




Nondestructive verification of entangled states via fidelity witnessingFerran Riera-Sàbat ^{*}, Jorge Miguel-Ramiro ^{*}, and Wolfgang Dür *Universität Innsbruck, Institut für Theoretische Physik, Technikerstraße 21a, 6020 Innsbruck, Austria*

(Received 12 October 2022; accepted 23 January 2023; published 10 February 2023)

Assessing the quality of an ensemble of noisy entangled states is a central task in quantum information processing. Usually, this is done by measuring and hence destroying multiple copies, from which state tomography or fidelity estimation can be employed to characterize states. Here we propose several methods to directly distinguish between two different sets of states, e.g., if their fidelity is above or below a certain threshold value. This turns out to be significantly more efficient and importantly keeps the verified states intact. We make use of auxiliary entanglement or an ensemble of larger size, where we operate on the whole ensemble, but measure only a small fraction where information has been concentrated. For certain state families, we demonstrate that such an approach can even outperform optimal methods that collectively measure directly a fixed fraction of the ensemble.

DOI: [10.1103/PhysRevA.107.022414](https://doi.org/10.1103/PhysRevA.107.022414)**I. INTRODUCTION**

Quantum entanglement is the key resource for multiple applications in quantum technology, including quantum communication and cryptography [1,2], quantum networks [3–5], distributed computation [6–8], and distributed sensing [9–11]. However, in any realistic scenario channels and devices are imperfect, and resulting states will be noisy. Assessing whether the quality of produced or maintained entangled states is sufficient for the desired application is hence a central task for all these applications.

The typical approach to determine the quality of an ensemble of mixed states is to perform local measurements on some individual copies, from which features of the states can be assessed. Multiple strategies for certifying entangled states have been proposed [12–16]. The approaches differ in the amount of information learned from the states, which is generally related to the amount of resources spent in the process. The existing strategies range from a complete characterization of the states via state tomography [17,18], to the learning of some specific properties such as the fidelity as in fidelity estimation [19]. In this work we consider a still less information-demanding problem, consisting in determining whether the fidelity of an entangled state is above or below a certain threshold value, a natural and realistic extension of the state verification problem [20–26]. We denote this decision problem as fidelity witnessing, which can be relevant in multiple scenarios, whenever it suffices to know if the quality of the states of an ensemble is large enough to perform the desired task. For instance, in a communication scenario, the fidelity directly indicates the error rate of transmitted quantum information via teleportation, but also if the states can be used to expand a secure secret key. The main advantage of such an

approach lies in the reduced required resources as compared to schemes that acquire more information.

Here, in contrast to many previous approaches [15,25], we assume that we have access to the whole ensemble, and not just individual copies that are processed locally and individually, and also consider entanglement-assisted protocols. While this poses additional experimental challenges, we find that these approaches have significant advantages: First, they are more efficient and can lead to up to exponential enhancements as compared to previous schemes, even outperforming optimal, nonlocal methods that measure all states from an ensemble of fixed size. Second, certified states are not destroyed; the remaining states are directly certified, without the necessity to assume a tensor product structure of the initial ensemble. The key element is an information transfer from multiple copies of the states in the ensemble to a certain subset, or to some auxiliary entangled states, where only these few copies are subsequently measured and hence destroyed. In this way, a much larger fraction of an ensemble can be left intact, while still deciding if the remaining states are suitable for the desired application. We also take care of properly accounting for additional entanglement resources, by relating auxiliary entanglement to the required number of noisy copies.

We introduce three different protocols, which are compared with the typically considered case of sequential measurements of single copies of identical, noisy entangled states $\rho^{\otimes n}$. We propose strategies that rely on collective operations which allow us to transfer information about the noise of several copies into a few auxiliary state(s), in the spirit of [27,28]. By partially or completely measuring the auxiliary system(s), one can access the information of the accumulated noise with increased efficiency, in such a way that the copies that are certified are not consumed in the process. We make use of this powerful tool and introduce several approaches, each of which works better in specific situations. To this aim we consider different state families, including noisy

*These authors contributed equally to this work.

ensembles that result from maximally entangled states affected by decay noise, phase-flip noise, or depolarizing noise, mimicking relevant situations such as distributing entanglement through noisy channels or storing entangled states for some time in an imperfect quantum memory. The main findings can be summarized as follows:

(i) We introduce three different protocols for the decision problem of distinguishing between two state families of noisy entangled states with respect to their fidelity.

(ii) We demonstrate that auxiliary entanglement can be used to increase the performance of this task.

(iii) We show that collective but local operations performed on the whole ensemble can be used to transfer and concentrate information into a few copies, thereby significantly reducing the number of states that need to be measured and hence destroyed, while maintaining more and fully certified states.

(iv) We find that for decay noise, our protocols perform exponentially better than optimal, global, and collective strategies that only operate on ensembles of a fixed size where all states are measured.

The paper is organized as follows. We review some basic concepts and operations in Sec. II, while the problem setting is formally defined in Sec. III. In Sec. IV we introduce the different strategies we propose to solve the fidelity witnessing problem, where we also analyze and compare their efficiency and performance. Finally, we present some concluding remarks in Sec. VI.

II. BACKGROUND

We discuss here the basic notions and operations we make use of throughout this work.

A. Maximally entangled states

Bell states. Bell states are maximally entangled quantum states shared by two qubits. The set of Bell states form a basis of $\mathbb{C}_A^2 \otimes \mathbb{C}_B^2$ given by the elements

$$|\Psi_{ij}\rangle_{AB} \equiv \mathbb{1} \otimes \sigma_x^j \sigma_z^i \left(\frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}} \right),$$

where $i, j \in \{0, 1\}$ and σ_k is the k th Pauli operator. These states are a fundamental resource for multiple applications such as, e.g., superdense coding [29], quantum teleportation [30,31], quantum key distribution (QKD) [1,2], or distributed quantum computation [6,7].

Higher-dimensional maximally entangled states. Qudits are natural extensions of qubit systems for d -dimensional systems. A bipartite system of qudits is associated with the Hilbert space $\mathcal{H}_{AB} = \mathbb{C}_A^d \otimes \mathbb{C}_B^d$, where we can define an orthonormal basis of maximally entangled states of the form [30]

$$|\Phi_{mn}^d\rangle_{AB} \equiv \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{i2\pi km/d} |k\rangle_A |k \ominus n\rangle_B, \quad (1)$$

where $m, n \in \mathbb{Z}_d$ are called the phase and amplitude index of the state, respectively, and where $k \ominus n \equiv (k - n) \bmod d$ and d is the dimension of the qudit systems.

B. Fidelity of quantum states

The fidelity of two quantum states ρ, σ is a measure of how close the two states are, with respect to the probability of identifying one as the other with an optimal measurement. Formally, it is defined as

$$F = \left[\text{tr} \sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} \right]^2. \quad (2)$$

We use fidelity as a natural figure of merit to measure the amount of noise affecting a quantum state. Since we mainly deal with maximally entangled states, the fidelity in our case refers to the distance between some state ρ and the maximally entangled state $|\Psi_{00}\rangle$, such that Eq. (2) reduces to $F = \langle \Psi_{00} | \rho | \Psi_{00} \rangle$.

C. Families of states

We introduce here the different families of states we make use of throughout this work as probe states to be verified or witnessed. All of them correspond to dominant noise processes relevant in many physical scenarios.

1. Bell diagonal states

Any arbitrary bipartite mixed state ρ can be always depolarized into a state diagonal in the Bell basis with local operations. This is achieved by implementing a quantum map with Kraus operators $\mathcal{D}_{\text{BD}} = \{\frac{1}{2} \sigma_i \otimes \sigma_i\}_{i=0}^3$, i.e.,

$$\begin{aligned} \mathcal{D}_{\text{BD}}: \rho &= \sum_{i_1, j_1, i_2, j_2=0}^1 \alpha_{i_1 j_1 i_2 j_2} |\Psi_{i_1 j_1}\rangle \langle \Psi_{i_2 j_2}| \\ \mapsto \rho_{\text{BD}} &= \sum_{i, j=0}^1 \alpha_{ijij} |\Psi_{ij}\rangle \langle \Psi_{ij}|. \end{aligned}$$

Note that the fidelity of the state remains unchanged.

2. Werner states

Further depolarization is possible by making all but one of the diagonal elements equal and transforming the state into a Werner state [32], i.e.,

$$\rho_w = q |\Psi_{00}\rangle \langle \Psi_{00}| + \frac{1-q}{4} \mathbb{1}_4, \quad (3)$$

while keeping the fidelity $F = (3q + 1)/4$ unchanged. This is accomplished by suitable twirling techniques (see, e.g., [33]), i.e.,

$$\mathcal{D}_w: \rho \mapsto \int (U \otimes U) \rho (U \otimes U)^\dagger dU = \rho_w,$$

where dU is the Haar measure. Depolarization can also be achieved using only local operations drawn from a discrete set [34]. Werner state can be conceived as the worst case in terms of the noise of the states, where with some probability no information about the state is left.

