LETTER

https://doi.org/10.1038/s41586-018-0066-6

Overcoming the rate–distance limit of quantum key distribution without quantum repeaters

M. Lucamarini[1]*, Z. L. Yuan[1], J. F. Dynes[1] & A. J. Shields[1]

Quantum key distribution (QKD)[1,2] allows two distant parties to share encryption keys with security based on physical laws. Experimentally, QKD has been implemented via optical means, achieving key rates of 1.26 megabits per second over 50 kilometres of standard optical fibre[3] and of 1.16 bits per hour over 404 kilometres of ultralow-loss fibre in a measurement-device-independent configuration[4]. Increasing the bit rate and range of QKD is a formidable, but important, challenge. A related target, which is currently considered to be unfeasible without quantum repeaters[5–7], is overcoming the fundamental rate–distance limit of QKD[8]. This limit defines the maximum possible secret key rate that two parties can distil at a given distance using QKD and is quantified by the secret-key capacity of the quantum channel[9] that connects the parties. Here we introduce an alternative scheme for QKD whereby pairs of phase-randomized optical fields are first generated at two distant locations and then combined at a central measuring station. Fields imparted with the same random phase are 'twins' and can be used to distil a quantum key. The key rate of this twin-field QKD exhibits the same dependence on distance as does a quantum repeater, scaling with the square-root of the channel transmittance, irrespective of who (malicious or otherwise) is in control of the measuring station. However, unlike schemes that involve quantum repeaters, ours is feasible with current technology and presents manageable levels of noise even on 550 kilometres of standard optical fibre. This scheme is a promising step towards overcoming the rate–distance limit of QKD and greatly extending the range of secure quantum communications.

To introduce our scheme, we plot in Fig. 1a several conceptual bounds for the rate–distance dependence of QKD, under ideal experimental conditions (see parameters in the inset). Lines I–IV represent the key rates of quantum schemes obtained without resorting to a quantum repeater[5–7]; they are therefore denoted 'repeaterless bounds'. Line IV, in particular, is the secret-key capacity (SKC) of an optical quantum channel with losses[9], which quantifies the maximum amount of secret information that can be transmitted in QKD[8]. On the experimental side, the key rates that can be achieved currently are represented by red symbols. They show a similar dependence on distance to that of the repeaterless bounds, but with lower key rates, owing to source and detector losses and other experimental imperfections. This highlights a limitation of existing QKD schemes—they can never surpass the SKC bound.

With the aid of a quantum repeater[5–7], it would be possible to overcome this barrier. However, despite recent advances[10–13], such a device remains difficult to realize. One of the simplest versions, tailored for intercity distances[13], avoids using quantum memories and quantum error correction, but still requires non-demolition measurements, conditional optical switches and the multiplexing of a large number of single photon sources, all of which is far from trivial to implement. As a result, there is yet to be an experimental realization of a scheme that surpasses the SKC barrier. Although a trusted-node network[14] and the use of satellites[15] can greatly extend the reach of quantum communications, they do not exceed the SKC barrier. In the former case, the information ceases to be quantum at each intermediate node. For the latter, outer space provides a low-loss propagation medium, but the key rate per loss unit remains unchanged.

On the other hand, the scheme presented here can overcome the point-to-point SKC[9]. This is demonstrated in Fig. 1a, in which we anticipate the twin-field QKD (TF-QKD) key rates (thick lines). The ideal TF-QKD (dashed line) overcomes the repeaterless bounds after 200 km of standard optical fibre (lighter-pink shaded area). Even when realistic parameters are considered (solid line), TF-QKD can surpass the ideal repeaterless bound after 340 km of optical fibre (darker-pink shaded area). The gradient of the TF-QKD key rates resembles that of a single quantum repeater connecting two end points[16] (also plotted in Fig. 1a). Whereas the key rate of conventional QKD scales linearly with the channel transmittance η when $\eta \ll 1$, that of TF-QKD scales with $\eta^{1/2}$, thus markedly improving the rate–distance figure. Although a rigorous proof of the key rate unconditional security is beyond the scope of this paper, this change in the loss dependence constitutes a fundamental advance in QKD.

