Realizing an Entanglement-Based Multiuser Quantum Network with Integrated Photonics

Wenjun Wen, Zhiyu Chen, Liangliang Lu, Wenhan Yan, Wenyi Xue, Peiyu Zhang, Yanqing Lu, Shining Zhu, and Xiao-song Ma[*]

National Laboratory of Solid-state Microstructures, School of Physics, College of Engineering and Applied Sciences, Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China

Quantum networks facilitate the secure transmission of information between different users. Establishing communication links among multiple users in a scalable and efficient way is important for realizing a large-scale quantum network. Here we develop an energy-time entanglement-based dense wavelength division multiplexed network based on an integrated silicon nitride microring resonator, which offers a wide frequency span (covering at least the entire C-band) and narrow bandwidth modes (~ 650 MHz). Six pairs of photons are selected to form a fully and simultaneously connected four-user quantum network. The observed quantum interference visibilities are well above the classical limits among all users. Each pair of users perform the BBM92 protocol for quantum key distribution. Our results pave the way for realizing large-scale quantum networks with integrated photonic architecture.

DOI: 10.1103/PhysRevApplied.18.024059

I. INTRODUCTION

Quantum entanglement, a counterintuitive feature of quantum physics, is the essential resource of quantum communication [1], quantum computation [2], and quantum metrology [3]. As quantum information carriers, photons have various degrees of freedom (DOFs) [4–13]. In particular, the frequency DOF of a single photon is attractive due to its compatibility with standard optical fiber infrastructure, and ability to perform routing based on optical frequencies [14]. Multiplexing the frequency DOF of photons is not only an efficient approach towards high data rates in classical communications [15] but also a promising way to provide connectivity for quantum networks (QNs) [16–20].

The development of QNs is essential for secure communication and information transfer among a larger number of users [21]. To date, QNs based on trusted relays or routing have been widely deployed [22–26], and entanglement-swapping-based quantum direct communication network have also been demonstrated [27,28]. Fully and simultaneously connected QN schemes have been proposed and realized based on entanglement distribution without relying on trusted nodes [16–19]. In these pioneering studies, each pair of users share a bipartite entanglement through carving the broadband signal/idler spectrum into a series of slices and multiplexing them. However, as the number of users increases, the need for available wavelength channels increases, which is limited by the entangled photon spectrum and thus prevents the technology from extending to a larger scale. For a scalable QN, it is necessary to include quantum memories, relying on narrow-band optical transitions. Therefore, it is also highly desirable to realize a narrow-bandwidth entangled photon pair source. Moreover, one would like to have a stable, alignment-free, high-volume production solution for such sources in practice. By leveraging advances in complementary metal-oxide-semiconductor (CMOS) fabrication techniques for classical communication, integrated quantum photonics is a promising approach. Recent progress has focused on the generation of energy-time entangled optical frequency combs within a resonator [29–32]. The discrete frequency modes generated from the resonators can easily extend the dimensionality of the system without significant overhead [9,10,33,34].

Here we realize a four-user fully connected QN by employing a Si_3N_4 microring resonator (MRR), which generates comb-like bipartite energy-time entangled states through the nonlinear process of spontaneous four-wave mixing (SFWM) [32,35–37]. There are three advantages of our scheme. First, advances in the fabrication techniques allow the dispersion to be flexibly engineered to be anomalous over a broad bandwidth, benefiting the generation of a broadband frequency comb covering S, C, and L bands with different frequency spacings matching with standard telecom filters [15,33]. Second, field enhancement offered by the MRR offers high-brightness photon pairs, reduces the pump power requirement, and directly provides

discrete narrow-linewidth spectral modes rather than filtering the photons after their generation [34,38], which reduces the photon count rate drastically. Such narrow linewidth is compatible with quantum memories, which are necessary components for realizing future scalable QNs [39]. Meanwhile, the relatively high bandgap makes the silicon nitride free of suffering two-photon absorption as compared with silicon MRR. Third, the source is chip-based, which offers stable and alignment-free operations with mature packaging technique. It is also CMOS compatible and hence is cost effective [30,40–44]. From a technological perspective, the time-bin qubit is the leading contender for fiber networks because this encoding does not suffer from random polarization rotation in fibers. By harnessing these advantages, we experimentally establish a four-user QN by employing six pairs of high-quality energy-time entangled photon pairs and distributing them between all users. Each user analyzes and decodes the time-bin qubits with a Franson interferometer.