3. Dephasing-type states

A less general family of states is given by rank-2 Bell diagonal states. These states are local unitary (LU) equivalent

to a Bell state, where one of the parties is affected by a bit-flip noise, i.e.,

$$\begin{aligned} & \mathbb{1} \otimes \mathcal{N}_F: |\Psi_{00}\rangle\langle\Psi_{00}| \\ & \mapsto \rho_d = F|\Psi_{00}\rangle\langle\Psi_{00}| + (1-F)|\Psi_{10}\rangle\langle\Psi_{10}|, \end{aligned} \quad (4)$$

where $\mathcal{N}_p = \{\sqrt{p}\mathbb{1}, \sqrt{1-p}Z\}$. Notice that states resulting from local dephasing noise are formally equivalent, where both qubits may be affected by Pauli σ_z noise. This kind of noise is relevant, e.g., when there are fluctuating fields or phase references.

4. Amplitude-damping-type states

A different class of states corresponds to amplitude-damping type. These states are the result of sending each party of a perfect Bell state $|\Psi_{11}\rangle$ through an amplitude damping channel with Kraus operators $\mathcal{A}_p = \{|0\rangle\langle 0| + \sqrt{p}|1\rangle\langle 1|, \sqrt{1-p}|0\rangle\langle 1|\}$ [35], i.e.,

$$\begin{aligned} & \mathcal{A}_F \otimes \mathcal{A}_F |\Psi_{11}\rangle\langle\Psi_{11}| \\ & \mapsto \rho = F|\Psi_{11}\rangle\langle\Psi_{11}| + (1-F)|00\rangle\langle 00|, \end{aligned}$$

where the state is LU equivalent to

$$\rho_a = F|\Psi_{00}\rangle\langle\Psi_{00}| + (1-F)|01\rangle\langle 01|. \quad (5)$$

This kind of state is relevant in scenarios where one describes decay processes of, e.g., atoms in a quantum memory.

D. Counter gate

In several of the strategies introduced in this work, we make use of a quantum gate introduced in [27,36] which allows us to transfer information from an ensemble of entangled qubit states into a higher-dimensional entangled state by means of local operations. The so-called counter gate [27,36] is a bilateral qubit-qudit controlled operation that takes a two-dimensional entangled state as control and a d -dimensional entangled state as a target. Given a target system consisting of a maximally entangled state with phase index zero [see Eq. (1)], its action is given by

$$bCX_{1 \rightarrow 2}^{AB} |mn\rangle_1 |\Phi_{0j}^d\rangle_2 = |mn\rangle_1 |\Phi_{0,j \oplus m \oplus n}^d\rangle_2, \quad (6)$$

where $|mn\rangle$ are the computational basis states, $bCX_{1 \rightarrow 2}^{(d)} = CX_{1 \rightarrow 2}^{A_1 A_2} \otimes CX_{1 \rightarrow 2}^{B_1 B_2}$, and

$$CX_{1 \rightarrow 2} = |0\rangle\langle 0| \otimes \mathbb{1}_d + |0\rangle\langle 1| \otimes X_d$$

is the hybrid *controlled-X* gate [37], where the action of X_d in the computational basis is given by $X_d|k\rangle = |k \oplus 1\rangle$. We denote as type-1, type-2, and type-3 error states the states corresponding to $|01\rangle$, $|10\rangle$, and $|\Psi_{10}\rangle$, respectively. The action of the counter gate taking a type-1 (-2) error state acting as control leads to an amplitude index value of the auxiliary state increased (decreased) by one, whereas it is left invariant for the type-3 error state.

We denote the operation consisting in applying the counter gate, Eq. (6), from each of the states of an ensemble of n copies into a d -dimensional auxiliary state, as error number gate (ENG), i.e.,

$$\text{ENG} = \prod_{k=1}^n bCX_{k \rightarrow \text{aux}}. \quad (7)$$

The name is motivated by the action of the gate on ensembles with only $|01\rangle$ error states, where the number of error states in the ensemble can be determined in this way.

E. Entanglement cost and relation to resources

In this work, we consider entanglement-assisted protocols that make use of (small) amounts of extra entanglement. In order to make a comparison with protocols that only measure states directly, we need to relate these entangled states with the states of the noisy ensemble. First, we point out that the amount of entanglement that is contained in a noiseless Bell state constitutes the basic unit of bipartite entanglement, usually denoted as *ebit* of entanglement. The number of ebits contained in a maximally entangled state of dimension d is given by $E(|\Phi_{00}^d\rangle) = \log_2 d$. Therefore, in an ensemble of n maximally entangled states the number of ebits is given by $E(|\Phi_{00}^d\rangle^{\otimes n}) = n \log_2 d$.

The evaluation of the amount of entanglement, in terms of the number of ebits, contained in mixed states is, however, not clear. The distillable entanglement E_D [38], i.e., the fraction of maximally entangled states that can be distilled from many noisy copies by means of local operations and classical communication is a suitable entanglement measure in this context. It tells us that from m noisy copies of the state ρ , one can generate mE_D ebits of entanglement. This provides the desired relation between noisy copies and ebits. However, E_D is hard to compute in general, and only some upper bounds [39,40] and lower bounds [41] are known. Here we make use of reachable lower bounds provided by entanglement purification protocols [34,40,42,43]. We compute the yield Y of a combination of the recurrence protocol [42] and hashing [40], i.e., the fraction maximally entangled states over initial noisy states, which is a lower bound for E_D [44]. While the recurrence protocol allows one to increase the fidelity of remaining pairs, hashing is only applicable for sufficiently high fidelities, but has a nonzero yield. Both protocols operate on states diagonal in the Bell basis, where any state can be transformed to such form as discussed above. The yield of the hashing protocols for Bell diagonal states ρ_{BD} is given by $[1 - S(\rho_{\text{BD}})]$, and one can obtain a smooth curve as a function of the initial fidelity F by mixing strategies, i.e., consider a mixture of states resulting from a certain number of rounds of the recurrence protocol, and apply Hashing to the resulting one.

So whenever auxiliary entanglement of m ebits is required, we assume that it is generated from the noisy ensemble by consuming $\lceil m/Y \rceil$ states from the ensemble, where Y is the yield of the entanglement purification protocol. Notice that we do not optimize over entanglement purification protocols, so we provide a conservative bound, thereby underestimating the operational advantage of entanglement-assisted protocols.

III. PROBLEM SETTING

Quantum state certification and verification have been studied and analyzed in different directions, ranging from learning more information about a state, as in state tomography, to less information as in fidelity estimation. The problems we study here are closely related to quantum state verification of

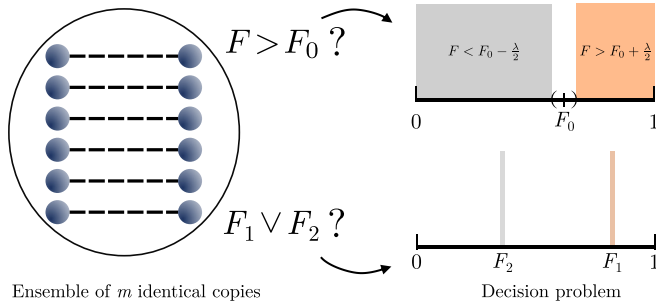


FIG. 1. Fidelity witnessing (upper right) and fidelity discrimination (lower right) problems. Given an ensemble of identical copies $\rho^{\otimes n}$, with some unknown local fidelity F (i.e., the fidelity of each copy, corresponding to their reduced density operator), the task of fidelity witnessing is to determine whether the fidelity is below or above certain threshold F_0 up to some additive error λ . Similarly, if there exists the promise that the ensemble states fidelity is either F_1 or F_2 , the task of fidelity discrimination reduces to deciding which of the two cases is present.

entangled states [13–15,28,45], where the task is to verify whether some ensemble of entangled states consisting of n identical copies is indeed maximally entangled. In terms of the fidelity of the states, state verification solves the problem of deciding whether the fidelity of the states is $F = \langle \Psi_{00} | \rho | \Psi_{00} \rangle = 1$ or not (i.e., $F \leq 1 - \epsilon$).

The problems we analyze enclose more realistic situations [13–15,25], where a certain level of noise is in general unavoidable, and therefore entangled states cannot be strictly verified with previous methods. The task reduces to a decision problem of determining whether the fidelity of an entangled state is above or below some threshold value, or corresponds to one out of two possible values. We define and analyze these two closely related problems, denoted as fidelity witnessing and fidelity discrimination (see Fig. 1).

