Efficient quantum computation in a network with probabilistic gates and logical encoding

J. Borregaard,[1] A. S. Sørensen,[2] J. I. Cirac,[3] and M. D. Lukin[1]

[1]*Department of Physics, Harvard University, Cambridge, MA 02138, USA*
[2]*The Niels Bohr Institute, University of Copenhagen,*
Blegdamsvej 17, DK-2100 Copenhagen Ø, Denmark
[3]*Max-Planck Institut für Quantenoptik, Hans-Kopfermann-Str. 1, D-85748 Garching, Germany*
(Dated: December 21, 2016)

A new approach to efficient quantum computation with probabilistic gates is proposed and analyzed in both a local and non-local setting. It combines heralded gates previously studied for atom or atom-like qubits with logical encoding from linear optical quantum computation in order to perform high fidelity quantum gates across a quantum network. The error-detecting properties of the heralded operations ensure high fidelity while the encoding makes it possible to correct for failed attempts such that deterministic and high-quality gates can be achieved. Importantly, this is robust to photon loss, which is typically the main obstacle to photonic based quantum information processing. Overall this approach opens a novel path towards quantum networks with atomic nodes and photonic links.

Quantum systems have the potential to revolutionize information technology by employing quantum computers [1, 2] and quantum cryptography [3]. In particular, quantum networks [4, 5] may enable novel applications ranging from distributed quantum computing [6–8] and secure multipartite function evaluation [9, 10] over cryptographic conferencing [11] to ultra-sensitive sensors [12]. However, a major obstacle against distributing quantum information is the detrimental effect of transmission losses. A so-called quantum repeater was first presented as a solution to this problem in the context of two-party quantum communication [13, 14]. In this approach, high-quality non-local entanglement is first created between quantum memories in a heralded fashion such that transmission losses only result in a finite success probability. Once the scheme is successful, the created high quality entangled states enable long distance communications through teleporation and deterministic local gate operations. The efficient light-matter coupling necessary for the entanglement generation can naturally be used to mediate the gate operation but such approaches suffer from photon losses and inefficiencies, which limit the gate fidelity. To overcome this, the concept of heralding was recently extended to gate operations [15–19]. In these schemes, the quantum gates are heralded by a measurement outcome that distinguishes whether a photon loss has occurred or not, similar to the non-local entanglement generation schemes. As a result, high fidelity gate operations are obtained in a successful event while the involved qubits must be discarded if the gate fails.

While heralded operations are directly applicable in quantum communication tasks [20], their application in quantum computation is less straightforward. It has been demonstrated how fault-tolerant, one-way quantum computation is possible with probabilistic operations [21–23] and in linear optical quantum computation (LOQC), the probabilistic operations are compensated by encoding in multi-photon states [24–27]. Both these approaches are, however, associated with substantial resource overhead

due to the necessity of generating large cluster states for one way quantum computing [28] and the upper bound of 50% for the success probability of Bell measurements with linear optics [29]. We present an alternative approach to universal quantum computation with probabilistic gates by combining heralded local operations previously studied for atomic qubits with logical encodings from LOQC. The heralding enables high fidelity operations while the logical encoding makes it possible to correct for failed attempts resulting in deterministic logical operations. Due to the higher success probability of the atomic gates, this approach is much less resource demanding than LOQC. Furthermore, the logical encoding enables computation within a circuit model, which circumvents the substantial qubit overhead of cluster state computation.

The proposed procedure is ideally suited for networks based on optically connected atoms or atom-like systems. The long coherence time of atomic qubits makes them ideal candidates for memory nodes in a quantum network. Entanglement can be efficiently distributed over long distances with photonic links, which enables non-local gates through teleportation. [6, 30]. By combining local heralded operations on atomic qubits with photonic links and encoding, we thus exploit the advantages of both approaches to perform efficient quantum computation in a network.

To illustrate the main idea, we consider combining the heralded controlled phase gate (CZ-gate) described in Ref. [15] with the parity encoding introduced in Refs. [26, 31]. The heralded CZ gate of Ref. [15] couples qubits through a cavity field and is heralded by a measurement on an auxiliary atom. This gate has a success probability, approaching unity in the limit of strong emitter cavity coupling with a unity fidelity $F = 1$ regardless of the coupling. A failed attempt of the gate leaks information about the two participating qubits to the environment corresponding to projecting onto the qubit basis. This type of error can be corrected (as described

below) if the cavity couples to closed transitions in the qubits such that the interaction with the environment is an effective dephasing process. Similar situations can be encountered in other heralded gate schemes [16–19] but we focus on the scheme of Ref. [15] for concreteness.

