LETTER

https://doi.org/10.1038/s41586-018-0766-y

An entanglement-based wavelength-multiplexed quantum communication network

Sören Wengerowsky[1,2]*, Siddarth Koduru Joshi[1,2,4], Fabian Steinlechner[1,2,5,6], Hannes Hübel[3] & Rupert Ursin[1,2]*

Quantum key distribution[1] has reached the level of maturity required for deployment in real-world scenarios[2–6]. It has previously been shown to operate alongside classical communication in the same telecommunication fibre[7–9] and over long distances in fibre[10,11] and in free-space links[12–15]. Despite these advances, the practical applicability of quantum key distribution is curtailed by the fact that most implementations and protocols are limited to two communicating parties. Quantum networks scale the advantages of quantum key distribution protocols to more than two distant users. Here we present a fully connected quantum network architecture in which a single entangled photon source distributes quantum states to many users while minimizing the resources required for each. Further, it does so without sacrificing security or functionality relative to two-party communication schemes. We demonstrate the feasibility of our approach using a single source of bipartite polarization entanglement, which is multiplexed into 12 wavelength channels. Six states are then distributed between four users in a fully connected graph using only one fibre and one polarization analysis module per user. Because no adaptations of the entanglement source are required to add users, the network can readily be scaled to a large number of users, without requiring trust in the provider of the source. Unlike previous attempts at multi-user networks, which have been based on active optical switches and therefore limited to some duty cycle, our implementation is fully passive and thus has the potential for unprecedented quantum communication speeds.

The quantum key distribution (QKD) networks that have been demonstrated so far can be grouped into five types of configuration. First, quantum repeater networks use quantum memories and entanglement swapping to extend and route quantum states and to form arbitrary network topologies. Although quantum repeaters are very likely to feature prominently in future quantum networks, technological advancement in quantum memories is needed for quantum repeater networks to be considered practical. However, quantum repeaters can also be used to improve the performance of other types of quantum network.

The second type of configuration uses high-dimensional or multipartite entanglement to share entanglement resources between several users[16]. This way, different users share different subspaces of the Hilbert space to generate their keys. However, adding or removing users requires changes in the dimensionality of the system, which makes complex alterations of the source necessary.

The third type of configuration is trusted node networks. They amount to a mesh of point-to-point links, each requiring a complete two-party communication set-up. Although trusted nodes have been used to extend bipartite quantum communication schemes to larger multi-user networks[2–5], they also relinquish the strong security offered by quantum cryptography. Furthermore, this approach creates a substantial resource overhead because it duplicates sender and receiver hardware.

The fourth type of configuration realizes a point-to-multipoint network consisting of two (or more) sets of users, in which a member of the first set can communicate with any member of the second set but not with members of the same set. This type of configuration allows multiple users to share receivers or sources and has been realized in configurations with passive beam splitters[7,17,18], active optical switches that establish a temporary quantum channel between two particular users at a time[6,19–21], and frequency multiplexing[21–24].

The final type of configuration—the most versatile and robust architecture—is a fully connected network architecture connecting every user to every other user simultaneously. A reconfigurable point-to-multipoint network, in which a user can request to be connected to any other user one at a time, has been used to achieve some of the benefits of a fully connected network[25].

Here we present a fully connected network architecture and its realization in the telecommunications band without any requirement for active switching. The transition to all-passive optical networks offers a substantial boost in terms of reliability and miniaturization. Further, it does not limit the distribution rate as per the duty cycle of the switching device. We connected four simultaneously active users to a polarization-entangled photon source via a single optical fibre each. Using the frequency correlations of the photons via wavelength-division multiplexing (WDM), we distributed bipartite entanglement between all pairs of users. This allows all pairs of users to generate their own private key using only a single source.

The complete network architecture can be better understood if divided into layers of abstraction (Fig. 1). The bottom ('physical') layer contains all of the tangible components (physical connections) and forms the physical topology of the network. Each of the four users (Alice, Bob, Chloe and Dave) receives a combination of three wavelength channels via a single-mode fibre. Thus, the source distributes six bipartite entangled photon states to the four users. The middle ('quantum correlation') layer represents the six entangled states (which each corresponds to a different secure key) that link the four users. The top ('communication') layer represents secure classical communication between users and the logical topology of the network.

To create a fully connected graph in the quantum correlation and communication layers with N users, we need a minimum of $N(N-1)/2$ links. Each of the N users is equipped with a single detection module, exactly the same as in standard two-party quantum communication schemes. The service provider multiplexes $N-1$ channels into each single-mode fibre. Thus, using $N(N-1)$ channels, $N(N-1)/2$ entangled photon pairs (and hence secure keys) can be shared by any pair of users. As the number of users increases, the physical topology of the resulting network remains elementary and grows linearly because all channels needed by each user are multiplexed into the same single-mode fibre and detection system. However, the logical topology (that is, the structure and number of quantum correlations and communication links) becomes increasingly complex and grows quadratically. This scalability allows us to easily create large complex networks

