nature COMMUNICATIONS

ARTICLE

Received 1 Jul 2015 | Accepted 10 Nov 2015 | Published 16 Dec 2015

DOI: 10.1038/ncomms10171 OPEN

All-photonic intercity quantum key distribution

Koji Azuma[1], Kiyoshi Tamaki[1] & William J. Munro[1]

Recent field demonstrations of quantum key distribution (QKD) networks hold promise for unconditionally secure communication. However, owing to loss in optical fibres, the length of point-to-point links is limited to a hundred kilometers, restricting the QKD networks to intracity. A natural way to expand the QKD network in a secure manner is to connect it to another one in a different city with quantum repeaters. But, this solution is overengineered unless such a backbone connection is intercontinental. Here we present a QKD protocol that could supersede even quantum repeaters for connecting QKD networks in different cities below 800 km distant. Nonetheless, in contrast to quantum repeaters, this protocol uses only a single intermediate node with optical devices, requiring neither quantum memories nor quantum error correction. Our all-photonic 'intercity' QKD protocol bridges large gaps between the conventional intracity QKD networks and the future intercontinental quantum repeaters, conceptually and technologically.

[1] NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan. Correspondence and requests for materials should be addressed to K.A. (email: azuma.koji@lab.ntt.co.jp).

In the conventional world, communication networks are connected to each other with backbone links. This way, a worldwide communication network such as the Internet is formed. Analogously, although recent field demonstrations for intracity quantum key distribution (QKD) networks hold promise for unconditionally secure communication with point-to-point links up to a 100 km (refs 1,2), such intracity networks will be connected by a backbone quantum link to build a worldwide QKD network in the future. In principle, from its core role, such a backbone quantum link might use more demanding devices than the usual links in the intracity QKD network, for example, in contrast to the cost-effective last-mile service[3,4]. Quantum repeaters[5–22] could be adopted as the backbone quantum link, given that the communication efficiency scales polynomially with the communication distance, compared with the exponential scaling of the conventional QKD links[1,2]. This polynomial scaling of quantum repeaters is necessary for intercontinental backbone quantum links. But, otherwise, quantum repeaters are overengineered from the following reasons: Major cities to be equipped with an intracity QKD network may be within a radius $<1{,}000$ km, and the polynomial scaling of quantum repeaters usually necessitates quantum memories[5–20] or quantum error correction[5,7,11,13,17–21]—which is extremely challenging as it requires a huge number of qubits as well as many repeater nodes. Therefore, an intercity backbone quantum link—which would be more effective in connecting intracity QKD networks in different major cities than quantum repeaters—may be in greater demand than an intercontinental one based on quantum repeaters, to compose the future worldwide QKD network.

The main point of this paper is to present such an intercity QKD protocol using only a single untrusted intermediate node between communicators. The node uses only single-photon sources, linear optical elements, single-photon detectors, optical switches and active feedforward techniques, requiring neither quantum memories nor quantum error correction, in contrast to other known protocols[5–24]. This implies that our protocol also has the following distinct advantages for the implementation. First, the absence of memories implies that the repetition rate can be increased as high as one wants within those allowed by the assumed optical devices. Second, the absence of matter systems makes coherent frequency converters for photons (to strengthen the coupling to matter[25] and to optical fibres[26]) unnecessary. Finally, our protocol could work at room temperature in principle, thanks to its all-photonic nature. Nonetheless, our scheme leads to a square root improvement in the secret key rate over conventional QKD schemes[1,2,27]. Moreover, our scheme could supersede even quantum repeater schemes[6,10,14] with atomic ensembles for the communication distances below 800 km. From a fundamental viewpoint, our scheme highlights conceptual differences between an entanglement-based QKD scheme[28,29] and its time-reversed version[30–32]—now called[32] measurement-device-independent QKD (mdiQKD) for the sake of closing all the security loopholes of measurement devices—as well as between QKD protocols and quantum repeaters for providing entanglement.

