LETTER

doi:10.1038/nature12493

A quantum access network

Bernd Fröhlich[1,2], James F. Dynes[1,2], Marco Lucamarini[1,2], Andrew W. Sharpe[1], Zhiliang Yuan[1,2] & Andrew J. Shields[1,2]

The theoretically proven security of quantum key distribution (QKD) could revolutionize the way in which information exchange is protected in the future[1,2]. Several field tests of QKD have proven it to be a reliable technology for cryptographic key exchange and have demonstrated nodal networks of point-to-point links[3–5]. However, until now no convincing answer has been given to the question of how to extend the scope of QKD beyond niche applications in dedicated high security networks. Here we introduce and experimentally demonstrate the concept of a 'quantum access network': based on simple and cost-effective telecommunication technologies, the scheme can greatly expand the number of users in quantum networks and therefore vastly broaden their appeal. We show that a high-speed single-photon detector positioned at a network node can be shared between up to 64 users for exchanging secret keys with the node, thereby significantly reducing the hardware requirements for each user added to the network. This point-to-multipoint architecture removes one of the main obstacles restricting the widespread application of QKD. It presents a viable method for realizing multi-user QKD networks with efficient use of resources, and brings QKD closer to becoming a widespread technology.

In a nodal QKD network, multiple trusted repeaters are connected by means of point-to-point links between a quantum transmitter ('Alice') and a quantum receiver ('Bob'). These point-to-point links can be realized with long-distance optical fibres, and in the future might even use ground-to-satellite communication[6–8]. Although point-to-point connections are suitable to form a backbone quantum core network to bridge long distances, they are less suitable to provide the last-mile service needed to give a multitude of users access to this QKD infrastructure. Reconfigurable optical networks based on optical switches or wavelength-division multiplexing have been suggested to achieve more flexible network structures[3,9–12]; however, they also require the installation of a full QKD system for each user, which is prohibitively expensive for many applications.

Giving a multitude of users access to the nodal QKD network requires point-to-multipoint connections. In modern fibre-optic networks point-to-multipoint connections are often realized passively by using components such as optical power splitters[13]. Single-photon QKD with the sender positioned at the network node and the receiver at the user premises[14] lends itself naturally to a passive multi-user network (see Fig. 1a). However, this downstream implementation has two major shortcomings. First, every user in the network requires a single-photon detector; these are often expensive and difficult to operate. Second, it is not possible to deterministically address a user. All detectors therefore have to operate at the same speed as the transmitter so as not to miss photons, which means that most of the detector bandwidth is unused.

Here we show that both problems associated with a downstream implementation can be overcome with a conceptual advancement: the most valuable resource should be shared by all users and should operate at full capacity. We propose and demonstrate an upstream quantum access network, in which the transmitters are placed at the end user