[1]Institute for Quantum Optics and Quantum Information—Vienna, Austrian Academy of Sciences, Vienna, Austria. [2]Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Vienna, Austria. [3]Austrian Institute of Technology, Vienna, Austria. [4]Present address: Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory, Department of Electrical and Electronic Engineering, University of Bristol, Bristol, UK. [5]Present address: Fraunhofer Institute for Applied Optics and Precision Engineering, Jena, Germany. [6]Present address: Friedrich Schiller Universitz Jena, Abbe Center for Photonics, Jena, Germany. *e-mail: Soeren.Wengerowsky@oeaw.ac.at; Rupert.Ursin@oeaw.ac.at

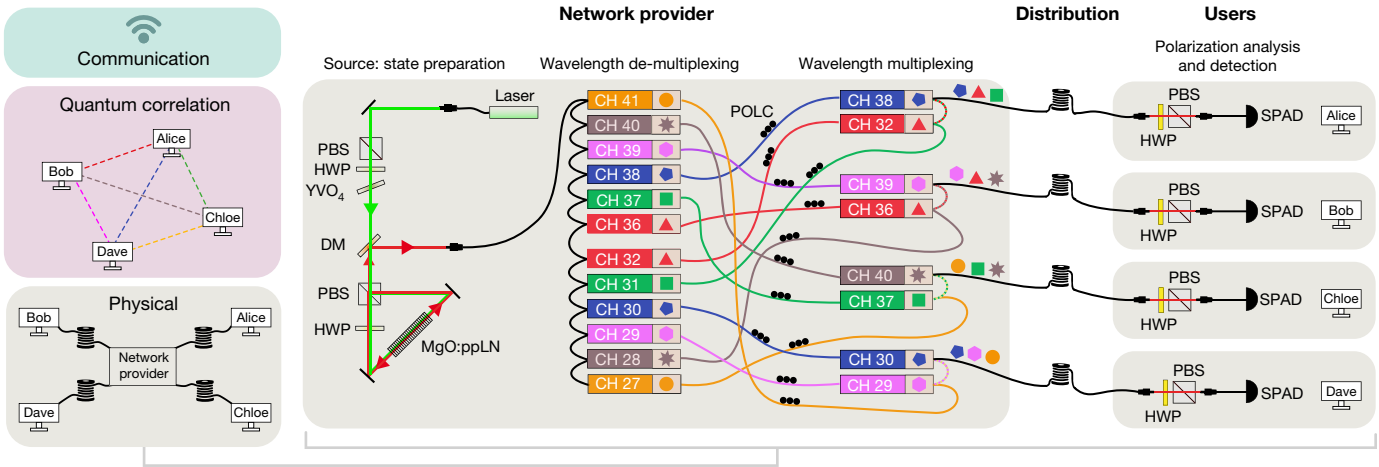


Fig. 1 | Network architecture and experimental set-up. On the left we illustrate the network architecture using three layers of abstraction. The bottom layer represents the physical topology of the network, including all the tangible components shown on the right. The operation of the physical layer allows the distribution of six different entangled states between the four users as shown in the quantum correlation layer (middle). The communication layer (top) exploits the entangled states to enable secure communication. The topology of the physical layer follows a hub-and-spoke model whereas the logical topology of the upper two layers is a fully connected mesh. At the network provider, a laser with a wavelength of 775 nm (green beam) is used to pump a temperature-stabilized magnesium-oxide-doped periodically poled lithium niobate crystal (MgO:ppLN) in a Sagnac-type configuration to create a polarization-entangled state ('state preparation'). The spectrum is then split into 12 International Telecommunication Union (ITU) channels (identified by different coloured symbols) by a cascade of band-pass filters ('wavelength de-multiplexing'). The resulting 12 frequency channels were combined into four single-mode fibres such that each user (Alice, Bob, Chloe and Dave) receives three frequency channels (indicated by the coloured symbols) and therefore shares a polarization-entangled pair with each of the other users ('wavelength multiplexing'). Each of the four users receives only one single-mode fibre from the network provider ('Distribution'), and analyses the polarization with a half-wave plate (HWP) and a polarizing beam splitter (PBS). The photons are then detected using one single-photon avalanche diode detector (SPAD) per user ('Polarization analysis and detection'). CH, ITU channel; DM, dichroic mirror; POLC, manual polarization controllers; YVO_4, yttrium orthovanadate plate.

without changing the source of entanglement, the type of quantum state produced or the user's hardware. At the same time, the topology can be reduced to all possible subgraphs.

The experimental set-up (Fig. 1) can be conceptualized by considering photon pairs from a polarization-entangled source that are separated into different wavelength channels (Fig. 2). Owing to energy conservation during the down-conversion process within the source, entangled photon pairs are observed only in correlated wavelength channels. Each pair of these correlated channels represents one logical link between two users (that is, a shared entangled state). Specific channels are multiplexed into a single fibre and are therefore passively rerouted to each user. Each user now receives $N-1$ channels, thus sharing a different entangled state with every other user.