II. EXPERIMENTAL SETUP AND SOURCE CHARACTERIZATION

As shown in Fig. 1, our setup includes four parts: photon-pair source, wavelength allocation, entanglement analysis, and quantum key distribution. In the source part [Fig. 1(a)], a single-mode fiber-coupled continuous wave (CW) laser (Santec TSL-770) at 1549.32 nm pumps the

MRR source. We use a fiber polarization controller to adjust the pump polarization and pump cleaning filters to remove unwanted spectral noise before injecting the pump light into the MRR. The MRR has a diameter of 460 μm, as shown in Fig. 1(b). The MRR is evanescently coupled to a single-bus waveguide via a 300 nm gap point coupler. Both the ring and waveguide have a cross-section of 1600 nm wide and 800 nm high. Light is coupled into and out from the chip by lens tapered fibers which is mounted on high-precision positioning mounts. The total insertion loss (for nonresonant frequency) of the chip is about 5 dB, including both input-output coupling loss and the propagation loss in the bus waveguide.

Frequency-correlated photons are generated from the integrated nonlinear MRR. The broadband phase matching SFWM enabled by anomalous dispersion of our device, combined with the cavity resonances, leads to the generation of a correlated signal and idler photon pairs that are symmetrically distributed to the pump laser. The spectra of the entangled photon pairs cover multiple resonances, and yield a frequency comb structure with a spacing given by the free spectral range (FSR) of the MRR. The photons are coupled out from the chip and are filtered by cascade filters. Then they are allocated to users to form a fully and simultaneously connected network by an array waveguide grating (AWG) and multiple dense wavelength division multiplexing (DWDM) filters with 100 GHz spacing [Fig. 1(c)]. We select six pairs of entangled
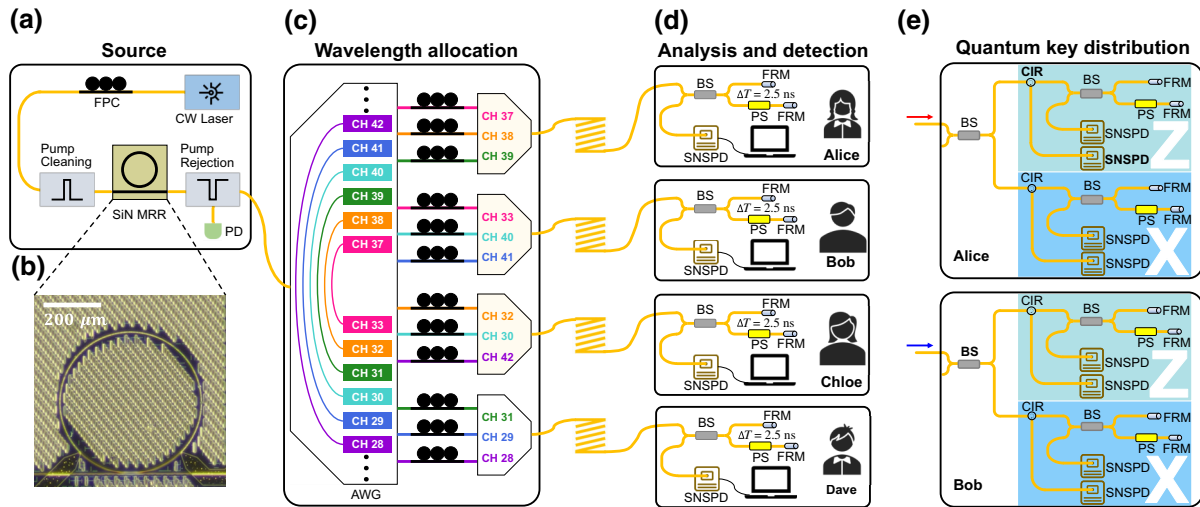