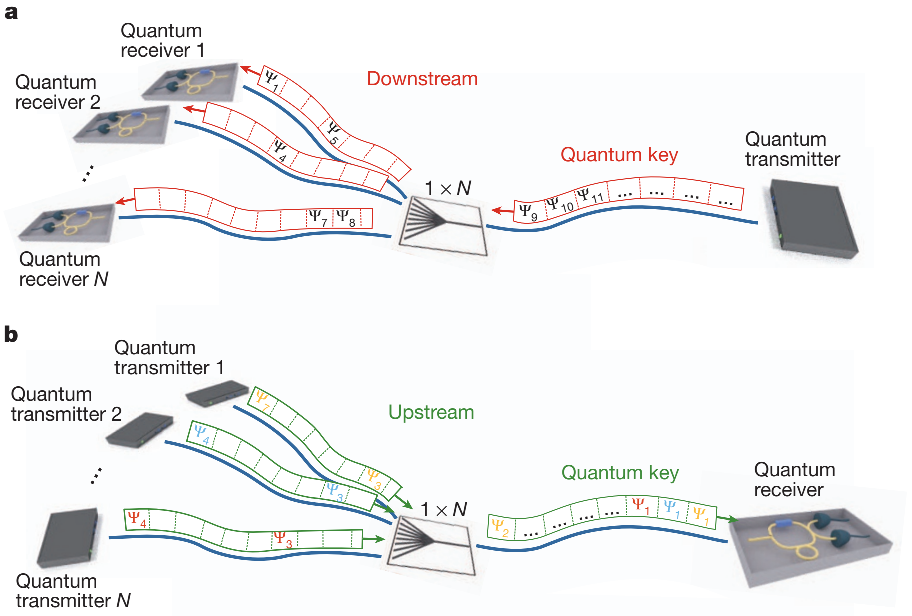

Figure 1 | Downstream and upstream quantum access network. a, In a downstream configuration the quantum transmitter is positioned at the network node. The transmitted quantum key is randomly directed to one of the quantum receivers by a passive optical splitter. Each user needs a single-photon detector, and the key is not distributed deterministically. **b**, The upstream configuration requires only a single detector at the network node. The quantum transmitters share this detector by ensuring that only photons from one transmitter at a time reach the receiver.

[1]Toshiba Research Europe Ltd, 208 Cambridge Science Park, Cambridge CB4 0GZ, UK. [2]Corporate Research and Development Center, Toshiba Corporation, 1 Komukai-Toshiba-Cho, Saiwai-ku, Kawasaki 212-8582, Japan.

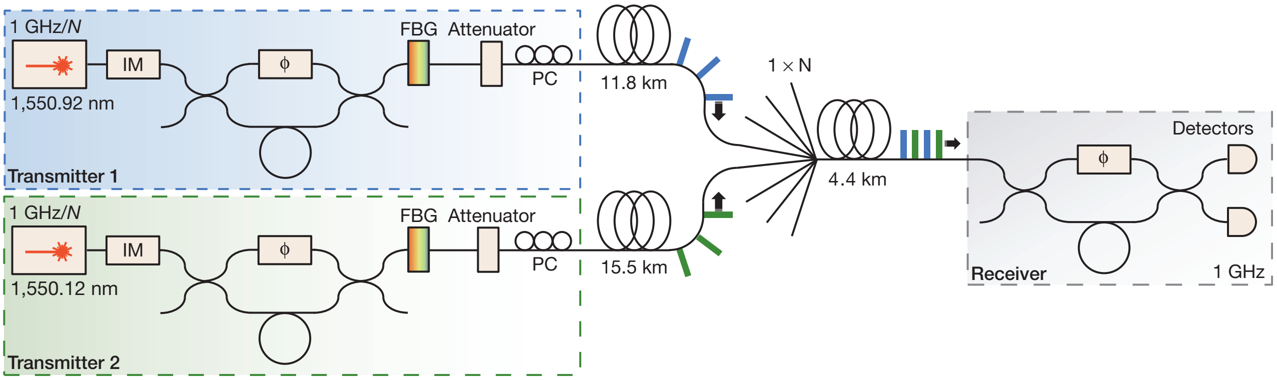

Figure 2 | Experimental set-up. Two quantum transmitters are connected to a single quantum receiver by means of a passive optical splitter and fibre spools. Each transmitter encodes bit and basis information on short laser pulses with an asymmetric Mach–Zehnder interferometer. The intensity of the pulses is modulated with an intensity modulator (IM) and attenuated to the single-photon level. A polarization controller (PC) pre-compensates the polarization and a fibre Bragg grating (FBG) compensates for pulse broadening in the fibre. The receiver decodes the phase information with a matching interferometer. The two outputs of this interferometer are connected to single-photon detectors operating at 1 GHz.

location and a common receiver is placed at the network node as shown in Fig. 1b. A careful study of the cross-talk between senders arising from the shared receiver topology shows that operation with up to 64 users is feasible, which we demonstrate by performing multi-user QKD over a 1 × 64 passive optical splitter. The results presented here highlight a practical and viable approach to extending the scope of QKD applications to many more users. Our approach would also be advantageous in a fully quantum network in which a quantum relay or repeater is located at the common node.