Notice that it is not required to learn the actual value of F to solve the underlying decision problem which essentially requires only learning one bit of information. This learning of a minimum amount of information can be enough and useful in many contexts and applications, for which the parties sharing the entanglement just require a minimum fidelity of the states to operate. In contrast to other methods, e.g., fidelity estimation or state tomography, fidelity witnessing and fidelity discrimination have the benefit of a significant reduction in the amount of consumed resources. We construct strategies that avoid measuring and hence destroying copies of the state in order to obtain information about it. As we show later, directly measuring copies of the state generally provides additional information that is not required to solve the witnessing problem, making such a strategy wasteful in terms of the required resources.

We consider an ensemble of identical copies of some noisy state, i.e., $\rho^{\otimes n}$, where we can collectively operate on the copies in a local way. All the strategies we propose and analyze rely on the only use of local operations, such that each state is not accessible or operated in a global way. We remark that our approaches do not only restrict to ensembles of the form $\rho^{\otimes n}$, but may also be extended to work with, e.g., non-IID ensemble states.

Fidelity witnessing. The witnessing problem consists in determining, with only the assistance of local operations and classical communication, if the fidelity of a certain noisy entangled state ρ is above or below a specific threshold value F_0 , i.e., $F > F_0 + \frac{\lambda}{2}$ or $F < F_0 - \frac{\lambda}{2}$, up to some additive error λ (see Fig. 1). This problem has been partially analyzed in the context of extending quantum state verification to more realistic settings [20–25].

Observe that there exist four different regimes or scenarios that need to be analyzed with any approach. On the one hand, if a protocol output determines that the fidelity is below the threshold, there is some probability of succeeding, i.e., the fidelity is actually below, or failing. Analogously, the other two regimes consist of the protocol determining that the fidelity is above and being right or failing. Each strategy we analyze can exhibit better performance, sometimes tunable, on some of these regimes at the expense of the others.

Fidelity discrimination. We also analyze a slightly modified problem, denoted as fidelity discrimination. Given an ensemble of identical entangled states shared by parties A and B , with the promise that the fidelity of the states is either F_1 or F_2 , with $F_1 > F_2$, the task is to discern which of the two fidelities correspond to the ensemble copies by consuming the minimum number of states (see Fig. 1). Since this task also entails a decision problem with simpler promises, all the protocols we introduce in the following are directly applicable with, in general, enhanced efficiency. In particular, the blocking strategy (protocol P3, see below) allows us to overcome optimal bounds in solving the fidelity discrimination problem.

IV. FIDELITY WITNESSING STRATEGIES

We propose different approaches to solve the fidelity witnessing and discrimination problems for ensembles of identical bipartite entangled states. While the most direct approach, a direct extension of strategies applied in fidelity estimation and verification [19,45], relies on a copy-by-copy measurement of a certain part of the ensemble, the remaining approaches make use of different tools in order to transfer information about the noise of the ensemble into auxiliary registers without destroying the original copies. The auxiliary registers are subsequently manipulated to extract the required information and solve the decision problems.

We remark that the protocols we introduce are suited for different state families. While protocol P0 (individual measurements) and P3 (blocking strategies) are suitable for all families, the error-counting protocol P1 and the coarse-graining protocol P2, are essentially only applicable to states of the form ρ_a resulting from decay or amplitude damping.

A. Protocol P0: Individual measurements

Reference [25] discusses how to perform fidelity witnessing by extending the strategy for verification of Bell states. In state verification [20–26], an arbitrary noisy ensemble is given and one aims to distinguish between either the states being perfect, i.e., $\rho = |\Psi_{00}\rangle\langle\Psi_{00}|$, or being noisy up to some fidelity, i.e., $\langle\Psi_{00}|\rho|\Psi_{00}\rangle \leq 1 - \epsilon \equiv F$. The optimal solution in this case consists in performing random copy-by-copy and local two-outcome measurements [see Fig. 2(a)], given by

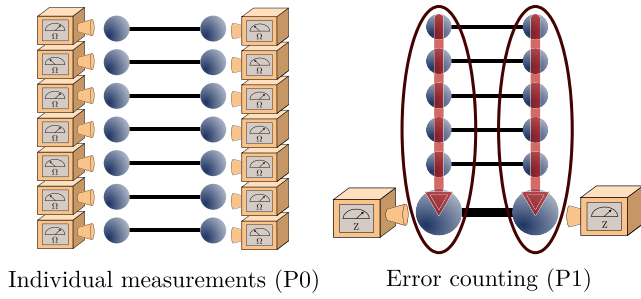


FIG. 2. (a) Schematic representation of the individual measurements protocol P0, which consists in individually measuring each of the copies. (b) An illustrative description of the underlying idea behind the strategies we introduce P1, P2, and P3, where some information of the ensemble is transferred into an auxiliary state that is then manipulated to learn the required information without destroying the verified ensemble copies.

$\{\Omega_i, \mathbb{1} - \Omega_i\}$, such that

$$\Omega_i |\Psi_{00}\rangle = |\Psi_{00}\rangle,$$

where the label “pass” (“fail”) is assigned to the outcome corresponding to Ω_i ($\mathbb{1} - \Omega_i$). The measurement can then be described by

$$\Omega = \sum_i p_i \Omega_i,$$

where $\{p_i\}$ is a probability distribution. The probability that one state passes the measurement test is given by

$$p = 1 - \epsilon \nu(\Omega),$$

where $\nu(\Omega)$ is the spectral gap between the largest and the second largest eigenvalues of Ω . Therefore, for an unknown state ρ the optimal strategy is such that maximizes $\nu(\Omega)$. For Bell states $|\Psi_{00}\rangle$ it is shown [45] that $\max_{\Omega} \nu(\Omega) = \frac{2}{3}$ and hence $p_{\max} = (1 + 2F)/3$.

After measuring n copies, the probability of finding j states that “fail” the test and $n - j$ states “pass” it is given by

$$\Pr(j|F) = \binom{n}{j} p^{n-j} (1-p)^j, \quad (8)$$

where F is the fidelity of the states. Thus, the value of j is related to the actual fidelity of the ensemble. We exploit this property by suitably acquiring and processing information about the value of j in order to tackle the fidelity witnessing and discrimination problems. We detail later in this section the strategy based on single copy measurements for these two problems. Before, we particularize the previous properties for two types of states that we make use of throughout the paper.

Amplitude-damping noise ensemble. Consider the states of the ensemble to be amplitude-damping type [Eq. (5)] with some unknown fidelity F . By measuring the state on the $Z_A \otimes Z_B$ basis, we consider the state “pass” the measurement test if these two outcomes coincide. This is given by

$$p = F < p_{\max}.$$

Since we can distinguish with total certainty between the two eigenvectors (with no-null eigenvalue) of ρ , and this measure-

ment is equivalent to a measurement with $\nu = 1$, what has been shown to be optimal for the verification problem [45].

Werner-type states. Consider now the case where the states of the ensemble are given by Werner states [see Eq. (3)]. Note that this corresponds to depolarizing noise acting on the states. In particular, any state can be brought to a Werner-type form by depolarization means [32], and hence this case represents a completely general situation.

The optimal measurement in this case also corresponds to locally measuring the states in the computational basis, i.e., with respect to the observable Z_A and Z_B , considering that the state “pass” the measurement test if the two outcomes coincide. However, the probability of a state with fidelity F passing the measurement is now given by $p = (1 + 2F)/3$, which is equivalent to performing the optimal measurement for an unknown state. Note that the process is analogous to first depolarizing the state to its Werner form and then performing the described measurement.

Fidelity witnessing. Given an ensemble of entangled states with fidelity F and some threshold fidelity F_0 , the expected value of j (see above) is given by

$$\langle j \rangle = n(1 - F)\nu(\Omega).$$

This allows us to extend this strategy to perform fidelity witnessing. After performing the measurement $\{\Omega, \mathbb{1} - \Omega\}$ on n copies, we can conclude that the fidelity lies on one or another regime, i.e.,

$$\begin{aligned} F > F_0 & \text{ if } j < n(1 - F_0)\nu(\Omega), \\ F < F_0 & \text{ if } j > n(1 - F_0)\nu(\Omega). \end{aligned} \quad (9)$$

Since the ensemble is in a tensor product structure, the success probability P_s of solving the witnessing problem based on Eq. (9) can be determined by the Chernoff-Hoeffding theorem [46]

$$P_s \geq 1 - e^{D(j||np)},$$

where

$$D(S||Q) = \sum_x S(x) \log_2 \left(\frac{S(x)}{Q(x)} \right)$$

is the Kullback-Leibler divergence (see [25]).

