Ultrafast Long-Distance Quantum Communication with Static Linear Optics

Fabian Ewert,[*] Marcel Bergmann,[†] and Peter van Loock[‡]
Institute of Physics, Johannes Gutenberg-Universität Mainz, Staudingerweg 7, 55128 Mainz, Germany

(Received 29 April 2015; revised manuscript received 9 September 2016; published 14 November 2016)

We propose a projection measurement onto encoded Bell states with a static network of linear optical elements. By increasing the size of the quantum error correction code, both Bell measurement efficiency and photon-loss tolerance can be made arbitrarily high at the same time. As a main application, we show that all-optical quantum communication over large distances with communication rates similar to those of classical communication is possible solely based on local state teleportations using optical sources of encoded Bell states, fixed arrays of beam splitters, and photon detectors. As another application, generalizing state teleportation to gate teleportation for quantum computation, we find that in order to achieve universality the intrinsic loss tolerance must be sacrificed and a minimal amount of feedforward has to be added.

DOI: 10.1103/PhysRevLett.117.210501

Introduction.—Since the ground breaking work of Duan *et al.* (DLCZ, [1]) who showed that long-distance quantum communication (LDQC) is possible with linear optics and atomic-ensemble quantum memories, numerous advanced versions of their quantum repeater protocol have been proposed [2]. However, the probabilistic nature of entanglement distribution over lossy channels, purification, and swapping makes this type of nested quantum repeaters extremely slow, relying on two-way classical communication and long-lived quantum memories.

In recent years, various proposals have been made to employ quantum error correction (QEC) codes for LDQC. Since these codes suppress errors deterministically, long waiting times and two-way classical communication (and hence the use of quantum memories) can be, in principle, completely avoided. While one class of schemes focused on the correction of operational errors [3–6], another class did include QEC against transmission losses making high-rate loss-tolerant [7–9] or even fully fault-tolerant [10–13] LDQC possible. These latter schemes are limited only by the speed of the local gate operations and thus they approach rates as obtainable in classical communication. Our scheme also allows for ultrafast LDQC, but unlike [7,10,11] it does so in an all-optical fashion without the use of difficult local quantum gates (implementable via local nonlinear matter-light interactions [7,11]).

For this purpose, by employing a certain version of loss-tolerant parity codes [7,11,14], we suggest sending encoded qubit states directly, which are then subject to a Bell measurement (BM) together with locally prepared, encoded Bell states after every few kilometers (see Fig. 1). These local state teleportations allow for a nondestructive loss-error syndrome detection and a qubit state recovery in one step. The use of QEC by teleportation [15] along the channel is conceptually similar to the protocol of Ref. [11]. However, in our scheme, every teleportation is performed with optical (encoded) Bell states and linear optical elements [16]. It turns out that the encoding has two positive effects: the larger the code is, the more efficient the ideal BM (despite the linear-optics constraint [18]) and the higher the amount of tolerable photon loss becomes. In contrast to the all-optical scheme of Ref. [8], our logical BMs are conceptually different and work entirely without feedforward. This not only reduces the local operation times, but also makes on-chip integration along an optical fiber channel more feasible, as optical switching in this case is very sensitive to loss [19–21]. In an extended version of this work [22], we give further details on the loss resistance of our scheme and we show that it is also robust against a variety of additional errors such as depolarizing errors and detector inefficiencies (loss and dark counts) by performing a detailed secure-key-rate analysis. It is also demonstrated there that the scheme still works when photon-number-resolving detectors (as considered here) are replaced by on-off detectors. Beyond quantum communication, here