One of the main challenges for realizing an upstream quantum access network is to develop independently operating quantum transmitters that exchange secure keys efficiently with the receiver in parallel. For example, active stabilization in QKD systems is typically implemented at the receiver side[15]. In our scheme, however, the receiver is the reference for multiple transmitters and therefore each user has to pre-compensate system fluctuations individually. Figure 2 shows a diagram of our experimental set-up (see also Methods). We developed two flexible quantum transmitters that can operate at varying repetition rates and contain all the stabilization components necessary for continuous operation. They also include additional polarization control elements to achieve higher key rates (see Methods). At the centre of the quantum network is a passive optical splitter, which connects multiple transmitters to the receiver. The fibre distance between transmitters and receiver was chosen to be close to the maximum distance defined for gigabit passive optical networks in the International Telecommunication Union (ITU) standardization document[13]. We use a phase-encoding BB84 QKD protocol with decoy states[16–19] implemented with asymmetric Mach–Zehnder interferometers and intensity modulators. The quantum receiver decodes the phase information with a matching interferometer and uses two high-speed detectors based on avalanche photodiodes to detect the single photons with a rate of 1 GHz (refs 20, 21). We implement phase encoding because it is robust against fluctuations on the transmission channel and permits a simple stabilization mechanism.

To share a single-photon detector between multiple transmitters we adopt a novel and efficient scheme that allows the continuous and stable exchange of keys necessary to reduce the detrimental effect of finite-size samples[22–26]. Large fluctuations during a key session will reduce the number of sifted bits that are transmitted and therefore reduce the number of secure bits that can be distilled after privacy amplification. In our scheme all quantum transmitters operate continuously in parallel, permitting uninterrupted key sessions. We operate each transmitter at a fraction of the speed of the receiver, for example 1 GHz/8 = 125 MHz in an eight-user network. The transmitters are synchronized such that their pulses fall into subsequent detection time slots and can be clearly assigned to each user, as shown in Fig. 1b. This scheme has two main advantages: first, polarization, phase and synchronization tracking is done continuously by each QKD transmitter against the common quantum receiver, thus allowing stable operation of the quantum network; and, second, the transmitter can be realized with simpler electronics and optics because of the lower operational speed.

In a first experiment we demonstrate stable operation, over 12 h, of a 1 × 8 quantum access network populated by two users. We operate both transmitters at 125 MHz and use a passive 1 × 8 splitter to combine their signals; the total transmission losses including the splitter are 13.6 and 14 dB for transmitters 1 and 2, respectively. Counts in each detection gate are either allocated to one of the transmitters or identified as an empty gate, depending on their timing information. In a 20-min key session we record almost 300 Mbits of counts per transmitter. Figure 3a shows the quantum bit error rate (QBER) and secure bit rate for each key session. Although assigned to a specific transmitter, both the transmitter and the receiver subsystem contribute to the QBER. As a result of the low QBERs (transmitter 1, 1.28%; transmitter 2, 1.53%) we can exchange secure bits very efficiently, with average secure bit rates of 47.5 and 43.1 kbits s^{-1} for transmitters 1 and 2, respectively. Continuous operation over a month would allow unconditionally secure one-time-pad encryption of more than 10 Gbytes of data for each user, which is enough to protect more than 10^5 emails, for example.

The key rate can be increased further by the use of wavelength-division multiplexing optics instead of passive splitters because of the lower insertion loss of these devices. We demonstrate this in a second experiment by replacing the 1 × 8 splitter with an eight-channel thin-film dense-wavelength-division multiplexing module. The specified loss of the multiplexing module of about 2.5 dB is one-fifth of that for the 1 × 8 splitter and accordingly leads to a proportional increase in the count rate. In this experiment the quantum transmitters do not need to be modified because we designed the emission wavelengths of transmitters 1 and 2 to coincide with channels 33 (1,550.92 nm) and 34 (1,550.12 nm) of the ITU grid, respectively. Figure 3b shows the resulting QBER and secure bit rate for each key session. In addition to the higher transmission rate, the ratio of dark counts to photon counts decreases, leading to a decrease in the QBER (transmitter 1, 1.06%; transmitter 2, 1.17%) and therefore to an even higher increase in the secure bit rate (sixfold), corresponding to almost 100 Gbytes of key material per month (transmitter 1, 303 kbits s^{-1}; transmitter 2, 259 kbits s^{-1}).