The criterion given by Eq. (9) can be generalized to tune the success probability as a function of F . To show this, we use a different approach. As a starting point, F is given by some prior probability $\varrho(F)$. However, as j and F are not independent random variables, once the value of j is obtained, the probability of F is then given by $\varrho(F|j)$. From the new probability distribution, we make a statement about F . In particular, if we define as Σ the set of values of j for which we conclude that the fidelity is above the threshold F_0 , Σ contains the values of j for which the probability of the conditioned probability of $F > F_0$ is larger than a parameter δ , which we can freely choose. Formally, we define Σ as

$$\Sigma = \left\{ j \mid \delta < \Pr(F > F_0 | j) = \int_{F_0}^1 \varrho(F|j) dF \right\}, \quad (10)$$

where we use Bayes' theorem to compute the conditioned density probability, i.e.,

$$\varrho(F|j) = \frac{\Pr(j|F)\varrho(F)}{\int_0^1 \Pr(j|F')\varrho(F')dF'}.$$

Considering a flat probability distribution for F , i.e., $\varrho(F) = \text{const.}$, we obtain

$$\varrho(F|j) = \frac{\Pr(j|F)}{1+n}.$$

For a given fidelity F , the success probability, i.e., the probability of deciding that the fidelity is above (or below) the threshold and being right, is given by

$$P_s(F) = \begin{cases} \sum_{j \notin \Sigma} \Pr(j|F) & \text{for } F < F_0, \\ \sum_{j \in \Sigma} \Pr(j|F) & \text{for } F > F_0. \end{cases}$$

The value of δ can be tuned in order to optimize the performance in certain regimes. Observe that, by appropriately choosing the value of δ in Eq. (10), one can increase or decrease the success probability P_s of the protocol within some of the regimes discussed in Sec. III, i.e., either enhance the success probability to correctly certify states with $F > F_0$, or correctly reject states with $F < F_0$. We analyze the performance of this protocol in detail in the following sections, comparing it with the other strategies we propose.

Fidelity discrimination. The information learning process is analogous for fidelity discrimination, where one learns the number j of states that “fail” the measurement test $\{\Omega, \mathbb{1} - \Omega\}$. Once a particular value of j is obtained, one simply concludes that the fidelity of the ensemble is F_1 in case $\Pr(j|F_1) > \Pr(j|F_2)$.

Similar as before, we separate all the possible values of j in two sets Σ_1 and Σ_2 , such that

$$\begin{aligned} \Sigma_1 &= \{j \mid \Pr(j|F_1) > \Pr(j|F_2)\}, \\ \Sigma_2 &= \{j \mid \Pr(j|F_2) > \Pr(j|F_1)\}. \end{aligned} \quad (11)$$

In case fidelity F_i is then given with probability η_i , the success probability reads as

$$P_s = \eta_1 \sum_{j \in \Sigma_1} \Pr(j|F_1) + \eta_2 \sum_{j \in \Sigma_2} \Pr(j|F_2).$$

If the two fidelities are given with the prior probability $\eta_1 = \eta_2$, the success probability P_s is then bounded by

$$P_s \leq \frac{1}{2} [1 + T(\rho_1^{\otimes n}, \rho_2^{\otimes n})], \quad (12)$$

where $\rho_i = \rho(F_i)$, and $T(\rho, \sigma)$ is the trace distance between states ρ and σ [35]. In particular, for amplitude-damping noise (see above), the success probability when performing fidelity discrimination reaches the optimal values, i.e., it saturates the trace distance between the two ensembles [Eq. (12)].

B. Protocol P1: Error counting

The first protocol we propose is an extension of the approach for quantum state verification we introduced in [28]. In the following, we will consider states of the form ρ_a resulting from amplitude damping. In general, given an ensemble of n identical copies of states ρ_a , the protocol consists in

Protocol P1: Error counting

Input: Ensemble of n identical noisy Bell states and auxiliary $(n+1)$ -level maximally entangled state.

1. Apply the ENG between the ensemble and the auxiliary system.
2. Obtain the amplitude index j by measuring locally in Z basis.
3. If $j \in \Sigma$ output $F > F_0$, otherwise output $F < F_0$.

Output: The fidelity of the initial ensemble was above or below F_0 with some success probability P_s .

applying the ENG gate, Eq. (7), between n copies of the ensemble and an auxiliary d -level system of the form $|\Phi_{00}^d\rangle$ [see Eq. (1)]. The ENG transfers information about the number of type-1 and type-2 errors in the ensemble into the auxiliary system [see Fig. 2(b)] by changing its amplitude index. By subsequently measuring this auxiliary state we can learn its amplitude index j , revealing information about the number of errors, and therefore the fidelity, of the ensemble. Crucially, the remaining ensemble that is witnessed is not destroyed in the process. Notice, though, that the state of the ensemble changes, and is no longer of tensor product structure, i.e., the copies are not independent. However, the fidelity of individual reduced states is known, and above the threshold value F_0 in case of successful certification. We detail in the following the steps for the different cases depending on the kind of noise affecting the ensemble copies.

Fidelity witnessing. Consider first that the noise affecting the states of the ensemble is amplitude-damping type [Eq. (5)]. An ensemble of n copies of states of the form (5) is given. Note that one can also interpret an ensemble of n states of this form as an unknown distribution of pure states where each state corresponds either to $|\Psi_{00}\rangle$ or $|01\rangle$. The joint state of the ensemble can then be written as

$$\rho^{\otimes n} = \sum_{j=0}^n \binom{n}{j} F^{n-j} (1-F)^j \Gamma_j,$$

where Γ_j is a density operator corresponding to all permutations of $\{|\Psi_{00}\rangle_{AB}^{\otimes(n-j)} |01\rangle_{AB}^{\otimes j}\}$.

Information about the noise of the ensemble can be transferred and accumulated in a single d -level state. For that end, a maximally entangled state of dimension $d = n+1$ is prepared, $|\Phi_{00}^d\rangle$ [see Eq. (1)]. The ENG gate, Eq. (7), is applied between the states of the ensemble and the auxiliary d -dimensional state, such that

$$\begin{aligned} \text{ENG: } & \rho^{\otimes n} \otimes |\Phi_{00}^d\rangle\langle\Phi_{00}^d| \\ \mapsto & \sum_{j=0}^n \binom{n}{j} F^{n-j} (1-F)^j \Gamma_j \otimes |\Phi_{0j}^d\rangle\langle\Phi_{0j}^d|. \end{aligned}$$

Observe that, given the nature of the noise and the effect of the ENG gate, the amplitude index of the auxiliary state j encodes very specific information about the number of errors contained in the ensemble, that directly relates to the fidelity of the copies.

By simply measuring the auxiliary state locally by parties A and B in the generalized Z basis, and subtracting their

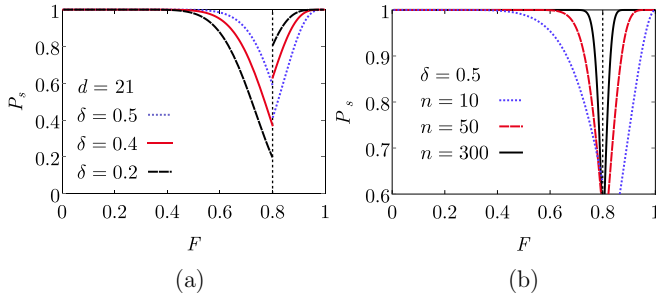


FIG. 3. Performance of the individual measurements (P0) and the error-counting (P1) strategies. (a) Shows the success probability of both protocols for an ensemble of $n = 20$ identical copies and different values of the heuristic δ value, as a function of the actual fidelity of the copies. Depending on the choice of δ , a better performance is found in one or another regime. (b) Shows the success probability of both protocols with a fixed value of $\delta = 0.5$ and different values of ensemble size n , as a function of the actual fidelity of the copies. A larger ensemble provides better performance.

outcomes, one learns the value of the amplitude index j , from which one can infer the number of errors in the ensemble. Each j value can be found with probability

$$\Pr(j|F) = \binom{n}{j} F^{n-j} (1-F)^j.$$

Note that this corresponds to the same distribution obtained with protocol P0 [see Eq. (8)], with $p = F$. Due to this close, but probabilistic, dependence, one can solve the decision problem by determining whether the measured value of j is above or below a certain value $j_0 = n(1 - F_0)$, which also depends on the threshold problem fidelity F_0 . Note that the same statistical analysis performed in protocol P0 can be applied here and, hence, the two protocols exhibit the same success probability (see Fig. 3). However, while in protocol P0 the whole ensemble is consumed, here we just destroy an auxiliary maximally entangled state of dimension $d = n + 1$, providing an exponential improvement in the amount of consumed resources. Importantly, the states that are witnessed or verified are not destroyed in the process, in opposition to protocol P0 and previous approaches. Notice, however, that the remaining ensemble is no longer of tensor product structure, but corresponds to Γ_j when obtaining the outcome j . The fidelity of reduced states, i.e., tracing out all but one copy, is given by $F = (n - j)/n$, which can be larger than the initial fidelity F .

