Collective Operations Can Exponentially Enhance Quantum State Verification

Jorge Miguel-Ramiro, Ferran Riera-Sàbat, and Wolfgang Dür
Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 21a, 6020 Innsbruck, Austria

(Received 11 January 2022; revised 15 August 2022; accepted 3 October 2022; published 31 October 2022)

Maximally entangled states are a key resource in many quantum communication and computation tasks, and their certification is a crucial element to guarantee the desired functionality. We introduce collective strategies for the efficient, local verification of ensembles of Bell pairs that make use of an initial information and noise transfer to few copies prior to their measurement. In this way the number of entangled pairs that need to be measured and hence destroyed is significantly reduced as compared to previous, even optimal, approaches that operate on individual copies. Moreover, the remaining states are directly certified. We show that our tools can be extended to other problems and larger classes of multipartite states.

DOI: 10.1103/PhysRevLett.129.190504

Introduction.—With the emergence of quantum technologies, the certification and verification of quantum devices and states have become necessary requirements for viable quantum communication and computation tasks, such as, e.g., quantum teleportation [1], quantum key distribution [2,3], and distributed or blind quantum computation [4–6]. In particular, certification of maximally entangled states by local operations is a crucial ingredient for a feasible implementation of bottom-up [7–10] and entanglement-based [11–14] quantum networks, where entanglement is a key resource to enable, e.g., long-distance communication, various security applications, or connecting distributed quantum processors. However, local measurements destroy entanglement, making the verification of entangled states costly.

Different approaches for certifying quantum states exist [15,16]. Some of them, as state tomography [17], are, however, very inefficient as all elements of the density matrix need to be determined by means of destructive measurements. A protocol called quantum state verification was introduced in [18], allowing for efficient verification of quantum states with local measurements and constant overhead with regard to optimal global strategies. Several extensions [19–23] have been proposed, and were implemented experimentally [24]. These approaches rely in general on suitable sequential pass-or-fail measurements applied on individual states. However, the improved control of quantum systems also makes feasible more advanced, collective strategies that operate jointly on multiple copies.

Here, we show that such a collective but local strategy can significantly improve the efficiency of previous, even global and optimal, strategies based on sequential measurements of single copies. Our approach operates on multiple copies of entangled states, where only a few of these states are designated for certifying the whole ensemble. This is achieved by accumulating the noise of the whole ensemble into a reduced set of states by collective local operations, so that by measuring and consuming only these states one can detect the noise with enhanced probability while certifying the remaining states without destroying them. This significantly reduces the amount of entanglement that is destroyed due to the certification process. We adapt techniques from entanglement purification [25,26] in order to transfer noise from states in the ensemble into a few target states that are then measured. Crucially, the nonmeasured states remain untouched and hence entangled, and can still be used as a resource for various nonlocal quantum tasks. Although we focus on maximally entangled Bell states throughout this Letter, we remark that our techniques can be extended to different quantum states, including, e.g., maximally entangled qudit states or multipartite Greenberger-Horne-Zeilinger (GHZ) states.

Problem statement.—Consider an ensemble of n copies of some bipartite entangled state ρ_{AB} shared by two parties A and B, ideally prepared in the maximally entangled state $|\Psi_{00}\rangle\langle\Psi_{00}|$, where $|\Psi_{ij}\rangle_{AB} = \mathbb{1} \otimes \sigma_x^j \sigma_z^i (|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$ are the four Bell states. There is the promise [18] that the states are all either perfect, i.e., $\rho_{\Psi_{00}} = |\Psi_{00}\rangle\langle\Psi_{00}|$, or they have some noise corresponding to a mixed state ρ with unknown fidelity $F = \langle\Psi_{00}|\rho|\Psi_{00}\rangle \leq 1 - \epsilon$. Some verification device is able to perform local operations on the parts of the states at A and B with the task of discerning which is the case, up to some failure probability δ_{fail}. In this process, part of the ensemble is destroyed in order to examine whether $F = 1$. If that is the case, the conclusion is extended to the whole ensemble. Otherwise, all states are discarded. We show how our collective approach outperforms previous optimal strategies based on individual measurements [18–23].