We can extrapolate the performance of a network with more users by studying the cross-talk between two transmitters in detail. To determine the cross-talk we measured the average count rate of one transmitter with the other transmitter either on or off (C_{on} and C_{off}, respectively). As shown in the inset of Fig. 4a, the transmitters are operated at 125 MHz, allowing us to vary the gate separation between them. From these data we extract how many spurious detection events the second transmitter (green) causes in the detection gates allocated to the first transmitter

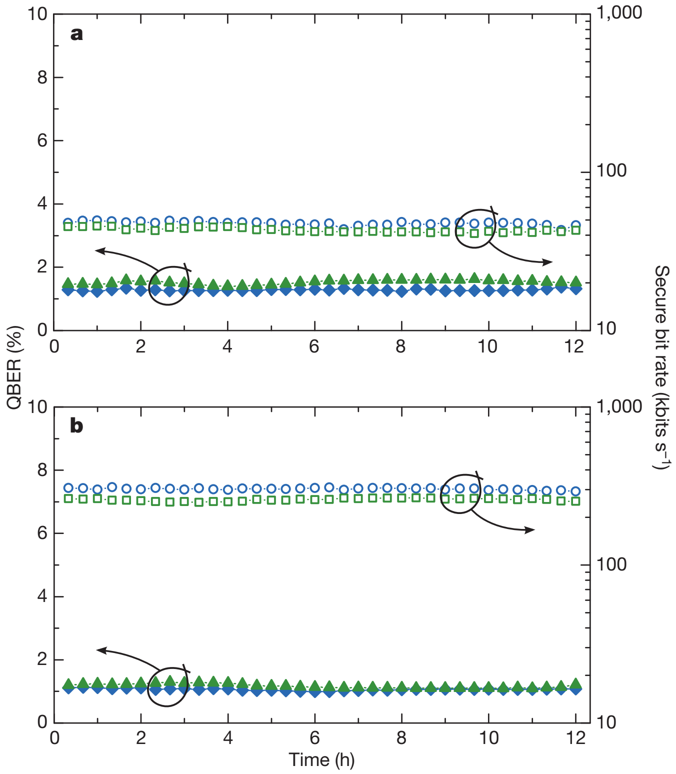

Figure 3 | Stable operation of quantum access network. a, Quantum bit error rate (QBER) (filled blue diamonds, transmitter 1; filled green triangles, transmitter 2) and secure bit rate (open blue circles, transmitter 1; open green squares, transmitter 2) for each 20-min key session in a network supporting eight users with a 1 × 8 passive optical splitter. **b**, QBER and secure bit rate for each 20-min key session in an eight-user network using dense-wavelength-division multiplexing optics.

(blue). Figure 4a displays the relative increase in count rate $(C_{\mathrm{on}} - C_{\mathrm{off}})/C_{\mathrm{off}}$ for various gate separations of transmitters 1 and 2. Two effects contribute to the increase. First, the detection of pulses sent from the second transmitter causes after-pulses in the gate periods of the first transmitter. This leads to an increase in the count rate for each added user, independently of the gate separation by p_{A}/N as indicated by the dashed line, where p_{A} is the after-pulse probability of the detector and N is the number of users that the network supports. Second, smaller gate separation between transmitters 1 and 2 increases the cross-talk, most probably as a result of the late arrival of photons or ringing of the detector electronics.

Using the cross-talk data we simulate how the key rate of a single transmitter changes when more users are added to the network (see also Methods). Figure 4b shows logarithmic colour-scale plots of the secure bit rate per user as a function of fibre distance from the transmitters to the node and number of active users in the network. We simulate the rate for various network capacities N, which are given by the splitting ratio of the passive optical splitter installed in the system. For the simulation we assume that each active transmitter operates with 1 GHz/N and that the fibre distance to the node is the same for all transmitters. The data show clearly that even for a 64-user network, which inherently has a loss of about 20 dB from the 1 × 64 splitter, secure transmission is possible up to the maximum distance for gigabit passive optical networks of 20 km with all users active. In networks supporting fewer users there is a margin to allow longer fibre distances or, correspondingly, higher loss in the system.

