Long-Range Big Quantum-Data Transmission

M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür

Phys. Rev. Lett. **120**, 030503 — Published 19 January 2018

DOI: 10.1103/PhysRevLett.120.030503

Long-range big quantum-data transmission

M. Zwerger[1,2], A. Pirker[1], V. Dunjko[1], H. J. Briegel[1,3] and W. Dür[1]
[1] *Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 21a, 6020 Innsbruck, Austria*
[2] *Departement Physik, Universität Basel, Klingelbergstraße 82, 4056 Basel, Switzerland*
[3] *Fachbereich Philosophie, Universität Konstanz, Universitätsstraße 10, 78464 Konstanz, Germany*
(Dated: November 28, 2017)

We introduce an alternative type of quantum repeater for long-range quantum communication with improved scaling with the distance. We show that by employing hashing, a deterministic entanglement distillation protocol with one-way communication, one obtains a scalable scheme that allows one to reach arbitrary distances, with constant overhead in resources per repeater station, and ultrahigh rates. In practical terms, we show that also with moderate resources of a few hundred qubits at each repeater station, one can reach intercontinental distances. At the same time, a measurement-based implementation allows one to tolerate high loss, but also operational and memory errors of the order of several percent per qubit. This opens the way for long-distance communication of big quantum data.

PACS numbers: 03.67.Hk, 03.67.Lx, 03.67.-a

Introduction.— Long-range quantum communication is a prominent application of emerging quantum technologies. It is a building block of quantum networks, with applications to secure channels [1–5], distributed quantum computation [6–9] or distributed sensing [10, 11]. Despite the quantum mechanical limits of repeater-less distribution of quantum information [12, 13], schemes which achieve the transmission of quantum information over noisy channels have been suggested. One approach uses quantum error correction (QEC), performed at regularly spaced stations, to protect quantum information [14–17]. Here the transmission is fast, however error thresholds for channel noise and local operations are rather stringent. Additionally, the overhead, i.e., the number of qubits that need to be processed and stored locally, are substantial, growing polylogarithmically with the distance. Entanglement-based quantum repeaters [18] (see also [19–27]) present a viable alternative, where entanglement is distributed over short distances, and a (nested) combination of entanglement swapping and distillation is used to create high fidelity entangled pairs over longer distances. Using recurrence-type entanglement distillation with two-way classical communication [28, 29], one obtains a scalable scheme with high noise tolerance for the channel and local operations, polynomially growing local resources and moderate rates [18]. The latter are mainly caused by the classical communication waiting times in entanglement distillation and can be overcome by using entanglement distillation protocols (EDP) with one-way communication [22].

Here, we present an alternative entanglement-based quantum repeater scheme utilizing hashing [30, 31] – an efficient, deterministic EDP with one-way classical communication. This allows the replacing of the nested entanglement purification and swapping of schemes based on recurrence protocols by a non-nested scheme, leading to an improved scaling of the required local resources with the distance [32]. Our scheme can handle channel errors and loss as well as operational and memory errors. It features ultra-high rates and large error thresholds achieved by a measurement-based implementation [15, 31, 33–35]. One-way classical communication also minimizes the required memory time, thereby reducing possible sources of imperfections. More importantly, the overhead in local resources, i.e., the number of ancillary qubits and operations needed at each repeater station per final qubit, is constant, i.e., independent from the distance. This is in stark contrast to previous schemes, where local resources grow polylogarithmically, or even polynomially. Furthermore, one can combine this approach with a heralded scheme to deal with arbitrary channel loss, the dominant source of noise in fiber or free-space photon transmission. This paves way towards efficient long-distance big quantum-data transmission, the essential ingredient in future quantum networks [36].