The counter gate and d-level systems.—Our protocol relies on a d-level auxiliary bipartite entangled state used to encode information of the whole ensemble. In particular, we denote the d-dimensional maximally entangled states as $|\Phi^d_{mn}\rangle_{AB} = \sum_{k=0}^{d-1} e^{i2\pi km/d}|k\rangle_A|k\ominus n\rangle_B/\sqrt{d}$, where $k\ominus n \equiv (k-n) \mathrm{mod}\, d$, and the index n (m) is called the amplitude (phase) index. The auxiliary state is used to accumulate and measure the noise of an ensemble of multiple noisy states. This is achieved by means of the so-called "counter gate" [25,26] that transfers information from the ensemble of qubit states into the amplitude index of the auxiliary. This amplitude index can be read by locally measuring the state in the computational basis. The counter gate is defined as a bilateral controlled-X gate, acting from a qubit pair as source, to a qudit pair as target. Notice that the gate can be implemented locally. If the target system is in a maximally entangled state with phase index zero, its action is given by

$$b\mathrm{CX}^{AB}_{1\to 2}|mn\rangle_{A_1B_1}|\Phi^d_{0j}\rangle_{A_2B_2} = |mn\rangle_{A_1B_1}|\Phi^d_{0,j\ominus m\oplus n}\rangle_{A_2B_2}, \quad (1)$$

where $b\mathrm{CX}^{AB}_{1\to 2} = \mathrm{CX}_{A_1\to A_2} \otimes \mathrm{CX}_{B_1\to B_2}$, and $\mathrm{CX}_{1\to 2}$ is the hybrid controlled-X gate [27] $\mathrm{CX}_{1\to 2} = |0\rangle\langle 0| \otimes \mathbb{1}_d + |1\rangle\langle 1| \otimes X_d$. For convenience, 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, Eq. (1), with a type-1 (type-2) error state acting as control, leads to an amplitude index value of the auxiliary state increased (decreased) by 1, whereas it is left invariant if the control is a type-3 error state. Importantly, this invariance property also applies in cases in which the control system is in the $|\Psi_{00}\rangle$ state.

Proof of concept.—We provide a basic example based on simplified assumptions in order to illustrate the details of our procedure, the so-called "general error number gate protocol." One can, however, relax these assumptions to tackle a completely general situation (see below).

Consider an ensemble of n copies with the promise that all the states are either perfect Bell states $|\Psi_{00}\rangle\langle\Psi_{00}|$, or rank-2 states with only type-1 errors, i.e., $\rho = F|\Psi_{00}\rangle\langle\Psi_{00}| + (1-F)|01\rangle\langle 01|$. This corresponds (up to local unitaries) to a situation where independent decay channels act on a maximally entangled state $|\Psi_{10}\rangle\langle\Psi_{10}|$. Physically this relates to the decay of electronic excitations in atomic or ensemble-based quantum memories, but also to photon loss of photon-number states.

The protocol comprises the following steps (see Fig. 1). First, we apply the counter gate, Eq. (1), from each state in the ensemble to an auxiliary pure state $|\Phi^d_{00}\rangle\langle\Phi^d_{00}|$ with $d = n+1$. We show below that the auxiliary state can be constructed directly from the (noisy) ensemble copies. We denote these local operations together as the error number gate (ENG). The ENG changes the amplitude index of the auxiliary state depending on the actual form of the ensemble. (i) Pure ensemble: the ensemble is given by n copies of the $|\Psi_{00}\rangle\langle\Psi_{00}|$ state, and the application of the ENG leaves the auxiliary state invariant. (ii) Noisy ensemble: the ensemble is given by $\rho^{\otimes n}$, and it can hence contain type-1 error states. Whenever the counter gate is applied with a single type-1 error state, the amplitude index of the auxiliary state is increased by 1. After the application of the ENG, the ensemble and auxiliary states get correlated, i.e., ENG: $\rho^{\otimes n} \otimes |\Phi^d_{00}\rangle\langle\Phi^d_{00}| \to \sum_{j=0}^{n}\binom{n}{j}F^{n-j}(1-F)^j\Gamma_j \otimes |\Phi^d_{0j}\rangle\langle\Phi^d_{0j}|$, where Γ_j is a density operator corresponding to all permutations of $\{|\Psi_{00}\rangle^{\otimes(n-j)}|01\rangle^{\otimes j}\}$. By measuring the auxiliary state, we learn the value of j, each found with probability $p(j) = \binom{n}{j}F^{n-j}(1-F)^j$, that depends on the state fidelity F. In this case, the value of j indeed corresponds to the actual number of errors in the ensemble.