Results

Entanglement-based QKD and mdiQKD. Our protocol emerges from highlighting a difference between an entanglement-based QKD scheme[28,29] and the mdiQKD scheme[32]. Let us start by considering this. The schemes assume a single untrusted node C in the middle of communicators Alice and Bob, separated over distance L (Fig. 1). Here node C shares optical channels with Alice and Bob, whose transmittance is described by $\eta_{L/2}=e^{-L/(2l_{\rm att})}$ with attenuation length $l_{\rm att}$. The transmittance is equal to the arrival probability of a single photon through the lossy channels. Those protocols could provide Alice and Bob with a pair of bits for the secret key only when both photons—exchanged between node C and Alice and between node C and Bob—survive the loss in the optical channels. Hence, the number of trials required on average to obtain a pair of bits for the secret key is η_L^{-1} in both of the protocols. In fact, all known QKD protocols—including prepare-and-measure QKD schemes[1,2] whose final key rates G per pulse are now limited[27] by the Takeoka–Guha–Wilde (TGW) bound $2\log_2[(1+\eta_L)/(1-\eta_L)]$ because of the lack of intermediate nodes—share[1,2] this scaling without quantum memories[5–20,23,24] or quantum error correction[5,7,11,13,17–21]. In contrast, our protocol improves the scaling from η_L^{-1} to $\eta_L^{-1/2}(=\eta_{L/2}^{-1})$ only with the help of a single node without any of such demanding devices. The essence of our idea is to notice that the original scaling η_L^{-1} is caused by a fact that the pairings at node C for Bell pairs in the entanglement-based QKD scheme or for Bell measurements in the mdiQKD scheme (cf. Fig. 1) are predetermined independently of the occurrence of photon losses. In other words, to outperform the η_L^{-1} scaling, we need to make the pairings depend on the occurrences of photon losses. Interestingly, this is possible solely for the mdiQKD protocol, because it entangles photons after the transmission in contrast to the entanglement-based QKD scheme (cf. Fig. 1).

Basic idea of our adaptive mdiQKD. To be precise, we introduce our protocol regarded as an mdiQKD scheme, where node C adaptively performs the Bell measurements only on surviving photons under losses (Fig. 2). This protocol proceeds as follows: (i) Alice and Bob send m optical pulses in single-photon states—each of which is randomly selected from the eigenstates of complementary observables $\hat{Z}$ and $\hat{X}$—to node C simultaneously, using multiplexing. (ii) On receiving the pulses, node C applies quantum non-demolition (QND) measurements to the pulses to confirm the arrival of the single photons over lossy channels. (iii) Then, successfully arriving photons from Alice are paired with ones from Bob via optical switches at node C. (iv) Node C then performs a Bell measurement on each of these pairs. (v) Node C then announces the pairings and the measurement outcomes of the Bell measurements. (vi) Finally, as bits for the secret key, Alice and Bob keep the eigenvalues corresponding to their sent eigenstates to which the Bell measurements have been successfully applied. The bits obtained in step (vi) will be processed with a manner similar to the data that are kept after the

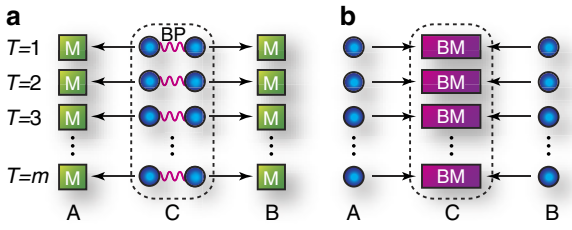

Figure 1 | Entanglement-based QKD and mdiQKD. T is the trial number. (**a**) In the entanglement-based QKD protocol, node C sends halves of Bell pairs (BP) to Alice and Bob who randomly perform Z-basis or X-basis measurement (M), respectively. (**b**) In the mdiQKD protocol, node C performs Bell measurements (BM) on photons that have been prepared randomly in one of the eigenstates of complementary observables $\hat{Z}$ and $\hat{X}$ and sent simultaneously by Alice and Bob. These protocols are related by a simple time reversal[32], requiring η_L^{-1} trials on average to obtain a pair of bits for the secret key.

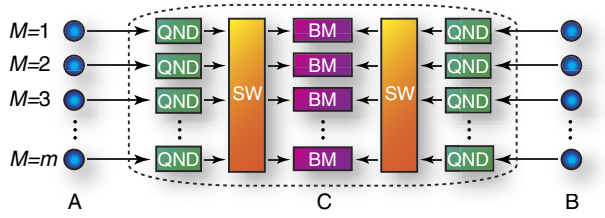

Figure 2 | Basic idea of our mdiQKD protocol with an adaptive Bell measurement. *M* is the pulse number. In this protocol, the node *C* first performs quantum non-demolition (QND) measurements to confirm the successful arrival of single photons, followed by optical switches (SW) to send the surviving photons to Bell measurement (BM) modules.

quantum communication phase of the original mdiQKD protocol[32].