Setting and scheme.— We consider the settings where the quantum channel and the local processing of quantum information are lossy and/or noisy. To circumvent the problem of the absorption probability of the channel (e.g. optical fiber connecting repeater stations) growing exponentially quickly in the distance, we divide the channel into N segments of length $l_0 = L/N$, over which (noisy) Bell pairs are generated. One can also use heralded schemes to handle arbitrary (non-unit) channel loss. We assume n such Bell pairs are generated over each segment using n_c parallel channels. The noisy Bell pairs between two neighboring nodes are purified using the hashing EDP [30], deterministically generating a fraction of cn output pairs, where c depends on the initial pairs entropy. The resulting pairs are connected at the intermediate nodes via entanglement swapping, thereby generating cn long-distance entangled pairs between the end nodes. Given perfect local operations, hashing produces ideal pairs (asymptotically in n), that can be used to yield perfect long-distance entangled pairs. Below we show how a measurement-based implementation [31, 33] allows us to obtain a scheme generating entangled Bell pairs over arbitrary distances in the imperfect setting, where only the end node noise limits the fidelity. All operations are parallelizable, as only one-way classical communication is required, and all Pauli correction operations, occurring in the protocol, can be postponed to be performed just at the final outputs. The overall scheme is summarized in Fig. 1. A purely QEC-based version

without local two-way communication is also conceivable [37].

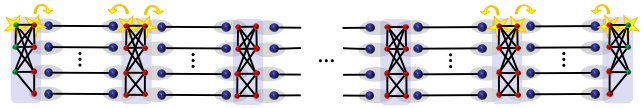

FIG. 1. Illustration of a quantum repeater based on hashing. The channel is divided into N elementary segments, where short-distance entangled pairs are generated over all segments, i.e., between all repeater stations, in parallel. Entanglement distillation via hashing and entanglement swapping are performed in a measurement-based way, by coupling the elementary pairs via Bell measurements to the locally stored resource state. In contrast to quantum repeaters based on recurrence protocols, no nesting is required. Direct encoded transmission would consist in sending encoded information sequentially through the channel. Please note that this is only an illustration, the real resource states contain at least order of one hundred qubits.

Measurement-based hashing.— We now briefly describe the key elements of our scheme, hashing and its measurement-based implementation, and discuss their features ensuring the efficiency and functionality in noisy settings.

Hashing distillation protocols operate collectively on a large ensemble of n noisy Bell-pairs. In a single round, bilateral CNOT operations between a subset of $\mathcal{O}(n)$ pairs and a target pair are applied, and the target pair is measured. This reveals information about the remaining ensemble, thereby purifying it. Repeating such rounds generates a fraction cn of perfect pairs deterministically in the limit $n \to \infty$. The protocol thus has a non-zero yield c in the noiseless case and only requires one-way classical communication. However, standard hashing fails if operations are noisy. As $\mathcal{O}(n)$ operations act on a single qubit, noise accumulates, washing out all information [31]. We resolve this using a measurement-based implementation [31], where local noise up to 7% per qubit, for imperfect resource states and imperfect measurements, is tolerated.

In a measurement-based implementation, quantum information is processed by measurements rather than gates [38, 39]. Similarly to teleportation, input qubits are coupled to an entangled resource state via Bell measurements, realizing the desired operation. For operations that include only Clifford gates and Pauli measurements – which is the case for EDP and entanglement swapping protocols considered here– the procedure is deterministic and the resource state consists of only input and output qubits. In fact, qubits that are measured in the Pauli basis (e.g., the target pairs in the hashing protocol) are unnecessary – a modified, smaller, resource state suffices, where the measurement results can be deduced from the in-coupling Bell measurement outcomes. The resource state corresponding to the hashing protocol has n input and cn output qubits, as the hashing protocol maps n Bell pairs to cn final pairs. The resource state at intermediate repeater stations, which combines hashing and entanglement swapping, is of size $2n$ (there are no output qubits, as entanglement swapping is performed on cn output pairs of the hashing protocol). This principle was used in [33, 35] to obtain resource states of minimal size for a recurrence-based repeater, and in [35, 40] the explicit construction of resource states for different tasks is considered. The key feature, that even complex circuits with many gates, can be implemented with a small resource state (in particular excluding qubits that are measured at any stage of the protocol) leads to a remarkable robustness of measurement-based implementations [15, 31, 33–35].