To implement our network architecture using commercially available dense WDM filters, we developed a source of frequency-correlated polarization-entangled photon pairs at telecommunications wavelengths (Methods; Fig. 1). The wide spectrum of the signal and idler photons (Fig. 2) was divided into six pairs of frequency-correlated channels. Of these 12 channels, each user received three, multiplexed together in a single optical fibre. Ultimately, the source distributed six pairs of polarization-entangled photons between four different users successively, in such a way that each pair of users shares one pair of photons with each other.

To characterize the performance of the entangled-photon source, we measured the fidelity of the state produced as compared to a $|\Phi^+\rangle$ Bell state (see equation (1) in Methods). This measurement was performed directly after de-multiplexing (that is, splitting of the signal and idler photons) but before the multiplexing of several channels to each user. For this measurement, the polarization-entanglement visibility was measured in all three mutually unbiased bases just after the first cascade of band-pass filters. In this case, the fibres were compensated in only one basis (HV, where H represents the horizontal polarization and V the vertical) and the pump state of the source was changed for each measurement to compensate for the other basis. It was important to confirm that the source can provide high-quality entanglement in all available channel pairs. Our measurements show that the fidelity was greater than 97.3% for all channel pairs (Extended Data Table 1). Once we confirmed that the source of entangled photon pairs was able to provide high-quality entanglement, we connected the multiplexers and sent three channels to each of the four users.

To measure the fidelities, all 12 fibre channels were compensated in two mutually unbiased bases from the source until the measurement module to demonstrate that the entangled states were created simultaneously in all channels without further alignment. Further, the multiplexing was implemented so that three channels were detected on each of the four detectors. Entangled pairs were identified using the temporal cross-correlation functions (Fig. 3b).

We used four free-running single-photon avalanche detectors based on a passively quenched InGaAs avalanche photodiode. Three detectors operated at a detection efficiency of 2%–3% and a dark count rate of 350–1,500 Hz with a dead time of 1 μs for the measurement modules 'Bob', 'Chloe' and 'Dave'. The measurement module 'Alice' used a detector with an efficiency of about 10%, 1,000 Hz dark counts and 4 μs dead time. The rate of coincident counts varied between 10 Hz and 65 Hz for the six entangled links because the losses and detection efficiencies were unequal. We measured the visibility of all six entangled links in two mutually unbiased bases, HV and DA (where D represents diagonal polarization and A antidiagonal), and computed the fidelity. This amounts to 16 different basis settings for the HV basis and for the DA basis. Each basis setting was measured for 30 s. The count rates of the four detectors were between 21 kHz and 73 kHz. An overview over the raw counts with the polarization analysers set to H_i, where i denotes Alice, Bob, Chloe or Dave, is given in Extended Data Table 2. At this position, the maximal coincidence rate is expected.

In Fig. 3a we show the results of the Bell-state fidelity measurements. Owing to the timing uncertainty of the detectors, we are limited to a rather large coincidence window of 1 ns. As a result, detector clicks are falsely identified as pairs and deteriorate the measured fidelity. The right-hand side of Fig. 3a shows the fidelity corrected for this error; the uncorrected values are shown on the left.

Using the uncorrected fidelities and count rates (Fig. 3), we estimated a raw key rate between 10 Hz and 34 Hz, which would yield

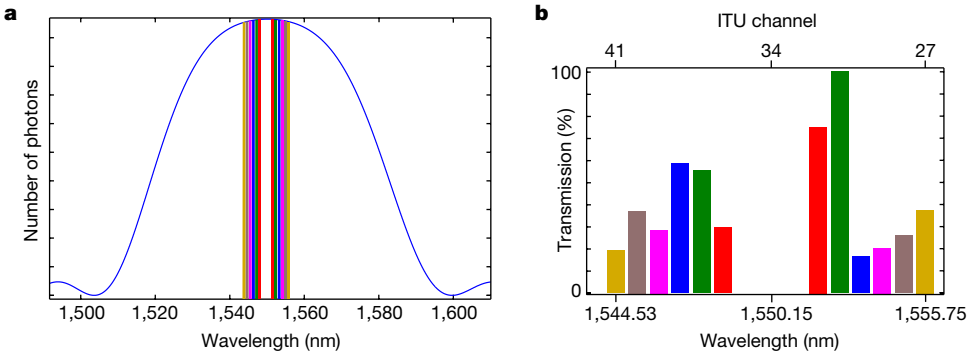


Fig. 2 | Spectrum and wavelength multiplexing. a, Spectrum of signal and idler photons; the bars are colour-coded to indicate entangled pairs of signal (lower-wavelength) and idler (higher-wavelength) photons. The spectrum of the source (blue curve) was calculated using Sellmeier equations for the MgO:ppLN used in the source[30] and information about the periodic poling from the supplier. **b**, Independently measured transmission of each of the wavelength channels (normalized).

a secure key rate between 3 Hz and 15 Hz[1,26]. A fidelity larger than 81% is necessary to obtain a positive secure key rate. Therefore, using their polarization-detection modules, the users were able to measure a non-classical polarization-correlation visibility in the HV and DA bases, from which we can calculate the lower bound on the Bell-state fidelity. These measurements show that we have successfully shared an entangled state between every pair of users.

