Experimental quantum conference key agreement

PHYSICS

Experimental quantum conference key agreement

Massimiliano Proietti[1†], Joseph Ho[1†], Federico Grasselli[2], Peter Barrow[1], Mehul Malik[1], Alessandro Fedrizzi[1]*

Quantum networks will provide multinode entanglement enabling secure communication on a global scale. Traditional quantum communication protocols consume pair-wise entanglement, which is suboptimal for distributed tasks involving more than two users. Here, we demonstrate quantum conference key agreement, a cryptography protocol leveraging multipartite entanglement to efficiently create identical keys between *N* users with up to *N-1* rate advantage in constrained networks. We distribute four-photon Greenberger-Horne-Zeilinger (GHZ) states, generated by high-brightness telecom photon-pair sources, over optical fiber with combined lengths of up to 50 km and then perform multiuser error correction and privacy amplification. Under finite-key analysis, we establish 1.5×10^6 bits of secure key, which are used to encrypt and securely share an image between four users in a conference transmission. Our work highlights a previously unexplored protocol tailored for multinode networks leveraging low-noise, long-distance transmission of GHZ states that will pave the way for future multiparty quantum information processing applications.

INTRODUCTION

Conference key agreement (CKA) is a multiuser protocol for sharing a common information-theoretic secure key beyond the two-party paradigm (*1*). This key allows group-wide encryption for authenticated users to communicate securely, wherein, exclusively, members of the group can decrypt messages broadcast by any other member. Traditional two-party quantum key distribution (2QKD) primitives (*2*–*5*) can be used to share *N-1* individual key pairs between *N* users followed by classical computational steps to distill a conference key. However, this is inefficient for producing conference keys when users have access to a fully connected quantum network, as envisioned in the "quantum internet" (*6*, *7*). An efficient alternative is to derive conference keys directly from multipartite entangled states created in these networks (*8*–*10*)—we refer to these methods as quantum CKA (QCKA).

QCKA is a generalization of entanglement-based QKD to *N* users (*1*). The currently most practical QCKA variant is based on the distribution of GHZ states (*9*). This protocol has been proven secure including for the finite-key scenario and offers performance advantages over conference key generation from pair-wise keys (2QKD) under different noise models, channel capacity constraints, and network router configurations (*8*, *9*, *11*–*15*). The clearest advantage of QCKA arises in true quantum networks (*16*): GHZ states can be distilled from an underlying network graph state in as little as a single network use, while 2QKD requires up to $N-1$ copies to generate the required key pairs (*8*).

Here, we experimentally demonstrate the salient features of the N-BB84 protocol introduced in (*9*) with a state-of-the-art photonic platform. An untrusted quantum server prepares and distributes L rounds of the maximally entangled GHZ state, $|GHZ\rangle \equiv (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})/\sqrt{2}$, to N participants in the network. In our work, we implement a four-party protocol consisting of Alice (A), Bob 1 (B_1), Bob 2 (B_2), and Bob 3 (B_3) (see Fig. 1A). Each user performs quantum measurements on their respective photon in either the Z-basis $\{|0\rangle, |1\rangle\}$ constituting type-1 rounds or the X-basis $\{|+\rangle \doteq (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle \doteq (|0\rangle - |1\rangle)/\sqrt{2}\}$ for type-2 rounds. Type-1 rounds contribute to the raw key, as these measurements ensure all users in the protocol obtain the same bit value owing to the structure of the GHZ state. A small portion of these outcomes will be consumed to determine the error rates. Type-2 rounds are carried out randomly with probability p, for a total of $m = L \cdot p$ rounds, and are used to detect the presence of an eavesdropper. Users coordinate the measurement sequence using $L \cdot h(p)$ bits of a preshared key; here, $h(\cdot)$ is the Shannon entropy. In particular, one user generates the L-bit string, indicating the measurement type of each round. The string can be classically compressed, shared, and decompressed by the other parties. Note that the values of p are typically on the order of 0.02, leading to a small value of $h(p)$, i.e., the amount of information to be initially preshared is small.

Once the measurements are complete, the users proceed to verifying the security of their key by performing parameter estimation. All users announce their outcomes for a subset of the type-1 rounds, m in total and randomly chosen, and all m type-2 rounds to determine $Q^m_{AB_i} = (1 - \langle \sigma_z^A \sigma_z^{B_i} \rangle)/2$ for $i = \{1, 2, 3\}$ and $Q^m_X = (1 - \langle \sigma_x^{\otimes 4} \rangle)/2$, respectively. We define the quantum bit error rate (QBER) as $\mathrm{QBER}^m \doteq \max Q^m_{AB_i}$. All users retain $n = L - 2m$ bits forming the raw conference key, subsequently corrected with an error correction scheme and shortened with privacy amplification to ensure security. Last, all users remove $L \cdot h(p)$ bits from their secret conference key to encode the preshared keys for subsequent protocols. Hence, our protocol is a key-growing routine, as in any known QKD scheme.