In TF-QKD, dim optical pulses are generated by two light sources, which are phase-randomized and then phase-encoded with secret bits and bases. The pulses are sent to interfere[17] on the beam splitter of an intermediate station, 'Charlie', who could even be a malicious party. Depending on which detector clicks, Charlie can infer whether the secret bits of the users (Alice and Bob) are equal (00 or 11) or different (01 or 10), but cannot learn their absolute values (0 or 1). This feature guards the scheme against eavesdropping, in a manner similar to phase-based measurement-device-independent (MDI) QKD[18,19]. However, TF-QKD also uses phase randomization and decoy states[20–22] to extend the distance of quantum communications considerably. This, in turn, resembles decoy-state MDI-QKD[23]. In decoy-state MDI-QKD, the users send two photons, one each, to the central station to cause a two-photon interference followed by a coincidence count in Charlie's detectors. In TF-QKD, on the other hand, they send two optical fields, to produce a single-photon interference followed by a single-photon detection event. This lets TF-QKD retain the MDI characteristic, while gaining the square-root dependance of the key rate on the channel transmittance. Moreover, this method provides an advantage over MDI-QKD even at short distances when Charlie's detectors have low efficiency.

As depicted in Fig. 1b, TF-QKD adopts the same components as decoy-state MDI-QKD, so it can readily be implemented. However, it requires the coordinated phase randomization of the twin fields. This randomization is initially performed by Alice and Bob independently of each other, by picking phase values ρ_a (Alice) and ρ_b (Bob) at random in the semi-open interval $[0, 2\pi)$, in a manner similar to what has been suggested for the error-correction routine of MDI-QKD[24]. The phase interval is split into M phase slices $\Delta_k = 2\pi k/M$, with $k = \{0, \ldots, M-1\}$ (see example in Fig. 1c), from which partial phase slices $\Delta_{k(a)}$ and $\Delta_{k(b)}$ are defined for Alice and Bob, respectively. The phase values that are picked randomly by the users necessarily fall in one of the phase slices. To identify the twin fields, the users publicly reveal $\Delta_{k(a,b)}$ together with the preparation bases. They keep only the runs with matching values and discard all of the others. This means that ρ_a and ρ_b will always differ by less than $2\pi/M$ for a pair of twin fields and that there will be

[1]Toshiba Research Europe, Cambridge, UK. *e-mail: marco.lucamarini@crl.toshiba.co.uk