FIG. 1. (a) Photon-pair source. A continuous wave laser at 1549.32 nm is filtered, polarized, and coupled into the Si_3N_4 microring resonator (MRR) to generate frequency-correlated photon pairs. At the output, the pump laser is rejected by a set of filters and measured by a power detector to monitor the source alignment. (b) Optical microscopy image of the Si_3N_4 MRR. (c) Wavelength allocation. Six bipartite states are selected to create a fully connected network between four users. (d) Each user is equipped with a Franson interferometer ($\Delta T = 2.5$ ns, time difference between two arms) and a superconducting single-photon detector to characterize the state. (e) The measurement setup for quantum key distribution using BBM92 protocol. For obtaining the secure keys, Alice/Bob split her/his photons with a 50:50 beam splitter and use two Franson interferometers with the phase settings corresponding to mutually unbiased bases Z and X, respectively. Abbreviations of components: CW, continuous wave; FPC, fiber polarization controller; MRR, microring resonator; PD, power detector; AWG, arrayed waveguide grating; BS, beam splitter; FRM, Faraday rotation mirror; PS, phase shifter; CIR, circulator; SNSPD, superconducting nanowire single-photon detector.
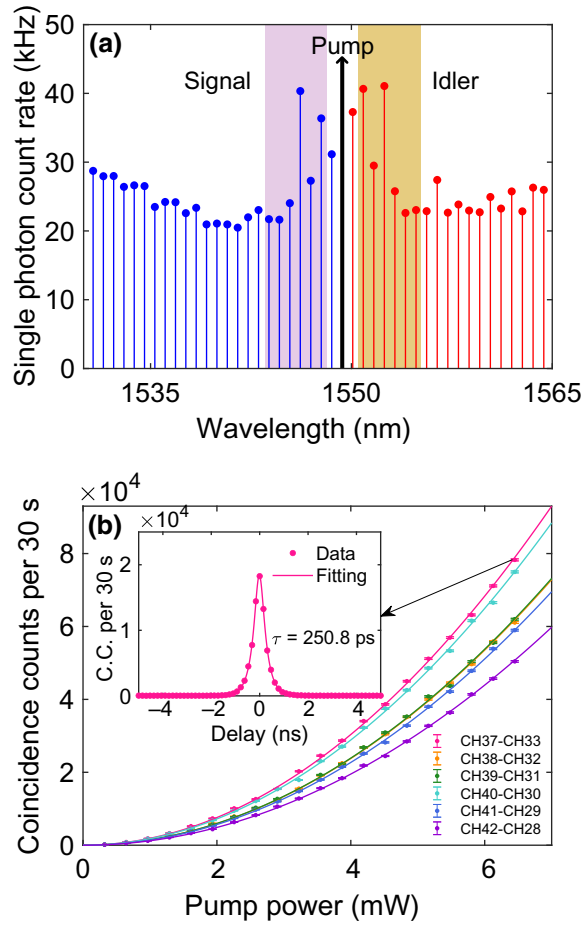
FIG. 2. (a) Experimental single-photon spectrum as a function of the wavelength with the on-chip pump power of 5 mW. The channels used in the network are indicated in shades. (b) Coincidence counts as a function of pump power for six photon pairs of different frequencies with a coincidence window of 2.5 ns. Solid lines are quadratic fits. Error bars are calculated by Poissonian distribution and are smaller than the symbol size. The inset is a typical histogram of coincidence measurements with the time-bin size of 156.25 ps, which shows the coherence time of the single photons τ_c of 250.8 ps.
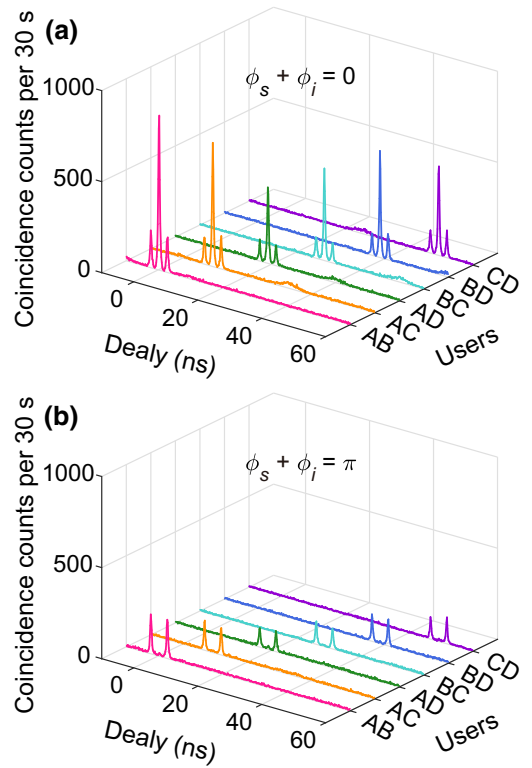
FIG. 3. Coincidences histogram for each two-party link measured at the output of the interferometers for two different phase settings. Each pair of users identify photon pairs by different delays.

