

Scalable Network for Simultaneous Pairwise Quantum Key Distribution via Entanglement-Based Time-Bin Coding

Erik Fitzke¹,^{*} Lucas Bialowons,¹ Till Dolejsky,¹ Maximilian Tippmann¹, Oleg Nikiforov¹,
Thomas Walther^{1,*}, Felix Wissel,² and Matthias Gunkel²

¹*Institute for Applied Physics, Technische Universität Darmstadt, Schlossgartenstraße 7, 64289 Darmstadt, Germany*

²*Deutsche Telekom Technik GmbH, Heinrich-Hertz-Straße 3–7, 64295 Darmstadt, Germany*



(Received 21 December 2021; accepted 25 April 2022; published 24 May 2022)

We present a scalable star-shaped quantum-key-distribution (QKD) optical-fiber network. We use wavelength-division demultiplexing (WDM) of broadband photon pairs to establish key exchange between multiple pairs of participants simultaneously. Our QKD system is the first entanglement-based network of four participants using BBM92 time-bin coding and the first network to achieve timing synchronization solely by clock recovery based on the photon arrival times. We demonstrate simultaneous bipartite key exchange between any possible combination of participants and show that the quantum bit error rate (QBER) itself can be used to stabilize the phase in the interferometers by small temperature adjustments. The key distribution is insensitive to polarization fluctuations in the network, enabling key distribution using deployed fibers even under challenging environmental conditions. We show that our network can be readily extended to 34 participants by using a standard arrayed-waveguide grating for WDM with 100 GHz channel spacing and that reconfigurable network connections are possible with a wavelength-selective switch. In a field test, we demonstrate secure key rates of 6.3 bits/s with a QBER of 4.5% over a total fiber length of 108 km with 26.8 km of deployed fiber between two participants with high stability. Our system features a relatively simple design of the receiver modules and enables scaling QKD networks without trusted nodes to distances up to more than 100 km and to more than 100 users. With such a network, a secure communication infrastructure on a metropolitan scale can be established.

DOI: [10.1103/PRXQuantum.3.020341](https://doi.org/10.1103/PRXQuantum.3.020341)

I. INTRODUCTION

The advent of quantum computers poses a risk for classical public key cryptography [1–3]. One possible solution to this problem is quantum key distribution, which uses quantum signals to share cryptographic keys between users [4–6]. To date, a variety of QKD protocols, setups, and testing links have been implemented and the achievable key rates and distances have continuously been increased [6]. One major research direction has been to demonstrate long-distance QKD. Key exchange over hundreds of kilometers of optical fiber [7–11] as well as with satellite-based links spanning thousands of kilometers [12,13] have been demonstrated. Another focus of current research is the implementation of multiuser QKD networks often based

on trusted nodes, i.e., relay stations set up between the network users that have full knowledge of the keys.

Currently, the largest of such networks is the Chinese QKD network connecting Beijing and Shanghai via a 2000-km-long quantum backbone link that includes multiple metropolitan-area QKD networks [14]. The big drawback of this trusted-node approach is that it is not applicable in situations where the users do not trust the network provider operating the central node. Alternative approaches to setting up QKD networks not requiring trust in the central node can be realized by measurement-device-independent protocols or with entanglement-based protocols [6,15–17].

We set up a star-shaped network for simultaneous pairwise QKD between multiple participants using time-bin entangled photon pairs. From a practical point of view, our system has some advantages over other approaches to QKD networks. For example, in order to realize larger networks with prepare-and-measure two-party links based on weak coherent pulses and wavelength-division multiplexing (WDM), a wavelength-tunable sender module would be required for each participant. Our setup only

^{*}thomas.walther@physik.tu-darmstadt.de

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

requires a receiver module for each participant, which is beneficial especially when higher numbers of users are connected because it reduces the hardware complexity and cost. A star-shaped network can also be realized with measurement-device-independent (MDI) or twin-field (TF) QKD requiring additional fiber links for phase stabilization or locking of remote lasers [8,9,18,19]. In multiuser networks, the distances between users typically vary, essentially requiring the stabilization of large unbalanced Mach-Zehnder interferometers for such TF networks. In Ref. [20], a ring-shaped multiuser TF network has been realized to overcome these limitations. However, its scalability is limited in the number of participants and their distances, since it requires the signals to be sent over one single fiber link passing through the locations of all of the participants.

We employ dense wavelength-division multiplexing (DWDM) to realize QKD between multiple pairs of participants. Setups using DWDM for the distribution of polarization-entangled photons via optical fibers have been realized for photons generated by spontaneous parametric down-conversion (SPDC) in periodically poled fibers [21] or crystals [22–24]. The distribution of polarization-entangled photon pairs has been successfully implemented over submarine fibers [25,26] and has been the basis for a demonstration of a city-scale QKD network with eight users based on polarization coding [16]. QKD protocols using photon polarization require active polarization control because the birefringence in single-mode fibers can change over time, leading to large fluctuations of the initial polarization state. For fiber deployed underground, the polarization change in short fibers can be on a time scale of hours to days [27]. However, substantially faster polarization changes have been observed in urban areas [28]. In Ref. [29], polarization fluctuations and their impact on QKD systems have been systematically characterized and the required polarization tracking speed has been measured to be on the order of multiple rad/s for intercity and aerial links. Estimates show that polarization adjustments on a millisecond time scale are necessary for stable operation of a 68-km-long aerial fiber QKD link [30]. Compensation schemes for the stabilization of the polarization drift have been proposed [31–33] but considerably increase the complexity of QKD setups. Schemes readjusting the polarization based on the quantum bit error rate (QBER) can only compensate relatively slow polarization changes. Depending on the key rate, some time is required in order to accumulate sufficiently many bits so that the QBER can be reliably estimated. Hence, QBER-based polarization stabilization may become infeasible for long transmission distances with low key rates and fast polarization changes.

In contrast to polarization-based QKD, protocols using the phase and arrival time of photons to encode qubits are very robust and are independent of polarization changes. However, for phase-coding protocols, the critical parts of

the setup that need stabilization are the interferometers, which are set up in controlled environments at the photon source and the receiver stations, respectively.

Achieving stable operation is therefore independent of environmental influences on the transmission link. Thus, stable key exchange is even possible under relatively harsh environmental conditions such as urban areas, where vibrations impair the polarization stability of the transmission link.

Therefore, we implement a four-party quantum network using a time-bin protocol described in Sec. II. We achieve synchronization by clock recovery so that no separate synchronization channel is required. Our setup aligns the phases automatically and solely based on the QBER itself by tuning the interferometer temperatures. Employing a broad SPDC spectrum of a single photon-pair source and DWDM in the optical *C* band, we demonstrate simultaneous key exchange between the four participants. Scaling the network to higher numbers of participants only requires connecting more receiver modules to the source. The simple design and building method of our receiver modules aids the scalability in the number of participants. It is readily scalable to 34 network users and compatible with DWDM multiplexing schemes that have previously been used to establish QKD networks [16,24,34,35]. With only slight modifications, it can even scale up to 102 participants.

II. QKD PROTOCOL

We implement a time-bin variant of the BBM92 protocol [36,37]. In the original implementation of the protocol, a photon-pair source is placed between two participants, Alice and Bob [38]. Each participant holds a receiver module consisting of an imbalanced interferometer with two single-photon detectors, one at either output [cf. Fig. 1(a)].

The basic idea of the protocol is as follows. In the photon-pair source, pump pulses are sent through an imbalanced interferometer. The pulse duration is chosen to be shorter than the time delay, so that each pump pulse is split into a pair of noninterfering pulses. These pulses are then used to pump a nonlinear process such as SPDC or spontaneous four-wave mixing, to produce entangled photon pairs. The pulse energy is chosen such that the mean number of photon pairs per pulse $\mu \ll 1$, and therefore also the probability that a pulse generates more than one photon pair, is low.