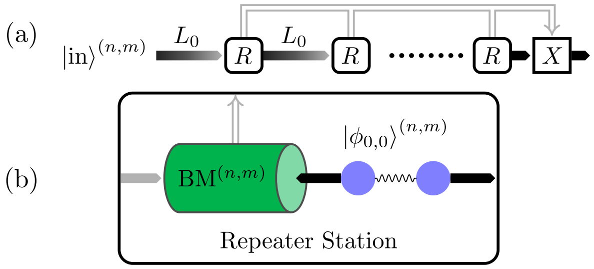

FIG. 1. One-way communication scheme: (a) To send a quantum state $|\mathrm{in}\rangle^{(n,m)}$ over a long distance, repeater stations (R) at shorter distances L_0 are used to recover the qubit from accumulated losses (fading arrows). A classical signal (double line) defines a single Pauli correction X at the receiver. (b) Each repeater station consists of an encoded Bell state and a highly efficient, loss-resistant, logical Bell Measurement ($\mathrm{BM}^{(n,m)}$) acting on the incoming signal and one half of the Bell state. The other half of the Bell state is sent to the next station along with the result of the BM (classical signal).

we show that for universal quantum computation, our encoded BM ceases to work under full loss tolerance, but ideal scalable quantum computation with linear optics is still possible with some but less feedforward compared to the Knill *et al.* (KLM [23]) and cluster-based [24–26] approaches.

Encoded Bell measurements.—The quantum parity code [QPC(n,m)] [11,14] encodes a logical qubit into nm physical qubits. The code can be understood as having three different levels of encoding. On the lowest level, which we call the physical level, we have standard dual-rail (DR, two-mode) qubits. These are typically realized by two orthogonal polarization modes of photons $\{|0\rangle = |H\rangle, |1\rangle = |V\rangle\}$, but also other realizations like spatial or temporal modes are possible. On the second level of encoding, the block level, m physical qubits are collected to represent a block qubit $\{|0\rangle^{(m)} = |H\rangle^{\otimes m}, |1\rangle^{(m)} = |V\rangle^{\otimes m}\}$. This repetition part of the code is crucial for the loss robustness as we see later. The highest encoding level is the logical level. Here n block qubits are used to construct the logical qubits as $|\pm\rangle^{(n,m)} = [|0\rangle^{(m)} \pm |1\rangle^{(m)}]^{\otimes n}/\sqrt{2^n} = [|\pm\rangle^{(m)}]^{\otimes n}$. The codewords are then naturally obtained by $|\pm\rangle^* = [|0\rangle^* \pm |1\rangle^*]/\sqrt{2}$, where the $*$ denotes the encoding level [blank for physical, (m) for block, and (n,m) for logical].

In all three encoding levels the four Bell states are defined as

$$|\phi_{k,l}\rangle^* = \frac{1}{\sqrt{2}}[|0,k\rangle^* + (-1)^l|1,1-k\rangle^*], \qquad (1)$$

with $k,l \in \{0,1\}$. A Bell measurement has to distinguish between these four Bell states. On the physical level, this can be partially achieved by combining the two polarization qubits at a 50:50 beam splitter followed by polarizing beam splitters and photon detectors [see Fig. 2(c)]. Unique click patterns are obtained for $|\phi_{1,0}\rangle$ and $|\phi_{1,1}\rangle$, whereas the states $|\phi_{0,l}\rangle$ are indistinguishable from each other. Thus, the overall BM efficiency is 50%, which is optimal for dual-rail encoding without ancilla photons or feedforward [18].

Our approach to a BM on QPC(n, m)-encoded qubits is based on the observation that Bell states of the higher encoding levels can be represented in terms of lower-encoding-level Bell states,

$$|\phi_{k,l}\rangle^{(m)} \cong \frac{1}{\sqrt{2^{m-1}}}\sum_{\vec{r}\in A_{l,m}}\bigotimes_{i=1}^{m}|\phi_{k,r_i}\rangle, \qquad (2)$$

$$|\phi_{k,l}\rangle^{(n,m)} \cong \frac{1}{\sqrt{2^{n-1}}}\sum_{\vec{s}\in A_{k,n}}\bigotimes_{i=1}^{n}|\phi_{s_i,l}\rangle^{(m)}, \qquad (3)$$

where the index set is defined as $A_{l,m} = \{\vec{r} \in \{0,1\}^m | \sum_{i=1}^m r_i = l (\mathrm{mod}\ 2)\}$ [27]. These relationships between Bell states of different encoding levels show that a logical BM can be realized by nm simultaneous standard BMs on the physical level.