The protocol can equivalently be applied to Werner states of the form (3). The steps of the protocol are identical as before. However, the ensemble can now contain the three different kinds of errors and, hence, the value of j after the application of the ENG does not encode the number of errors in the ensemble. Instead, it provides information about the difference between type-1 and type-2 error states. In this case, the probability of obtaining j for a given F corresponds to the sum of all configurations with a difference of j errors, i.e.,

$$\Pr(j|F) = \sum_{\substack{i,k,l=0 \\ i+k+l=n \\ k-l=j}}^n \frac{n!}{i!k!l!} A^i (1-A)^{k+l},$$

where $A \equiv (1 + 2F)/3$.

Note that, due to the different effect of the counter gate in this case (Sec. IID), we can now obtain $2n + 1$ different values of j , i.e., $j \in \{-n, \dots, n\}$. In order to differentiate between all these possible values of j , we require an auxiliary state of dimension $d = 2n + 1$. We remark, though, that we did not succeed in using this to obtain an efficient protocol for witnessing Werner states, i.e., a protocol that outperforms P0.

Fidelity discrimination. The error-counting protocol can be directly applied for solving the fidelity discrimination problem. This is accomplished by simply processing the information learned about the value of j as in the protocol P0 case [see Eqs. (11) and (12)], finding comparable efficiency.

C. Protocol P2: Coarse graining

In the strategies introduced above, i.e., the single copy measurement and the error-counting protocols, the information obtained about the ensemble is unnecessarily excessive. Instead of learning information about whether the number of errors in the ensemble is above or below some value, we, indirectly, also obtain information about the concrete number of errors in the ensemble. This implies that the protocols likely spend more resources than the ones required to just solve the witnessing and discrimination problems.

We propose here a modified protocol that tries to minimize the amount of obtained information, therefore reducing the amount of resources spent during the process. The strategy relies on the application of coarse-grained techniques that allow us to locally access partial information about the amplitude index j of the previous protocol, without destroying the auxiliary state or the ensemble copies.

Fidelity witnessing. We restrict to the amplitude-damping noise case for simplicity, i.e., states of the form ρ_a . The first steps of the protocol are identical to the error-counting approach. A d -dimensional auxiliary state $A_1 B_1$ is prepared in the state $|\Phi_{00}^d\rangle$ with $d = n + 1$, and the ENG operation is applied from n states of the ensemble to the auxiliary, such that the information of the number of errors of the ensemble gets accumulated in the amplitude index j of the auxiliary state, i.e., $|\Phi_{0j}^d\rangle$. Here, however, we do not measure the auxiliary state to learn the value of j . In fact, as shown later,

Protocol P2: coarse-graining

Input: Ensemble of n identical noisy Bell states and auxiliary $(n + 1)$ -level maximally entangled state.

1. Apply the ENG between the ensemble and the auxiliary state. The information of the noise is accumulated in its amplitude index j .
2. Apply the coarse-grained operation (14) from the auxiliary into an additional extra register.
3. Measure the extra register to learn information about where j lies.
4. Apply the decorrelation process to recover the auxiliary state untouched.

Output: The witnessing decision problem is solved, i.e., the fidelity of the ensemble states is determined to be above or below some threshold up to some failure probability.

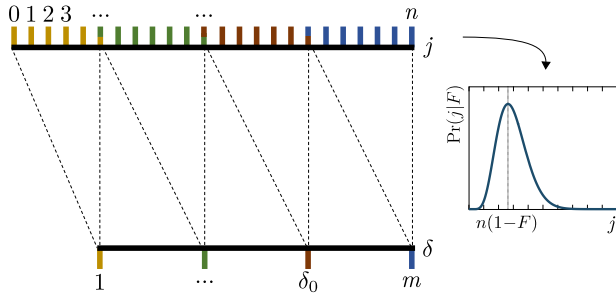


FIG. 4. Schematic representation of the coarse-graining protocol P2. Given all the possible values that the amplitude index j of the auxiliary state (upper part) can take, we group them into a few sets encoded in an extra register (lower part). By suitably measuring this extra register, we can learn, up to some failure probability, the information about whether j is above a certain threshold δ_0 without consuming the entanglement of the auxiliary state, whereas the values of j and δ are directly related with the fidelity F of the states.

the auxiliary state is kept unchanged (and the entanglement is not consumed).

We introduce an additional two-system register A_2B_2 , that we denote as *extra register*, of dimension $m \leq d$. For simplicity, we assume that m divides d , i.e., $d/m \in \mathbb{N}$; however, this assumption can be lifted. The extra register is initially prepared in the $|00\rangle_{A_2B_2}$ state locally by parties A and B . A bilateral local operation U_{12} is applied from the auxiliary to the extra register such that

$$U_{12} = \sum_{k=0}^{d-1} |k\rangle\langle k|_1 \otimes X_2^{\lceil \frac{k}{d/m} \rceil}, \quad (13)$$

which transfers information of the amplitude index into the extra register in a coarse-graining way (see Fig. 4). The effect of this operation reads as

$$U_{A_1A_2} \otimes U_{B_1B_2} |\Phi_{0j}^d\rangle_{A_1B_1} |00\rangle_{A_2B_2} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \left| k, \left\lceil \frac{k}{d/m} \right\rceil \right\rangle_{A_1A_2} \left| k \oplus j, \left\lceil \frac{k \oplus j}{d/m} \right\rceil \right\rangle_{B_1B_2}. \quad (14)$$

The different j values get grouped into different sets of certain size and the group or interval δ_0 is identified as the interval containing the threshold j_0 value, where j_0 is the most likely value of the distribution $\text{Pr}(j|F_0)$.

The qubit of the extra register that belongs to party A is subsequently teleported to party B , by consuming $\log_2 m$ ebits of entanglement, such that the global state becomes

$$|\psi\rangle_{A_1B_1B_2B_3} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_{A_1} \otimes \left| k \oplus j, \left\lceil \frac{k \oplus j}{d/m} \right\rceil \right\rangle_{B_1B_2} \left| \left\lceil \frac{k}{d/m} \right\rceil \right\rangle_{B_3}, \quad (15)$$

where we have relabeled qubit $A_2 \rightarrow B_3$. Finally, party B performs a two-outcome positive-operator-valued measure (POVM) measurement defined by the projectors $\{M, \mathbb{1} - M\}$

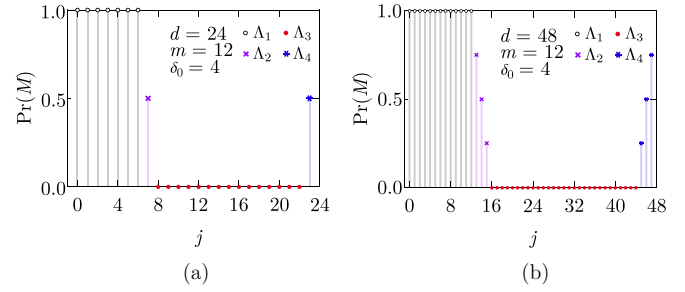


FIG. 5. Analysis of the coarse-graining protocol P2. Given a state $|\Phi_{0j}^d\rangle$, the probability of measuring outcome M as a function of j is plotted for a dimension of the auxiliary state of $d = 24$ (a) and $d = 48$ (b). The elements of the different sets Λ_i are indicated.

on the extra register qubits B_2, B_3 , i.e.,

$$M = \sum_{\delta=0}^{\delta_0-1} \sum_{l=0}^{m-1} |l \oplus \delta, l\rangle\langle l \oplus \delta, l|, \quad (16)$$

where the projector acts on the $\mathcal{H}_{B_2} \otimes \mathcal{H}_{B_3}$ Hilbert space.

In case the outcome $M(\mathbb{1} - M)$ is found, we conclude that the fidelity of the probe ensemble states is above (below) the threshold F_0 , up to a certain failure probability. Importantly, the process only consumes the entanglement required to teleport qubit A_2 to party B . We consider the number of ebits required by the process (see Sec. II E) to evaluate the protocol performance. From a practical perspective, the entanglement required for the teleportation can be obtained by entanglement distillation means (see, e.g., [27,36]) of the ensemble copies directly.