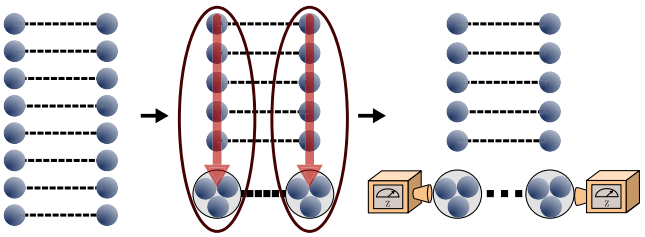

FIG. 1. Schematic representation of the protocol. The ENG is applied from the ensemble states to concentrate the noise into an auxiliary qudit state (which can be constructed by embedding ensemble copies). Finally, the d-level system is locally measured to detect the noise while the rest of copies are left untouched.

Whenever a value $j \neq 0$ is found, we can assert with certainty that we are in case (ii) and the ensemble is noisy with $F < 1$. On the other hand, if we obtain $j = 0$ we conclude, with some success probability, that the states of the ensemble are perfect Bell pairs $F = 1$ [case (i)]. In particular, the failure probability, i.e., measuring $j = 0$ while the initial state was $\rho^{\otimes n}$, is $\delta_f = F^n$. In this case we failed to identify the noisy ensemble, and would draw a wrong conclusion. For a fixed failure probability, one can determine the minimum number of ensemble states n (and therefore the minimum dimension of the auxiliary state) necessary to identify the case (i). Notice that the dimension d of the auxiliary state increases linearly with n, leading to an amount of entanglement (ebits) that only scales logarithmically with n, $\mathcal{O}(\log n)$. As we show below, this corresponds to the number of states from the initial ensemble that needs to be measured and destroyed.

A further improvement is possible. Since we are only interested in detecting whether $j \neq 0$, directly measuring the whole auxiliary state might not be the most efficient strategy. By performing a two-outcome measurement on each part of the auxiliary state, of the form $\{P_1, \mathbb{1} - P_1\}$, where $P_1 = \sum_{i=0}^{d/2-1}|2i\rangle\langle 2i|$ (note the sum up to $d/2-1$), one can determine the parity of j. Same (different) outcomes in A and B correspond to an even (odd) j value. We

denote this protocol as the "ENG subspaces protocol." Whenever j odd is obtained, we know with certainty that $j \neq 0$, and the ensemble is noisy [case (ii)]. In this case, one can recover the entanglement by performing an uncorrelating operation between the auxiliary state and the ensemble, such that we leave the auxiliary system in the $|\Phi^{d/2}_{0,j/2}\rangle\langle\Phi^{d/2}_{0,j/2}|$ state (see Sec. A in Supplemental Material (SM) [28] for details). The case (ii) is identified by consuming only 1 ebit. On the other hand, if j even is found, the ensemble is considered to be perfect [case (i)] up to some failure probability δ_1, which is now given by the probability of measuring that j is even, while the ensemble is still noisy, $\delta_1 = \sum_{j=0}^{n/2} \binom{n}{2j} F^{n-2j}(1-F)^{2j}$. One can reduce δ_1 by iteratively performing additional two-outcome measurements of the same form, learning—and consuming—1 ebit of information from the auxiliary state. The mth measurement can be written as $\{P_m, \mathbb{1} - P_m\}$, where now