To verify this result experimentally we switch to 500-MHz operation of the transmitters and vary the splitting ratio from 1 × 8 to 1 × 64. Operation at 500 MHz with two transmitters allows us to emulate a fully occupied network because photon detections are possible in all detector time slots. Figure 4c displays the estimated key rate per user based on the measured secure bit rates of transmitters 1 and 2, and shows how it compares with the expected value from the simulation. For the key rate estimation we add the key rate of the two transmitters and divide it by the network capacity. The data confirm

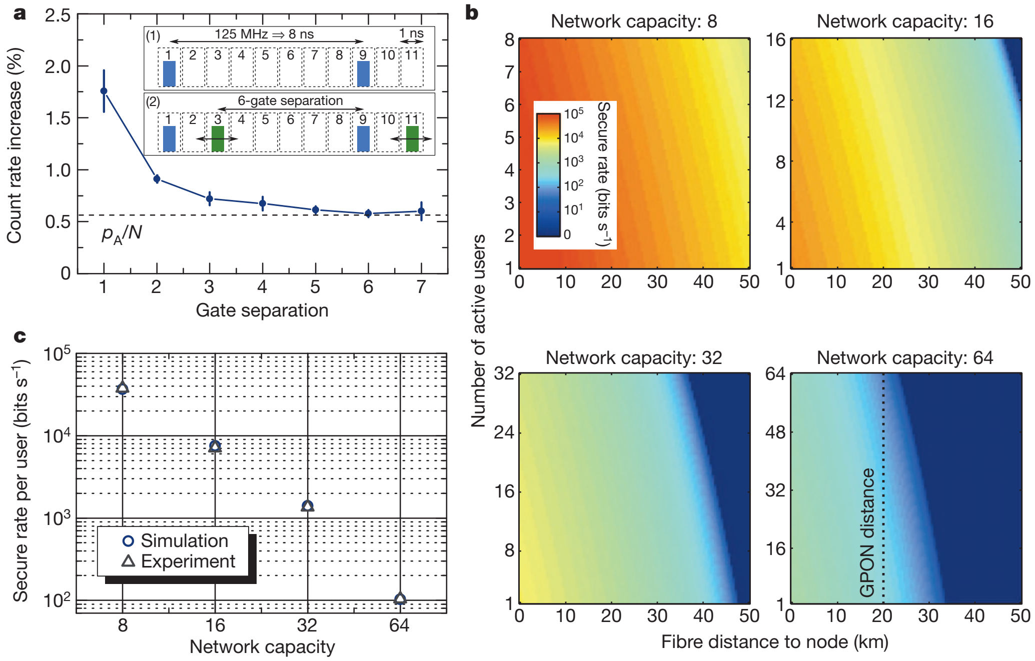

Figure 4 | Quantum access network with varying capacity. a, Relative increase of count rate due to cross-talk between the transmitters as a function of gate separation. The dashed line indicates the limit given by detector after-pulses. Error bars correspond to one standard deviation of three consecutive measurements. Inset: measurement principle (see the text). **b**, Simulation of the secure bit rate per user as a function of fibre distance and number of active users in the network for various network capacities (see the text and Methods). **c**, Secure bit rate per user in a quantum network with varying capacity estimated from a two-user measurement at 500 MHz.

the result obtained from the simulation: it demonstrates that a 64-user network is feasible with our scheme.

We have demonstrated that passive optical networks have the potential to scale up the number of users in a nodal QKD network. We have shown that the decrease in the secure key rate accompanying a time-division multiplexing approach can be greatly mitigated by using a high-speed single-photon detector. The network node in our scheme acts as a receiver and has to be trusted intrinsically; however, techniques such as classical secret sharing[27] or measurement-device-independent QKD[28] might be used to relax this requirement in the future. It might also be possible to combine classical data transport on the same fibre in quantum-secured access networks[29]. Quantum access networks could initially find application in protecting smart community or smart grid networks, for example, allowing authenticated data collection from multiple locations in a critical infrastructure network[30].

METHODS SUMMARY

Experimental set-up. We implement the standard BB84 protocol with decoy states[16–19], with photon fluxes of 0.5, 0.1 and 0.0002 photons per pulse sent with probabilities of 98.83%, 0.78% and 0.39%, respectively. Detection events are sorted into N time bins, where N is the number of users that the network supports. Each transmitter is aligned relative to a master clock from the receiver such that their photons fall into a specific time bin. We determine the secure bit rate for each user individually by estimating single-photon parameters from decoy states. Our security analysis[26] takes finite-size effects into account[23–25] and achieves bit rates close to the asymptotic limit for key sessions of 20 min.