Alice and Bob each receive one of the photons and detect it in one of three different time bins, as shown in Fig. 1(b). If the first laser pulse produces a photon pair, Alice and Bob detect their photons in the early or central time bin. Photons generated by the late laser pulse are detected in the central or late time bin. For detections in the early or late time bin, Alice and Bob note down a 0 or 1, respectively. Detections in the central time bin are noted

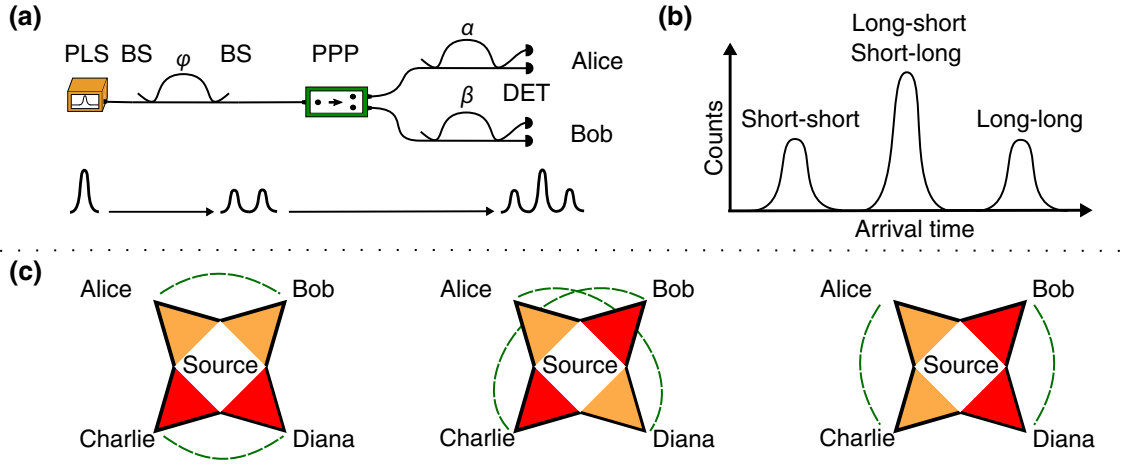


FIG. 1. (a) The scheme for time-bin entanglement quantum key distribution with the BBM92 protocol [36–38]: PLS, pulsed laser source; BS, 50:50 beam splitter; PPP, photon-pair production; DET, single-photon detector. The symbols ϕ , α , and β indicate the phase delay of the interferometers. (b) The arrival-time histogram at one of the detectors. Depending on the combination of long and short paths taken in the pump and receiver interferometers, the photons arrive in one of three time bins. Detection events in the early (short-short) and late (long-long) peak yield detections in the time basis, while events in the central peak (long-short and short-long) yield detections in the phase basis. (c) The possible configurations in a four-participant star-shaped network with pairwise mutually exclusive combinations. For one given configuration, each participant is linked to exactly one other participant, so that two connected pairs can exchange keys simultaneously and independently. The dotted green lines indicate the communication over a classical channel, which is required in addition to the unidirectional quantum channel.

down as 0 or 1 depending on which of the two detectors registers the event. When the time delays of all three interferometers are matched, two-photon Franson interference [39] leads to detection in correlated outputs for photons arriving in the central time bin.

In an ideal setup with perfectly indistinguishable interferometers, the probability for detection at two correlated outputs is given by [38,40]

$$P_{A_i B_j}(\alpha, \beta, \phi) = \frac{1}{4} (1 + (-1)^{i+j} \cos(\alpha + \beta - \phi)), \quad (1)$$

with detector labels $i, j \in \{0, 1\}$. When the phases in the interferometers of Alice (α), Bob (β), and the source (ϕ) are aligned to $\alpha + \beta - \phi = 2\pi n$ with $n \in \mathbb{Z}$, Alice and Bob will always obtain the same bit values. In this protocol, the two orthogonal bases required for QKD are the time basis consisting of measurements in the early and late time bins and the phase basis consisting of measurements of the detector number in the central time bin. In the key-sifting step, Alice and Bob announce in which basis they have measured the photon. If both have detected a photon in the same basis, they append the corresponding bit value to the key. All events measured in different bases are discarded.

The distribution of such time-bin entangled photons has been realized over 50 km [40] and 300 km [41] and QKD using this scheme has been implemented in a field test between two participants over 100 km [42]. The distribution of time- and wavelength-entangled photons with

DWDM has previously been demonstrated using photon sources based on spontaneous four-wave mixing in optical fibers [34] and silicon waveguides [43].

We extend wavelength-multiplexed entanglement distribution to a multiuser QKD network.

III. SETUP

Wavelength demultiplexing can distribute photon pairs by splitting the spectrum into different wavelength bins and sending them to more than two participants extending the key-distribution scheme to a star-shaped multiuser network with the photon-pair source at the center [Fig. 1(c)]. In our experimental setup, depicted in Fig. 2(a), we connect an arrayed-waveguide grating (AWG) for WDM to a photon-pair source to realize this network structure.

In contrast to the idealized setup shown in Fig. 1(a), we use Michelson interferometers with Faraday mirrors instead of Mach-Zehnder interferometers in order to remove the polarization dependence from our setup [cf. Fig. 2(b)] [44–46]. Therefore, our setup does not require polarization stabilization. We set up four identical receiver modules for the four participants, Alice, Bob, Charlie, and Diana, to demonstrate simultaneous pairwise key exchange. The receiver modules are connected to the AWG via fiber spools of single-mode fiber with an attenuation of around 0.22 dB/km typical for field-deployed optical fibers.

The all-fiber design makes our setup compact and robust. As pointed out earlier, phase stability of the

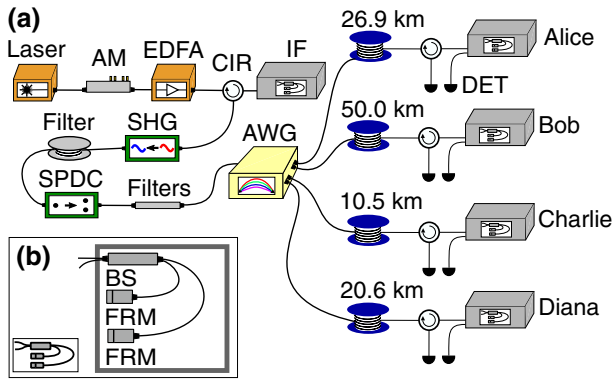


FIG. 2. (a) The setup for time-bin entanglement quantum key distribution with four participants: AM, amplitude modulator; EDFA, erbium-doped fiber amplifier; CIR, circulator; IF, interferometer; SHG, second-harmonic generation; SPDC, spontaneous parametric down-conversion; AWG, arrayed-waveguide grating; DET, single-photon detector. (b) The setup of the interferometers: BS, 50:50 beam splitter; FRM, Faraday rotator mirror. All interferometers are placed in temperature-stabilized boxes.

interferometers is critical. Our phase stabilization is based on the precise temperature control of the interferometer temperatures. Due to the high temperature stability of approximately 0.5 mK, the phase adjustment can be solely based on the estimated QBER. In the following, we briefly discuss the experimental details.

A. Photon source

Photon pairs are created in a multistage process. The primary light source is a continuous-wave laser (model Clarity, Wavelength References) frequency locked to 1550.52 nm, i.e., between channels C33 and C34 of the International Telecommunication Union (ITU) DWDM grid. A LiNbO₃ amplitude modulator (iXblue, 10 GHz) shapes pulses with a repetition rate of 219.78 MHz and a width of about 300 ps. The repetition time of 4.55 ns is chosen such that there is no overlap between the time bins that belong to two successive pump pulses (Fig. 3).

