and gates, as well as sending qubits from A to B (steps (b)–(d)),

$$\tilde{\mathcal{P}}^{k,(Q)} = \bigcirc_{j=1}^{k_{\mathcal{P}}} \left[\left(\tilde{G}_{A_j}^{(q_j)} \circ M_{A_j}^{(q_j)} \right) \otimes \left(\tilde{G}_{B_j}^{(Q-q_j)} \circ M_{B_j}^{(Q-q_j)} \right) \right] \circ \mathcal{E}_j. \tag{G3}$$

- $\Pi_A^{(q)} \otimes \Pi_B^{(Q-q)}$ is a local measurement of all the local qubits. (step (e))

Now let us describe a test that certifies the above functionality. It is a straightforward extension of the ping-pong test we have discussed before. The idea of the Q-qubit teleportation-based ping-pong test is

instead of teleporting a single qubit, to teleport all Q qubits back and forth between nodes A and B and sample a random Q-qubit Clifford gate ($\mathsf{Cliff}(2^Q)$) at line 3: of test 2. The initial state of Q qubits $|\psi\rangle\langle\psi|^{(Q)}$ is chosen uniformly at random from a 2-design of Q-qubit states. In this case the test can be described with a map

$$\mathcal{T}^{\kappa,(Q)} = \bigcirc_{j=1}^{\kappa} C_j^{(Q)} \circ M_j^{\mathcal{T}(Q)}, \tag{G4}$$

where, as before, the parity of j indicates on which side all the qubits are, and $M_j^{\mathcal{T}(Q)} \equiv M_j^{(Q)} \circ \mathcal{E}_j$ accounts for operations associated with transmission (here teleportation). Note that $M_j^{\mathcal{T}(Q)}$ can still be written in the product form, i.e. acting individually on each qubit, since we have assumed that $M_j^{(Q)}$ and $\mathcal{E}_j$ are both in the product form. Therefore, in the presence of noise, we employ the same model as for k-round Q-qubit protocols, i.e. $\tilde{M}_j^{\mathcal{T}(Q)} = (\tilde{M}_j^{\mathcal{T}})^{\otimes Q}$ and $\tilde{C}_j^{(Q)} = C_j^{(Q)} \circ N_j^{\otimes Q}$.

Based on the average fidelity estimate of this test $r(\tilde{\mathcal{T}}^{\kappa,(Q)})$ one can, again, check whether memories and gates were used together by satisfying an analog of the bound (22). This can be done provided one has access to estimates of quality of memories $\bar{F}(\tilde{M}_j^{(Q)}) = \int \mathrm{d}\psi^{(Q)} \mathrm{Tr}\left[(\tilde{M}_j^{\mathcal{T}})^{\otimes Q}(|\psi\rangle\langle\psi|^{(Q)}) \cdot |\psi\rangle\langle\psi|^{(Q)}\right]$ and gates $\bar{F}(N_j^{(Q)}) = \int \mathrm{d}\psi^{(Q)} \mathrm{Tr}\left[N_j^{\otimes Q}(|\psi\rangle\langle\psi|^{(Q)}) \cdot |\psi\rangle\langle\psi|^{(Q)}\right]$, for all j. Note that here we necessarily use the fidelity of $\tilde{M}_j^{(Q)}$ and $N_j^{(Q)}$ evaluated on the space of all Q-qubit states.

Now we can extend theorem 6 onto Q-qubit protocols using the noise assumptions on the class of protocols. We arrive at the following statement.

Theorem 7 (Bounding the behavior of $Q-$ qubit $k-$ round protocols). *Given the noise model is the same for all Q qubits at each round j, the performance of any Q-qubit Q-qubit k-round protocol, can be bounded in terms of an estimate for the double-averaged fidelity $R(\tilde{\mathcal{T}}^{\kappa,(Q)})$ of the Q-qubit test in the following way*

$$\begin{aligned} &\|\tilde{\mathcal{P}}^{k,(Q)} - \mathcal{P}^{k,(Q)}\|_{\diamond} \\ &\leqslant 2\sqrt{d(d+1)} \sum_{\kappa} \sqrt{|\mathsf{Cliff}(d)|^{\kappa}\left(1 - R(\tilde{\mathcal{T}}^{\kappa,(Q)})\right)} \end{aligned} \tag{G5}$$

where $d = 2^q$ is the dimension of the underlying Hilbert space, and $|\mathsf{Cliff}(d)|$ is a size of the Clifford group for dimension d.