We have successfully realized a proof-of-principle demonstration of a quantum communication network. The use of telecommunications wavelengths makes it compatible with existing infrastructure. We observed no detectable cross-talk between adjacent channels. The network architecture can be readily adapted to any other network topology. This networking concept can also be combined with previous ideas about access networks[27] and about integration into classical networks[7,17,18]. Further, our experimental demonstration of the network architecture used WDM and a polarization-entangled photon pair source. These choices are specific to the implementation and are not limited by the network architecture or logical topology. Our architecture could instead be implemented using time-division multiplexing (TDM) or time-bin entanglement. The scalability and ease of upgrading of our network architecture make it a good candidate for commercial quantum communication networks.

Our network offers all the security benefits of entanglement-based QKD and does not require trusted nodes. In contrast to networks based on active switching[20,21,25], the only limit on the communication speed in our (passive) scheme is given by the brightness of the source and the quality of the detector (efficiency, timing jitter and dead time). The finite duty cycle and switching rate characteristic of active components do not limit our network.

An alternative method to implement a fully connected quantum network with a similar topology would be to use a 1:N beam splitter and probabilistically distribute entangled photon pairs between all users. The main benefit of our wavelength-multiplexed implementation reveals itself when each user opts to de-multiplex the different wavelength channels onto m single-photon detectors (where $1 < m < N$). In this case, owing to the deterministic frequency correlations, every pair of frequency channels can be considered an independent communication link and an increase in the total key generation rate by a factor of m is achieved while maintaining the same signal-to-noise ratio of a two-party communication. Conversely, probabilistic distribution using a 1:N beam splitter would always reduce the signal-to-noise ratio as users are added.

An interesting question is how many users can be added to our network architecture while maintaining its performance. Because we used one detector per user to detect all three frequency channels, our network is linearly scalable in terms of user resources, and additional users can be added to the network without changing a user's hardware. To add a new user into a network that uses our architecture, the service provider simply multiplexes more channels into each user's fibre. As mentioned above, compared to a two-party communication scheme, detecting more than one channel on the same detector gives a higher noise level because the count rate of each detector is tripled and the coincidence rate per link is unchanged. The measured fidelities show that the network architecture is sound despite the increased noise. The number of available wavelength channels within the entangled photon spectrum and the performance of the detectors used (dark counts, timing jitter and efficiency) also limit the number of users. Our calculations (Extended Data Fig. 1) show that the network can support more

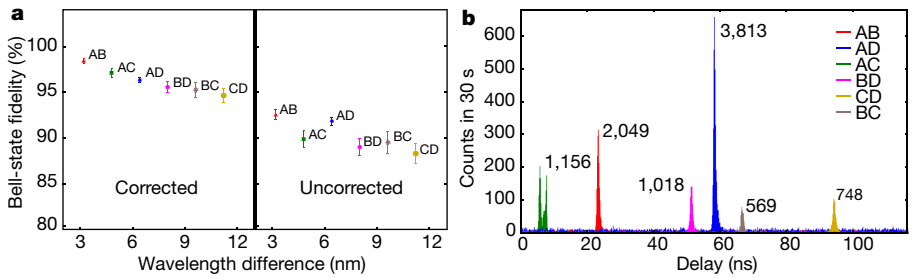


Fig. 3 | Experimental results. a, Measured Bell-state fidelities with (left) and without (right) subtraction of accidental coincidences. Each point is measured using the two WDM channels that connect the respective users (A, Alice; B, Bob; C, Chloe; D, Dave; each two-letter combination represents a link between those two users). The x axis represents the difference in wavelength between the channels of the two partner photons. The error bars correspond to one standard deviation assuming Poissonian statistics. **b**, Temporal cross-correlations between the time traces of the four users' detectors. Each cross-correlation between a pair of time traces (as indicated in the legend) has a distinct peak. The different peak positions correspond to different combinations of channel lengths and detector latencies. Because these are six different correlation functions, the unambiguous identification of the coincidence clicks is guaranteed even if some of the peaks are at the same position in time. The numbers next to each peak correspond to the total number of photon pairs, accumulated over 30 s, that arrived within 0.5 ns from the maximum of a peak at each of the two users.

than eight nodes with our current detectors (1 ns coincidence window, 500 background counts per second) and more than 25 nodes when using 100 ps coincidence windows with the same noise count. However, this limitation can be avoided because all users have the option to split the signal to detect only a few or one frequency channel(s) per detector, which recovers the signal-to-noise ratio of two-party communication. Alternatively, groups of users could temporarily block frequency channels that are not currently needed for their communication. In this way, the network could also be used like an access network with switching on the user side.

Instead of continuous entanglement distribution, it is also conceivable to use a pulsed pump laser for the entangled-photon source (Methods). This would improve the signal-to-noise ratio because it would enable communication between different users to be detected in different time slots, as discussed previously[23]. As well as standard entanglement-based QKD protocols, distributed computation tasks such as the millionaire's problem[28], Byzantine fault tolerance[29] and asynchronous reference-frame agreement[29] can be implemented on our network.