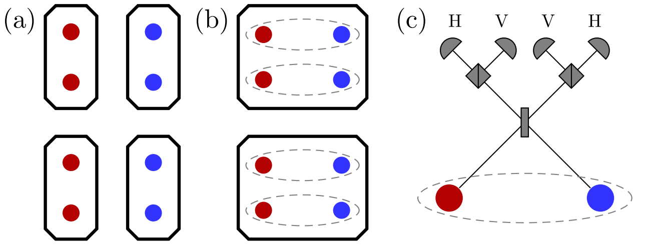

FIG. 2. Block structure and Bell measurement: (a) The block structure for two QPC(2,2)-qubits. The polarization qubits on the left (red) belong to the incoming signal and are thus subject to channel errors, while those on the right (blue) are part of the encoded Bell state provided in the repeater station. (b) In a Bell state in QPC encoding the qubits are joined blockwise. The dashed ellipses highlight physical-level qubit pairs that are combined at the BM. (c) Optical BM setup on the physical level adapted to polarization encoding.

Note that the above representations (2), (3) only hold after an appropriate reordering of the modes (indicated by $\cong$). Quite naturally, the photons of two logical qubits in a Bell state are each paired with their equivalent [see Figs. 2(a) and 2(b)]. In the following this reordering is omitted in the notation.

A Bell measurement on the block level is limited by the same $\frac{1}{2}$-efficiency as a physical BM, because the index k determining whether a BM on the physical level is successful is the same for all physical Bell states within a block Bell state. On the other hand, the index l is always identified correctly for $k=1$, because in that case the values r_i are all accessible. On the logical level, the situation is quite different. The index k is always identified correctly, because the values s_i from the block level are always available. Additionally, almost every time the index l will now be identified correctly as well, since it suffices to identify it in a single block. The only case where this is not possible is when all block-level Bell states are $|\phi_{0,l}\rangle^{(m)}$ states. This can only occur in the states $|\phi_{0,l}\rangle^{(n,m)}$ with a statistical weight of 2^{1-n}. Consequently, the chance to identify a logical Bell state correctly, i.e., the logical BM efficiency, is $1–2^{-n}$.

In addition to boosting the BM efficiency to near unity, the QPCs also protect the Bell measurement against photon loss. In accordance with our communication scheme depicted in Fig. 1, we assume that only the photons of one logical qubit participating in the BM are affected by loss [28]. Furthermore, we make the usual assumption that the probability to lose a photon $(1-\eta)$ is the same for all modes of a logical qubit. The probability of a successful logical Bell measurement in the presence of loss quantified by η can be derived from the Bell state representations (2) and (3). To identify the value of k in the state $|\phi_{k,l}\rangle^{(n,m)}$, a correct identification of every value s_i is required; i.e., in

TABLE I. BM success probability p in % for various QPC(n, m) and varying loss η.

(n, m)	$\eta = 1$	0.99	0.95	0.90	0.75	0.50	0.30
(1,1)	50	49.5	47.5	45	37.5	25	15
(2,2)	75	73.99	69.66	63.79	44.82	17.19	4.39
(3,10)	87.5	83.56	65.61	43.71	8.21	0.15	0.00
(6,5)	98.44	97.92	94.69	87.74	52.86	7.68	0.29
(10,3)	99.90	99.87	99.51	97.95	77.77	13.77	0.28
(23,5)	100.00	100.00	100.00	99.95	92.44	15.03	0.05