The pulses are amplified to an energy of up to 90 pJ by an in-house-built erbium-doped fiber amplifier (EDFA) and are passed through the Michelson interferometer of the source. As our QKD protocol does not require the photon-pair source to be trusted, no side channels are introduced by placing the interferometer before the second-harmonic generation (SHG). A fiber-coupled PPLN crystal (NTT Electronics) converts the wavelength to 775 nm via SHG. Tightly wound PM-780 fiber is used to filter out remaining light around 1550 nm. Two meters of such a coiled fiber result in a suppression of 79 dB and we use 5 m in our setup. A second PPLN crystal of the same type as above is used to generate energy-time entangled photon pairs in a

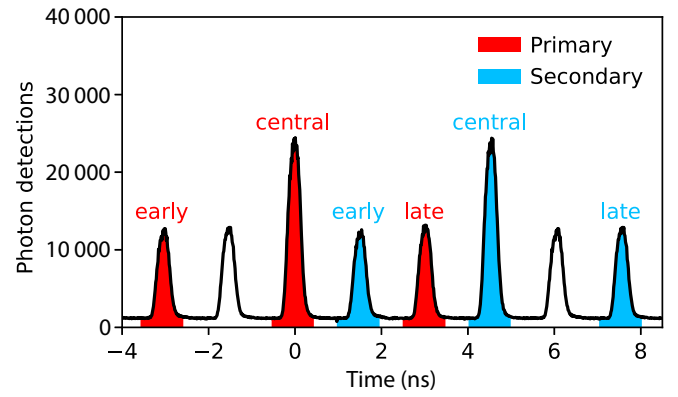


FIG. 3. The histogram of photons traveling through 10.5 km of fiber before detection at one of Charlie's detectors. The histogram shows the pulse interleaving. The structure of three peaks (early, central, and late) for each color is produced by the interferometer time delay of 3.03 ns [cf. Fig. 1(b)]. By setting the source repetition time to 4.55 ns (corresponding to 219.78 MHz), a secondary triplet of time bins (blue) is interleaved with the primary triplet (red). The data are accumulated over 90 s. Although the peaks in the detection histogram are broader than the laser pulses of the photon source due to chromatic dispersion and detector timing jitter, they are sufficiently separated to avoid overlap, so that the QBER is kept low.

type-0 SPDC process [47,48]. High-pass filters remove the remaining 775 nm-light.

In our setup, the source interferometer is placed before the SHG. In the original implementation of the protocol, the source interferometer was set up directly before the SPDC crystal, requiring a design for the second harmonic [37,38,40]. In Ref. [34,43], SFWM is used instead of SPDC, which has the advantage that components at the telecom wavelengths can also be used for the pulse generation and the pump interferometer. However, the removal of residual pump light is more complex due to the small frequency separation between the pump photons and the SFWM photons. Finally, in Ref. [41,42], rather than using an imbalanced interferometer, double pulses were produced at the telecom wavelength by employing two intensity modulators and were frequency doubled for a SPDC process. With this scheme, the separation of the electronically generated double pulses must precisely match the interferometer delays and must not show timing jitter in order to obtain a low QBER. By placing the interferometer before the SHG, we choose a different solution but combine the advantages of these setups: only readily available components for the 1550 nm wavelength range are required and the time delay can be precisely matched to the receiver interferometers, as it can be built employing identical techniques (see Sec. III B). Nevertheless, the pulsed pump-laser light can be efficiently separated from the second harmonic and, conversely, remaining 775 nm

light can be efficiently removed from the photon pairs after the SPDC crystal.

The SPDC frequency spectrum is symmetric around the center frequency with a full width at half maximum (FWHM) of approximately 9.3 THz (75 nm). After passing a C-band filter transmitting all photons within a range of ± 2.55 THz around the center frequency, the photons are distributed to the receivers by a standard telecommunication AWG with 100 GHz channel spacing.

In order to set up a key exchange between a pair of participants, their fibers are connected to a pair of AWG channels that is symmetric around the center frequency and within the pass band of the C-band filter. The number of available channels is limited by the lowest channel number of our AWG, which is C17. Therefore, 17 symmetric pairs of 100-GHz channels from C17 to C50 are available for key exchange, so that 34 participants can be connected to the network.

B. Receiver interferometers

In order to obtain low QBERs, the interferometers in the source and the receivers should be as similar as possible. Furthermore, the phase stability between the interferometers is of the utmost importance. Therefore, we pay special attention to the design of the interferometers.

The Michelson-type interferometers feature path-length differences of 3.03 ns. They consist of polarization-independent 50:50 beam splitters and Faraday rotator mirrors, eliminating the sensitivity to birefringence in the interferometer arms [44–46] and enabling two-photon interference independent of the polarization state of incoming photons. The path combinations long-short and short-long in the pump and receiver interferometers need to be almost indistinguishable in order to achieve a sufficient two-photon interference visibility. Therefore, the differences between the time delays of the interferometers must be much smaller than the coherence lengths of the photon pairs. We carefully manufactured our interferometers and monitor and correct the path-length deviations in each construction step. As we place the source interferometer before the SHG, the components of all five interferometers are identical. Thus, we were able to manufacture them all in a single attempt without resplicing. We then reduce the differences further to a few 10 μm by fiber expansion. These techniques enable the fast and precise manufacturing of the larger numbers of interferometers required to achieve scalability of our approach.

Each interferometer is enclosed by a box to shield it from environmental temperature fluctuations. The box temperature can be adjusted with thermoelectric elements driven by digitally controlled temperature controllers developed in house. The sensitivity of the interferometer phase to temperature changes is in the range of $0.033\pi/\text{mK}$

to $0.045\pi/\text{mK}$ and the box temperature can be adjusted with a precision of 0.5 mK.

Chromatic dispersion in fibers broadens the peaks in the arrival-time histogram.

If the time delay in the interferometers is chosen too small, chromatic dispersion will lead to overlapping peaks in the photon arrival-time histograms and thus to an increased QBER for transmission over long fibers. For a two-user system, the repetition rate and time-bin width can be optimized for a particular transmission distance, but for a multiuser system, the maximum distance from the source to a participant limits the maximum repetition rate. In principle, dispersion-compensation modules can be used but they increase the insertion loss. As our goal is to keep the receiver modules as simple as possible for the sake of scalability in the number of users, we opted for an implementation without dispersion compensators. Therefore, we choose a time delay of approximately 3 ns. However, a large time delay limits the pulse repetition rate. A natural choice for the repetition time of the pulse generator would be three times the interferometer time delay, resulting in equidistant peaks in the arrival-time histogram. For the fiber lengths used in this paper, the broadening from chromatic dispersion is relatively small, leaving relatively large unused gaps between the peaks in the arrival-time histogram. In order to efficiently use these gaps, we interleave consecutive repetition cycles by setting the repetition time of the pulse generator to $3/2$ of the interferometer time delay (cf. Fig. 3), thereby effectively lifting the constraint that large time delays would otherwise impose on the maximum repetition rate. To the best of our knowledge, this is the first demonstration of such an interleaving technique to increase the effective repetition rate for comparatively large interferometer time delays.

C. Data acquisition and phase calibration

We extensively automate the operation of the setup. Data acquisition is split into 90-s-long runs with approximately 6-s-long intermissions for qubit evaluation. The photons are detected by avalanche single-photon detectors (ID Quantique ID220) with a timing jitter of about 250 ps. All detectors are set to 20% quantum efficiency with a dead time of 10 μs . Time stamps are recorded by time taggers (ID Quantique ID900) with 13-ps resolution. For the experiments presented in Sec. IV, we synchronize the time taggers by sharing a 10-MHz clock signal and in Sec. V we show that synchronization can also be achieved by clock recovery from the photon arrival times.

A common time reference $t_0 = 0$ needs to be established, so that the participants can assign their detected photons correctly to the events registered by their counterpart. We establish t_0 by determining the maximum of the cross-correlation of detection events in the first run. For a key exchange between distant users, this would require a

public comparison of all photon arrival times of this run. Consequently, the data from the first run cannot be used to generate key bits. However, using the data from the first run to establish t_0 has the advantage that there is no need for a separate alignment phase. Furthermore, for our offset-alignment procedure, it is neither necessary to stop data acquisition for recalibration nor are additional components required.

Temperature changes of the link fibers can cause an arrival-time drift due to a change of the optical path lengths. Our system can automatically compensate for drifts up to 2.2 ns per run, i.e., per 90 s. The thermal sensitivity of the propagation delay in single-mode fibers around 1550 nm has been reported to be around 39 ps/(km K) [49–51]. For the maximum transmission distance of almost 77 km that we consider in Sec. IV, the system could thus compensate heating rates of more than 0.7 K per 90 s acting on the whole transmission link simultaneously. Typical temperature-change rates affecting the transmission link should be much smaller on this time scale, especially for fibers deployed underground. Note that in Sec. V, we introduce clock recovery, which also lifts this limitation.

In addition to the arrival-time calibration, the interferometer phases are automatically calibrated such that a minimal QBER is achieved. In the 6-s-long intermissions between runs, the QBER is estimated automatically every 3 min and the box temperatures are adjusted such that a minimal QBER is attained.