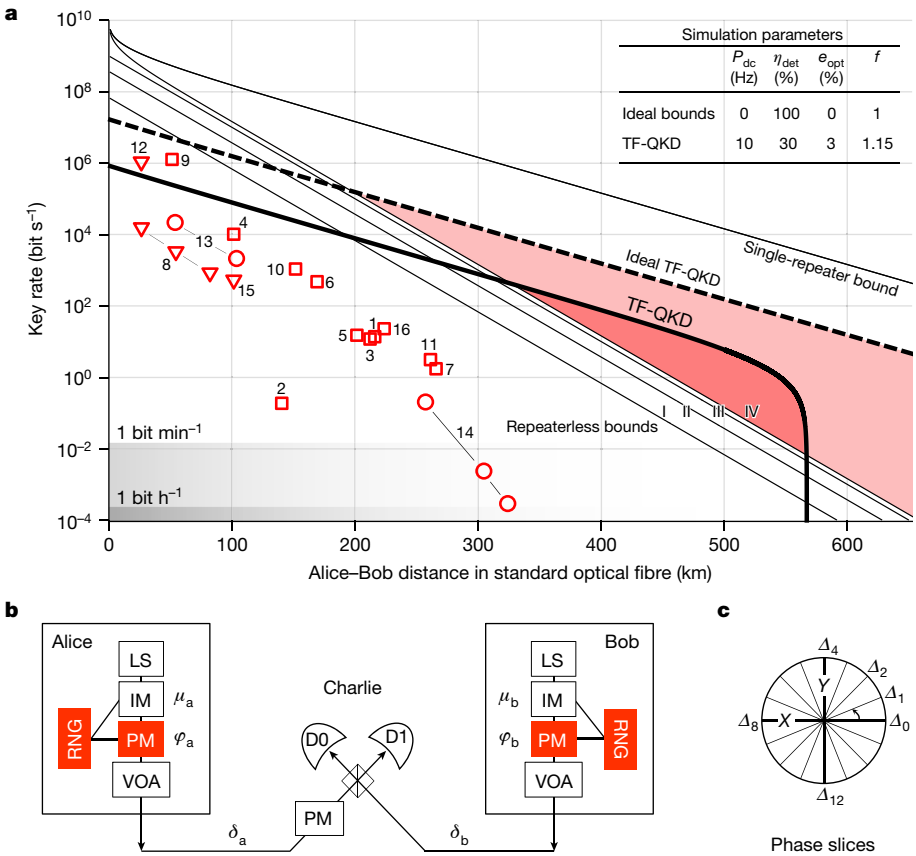

Fig. 1 | Scheme to overcome the rate–distance limit of QKD. **a**, Theoretical bounds (lines) and experimental results (symbols) for fibre-based quantum schemes (details in Supplementary Information). To make a homogeneous comparison, all of the distances have been normalized to the length L of a standard optical fibre with an attenuation coefficient of $\alpha = 0.2\,\mathrm{dB\,km^{-1}}$. The theoretical bounds are: I, decoy-state MDI-QKD; II, decoy-state QKD; III, single-photon QKD; IV, SKC[9]. The single-repeater bound[16] is also shown. The experimental results for QKD, continuous-variable QKD and MDI-QKD are shown as squares, triangles and circles, respectively, and are numbered in chronological order. TF-QKD is the scheme described in this work. The solid (dashed) line respresents the realistic (ideal) TF-QKD key rate given in equation (3) and the darker-pink (lighter-pink) shaded area is the region in which it overcomes the SKC. Inset, parameters used for numerical simulations: P_{dc}, dark-count probability; η_{det}, total detection efficiency; e_{opt}, optical error rate of the channel; f, error-correction coefficient. **b**, Set-up to implement TF-QKD. The light sources (LSs) at Alice's and Bob's stations generate pulses with intensities $\mu_{a,b}$ that are varied randomly by intensity modulators (IMs) to implement the decoy-state technique[20–22]. Phase modulators (PMs) are combined with random number generators (RNGs) to encode each light pulse with phases $\varphi_{a,b}$, which include bit and basis information as well as the random phases $\rho_{a,b}$ (see text). The variable optical attenuators (VOAs) set the average output intensity of the pulses to bright (classical regime) or dim (quantum regime). The pulses travel along independent channels, acquiring phase noise $\delta_{a,b}$, to then interfere on Charlie's beam splitter and be detected by the single-photon detectors D0 and D1. Charlie uses the bright pulses in the classical regime and the phase modulator in his station to phase-align the dim pulses that are emitted in the quantum regime, which provide the bits of the key. **c**, Discretization of phase space to identify the twin fields during the public discussion.

an intrinsic quantum-bit error rate (QBER) E_M due to the twins being close but not exactly identical. On average, this QBER will be

$$E_M = \frac{M}{2\pi}\int_0^{2\pi/M} \sin^2\left(\frac{t}{2}\right)\mathrm{d}t = \frac{1}{2} - \frac{\sin(2\pi/M)}{4\pi/M} \qquad (1)$$

which tends to zero for $M \to \infty$. However, the probability of matching two phase slices scales with $1/M$. As a consequence, there is an optimal M that guarantees the best performance. We ran a realistic simulation to maximize the darker-pink-shaded area in Fig. 1a and obtained an optimal value of $M_{opt} = 16$, which corresponds to $E_{M_{opt}} = 1.275\%$.