RESULTS

In our experiment (see Fig. 1B), we use two high-brightness, polarization-entangled photon-pair sources (*17*) at telecommunication wavelength (1550 nm). We generate four-photon GHZ states by nonclassically interfering one photon from each source on a polarizing beamsplitter (PBS), which has success probability of 1/2 [see, for example, (*18*) or Materials and Methods for details]. We use commercially available superconducting nanowire single-photon detectors (SNSPDs) with typical quantum efficiencies of >80% at this wavelength.

[1]Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK. [2]Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany.
*Corresponding author. Email: a.fedrizzi@hw.ac.uk
†These authors contributed equally to this work.

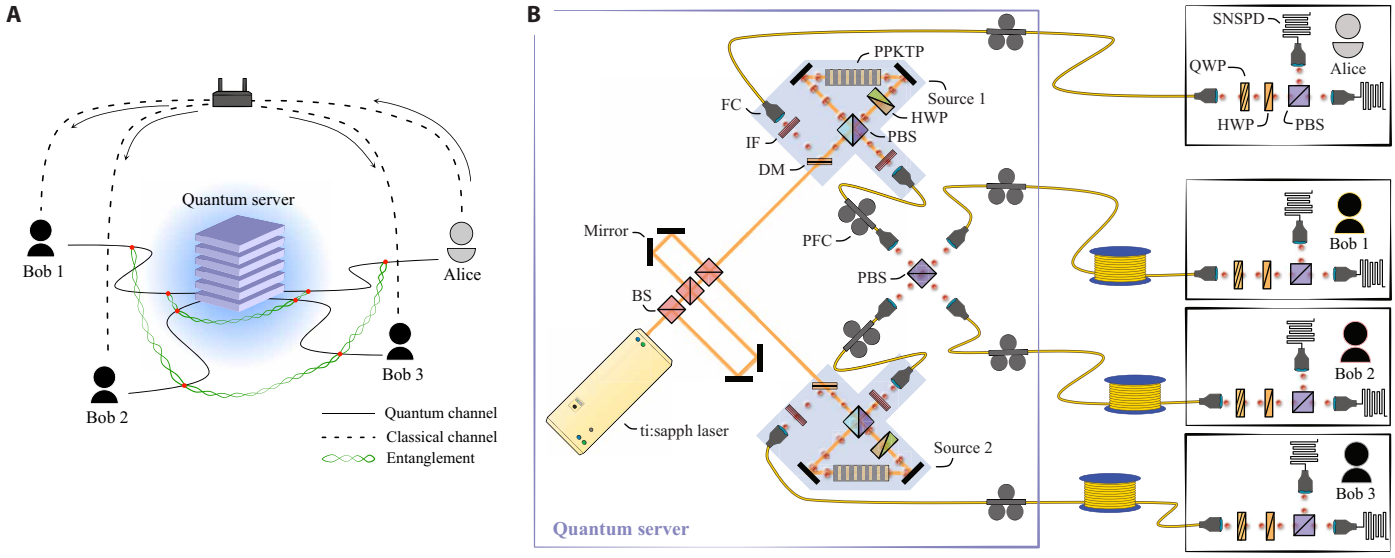

Fig. 1. Quantum conference key agreement scheme and experimental layout. (**A**) A quantum server distributes entangled GHZ states to Alice, who initiates the protocol, and Bob 1, Bob 2, and Bob 3. They establish a common key from a pre-agreed sequence of *Z* measurements while checking the security by measuring *X*. (**B**) A mode-locked picosecond laser (ti:sapph) multiplexed to 320 MHz repetition rate, using a series of beamsplitters (BSs), supplies two entangled photon sources, which are based on parametric downconversion in periodically poled KTP (PPKTP) crystals, pumped bidirectionally in a Sagnac loop for producing polarization-entangled Bell pairs (*17*). Down-converted photons are separated from the pump with dichroic mirrors (DMs), interference filters (IFs), and single-mode fiber couplers (FCs). Fiber links are housed in fiber polarization controllers (FPCs) to undo unwanted rotations. One photon from each source nonclassically interferes on a polarizing beamsplitter (PBS), creating the four-photon GHZ state (see Materials and Methods for details). Each user receives their photon via single-mode fibers and performs projective measurements in the *Z*(*X*)-basis by using a quarter wave plate (QWP) and half-wave plate (HWP), and a PBS before detection with superconducting nanowire single-photon detectors (SNSPDs). Detection events are time-tagged and counted in coincidence within a 1-ns time window.