Online content

Any methods, additional references, Nature Research reporting summaries, source data, statements of data availability and associated accession codes are available at https://doi.org/10.1038/s41586-018-0766-y.

Received: 16 February 2018; Accepted: 25 October 2018;
Published online 12 December 2018.

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
2. Stucki, D. et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys.* **13**, 123001 (2011).
3. Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD network. *Opt. Express* **19**, 10387–10409 (2011).
4. Peev, M. et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001 (2009).
5. Xu, F. et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. *Chin. Sci. Bull.* **54**, 2991–2997 (2009).
6. Elliott, C. et al. Current status of the DARPA quantum network. *Proc SPIE* **5815**, 138–149 (2005).
7. Choi, I., Young, R. J. & Townsend, P. D. Quantum information to the home. *New J. Phys.* **13**, 063039 (2011).
8. Mao, Y. et al. Integrating quantum key distribution with classical communications in backbone fiber network. *Opt. Express* **26**, 6010–6020 (2018).
9. Patel, K. et al. Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Phys. Rev. X* **2**, 041010 (2012).
10. Korzh, B. et al. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photon.* **9**, 163–168 (2015).
11. Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
12. Ursin, R. et al. Entanglement-based quantum communication over 144 km. *Nat. Phys.* **3**, 481–486 (2007).
13. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
14. Takenaka, H. et al. Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. *Nat. Photon.* **11**, 502–508 (2017).
15. Günthner, K. et al. Quantum-limited measurements of optical signals from a geostationary satellite. *Optica* **4**, 611–616 (2017).
16. Törmä, P. & Gheri, K. M. Establishing multi-party entanglement with entangled photons. *AIP Conf. Proc.* **461**, 220–228 (1999).
17. Townsend, P. D. Quantum cryptography on multiuser optical fibre networks. *Nature* **385**, 47–49 (1997).
18. Fröhlich, B. et al. A quantum access network. *Nature* **501**, 69–72 (2013).
19. Toliver, P. et al. Experimental investigation of quantum key distribution through transparent optical switch elements. *IEEE Photonics Technol. Lett.* **15**, 1669–1671 (2003).
20. Chen, T.-Y. et al. Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **18**, 27217–27225 (2010).
21. Chang, X.-Y., Deng, D.-L., Yuan, X.-X. et al. Experimental realization of an entanglement access network and secure multi-party computation. *Sci. Rep.* **6**, 29453 (2016).
22. Aktas, D. et al. Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography. *Laser Photonics Rev.* **10**, 451–457 (2016).
23. Zhu, E. Y. et al. Multi-party agile QKD network with a fiber-based entangled source. In *2015 Conf. on Lasers and Electro-optics (CLEO): Science and Innovations* abstr. JW2A.10 (Optical Society of America, 2015).
24. Lim, H. C., Yoshizawa, A., Tsuchida, H. & Kikuchi, K. Broadband source of telecom-band polarization-entangled photon-pairs for wavelength-multiplexed entanglement distribution. *Opt. Express* **16**, 16052–16057 (2008).
25. Herbauts, I., Blauensteiner, B., Poppe, A., Jennewein, T. & Hübel, H. Demonstration of active routing of entanglement in a multi-user network. *Opt. Express* **21**, 29013–29024 (2013).
26. Ma, X., Fung, C.-H. & Lo, H.-K. Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76**, 012307 (2007).
27. Ciurana, A. et al. Quantum metropolitan optical network based on wavelength division multiplexing. *Opt. Express* **22**, 1576–1593 (2014).
28. He, G. P. Simple quantum protocols for the millionaire problem with a semi-honest third party. *Int. J. Quant. Inf.* **11**, 1350025 (2013).
29. Islam, T. & Wehner, S. Asynchronous reference frame agreement in a quantum network. *New J. Phys.* **18**, 033018 (2016).
30. Gayer, O., Sacks, Z., Galun, E. & Arie, A. Temperature and wavelength dependent refractive index equations for MgO-doped congruent and stoichiometric $LiNbO_3$. *Appl. Phys. B* **91**, 343–348 (2008).

Acknowledgements We thank J. Slim for help with the software and E. Acuña Ortega for assistance in the laboratory. We acknowledge financial support from the Austrian Research Promotion Agency (FFG) Projects—Agentur für Luft- und Raumfahrt (FFG-ALR contracts 854022 and 866025), the European Union (EU) under Horizon 2020 contract number FETOPEN-801060 quantum-enhanced on-chip interference microscopy (Q-MIC) and the Austrian Academy of Sciences.

Reviewer information *Nature* thanks V. Martin and the other anonymous reviewer(s) for their contribution to the peer review of this work.

Author contributions The set-up was built by S.W. and the experiment was conducted by S.W. and S.K.J. The network architecture was conceived by S.K.J. and S.W. The source was designed by F.S., S.W. and S.K.J. H.H. helped with the detection of the single photons. R.U. contributed to the experimental design, source and network and to supervising the project. The paper was written by S.W., S.K.J. and F.S. All authors discussed the results and commented on the manuscript.

Competing interests The authors declare no competing interests.