The logic encoding of Refs. [26, 31] was developed to protect against photon loss but as we show here, it can also be used to correct for the dephasing error following a failed attempt of the gate. The logical qubit states are encoded across n physical qubits in the form of GHZ states $|0^n\rangle = \frac{1}{\sqrt{2}}(|+\rangle^{\otimes n} + |-\rangle^{\otimes n})$ and $|1^n\rangle = \frac{1}{\sqrt{2}}(|+\rangle^{\otimes n} - |-\rangle^{\otimes n})$ where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. We will refer to $\{|+\rangle, |-\rangle\}$ as the rotated basis and $\{|0\rangle, |1\rangle\}$ as the qubit basis. A logical encoded qubit $|\Psi^n\rangle = a|0^n\rangle + b|1^n\rangle$ is protected from heralded errors leading to dephasing of a physical qubit. Following a dephasing error, the relevant qubit is measured in the qubit basis. If the qubit is measured to be in state $|0\rangle$, the remaining qubits will be in the state $|\Psi^{n-1}\rangle$ while if it is measured to be in state $|1\rangle$, the remaining qubits will be in state $a|1^{n-1}\rangle + b|0^{n-1}\rangle$, which is identical to $|\Psi^{n-1}\rangle$ up to a single qubit rotation. The logical state can thus be recovered after dephasing. Consequently, this encoding can be used to correct for a failed CZ-gate by measuring the state of the physical qubits and applying appropriate single qubit rotations. Every failed gate will remove one level of encoding from the logical states.

The logical qubits can be grown efficiently using methods known from cluster state preparation [23, 26]. To do this, we fuse together a (n)-qubit GHZ state with a (m)-qubit GHZ state by making a CNOT gate between one qubit from each GHZ state. We then measure the target qubit in the rotated basis and apply appropriate single qubit rotations based on the measurement result. The logical encoding means that if the CNOT gate fails, a qubit is removed from each of the two GHZ states resulting in ($n-1$)-qubit and ($m-1$)-qubit GHZ states. However, if the fusion succeeds a ($n+m-1$)-qubit GHZ state is prepared. Having prepared the resource state $|0^n\rangle$, a logical qubit $|\Psi^n\rangle = a|0^n\rangle + b|1^n\rangle$ is prepared by applying the operation $U_\psi = a\mathrm{I} + b\sigma_x$, on a single qubit belonging to $|0^n\rangle$. Here I is the identity and σ_x is a Pauli x-rotation of the qubit.

A universal set of quantum gates within the logical encoding can be obtained through Bell measurements, single qubit rotations, and an auxiliary multi-qubit resource state ($|0^n\rangle$) as described in Ref. [31]. The multi-qubit resource state is necessary for some of the gates in the universal set of which the logical CNOT gate is the most demanding [26] and we therefore focus on this. We transform the logical CNOT of Ref. [26] into our setup employing heralded CZ gates and auxiliary qubits. A schematic of the corresponding logical CNOT gate is shown in Fig. 1. Note that the logical CNOT, in principle, only requires two CNOT gates between physical qubits but we require two additional CNOT gates with auxiliary qubits in our setup. The auxiliary qubits are necessary because we are not making a direct CNOT gate