$$P_m = \sum_{i=0}^{\frac{d}{2m}-1} \sum_{j=0}^{m-1} |2mi \oplus j\rangle\langle 2mi \oplus j|, \tag{2}$$

revealing whether the value of j is multiple of 2^m (or 0). The failure probability, i.e., the probability of the ensemble being noisy and the outcomes of all k measurements coinciding for A and B is

$$\delta_m = \sum_{k=0}^{n2^{-m}} \binom{n}{2^m k} F^{n-2^m k}(1-F)^{2^m k}. \tag{3}$$

For some fixed δ_t one can obtain the number (m) of measurements—number of ebits—required as a function of the ensemble fidelity F.

Observe that if an asymptotically large ensemble $n \to \infty$ is available, the required auxiliary entanglement needed for fixed δ_t becomes constant and independent of the fidelity of the initial states. In particular, the failure probability in the asymptotic case is $\delta_m = 2^{-m}$. The entanglement of the remaining subspaces is not spent or destroyed.

General case and results.—We show here that all the assumptions can be relaxed and a completely general scenario can be tackled, exhibiting a performance enhancement with respect to previous approaches. We consider arbitrary ensembles, where importantly, the auxiliary state can be directly constructed from several copies of the ensemble.

We have the promise that all the ensemble states are either perfect Bell states or Werner states [32] of the form

$$\rho = q|\Phi^d_{00}\rangle\langle\Phi^d_{00}| + \frac{1-q}{d^2}\mathbb{1}_{d^2}, \tag{4}$$

with $d = 2$, where the fidelity is given by $F = (1+3q)/4$. This situation is completely general since any state can be brought to this form by applying random local operations [33], without changing the fidelity. The protocol comprises the same steps as before, assuming for the moment (see below) that a maximally entangled state is available as auxiliary. However, one has to consider that now there are different kinds of errors, i.e., type-1 that increase, type-2 that decrease, and type-3 that leave invariant the amplitude bit j of the auxiliary state under the action of the ENG operation. A single copy of a Werner state can be interpreted as mixture of type-1,2,3 error states with probability $p_{1,2,3} = (1-F)/3$, and a Bell state with $p_0 = F$. Therefore, when applying the ENG from an ensemble of n copies, the value of the auxiliary amplitude index becomes $j = \Delta_{12} \bmod d$, where $\Delta_{12} = \#\text{type-1} - \#\text{type-2}$. The probability of obtaining a certain j is given by

$$\Pr(j) = \sum_{\substack{i,k,\ell=0 \\ i+k+\ell=n \\ k\ominus\ell=j}}^{n} \frac{n!}{i!k!\ell!}(p_0+p_3)^i p_1^k p_2^\ell. \tag{5}$$

In each term of the sum, the number of type-1 (type-2) errors is given by k (ℓ), and the number of states that are either $|\Psi_{00}\rangle$ or type-3 error state by i.

Note that the difference of errors can take $2n+1$ different values $\Delta_{12} \in \{-n, \ldots, n\}$, and one would need an auxiliary state of $d = 2n+1$ to distinguish between all of them. However, for our purpose we just need to determine when $\Delta_{12} = 0$, and therefore an auxiliary state of $d = n+1$ is sufficient, as $\Delta_{12} = 0 \Leftrightarrow \Delta_{12} \bmod (n+1) = 0$. The failure probability reads now $\delta = \Pr_{(j=0)}$.

We also consider here the subspaces ENG protocol. After measuring m subspaces, and following the same steps as before, one obtains information about the 2^m multiplicity of the auxiliary amplitude index. In this case, the probability of failing in determining the noiseless scenario after measuring m different subspaces is

$$\delta_m = \sum_{k=0}^{\lfloor n2^{-m} \rfloor} \Pr(2^m k). \tag{6}$$

Importantly, in the asymptotic limit we recover the constant behavior, i.e., the number of copies for a fixed failure

Algorithm 1. General ENG protocol overview.