In order to properly understand the effect of the measurement $\{M, \mathbb{1} - M\}$, we can classify the values of j in four sets (see Fig. 5):

$$\begin{aligned} \Lambda_1 &= \{0, \dots, \tilde{d}(\delta_0 - 1)\}, \\ \Lambda_2 &= \{\tilde{d}(\delta_0 - 1) + 1, \dots, \delta_0\tilde{d} - 1\}, \\ \Lambda_3 &= \{\delta_0\tilde{d}, \dots, \tilde{d}(m - 1)\}, \\ \Lambda_4 &= \{\tilde{d}(m - 1) + 1, \dots, d - 1\}, \end{aligned}$$

where $\tilde{d} = d/m$. The measurement given by Eq. (16) can deterministically distinguish between sets Λ_1 and Λ_3 , such that in case j lies either in Λ_1 or Λ_3 , the decision problem is solved deterministically and the auxiliary state is recovered untouched (see below). This is, however, not the case for the set Λ_2 , for which certain overlapping exists that has to be taken into account. In summary, depending on where the actual set where j lies, the success probability of the witnessing problem reads as

$$\begin{aligned} \text{Pr}(M) &= 1 && \text{if } j \in \Lambda_1, \\ \text{Pr}(M) &= 0 && \text{if } j \in \Lambda_3, \\ 0 < \text{Pr}(M) &< 1 && \text{if } j \in \Lambda_2 \cup \Lambda_4. \end{aligned}$$

The performance of the protocol can be directly analyzed given the previous reasoning and given the probability distribution of the j value as a function of the state fidelity. Figure 6 shows the efficiency for different settings and ensemble sizes. Observe how for the witnessing problem of determining whether the value of the fidelity is $F > F_0 + \frac{\lambda}{2}$

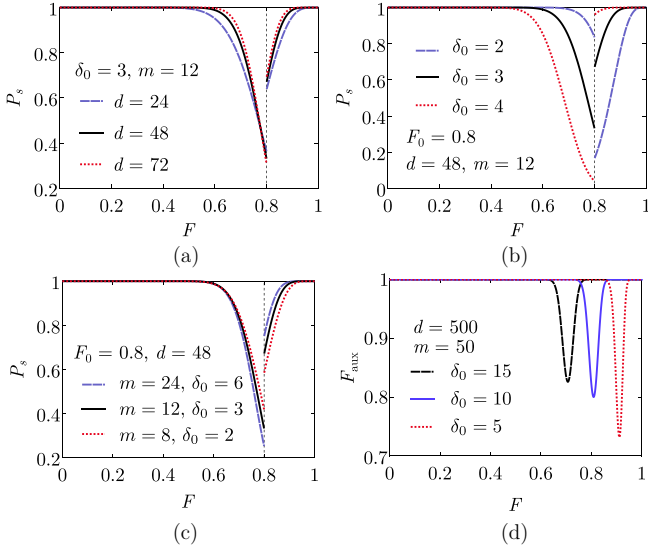


FIG. 6. Performance of the coarse-graining protocol P2. (a) The success probability of the protocol for a fixed amount of resources consumed (i.e., fixed extra register of dimension $m = 12$) for increasing dimension of the auxiliary register d . Note that as long as the entanglement of the auxiliary is recovered, the performance of the protocol can be freely enhanced. (b) Success probability for fixed auxiliary states $d = 48$ and $m = 12$, and decreasing δ_0 . (c) Success probability for a fixed auxiliary $d = 48$ and with different dimensions of the register m . For each value of m we use the maximum ensemble size n and the value of δ_0 that minimizes the discontinuity in F_0 . (d) Fidelity of the remaining auxiliary state after the implementation of the coarse-gaining protocol P2 for different values of δ_0 .

or $F < F_0 - \frac{\lambda}{2}$, the success probability of the protocol can approach 1 for relatively small additive error λ .

Once the decision problem is solved, the last step of the protocol entails the recuperation of the auxiliary state, which has been entangled with the extra register during the process. The following steps are required to disentangle the extra register and leave the auxiliary state, and the entanglement associated, untouched. First, the operation $U_{B_1 B_2}$ [Eq. (13)] is undone on the remaining measured state (15), i.e.,

$$U_{B_1 B_2}^\dagger |\psi\rangle_{A_1 B_1 B_2 B_3} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k, k \oplus j, 0, \lceil \frac{k}{d/m} \rceil\rangle_{A_1 B_1 B_2 B_3}.$$

Then, qubit B_3 is measured in the generalized Fourier basis, given by the basis elements $\{|\alpha_l\rangle = \sum_q \exp(-2\pi i q/m) |q\rangle\}$, leading to a state

$$\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{2\pi i \lceil \frac{k}{d/m} \rceil l/m} |k, k \oplus j, 0, \alpha_l\rangle_{A_1 B_1 B_2 B_3},$$

where l refers to the outcome $|\alpha_l\rangle$ obtained. By simply applying a phase gate on party A of the form

$$U_{A_1} = \sum_{k=0}^{d-1} e^{-2\pi i \lceil \frac{k}{d/m} \rceil l/m} |k\rangle\langle k|,$$

the initial auxiliary state is recovered.

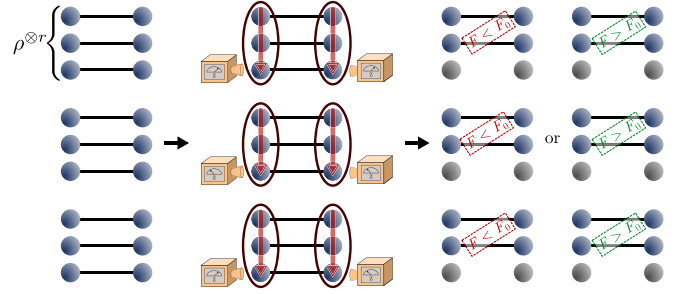


FIG. 7. Schematic representation of the blocking strategy (P3). The initial ensemble of n Bell diagonal states is divided into several blocks of size r . Then, the parity of each block is encoded in one of the states which later is measured revealing the actual parity value of the block. From the number of obtained “even” parties, we can determine if the initial fidelity F was above or below the threshold F_0 with some success probability.

Fidelity discrimination. The coarse-graining strategy is also directly applicable to fidelity discrimination. In this case, to enhance its performance, the dimension of the extra register should be chosen depending on the possible fidelity values F_1, F_2 . Performance is comparable to the efficiency for the witnessing problem.

D. Protocol P3: Ensemble blocking

We finally consider a strategy based on parity measurements of subsets or blocks of the ensemble. In contrast to the previously discussed protocols P1 and P2, this approach is not limited to states ρ_a resulting from amplitude damping, but also to other state families such as Werner states ρ_w .

Fidelity witnessing. Given an ensemble of N unknown states we first depolarize them into a Werner state form, i.e., $\rho^{\otimes N} \mapsto \rho_w^{\otimes N}$ (see Sec. II C). Then, we divide the ensemble into n blocks of r states each. Making use of bilateral CNOT gates, in analogy to purification hashing techniques [40], which act locally from the states of each block into one of the states, we can learn the parity of each block (see Fig. 7), i.e.,

$$\begin{aligned} & \text{CNOT}_{1 \rightarrow 2}^{A_1 A_2} \otimes \text{CNOT}_{1 \rightarrow 2}^{B_1 B_2} |\Psi_{ij}\rangle_{A_1 B_1} |\Psi_{kl}\rangle_{A_2 B_2} \\ & = |\Psi_{i \oplus k, j}\rangle_{A_1 B_1} |\Psi_{k, l \oplus j}\rangle_{A_2 B_2}. \end{aligned} \quad (17)$$

Note that maximally entangled copies are not required since the parity can be encoded in one of the states of the block. We denote as κ the number of *even* parties obtained, whose

Protocol P3: Ensemble blocking

Input: Ensemble of n identical noisy Bell states.

1. Depolarize the ensemble to the form of Eq. (3).
2. Apply bilateral CNOT gates (17) from ensemble blocks to some target ensemble states.
3. Learn the parity of each block by measuring the target states.
4. If $\kappa \in \sigma$ assume $F > F_0$, where κ is the number of even parities.

Output: The fidelity of the initial ensemble was above or below F_0 with some success probability P_s .

probability follows a binomial distribution of the form

$$\Pr(\kappa|\rho) = \binom{n}{\kappa} [\pi_0(\rho^{\otimes r})]^{n-\kappa} [1 - \pi_0(\rho^{\otimes r})]^\kappa,$$

where the probability of measuring even parity in a block of size r is

$$\pi_0(\rho^{\otimes r}) = \sum_{k=0}^{r/2} \binom{r}{2k} A^{r-2k} (1-A)^{2k},$$

where $A \equiv (1 + 2F)/3$.