In Fig. 2 we relate our scheme to conventional QKD. We first represent the typical interferometer for a phase-encoded QKD set-up (Fig. 2a). The light source generates a coherent state $|\mathrm{e}^{i\rho}\sqrt{\mu}\rangle$, with μ the intensity and ρ the electromagnetic phase that carries the 'global phase information'. The phase ρ is uniformly random and the actual state averaged over repeated runs is

$$\int_0^{2\pi} |\mathrm{e}^{i\rho}\sqrt{\mu}\rangle\langle \mathrm{e}^{i\rho}\sqrt{\mu}|\,\frac{\mathrm{d}\rho}{2\pi} = \sum_{n=0}^{\infty} p_{n|\mu}\,|n\rangle\langle n|$$

where $p_{n|\mu} = \mathrm{e}^{-\mu}\mu^n/n!$ is the (Poisson) probability of emitting n photons when a state with intensity μ is prepared. When the tagging argument[25] is applied to the efficient BB84 protocol[26] endowed with decoy states, the key rate of QKD in the asymptotic scenario is[22]

$$R_{\mathrm{QKD}}(\mu, L) = \underline{Q}_1|_{\mu,L}[1 - h(\bar{e}_1|_{\mu,L})] - fQ_{\mu,L}h(E_{\mu,L}) \qquad (2)$$

In this equation we have explicitly written, for later convenience, the dependence on the total intensity μ and on the distance L between Alice and Bob. $\underline{Q}_1 = p_{1|\mu}\underline{y}_1$ is the lower bound for the single-photon gain; $\underline{y}_1$ and $\bar{e}_1$ are the lower bound for the single-photon yield and the upper bound for the single-photon phase-error rate, respectively, estimated using the decoy-state technique; Q and E are the gain and the QBER measured in the QKD session; f accounts for the efficiency of error correction; and h is the binary entropy.

As an intermediate step towards our scheme, the QKD interferometer (Fig. 2a) is unfolded (Fig. 2b). In this case, the two pulses travel on separate channels and are encoded separately with the same phase ρ. These are the twin fields that will interfere on Charlie's beam splitter. The emitted state is unchanged from the previous scheme, as is the classical information disclosed, so the two schemes are equivalent from a security perspective.

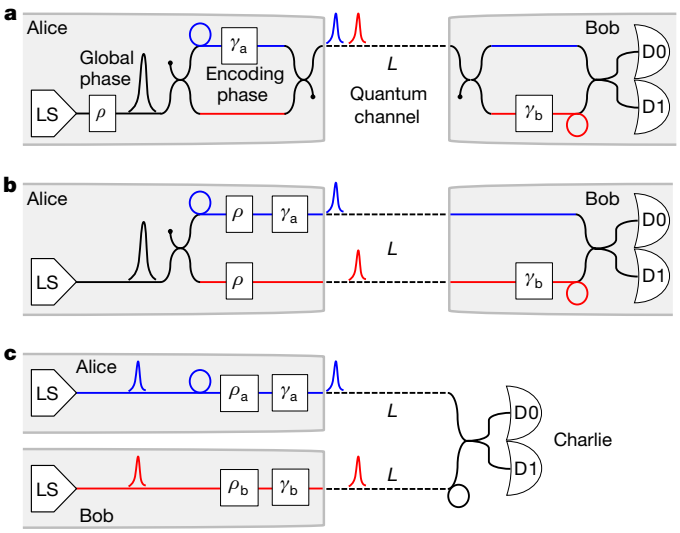

Fig. 2 | Schematics of the quantum distribution of encryption keys. The grey-shaded areas are inaccessible to the eavesdropper. **a**, Typical phase-based QKD set-up. A light source (LS) emits optical pulses with random global phase ρ. The primary pulse is split in two sub-pulses at the input of an asymmetric Mach–Zehnder interferometer. The pulse on the longer path (blue) acquires a phase γ_a with respect to the other pulse (red). The pulses are sent on a quantum channel of length L towards the receiving user (Bob), who owns a matched asymmetric Mach–Zehnder interferometer. After imparting a phase γ_b to the red pulse, Bob makes the two pulses interfere and measures them with the detectors D0 and D1. **b**, Unfolded QKD set-up. The common path of length L in **a** is now split into two separate paths of equal length L. The two secondary pulses travel on separate quantum channels to then interfere and eventually be detected by Bob. **c**, Scheme analysed in this work. Alice and Bob are both transmitters. Each of them is provided with one laser source and one interferometer arm. Alice (Bob) prepares an optical pulse with random phase ρ_a (ρ_b) and encoding phase γ_a (γ_b) and transmits it on the quantum channel. Charlie overlaps the input pulses on a beam splitter and measures them. After Charlie announces which detector clicked, the users announce the basis values in $\gamma_{a,b}$ and the phase slices that contain $\rho_{a,b}$.