Input: Ensemble of n identical quantum states, either $|\Psi_{00}\rangle$ or Werner-type states, Eq. (4), with $F < 1$.
1. Construct an auxiliary state of $d = n+1$ by embedding $\lceil \log_2(n+1) \rceil$ ensemble states.
2. Apply the ENG between the states of the ensemble and the auxiliary state.
3. Locally measure the auxiliary amplitude index j.

Output: Information of noise of the ensemble. If $j \neq 0$, the noisy case is identified with $P = 1$. If $j = 0$, the ensemble is certified with $P = 1 - \delta$.

Algorithm 2. Subspaces ENG protocol overview.

Input: Ensemble of n identical quantum states, either $|\Psi_{00}\rangle$ or Eq. (4).
1. Proceed as in Algorithm 1 steps 1-2.
2. Parties A and B measure the subspace corresponding to the first Bell pair of the auxiliary.
3. If different outcome is found in A and B, stop.
4. Measure the next subspace until different outcome is found or enough P_{fail} is achieved.

Output: 2^k multiplicity of the value of j after k rounds. The noisy case is identified with certainty if measurement outcomes differ at any point; otherwise the ensemble is certified with $P = 1 - \delta$.

probability is insensitive to the fidelity of the initial states, such that $\delta_m = 2^{-m}$.

So far we have assumed, for illustrative purposes, that a maximally entangled auxiliary state is available. This assumption is, however, not necessary, since the d-level auxiliary state can be always obtained by directly embedding—noisy—copies of the initial ensemble. Since the protocol is based on accumulating noise into the auxiliary state, by embedding several copies of the ensemble the performance is indeed enhanced, because noise already accumulates via embedding, before any other operation is applied. We define the embedding for perfect Bell states as $|\Phi_{00}^{2^k}\rangle_{AB} = |\Psi_{00}\rangle_{AB}^{\otimes k} = \sum_{i_1,\ldots,i_k} |i_k \ldots i_1\rangle_A |i_k \ldots i_1\rangle_B / \sqrt{2^k}$. This process with m copies of noisy Bell states ρ with fidelity F leads to a noisy d-level state of $d = 2^m$. The resulting state can be always depolarized into an isotropic form [34] of the form Eq. (4), with $d = 2^m$ and $q = (d^2 F^m - 1)/(d^2 - 1)$. If one directly measures the amplitude bit (j) of this state, before applying the ENG operation, the probability of measuring $j = 0$ is given by $\delta = (1 + dF^m)/(1 + d)$. The performance already approaches the optimal possible strategy based on measurements (see Sec. B in SM [28] for details). The number of copies needed in this global optimal strategy based on single-copy measurements scales as $k = \ln \delta / \ln F$ [18,35].

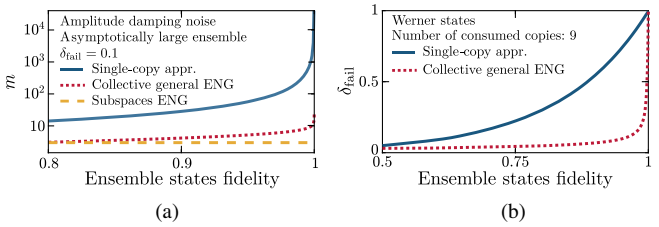

FIG. 2. Performance of the collective general ENG and the subspaces ENG protocols in comparison to optimal single-copy approach [18]. In (a) the number of consumed copies for rank-2 states for a fixed failure probability $\delta_{\text{fail}} = 0.1$. In (b) the failure probability when 9 copies are consumed for each strategy.

One can, however, enhance the protocol performance—overcoming previous optimal single-copy strategies—by applying the ENG operation from the ensemble states into the auxiliary one. This process collects the noise of the ensemble into the auxiliary and, together with the noise already accumulated by the embedding, increases the probability of detecting the noise. As before, in case noise is detected, we discard all the ensemble, whereas if the noiseless case is identified, the ensemble is kept and certified, and only the auxiliary states are consumed.