photons with wavelengths aligned with the International Telecommunication Union's (ITU) grids. These six pairs of photons are then distributed to four users: Alice (A), Bob (B), Chloe (C), and Dave (D). Each user receives three channels/wavelengths and shares an entanglement state with every other user in the network. The analysis and detection module held by every user consists of a Franson interferometer [45] with a time difference between two arms of $\Delta T = 2.5$ ns, and a superconducting nanowire single-photon detector (SNSPD, Quantum Opus). All interferometers are composed of fiber optic components and are buried in quartz sand and wrapped in thick insulation to mitigate the phase shifts caused by room temperature changes. As shown in Fig. 1(d), the generated photons can either take a short (S) or a

long (L) path in the interferometer. We select the case when both photons take the same path, which gives the bipartite entangled state $|\psi\rangle = 1/\sqrt{2}\left(|SS\rangle + e^{\phi_s + \phi_i}|LL\rangle\right)$ shared between each user [27,46], where ϕ_s (ϕ_i) is the phase of the signal (idler) set by the phase shifter.

The MRR under test has an average Q factor of 3.1×10^5 and an average FSR of 97.8 GHz. The full width at half maximum (FWHM) of the resonance mode near the pump wavelength is 5.2 pm (649 MHz). In Fig. 2(a), we show the spectrum of the single photons emitted from the MRR and then measured with a reconfigurable optical processor (Finisar waveshaper 16000S-CB, not shown in the setup) and a SNSPD. Owing to the low anomalous dispersion of the MRR, we obtain the single-photon spectrum covering the entire C-band (only limited by our measurement spectrometer, not the comb itself). Figure 2(b) illustrates the dependence of coincidences on pump power for all six photon pairs with a coincidence window of 2.5 ns measured directly from the output of the AWG. The generated rate of photon pairs shows a quadratic behavior with increasing pump power, which confirms the correlated photons are generated from the SFWM process. An instance of a histogram of the channel pairs (ITU CH37 and CH33) at the input pump power of 6.45 mW is shown in the inset measured by a time-tagger unit
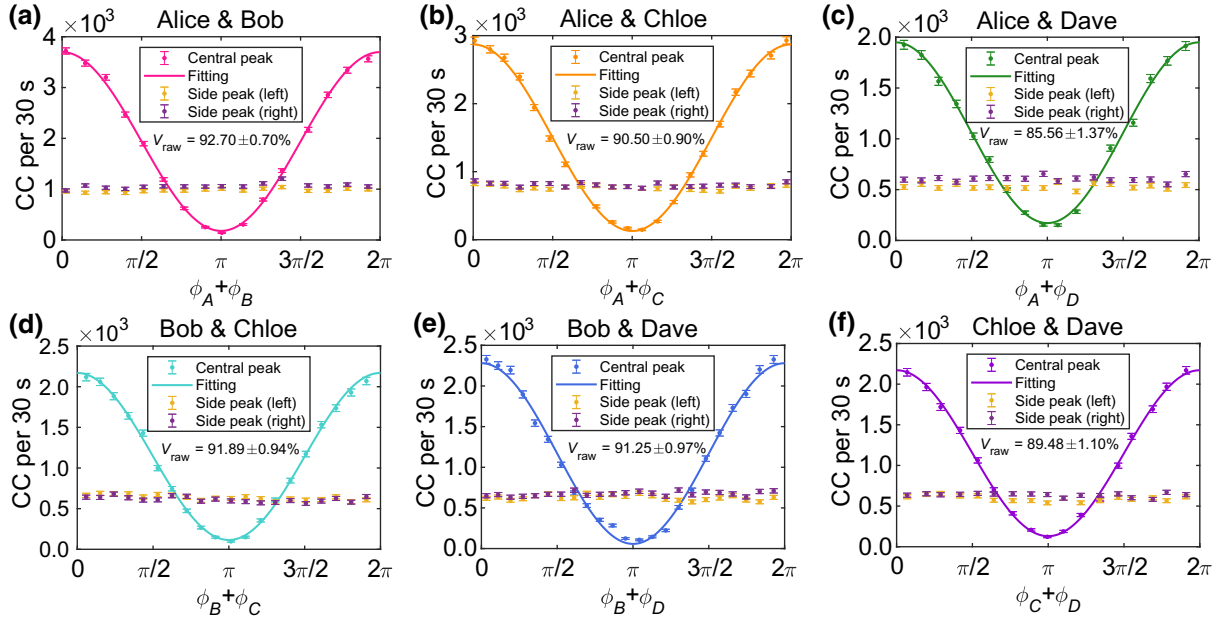
FIG. 4. (a)–(f) Coincidence counts (CC) of the central and side peaks in 30 s as a function of the phase $\phi_s + \phi_i$ for six combinations among four users. All coincidence windows are 2.5 ns. The solid curves are fits of the experimental data of the central peak. Experimentally we scan the phase of the signal while keeping the idler's phase without active tuning.