We establish the upper bound on the performance of our protocol by assuming an infinite number of rounds can be performed, $L \to \infty$. In this asymptotic regime, nearly all rounds are used to extract the raw key, $p \to 0$. We evaluate the asymptotic key rate (AKR) as the fraction of secret bits, ℓ, extracted from the total rounds (*9*)

$$\mathrm{AKR} = \frac{\ell}{L} = 1 - h(Q_X) - h(\mathrm{QBER}) \quad (1)$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. From Eq. 1, we note that the AKR depends only on the noise parameters Q_X and QBER. We estimate these parameters experimentally using a large sample size of type-1 and type-2 measurements to minimize uncertainties. The results are shown in Fig. 2.

We denote the network topology as {d_1, d_2, and d_3}, where d_i is the fiber length in kilometers between B_i and the server. Alice remains fixed at 2 m from the server in all cases. We implement four scenarios, such as {0, 0, 0}, {0, 0, 20}, {0, 10, 20}, and {20, 10, 20}, corresponding to measured network losses (in dB) of 0, 4.84, 7.57, and 11.77. The observed four-photon generation rates g_R for these scenarios are 40.89, 12.68, 6.31, and 2.03 Hz. The conference key rate is determined as a product of the fractional AKR and the recorded generation rates g_R. In all cases, we observe similar noise parameters, and thus AKR, indicating that the entanglement quality is not degraded substantially by the transmission in fibers. The experimental AKR is mainly limited by multiple-pair generations at the sources and by spectral impurities of the photons (see the Supplementary Materials for details). Our work demonstrates the distribution of 1550-nm four-qubit entangled state in long telecom fibers, proving the viability of polarization-encoded photons to remain highly entangled over long distances.

We also include the adjusted conference key rates when we perform the protocol with actively switched measurement bases. In our experiment, this is accomplished by rotating wave plates with motorized stages that are slow compared to the clock rate of our sources. Hence, this leads to a reduced overall rate as shown in Fig. 2 (see Materials and Methods for details).

The AKR results allowed us to establish upper bounds for several different fiber arrangements comparably quickly. To also show the N-BB84 performance in a real-world scenario, we implemented the complete protocol, including error correction and privacy amplification, for a fifth asymmetric fiber network {5, 10, 20} with a measured loss of 9.53 dB in total. Because of the low rates, we need to apply finite-key analysis for this step, i.e., the secret key rate (SKR) is adjusted to account for finite statistics from parameter estimation. For our experiment, we determine the optimal fraction of type-2 measurements to be $p = m/L = 0.012$. With this value of p, the amount of information reserved for the preshared key is $h(p) = 0.093$ (see Materials and Methods for more details). Moreover, we set a total security parameter i.e., the maximal probability that an eavesdropper gains nonzero information about the key to be 1.8×10^{-8} (see the Supplementary Materials for details).

We obtain more than 4.09×10^6 type-1 rounds and 5.01×10^4 type-2 rounds during 177 hours of continuous measurement. Because of the long measurement time, active polarization feedback was implemented to minimize noise owing to thermal drifts in the laboratory (see Materials and Methods for details). Once the raw key is distilled by all users, we implement one-way error correction using low-density parity check (LDPC) codes complying with the Digital Video Broadcasting (DVB-S2) standard (*19*). The code was adapted to our multiparty scenario, simultaneously correcting Bob 1,