Let us consider the scaling of our protocol. When Alice's and Bob's pulses are perfectly in single-photon states, the transmittance $\eta_{L/2}$ of the channels affects only the probability of confirming the arrival of single photons via QND measurements in step (ii). Since this probability is proportional to $\eta_{L/2}$, if the number m of multiplexing is larger than $\eta_{L/2}^{-1}$, one or more single photons arrive at node *C* from each of Alice and Bob with a high probability. Since the successful application of the Bell measurement to these single photons leads to a pair of bits for the secret key in step (vi), the communication resources such as required optical pulses and devices—which are proportional to the number m of the multiplexing—are in the order of $\eta_{L/2}^{-1}$. This is a square root improvement over conventional protocols[1,2], which results from making the pairings for the Bell measurement depend on the successful arrival of single photons.

More precisely, our protocol has a direct impact on the asymptotic sifted-key generation rate $R=\lim_{m\to\infty}\bar{n}_m/m$, where $\bar{n}_m$ is the average number of the sifted pairs for the number m of multiplexing. R is included in the final key rate formula G per pulse (normalized by the number of events of the same basis choice by Alice and Bob) as[1]

$$G=R[1-h(e_z)-h(e_x)], \tag{1}$$

where $h(x)$ is the binary entropy function defined by $h(x)=-x\log_2 x-(1-x)\log_2(1-x)$ and e_Z (e_X) is the error rate for Alice's and Bob's choice of *Z*-basis (*X*-basis)—called the bit-error rate (the phase-error rate). R for our protocol is given by

$$R=p_{\rm BM}p_{\rm QND}\eta_{L/2}\eta_{\rm s} \tag{2}$$

for Alice's and Bob's photon sources with efficiency $\eta_{\rm s}$, QND measurements with success probability $p_{\rm QND}$ and Bell measurements with success probability $p_{\rm BM}$ (see Methods). As the rate of the original mdiQKD protocol is $R=p_{\rm BM}\eta_L\eta_{\rm s}^2$, our protocol necessitates, at least,

$$p_{\rm QND}>\eta_{L/2}\eta_{\rm s} \tag{3}$$

to outperform it in terms of R. Given that $p_{\rm BM}$ contributes to $\bar{n}_m$ independently of m (see Methods), the number of multiplexing should be $m\sim(p_{\rm QND}\eta_{L/2}\eta_{\rm s})^{-1}$ to obtain R in the order of equation (2).

All-photonic implementation. To implement our protocol, we only need optical devices. The Bell measurement in step (iv) can be conducted just by using linear optical elements and single-photon detectors[33], similarly to the original mdiQKD scheme[32]. A challenging technique in our protocol is the QND measurement in step (ii). Besides many schemes for the QND measurement involving matter qubits or matter quantum memories, fortunately, there are several all-photonic schemes for the QND measurement for single photons[33]. Here we focus on a simple example, that is, a QND measurement for a single photon[34] based on quantum teleportation[35]. This scheme teleports the single-photon state of the incoming pulse to that of a half of a photonic Bell pair via the linear-optics-based Bell measurement, using the feature that the teleportation fails when the incoming pulse is in the vacuum state.

The protocol composed of steps (i)–(vi) is now implementable by using optical devices alone. However, the optical switch required in step (iii) may still be challenging because it should have the input modes in the order of $m\sim(p_{\rm QND}\eta_{L/2}\eta_{\rm s})^{-1}$ (for one or a few output modes). In particular, a large-scale optical switch to route a single photon in one of the many input modes into a Bell measurement module in step (iv) may be much more difficult than the existing ones[36–38] with a small number of input modes. For instance, although we can realize an $m\times 1$ optical switch by concatenating 2×1 optical switches with transmittance $\eta_{\rm sw}$ in a knockout tournament manner with depth $\lceil\log_2 m\rceil$, the transmittance of the large-scale optical switch decreases as $\eta_{\rm sw}^{\lceil\log_2 m\rceil}$, which may thus be needed to be taken care of in this case. However, remarkably, it is also possible to perform our protocol without using such a large-scale optical switch, that is, by using only single-mode on/off switches, a passive Hadamard linear optical circuit and single-photon detectors.