Additional information
Extended data is available for this paper at https://doi.org/10.1038/s41586-018-0766-y.
Reprints and permissions information is available at http://www.nature.com/reprints.
Correspondence and requests for materials should be addressed to S.W. or R.U.
Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

METHODS

Polarization-entangled photon source. The experiment consisted of a source of bipartite polarization-entangled photon pairs, multiplexing and de-multiplexing modules, and user hardware. The source was based on type-0 spontaneous parametric down-conversion in a 4 cm-long magnesium-oxide-doped periodically poled lithium niobate (MgO:ppLN) bulk crystal with a poling period of 19.2 μm. The type-0 process converts, with low probability, one pump photon with a wavelength of 775.075 nm from a continuous-wave laser to a co-polarized signal and idler photons in the telecommunications C-band[31–33].

The MgO:ppLN crystal was bi-directionally pumped inside a Sagnac-type set-up (Fig. 1)[24,34,35], creating a polarization-entangled state in two wavelength channels:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|V_{\lambda_1}V_{\lambda_2}\rangle + |H_{\lambda_1}H_{\lambda_2}\rangle) \quad (1)$$

The spatial mode that contains the signal and idler photons from the source was coupled into one single-mode fibre and spectrally split by a cascade of band-pass filters. The spectrum of the signal and idler photons was centred at 1,550.15 nm (Fig. 2) and the filters were chosen to be symmetric with respect to this centre wavelength. We used 100 GHz band-pass filters as defined by the ITU in G.694.1. On the red side of the spectrum we used ITU frequency channels 27–32; we used channels 36–41 on the blue side. Owing to the well-defined pump wavelength of the continuous-wave laser and energy conservation during down-conversion, we obtained polarization entanglement between pairs of channels (27 and 41, 28 and 40, and so on). Each user receives three channels (Fig. 2) via one fibre and used a polarization analysis module to measure in the HV or DA polarization basis. Single-photon detection events were time-tagged and two-photon coincidence events were identified within a coincidence window of 1 ns. Fibre polarization controllers were used to neutralize the birefringence of the optical fibres.

The energy correlations of the signal and idler photons (see equation (1) and Fig. 2) produced by the source were used to separate these modes into separate fibres (de-multiplexing). We used channels 27 to 32 for the signal photons, while the idler photons were collected in channels 36 to 41. The corresponding wavelengths are provided in Extended Data Table 1. Entangled photon pairs are found in pairs of channels that have the same spectral distance from the centre wavelength. This means that the channel pairs 27 and 41, 28 and 40, and so on, each share a polarization-entangled state (Fig. 2). A viable alternative to the cascade of dense WDM filters is an arrayed waveguide grating, provided that the polarization-dependent loss is low enough.

The 12 channels were combined into four fibres using two band-pass filters per fibre, so that three channels reach each one of the four users via one fibre. This way, every pair of users shares a pair of channels and therefore entangled photons (Fig. 1). The three channels received by each user were analysed on a single polarization analysis module with a single photon detector attached. Each user implemented a basis choice by rotating a half-wave plate.

QKD and signal-to-noise ratio considerations. In general, the chief drawback of our architecture is the amount of noise introduced by detecting several channels on a single detector. The noise results in a loss of fidelity (or quality of the entanglement). To implement a QKD scheme, all users would announce their time tags and correlation functions (Fig. 3b) publicly, so that everybody is able to ignore counts that do not belong to their communication and therefore improve the signal-to-noise ratio. The security of the implementation is preserved, because the annunciation of the time tags does not contain any information about the basis choice or the outcome of the measurement. This improvement is related to the total losses in the system, as shown in Extended Data Fig. 1. This is equivalent to ignoring all global ($n > 2$)-fold events. However, it makes a noticeable effect only for very low-loss scenarios, as can be seen from Extended Data Fig. 1.

In other words, the count rate S_i per user in a network with N nodes, the link and system efficiency η and the dark count rate D would be reduced by a term that scales proportional to the coincidence probability:

$$S_i = D + (N-1)\frac{P}{2}\eta - (N-2)\frac{P}{2}\eta^2$$

with P being the total number of available pairs in the spatial and spectral collection mode of the source. The rate of coincidence clicks can be estimated as

$$C = \frac{P}{2}\eta^2 + \tau S_i^2$$

The accidental coincidences (τS_i^2) account for the minimum number of coincidences observable using a coincidence window of length τ and therefore reduce the contrast.

Another substantial improvement can be made by decreasing the coincidence time window. This can be achieved by using faster detectors with a much smaller timing jitter. For example, reducing the coincidence window to 100 ps results in the maximum fidelities shown in Extended Data Fig. 1.

Scalability. Our network architecture is easily scalable and users can be added and removed without any change to the user's hardware. However, like most existing network hardware there are limitations to the scalability. The three main limitations are: first, the brightness of the source; second, the limited bandwidth of the source, which dictates how many wavelength channels can be used; and third, accidental coincidences, which contribute substantially to the quantum-bit error rate and increase markedly with the number of users. The first limitation can be overcome by using more or longer waveguides and crystals, and stronger pumping; the second can be overcome by using narrower wavelength channels; and the third can be mitigated by using the method described above to help reduce the noise. Naturally, using faster detectors and therefore shorter coincidence windows can also help. A pulsed pump experiment would further mitigate the problem of accidental coincidences by defining fixed time slots for the arrival of each channel at the detector.