every block the first index must be determined. Equation (2) shows that this is possible, as long as in every block at least one physical Bell measurement identifies the first index. Since this is guaranteed as long as in every block at least one of the m photons (belonging to that logical qubit subject to loss) is not lost, the probability of correctly identifying k is given by $[1-(1-\eta)^m]^n$. In addition, in order to identify the index l in $|\phi_{k,l}\rangle^{(n,m)}$, it must be determined in at least one block. The probability to identify l in a block is given by $\eta^m/2$, because all values r_i are required, which means there are no photons lost at all, and because only the states $|\phi_{1,l}\rangle^{(m)}$ allow us to detect l with standard linear optical means. In other words, for the relevant logical qubit subject to loss, at least one photon must be left in every block and at least one block must remain entirely uncorrupted. The success probability of the logical BM is therefore given by

$$p = [1-(1-\eta)^m]^n - \left[1-(1-\eta)^m - \frac{\eta^m}{2}\right]^n, \qquad (4)$$

where the second term expresses that all terms where enough photons were left to identify k but no block allowed to identify l have to be discarded [29].

Table I shows the attainable BM efficiency for various amounts of loss. It indicates that the QPCs indeed protect the logical qubit from loss as long as $\eta > 0.5$, and also that, in general, n should be chosen sufficiently larger than m: a too large m increases the chance of corrupting every block. However, a too small m risks corrupting all photon pairs in a block. Increasing n on the other hand only gives more blocks, thus increasing the chance to get at least one without any corruption. Conceptually, this is the most important result obtained here: a larger code with a larger number of blocks n results in a higher linear-optics BM efficiency and a higher loss tolerance at the same time. This is different from other BM schemes where the loss tolerance is decreasing, which has to be counteracted by additional quantum error correction [30] or fast feedforward operations [8].

Long-distance quantum communication.—To send a QPC(n, m)-encoded qubit state over a total distance L we propose placing repeater stations after every channel segment with length L_0. At every station an encoded Bell state $|\phi_{0,0}\rangle^{(n,m)}$ is available on demand (i.e., created and consumed locally), and a logical BM is performed on one half of the Bell state together with the incoming encoded qubit (see Fig. 1). Between two stations every physical qubit suffers from loss according to a transmission coefficient of $\eta = \exp(-L_0/L_{\mathrm{att}})$ (with attenuation length $L_{\mathrm{att}} = 22$ km). Whenever the BM succeeds, the qubit state is recovered from loss and appears at the other half of the Bell state to be sent to the next station [15,31]. The total success rate [32] of the communication scheme is then given as $R = p^{L/L_0}/t_0$, where t_0 is the elementary time needed at every repeater station until the incoming signal qubit has been processed and a fresh encoded Bell state is ready for teleporting and error correcting the next qubit.

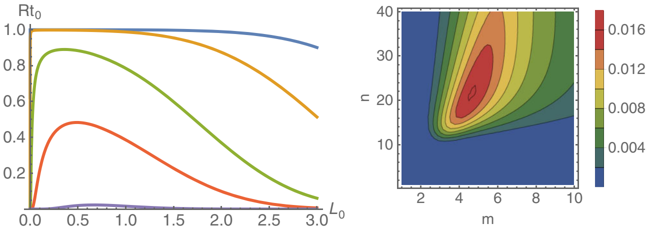

FIG. 3. Left: Total success probability Rt_0 vs repeater spacing L_0 in km for a communication distance of $L = 1000$ km and various encodings [from bottom to top, (10,3),(13,4),(16,4),(23,5),(35,6)]. Right: Inverse of the cost function $C_{1000\ \mathrm{km}}$ as a function of the code parameters n, m. At every point the optimal repeater spacing L_0 is chosen. The most cost-efficient code is (23,5) with a repeater spacing of $L_0 \approx 2.36$ km yielding $Rt_0 = 77.62\%$.

In addition to the repeater success probability Rt_0, which is depicted in Fig. 3 as a function of the repeater spacing L_0 for various code sizes, we are also interested in the cost effectiveness of our communication scheme. To this end, we define the cost function $C_L = (nm/Rt_0L_0)$ for a given total distance L similar to that in [11]. It relies on the assumption that the cost for creating the ancillary encoded Bell states at every repeater station scales linearly in nm (an all-optical method for state generation based on coherent photon conversion [33] that achieves this kind of scaling is presented in the Supplemental Material [34]). The inverse $1/C_L$, which corresponds to the repeater success probability per photons used, is also shown in Fig. 3 for a total communication distance $L = 1000$ km. Figure 3 indicates that total success rates extremely close to $R = 1/t_0$ can be achieved even for fairly large repeater spacings, but in terms of cost effectiveness a rate of about $R \approx 0.75/t_0$ yields better results [35].