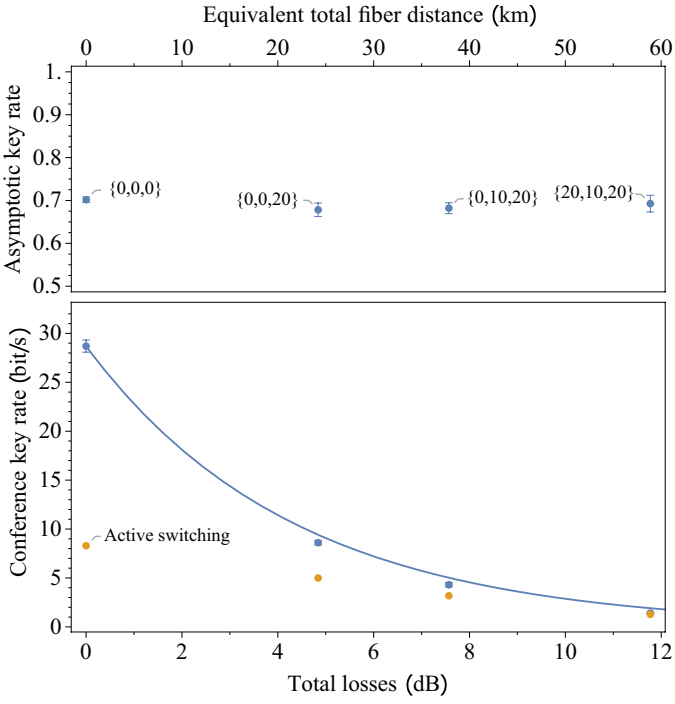

Fig. 2. Asymptotic N-BB84 key rate for the implemented range of total loss / fiber distances. (**Top**) The AKR is determined by evaluating Eq. 1 via parameter estimation of Qx and QBER, assuming ideal performance of error correction and privacy amplification. The measured QBER in these four scenarios, from smallest to greatest total loss, are {0.013 ± 0.001, 0.012 ± 0.002, 0.014 ± 0.002, and 0.015 ± 0.002}, and the measured QX are {0.031 ± 0.001, 0.037 ± 0.002, 0.034 ± 0.002, and 0.031 ± 0.003}. (**Bottom**) The conference key rate is plotted as a function of the total fiber length in the network. We include results of the generation rates with measurement-basis switching using our implementation (see Materials and Methods for details).

Bob 2, and Bob 3's keys. This step ensures that all parties share a common key, which is not yet perfectly secure because of information leaked during error correction and any potential eavesdropping during the distribution step. To reduce the information held by any potential eavesdropper, we implement one round of privacy amplification on the entire raw key, reducing its final length. We use Toeplitz matrices for this purpose, a class of 2-universal hash functions (*20*) that can be implemented efficiently for our given key size.

We estimate the theoretical performance of our postprocessing steps by evaluating the noise parameters Q_X = 0.05 and QBER = 0.0159, which we use to calculate the upper bound set by Eq. 5 (see Materials and Methods) and plotted in Fig. 3A (dashed line). When performing the protocol in earnest with a finite dataset to estimate these parameters, we replace the Shannon limit for the error correction term $h(\mathrm{QBER}^m + 2\xi_z)$ in Eq. 5, with the fraction of parity bits disclosed by Alice.

Last, we use the secret conference key to encrypt an image of a Cheshire cat that is shared between the parties in a brief conference call (Fig. 3B). As shown, the key established by CKA enables any honest user in the group to share a secret message among all other honest parties. This is in contrast with quantum secret sharing, a multiuser task demonstrated previously (*21*, *22*), which requires cooperation among a majority subset of users to verify honesty and obtain the secret message.

DISCUSSION

A number of QCKA protocols have been proposed, including "*N*-six-state" with three measurement bases (*8*). We implemented N-BB84 because it is experimentally friendly and enables higher rates for short keys (*9*). Novel QCKA variants include adaptations of two-party twin-field (*23*) and phase-matching (*24*) protocols. These are attractive due to the high rates achievable with weak coherent pulse sources. However, they require a common phase reference between all *N* users, which will be challenging in a network.

The N-BB84 protocol inherits several features from the entropic security proofs (*25*) for the entanglement-based two-party protocols it is based on. In particular, an eavesdropper's knowledge can be bounded without full characterization of all parties' measurement devices. The GHZ-state source can be completely untrusted. Alice's measurement device is trusted to ensure mutually unbiased measurement bases. The Bob devices can then be untrusted, since any deviation from ideal *X* measurements negatively affects the security parameter Q_X (*9*). Last, all measurement devices are assumed to be memoryless, i.e., each measurement outcome is independent from any other outcome, and detector efficiencies must be basis independent (*25*). Adapting the QCKA protocol for full (measurement-) device independence is work in progress (*26*, *27*).

Another open question is that of the achievable rates in conference settings. For direct GHZ-state transmission as demonstrated here, quantum CKA scales unfavorably with the number of users due to the exponential reduction in multiphoton detection due to unavoidable transmission losses. However, loss will not be a problem in fully featured quantum networks, where CKA has a significant (*N-1*) rate advantage. General bounds for distributing multipartite entanglement in networks with nontrivial connectivity and noise have only very recently been established (*28*). For our own four-user scenario, we show in the Supplementary Materials that the QCKA rates have a nontrivial dependence on asymmetric network noise.

The rate comparison between QCKA and 2QKD in (*8*) did not account for the fact that 2QKD primitives incur not only postprocessing overheads in respect to QCKA but also a cost on the SKRs with respect to the underlying point-to-point rates. In 2QKD, (*N-1*) unique pair-wise keys are transformed into a common secret key via bit-wise XOR operations. If each bipartite key is ϵ-secure, then the final conference key is $(N-1)\epsilon$-secure owing to the composability of this multistep approach (*29*). To obtain an ϵ-secure conference key, the individual keys have to be postprocessed to a security threshold $\frac{\epsilon}{N-1}$, which lowers the final key rate.