Our network architecture offers the advantage of simultaneous communication between one node and every other node. Nevertheless, should one user choose to completely block the signal from a set of other users, an active switch capable of selecting certain channels can be used. This would allow users to control the network topology and create custom subgraphs without the intervention of the service provider. Further, detecting only a chosen subset of channels would limit the accidental coincidence rates and allow for faster communication with a chosen subgraph.

Pulsed network scheme. The drawback of the scheme presented here is the increase in the accidental count rates due to the multiplexing of many quantum channels onto a single detector. This limitation can be completely overcome by using a pulsed scheme. Consider the experiment presented here, but using a pulsed laser with a pulse width much smaller than the detector jitter. Further, each of the N users has gated detector(s) for which the gate is opened $N-1$ times for each laser pulse. Each opening of the gate corresponds to the time delay between different coincidence peaks among all users with each user in question. With ideal detectors, the performance of the pulsed scheme will be equivalent to $N-1$ separate quantum communication set-ups with the same detectors and comparable count rates per link. When using real-world detectors such as InGaAs SPADs that have a large dead time, the performance of our pulsed network scheme can exceed that of $N-1$ independent set-ups. When the dead time of the detector is larger than the interval between opening each of the $N-1$ gates for each pulse of the source, a noise count in one gate prevents the occurrence of a noise count in all subsequent gates within the dead time. This suppression of noise clicks can lead to improved key rates and quantum-bit error rate[1]. The advantage is strongest when there is only one photon pair in the given set of $N-1$ links per user.

This pulsed network scheme would require an additional gating signal to be sent to each user. Further, it could be unsuitable for mobile nodes because all nodes need to compensate the delays to all other nodes. However, for fixed users, the pulsed network scheme is ideal and greatly improves the network throughput by reducing the accidental count rate by a factor equal to the duty cycle of the gating.

Multiplexing and types of entanglement. The logical network topology that we have outlined here is independent of the type of entanglement or multiplexing used. Nevertheless, different types of multiplexing have advantages. For example, a scheme based on WDM has a few advantages over that based on TDM. First, the active switching used in TDM is prone to mechanical breakdown and in more complex networks several switches may need to operate synchronously. Second, a bright source can produce multiple photon pairs within a single coincidence time window. However, the probability that multiple pairs are produced in exactly the same wavelength channel is negligible. Thus, WDM-based networks could have a distinct advantage. Third, introducing an additional TDM channel will reduce the coincidence rates seen by all users, but an additional WDM channel will not affect existing connections. Last, cross-talk between the channels is not harmful, because photons in the wrong channel would, owing to the different delay introduced by the WDM filters, contribute to only the accidental rate and not be seen as a separate coincidence peak. On the other hand, a TDM-based scheme would need only $2N$ channels. Large-scale networks could also combine the advantages of WDM and TDM by using both together.

Fibre-based quantum communication has often been performed using time-bin entanglement[22,36] to avoid having to compensate for the birefringence of the fibre. However, this requires the service provider and users to have matched and stabilized interferometers (the stabilization of which often requires another stable laser). Although the logical network topology is compatible with this form of entanglement, we chose to use polarization entanglement because it simplifies the user's hardware. Changes in the birefringence of the optical fibre are easily monitored and compensated for by using regular test signals.

In principle, our network architecture is not limited to the use of single photons. It is also conceivable to perform continuous-variable QKD with a source of entanglement, as proposed previously[37].

Usage scenarios. Quantum communication is often thought of as a purely academic concept or experiment. However, the technology is mature enough to consider practical problems regarding the deployment and use of QKD links. Typical classical networks consist of smaller local-area networks (LANs) and similar as well as much larger inter-city networks. Both a LAN and an inter-city network have a limited number of users. To connect a large number of users together the networks must be interconnected to create the 'internet'. Similarly, a quantum internet must also be an interconnection of several networks. A single user in our network architecture could be replaced by a quantum repeater or entanglement swapping set-up to interconnect several similar quantum networks. The most substantial differences between the two types of network are the distances spanned, the costs and the target market.

To realize a cheap LAN with current technologies and our network architecture, we propose using a cheaper type of single photon detector—SPADs. These typically have a low detection efficiency and large timing jitter. As can be seen by extrapolating Extended Data Fig. 1a, the network will be able to tolerate more than 30 dB of loss with up to 12 users. This loss is more than sufficient to account for a few kilometres of optical fibre, the heralding efficiency of a typical source and the poor detection efficiency of SPADs.