Furthermore, for comparison the cost function C can also be applied to the case of (near) perfect Bell measurements on the physical level [38–40] (e.g., realized with additional atomic processing qubits [11]). While these better BMs allow for an efficient use of smaller codes, we found that for the optimal choices of n, m, and L_0 the ratio

$C_L(p_{\mathrm{BM}} = 0.5)/C_L(p_{\mathrm{BM}} = 1) \approx 3$ is almost independent of the communication distance L. This imposes a limit on how much more expensive perfect BMs should be compared to a standard optical BM with efficiency $\frac{1}{2}$.

We should also consider the effect of the elementary processing time t_0. Since our logical Bell states are assumed to be available on demand, t_0 corresponds only to the duration of the linear-optics processing with photon detection. Compared to those times required in a matter-based scheme with $t_0 \sim 1\ \mu\mathrm{s}$ (even assuming future enhanced ion-cavity coupling strengths [11]) or an all-optical scheme including feedforward [8] with $t_0 \sim 10$ ns (provided all circuits can be integrated [41]), corresponding to rates $R \sim$ MHz or $R \sim 0.1$ GHz, respectively, our static linear optical scheme allows, in principle, for GHz rates and beyond [42]. For our scheme to be free of feedforward at the intermediate stations, the updated (logical) Pauli frame after each teleportation must be classically communicated to the end of the channel for a final Pauli correction [43]. In general, let us discuss next universal gates and gate teleportation based on our encoded BM.

Quantum gate teleportation and quantum computation.—The physical Pauli operators of the QPC(n, m) may be denoted as $X_{i,j}, Y_{i,j}, Z_{i,j}$, with $i = 1 \ldots n$ and $j = 1 \ldots m$ labeling the (i, j)th DR qubit, while the logical operators are $X^{(n,m)} = X_{i,1} \ldots X_{i,m}$ (for any i) and $Z^{(n,m)} = Z_{1,j} \ldots Z_{n,j}$ (for any j) [11]. Therefore, Pauli logic can be performed directly via suitable Pauli gates on the DR qubits. This is sufficient for the final Pauli frame correction in our LDQC scheme as well as for quantum key distribution applications. More generally, logical X and Z rotations are then given by $\exp[-iX^{(n,m)}\theta/2]$ and $\exp[-iZ^{(n,m)}\theta/2]$, respectively, and for any $\theta \notin \pi\mathbb{Z}$ and $n > 1, m > 1$, an entangling operation is needed that acts on the physical qubits. Based on our encoded linear-optics BM, we can use logical gate teleportation with suitable encoded offline resource states [44] to implement arbitrary Clifford computations [including logical two-qubit gates such as $\textsc{cnot}^{(n,m)}$] in an intrinsically loss-tolerant fashion with no need for feedforward between the Clifford gates (and with only a final Pauli frame correction). This is a huge simplification compared to KLM [23] who require feedforward for every single CNOT and additional QEC codes to correct photon-loss errors. However, for universality, any single-qubit gate of KLM can be performed directly on the DR qubits, whereas in our general QPC(n, m) scheme, the logical non-Clifford gates do not allow for a static BM-based gate teleportation or a nonentangling transversal gate application. Therefore, for universality, we have to sacrifice the intrinsic loss tolerance and employ the most simple versions of the QPC such as QPC$(n, 1)$ [45]. In this case, an arbitrary logical X rotation $\exp[-iX^{(n,1)}\theta/2]$ can be done via the same rotation $\exp[-iX_{i,1}\theta/2]$ directly on the ith DR qubit (for any i) and the remaining set of Clifford operations [including a single-qubit $\pi/2$ rotation $\exp[-iZ^{(n,1)}\pi/4]$ for universality] can be achieved through gate teleportation using the static linear-optics BM scheme. Since QPC$(n, 1)$ is enough to realize arbitrarily efficient BMs (for sufficiently high n), efficient linear-optics quantum computation is possible provided a little, simple Pauli feedforward is added every time when a sequence of Clifford gates is followed by a non-Clifford gate. In terms of feedforward, this is also a simplification compared to existing schemes [48], where every two-qubit gate requires Pauli corrections on randomly selected physical qubits (for KLM [23]) or even non-Pauli feedforward is needed (for one-way quantum computation [24,41]).