To achieve our protocol without large-scale optical switches, steps (iii)–(v) can be replaced with the followings: (iii') Then, a mode i ($i=1, 2, \ldots, m$) with a successfully arriving photon from Alice and a mode j ($j=m+1, m+2, \ldots, 2m$) with a successfully arriving photon from Bob are directly sent to the Hadamard linear optical circuit that acts on the $2m$ modes of node *C* as $\hat{a}_\nu^X=\sum_{\mu=1}^{2m}h_{\mu\nu}\hat{b}_\mu^X$ with an orthogonal $2m\times 2m$ Hadamard matrix $H=[h_{\mu\nu}]$ and annihilation operators $\{\hat{a}_\mu^X\}_{\mu=1,\ldots,2m;X=H,V}$ ($\{\hat{b}_\mu^X\}_{\mu=1,\ldots,2m;X=H,V}$) for the input (output) modes and their orthogonal polarizations H and V. Except for two modes i and j, all the optical modes are blocked off with the single-mode on/off switches. (iv') Node *C* then measures all the $2m$ output modes of the Hadamard linear optical circuit with polarization discriminating photon counters, and, if a photon with polarization H is found in output mode k and a photon with polarization V is found in output mode l ($k, l=1, 2, \ldots, 2m$), it regards this trial as successful application of a Bell measurement showing that input modes i and j have been in unnormalized Bell state $h_{ki}h_{lj}|HV\rangle_{ij}+h_{li}h_{kj}|VH\rangle_{ij}$. (v') Node *C* then announces input modes i and j and output modes k and l.

In the modified protocol here, since the sifted-key generation rate $R=P_m/m$ with success probability P_m of the protocol and error rates e_X and e_Z in the formula for the final key rate G per pulse are the functions of the number m of multiplexing, m should be chosen to maximize G, but $m\sim(p_{\rm QND}\eta_{L/2}\eta_{\rm s})^{-1}$ gives the maximum of G. The property of the Hadamard matrix that all the elements $h_{\mu\nu}$ are $1/\sqrt{2m}$ or $-1/\sqrt{2m}$ would be needed to suit the phase-error estimation in the mdiQKD (ref. 32). In fact, thanks to this property, the sequence of (iii')–(v') essentially performs a Bell measurement to distinguish Bell states $(|HV\rangle_{ij}\pm|VH\rangle_{ij})/\sqrt{2}$ from the other states, and the phase-error estimation in the original mdiQKD protocol[32] thus works even for our modified mdiQKD scheme in the same way. However, the Hadamard matrix exists only on restricted dimensional vector spaces, in contrast to a general Fourier transformation. For instance, it exists on 2^s-dimensional vector spaces with $s=1, 2, \ldots$. Hence, we use the Hadamard matrix on 2^s-dimensional vector spaces with $2^s=2m$, based on Sylvester's construction. The symmetry of this construction is indeed

favourable for calculating the performance of the modified protocol, because the effects of non-unity quantum efficiency of single-photon detectors in step (iv') can be regarded as losses in the input modes of the Hadamard linear optical circuit.

Performance of our all-photonic scheme. We now estimate the final key rate G for the original protocol with (iii)–(v) and the modified one with (iii')–(v'), assuming the all-photonic QND measurement based on quantum teleportation for step (ii). Our protocol needs an active feedforward technique with an optical switch. Suppose that a single active feedforward can be completed within time τ_a, during which photons run in optical fibres, being subject to the corresponding loss. In addition, we assume single-photon sources with efficiency η_s that emit pulses with duration τ_s and single-photon detectors with quantum efficiency η_d and with dark count rate ν_d. For simplicity, despite the being of various schemes for single-photon sources[39], since our protocol, in any case, necessitates the active feedforward technique, we assume a single-photon source[36,37,40] based on multiplexing of heralded single-photon sources. In fact, this photon source holds[40] promise for producing high-fidelity telecom single photons with the repetition rate of the slowest optical device at the expense of the use of (at least) one active feedforward, and it would be realizable just by using only a small amount of multiplexing[41,42]. Bell pairs for the all-photonic QND measurements in step (ii) can be generated in constant time τ_a with single-photon sources rather than a Bell-pair photon source, by paralleling a probabilistic procedure[43] with the active feedforward technique. In practice, this kind of step-wise preparation of Bell pairs may be useful for suppressing the unnecessary multi-photon components, because such multi-photon components may just contribute to events to be discarded as failure (as this kind of phenomenon indeed occurs sometimes[44]). In addition, note that we need to use one active feedforward in step (iii) or (iii').