Simulation. We first estimate the probability of obtaining an error count for a single transmitter in an otherwise empty network η_{err} on the basis of measured values for encoding imperfections and detector imperfections (after-pulses and dark counts). The QBER including cross-talk counts is then given by

$$e=\frac{\eta_{\text{err}}+\frac{1}{2}p_{\text{X}}(n-1)\eta}{\eta(1+p_{\text{A}}/N)+p_{\text{D}}+p_{\text{X}}(n-1)\eta}$$

where n is the number of active users populating the network, η is the system detection probability, p_{A} is the after-pulse probability and p_{D} is the dark count probability. The average count rate increase per added user p_{X} is extracted from the data shown in Fig. 4a under the assumption of equal losses for all users. The secure bit rate is determined from a refined analysis calculating the count rates and QBER for all three signal levels of the decoy-state protocol. For the 32-user and 64-user networks we increased the key session length from 20 min to 2 h and 12 h, respectively, to compensate for the decreasing sample size due to the slower operation of the transmitter. Our measurements shown in Fig. 3 indicate that longer key sessions are feasible. For the comparison of simulation and experiment shown in Fig. 4c we adopt the simulation to account for the unequal fibre distances of the two transmitters, as well as the higher operational speed leading to different sample sizes compared with Fig. 4b.

Full Methods and any associated references are available in the online version of the paper.

Received 1 May; accepted 18 July 2013.

1. Lütkenhaus, N. & Shields, A. J. Focus on quantum cryptography: theory and practice. *New J. Phys.* **11,** 045005 (2009).
2. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
3. Elliott, C. *et al.* in *Quantum Information and Computation III* (*Proc. SPIE*, vol. 5815) (eds Donkor, E. J., Pirich, A. R. & Brandt, H. E.) 138–149 (SPIE, 2005).
4. Peev, M. *et al.* The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11,** 075001 (2009).
5. Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19,** 10387–10409 (2011).
6. Ursin, R. *et al.* Entanglement-based quantum communication over 144 km. *Nature Phys.* **3,** 481–486 (2007).
7. Nauerth, S. *et al.* Air-to-ground quantum communication. *Nature Photon.* **7,** 382–386 (2013).
8. Wang, J.-Y. *et al.* Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nature Photon.* **7,** 387–393 (2013).
9. Toliver, P. *et al.* Experimental investigation of quantum key distribution through transparent optical switch elements. *IEEE Photon. Technol. Lett.* **15,** 1669–1671 (2003).
10. Chapuran, T. E. *et al.* Optical networking for quantum key distribution and quantum communications. *New J. Phys.* **11,** 105001 (2009).
11. Chen, T.-Y. *et al.* Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **18,** 27217–27225 (2010).
12. Wang, S. *et al.* Field test of the wavelength-saving quantum key distribution network. *Opt. Lett.* **35,** 2454–2456 (2010).
13. International Telecommunication Union. G.984.1: Gigabit-capable passive optical networks (GPON): general characteristics. http://www.itu.int/rec/T-REC-G.984.1-200803-I/en (2008).
14. Townsend, P. D. Quantum cryptography on multiuser optical fibre networks. *Nature* **385,** 47–49 (1997).
15. Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W. & Shields, A. J. Continuous operation of high bit rate quantum key distribution. *Appl. Phys. Lett.* **96,** 161102 (2010).
16. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
17. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
18. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
19. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72,** 012326 (2005).
20. Yuan, Z. L., Kardynal, B. E., Sharpe, A. W. & Shields, A. J. High speed single photon detection in the near infrared. *Appl. Phys. Lett.* **91,** 041114 (2007).
21. Yuan, Z. L. *et al.* Gigahertz quantum key distribution with InGaAs avalanche photodiodes. *Appl. Phys. Lett.* **92,** 201104 (2008).
22. Hayashi, M. Upper bounds of eavesdropper's performances in finite-length code with the decoy method. *Phys. Rev. A* **76,** 012329 (2007).
23. Scarani, V. & Renner, R. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.* **100,** 200501 (2008).
24. Scarani, V. & Renner, R. Security bounds for quantum cryptography with finite resources. Preprint at http://arxiv.org/abs/0806.0120 (2008).
25. Cai, R. Y. Q. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *New J. Phys.* **11,** 045024 (2009).
26. Lucamarini, M., Dynes, J. F., Yuan, Z. L. & Shields, A. J. in *Electro-Optical Remote Sensing, Photonic Technologies, and Applications VI* (*Proc. SPIE*, vol. 8542) (eds Kamerman, G. W. *et al.*) 85421K (SPIE, 2012).
27. Barnett, S. & Phoenix, S. J. D. in *GCC Conference and Exhibition (GCC), 2011 IEEE* 143–145, http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5746659 (IEEE, 2011).
28. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
29. Patel, K. A. *et al.* Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Phys. Rev. X* **2,** 041010 (2012).
30. Hughes, R. J. *et al.* Network-centric quantum communications with application to critical infrastructure protection. Preprint at http://arxiv.org/abs/1305.0305 (2013).