The proof of that statement is analogous to the single-qubit case, with the difference that here one uses the properties of the unitary 2-design given by the Clifford group of dimension 2^Q.

ORCID iDs

Victoria Lipinska https://orcid.org/0000-0003-0760-861X

References

[1] Bennett C H and Brassard G 2014 *Theor. Comput. Sci.* **560** 7
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Wehner S, Elkouss D and Hanson R 2018 *Science* **362** 6412
[4] Chuang I L and Nielsen M A 1997 *J. Mod. Opt.* **44** 2455
[5] Poyatos J F, Cirac J I and Zoller P 1997 *Phys. Rev. Lett.* **78** 390
[6] Merkel S T, Gambetta J M, Smolin J A, Poletto S, Córcoles A D, Johnson B R, Ryan C A and Steffen M 2013 *Phys. Rev.* A **87** 062119
[7] Blume-Kohout R, Gamble J K, Nielsen E, Mizrahi J, Sterk J D and Maunz P 2013 (arXiv:1310.4492)
[8] Emerson J, Alicki R and Życzkowski K 2005 *J. Opt. B: Quantum Semiclass. Opt.* **7** S347
[9] Knill E, Leibfried D, Reichle R, Britton J, Blakestad R B, Jost J D, Langer C, Ozeri R, Seidelin S and Wineland D J 2008 *Phys. Rev.* A **77** 012307
[10] Magesan E, Gambetta J M and Emerson J 2011 *Phys. Rev. Lett.* **106** 180504
[11] Pfister C, Rol M A, Mantri A, Tomamichel M and Wehner S 2018 *Nat. Commun.* **9** 27
[12] Montanaro A and de Wolf R 2016 A Survey of Quantum Property Testing *Theory of Computing* (Graduate Surveys) vol 7 p 1
[13] Bancal J-D, Redeker K, Sekatski P, Rosenfeld W and Sangouard N 2018 arXiv:1812.09117 [quant-ph]
[14] Reichardt B W, Unger F and Vazirani U 2013 *Nature* **496** 456
[15] Mahadev U 2018 *2018 IEEE 59th Annual Symp. on Foundations of Computer Science*
[16] Vidick T and Watrous J 2016 *Quantum Proofs* DOI: 10.1561/0400000068
[17] Wootters W K and Zurek W H 1982 *Nature* **299** 802
[18] Gisin N and Massar S 1997 *Phys. Rev. Lett.* **79** 2153
[19] Hoeffding W 1963 *J. Am. Stat. Assoc.* **58** 13
[20] Dugas A C, Wallman J J and Emerson J 2016 (arXiv:1610.05296)
[21] Watrous J 2018 *The Theory of Quantum Information* (Cambridge: Cambridge University Press)

[22] Wallman J J and Flammia S T 2014 *New J. Phys.* **16** 103032
[23] Goldenberg L, Vaidman L and Wiesner S 1999 *Phys. Rev. Lett.* **82** 3356
[24] Nebe G, Rains E M and Sloane N J A 2001 *Des. Codes Cryptogr.* **24** 99
[25] Boykin P O, Mor T, Pulver M, Roychowdhury V and Vatan F 1999 (arXiv:quant-ph/9906054)
[26] Roy A and Scott A J 2009 *Des. Codes Cryptogr.* **53** 13
[27] Gross D, Audenaert K and Eisert J 2007 *J. Math. Phys.* **48** 052104
[28] Nielsen M A 2002 *Phys. Lett.* A **303** 249