In Fig. 2c we present the TF-QKD scheme. The detectors have been outsourced to Charlie and the users' stations have been separated, so that Bob's station is now located at distance $2L$ from Alice. The users' lasers emit optical pulses that interfere[17] on Charlie's beam splitter. The pulses are encoded with random phases $\rho_{a,b}$, which will then be revealed to a finite precision through the public announcement of the phase slices $\Delta_{k(a,b)}$. This aspect is different from conventional QKD, in which the value of the global phase is never revealed.

The key feature of TF-QKD is the doubling of the distance between Alice and Bob for a given count rate. As can be seen from Fig. 2, the red and blue pulses each travel a distance L in both QKD and TF-QKD, thus producing the same count rate. However, whereas in QKD the pulses co-propagate from Alice to Bob, in TF-QKD they run from Alice and Bob towards Charlie, thus effectively increasing the transmission distance.

In Supplementary Information, we show that if revealing the global phase ρ after Charlie's measurement does not contribute to the eavesdropper's information, the key rate of TF-QKD can be expressed through equation (2), as

$$R^{(\neg\rho)}_{\mathrm{TF-QKD}}(\mu, L) = \frac{d}{M}\left[R_{\mathrm{QKD}}\left(\mu, \frac{L}{2}\right)\right]_{\oplus E_M} \quad (3)$$

However, the public disclosure of ρ, even after Charlie's measurement, can leak information to the eavesdropper (Eve). In Supplementary Information, we consider a specific attack built on this leakage and