Future experimental development will focus on increasing GHZ rates, the extension to more conference parties, and field tests in established fiber networks (*4*). Multiparty entanglement applications beyond CKA include entanglement-assisted remote clock synchronization (*30*), quantum secret sharing (*21, 22, 31*), and GHZ-based repeater protocols (*32*).

MATERIALS AND METHODS

Entangled photon source

We produce photon-pairs using type-2 collinear spontaneous parametric down conversion implemented in a 22-mm-long periodically poled KTP (PPKTP) crystal. Both of our sources are optically pumped using a mode-locked laser operating with a nominal repetition rate of 80 MHz, 1.4-ps pulses, and its central wavelength at 774.9 nm. A passive pulse interleaver is used to quadruple the 80-MHz

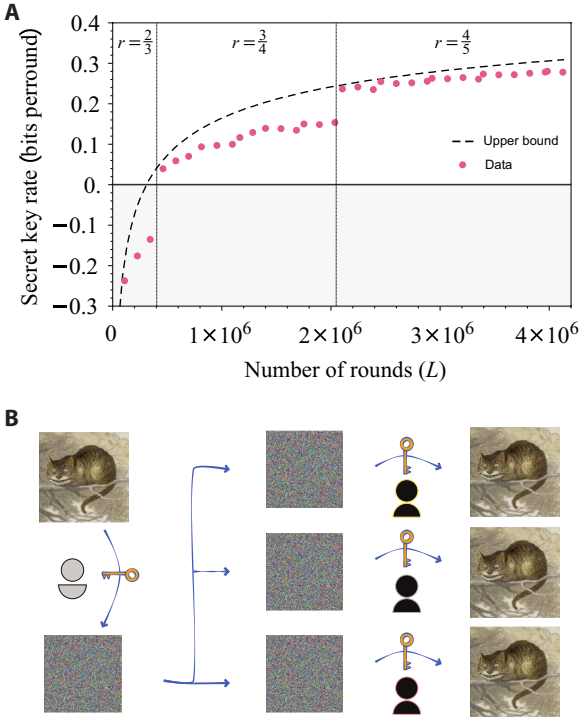

Fig. 3. Finite-key results and application in multi-user encryption. (**A**) We implement all steps in the N-BB84 protocol for a range of L rounds to retrieve the final key of length ℓ and evaluate the SKR, SKR = ℓ/L. In our experiment, we use LDPC codes with fixed code rates, r, using the estimated QBER in each run. We implement privacy amplification using Toeplitz matrices and then remove a portion of the final key for the preshared bits used to encode the measurement-type rounds. The upper bound given by Eq. 5 is shown compared to the experimental data. (**B**) We generate an ϵ_{tot}-secure conference key of 1.15×10^6 bits. Using 1.06×10^6 bits, Alice encrypts an image [8-bit red green blue (RGB), 211 by 211 pixels] using a one-time pad-like scheme. Alice sends the encrypted image over a public channel, allowing only Bob 1, Bob 2, and Bob 3, who share the conference key, to decode the image.

pulse train to 320 MHz (*33*). The PPKTP crystals are embedded within a polarization-based Sagnac interferometer (*17*) and pumped bidirectionally using a half-wave plate (HWP) to set diagonally polarized light to create polarization-entangled photons at 1549.8 nm in the approximate state

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|h\rangle|v\rangle - |v\rangle|h\rangle) \quad (2)$$

where $|h\rangle \equiv |0\rangle$ and $|v\rangle \equiv |1\rangle$ represent horizontal and vertical polarizations, respectively. This state can be mapped to any Bell state via local operation on one of the two photons.

With loose bandpass filters of 3-nm bandwidth, we measure an average source brightness of ~4100 pairs/mW per second, with a symmetric heralding efficiency of ~60% (*34*). The average heralding efficiency reduces by ~12%, with a commensurate decrease of 45% in source brightness at the point of detection of the four users for zero fiber length. We characterize each photon pair source by performing quantum state tomography, reconstructing the density matrix using a maximum-likelihood estimation followed by Monte-Carlo simulations based on Poissonian count statistics to determine errors. For each source, we obtain a typical two-photon Bell-state fidelity $F = 95.58 \pm 0.15\%$ and purity $P = 92.07 \pm 0.27\%$, while entanglement is measured by $\mathcal{C} = 92.38 \pm 0.21\%$.