In a measurement-based approach, the noise is manifest in imperfect resource states and Bell measurements. We assume a local noise model for the resource states where local depolarizing noise (LDN) is applied independently to each of the resource qubits (see also [37]), as in [15, 31, 33–35]. Such a model is faithful if resource states are affected by local decoherence, or are themselves generated via distillation, as explained in [41] and [42]. Furthermore, this model accounts for the fact that generating entangled states of a larger number of qubits is experimentally more demanding. The imperfect Bell measurements are also modeled by local noise preceding an otherwise perfect measurement. Memory errors, modeled by local depolarizing noise, can also be accounted for in this way.

When performing a Bell measurement, one can effectively shift the noise between the two qubits [34, 35]. In particular, one can (formally) move the noise from input qubits of the local resource states onto the input Bell pair qubits, see figure 1, resulting in perfect resource states. Only noise on output qubits needs to be considered, which can be done afterwards. Hence, a noisy protocol is equivalent to a *perfect* protocol acting on more noisy inputs, where the output state is subsequently affected by local noise.

Repeater scheme in asymptotic noisy setting.— We now apply these insights to our repeater protocol in a setting where channels are lossy and noisy, entanglement distillation and Bell measurements are imperfect and memory errors for the storage of resource states or entangled pairs are accounted for. All noise processes can be included in noise acting on resource states, as argued above (for details regarding memory errors see [37]).

Resource states that we use at intermediate repeater stations have only input qubits, hence all noise can be (formally) moved to input pairs. Thus perfect hashing followed by perfect entanglement swapping is performed on more noisy Bell pairs. As perfect hashing asymptotically produces perfect states, we are in a situation where *perfect* Bell states are connected via entanglement swapping. This leads to Bell states at the end nodes, which are affected only by one-step local noise at the final stations. Note that the noise that acts at these final stations is independent from the distance, and is the only factor which determines the final achievable fidelity, in an asymptotic setting. The error threshold for the overall repeater scheme is the same as for measurement-based hashing, up to 7% local noise per qubit.

Communication rates and multiplexing.— Our version of the hashing protocol operates on n initial pairs, generated over short distance with sufficiently high fi-

delity. For instance, one can use a probabilistic (but heralded) scheme at this stage, where a pair is generated with probability η. We denote the required time that involves pair creation, photon transmission, classical communication time for heralding within an elementary segment by t_0. η includes channel loss and probabilistic interfaces, and can in principle be arbitrary small. The time required for the local processing of the pairs (in our case, the time to perform the Bell measurements) is denoted by t_p. In order to minimize the waiting time (and maximize the rate), we use n_c parallel channels. Choosing $n_c = n\,(1/\eta + \epsilon)$ suffices to obtain an elementary pair on n of these channels, except with probability $\mathcal{O}(e^{-\epsilon^2 n})$, from which $m = cn$ long-distance pairs are deterministically generated. We can choose $\epsilon = n^{-1/4}$, such that it vanishes as n increases. We obtain m Bell pairs over all N links within a *single* time step t_0 with exponentially increasing probability $\left(1 - \mathcal{O}(e^{-\epsilon^2 n})\right)^N$. Only the classical communication time $t_c = L/c_{fiber}$ (c_{fiber} is the speed of light in fiber) to transmit measurement outcomes depends on the distance L. The rate per channel is then given by $R = \frac{c\eta}{t_0 + t_p}$ in the limit $n \to \infty$. The classical communication time t_c does not enter because one can already start to process new elementary Bell pairs once the pairs from the previous round are processed. Note that t_0 can be made as small as the processing time by making the elementary segments short enough. The rate R is thus ultimately limited by $\frac{c\eta}{t_p}$, and thus by t_p, which is also the time scale which limits the rate of QEC-based repeaters [14]. For more details and examples see [37].