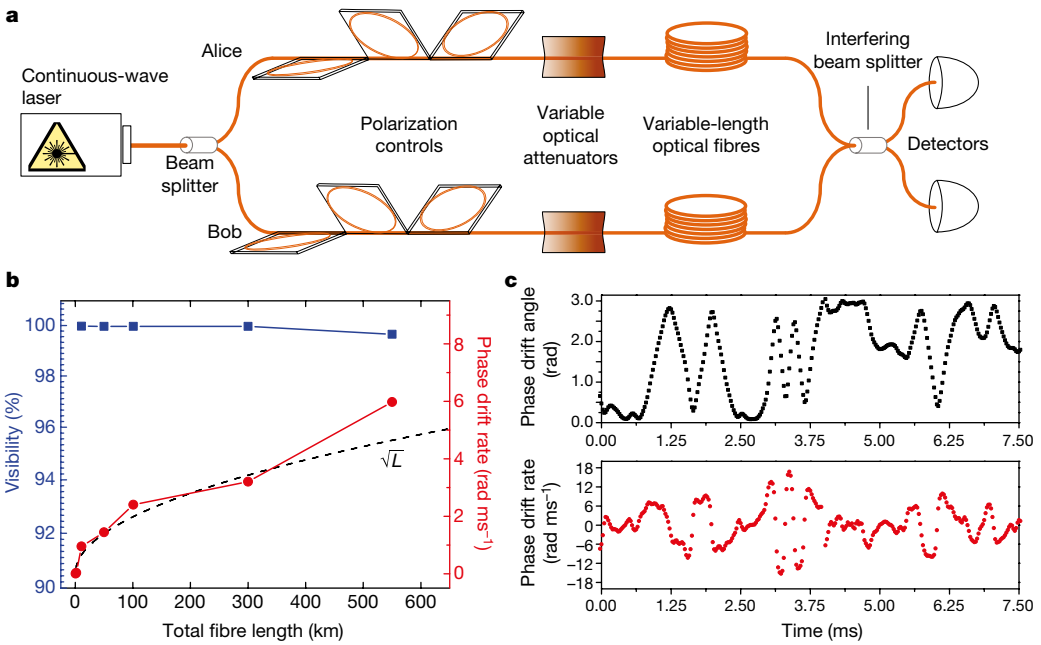

Fig. 3 | Experimental characterization of phase drift and visibility. **a**, Experimental set-up. A light beam emitted by a continuous-wave laser is sent through the two arms of the interferometer. Polarization controls are used to set the correct polarization, which remains stable for a time much longer than the scale of the phase drift. Variable optical attenuators equalize the intensity of the fields that enter the interfering beam splitter. Two equal reels of single-mode optical fibre connect the preparation stage to the beam splitter and the detection stage, where a power meter (Keysight 7748 A) with a sampling rate of 40 kHz and power range between −110 dBm and 10 dBm is used to monitor the phase drift. **b**, Maximum visibility obtained in the experiment (blue) and phase drift rate (red) as function of the total fibre length L. The dashed line represents a qualitative fit that assumes a random-walk model for the phase drift. **c**, Measured phase drift (top, black) and related phase drift rate (bottom, red) in the longest-distance configuration of 550 km, obtained with two fibre spools of length 275 km each. The maximum visibility observed at this specific distance is 99.65%.

show that the resulting key rate is lower, but still above the SKC at long distance. However, we stress that equation (3) does not cover the most general attack by Eve and that the analysis of general attacks is an outstanding challenge.

The notation $\oplus E_M$ in equation (3) prompts the intrinsic QBER of TF-QKD, E_M, owing to its phase-randomization. The total intensity of the optical pulses is $\mu = \mu_a + \mu_b$, with μ_a (μ_b) the intensity of the pulse emitted by Alice (Bob). The coefficient $1/M$ stems from sifting the phase slices, and d is the duty cycle between the classical and the quantum modalities, described below. Equation (3) makes it apparent that a distance $L/2$ in QKD corresponds to a distance L in TF-QKD.

The main technical challenge in implementing TF-QKD is controlling the phase evolution of the twin fields, which travel hundreds of kilometres before interfering on Charlie's beam splitter. The differential phase fluctuation between the two optical paths that link the users to Charlie can be written as

$$\delta_{ba} = \frac{2\pi}{s}(\Delta\nu L + \nu\Delta L) \quad (4)$$

where s is the speed of light in the fibre. The first term arises from the frequency difference $\Delta\nu$ between the users' lasers and can easily be compensated using the phase-locking techniques[27] that are routinely used in optical communications[28]. With a feasible value[29] of $\Delta\nu < 1$ Hz, the phase uncertainty would be about 0.01 rad over 300 km of fibre, negligibly contributing to the QBER. The second term represents a more serious impairment. During propagation in the very long fibres, the twin fields travel different paths, so their relative phase will vary. The phase drift of a fibre-based Mach–Zehnder interferometer with 36.5-km-long arms was previously[30] characterized to be around 0.3–1 rad ms^{-1}.

To determine the phase drift over much longer fibres, we used the experimental set-up shown in Fig. 3a. The presence of a single laser assures that $\Delta\nu = 0$ in equation (4), thus letting us measure only the noise due to the fluctuations in the channel. The measured phase drift rate follows a Gaussian distribution with zero mean and a standard deviation equal to 2.4 rad ms^{-1} at a total distance of 100 km and 6.0 rad ms^{-1} at the longest distance of 550 km (Fig. 3b, c). Compensating the phase drift would require bright pulses and active feedback, realized by Charlie acting on his phase modulator (details in Supplementary Information). In Fig. 3b we also show the visibility measured as a function of the fibre length. The visibility remains above 99.65% for all distances, thus causing a negligible 0.175% contribution to the QBER due to a loss of coherence along the fibre.