Acknowledgements This research is partly supported by Research and Development of Secure Photonic Network Technologies, the Commissioned Research of the National Institute of Information and Communications Technology (NICT), Japan.

Author Contributions B.F. performed the measurements and simulations. B.F., J.F.D. and A.W.S. developed the system. M.L. performed calculations for the security analysis. Z.Y. and A.J.S. conceived the experiment and guided the work. B.F. wrote the manuscript with contributions from the other authors. All authors discussed experiments, results and the interpretation of results.

Author Information Reprints and permissions information is available at www.nature.com/reprints. The authors declare no competing financial interests. Readers are welcome to comment on the online version of the paper. Correspondence and requests for materials should be addressed to A.J.S. (andrew.shields@crl.toshiba.co.uk), Z.Y. (zhiliang.yuan@crl.toshiba.co.uk) or B.F. (bernd.frohlich@crl.toshiba.co.uk).

METHODS

Experimental set-up. Each quantum transmitter consists of a source of short laser pulses, an intensity modulator, an asymmetric Mach–Zehnder interferometer including a phase modulator in one arm, a fibre Bragg grating, an attenuator and a polarization controller (see Fig. 2). The laser source is a distributed feedback laser generating laser pulses shorter than 50 ps with a selectable repetition rate of up to 1 GHz. The wavelengths of transmitters 1 and 2 are tuned to coincide with channels 33 and 34, respectively, of the grid defined by the International Telecommunication Union (ITU). The intensity modulator in combination with the attenuator at the output sets the power of each pulse to one of three power levels necessary for the decoy protocol[16–19]: 0.5 photons per pulse for signal pulses, 0.1 photons per pulse for decoy pulses and 0.0002 photons per pulse for vacuum pulses. We send signal, decoy and vacuum pulses with probabilities of 98.83%, 0.78% and 0.39%, respectively.

The asymmetric Mach–Zehnder interferometer is made of off-the-shelf fibre optic components, and the length difference between the long and short arms is matched to the receiver interferometer with a tunable optical delay. The components do not require temperature stabilization or vibration isolation. Drifts of the relative phase between the long and short arms of the interferometer with respect to the receiver interferometer are compensated for by applying a bias voltage across the phase modulator. Each transmitter compensates for the phase difference individually and independently of other users in the network. No compensation is necessary in the receiver interferometer, which acts as a phase reference. The output beam splitter of the transmitter interferometer and the input beam splitter of the receiver interferometer are polarizing to direct the photons into the correct arm of the receiver interferometer, thus avoiding a 3 dB penalty when using polarization-insensitive interferometers. We therefore additionally pre-compensate the polarization of the transmitted pulses with a polarization controller to achieve maximum count rate at the receiver. The fibre Bragg grating compensates for pulse broadening across the fibre link to avoid a further 1.5 dB decrease in the count rate.

The quantum receiver consists of the reference Mach–Zehnder interferometer that decodes the phase information of the pulses sent from the transmitters and detects the photons with InGaAs single-photon avalanche photodiodes with a rate of 1 GHz using a self-differencing technique[20,21]. The avalanche photodiodes are operated at a temperature of $-30\,^{\circ}\mathrm{C}$. A typical detection efficiency is 15%, with 8×10^{-6} dark counts per gate and an after-pulse probability of 4.5%. Detection events are sorted into N time bins, where N is the number of users that the network supports. Each transmitter is aligned relative to a master clock from Bob such that their photons coincide with a specific time bin and can be clearly assigned to a user. A variable time delay implemented in each transmitter permits control of the alignment continuously with a feedback signal generated from the detector count rate.