This whole startup takes at most 45 min due to the heat capacity of the boxes and is completed significantly faster if the interferometers are already prealigned. The box design comes with a trade-off: a high heat capacity limits the alignment speed but stabilizes the interferometer against fast temperature fluctuations. With our interferometer design, we opt for a trade-off providing both sufficient temperature stability and an acceptable alignment speed.

After the startup, key exchange can commence. The QBER is estimated automatically every 3 min in order to detect interferometer phase drifts and the interferometer temperatures are adjusted automatically in order to keep the QBER as low as possible. In the current setup, the time stamps are processed on the same computer. When the users are spatially separated, a randomly sampled fraction of the sifted key is made public to estimate the QBER for the postprocessing steps [4,6]. This QBER information can simultaneously be used to align the interferometers, so that no further security risks or information leakage results from adjusting the phases based on the QBER.

IV. RESULTS

The QBER during key exchange with our setup strongly depends on the mean number of photon pairs per pulse μ . For values of μ below 1×10^{-3} , low QBERs are expected

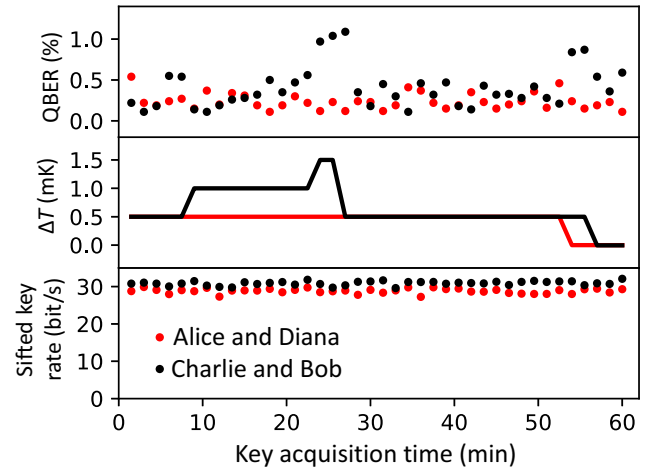


FIG. 4. A simultaneous key exchange for Alice and Diana (red) and Charlie and Bob (black) without fiber spools and with a mean photon-pair number per pulse μ below 1×10^{-3} demonstrating low QBERs. The temperature change ΔT shows adjustments made at Alice’s and Bob’s receivers to minimize the error rate. Each data point is obtained from one run of 90 s. The average QBER is 0.24% for Alice and Diana and 0.41% for Charlie and Bob, respectively.

because the emission of multiple photon pairs per pulse becomes highly unlikely. In order to assess the achievable quality of the correlations in the phase basis, measurements with an average SHG power of 0.75 μ W are performed without additional fiber spools between the source and the receivers. Figure 4 shows a 1-h-long key exchange for such low values of μ . An average QBER of 0.24% and 0.41% is reached for the combinations (i) Alice and Diana and (ii) Charlie and Bob. The QBER between Charlie and Bob shows maxima around 28 min and 55 min, which are caused by phase drifts in the respective interferometers during the measurement. However, the automatic phase calibration compensates for the drift and the QBER quickly returns to lower values. Since the QBER is a symmetric error function yielding no information regarding the direction of the phase drift, the algorithm occasionally adjusts the temperature in the wrong direction, as seen for the peak at 28 min. However, the algorithm quickly recognizes the wrong decision and corrects it automatically. Between 30 min and 50 min, no temperature adjustments are necessary for either party. Key exchange between Alice and Diana does not require any temperature adjustments for more than 50 min. The very low error rates show that the losses and time delays in the arms of our interferometers are well matched.

The reliability of our phase-stabilization algorithm is estimated in a long-term measurement over several hours of continuous operation. For these measurements, the average number of photon pairs per pulse μ created in the frequency range of one channel pair is increased to be

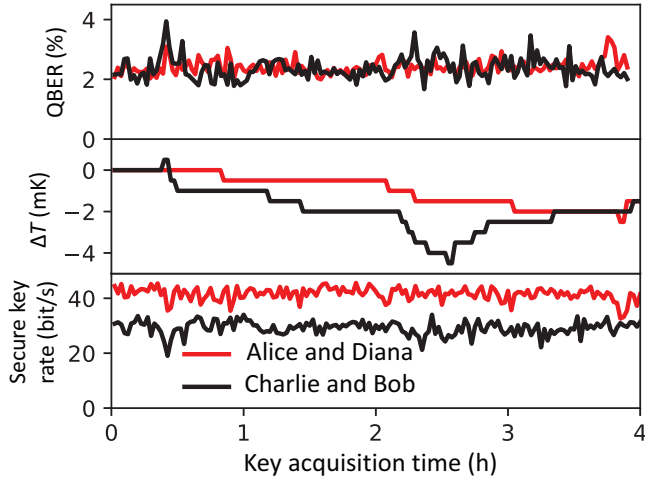


FIG. 5. The estimated secure key rates and QBERs for simultaneous key exchange over fiber spools with a total length of 47.5 km for Alice and Diana (red) and 60.5 km for Charlie and Bob (black) with a μ in the range of 0.03. ΔT denotes the temperature adjustments made at Alice's and Bob's receiver interferometers. Each data point represents one 90 s-long run.

in the range of 0.03, corresponding to an average SHG pump power of $30 \mu\text{W}$, to maximize the average secure key rate. For this mean photon number, the probability that a pulse will produce a photon pair is greatly increased. For even higher values of μ , the probability of detecting photons from different pairs due to multi-photon-pair emission becomes relevant for the QBER.

A 4-h-long key exchange between the pairs (i) Alice and Diana and (ii) Charlie and Bob with average QBERs of 2.41% and 2.36% is shown in Fig. 5. As before, the automatic phase-stabilization algorithm adjusts the interferometer temperatures such that the error rates stay at a minimum. Even though the temperature of the interferometers can be adjusted every 3 min, the error rates remain stable over much longer periods. As the QBER for each run is calculated over the duration of the run (90 s), phase fluctuations occurring during a run would increase its QBER. Similarly, slower phase drifts would lead to a trend in the QBER showing up for multiple runs. The QBER during the entire measurement stays low and neither the interferometer temperature nor the QBER show a significant drift over time, demonstrating the excellent short- and long-term phase stability of our system. If the secure key rate was to drop to zero, the key exchange would have to be paused until stable operations became possible again. However, the secure key rate in Fig. 5 never drops to zero, i.e., keys are exchanged without interruption.

The sum of the fiber lengths from the source to Alice and from the source to Diana, i.e., the effective key transmission distance, is 47.5 km and an average sifted key rate of 70 bits/s is achieved. Between Charlie and Bob, the effective distance is 60.5 km [cf. Fig. 2(a)] with a sifted key

rate of 49 bits/s. Assuming error reconciliation based on low-density parity-check codes, we estimate the secure key rates r_{sec} , which can be calculated from the sifted key rate r_{sift} , the QBER q , and the reconciliation efficiency f (cf. Ref. [52]):

$$r_{\text{sec}} = r_{\text{sift}} \left(1 - (1 + f) (-q \log_2(q) - (1 - q) \log_2(1 - q)) \right). \quad (2)$$

Using a conservative estimate for the reconciliation efficiency of $f = 1.5$ (cf. Ref. [52]), we estimate the average secure key rate as (42 ± 3) bits/s for Alice and Diana and (29 ± 3) bits/s for Charlie and Bob.

One main advantage of our system is the scalability of the photon source with respect to the number of users. In order to demonstrate that all 34 available channels are usable for key exchange, we connect the pair Charlie and Bob over a distance of 60.5 km of fiber and measure the QKD performance with each of the 17 available channel pairs (cf. Fig. 6). All channel pairs in the pass band of the C-band filter offer similar performance. Thus, with a channel spacing of 100 GHz of the AWG, we conclude that 34 participants can be connected to our source simultaneously.