(UQDevices Logic-16) with the temporal resolution of 156.25 ps. The peak represents the time correlation of the signal-idler pairs and a high coincidence-to-noise ratio (CAR, $\sim$ 88). Following the fitting method used in [29,47], the results show that the coherence time of the single photons is $\tau_c = 250.8$ ps and, hence, the bandwidth is $\Delta \nu = 1/(2\pi\tau_c) = 634.7$ MHz (consistent with the resonance linewidth of the MRR), and the time jitter of the detection system (including SNSPD and time-tagger unit) is $\sigma = 138.3$ ps. The pair generation rate (PGR) can be calculated by PGR $= S_s S_i / R_c$, where S_s (S_i) is the single counts of the signal (idler) due to SFWM, and R_c is the coincidence count. After dividing by their respective bandwidth, the PGRs show a minimum of 11.2 s^{-1} mW^{-2} MHz^{-1}, a maximum of 15.3 s^{-1} mW^{-2} MHz^{-1}, and an average of 12.9 s^{-1} mW^{-2} MHz^{-1}. The details of the characterization are shown in Appendix A, and the results show that our source has the advantages of large spectral range, narrow linewidth of comb lines, high CAR, and high PGR, showing potential for applications in multiuser QNs and interfacing solid-state quantum memories at telecommunication wavelengths [48].

III. RESULTS

Each user receives three frequency modes, corresponding to three communication channels with the other three users in the four-user network. One way to distinguish the channel is to implement frequency-resolved detection at each user's detection module, which will drastically

increase the complexity of the setup for each user. Instead, we employ the method used in ref [16] by harnessing the temporal DOF. We add different optical fiber delays for each wavelength channel between wavelength demultiplexing and wavelength remultiplexing, i.e., directly behind the first AWG shown in Fig. 1(c). By doing so, we can identify different combinations of users by the relative arrival times of respective photons.

To verify the feasibility of the network, we measure the two-photon coincidences for two representative phase settings as shown in Fig. 3, i.e., $\phi_s + \phi_i = 0$ in Fig. 3(a) and $\phi_s + \phi_i = \pi$ in Fig. 3(b). Each coincidence histogram has three peaks, revealing three relative arrival times due to the intrinsic nature of the Franson interferometer [45]. The middle peak corresponds to the indistinguishable event, in which both photons travel along the long or the short paths. For this reason, the coincidences of central peaks vary remarkably between close to zero count ($\phi_s + \phi_i = \pi$) and close to four times the side peaks ($\phi_s + \phi_i = 0$), whereas the side peaks have heights that are independent of phase. The time difference between the two arms of the Franson interferometer ($\Delta T = 2.5$ ns) is larger than the coherence time of the generated photons ($\tau_c \sim 250$ ps), and much smaller than the coherence time of the CW pump laser ($\tau_p \sim 2.7$ μs for a typical linewidth ~ 60 kHz), which guarantees high interference visibility and, thus, high purity of energy-time entanglement.