Hashing and repeaters with finite number of copies n.— So far we considered the scaling properties of the protocol in an asymptotic setting. Next, we show that for any fixed channel length, a finite number of pairs suffices. For this, we bound the fidelity of the resulting Bell pairs from the basic hashing from below. With this, one can then compute the fidelity of the final Bell pairs resulting from our protocol, the required number of copies for a hashing-based repeater, and the overall efficiency. Hashing produces $m = cn$ resulting Bell pairs out of n initial/noisy Bell pairs, which is also the number of final, long-distance output pairs, as hashing is deterministic. The yield is given by $c = m/n = 1 - S(W) - 2\delta$ [30], where $S(W)$ is the entropy of the ensemble of initial pairs and δ is a parameter which affects both the yield and the fidelity for finite sizes. The overhead per pair at each repeater station is determined by $O = 4n/m$ as $2n$ qubits are needed for the resource state and another $2n$ for the Bell pairs. The overhead is thus given by $O = 4(1 - S(W) - 2\delta)^{-1}$ and reaches the constant $4(1 - S(W))^{-1}$, which does not scale with the distance $L \sim N$, in the large n limit.

Next, we compute how the distance affects the final pair fidelity, before the noise of the local devices acts on the output pairs at the final repeater stations. This quantity, called *private fidelity*, bounds the correlations which an eavesdropper might have with the output pairs given the last noise step is independent of the eavesdropper [1, 5, 43]. Due to the measurement-based implementation we only need to analyze the scaling of the noiseless setting. The hashing protocol succeeds with a probability

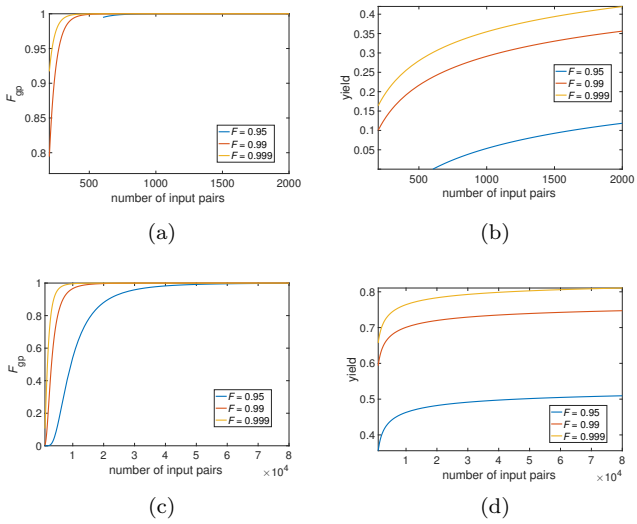

FIG. 2. Plot of the global, private fidelity and yield as a function of the number of initial pairs for $\delta = n^{-1/5}$ (a,b) and $\delta = n^{-1/3}$ (c,d). F denotes the fidelity of the initial Bell pairs, the number of repeater links is $N = 100$. We assume local depolarizing noise of 1% per qubit. The fact that the blue curve in (a) seems to starts "out of the blue" at around $n \approx 600$ is a consequence of the vanishing yield below this number (see (b)). In the choice of δ there is tradeoff between a higher fidelity (larger δ) and a higher yield (smaller δ). Additional data for more links can be found in [37].

of $1 - \mathcal{O}(\exp(-n\delta^2))$ [30], provided that the fidelity of the initial pairs is large enough (for Werner states the minimum fidelity is $F_{min} \approx 0.8107$). An appropriate choice of δ, such as $\delta = n^{-1/4}$, ensures that the success probability approaches unity. For the quantum repeater to succeed, the entanglement distillation processes at each of the N segments have succeed. The number of links N is proportional to the total length of the channel. For the global, private fidelity of all m outputs, one then obtains (see [37])

$$F_{\text{gp}} \geq (1 - \alpha\exp(-\beta n\delta^2))^N \approx 1 - N\alpha\exp(-\beta n\delta^2) \quad (1)$$

where α and β are constants depending on the form of the input Bell pairs (see also [37]). This shows that the choice of the number n of initial pairs has to depend on N, and therefore the length. While this number is increasing, the overhead per transmitted qubit is constant. Choosing n such that $N\alpha\exp(-\beta n^{1/2}) < \epsilon$ with ϵ small leads to F_{gp} close to unity, i.e., $F_{\text{gp}} \geq 1 - \epsilon$. We note that, from a practical perspective, one would however like to limit n, as a resource state of size $2n$ needs to be stored at each repeater station. The fidelity in eq. 1 is the fidelity of the entire set of m output pairs relative to a tensor-product state of m perfect pairs, and consequently, the same value is a (lousy) bound for the final fidelity of the individual pairs. From this one can also compute (a bound on) the output fidelity by applying the local depolarizing noise from the output qubits of the resource states.