In order to assess the capabilities of our system over distances typical for metropolitan quantum networks, the performance of the network is investigated by connecting the AWG and the receivers with fibers of different lengths for each participant [cf. Fig. 2(a)]. In this case, the communication between different pairs of participants is set up by reconfiguring the AWG connections and recalibrating

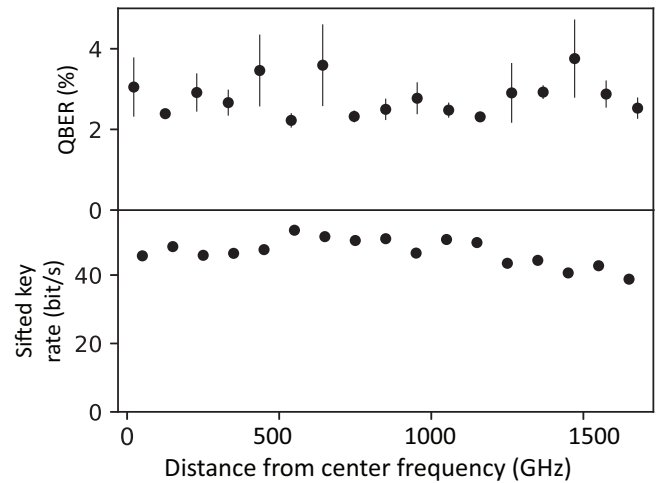


FIG. 6. The QBER and sifted key rate for key exchange between Charlie and Bob over 60.5 km of fiber for different AWG channel pairs symmetric around our center frequency. Each data point is averaged over eight consecutive 90-s runs. The error bars represent the standard deviation of the QBER for each channel. The error bars of the sifted key rate are so small that they are not visible.

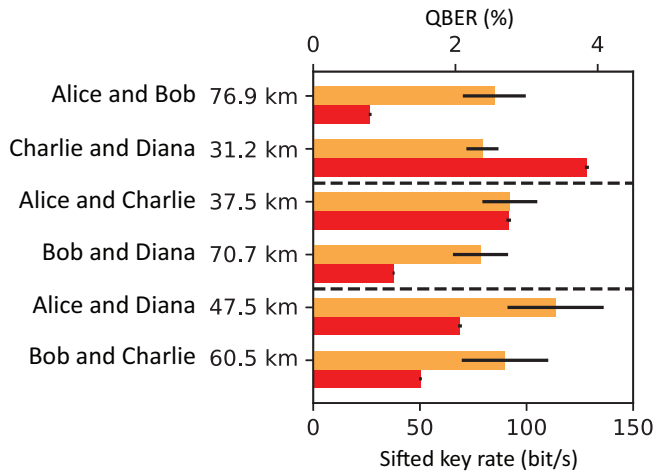


FIG. 7. The QBERs (orange) and sifted key rates (red) for all combinations of the four participants, Alice, Bob, Charlie, and Diana, over different fiber lengths. Fiber spools are assigned as shown in Fig. 2(a). The data are obtained during three 20-run measurements via simultaneous pairwise key exchange. The dashed lines separate the results of the three measurements. The error bars represent the standard deviation of the results for each combination.

the receiver interferometer phases. This is done via the same startup procedure as described above. We test all possible network configurations shown in Fig. 1(c) and demonstrate successful key exchange between all combinations of all four participants, as shown in Fig. 7. The results are obtained with the same mean photon-pair number per pulse μ for all combinations. Hence, a simultaneous key exchange over total distances between 31.2 km and 76.9 km is achieved.

V. FIELD TEST: TOWARD A DISTRIBUTED QKD NETWORK

The results presented above demonstrate the feasibility and advantages of our approach to QKD networks. In order to address typical challenges to be overcome on the way toward a real-world multiuser distributed network, first results of a field test with our system are reported in this section. The entire system is moved to a facility of Deutsche Telekom, where Alice is connected via a 26.8-km deployed dark-fiber loop running from the city of Darmstadt to Griesheim and back to Darmstadt (cf. Fig. 8). Bob, Charlie, and Diana are connected via 81.2 km, 9.6 km and 20.9 km of spooled fiber. Compared to Sec. III C, we change the operation mode of the data acquisition: a measurement is still split into 90-s-long runs but the evaluation of one run is performed while the next run is recorded without intermissions, so that the transmission time is used most efficiently for qubit exchange. We now address two further challenges on the way toward a distributed QKD

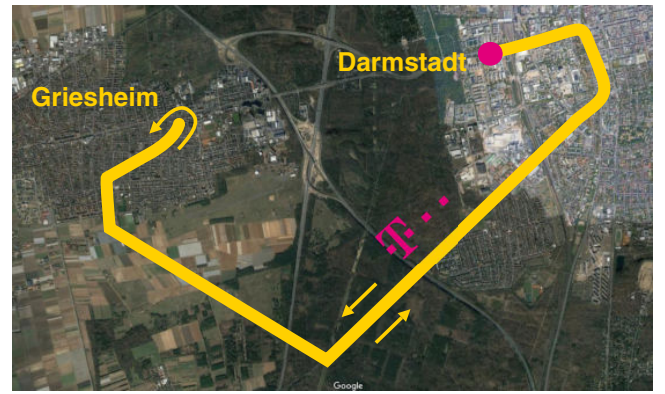


FIG. 8. The deployed standard single mode dark-fiber link of Deutsche Telekom for the field test. The link consists of a looped fiber running from the Deutsche Telekom facility in Darmstadt to Griesheim and a parallel fiber running back to Darmstadt. The fiber length is 26.8 km, with a total loss of 6.7 dB. (Google Maps 2021 ©).

network using our approach: channel reconfiguration and clock synchronization.

A. Automatic channel reconfiguration

In our setup described above, a communication with fixed channel allocations requires manual reconfiguration of the AWG when different pairs of participants want to exchange quantum keys. WDM schemes as presented in Ref. [16,24] can be used to implement fully connected networks with our setup, since they also use broadband photon sources. Moreover, in combination with active or passive time multiplexing, networks with participants grouped in fully connected subnetworks or fully connected networks can be realized [43,53]. Recently, a fully connected network with 40 users using time and wavelength multiplexing has been presented in Ref. [35].

An alternative to such schemes with a fixed channel allocation are networks employing a wavelength-selective switch (WSS) [17,54,55] for demultiplexing of the photon-pair spectrum. In contrast to an AWG, a WSS can be reconfigured electronically. This would allow us to define which parts of the spectrum are routed to which users, enabling routing and allocation of bandwidth tailored to the key demands of the participants and enabling dynamic adaption when the demands change over time. In order to show that our system can readily be used with a WSS, we replace the AWG by a WSS for the field test.

B. Synchronization by clock recovery

Another challenge is the synchronization of the clocks of the photon source and the receiver modules when they are located at distant locations. A variety of approaches exist to achieve synchronization between distant QKD modules. For example, synchronization can be achieved

via a dedicated synchronization channel. Such a channel can be implemented by employing a separate fiber or by wavelength or time multiplexing of synchronization signals with the photons used for QKD in the same fiber [56–60]. Another approach is to rely on stable local clocks and to link them to an external time reference such as the Global Positioning System (GPS) [61–63]. However, this makes the system prone to denial-of-service attacks by an attacker who has access to the reference signal. All of these approaches have the disadvantage that they require additional resources such as a dedicated classical channel or hardware such as GPS clocks, complicate the setup, or reduce the achievable key rate by using time slots that therefore cannot be used for qubit exchange.

An alternative is to perform clock recovery on the photon arrival times [64–67]. Clock synchronization between two distant stations receiving entangled photons has been demonstrated by evaluating the cross-correlation of detections [68,69]. Clock recovery based on the arrival times of nonentangled photons has been implemented and named Qubit4Sync in Ref. [64] and applied in a QKD system in Ref. [65]. Frequency recovery from photon arrival times for satellites has been investigated in Ref. [67].

In our system, the time-bin-based BBM92 protocol leads to an arrival-time distribution of the photons with the periodicity of the photon-source repetition time (cf. Fig. 3). By analyzing the photon arrival times, the clock speed of the source can be retrieved. This approach requires neither additional hardware nor the sacrifice of additional qubits for synchronization purposes.

In order to demonstrate QKD with clock recovery, we set up a separate time tagger for each participant. Diana's time tagger provides a 10-MHz clock signal to the photon source, so that the clock stability of the source is essentially that of Diana's time tagger. Alice's, Bob's, and Charlie's time taggers are not connected to any reference clock. For synchronization between the participants, we perform clock recovery on the time stamps with a self-developed algorithm. The clock recovery for each participant is completely independent and no further data exchange between the participants is required. Note that the employment of clock recovery also lifts the requirement from Sec. III C that the propagation-delay drift due to thermal expansion of the link fiber must be less than 2.2 ns per run. Drifts of the propagation delay are compensated along with clock drifts.