Under these assumptions, the final key rates G are illustrated in Fig. 3 by assuming a collection of the state-of-art technologies[36,40,45–49]. Although the modified protocol merely uses the Hadamard matrix on 2^s-dimensional vector spaces with $2^s = 2m$, the key rates G labelled line (II) in Fig. 3 look like continuous for distance L, implying that the restricted choice of the Hadamard matrices is not a problem. Figure 3 shows that both of our original and modified protocols outperform the original mdiQKD protocol[32] (the TGW bound[27]) for distances L larger than $\sim$100 km ($\sim$200 km). These crossing distances are much smaller than those for quantum repeaters (for example, $\sim$500 km for protocols[14] based on atomic ensembles). Moreover, the performance of both our protocols is seven orders of magnitude better than that of the original mdiQKD protocol for $L = 800$ km. Since the assumed state-of-art technologies[36,40,45–49]—including the synchronization as seen in the experimental demonstrations[50–55] of the original mdiQKD (ref. 32)—work with 15 MHz at least[36], the key generation rate per second of our original protocol (the modified one) is then 1.7 kHz (0.69 kHz) for $L = 307$ km, which is a couple orders of magnitude better than experimental demonstrations[47,56] of QKD over the current record distance. More interestingly, the rate is 13 mHz (3.8 mHz) for $L = 800$ km, which is the same order of (only one order of magnitude less than) that of the best quantum repeater scheme[10] with atomic ensembles[14]. It is then clear that both of our schemes outperform the best quantum repeater scheme[10] below 800 km, if all the optical components work with 1 GHz as predicted to be possible[14,36,53,54]. The cutoff distances of $L \simeq 850$ km for both protocols in Fig. 3 are determined by the signal-to-noise ratio associated with the dark counting of the single-photon detectors. But the cutoff distances could be extended[57] if we replace the prepare-and-measure scheme of Fig. 2 between Alice (Bob) and node C with an entanglement-based one by putting an additional node with Bell-pair sources in between them.

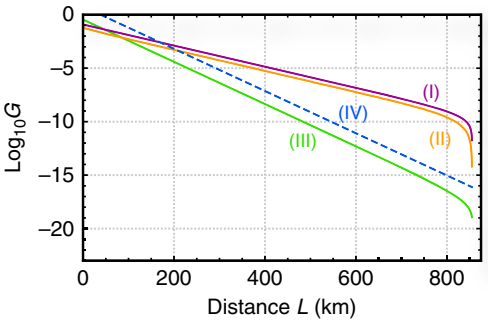

Figure 3 | Secret key rates G per pulse versus distances L. G is normalized by the number of events of the same basis choice by Alice and Bob. Here $\eta_s = 0.90$ (refs 40,45,46), $\tau_s = 100$ ps (ref. 47), $\eta_d = 0.93$ (ref. 48), $\nu_d = 1\,s^{-1}$ (refs 48,49), $\tau_a = 67$ ns (ref. 36), $l_{att} = 22$ km and $c = 2.0 \times 10^8\,m\,s^{-1}$. Lines (I)-(IV) represent our original protocol with steps (iii)-(v), our modified protocol with steps (iii')-(v'), the original mdiQKD protocol[32] with the same single-photon sources and the TGW bound[27] $2\log_2[(1+\eta_L)/(1-\eta_L)]$, respectively.