between physical qubits but an effective CNOT gate using single qubit rotations and a CZ-gate. An effective CNOT gate between qubit 1 (control) and qubit 2 (target) belonging to each their logical state is given by the operation $\mathcal{H}_2(CZ_{12})\mathcal{H}_2$ where $\mathcal{H}_i$ is a Hadamard transform on the i'th qubit and CZ_{ij} is a CZ-gate on qubits i and j. The first Hadamard on the target qubit, however, results in information about the logical state being leaked to the environment if the subsequent CZ gate fails. This can be circumvented by first entangling qubit 2 (control) with an auxiliary qubit (target) as incorporated in Fig. 1. This entanglement with the auxiliary qubit can be achieved with an effective CNOT gate since the auxiliary qubit will not leak information about the logical state in case of a failed CZ-gate. An effective CNOT can then be performed between qubit 1 (control) and the auxiliary qubit (target) and due to the entanglement with qubit 2, the auxiliary qubit will not leak information about the logical state if the CZ gate fails. In that case, the three qubits are simply measured and the logical states can be recovered with single qubit rotations. If the gate succeeds, qubit 2 is measured in the rotated basis and based on the measurement result, single qubit rotations are applied to the auxiliary qubit and qubit 1. This amounts to an effective CNOT between qubit 1 (control) and 2 (target) together with a state transfer of qubit 2 to the auxiliary qubit.
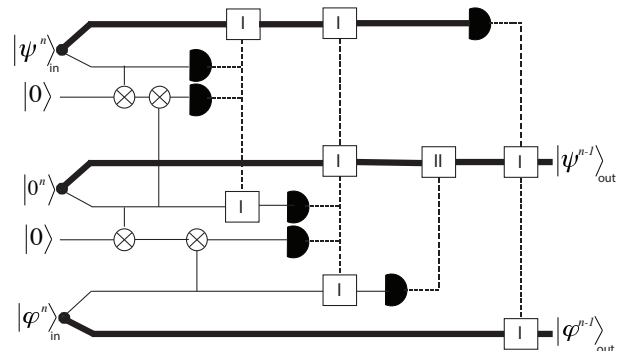

FIG. 1. Scheme of the logical CNOT gate. Crossed circles represent effective CNOT-gates with the cross marking the target qubit. Filled half-circles represent detectors, thick lines represent multi-qubit states and narrow lines are single qubit states. Based on the measurement results, Pauli rotations σ_z or σ_x are applied to either a single qubit (I) or multiple qubits (II). The final multi-qubit detection is a parity measurement. The scheme makes a logical CNOT between $|\psi\rangle$ (control) and $|\phi\rangle$ (target) and consumes at least one physical qubit from each state. Note that $|\psi\rangle$ is swapped to the resource state $|0^n\rangle$ in the process.

We numerically simulate a logical CNOT gate assuming all measurements and single qubit rotations are deterministic and that the associated errors of these are negligible compared to errors due to e.g. limited coherence time of the qubits. Failed gates decrease the encoding level and we require final re-encoding of the logical

qubits at the end of the logical gate operation to have a successful logical gate [32]. To simulate final re-encoding, we have assumed that the qubits that have been removed from the encoding are recycled at the end of the logical gate operation and grown into a GHZ state, which is then fused with the qubit state as described above using an auxiliary qubit and a heralded CZ gate.

The optimal performance of the logical CNOT gate for a given success probability of the heralded CZ-gate is found through numerical optimization. In the optimizations, we vary the encoding level n and calculate the mean total error probability for each n. This error probability consists of both the probability of non-heralded errors, e.g. due to finite coherence time, and the probability that the logical encoding is lost because of too many failed attempts. While increasing n decreases the probability of losing the logical encoding, it also decreases the effective coherence time of the logical state. From the simulations, we then find the encoding resulting in the smallest total error probability of the logical CNOT operation. We study two scenarios for implementing a logical CNOT gate. First, we describe a simple, local implementation where all qubits are trapped at the same node. Next, we describe a non-local implementation where the logical qubits are contained at different nodes in a network. Here, remote entanglement is used to teleport gate operations between the nodes resulting in a non-local logical CNOT gate for quantum networks. In both situations, we assume that a heralded CZ-gate can be performed between any two qubits at the same node.

In order to simulate the logical CNOT, we assume that the coherence time of the physical qubits is 1 s. Although this coherence time might be challenging in some systems, it has been achieved both with trapped ions [33] and in solid-state emitters [34]. The gate time and error of the heralded CZ-gate are assumed to be 10 μs and 10^{-4} motivated by a realization with Rb atoms [15]. Note that fast and efficient atomic state readout can be achieved through the cavity field [35]. The optimal performance and encoding level found from the simulations of a local CNOT gate are shown in Fig. 2a. The error in Fig. 2a is determined by the combination of a finite coherence time of the atoms and the gate time of the heralded CZ gate together with the error of the heralded CZ gate. The steep increase in the error probability shown in Fig. 2a for near-deterministic CZ-gates is where no encoding is used and the failure probability of the gate directly adds to the error probability. However, as encoding is employed to correct for the failed attempts, the error only increases by a factor of ~ 10 as the success probability of the CZ gate decreases from 99.5% to 70%. Even with a modest success probability of 75% for the heralded gates, an error probability of 1% can be attained. This demonstrates how the encoding can enable high fidelity, deterministic gates from heralded gates.