The reliability of the clock recovery depends on the intrinsic stability of the clocks of the receiver and the photon source. Clearly, recovering the clock reliably becomes more challenging for less stable clocks and smaller photon arrival rates. Consequently, clock recovery is most challenging for Bob because his transmission link is the longest. Due to the high losses, Bob only measures a mean count rate of around 9700 cps. For such low count rates, the clock-recovery algorithm occasionally slips by one or

multiple time bins and a sudden increase in the time-basis QBER is the consequence. Such an event is automatically detected by our algorithm and the time reference is then recalibrated by cross-correlation analysis of the current run to reestablish synchronization as it is described in Sec. III C for the initial determination of the time reference t_0 . A detailed discussion of our clock-recovery algorithm is beyond the scope of this paper and will be presented elsewhere.

For our synchronization scheme, it is neither necessary to stop data acquisition nor are additional components required. Thus, by combining clock recovery and the reference agreement on t_0 by the initial cross-correlation, the system can be operated without an additional high-accuracy timing synchronization channel.

C. Results of the field test

Measurement results of the field test, including the modified setup using the WSS, clock recovery, as well as the deployed fiber, are shown in Fig. 9. The WSS is set up so that Alice and Bob each receive a bandwidth of 50 GHz of the photon-pair spectrum while Charlie and Diana each receive 25 GHz. This choice represents a scenario in which Alice and Bob require a higher key rate and therefore obtain a wider part of the SPDC bandwidth. Note that in order to obtain mean photon-pair numbers per pulse and channel pair μ comparable to the measurements with the

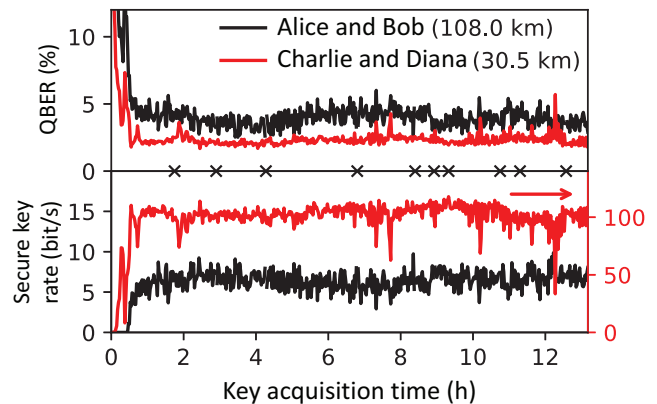


FIG. 9. The QBER and secure key rate acquired during the field test. A wavelength-selective switch is employed for demultiplexing of the SPDC spectrum. Alice is connected via the deployed fiber (26.8 km; see Fig. 8). The other participants are connected via spooled fiber: Bob via 81.2 km, Charlie via 9.6 km, and Diana via 20.9 km. The total distance between two users is the sum of the individual link lengths. Diana's time tagger is synchronized to the photon source, while for the other participants synchronization is achieved via clock recovery from the photon arrival times. Black crosses indicate runs where Bob's clock recovery fails and the delay to Alice is therefore automatically recalibrated via cross-correlation.

100 GHz AWG, we increase the SPDC pump power from $30\text{ }\mu\text{W}$ to $90\text{ }\mu\text{W}$.

It can be seen in Fig. 9 that after the startup phase of approximately 45 min, the sifted key rate and QBER are stable over hours. Disregarding the startup phase, the QBER between Alice and Bob is, at $(4.5 \pm 2.0)\%$, slightly higher than the QBER of $(2.6 \pm 1.2)\%$ between Charlie and Diana. This is a consequence of the larger channel width for Alice and Bob resulting in a higher probability of multi-photon-pair emission. A few spikes in the QBER between Charlie and Diana are visible in the second half of the measurement. They are caused by phase instabilities, which are quickly compensated for by the automatic phase-alignment algorithm. The secure key rate and standard deviation after the startup phase are (6.3 ± 1.1) bits/s between Alice and Bob and (102 ± 8) bits/s between Charlie and Diana. Over the measurement time of more than 13 h, only ten automatic recalibrations of the clock time by cross-correlation are performed between Alice and Bob and none for Charlie and Diana. This means that despite the high losses in the link to Bob, the clock-recovery algorithm slips in less than 2% of the runs, demonstrating its excellent stability.

VI. DISCUSSION AND OUTLOOK

Our QKD system proves to be able to distribute quantum keys between any two pairs of participants simultaneously without requiring a trusted node. The high stability of the QBER is reflected in the low standard deviation of the secure key rates. These results demonstrate the stability improvement of time-bin entangled protocols versus polarization-based protocols in comparable networks [16]. We attribute this increased stability to the fact that our protocol is insensitive to environmental effects impairing the polarization stability of the transmission fiber. For the same reason, we expect that our system, when used in the field with deployed fiber, can achieve a stability comparable to the performance demonstrated with fiber spools. This will enable QKD even in challenging environmental conditions, such as transmission via aerial fiber or through densely populated urban areas. In a field test with Alice connected to more than 26 km of deployed fiber and Bob connected to more than 81 km of spooled fiber, we verify that the QBER indeed exhibits excellent stability even for a total fiber length between the users of 108 km.

We demonstrate wavelength demultiplexing with an AWG and with a WSS. The WSS will enable dynamical bandwidth allocation for the participants based on the key demands in the network. We show that we can reduce the channel widths at least down to 25 GHz with the WSS and that we can route different bandwidths to different pairs of participants. We show that, as an alternative to the WSS, an arrayed-waveguide grating with 100 GHz channel spacing

can be used to connect 34 participants in 17 pairs. However, this AWG only uses a span of 3.4 THz of the SPDC spectrum.

If the full width of our C-band filter was used, QKD would be possible for ITU channels 8 to 59. Thus, up to 102 participants could be connected to our photon source for simultaneous pairwise key exchange with a suitable 50-GHz demultiplexer. AWGs with 50-GHz channel spacing are commercially available and even lower channel widths and thus greater numbers of participants would be possible with a wavelength-selective switch, given that it has sufficiently many output ports.

We demonstrate timing synchronization solely based on the evaluation of the photon cross-correlation and local clock recovery at the receivers. In order to operate the network with remote participants (Alice and Bob, for example) all they have to do is to reset the clocks of their time taggers roughly at the same time. We evaluate the cross-correlation in a range of ± 2.5 ms, which is enough to cover all optical and electronic delays between participants in our setup. However, given sufficient computing power, the cross-correlation could be evaluated in the range of seconds. Alice and Bob would then only need to agree on the starting time with a precision of milliseconds to seconds, which can be easily achieved, for example, via classical network communication and the network time protocol (NTP) [70]. Alice then sends the time stamps of all her detection events in the first run to Bob, who calculates the cross-correlation with his detected events and deduces the time shift between his clock and Alice's. The time stamps of the first block are then discarded. All clock drifts are determined locally by Alice and Bob solely based on their own detection events. High-precision clocks or synchronization signals are not required with our scheme. Especially, the classical channel is not timing critical and could instead be realized, e.g., via regular communication over the Internet.

Clock recovery is one of our measures to make the receiver modules simpler and cheaper. Due to the chosen QKD protocol itself, the modules do not comprise active components such as phase modulators or polarization controllers. All in all, due to the relatively simple design, manufacturing of higher numbers of such modules for networks with dozens of users becomes feasible.

The key rates of our setup are currently limited by the repetition rate of our source and the detection efficiency and dead time of our avalanche photodiodes. For example, commercial superconducting-nanowire single-photon detectors (SNSPD) can reach polarization-independent efficiencies greater than 70% with full recovery times around 60 ns (e.g., IDQ ID281) [71]. The use of such detectors could increase the key rate by a factor of at least 12.3, solely by improving the detection efficiency from 20% to 70%. In addition, the limit on the key rate imposed by our detector dead time of 10 μs can be overcome with SNSPDs

due to their short recovery time. An increase of the repetition rate for a constant mean photon-pair number per pulse μ will lead to an almost proportional increase of key rates when the detector dead times are short compared to the mean arrival time between photons.