Secure key rate. We implement the standard BB84 protocol with decoy states in our set-up. The quantum transmitter prepares one of four phase states (0, $\pi/2$, π and $3\pi/2$) with equal probabilities, and the receiver chooses either phase 0 or $\pi/2$. All events with non-matching basis are discarded in the sifting process. On the basis of the individual error rates of signal, decoy and vacuum states we estimate single-photon parameters for each user individually. Our security analysis[26] takes finite-size effects into account[23–25] and achieves bit rates close to the asymptotic limit for key sessions of 20 min. The secure key rate is bounded from below by

$$R=\{Q_1[1-H(e_1)]-Q f_{\mathrm{EC}}(e)H(e)+Q_0-\Delta\}/t$$

Here Q_1 is the estimated number of sifted bits from single-photon states, $H(e_1)$ is the binary entropy function of the estimated error rate of those bits, Q is the total number of sifted bits, f_{EC} is the error correction efficiency, which is set to 1.1, e is the QBER of sifted bits, Q_0 is the estimated number of sifted bits originating from vacuum pulses and t is the key session time. Finite-size effects are included by subtracting Δ, which is proportional to $\sqrt{Q}$ and to $\log_2(\varepsilon^{-1})$, where ε, equal to 10^{-10} in our system, is related to the overall security of the system[26].

Parameters of the protocol such as decoy level and decoy probability have to be chosen carefully to achieve optimal secure key rates. For example, the estimation of Q_1 depends directly on the chosen decoy photon flux and probability. We simulate the achievable secure key rates in advance to select suitable parameters for the experiment. For convenience we use one set of parameters for all measurements presented here, which we found to lead to stable results in all configurations considered.

Simulation. We simulate the secure key rate per user in a network that is populated by more than two users based on measured experimental parameters. For the simulation we assume that each active transmitter operates with 1 GHz/N and that the fibre distance to the node is the same for all transmitters. The starting point is calculating the probability to obtain an error count for a single transmitter in an otherwise empty network, using $\eta_{\mathrm{err}}=\eta(e_{\mathrm{opt}}+p_{\mathrm{A}}/2N)+p_{\mathrm{D}}/2$. Here e_{opt} is the optical error due to encoding imperfections, p_{A} is the after-pulse probability and p_{D} is the dark count probability of the detector, and the detection probability η is given by $\eta=\mu\times10^{-0.2L/10}\,l_{\mathrm{spl}}\eta_{\mathrm{Bob}}$, with μ being the photon flux, L the total fibre length in kilometres, l_{spl} the splitter loss and η_{Bob} the system detection efficiency of the receiver. We use the following parameters in the simulation: $e_{\mathrm{opt}}=0.5\%$, $p_{\mathrm{A}}=4.5\%$, $p_{\mathrm{D}}=2\times8\times10^{-6}$ and $\eta_{\mathrm{Bob}}=9.04\%$.

Adding more users to the network will increase the error rate as a result of cross-talk between the users. The QBER including cross-talk counts is then given by

$$e=\frac{\eta_{\mathrm{err}}+\frac{1}{2}p_{\mathrm{X}}(n-1)\eta}{\eta(1+p_{\mathrm{A}}/N)+p_{\mathrm{D}}+p_{\mathrm{X}}(n-1)\eta}$$

with n the number of active users in the network. The average increase in count rate per added user $p_{\mathrm{X}}=1.9\%/(N-1)+p_{\mathrm{A}}/N$ is extracted from the data shown in Fig. 4a by taking both the base increase by p_{A}/N and the enhanced cross-talk at short gate separation into account. For the splitter loss l_{spl} we use our measured values of 9.7, 13, 16.1 and 19.5 dB for 1 × 8, 1 × 16, 1 × 32 and 1 × 64 splitting ratios, respectively.

The secure key rate is determined from a refined analysis calculating the count rates and QBER for all three signal levels of the decoy-state protocol. We use the same routine as for the experimental data to determine the secure key rate from these values. For the 32-user and 64-user networks we increased the key session length from 20 min to 2 h and 12 h, respectively, to compensate for the decreasing sample size due to the slower operation of the transmitter. Our measurements shown in Fig. 3 indicate that longer key sessions are feasible. For the comparison of simulation and experiment shown in Fig. 4c we adopt the simulation to account for the unequal fibre distances of the two transmitters, as well as the higher operational speed leading to different sample sizes compared with Fig. 4b.