We now describe the non-local implementation of the logical CNOT gate, which exploits the efficient inter-
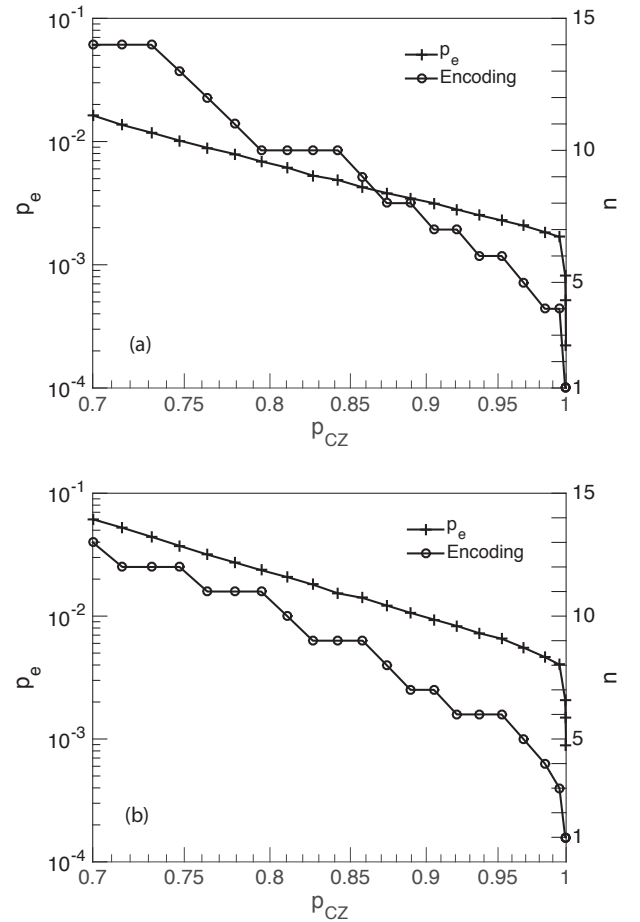

FIG. 2. Total error probability, p_e (left axis) and encoding level, n (right axis) of a (a) local and (b) non-local logical CNOT gate as a function of the success probability, p_{CZ} of the heralded CZ-gate. We have assumed that all qubits have a coherence time of 1 s and that the error of the heralded CZ-gate is 10^{-4}. The time of the CZ-gate is assumed to be 10 μs. Furthermore, we have assumed that the time necessary to make a Bell pair between two nodes (neighboring cavities) is 160 μs (10 μs) for the non-local implementation (see Fig. 3). Each point in the plots is obtained from averaging over $5 \cdot 10^4$ Monte Carlo simulations where the gates are picked to succeed or fail at random according to p_{CZ}. For non-encoded states ($n = 1$), a direct CNOT-gate is performed between the qubits without the use of a resource state.

face between photons and atomic or atom-like qubits provided by a cavity. If a high fidelity Bell pair can be generated between two nodes, a non-local gate between the nodes can be obtained by teleporting the local gates through the Bell pair as described in Refs. [6, 30]. There exist many proposals for non-local entanglement generation [36–38] but, in general, two-photon detection schemes [37, 38] obtain higher fidelity than one-photon detection schemes [36] and these have therefore been considered in great detail for quantum communication [20, 39, 40]. Inefficient photo detection, however, is detrimental to the rate in this case. Instead we consider