The width of the time bins could be reduced further by using shorter pump pulses, dispersion compensation, and a detection setup with less jitter. Our pulse-interleaving technique (cf. Fig. 3) could then be extended by setting the repetition time of the pulse generator to $3/2^n$ times the interferometer delay without requiring any further components. It is reasonable to assume that a width of 95 ps per time bin is sufficient to accommodate short source-laser pulses and detector timing jitter when SNSPDs and fast high-precision acquisition electronics with a timing jitter as low as 25 ps [71] are used. Thus, the repetition rate could be increased by a factor of 16 to approximately 3.5 GHz by interleaving 32 pulses without overlap between time bins.

The increase in efficiency and repetition rate will result in an overall improvement of the sifted key rate by a factor of approximately 197 compared to the data presented here, i.e., sifted key rates above 9 kbits/s over a distance of 60 km of standard telecommunication fiber are feasible. While our setup in its current configuration is already suitable for communication over metropolitan-area distances, SNSPDs and higher repetition rates can conversely be used to increase the transmission distances significantly beyond the 108 km that we demonstrate.

VII. CONCLUSIONS

We present, for the first time, an all-fiber time-bin entanglement-based quantum-key-distribution system enabling simultaneous QKD between any two pairs of participants by employing WDM. Simultaneous key exchange is demonstrated over fiber lengths up to 108 km between the participants. We demonstrate the first entanglement-based QKD network to achieve synchronization between the users solely by clock recovery from the photon arrival times themselves. Our system therefore requires neither special signals or hardware for the phase alignment nor particularly stable clocks.

The QBER is automatically optimized by aligning the phases of the receiver interferometers via temperature adjustments. The receiver modules are therefore technically simple. Our precise method enables the building all five interferometers in a single attempt, which makes fast and reliable manufacturing of higher numbers of receiver modules feasible.

We obtain sifted key rates of 29 bits/s and a QBER of 2.63% over a total fiber length of 60.5 km as well as 6.3 bits/s with high stability. We also obtain a QBER of 4.5% over a total fiber length of 108 km, of which 26.8 km is field-deployed fiber.

Time- and wavelength-division-multiplexing schemes demonstrated with polarization-based entanglement protocols can be applied to our scheme as well. However, in contrast to networks using polarization encoding, our setup is unaffected by environmental disturbances deteriorating the polarization in the transmission fiber. This allows for a considerable improvement in terms of the stability of secure key rates due to the reduced QBER. These advantages of time-bin coding can be readily combined with WDM for robust metropolitan-scale networks. We demonstrate demultiplexing with a regular arrayed-waveguide grating with 100 GHz channel spacing as well as with a wavelength-selective switch, which enables us to dynamically change the user combinations and bandwidth for user pairs.

Currently, our system is readily scalable to simultaneously provide at least 34 participants in 17 pairs with keys. With suitable 50-GHz demultiplexing, the size of our network can be extended to more than 100 participants grouped in pairs solely based on wavelength demultiplexing. Even higher numbers of users or networks with subnets will become feasible when additional time multiplexing is used.

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ACKNOWLEDGMENTS

This research has been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation), under Grant No. SFB 1119—236615297. We thank Paul Wagner from Deutsche Telekom Technik GmbH for lending us the AWG and fiber spools.

-
- [1] R. A. Grimes, *Cryptography Apocalypse—Preparing for the Day When Quantum Computing Breaks Today's Crypto* (John Wiley & Sons, New York, 2019).
 - [2] D. Cheung, D. Maslov, J. Mathew, and D. K. Pradhan, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by Y. Kawano and M. Mosca (Springer, Berlin, Heidelberg, 2008), p. 96.
 - [3] E. Gerjuoy, Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers, *Am. J. Phys.* **73**, 521 (2005).
 - [4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).
 - [5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
 - [6] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).

- [7] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, *Nat. Photonics* **16**, 154 (2022).
- [8] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, *Nat. Photonics* **15**, 530 (2021).
- [9] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km, *Phys. Rev. Lett.* **124**, 070501 (2020).
- [10] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, *Nat. Photonics* **15**, 570 (2021).
- [11] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussi eres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure Quantum Key Distribution over 421 km of Optical Fiber, *Phys. Rev. Lett.* **121**, 190502 (2018).
- [12] J. Yin, *et al.*, Satellite-based entanglement distribution over 1200 km, *Science* **356**, 1140 (2017).
- [13] S.-K. Liao, *et al.*, Satellite-Relayed Intercontinental Quantum Network, *Phys. Rev. Lett.* **120**, 030501 (2018).
- [14] Y.-A. Chen, *et al.*, An integrated space-to-ground quantum communication network over 4600 kilometres, *Nature* **589**, 214 (2021).
- [15] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Measurement-device-independent quantum key distribution over untrusted metropolitan network, *Phys. Rev. X* **6**, 011024 (2016).
- [16] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lon ari , S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo,  . Samec, L. Kling, A. Qiu, M. Razavi, M. Stip evi , J. G. Rarity, and R. Ursin, A trusted node-free eight-user metropolitan quantum communication network, *Sci. Adv.* **6**, eaba0959 (2020).
- [17] M. Alshowkan, B. P. Williams, P. G. Evans, N. S. V. Rao, E. M. Simmerman, H.-H. Lu, N. B. Lingaraju, A. M. Weiner, C. E. Marvinney, Y.-Y. Pai, B. J. Lawrie, N. A. Peters, and J. M. Lukens, Reconfigurable Quantum Local Area Network over Deployed Fiber, *PRX Quantum* **2**, 040304 (2021).
- [18] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending, *Phys. Rev. Lett.* **123**, 100505 (2019).
- [19] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, *Nat. Photonics* **13**, 334 (2019).
- [20] X. Zhong, W. Wang, R. Mandil, H.-K. Lo, and L. Qian, Simple Multiuser Twin-Field Quantum Key Distribution Network, *Phys. Rev. Appl.* **17**, 014025 (2022).
- [21] E. Y. Zhu, C. Corbari, A. Gladyshev, P. G. Kazansky, H.-K. Lo, and L. Qian, Toward a reconfigurable quantum network enabled by a broadband entangled source, *J. Opt. Soc. Am. B* **36**, B1 (2019).
- [22] W. Grice, R. Bennink, D. Earl, P. Evans, T. Humble, R. Pooser, J. Schaake, and B. Williams, in *SPIE Optical Engineering + Applications*, edited by R. E. Meyers, Y. Shih, and K. S. Deacon, Vol. 8163 (SPIE, San Diego, California, 2011), p. 89.
- [23] F. Kaiser, L. A. Ngah, A. Issautier, T. Delord, D. Aktas, V. D'Auria, M. De Micheli, A. Kastberg, L. Labont , O. Alibert, A. Martin, and S. Tanzilli, Polarization entangled photon-pair source based on quantum nonlinear photonics and interferometry, *Opt. Commun.* **327**, 7 (2014).
- [24] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. H bel, and R. Ursin, An entanglement-based wavelength-multiplexed quantum communication network, *Nature* **564**, 225 (2018).
- [25] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, H. H bel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, and R. Ursin, Entanglement distribution over a 96-km-long submarine optical fiber, *Proc. Natl. Acad. Sci.* **116**, 6684 (2019).
- [26] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, B. Liu, T. Scheidl, S. M. Dobrovolskiy, R. v. D. Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, A. Zeilinger, A. Xuereb, and R. Ursin, Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre, *npj Quantum Inf.* **6**, 5 (2020).
- [27] Y. Shi, S. Moe Thar, H. S. Poh, J. A. Grieve, C. Kurtsiefer, and A. Ling, Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber, *Appl. Phys. Lett.* **117**, 124002 (2020).
- [28] K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days, *Opt. Express* **21**, 31395 (2013).
- [29] Y.-Y. Ding, H. Chen, S. Wang, D.-Y. He, Z.-Q. Yin, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Polarization variations in installed fibers and their influence on quantum key distribution systems, *Opt. Express* **25**, 27923 (2017).
- [30] R. Liu, H. Yu, J. Zan, S. Gao, L. Wang, M. Xu, J. Tao, J. Liu, Q. Chen, and Y. Zhao, Analysis of polarization fluctuation in long-distance aerial fiber for QKD system design, *Opt. Fiber Technol.* **48**, 28 (2019).
- [31] J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng, Active polarization stabilization in optical fibers suitable for quantum key distribution, *Opt. Express* **15**, 17928 (2007).
- [32] G. B. Xavier, G. V. de Faria, T. F. da Silva, G. P. Tempor o, and J. P. von der Weid, Active polarization control for quantum communication in long-distance optical fibers with shared telecom traffic, *Microw. Opt. Technol. Lett.* **53**, 2661 (2011).
- [33] D.-D. Li, S. Gao, G.-C. Li, L. Xue, L.-W. Wang, C.-B. Lu, Y. Xiang, Z.-Y. Zhao, L.-C. Yan, Z.-Y. Chen, G. Yu,