Discussion

We have presented an adaptive mdiQKD scheme that can present a square root improvement over conventional QKD schemes[1,2,27], superseding even quantum repeaters[14] for intercity distances. The 'adaptive' Bell measurement performed by node C in our scheme is also useful for providing a square root improvement for any single-photon-based entanglement generation protocol, for example, entanglement generation schemes for quantum repeaters with atomic ensembles[14]. However, note that it is impossible for our protocol alone to serve as quantum repeaters blessing an exponential improvement. In fact, although we can use our protocols as the entanglement generation for Alice's and Bob's stationary qubits by starting from entangling their photons with their stationary qubits, they need to wait the arrival of the heralding signals from node C in step (v) or (v') to identify the stationary qubits that have successfully been entangled, which is impossible without the memory function of their stationary qubits. This is an unbridgeable gap between our QKD protocol and quantum repeaters, and hence, for extremely long distances such as thousands of kilometres, quantum repeaters are needed. However, combined with all-photonic quantum repeaters[21], our protocol certainly paves a seamless route towards the all-optical realization of a worldwide QKD network—which would be not only a certain milestone[21] towards the all-photonic quantum computation[43,58] but also an ultimate challenge for the all-optical approach[59] in the field of conventional communication. Our protocol would also lead to unforeseeable attractive new twists—such as the realization of telescope arrays with much longer baselines than existing facilities[60] without quantum repeaters, the understanding of the fundamental limit for intercity/intercontinental quantum communication beyond the TGW bound and the finding of more practical variants of our protocol (for example, based on the combination of the time multiplexing with ultrafast single-photon sources for reducing the number of the QND measurement modules and on the hybridization of moderate-size optical switches and Hadamard-circuit-based Bell measurements

for decreasing the number of the required single-photon detectors).

Methods

Asymptotic sifted-key generation rate. The asymptotic sifted-key generation rate R of our protocol can be evaluated as follows. The probability $p_{k|m}$ with which node C finds the existence of $k(\leq m)$ single photons from Alice or Bob via QND measurements in step (ii) is

$$p_{k|m} = B_{k|m}\left(p_{\mathrm{QND}}\eta_{L/2}\eta_{\mathrm{s}}\right), \tag{4}$$

where $B_{k|m}(p)$ is the binomial distribution with $B_{k|m}(p) = \binom{m}{k}p^k(1-p)^{m-k}$. To make l pairs in step (iii), the node C should have found the existence of single photons $\geqslant l$ from both of Alice and Bob in step (ii), which occurs with probability $f_{l|m} = 2p_{l|m}\sum_{k=l}^{m}p_{k|m} - p_{l|m}^2$. Hence, the probability $P_{n|m}^{\mathrm{sif}}$ with which our protocol provides n pairs of bits for the sifted key in step (vi) is described as

$$P_{n|m}^{\mathrm{sif}} = \sum_{l=n}^{m} B_{n|l}(p_{\mathrm{BM}})f_{l|m}. \tag{5}$$

The average number $\bar{n}_m$ of sifted pairs is then

$$\bar{n}_m = \sum_{n=0}^{m} nP_{n|m}^{\mathrm{sif}} = p_{\mathrm{BM}}\sum_{l=0}^{m} f_{l|m}l = mp_{\mathrm{BM}}\left[p_{\mathrm{QND}}\eta_{L/2}\eta_{\mathrm{s}} - g_m\left(p_{\mathrm{QND}}\eta_{L/2}\eta_{\mathrm{s}}\right)\right], \tag{6}$$

where g_m is shown to be

$$g_m(p) = p(1-p)\left[\sum_{l=0}^{m-1} B_{l|m-1}^2(p) + \sum_{l=1}^{m-1} B_{l|m-1}(p)B_{l-1|m-1}(p)\right] \tag{7}$$

by using $lB_{l|m}(p) = mpB_{l-1|m-1}(p)$ for $l>0$ and $B_{k|m}(p) = (1-p)B_{k|m-1}(p) + pB_{k-1|m-1}(p)$ for $0<k<m$. Since the maximum of $B_{l|m-1}(p)$ over l goes to zero in the limit of $m\to\infty$, we have $\lim_{m\to\infty} g_m = 0$. Therefore, the asymptotic sifted-key generation rate $R = \lim_{m\to\infty}\bar{n}_m/m$ is described by equation (2).