Since κ is given by a binomial distribution, we can then repeat the same analysis performed for protocol P0 (see Sec. IV A), but using $\Pr(\kappa|\rho)$ instead of $\Pr(j|F)$. Observe how, despite N states being involved in the protocol, only n are destroyed and the remaining $(r-1)n$ states are now correlated. After the first parity round is complete, the fidelity of the remaining states is changed depending on the value of the parity obtained. Due to the back-action effect of the bilateral control gate [see Eq. (17)], the expected value of the local fidelity is given by

$$F' = F^2 + F \left(\frac{1-F}{3} \right) + 2 \left(\frac{1-F}{3} \right)^2.$$

The performance of the protocol can be further enhanced in case the initial states of the ensembles are of a certain form. One case of particular interest involves states affected by dephasing type noise [Eq. (4)], for which the first depolarization step is not required. For this kind of state, there is no back-action effect from the bilateral CNOT gate, and hence the average fidelity remains unchanged, i.e., $F' = F$.

Additionally, one can implement a second round of parity measurements to further enhance the performance. This is accomplished by simply learning again the parity of the blocks where an even parity was found, leading to a recursive improvement in the protocol efficiency.

From the value of κ we can again solve the fidelity witnessing problem following an analogous analysis as the one described for protocol P0, Sec. IV A, by including the block size r as an extra parameter to consider, such that the success probability can be optimized by simply defining a block size r^* that maximizes it i.e.,

$$\int_0^1 P_s(r^*, F) dF = \max_r \int_0^1 P_s(r, F) dF.$$

Fidelity discrimination. The value of even parities κ can be also used to solve the discrimination problem. In this case, the optimal r^* is such that the difference of obtaining an even parity is maximum, i.e.,

$$\pi_0(\rho_1^{\otimes r^*}) - \pi_0(\rho_2^{\otimes r^*}) = \max_r \pi_0(\rho_1^{\otimes r}) - \pi_0(\rho_2^{\otimes r}),$$

where the larger the difference, the more distinguishable the two probability distributions are. Importantly, the blocking strategy allows us to overcome the optimal success probability for fidelity discrimination by involving the whole ensemble in the process but only partially consuming it.

Figures 8(a) and 8(b) show the performance of the blocking strategy, compared with protocol P0 based on individual measurements. Observe how the blocking strategy provides

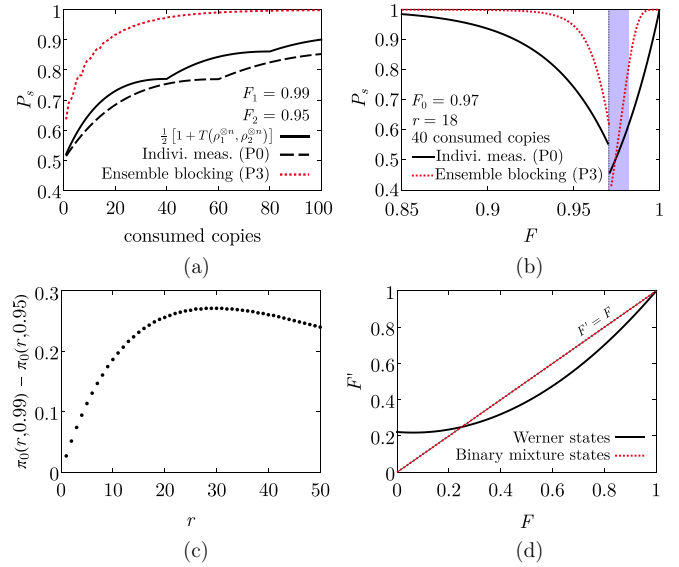


FIG. 8. Performance of the blocking protocol for Werner-type states. (a) Fidelity discrimination with equal prior probability for each state, i.e., $\eta_1 = \eta_2 = 1/2$. Success probability as a function of the number of consumed copies. (b) Fidelity witnessing with $F_0 = 0.97$. Success probability as a function of the fidelity of the ensemble. The shadow region corresponds to the range of $F > F_0$ such that $F' < F_0$. (c) Difference of probability of obtaining parity 0 as a function of the block size r for two blocks of fidelities $F_1 = 0.99$ and $F_2 = 0.95$. The difference is maximized for $r = 29$. (d) Fidelity of the remaining states of the ensemble after the application of a single round of the blocking protocol.

significant performance enhancement with respect to the individual measurements strategy (P0).

V. COMPARISON OF APPROACHES

In order to compare different protocols, we use the number of required resources R to obtain a certain success probability P_s as a measure. We demand that the success probability for a fixed fidelity is the same for all protocols. We use the success probability of the single-copy approach P0 as a reference value, and adjust the parameters of the other protocols to guarantee that they lead to the same or a larger success probability. The resources are the number of copies that are measured and hence destroyed. Notice that for the error-counting and coarse-graining protocols, P1 and P2, we also take the cost for used maximally entangled auxiliary states into account. In order to do so, we assume that these auxiliary states are generated from noisy states of the ensemble, e.g., via entanglement purification, where the yield (Y) of the entanglement purification protocol (a combination of the recurrence protocol of [42] and hashing [40]) determines how many noisy copies correspond to a perfect ebit. For an entangled auxiliary register of dimension d , $\log_2(d)/Y$ states of the ensemble are required.

An overview of the applicability and strengths of the different protocols is given in Table I. All protocols are applicable for states of the form ρ_a resulting from amplitude damping, where both P1 and P2 give an (up-to) exponential advantage as compared to the standard approach P0. Notice though that the

TABLE I. General comparison between protocols. We use the required resources R to obtain a certain success probability P_s as a figure of merit to assess the performance of the different protocols, where we denote by R_0 the required resources of the reference protocol P0 to achieve P_s , and we demand the same or larger success probability for the other protocols. The resources depend on the problem setting (threshold fidelity F_0 in witnessing and F_1, F_2 in discrimination) and the required success probability. $\alpha(n)$ and $\beta(F_0)$ are factors that depend on the ensemble size or the threshold fidelity, respectively, and which are typically smaller than 1, i.e., they indicate an improvement over P0. Efficient variants of the P1 and P2 protocols that offer an exponential improvement over P0 are not known for dephasing and Werner-type states.

| State type | Protocol efficiency: Required resources R | | | |
|----------------------------|---|---------------------|-------------------------|------------------------|
| | Indiv. meas. (P0) | Error counting (P1) | Coarse graining (P2) | Ensemble blocking (P3) |
| Amplitude damping ρ_a | R_0 | $O[\log R_0]$ | $O[\alpha(n) \log R_0]$ | $O[\beta(F_0) R_0]$ |
| Dephasing ρ_d | R_0 | Nonefficient | Nonefficient | $O[\beta(F_0) R_0]$ |
| Werner ρ_w | R_0 | Nonefficient | Nonefficient | $O[\beta(F_0) R_0]$ |

error-counting and coarse-graining protocols P1 and P2 are not efficient for Werner states. However, the blocking protocol P3 still outperforms the standard approach P0 also in this case, as is shown in Figs. 8(a) and 8(a).

In Fig. 9 we compare the different protocols (see also Table I), and plot the required resources r as a function of the fidelity of the initial states in the ensemble for the fidelity witnessing problem, i.e., to decide if the state has a fidelity larger or smaller than F_0 . One clearly observes that P1 and P2 offer a large improvement for fidelities that are close to the threshold fidelity F_0 , though they work even better if one excludes a small interval around F_0 , i.e., considers the promise problem that $F \geq F_0 + \lambda/2$ or $F < F_0 - \lambda/2$. Similarly, for

the fidelity discrimination problem, one obtains an even larger improvement for P1 and P2.

VI. CONCLUSIONS AND OUTLOOK

In this work, we have considered the verification of noisy entangled states, with the aim to decide if the quality of states in a (large) ensemble is sufficient to use them for some desired application. We introduced methods to distinguish between two sets of entangled states by means of local operations and classical communication, eventually assisted by entanglement. We have concentrated on specific state families and fidelity as the central feature. Specifically, we introduced protocols to solve the decision problems of determining if the ensemble consists of states with fidelity F_1 or F_2 (discrete sets), or if the fidelity of the states is above or below a certain threshold value F_0 , possibly excluding a small interval around F_0 . The nature of the problem that we called fidelity witnessing requires as output only one bit of information, in contrast to well-studied problems such as state tomography or fidelity estimation, where a significantly larger amount of information needs to be determined. As a first result, we have found that this practically relevant decision problem can for some state families, e.g. resulting from imperfect storage with decay as the dominant noise source, be solved more efficiently than using fidelity estimation or full state tomography.