Our findings suggest that the point-to-point SKC of a quantum channel can be overcome without using quantum repeaters, with a scheme that borrows components and techniques from ordinary QKD. This is not at variance with existing results[8,9], because TF-QKD is not a point-to-point scheme. As in MDI-QKD, the security of the scheme described here does not depend on the measurement devices. At the same time, the single-photon nature of our scheme results in count and error rates similar to those for standard QKD. Further work is necessary to prove the unconditional security of the scheme. We expect that this and the counter-intuitive features of TF-QKD will stimulate further research to extend the limits of QKD.

Data availability

All data generated and analysed during this study is available from the corresponding author on reasonable request.

Received: 27 April 2017; Accepted: 5 February 2018;
Published online 2 May 2018.

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
2. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
3. Comandar, L. C. et al. Room temperature single-photon detectors for high bit rate quantum key distribution. *Appl. Phys. Lett.* **104**, 021101 (2014).
4. Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
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. Sangouard, N., Simon, C., de Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33–80 (2011).
8. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
9. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
10. Jiang, L. et al. Quantum repeater with encoding. *Phys. Rev. A* **79**, 032325 (2009).
11. 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).
12. Azuma, K., Tamaki, K. & Lo, H.-K. All-photonic quantum repeaters. *Nat. Commun.* **6**, 6787 (2015).
13. Azuma, K., Tamaki, K. & Munro, W. J. All-photonic intercity quantum key distribution. *Nat. Commun.* **6**, 10171 (2015).
14. Qiu, J. Quantum communications leap out of the lab. *Nature* **508**, 441–442 (2014).
15. Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140–1144 (2017).
16. Pirandola, S. Capacities of repeater-assisted quantum communications. Preprint at https://arxiv.org/abs/1601.00966 (2016).
17. Pfleegor, R. L. & Mandel, L. Interference of independent photon beams. *Phys. Rev.* **159**, 1084–1088 (1967).
18. Tamaki, K., Lo, H.-K., Fung, C.-H. F. & Qi, B. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Phys. Rev. A* **85**, 042307 (2012).
19. Bovino, F. A. & Messina, A. Increasing operational command and control security by the implementation of device independent quantum key distribution. *Proc. SPIE* **9996**, 999606 (2016).
20. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
21. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
22. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
23. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
24. Ma, X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 062319 (2012).
25. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **4**, 325–360 (2004).
26. Lo, H.-K., Chau, H. F. & Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **18**, 133–165 (2005).
27. Santarelli, G., Clairon, A., Lea, S. & Tino, G. Heterodyne optical phase-locking of extended-cavity semiconductor lasers at 9 GHz. *Opt. Commun.* **104**, 339–344 (1994).
28. Appel, J., MacRae, A. & Lvovsky, A. I. A versatile digital GHz phase lock for external cavity diode lasers. *Meas. Sci. Technol.* **20**, 055302 (2009).
29. Lipka, M., Parniak, M. & Wasilewski, W. Optical frequency locked loop for long-term stabilization of broad-line DFB lasers frequency difference. *Appl. Phys. B* **123**, 238–245 (2017).
30. Minář, J., de Riedmatten, H., Simon, C., Zbinden, H. & Gisin, N. Phase-noise measurements in long-fiber interferometers for quantum-repeater applications. *Phys. Rev. A* **77**, 052325 (2008).

Acknowledgements We acknowledge K. Tamaki for constructive criticism on the security argument. We acknowledge discussions with X. Ma, N. Lütkenhaus, B. Fröhlich, R. M. Stevenson, D. G. Marangon and A. J. Bennett.

Reviewer Information *Nature* thanks X. Ma and the other anonymous reviewer(s) for their contribution to the peer review of this work.

Author contributions M.L. and Z.L.Y. developed the TF-QKD scheme. Z.L.Y. and J.F.D. set up and performed the experiments, and all authors analysed the results. A.J.S. guided the work. M.L. wrote the manuscript with contributions from all authors.

Competing interests The authors declare no competing interests.

Additional information
Supplementary information is available for this paper at https://doi.org/10.1038/s41586-018-0066-6.

Correspondence and requests for materials should be addressed to M.L.