References

1. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301 (2009).
2. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8,** 595–604 (2014).
3. Fröhlich, B. *et al.* A quantum access network. *Nature* **501,** 69–72 (2013).
4. Hughes, R. J. *et al.* Network-centric quantum communications with application to critical infrastructure protection, Preprint at http://arxiv.org/abs/1305.0305.
5. Briegel, H. J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81,** 5932–5935 (1998).
6. Duan, L.-M., Lukin, M. D., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414,** 413–418 (2001).
7. Kok, P., Williams, C. P. & Dowling, J. P. Construction of a quantum repeater with linear optics. *Phys. Rev. A* **68,** 022301 (2003).
8. Childress, L., Taylor, J. M., Sørensen, A. S. & Lukin, M. D. Fault-tolerant quantum communication based on solid-state photon emitters. *Phys. Rev. Lett.* **96,** 070504 (2006).
9. van Loock, P. *et al.* Hybrid quantum repeater using bright coherent light. *Phys. Rev. Lett.* **96,** 240501 (2006).
10. Simon, C. *et al.* Quantum repeaters with photon pair sources and multimode memories. *Phys. Rev. Lett.* **98,** 190503 (2007).
11. Jiang, L. *et al.* Quantum repeater with encoding. *Phys. Rev. A* **79,** 032325 (2009).
12. Azuma, K. *et al.* Optimal entanglement generation for efficient hybrid quantum repeaters. *Phys. Rev. A* **80,** 060303 (2009).
13. Munro, W. J., Harrison, K. A., Stephens, A. M., Devitt, S. J. & Nemoto, K. From quantum multiplexing to high-performance quantum networking. *Nat. Photon.* **4,** 792–796 (2010).
14. Sangouard, N., Simon, C., de Riedmatten, N. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83,** 33–80 (2011).
15. Azuma, K., Takeda, H., Koashi, M. & Imoto, N. Quantum repeaters and computation by a single module: remote nondestructive parity measurement. *Phys. Rev. A* **85,** 062309 (2012).
16. Azuma, K. & Kato, G. Optimal entanglement manipulation via coherent-state transmission. *Phys. Rev. A* **85,** 060303 (2012).
17. Zwerger, M., Dür, W. & Briegel, H. J. Measurement-based quantum repeaters. *Phys. Rev. A* **85,** 062326 (2012).
18. Munro, W. J., Stephens, A. M., Devitt, S. J., Harrison, K. A. & Nemoto, K. Quantum communication without the necessity of quantum memories. *Nat. Photon.* **6,** 777–781 (2012).
19. Li, Y., Barrett, S. D., Stace, T. M. & Benjamin, S. C. Long range failure-tolerant entanglement distribution. *New J. Phys.* **15,** 023012 (2013).
20. Grudka, A. *et al.* Long-distance quantum communication over noisy networks without long-time quantum memory. *Phys. Rev. A* **90,** 062311 (2014).
21. Azuma, K., Tamaki, K. & Lo, H.-K. All-photonic quantum repeaters. *Nat. Commun.* **6,** 6787 (2015).
22. Munro, W. J., Azuma, K., Tamaki, K. & Nemoto, K. Inside quantum repeaters. *IEEE J. Sel. Top. Quantum Electrons.* **21,** 6400813 (2015).
23. Abruzzo, S., Kampermann, H. & Bruß, D. Measurement-device-independent quantum key distribution with quantum memories. *Phys. Rev. A* **89,** 012301 (2014).
24. Panayi, C., Razavi, M., Ma, X. & Lütkenhaus, N. Memory-assisted measurement-device-independent quantum key distribution. *New J. Phys.* **16,** 043005 (2014).
25. Tanzilli, S. *et al.* A photonic quantum information interface. *Nature* **437,** 116–120 (2005).
26. Ikuta, R. *et al.* Wide-band quantum interface for visible-to-telecommunication wavelength conversion. *Nat. Commun.* **2,** 537 (2011).
27. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5,** 5235 (2014).
28. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
29. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68,** 557–559 (1992).
30. Biham, E., Huttner, B. & Mor, T. Quantum cryptographic network based on quantum memories. *Phys. Rev. A* **54,** 2651–2658 (1996).
31. Inamori, H. Security of practical time-reversed EPR quantum key distribution. *Algorithmica* **34,** 340–365 (2002).
32. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
33. Kok, P. *et al.* Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.* **79,** 135–174 (2007).
34. Kok, P., Lee, H. & Dowling, J. P. Single-photon quantum-nondemolition detectors constructed with linear optics and projective measurements. *Phys. Rev. A* **66,** 063814 (2002).
35. Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70,** 1895–1899 (1993).
36. Ma, X.-S., Zotter, S., Kofler, J., Jennewein, T. & Zeilinger, A. Experimental generation of single photons via active multiplexing. *Phys. Rev. A* **83,** 043814 (2011).
37. Collins, M. J. *et al.* Integrated spatial multiplexing of heralded single-photon sources. *Nat. Commun.* **4,** 2582 (2013).
38. Takesue, H. Entangling time-bin qubits with a switch. *Phys. Rev. A* **89,** 062328 (2014).
39. Eisaman, M. D., Fan, J., Migdall, A. & Polyakov, S. V. Invited review article: single-photon sources and detectors. *Rev. Sci. Instrum.* **82,** 071101 (2011).
40. Migdall, A. L., Branning, D. & Castelletto, S. Tailoring single-photon and multiphoton probabilities of a single-photon on-demand source. *Phys. Rev. A* **66,** 053805 (2002).
41. Christ, A. & Silberhorn, C. Limits on the deterministic creation of pure single-photon states using parametric down-conversion. *Phys Rev. A* **85,** 023829 (2012).
42. Bonneau, D., Mendoza, G. J., O'Brien, J. L. & Thompson, M. G. Effect of loss on multiplexed single-photon sources. *New J. Phys.* **17,** 043057 (2015).
43. Browne, D. E. & Rudolph, T. Resource-efficient linear optical quantum computation. *Phys. Rev. Lett.* **95,** 010501 (2005).
44. Zhao, B., Chen, Z. B., Chen, Y. A., Schmiedmayer, J. & Pan, J. W. Robust creation of entanglement between remote memory qubits. *Phys. Rev. Lett.* **98,** 240502 (2007).
45. Giustina, M. *et al.* Bell violation using entangled photons without the fair-sampling assumption. *Nature* **497,** 227–230 (2013).
46. Christensen, B. G. *et al.* Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.* **111,** 130406 (2013).
47. Shibata, H., Honjo, T. & Shimizu, K. Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors. *Opt. Lett.* **39,** 5078–5081 (2014).
48. Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nat. Photon.* **7,** 210–214 (2013).
49. Shibata, H. *et al.* Single-photon detection using magnesium diboride superconducting nanowires. *Appl. Phys. Lett.* **97,** 212504 (2010).
50. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111,** 130501 (2013).
51. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111,** 130502 (2013).