Perhaps more importantly, we demonstrate that using a larger ensemble while measuring and hence consuming only a small subset of states provides a significant advantage. This is similar in spirit as utilized in [27,28] in the context of entanglement purification or state certification, but generalizes and extends these ideas in a nontrivial way and makes them applicable to new problems. This in fact leads to an up-to-exponential improvement as compared to methods, extensions of state verification [20–25], that operate on ensembles of a fixed size where all states are measured. Some protocols we introduce in this context operate on states of the ensemble directly (protocol P3), without any extra resources, where blocks of a certain size are locally manipulated by collective operations and only a few states are measured. The rest of the ensemble remains intact and can be used for the desired application after successful verification. Other approaches we introduce, such as protocols P1 and P2, require auxiliary entangled states to write in and read out relevant information of the whole ensemble. While in protocol P1 this auxiliary

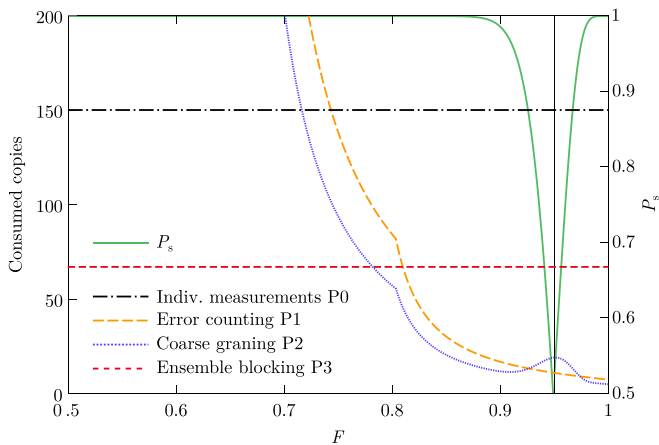


FIG. 9. Comparison between different protocols. The required resources R , i.e., the number of consumed copies, are plotted as a function of the fidelity for different protocols. We assume a threshold fidelity of $F_0 = 0.95$, and an ensemble of size n corresponding to states resulting from amplitude damping ρ_a . We consider a fixed success probability for all protocols that varies with the fidelity (right vertical axis). Notice that ensemble sizes differ for different protocols in order to match success probabilities, but the relevant quantity is the consumed resources which are plotted. Parameter used for the different protocols are as follows. P0: ensemble size $n = 150$, where all copies are measured; P1: ensemble size $n = 150$, dimension $d = \log_2 151$ for auxiliary register; P2: ensemble size $n = 290$, dimension of auxiliary register $d = 300$, dimension of coarse-grained register $m = 30$, $\delta_0 = 2$; P3: ensemble size $n = 603$, block size $r = 9$ measured copies 67.

register is measured and hence destroyed, in protocol P2 the information is first coarse grained, and most of the auxiliary entanglement is preserved and can be recovered. Only the read-out of a small amount of coarse-grained information is required, and little entanglement is consumed to access this (nonlocal) information with local operations only. It is in fact the latter protocol that yields a provable exponential advantage as compared to strategies that operate on fixed-size ensembles that are fully measured. Notice that consumed auxiliary entanglement can be directly related to the number of copies of states in the ensemble that need to be measured. One may either actually use noisy states from the ensemble as auxiliary states, or first produce, e.g., by means of entanglement purification, high-fidelity or even perfect auxiliary entangled states from noisy copies. The conversion rate is given by the performance of entanglement purification, where reachable bounds are known. One can hence translate also protocols using auxiliary entanglement into schemes that only use noisy states from the ensemble, and find the total number of consumed states. This allows one to compare the different

strategies, and assess performance (e.g., success probability) for a given number of consumed copies, or the required number of copies to reach a certain accuracy.

We remark that the ideas and tools we present here are not limited to the specific state classes we consider, but may be more broadly applicable. For instance, we believe that a generalization to multipartite entangled states such as Greenberger-Horne-Zeilinger states or certain graph states is straightforward, and will be presented elsewhere. Also, the idea of using a larger ensemble, concentrating information and measuring only a small fraction might be useful for other related problems, such as, e.g., for improving fidelity estimation.

ACKNOWLEDGMENTS

This work was supported by the Austrian Science Fund (FWF) through Projects No. P30937-N27, No. P36009-N, and No. P36010-N. Finanziert von der Europäischen Union-NextGenerationEU.

-
- [1] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [2] H.-K. Lo, M. Curty, and K. Tamaki, *Nat. Photonics* **8**, 595 (2014).
- [3] S. Wehner, D. Elkouss, and R. Hanson, *Science* **362**, eaam9288(2018).
- [4] A. Pirker and W. Dür, *New J. Phys.* **21**, 033003 (2019).
- [5] K. Azuma, S. Bäuml, T. Coopmans, D. Elkouss, and B. Li, *AVS Quantum Sci.* **3**, 014101 (2021).
- [6] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, *Phys. Rev. A* **59**, 4249 (1999).
- [7] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, *IEEE Network* **34**, 137 (2020).
- [8] M. Hayashi and T. Morimae, *Phys. Rev. Lett.* **115**, 220502 (2015).
- [9] P. Sekatski, S. Wölk, and W. Dür, *Phys. Rev. Res.* **2**, 023052 (2020).
- [10] E. M. Kessler, I. Lovchinsky, A. O. Sushkov, and M. D. Lukin, *Phys. Rev. Lett.* **112**, 150802 (2014).
- [11] Z. Eldredge, M. Foss-Feig, J. A. Gross, S. L. Rolston, and A. V. Gorshkov, *Phys. Rev. A* **97**, 042337 (2018).
- [12] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, *Nat. Rev. Phys.* **2**, 382 (2020).
- [13] C. Bădescu, R. O'Donnell, and J. Wright, *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing* (ACM, New York, 2019).
- [14] L. P. Thinh, M. Dall'Arno, and V. Scarani, *Quantum* **4**, 320 (2020).
- [15] X.-D. Yu, J. Shang, and O. Gühne, *Adv. Quantum Technol.* **5**, 2100126 (2022).
- [16] M. Kliesch and I. Roth, *PRX Quantum* **2**, 010201 (2021).
- [17] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, *Nat. Commun.* **1**, 149 (2010).
- [18] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, *IEEE Trans. Inf. Theory* **63**, 5628 (2017).
- [19] S. T. Flammia and Y.-K. Liu, *Phys. Rev. Lett.* **106**, 230501 (2011).
- [20] K. Wang and M. Hayashi, *Phys. Rev. A* **100**, 032315 (2019).
- [21] Z. Li, Y.-G. Han, and H. Zhu, *Phys. Rev. A* **100**, 032316 (2019).
- [22] H. Zhu and M. Hayashi, *Phys. Rev. Lett.* **123**, 260504 (2019).
- [23] H. Zhu and M. Hayashi, *Phys. Rev. A* **100**, 062335 (2019).
- [24] H. Zhu and M. Hayashi, *Phys. Rev. A* **99**, 052346 (2019).
- [25] X.-D. Yu, J. Shang, and O. Gühne, *npj Quantum Inf.* **5**, 112 (2019).
- [26] M. Hayashi, *New J. Phys.* **11**, 043028 (2009).
- [27] F. Riera-Sàbat, P. Sekatski, A. Pirker, and W. Dür, *Phys. Rev. Lett.* **127**, 040502 (2021).
- [28] J. Miguel-Ramiro, F. Riera-Sàbat, and W. Dür, *Phys. Rev. Lett.* **129**, 190504 (2022).
- [29] X. S. Liu, G. L. Long, D. M. Tong, and Feng Li, *Phys. Rev. A* **65**, 022304 (2002).
- [30] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [31] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Nature (London)* **390**, 575 (1997).
- [32] R. F. Werner, *Phys. Rev. A* **40**, 4277 (1989).
- [33] M. Horodecki and P. Horodecki, *Phys. Rev. A* **59**, 4206 (1999).
- [34] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).
- [35] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).
- [36] F. Riera-Sàbat, P. Sekatski, A. Pirker, and W. Dür, *Phys. Rev. A* **104**, 012419 (2021).
- [37] J. Daboul, X. Wang, and B. C. Sanders, *J. Phys. A: Math. Gen.* **36**, 2525 (2003).
- [38] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Rev. Mod. Phys.* **81**, 865 (2009).
- [39] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, *Phys. Rev. Lett.* **78**, 2275 (1997).

- [40] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
- [41] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Nat. Commun.* **8**, 15043 (2017).
- [42] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).
- [43] W. Dür and H. J. Briegel, *Rep. Prog. Phys.* **70**, 1381 (2007).
- [44] E. Hostens, J. Dehaene, and B. De Moor, *Phys. Rev. A* **73**, 062337 (2006).
- [45] S. Pallister, N. Linden, and A. Montanaro, *Phys. Rev. Lett.* **120**, 170502 (2018).
- [46] H. Chernoff, *Ann. Math. Statist.* **23**, 493 (1952).