Further, we measure the two-photon interference fringes by post-selecting each peak with a coincidence window of 2.5 ns. The results are shown in Figs. 4(a)–4(f) as a
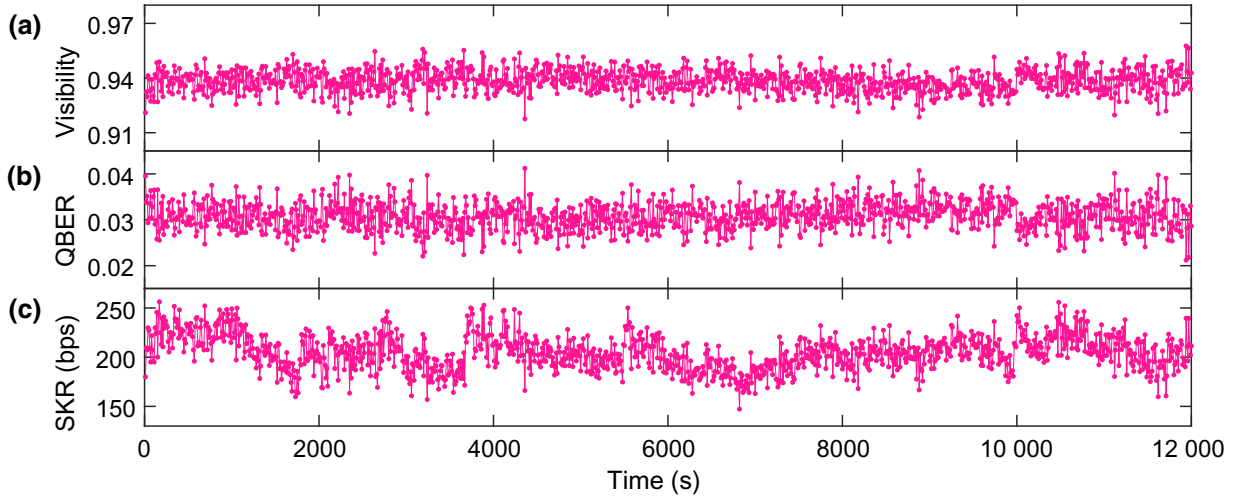
FIG. 5. (a) Visibility, (b) quantum bit error rate (QBER), and (c) secure key rate (SKR) over time for Alice and Bob. Each data point stands for a 10 s average value.

function of the phase $\phi_s + \phi_i$ for both central and side peaks in the coincidence histograms. One can clearly see that the central peak oscillates sinusoidally with the phase, and no interference can be observed for the side peaks. The fitting results show that all the raw visibilities are above 0.856, which are greater than the classical bound (~ 0.707), required for the violation of the Clauser–Horne–Shimony–Holt (CHSH) form of the Bell's inequality [49]. The detected brightness (including all the insertion losses of all components), is defined as detected photon pairs rate per squared milliwatt per megahertz. In our work, the average detected brightness for all user pairs is 0.52×10^{-2} s^{-1} mW^{-2} MHz^{-1}, with a minimum of 0.40×10^{-2} s^{-1} mW^{-2} MHz^{-1} and a maximum of 0.78×10^{-2} s^{-1} mW^{-2} MHz^{-1}, and details can be found in Appendix B.

We use the BBM92 protocol [50] to establish the keys between Alice and Bob. In Fig. 1(e), we show the measurement setup. Alice/Bob splits their photons with a 50:50 beam splitter, which performs the random choice of measurement basis between Z ($0/\pi$) and X ($\pi/2$ / $3\pi/2$). An additional circulator is added at the input of each interferometer to obtain two-port data from each interferometer. All eight outputs are monitored with SNSPDs. For the long-term operation of the whole setup, we have made some experimental technical efforts as described in Appendix D. For example, we use feedback control to move the pump wavelength to follow the resonance drift of the MRR resonance due to the thermal instability of the laboratory, which makes the resonance stable for more than 20 h. Figure 5 shows the quantum key distribution data between Alice and Bob in 12 000 s, which are measured between CH33 and 37 directly from the outputs of AWG. In Fig. 5(a), we show the entanglement visibility and obtain an average value of $93.84 \pm 0.61\%$. The