Discussion and conclusions.—We proposed an efficient linear-optics BM onto QPC-encoded Bell states and showed that, by incorporating protection against transmission losses, it can be used to realize ultrafast high-rate LDQC in an all-optical fashion. With no need for matter qubits (neither as quantum memories nor as local quantum processors) or feedforward operations, our communication scheme is most suitable to be integrated along an optical fiber channel via chips that contain quantum sources [49–51], interferometers [52], and photon detectors [53]. Encoded-state preparations may be based either on nonlinear optical techniques [33] or on linear optics [8,9,22], then including feedforward [34].

We acknowledge support from Q.com (BMBF) and Hipercom (ERA-NET CHISTERA).

[*]ewertf@uni-mainz.de
[†]marcel.bergmann@uni-mainz.de
[‡]loock@uni-mainz.de

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

[2] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).

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

[4] W. Munro, K. Harrison, A. Stephens, S. Devitt, and K. Nemoto, Nat. Photonics **4**, 792 (2010).

[5] N. K. Bernardes and P. van Loock, Phys. Rev. A **86**, 052301 (2012).

[6] S. Bratzik, H. Kampermann, and D. Bruß, Phys. Rev. A **89**, 032335 (2014).

[7] W. Munro, A. Stephens, S. Devitt, K. Harrison, and K. Nemoto, Nat. Photonics **6**, 777 (2012).

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

[9] M. Pant, H. Krovi, D. Englund, and S. Guha, arXiv:1603.01353.

[10] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg, Phys. Rev. Lett. **104**, 180503 (2010).