- and J.-H. Liu, Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback, *Opt. Express* **26**, 22793 (2018).
- [34] Y.-H. Li, Z.-Y. Zhou, Z.-H. Xu, L.-X. Xu, B.-S. Shi, and G.-C. Guo, Multiplexed entangled photon-pair sources for all-fiber quantum networks, *Phys. Rev. A* **94**, 043810 (2016).
- [35] X. Liu, J. Liu, R. Xue, H. Wang, H. Li, X. Feng, F. Liu, K. Cui, Z. Wang, L. You, Y. Huang, and W. Zhang, 40-user fully connected entanglement-based quantum key distribution network without trusted node, *Photonix* **3**, 2 (2022).
- [36] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography without Bell's Theorem, *Phys. Rev. Lett.* **68**, 557 (1992).
- [37] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication, *Phys. Rev. Lett.* **82**, 2594 (1999).
- [38] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Quantum Cryptography Using Entangled Photons in Energy-Time Bell States, *Phys. Rev. Lett.* **84**, 4737 (2000).
- [39] J. D. Franson, Bell Inequality for Position and Time, *Phys. Rev. Lett.* **62**, 2205 (1989).
- [40] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, Distribution of Time-Bin Entangled Qubits over 50 km of Optical Fiber, *Phys. Rev. Lett.* **93**, 180502 (2004).
- [41] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, Entanglement distribution over 300 km of fiber, *Opt. Express* **21**, 23241 (2013).
- [42] T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, and Y. Yamamoto, Long-distance entanglement-based quantum key distribution over optical fiber, *Opt. Express* **16**, 19118 (2008).
- [43] W.-T. Fang, Y.-H. Li, Z.-Y. Zhou, L.-X. Xu, G.-C. Guo, and B.-S. Shi, On-chip generation of time-and wavelength-division multiplexed multiple time-bin entanglement, *Opt. Express* **26**, 12912 (2018).
- [44] M. D. A. D. Kersey and M. J. Marrone, Polarisation-insensitive fibre optic Michelson interferometer, *Electron. Lett.* **27**, 518 (1991).
- [45] V. Secondi, F. Sciarrino, and F. De Martini, Quantum spin-flipping by the Faraday mirror, *Phys. Rev. A* **70**, 040301(R) (2004).
- [46] M. Martinelli, A universal compensator for polarization changes induced by birefringence on a retracing beam, *Opt. Commun.* **72**, 341 (1989).
- [47] O. Alibart, V. D'Auria, M. D. Micheli, F. Doutre, F. Kaiser, L. Labonté, T. Lunghi, É. Picholle, and S. Tanzilli, Quantum photonics at telecom wavelengths based on lithium niobate waveguides, *J. Opt.* **18**, 104001 (2016).
- [48] D. Aktas, B. Fedrici, F. Kaiser, T. Lunghi, L. Labonté, and S. Tanzilli, Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography, *Laser. Photon. Rev.* **10**, 451 (2016).
- [49] M. Bousonville, M. Czwalinna, M. Felber, T. Ladwig, H. Schlarb, S. Schulz, C. Sydlo, P. Kownacki, and S. Jablonski, in *Proceedings of BIW2012, Newport News, Virginia, USA* (2022).
- [50] A. H. Hartog, A. J. Conduit, and D. N. Payne, Variation of pulse delay with stress and temperature in jacketed and unjacketed optical fibres, *Opt. Quantum Electron.* **11**, 265 (1979).
- [51] R. Slavík, G. Marra, E. N. Fokoua, N. Baddela, N. V. Wheeler, M. Petrovich, F. Poletti, and D. J. Richardson, Ultralow thermal sensitivity of phase and propagation delay in hollow core optical fibres, *Sci. Rep.* **5**, 15447 (2015).
- [52] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, in *2009 IEEE International Symposium on Information Theory*, p. 1879 (IEEE, Seoul, South Korea, 2009).
- [53] X. Liu, X. Yao, R. Xue, H. Wang, H. Li, Z. Wang, L. You, X. Feng, F. Liu, K. Cui, Y. Huang, and W. Zhang, An entanglement-based quantum network based on symmetric dispersive optics quantum key distribution, *APL Photonics* **5**, 076104 (2020).
- [54] N. B. Lingaraju, H.-H. Lu, S. Seshadri, D. E. Leaird, A. M. Weiner, and J. M. Lukens, Adaptive bandwidth management for entanglement distribution in quantum networks, *Optica* **8**, 329 (2021).
- [55] F. Appas, F. Baboux, M. I. Amanti, A. Lemaître, F. Boitier, E. Diamanti, and S. Ducci, Flexible entanglement-distribution network with an AlGaAs chip for secure communications, *npj Quantum Inf.* **7**, 118 (2021).
- [56] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, C. J. Williams, E. W. Hagley, and J. Wen, Quantum key distribution with 1.25 Gbps clock synchronization, *Opt. Express* **12**, 2011 (2004).
- [57] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. ichiro Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization, *Opt. Express* **16**, 11354 (2008).
- [58] J. Williams, M. Suchara, T. Zhong, H. Qiao, R. Kettimuthu, and R. Fukumori, in *Quantum Computing, Communication, and Simulation*, edited by P. R. Hemmer and A. L. Migdall, International Society for Optics and Photonics, Vol. 11699 (SPIE, 2021), p. 16.
- [59] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, *Sci. Adv.* **3**, e1701491 (2017).
- [60] N. Walenta, *et al.*, A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing, *New J. Phys.* **16**, 013047 (2014).
- [61] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Entanglement-based quantum communication over 144 km, *Nat. Phys.* **3**, 481 (2007).
- [62] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein, and A. Zeilinger, Feasibility of 300 km quantum key distribution with entangled states, *New J. Phys.* **11**, 085002 (2009).
- [63] S. Ecker, B. Liu, J. Handsteiner, M. Fink, D. Rauch, F. Steinlechner, T. Scheidl, A. Zeilinger, and R. Ursin,

- Strategies for achieving high key rates in satellite-based QKD, [npj Quantum Inf. 7, 5 \(2021\)](#).
- [64] L. Calderaro, A. Stanco, C. Agnesi, M. Avesani, D. Dequal, P. Villorresi, and G. Vallone, Fast and Simple Qubit-Based Synchronization for Quantum Key Distribution, [Phys. Rev. Appl. 13, 054041 \(2020\)](#).
- [65] C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Foletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, and P. Villorresi, Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder, [Optica 7, 284 \(2020\)](#).
- [66] R. D. Cochran and D. J. Gauthier, Qubit-based clock synchronization for QKD systems using a Bayesian approach, [Entropy 23, 988 \(2021\)](#).
- [67] C.-Z. Wang, Y. Li, W.-Q. Cai, W.-Y. Liu, S.-K. Liao, and C.-Z. Peng, Synchronization using quantum photons for satellite-to-ground quantum key distribution, [Opt. Express 29, 29595 \(2021\)](#).
- [68] A. Valencia, G. Scarcelli, and Y. Shih, Distant clock synchronization using entangled photon pairs, [Appl. Phys. Lett. 85, 2655 \(2004\)](#).
- [69] C. Ho, A. Lamas-Linares, and C. Kurtsiefer, Clock synchronization by remote detection of correlated photon pairs, [New J. Phys. 11, 045011 \(2009\)](#).
- [70] D. Mills, Internet time synchronization: The network time protocol, [IEEE Trans. Commun. 39, 1482 \(1991\)](#).
- [71] ID Quantique SA, “ID 281 Superconducting nanowire system—Product brochure” (2021).