52. Ferreira da Silva, T. *et al.* Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88,** 052303 (2013).
53. Tang, Z. *et al.* Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112,** 190503 (2014).
54. Tang, Y.-L. *et al.* Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113,** 190501 (2014).
55. Tang, Y.-L. *et al.* Field test of measurement-device-independent quantum key distribution. *IEEE J. Sel. Top. Quantum Electron.* **21,** 6600407 (2015).
56. Korzh, B. *et al.* Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photon.* **9,** 163–168 (2015).
57. Jacobs, B. C., Pittman, T. B. & Franson, J. D. Quantum relays and noise suppression using linear optics. *Phys. Rev. A* **66,** 052307 (2002).
58. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409,** 46–52 (2001).
59. Shacham, A., Bergman, K. & Carloni, L. P. Photonic networks-on-chip for future generations of chip multiprocessors. *IEEE Trans. Comput.* **57,** 1246–1260 (2008).
60. Gottesman, D., Jennewein, T. & Croke, S. Longer-baseline telescopes using quantum repeaters. *Phys. Rev. Lett.* **109,** 070503 (2012).

Acknowledgements

We thank G. Kato, G. Knee, K. Matsumoto, F. Morikoshi, H. Takesue and A. Tomita, and especially M. Curty, H.-K. Lo and N. Lütkenhaus for valuable discussions.

This research is in part supported by the Project UQCC by the National Institute of Information and Communications Technology.

Author contributions

K.A. conceived the first version of the main concepts for our protocols. Then, all the authors contributed to the refinement and generalization of the concept and its presentation of the present paper.

Additional information

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Azuma, K. *et al.* All-photonic intercity quantum key distribution. *Nat. Commun.* 6:10171 doi: 10.1038/ncomms10171 (2015).