In order to construct an auxiliary state of dimension $d = n + 1$, which allows us to accumulate information about the noise of n ensemble states, one just needs to embed $m = \log_2(n + 1)$. Therefore, only m copies are eventually consumed, since the dimension of the auxiliary scales exponentially with the number of embedded states, leading to an exponential improvement in the scaling and allowing us to overcome previous optimal bounds.

Figure 2 shows several results comparing the performance of our protocol with respect to the optimal approaches based on individual measurements, under different situations. One can see an exponential-type improvement in all the cases. In particular, if an arbitrarily large ensemble is available, the subspaces ENG strategy exhibits a constant behavior independent of the fidelity of the initial states. See Sec. C in SM [28] for further analysis.

Generalizations.—We have considered the verification of Bell states. However, the applicability of our approach goes beyond such states. In particular, these techniques can be applied to verify any set of states for which there exists a subspace that is invariant under the counter operations [Eq. (1)] (or equivalent).

Some instances of states that can be verified include maximally entangled qudit states, or more general multipartite states. For the former case, the generalization is straightforward. Applying a generalized qudit-qudit controlled-X [36], $G\text{CX}|m\rangle|n\rangle = |m\rangle|n \oplus m\rangle$, in a bilateral way between a bipartite qudit and a maximally entangled system of dimension D [37], the effect is $bG\text{CX}|m^d n^d\rangle|\Phi_{0j}^D\rangle = |m^d n^d\rangle|\Phi_{0,j\ominus n\oplus m}^D\rangle$, where $j \ominus n \oplus n = (j - n + m) \bmod D$, similar than in the qubit case. Note that the dimension of the auxiliary should be adapted to the fact that errors can now increase or decrease the auxiliary amplitude bit by more than 1.

In a similar way, these techniques can be adapted to verify multipartite states. The invariant subspace of the generalized counter gate mCX [26] is spanned by $|00\ldots0\rangle$ and $|11\ldots1\rangle$, while the amplitude vector of the auxiliary d-level system is modified depending on the error state. Therefore, a verification procedure for the Greenberger-Horne-Zeilinger state $(|00\cdots0\rangle + |11\cdots1\rangle)/\sqrt{2}$ can be designed by extending the protocol for Bell states, since after applying the extended ENG the probability of obtaining a zero-valued amplitude index approaches zero when the number of copies in the ensemble increases.

However, to make the procedure fully general extra operations are required to detect phase errors; see Sec. D in SM [28] for details. Extension to more general graph states, following [38,39], might also be possible.

Conclusions.—We have proposed collective techniques that allow us to verify maximally entangled quantum states with enhanced performance as compared to previous (even optimal) strategies that operate on individual states. This is accomplished by transferring and accumulating (via a so-called ENG operation) the noise of some ensemble of states into a higher-dimensional auxiliary state. This auxiliary state can be constructed using a logarithmically reduced number of ensemble copies, which are the only ones eventually consumed. Because of the embedding process and the ENG operation, noise is enlarged into the auxiliary state, making its detection more efficient. In addition, we propose a strategy based on measuring only certain subspaces of the auxiliary state, such that in the asymptotic limit of a large enough ensemble, a constant number of consumed copies is enough for verifying the states independently of the fidelity or form of the states. The tools we introduce and make use of here are not only interesting in the context of certification of quantum states, but they can be particularly useful in other scenarios such as, e.g., fidelity estimation (see Sec. E in SM [28]) or fidelity witnessing (see follow-up work [29]). For the rank-2 example originating from decay noise, we can actually use our strategy not only to verify the ensemble, but to accurately estimate the fidelity by using only a logarithmic amount of extra entanglement, exponentially outperforming single-copy strategies.