For an illustration of the bounds on the global, private fidelity and the yield c for different values of the fidelity of the initial pairs for reasonable parameters, see Fig. 2.

We obtain the highest attainable fidelity if one measures all initial pairs except one, leading to a $n \to 1$

TABLE I. Comparison of key features of different quantum repeater architectures [14, 18, 22, 25] and our new protocol.

scheme	Knill & Laflamme	Briegel, Dür, Cirac & Zoller	Hartmann, Kraus, Briegel & Dür	Jiang, Taylor, Nemoto, Munro, Van Meter & Lukin	Zwerger, Pirker, Dunjko, Briegel & Dür
year	1996	1998	2007	2009	2017
based on	QEC	Bell pairs & two-way EDP	Bell pairs & one-way EDP	Bell pairs & QEC	Bell pairs & hashing
scaling of local resources	$\mathcal{O}\left(\text{polylog}(L)\right)$	$\mathcal{O}\left(\text{poly}(L)\right)$	$\mathcal{O}\left(\text{poly}(L)\right)$	$\mathcal{O}\left(\text{polylog}(L)\right)$	constant
rate determined by	$\frac{1}{\text{polylog}(L)\cdot t_p}$	$\frac{1}{\text{poly}(L)\cdot t_c}$	$\frac{1}{\text{poly}(L)\cdot max(t_p,t_0)}$	$\frac{1}{\text{polylog}(L)\cdot max(t_p,t_0)}$	$\frac{1}{\text{constant}\cdot max(t_p,t_0)}$
constraint on loss	yes	no	no	no	no

hashing protocol. The performance of the $n \to 1$ protocol is discussed in detail in [37]. The required number of copies to achieve purification depends on the initial fidelity of the pairs, where for channel noise of several percent a few hundred copies suffice.

Comparison of approaches The main advantage of our scheme over existing ones [14, 18, 22, 25] is the superior scaling of the local resources with the distance, which is reduced from polynomial [18, 22] or polylogarithmic [14, 25] to constant. The robustness to operational errors is comparable for all approaches assuming a measurement-based implementation [15, 31, 33]. Our scheme shares the high tolerance of loss errors during transmission with other entanglement-based quantum repeater architectures [18, 22, 25], which is due to the fact that one can use heralded schemes to create the initial Bell pairs. QEC-based schemes [14] are constrained, with a fundamental limit of 50% loss tolerance imposed by the no-cloning theorem [12]. The long distribution times of the 1998 protocol [18] are avoided since hashing is a deterministic one-way EDP. For a comparison of key features of quantum repeater protocols see Table I. In [37] we also compare the achievable rates and fidelities for our, and the 1998 protocol [18] for a measurement-based implementation with 1% LDN, up to 10^4 links. We find that the rates are up to nine orders of magnitude higher, and anticipate that they are two to three orders of magnitude higher compared to what QEC based quantum repeaters [14] achieve. Thus our new scheme, beyond superior asymptotic performance, also yields better numbers in real world regimes.

We note that since hashing protocols for the distillation of general graph states exist as well [44], the extension of our architecture to general multipartite quantum networks [45] is straightforward.

Summary and conclusion.— We have constructed a quantum repeater which operates with a constant local overhead. This is in stark contrast to all previous long-range communication proposals, which exhibit polynomial or poly-logarithmical overheads in local resources. This guarantees a non-zero yield, high rates and error thresholds for resource states of several percent, and opens the way for big data long-distance quantum communication. The scheme requires only short-time quantum memories for large resource states, and even intercontinental distances can be reached using only a few hundred qubits storage at each repeater station. The protocol has a computational overhead – the determination of the local correction operations from the classical hash functions, which is generally computationally expensive and might become relevant when the number of pairs becomes very large [46]. Even this eventuality could be circumvented by either using concatenated hashing of moderate-sized blocks, as discussed above, or through different one-way entanglement distillation protocols (with the same key features as hashing), based on e.g. efficiently decodable low-density parity check codes [46, 47] or Polar codes [48].