the scheme of Refs. [41, 42]. Here atomic detection, which in general is much more efficient, is employed instead of photo detection. Consequently, the rate of entanglement generation can be increased substantially while maintaining a high fidelity. To simulate a non-local version of the logical CNOT gate, we assume that such a scheme is used to generate high fidelity ($F \sim 1$) entanglement between cavities in a minimalistic setup shown in Fig. 3. The logical qubit and the resource state are assumed to be held in two different cavities that are spatially close to each other while optical fibers are used as channels between different nodes in the network. We have numer-
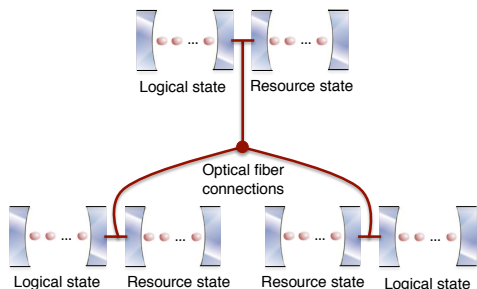

FIG. 3. Structure of the minimalistic quantum network with optical cavities considered for the simulation of the non-local CNOT gate. Each node consists of two cavities - one containing the encoded qubit state and one containing a resource state for logical operations. The nodes are assumed to be connected through optical fibers.

ically optimized the distributed CNOT gate and found the optimal encoding level for a given success probability of the heralded gate.

The result of the optimization is shown in Fig. 2b. As before, we have assumed a single qubit coherence time of 1 s and a heralded error of the CZ gate of 10^{-4}. The gate time was assumed to be 10 μs while the Bell state preparation time was assumed to be 160 μs corresponding to internodal distances around 10 km assuming that fiber losses at telecom wavelength limit the rate. The entanglement generation time between cavities within the same node was assumed to be 10 μs. The heralded error of a Bell state was assumed to be 10^{-4} and we have neglected any measurement error. Compared to Fig. 2a, the error in Fig. 2b is enhanced due to the relatively long preparation time of the Bell states. Furthermore, the scaling of the error with the success probability is less favorable due to the extra CZ-gates necessary to teleport the gate

operation through the Bell pairs. Nonetheless, the error only increases by a factor ~ 15 as the failure probability decreases from 99.5% to 70% in this minimalistic setup. An encoded error rate of 1% can be obtained with a success probability of $\sim 89\%$ for the heralded gates. The combination of heralded schemes ensuring high-fidelity operations in cavity setups with logical encoding is thus a promising approach to realize high-fidelity operations in an extended quantum network.

In conclusion, we have shown how heralded gate operations can be combined with logical encoding from LOQC to make efficient non-local operations in a quantum network. As opposed to the alternative method of using probabilistic gates for one way quantum computation our approach circumvents the generation of large graph states. In particular, it was argued in Ref. [28] that in order to simulate a quantum circuit of logical depth d involving n qubtis, an upper bound on the size of the graph state is on the order of $n^3 d$. The approach considered here thus gives a more efficient approach towards distributed quantum computing [6, 7] based on probabilistic gates, where separated resources are combined in order to perform a quantum algorithm. Given the difficulty in scaling up systems locally, the possibility of combining spatial separated resources might be an important step towards realizing realistic quantum computation. Non-local quantum gates are also naturally applicable in delegated quantum computing [43, 44] and secure multiparty function evaluation [9, 10] where quantum operations are performed on encrypted data in order to ensure the privacy of the involved parties. Other applications of quantum networks such as quantum enhanced metrology [12], anonymous quantum communication [45] and cryptographic conferencing [46] use non-local GHZ states between the nodes as resources. Such non-local GHZ states could be obtained using the deterministic non-local CNOT gate described here to fuse smaller GHZ state together in a repeater like setup.

[1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O/'Brien, Nature **464**, 45 (2010).
[2] N. Michael A. and C. Isaac L., *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] L.-M. Duan and C. Monroe, Rev. Mod. Phys. **82**, 1209 (2010).
[5] H. J. Kimble, Nature **453**, 1023 (2008).
[6] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000).

[7] 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), 10.1098/rspa.2012.0686.

[8] N. H. Nickerson, J. F. Fitzsimons, and S. C. Benjamin, Phys. Rev. X **4**, 041041 (2014).

[9] M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith, Foundations of Computer Science, 2006. FOCS '06. 47th Annual IEEE Symposium on , 249 (2006).

[10] F. Dupuis, J. Nielsen, and L. Salvail, Advances in Cryptology – CRYPTO 2012 **7417**, 794 (2012).

[11] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).