The four-photon GHZ state is created by interfering one photon from each source on a PBS, which transmits horizontally and reflects vertically polarized photons. After selecting on the case where one photon is emitted in each output, which occurs with a probability of 1/2, we obtain the state

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|hhhh\rangle - |vvvv\rangle) \quad (3)$$

We measure independent two-photon interference visibility of 92.96 ± 0.95% using 100 mW pump power, and four-qubit state tomography returns a purity and fidelity of $P = 81.39 \pm 0.83\%$ and $F = 87.58 \pm 0.48\%$, respectively.

Active switching

Most QKD protocols require random switching of the measurement basis, either passively or actively, with each clock cycle. This is also required for the N-BB84 protocol, with the optimal performance attained by ensuring users switch between the Z/X measurement bases according to a pre-agreed random sequence. Since all users implement the same measurement sequence, passive basis choice cannot be used to achieve the optimal key rates. Note that if passive random measurements are used followed by reconciliation among the N users, then the overall key rate incurs a $\sim 1/(2^N)$ reduction, as the fraction of useable rounds depends on attaining the correct $Z^{\otimes N}$ and $X^{\otimes N}$, respectively.

As noted, p is typically small; hence, switching between bases occurs relatively infrequently. In addition, the multiphoton detection rates in our experiment are low; hence, the standard method of polarization switching with electro-optic modulators would be excessive. We therefore implemented active switching using motorized rotation stages with switching speeds on the order of seconds—marginally slower than our average required switching periods, which reduces the maximum possible raw generation rate g_R.

We evaluate the adjusted generation rate g_R' for the finite-key scenario for the {5, 10, 20} topology by performing 1000 rounds of the protocol with active basis switching. We set $p = 0.02$; thus, 20 type-2 rounds are randomly allocated in the measurement sequence. We measured the reduced key generation rate and found $g_R'/g_R = 0.91$.

This adjustment ratio is rate dependent. We find the lower bound on g_R' by assuming the type-2 rounds are never sequential; hence, each occurrence requires time to switch. This leads to the general expression

$$g_R' \geq \frac{1}{\tau_s p + \frac{1-p}{g_R}} \quad (4)$$

where τ_s is the switching speed. We use this equation to extrapolate the adjusted generation rates obtained in the asymptotic case, as shown by orange dots in Fig. 2.

Active polarization control

The optical fiber links in our experiment are realized by spools of bare SMF28 fiber. Thermal drifts in the laboratory introduces unwanted rotations in polarization, which, if uncorrected, leads to added noise in the protocol. These effects are typically negligible for short-fiber lengths, e.g., in our testing, we found that the 5-km spool

added no observable noise greater than with a 2-m fiber link, while the 10- and 20-km spools showed significant added noise in Q_{ABi} measurements.

We implement active polarization control to correct for these effects during key transmission to preserve low-noise operation throughout the protocol. The feedback control loop is implemented by performing single-qubit tomography in each fiber to characterize the unitary transformation on the polarization qubits. We then use the polarization optics in the measurement stages to undo the rotations on the qubits and perform measurements in the required basis. In our setup, we carry out one-qubit tomography of all four fiber links simultaneously, including postprocessing, to obtain an estimate of the unitary operation and implement the corrective action on the motorized waveplates. This takes less than 30 s and is performed once every ~20 min for an optimal trade-off between maintaining a high-duty cycle while minimizing bit error rates.

This feedback loop is not monitored for tampering by an eavesdropper. From a strict security perspective, a clever adversary may exploit this channel for executing a variant of the "time-shift" attack to gain control over a user's detectors. In principle, this can be mitigated by each user who swaps which detectors register the $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ events randomly in each round by rotating their waveplates. This can be performed locally without additional communication overhead among users.

Error correction using LDPC codes

The use of LDPC codes allows one party to initialize the routine by computing $(j - k)$ parity check bits from a block of k raw bits using a $H_{(j-k)\times k}$ parity check matrix. The ratio $r = k/j$ defines the code rate, and higher code rates correspond to a smaller amount of information disclosed for error correction. The DVB-S2 standard provides H matrices already computed for a set of different code rates specified by an encoding block size of $j = 64'800$ bits. In our experiment, we set the code rate according to the estimated QBER using m samples with appropriate ξ_Z correction. From the provided set of code rates, we used 2/3, 3/4, and 4/5 for small, mid, and large values of L, as shown in Fig. 3A. Alice computes the parity check bits by applying the parity check matrix H to k-bit blocks of her raw key. She then sends the parity check bits, together with H, to all parties through authenticated classical channels. With the information provided by the parity check bits, each Bob implements a decoding algorithm on his respective raw key, consisting of simple addition, comparison, and table look-up operations. The codes used here have been modified from MATLAB communication packages based on the DVB-S2 standards (*19*). The number of parity bits communicated during error correction (EC) is discarded to ensure security of the final conference key.