Our approach requires short-time storage of a number of qubits at each repeater station which is, arguably, large when compared to recent works focused on readily implementable settings. However, our scheme compensates by overcoming many of the drawbacks of existing schemes: it achieves high rates, makes repeaters fully scalable with a small overhead, while being robust against realistic channel and memory errors, and loss.

Acknowledgements.— This work was supported by the Austrian Science Fund (FWF): P28000-N27 and SFB F40-FoQus F4012, by the Swiss National Science Foundation (SNSF) through Grant number PP00P2-150579, the Army Research Laboratory Center for Distributed Quantum Information via the project SciNet and the EU via the integrated project SIQS.

[1] H. Aschauer and H. J. Briegel, Phys. Rev. Lett. **88**, 047902 (2002).
[2] C. Portmann, "Quantum authentication with key recycling," (2016), arXiv:1610.03422.
[3] S. Garg, H. Yuen, and M. Zhandry, "New security notions and feasibility results for authentication of quantum data," (2016), arXiv:1607.07759.

[4] A. Broadbent and E. Wainewright, Information Theoretic Security: 9th International Conference, ICITS 2016, Tacoma, WA, USA, August 9-12, 2016, Revised Selected Papers , 72 (2016).

[5] A. Pirker, V. Dunjko, W. Dür, and H. J. Briegel, New Journal of Physics (2017).

[6] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Phys. Rev. A **59**, 4249 (1999).

[7] R. V. Meter and M. Oskin, J. Emerg. Technol. Comput. Syst. **2**, 31 (2006).

[8] R. V. Meter, W. J. Munro, K. Nemoto, and K. M. Itoh, J. Emerg. Technol. Comput. Syst. **3**, 2:1 (2008).

[9] R. Beals, S. Brierley, O. Gray, A. W. Harrow, S. Kutin, N. Linden, D. Shepherd, and M. Stather, Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences **469** (2013).

[10] P. Komar, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sorensen, J. Ye, and M. D. Lukin, Nat Phys **10**, 582 (2014).

[11] Z. Eldredge, M. Foss-Feig, S. L. Rolston, and A. V. Gorshkov, "Optimal and Secure Measurement Protocols for Quantum Sensor Networks," (2016), arXiv:1607.04646.

[12] W. Wootters and W. Zurek, Nature **299**, 802 (1982).

[13] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).

[14] E. Knill and R. Laflamme, "Concatenated Quantum Codes," (1996), arXiv:quant-ph/9608012.

[15] M. Zwerger, H. J. Briegel, and W. Dür, Scientific Reports **4**, 5364 (2014).

[16] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014).

[17] F. Ewert, M. Bergmann, and P. van Loock, Phys. Rev. Lett. **117**, 210501 (2016).

[18] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[19] T. D. Ladd, P. van Loock, K. Nemoto, W. J. Munro, and Y. Yamamoto, New Journal of Physics **8**, 184 (2006).

[20] P. van Loock, T. D. Ladd, K. Sanaka, F. Yamaguchi, K. Nemoto, W. J. Munro, and Y. Yamamoto, Phys. Rev. Lett. **96**, 240501 (2006).

[21] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. Lett. **96**, 070504 (2006).

[22] L. Hartmann, B. Kraus, H.-J. Briegel, and W. Dür, Phys. Rev. A **75**, 032310 (2007).

[23] L. Jiang, J. M. Taylor, N. Khaneja, and M. D. Lukin, Proceedings of the National Academy of Sciences **104**, 17291 (2007), http://www.pnas.org/content/104/44/17291.full.pdf.

[24] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, Phys. Rev. Lett. **98**, 060502 (2007).