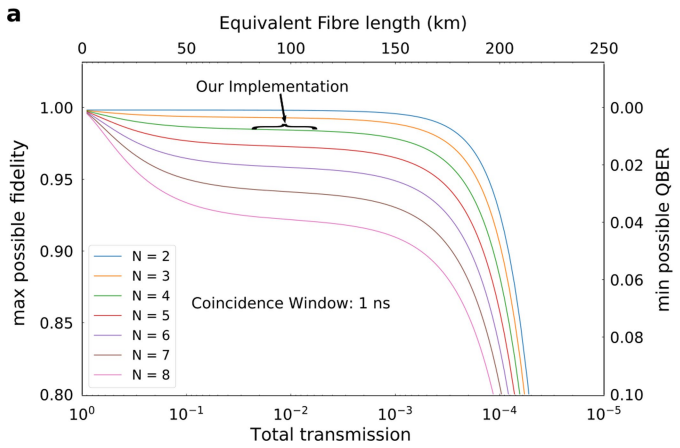
Inter-city networks naturally cost much more than a LAN. Our network architecture can be used to build large-scale inter-city quantum networks by using high-efficiency low-timing-jitter detectors such as nano-wire detectors. Extended Data Fig. 1b shows that we can tolerate more than 43 dB of loss with up to 25 users spanning distances of more than 200 km.

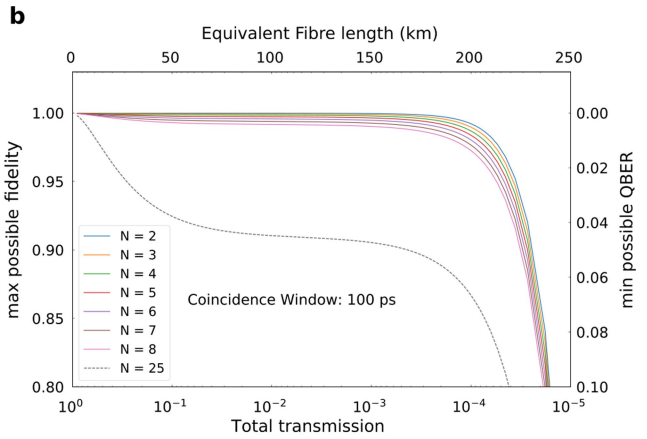
Further, in any network it is always advantageous to make the user's hardware requirements as simple as possible, with the centralized network hardware having the majority of the complexity. We have designed our network architecture along these principles, with almost all complexity in the three centralized stages—source, de-multiplexing and multiplexing.

Data availability

The data that support the findings of this study are available from the corresponding authors on request.

31. Oh, J., Antonelli, C. & Brodsky, M. Coincidence rates for photon pairs in WDM environment. *J. Lightwave Technol.* **29**, 324–329 (2011).
32. Ghalbouni, J., Agha, I., Frey, R., Diamanti, E. & Zaquine, I. Experimental wavelength-division-multiplexed photon-pair distribution. *Opt. Lett.* **38**, 34–36 (2013).
33. Monteiro, F., Martin, A., Sanguinetti, B., Zbinden, H. & Thew, R. T. Narrowband photon pair source for quantum networks. *Opt. Express* **22**, 4371–4378 (2014).
34. Kim, T., Fiorentino, M. & Wong, F. N. C. Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer. *Phys. Rev. A* **73**, 012316 (2006).
35. Fedrizzi, A., Herbst, T., Poppe, A., Jennewein, T. & Zeilinger, A. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Opt. Express* **15**, 15377–15386 (2007).
36. Inagaki, T. et al. Entanglement distribution over 300 km of fiber. *Opt. Express* **21**, 23241–23249 (2013).
37. Roslund, J., De Araújo, R. M., Jiang, S., Fabre, C. & Treps, N. Wavelength-multiplexed quantum networks with ultrafast frequency combs. *Nat. Photon.* **8**, 109–112 (2014).





Extended Data Fig. 1 | Calculated fidelities and quantum-bit error rate (QBER) for two to nine users versus the system efficiency and equivalent fibre length, assuming an attenuation of 0.2 dB km^{-1}. **a**, Using detectors with a 1 ns timing jitter. This is great for cheap networks with low losses (those over a small area such as a LAN). **b**, Using detectors with a 100 ps jitter allows us to sustain much higher losses and many more users. This is useful for long-distance inter-city links. Both graphs were calculated using a generated pair rate of 1.7 million pairs per second and a dark count rate of 500 per second per detector.

Extended Data Table 1 | Measured fidelities

ITU Ch. Numbers	Channel Wavelengths (nm)	Fidelity (±0.3%)
27 / 41	1555.75 / 1544.53	98.0 %
28 / 40	1554.94 / 1545.32	98.7 %
29 / 39	1554.13 / 1546.12	99.1 %
30 / 38	1553.33 / 1546.92	99.0 %
31 / 37	1552.52 / 1547.72	99.2 %
32 / 36	1551.72 / 1548.52	97.3 %

The Bell-state fidelity of the entangled state produced by the source is measured directly at the channel pairs before multiplexing.

Extended Data Table 2 | Count rates

	Alice	Bob	Chloe	Dave
Alice	2204203	2049	1156	3813
Bob		878692	569	1018
Chloe			636268	748
Dave				1231478

Measured coincidence counts between two users in 30 s are given for all four measurement stations at the setting HHHH. The total counts in 30 s at each station are shown on the diagonal.