Optimal multiuser postprocessing for QCKA is still an open question. We know that CASCADE (*35*) can be more efficient than LDPC in the two-party setting for small error rates (*36*). However, as CASCADE relies on bidirectional communication, any benefits are quickly diminished by the increased communication overhead and required additional bit disclosures incurred between Alice and each Bob. In contrast, LDPC codes disclose a fixed amount of information that depends only on the largest QBER between Alice and any of the Bobs in the network. To the best of our knowledge, no proof exists for the optimal strategy to achieve the minimal bit disclosure rate when implementing error correction in multiuser QKD, and we leave this as an open question for future work.

Finite-key conference rate

When using a finite number of rounds, the estimated parameters Q_X^m and QBER from the m type-2 and type-1 rounds, are affected by statistical error which must be taken into account in the final key rate. The fractional key rate is given by

$$\frac{\ell}{L} = \frac{n}{L}\left[1 - h\left(Q_X^m + 2\xi_x\right) - h\left(\mathrm{QBER}^m + 2\xi_Z\right)\right] - \log_2\left[\frac{2(N-1)}{\epsilon_{EC}}\right]^{\frac{1}{L}} - 2\log_2\left[\frac{1 - 2(N-1)\epsilon_{PE}}{2\epsilon_{PA}}\right]^{\frac{1}{L}} - h(p) \quad (5)$$

where N is number of users in the protocol, (ξ_X, ξ_Z) are finite-key correction terms, and $(\epsilon_{EC}, \epsilon_{PE}, \epsilon_{PA})$ sets are the security parameters of our protocol (see the Supplementary Materials for further details). The $h(p)$ term in Eq. 5 is the fraction of the final key removed after privacy amplification (PA) to account for the preshared key required for marking the type-2 rounds.

SUPPLEMENTARY MATERIALS

Supplementary material for this article is available at http://advances.sciencemag.org/cgi/content/full/7/23/eabe0395/DC1

REFERENCES AND NOTES

1. K. Chen, H.-K. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states. *Quantum Inf. Comput.* **7**, 689–715 (2007).
2. M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J. D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J. B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z.-L. Yuan, H. Zbinden, A. Zeilinger, The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001 (2009).
3. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z.-L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J. B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, A. Zeilinger, Field test of quantum key distribution in the Tokyo QKD network. *Opt. Express* **19**, 10387–10409 (2011).
4. J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, A. J. Shields, Cambridge quantum network. *Npj Quantum Inf.* **5**, 101 (2019).
5. S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, R. Ursin, An entanglement-based wavelength-multiplexed quantum communication network. *Nature* **564**, 225–228 (2018).
6. H. J. Kimble, The quantum internet. *Nature* **453**, 1023–1030 (2008).
7. S. Wehner, D. Elkouss, R. Hanson, Quantum internet: A vision for the road ahead. *Science* **362**, eaam9288 (2018).
8. M. Epping, H. Kampermann, Multi-partite entanglement can speed up quantum key distribution in networks. *New J. Phys.* **19**, 093012 (2017).
9. F. Grasselli, H. Kampermann, D. Bruß, Finite-key effects in multipartite quantum key distribution protocols. *New J. Phys.* **20**, 113014 (2018).
10. Y. Fu, H.-L. Yin, T.-Y. Chen, Z.-B. Chen, Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **114**, 090501 (2015).
11. M. Epping, H. Kampermann, D. Bruß, Large-scale quantum networks based on graphs. *New J. Phys.* **18**, 053036 (2016).
12. J. Ribeiro, G. Murta, S. Wehner, Fully device-independent conference key agreement. *Phys. Rev. A* **97**, 022307 (2018).
13. M. Pivoluska, M. Huber, M. Malik, Layered quantum key distribution. *Phys. Rev. A* **97**, 032312 (2018).
14. Y. Jo, W. Son, Semi-device-independent multiparty quantum key distribution in the asymptotic limit. *OSA Continuum* **2**, 814 (2019).
15. F. Hahn, A. Pappa, J. Eisert, Quantum network routing and local complementation. *Npj Quantum Inf.* **5**, 76 (2019).