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

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

[14] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).

[15] J. Borregaard, P. Kómár, E. M. Kessler, A. S. Sørensen, and M. D. Lukin, Phys. Rev. Lett. **114**, 110502 (2015).

[16] S. Mahmoodian, P. Lodahl, and A. S. Sørensen, Phys. Rev. Lett. **117**, 240501 (2016).

[17] S. Das, A. Grankin, I. Iakoupov, E. Brion, J. Borregaard, R. Boddeda, I. Usmani, A. Ourjoumtsev, P. Grangier, and A. S. Sørensen, Phys. Rev. A **93**, 040303 (2016).

[18] L.-M. Duan, B. Wang, and H. J. Kimble, Phys. Rev. A **72**, 032333 (2005).

[19] I. Iakoupov, J. Borregaard, and A. S. Sørensen, arXiv:1610.09206 (2016).

[20] J. Borregaard, P. Kómár, E. M. Kessler, M. D. Lukin, and A. S. Sørensen, Phys. Rev. A **92**, 012307 (2015).

[21] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, Phys. Rev. Lett. **105**, 250502 (2010).

[22] K. Fujii and Y. Tokunaga, Phys. Rev. Lett. **105**, 250503 (2010).

[23] L.-M. Duan and R. Raussendorf, Phys. Rev. Lett. **95**, 080503 (2005).

[24] E. Knill, R. Laflamme, and G. J. Milburn, Nature **409**, 46 (2001).

[25] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).

[26] T. C. Ralph, A. J. F. Hayes, and A. Gilchrist, Phys. Rev. Lett. **95**, 100501 (2005).

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

[28] R. Raussendorf and H. J. Briegel, Quantum Info. Comput. **2**, 443 (2002).

[29] Y. Li, P. C. Humphreys, G. J. Mendoza, and S. C. Benjamin, Phys. Rev. X **5**, 041007 (2015).

[30] A. Sørensen and K. Mølmer, Phys. Rev. A **58**, 2745 (1998).

[31] A. Gilchrist, A. J. F. Hayes, and T. C. Ralph, Phys. Rev. A **75**, 052328 (2007).

[32] One could also employ intermediate re-encoding during the logical gate operation such that if the encoding level of any logical state drops below a certain limit, one attempts re-encoding before continuing with the logical gate operation. However, we only find very modest improvements for such strategies in the regime considered here and for simplicity, we therefore consider the case of no intermediate re-encoding.

[33] C. Langer, R. Ozeri, J. D. Jost, J. Chiaverini, B. De-Marco, A. Ben-Kish, R. B. Blakestad, J. Britton, D. B. Hume, W. M. Itano, D. Leibfried, R. Reichle, T. Rosenband, T. Schaetz, P. O. Schmidt, and D. J. Wineland, Phys. Rev. Lett. **95**, 060502 (2005).

[34] 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.

[35] A. Reiserer and G. Rempe, Rev. Mod. Phys. **87**, 1379 (2015).

[36] D. E. Browne, M. B. Plenio, and S. F. Huelga, Phys. Rev. Lett. **91**, 067901 (2003).

[37] L.-M. Duan and H. J. Kimble, Phys. Rev. Lett. **90**, 253601 (2003).

[38] D. Hucul, I. Inlek, V. G., C. Crocker, S. Debnath, S. M. Clark, and C. Monroe, Nature Physics **11**, 37 (2014).

[39] N. Sangouard, R. Dubessy, and C. Simon, Phys. Rev. A **79**, 042340 (2009).

[40] N. Sangouard, C. Simon, B. Zhao, Y.-A. Chen, H. de Riedmatten, J.-W. Pan, and N. Gisin, Phys. Rev. A **77**, 062301 (2008).

[41] S. J. van Enk, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **78**, 4293 (1997).

[42] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, Phys. Rev. Lett. **78**, 3221 (1997).

[43] A. Broadbent, Canadian Journal of Physics **93**, 941 (2015), http://dx.doi.org/10.1139/cjp-2015-0030.

[44] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, Nat Commun **5** (2014).

[45] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, Advances in Cryptology – ASIACRYPT 2007 **4833**, 460 (2007).

[46] K. Chen and H.-K. Lo, Proc. ISIT 2005. , 1607 (2005).