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

J. M.-R. and F. R.-S. contributed equally to this work.

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).
[4] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Phys. Rev. A **59**, 4249 (1999).
[5] M. Hayashi and T. Morimae, Phys. Rev. Lett. **115**, 220502 (2015).
[6] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Theory Comput. Syst. **63**, 715 (2019).
[7] H. J. Kimble, Nature (London) **453**, 1023 (2008).
[8] S. Wehner, D. Elkouss, and R. Hanson, Science **362**, eaam9288 (2018).
[9] W. Kozlowski and S. Wehner, *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication, NANOCOM 2019* (Association for Computing Machinery, New York, 2019), 10.1145/3345312.3345497.
[10] K. Azuma, S. Bäuml, T. Coopmans, D. Elkouss, and B. Li, AVS Quantum Sci. **3**, 014101 (2021).
[11] A. Pirker, J. Wallnöfer, and W. Dür, New J. Phys. **20**, 053054 (2018).
[12] A. Pirker and W. Dür, New J. Phys. **21**, 033003 (2019).
[13] C. Meignant, D. Markham, and F. Grosshans, Phys. Rev. A **100**, 052333 (2019).
[14] L. Gyongyosi and S. Imre, Sci. Rep. **9**, 2219 (2019).
[15] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Nat. Rev. Phys. **2**, 382 (2020).
[16] X.-D. Yu, J. Shang, and O. Gühne, Adv. Quantum Technol. **5**, 2100126 (2022).
[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] S. Pallister, N. Linden, and A. Montanaro, Phys. Rev. Lett. **120**, 170502 (2018).
[19] Z. Li, Y.-G. Han, and H. Zhu, Phys. Rev. A **100**, 032316 (2019).
[20] K. Wang and M. Hayashi, Phys. Rev. A **100**, 032315 (2019).
[21] C. Bădescu, R. O'Donnell, and J. Wright, in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing* (ACM, New York, 2019), 10.1145/3313276.3316344.
[22] H. Zhu and M. Hayashi, Phys. Rev. A **99**, 052346 (2019).
[23] J. Morris, V. Saggio, A. Gočanin, and B. Dakić, Adv. Quantum Technol. **5**, 2100118 (2022).
[24] W.-H. Zhang, C. Zhang, Z. Chen, X.-X. Peng, X.-Y. Xu, P. Yin, S. Yu, X.-J. Ye, Y.-J. Han, J.-S. Xu, G. Chen, C.-F. Li, and G.-C. Guo, Phys. Rev. Lett. **125**, 030506 (2020).
[25] F. Riera-Sàbat, P. Sekatski, A. Pirker, and W. Dür, Phys. Rev. Lett. **127**, 040502 (2021).
[26] F. Riera-Sàbat, P. Sekatski, A. Pirker, and W. Dür, Phys. Rev. A **104**, 012419 (2021).
[27] J. Daboul, X. Wang, and B. C. Sanders, J. Phys. A **36**, 2525 (2003).
[28] See Supplemental Materials, which includes Refs. [29–31], at http://link.aps.org/supplemental/10.1103/PhysRevLett.129.190504 for discussions about decorrelation of the auxiliary state, further protocol performance and extensions analyses. All files related to a published paper are stored as a single deposit and assigned a Supplemental Material URL. This URL appears in the article's reference list.
[29] F. Riera-Sàbat, J. Miguel-Ramiro, and W. Dür, arXiv:2209.06849.
[30] W. Dür and J. I. Cirac, Phys. Rev. A **61**, 042314 (2000).
[31] S. T. Flammia and Y.-K. Liu, Phys. Rev. Lett. **106**, 230501 (2011).
[32] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[33] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[34] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[35] H. Zhu and M. Hayashi, Phys. Rev. A **99**, 052346 (2019).
[36] G. Alber, A. Delgado, N. Gisin, and I. Jex, J. Phys. A **34**, 8821 (2001).
[37] J. Miguel-Ramiro and W. Dür, Phys. Rev. A **98**, 042309 (2018).
[38] W. Dür, H. Aschauer, and H.-J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).
[39] C. Kruszynska, A. Miyake, H. J. Briegel, and W. Dür, Phys. Rev. A **74**, 052316 (2006).