[11] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Phys. Rev. Lett. **112**, 250501 (2014).
[12] R. Namiki, L. Jiang, J. Kim, and N. Lütkenhaus, arXiv:1605.00527.
[13] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Sci. Rep. **6**, 20463 (2016).
[14] T. C. Ralph, A. J. F. Hayes, and A. Gilchrist, Phys. Rev. Lett. **95**, 100501 (2005).
[15] E. Knill, Nature (London) **434**, 39 (2005).
[16] In terms of resources, our all-optical scheme is actually most close to that of Ref. [8], which employs nonlocally distributed loss-resistent cluster states and standard (non-logical) linear-optics BMs for entanglement connection. However, there, in order to suppress the effect of losses, fast feedforward operations are required at every repeater station to separate successful from failed BM events (depending only on the local BM results and independent of the classical information about neighboring BM outcomes like in multiplexed standard repeaters [17]).
[17] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, Phys. Rev. Lett. **98**, 060502 (2007).
[18] J. Calsamiglia and N. Lütkenhaus, Appl. Phys. B **72**, 67 (2001).
[19] B. J. Metcalf, J. B. Spring, P. C. Humphreys, N. Thomas-Peter, M. Barbieri, W. S. Kolthammer, X.-M. Jin, N. K. Langford, D. Kundys, J. C. Gates *et al.*, Nat. Photonics **8**, 770 (2014).
[20] D. Bonneau, G. J. Mendoza, J. L. O'Brien, and M. G. Thompson, New J. Phys. **17**, 043057 (2015).
[21] Another important complication when integrating feedforward on a chip is the need for synchronizing the optical and electrical signals. To be compatible with optical pulses much shorter than 1 ns, fast integrated electronic circuits (including measurements) with electronic bandwidths much greater than 1 GHz are required. Therefore, instead of real-time feedforward, simple postselection is often employed [19].
[22] F. Ewert and P. van Loock, arXiv:1610.04519.
[23] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[24] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[25] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).
[26] D. E. Browne and T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).
[27] See Supplemental Material http://link.aps.org/supplemental/10.1103/PhysRevLett.117.210501 for details on the derivation of these formulas.
[28] A discussion on the effect of imperfect ancillary Bell states including loss on these is presented in the Supplemental Material [34].
[29] An alternative, maybe more intuitive, way to derive this probability is given in the Supplemental Material [34].
[30] S.-W. Lee, K. Park, T. C. Ralph, and H. Jeong, Phys. Rev. Lett. **114**, 113603 (2015).
[31] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[32] Since photon loss alone is incapable of inducing bit-flip or phase-flip errors on dual-rail qubits, the total success rate is also the secure key rate of our scheme, because the quantum bit error rate vanishes.
[33] N. K. Langford, S. Ramelow, R. Prevedel, W. J. Munro, G. J. Milburn, and A. Zeilinger, Nature (London) **478**, 360 (2011).
[34] See Supplemental Material http://link.aps.org/supplemental/10.1103/PhysRevLett.117.210501 for details on the state generation schemes.
[35] The recent benchmarks for repeaterless quantum communication, the so-called Takeoka-Guha-Wilde (TGW) bound [36] and its refinements [37] relating to the transmission rate per mode, are comfortably beaten by or scheme; see [22].
[36] M. Takeoka, S. Guha, and M. M. Wilde, Nat. Commun. **5** (2014).
[37] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, arXiv:1510.08863.
[38] H. A. Zaidi and P. van Loock, Phys. Rev. Lett. **110**, 260501 (2013).
[39] W. P. Grice, Phys. Rev. A **84**, 042331 (2011).
[40] F. Ewert and P. van Loock, Phys. Rev. Lett. **113**, 140403 (2014).
[41] R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger, Nature (London) **445**, 65 (2007).
[42] Provided that the signal repetition rates and the detector bandwidths are sufficiently high.
[43] Any active operations at a finite gate speed would, of course, reduce the achievable rates despite the complete avoidance of such operations along the channel. However, for certain applications such as quantum key distribution, a final Pauli frame correction is not needed. More generally, often simple postselection suffices.
[44] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).
[45] If feedforward is allowed, there are ways to achieve universality in a loss-tolerant or even fault-tolerant fashion on QPC-type encoding [46,47].
[46] A. J. F. Hayes, A. Gilchrist, and T. C. Ralph, Phys. Rev. A **77**, 012310 (2008).
[47] A. J. F. Hayes, H. L. Haselgrove, A. Gilchrist, and T. C. Ralph, Phys. Rev. A **82**, 022323 (2010).
[48] Another huge simplification compared to KLM is that in this loss-free case on-off detectors are sufficient.
[49] J. Silverstone, D. Bonneau, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. Natarajan, M. Tanner, R. Hadfield *et al.*, Nat. Photonics **8**, 104 (2014).
[50] J. W. Silverstone, R. Santagati, D. Bonneau, M. J. Strain, M. Sorel, J. L. O'Brien, and M. G. Thompson, Nat. Commun. **6** (2015).
[51] J. B. Spring, P. S. Salter, B. J. Metcalf, P. C. Humphreys, M. Moore, N. Thomas-Peter, M. Barbieri, X.-M. Jin, N. K. Langford, W. S. Kolthammer *et al.*, Opt. Express **21**, 13522 (2013).
[52] A. Peruzzo, A. Laing, A. Politi, T. Rudolph, and J. L. O'Brien, Nat. Commun. **2**, 224 (2011).
[53] B. Calkins, P. L. Mennea, A. E. Lita, B. J. Metcalf, W. S. Kolthammer, A. Lamas-Linares, J. B. Spring, P. C. Humphreys, R. P. Mirin, J. C. Gates *et al.*, Opt. Express **21**, 22657 (2013).