16. M. Epping, H. Kampermann, D. Bruß, Robust entanglement distribution via quantum network coding. *New J. Phys.* **18**, 103052 (2016).
17. A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, A. Zeilinger, A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Opt. Express* **15**, 15377–15386 (2007).
18. M. Proietti, M. Ringbauer, F. Graffitti, P. Barrow, A. Pickston, D. Kundys, D. Cavalcanti, L. Aolita, R. Chaves, A. Fedrizzi, Enhanced multiqubit phase estimation in noisy environments by local encoding. *Phys. Rev. Lett.* **123**, 180503 (2019).
19. A. Morello, V. Mignone, DVB-S2: The second generation standard for satellite broad-band services. *Proc. IEEE* **94**, 210–227 (2006).
20. M. Hayashi, Exponential decreasing rate of leaked information in universal random privacy amplification. *IEEE Trans. Inf. Theory* **57**, 3989–4001 (2011).
21. Y. A. Chen *et al.*, *Phys. Rev. Lett.* **95**, 1 (2005).
22. D. Markham, B. C. Sanders, Graph states for quantum secret sharing. *Phys. Rev. A* **78**, 042309 (2008).
23. F. Grasselli, H. Kampermann, D. Bruß, Conference key agreement with single-photon interference. *New J. Phys.* **21**, 123002 (2019).
24. S. Zhao, P. Zeng, W.-F. Cao, X.-Y. Xu, Y.-Z. Zhen, X. Ma, L. Li, N.-L. Liu, K. Chen, Phase-matching quantum cryptographic conferencing. *Phys. Rev. Appl.* **14**, 024010 (2020).
25. M. Tomamichel, C. C. W. Lim, N. Gisin, R. Renner, Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012).
26. T. Holz, D. Miller, H. Kampermann, D. Bruß, Comment on "Fully device-independent conference key agreement". *Phys. Rev. A* **100**, 026301 (2019).
27. J. Ribeiro, G. Murta, S. Wehner, Reply to "Comment on 'Fully device-independent conference key agreement' ". *Phys. Rev. A* **100**, 026302 (2019).
28. M. Takeoka, E. Kaur, W. Roga, M. M. Wilde, Multipartite entanglement and secret key distribution in quantum networks. arXiv:1912.10658 (2019).
29. J. Müller-Quade, R. Renner, Composability in quantum cryptography. *New J. Phys.* **11**, 085006 (2009).
30. P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, M. D. Lukin, A quantum network of clocks. *Nat. Phys.* **10**, 582–587 (2014).
31. L. Xiao, G. L. Long, F.-G. Deng, J.-W. Pan, Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A* **69**, 052307 (2004).
32. V. Kuzmin, D. Vasilyev, N. Sangouard, W. Dür, C. Muschik, Scalable repeater architectures for multi-party states. *Npj Quantum Inf.* **5**, 115 (2019).
33. M. A. Broome, M. P. Almeida, A. Fedrizzi, A. G. White, Reducing multi-photon rates in pulsed down-conversion by temporal multiplexing. *Opt. Express* **19**, 22698–22708 (2011).
34. F. Graffitti, J. Kelly-Massicotte, A. Fedrizzi, A. M. Brańczyk, Design considerations for high-purity heralded single-photon sources. *Phys. Rev. A* **98**, 053811 (2018).
35. G. Brassard, L. Salvail, *Workshop on the Theory and Application of of Cryptographic Techniques* (Springer, Berlin, Heidelberg, 1993), pp. 410–423.
36. D. Elkouss, A. Leverrier, R. Alléaume, J. J. Boutros, Efficient reconciliation protocol for discrete-variable quantum key distribution, in *2009 IEEE International Symposium on Information Theory* (IEEE, 2009), pp. 1879–1883.

Acknowledgments
Funding: This work was supported by the UK Engineering and Physical Sciences Research Council (grant numbers EP/N002962/1 and EP/T001011/1). F.G. acknowledges the financial support from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement no. 675662. M.M. acknowledges the funding from the QuantERA ERA-NET Co-fund (FWF project I3773-N36) and the UK EPSRC (EP/P024114/1).
Author contributions: A.F. and M.M. conceived the project. M.P., J.H., and P.B. performed the experiment and collected the data. J.H. and M.P. analyzed the data. F.G., M.P., and J.H. developed the theory results. All authors contributed to writing the manuscript. **Competing interests:** The authors declare that they have no competing interests. **Data and materials availability:** All data needed to evaluate the conclusions in the paper are present in the paper and/or the Supplementary Materials. Additional data related to this paper may be requested from the authors.

Submitted 28 July 2020
Accepted 19 April 2021
Published 4 June 2021
10.1126/sciadv.abe0395

Citation: M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, A. Fedrizzi, Experimental quantum conference key agreement. *Sci. Adv.* **7**, eabe0395 (2021).

Experimental quantum conference key agreement

Massimiliano Proietti, Joseph Ho, Federico Grasselli, Peter Barrow, Mehul Malik and Alessandro Fedrizzi

Sci Adv **7** (23), eabe0395.
DOI: 10.1126/sciadv.abe0395