[25] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, Phys. Rev. A **79**, 032325 (2009).

[26] S. Bratzik, S. Abruzzo, H. Kampermann, and D. Bruß, Phys. Rev. A **87**, 062335 (2013).

[27] K. Azuma, K. Tamaki, and H.-K. Lo, Nat Commun **6**, 6787 (2015).

[28] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[29] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[30] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[31] M. Zwerger, H. J. Briegel, and W. Dür, Phys. Rev. A **90**, 012314 (2014).

[32] Simply using hashing instead of recurrence-based purification in standard schemes still yields a polynomial scaling. Critically, here we employ a deterministic one-way EDP with non-zero yield and the non-nested setting to achieve the constant scaling.

[33] M. Zwerger, W. Dür, and H. J. Briegel, Phys. Rev. A **85**, 062326 (2012).

[34] M. Zwerger, H. J. Briegel, and W. Dür, Phys. Rev. Lett. **110**, 260503 (2013).

[35] M. Zwerger, H. J. Briegel, and W. Dür, Applied Physics B **122**, 1 (2016).

[36] H. J. Kimble, Nature **453**, 1023 (2008).

[37] See supplemental material, which includes [49–60].

[38] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[39] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, Nat. Phys. , 19 (2009).

[40] A. Pirker, J. Wallnöfer, H. J. Briegel, and W. Dür, Phys. Rev. A **95**, 062332 (2017).

[41] R. Raussendorf, J. Harrington, and K. Goyal, Annals of Physics **321**, 2242 (2006).

[42] J. Wallnöfer and W. Dür, Phys. Rev. A **95**, 012303 (2017).

[43] A. Pirker, M. Zwerger, V. Dunjko, H. J. Briegel, and W. Dür, "Simple proof of confidentiality for private quantum channels in noisy environments," (2017), arXiv:1711.08897.

[44] W. Dür and H. J. Briegel, Reports on Progress in Physics **70**, 1381 (2007).

[45] J. Wallnöfer, M. Zwerger, C. Muschik, N. Sangouard, and W. Dür, Phys. Rev. A **94**, 052307 (2016).

[46] H. F. Chau and K. H. Ho, Quantum Information Processing **10**, 213 (2011).

[47] D. Gottesman, "Fault-tolerant quantum computation with constant overhead," (2013), arXiv:1310.2984.

[48] J. M. Renes, F. Dupuis, and R. Renner, Phys. Rev. Lett. **109**, 050504 (2012).

[49] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).

[50] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).

[51] S. Anders and H. J. Briegel, Phys. Rev. A **73**, 022334 (2006).

[52] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).

[53] C. F. Roos, G. P. T. Lancaster, M. Riebe, H. Häffner, W. Hänsel, S. Gulde, C. Becher, J. Eschner, F. Schmidt-Kaler, and R. Blatt, Phys. Rev. Lett. **92**, 220402 (2004).

[54] H. Häffner, F. Schmidt-Kaler, W. Hänsel, C. F. Roos, T. Körber, M. Chwalla, M. Riebe, J. Benhelm, U. D. Rapol, C. Becher, and R. Blatt, Applied Physics B **81**, 151 (2005).

[55] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, D. J. Twitchen, J. I. Cirac, and M. D. Lukin, Science **336**, 1283 (2012), http://science.sciencemag.org/content/336/6086/1283.full.pdf.

[56] K. Saeedi, S. Simmons, J. Z. Salvail, P. Dluhy, H. Riemann, N. V. Abrosimov, P. Becker, H.-J. Pohl, J. J. L. Morton, and M. L. W. Thewalt, Science **342**, 830 (2013), http://science.sciencemag.org/content/342/6160/830.full.pdf.

[57] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[58] L. Childress, J. M. Taylor, A. S. Sørensen, and M. D. Lukin, Phys. Rev. A **72**, 052330 (2005).

[59] W. Hoeffding, Journal of the American Statistical Association **58**, 13 (1963).

[60] G. Bennett, Journal of the American Statistical Association **57**, 33 (1962).