average quantum bit error rate (QBER) is $3.08 \pm 0.30\%$, as shown in Fig. 5(b), which is calculated by QBER = $(1 - Visibility)/2$ [1]. The secure key rate (SKR) is calculate using SKR $\geq n_{\text{sift}} \left[1 - f\left(\delta_b\right) H_2\left(\delta_b\right) - H_2\left(\delta_p\right) \right]$ [51,52], where n_{sift} is the sifted key rate, $\delta_b(\delta_p)$ the bit (phase) error rate, $f(x)$ is the error correction efficiency as a function of error rate (here we set $f(x) = 1.2$), and $H_2(x)$ is the binary entropy function: $H_2(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$. Due to the symmetry of X- and Z-basis measurements, $\delta_b = \delta_p = E_\lambda$, where E_λ is the overall QBER. Within an integration time of 12 000 s, we obtain a total security key of 2.46×10^6 bits. This corresponds to an average SKR of 205 bits/s, as shown in Fig. 5(c). We have measured the quantum key distribution in 2000 s with all six pairs of entangled photons and present the data in Appendix C.

IV. CONCLUSION

In conclusion, we generate comb-like bipartite energy-time entangled states in a chip-integrated Si$_3$N$_4$ MRR, and experimentally demonstrated a fully connected four-user tabletop QN by multiplexing 12 DWDM channels such that correlation exists between every possible two-party link. The broadband and comb-like spectrum combined with considerable brightness, make the Si$_3$N$_4$ entangled source highly promising for large-scale, wavelength-multiplexed, fully connected QNs and flexible to interface to other integrated quantum photonics applications.

Based on our measured single-photon spectrum, a total of 44 wavelength channels can be used to build a fully connected quantum communication network with at least 7 users. To further expand the scale of network users requires more wavelength channels and the use of optical splitters or other optical components. In addition, with the recent
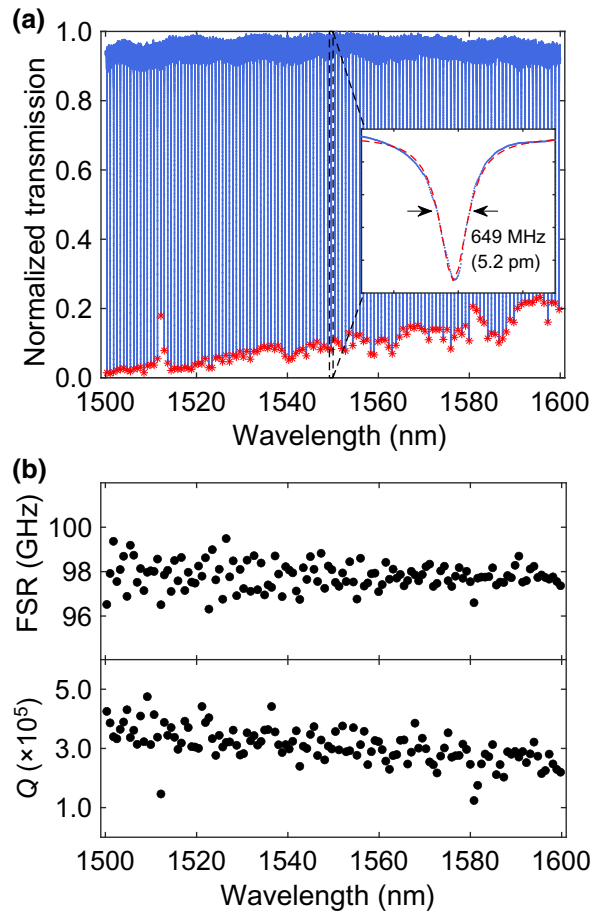
FIG. 6. Characterization of the MRR with laser. (a) The measured cavity transmission spectrum ranging from 1500 to 1600 nm. The inset shows the resonance spectra near the pump. (b) The free spectral range (FSR) and estimated quality (Q) factor of the resonator.
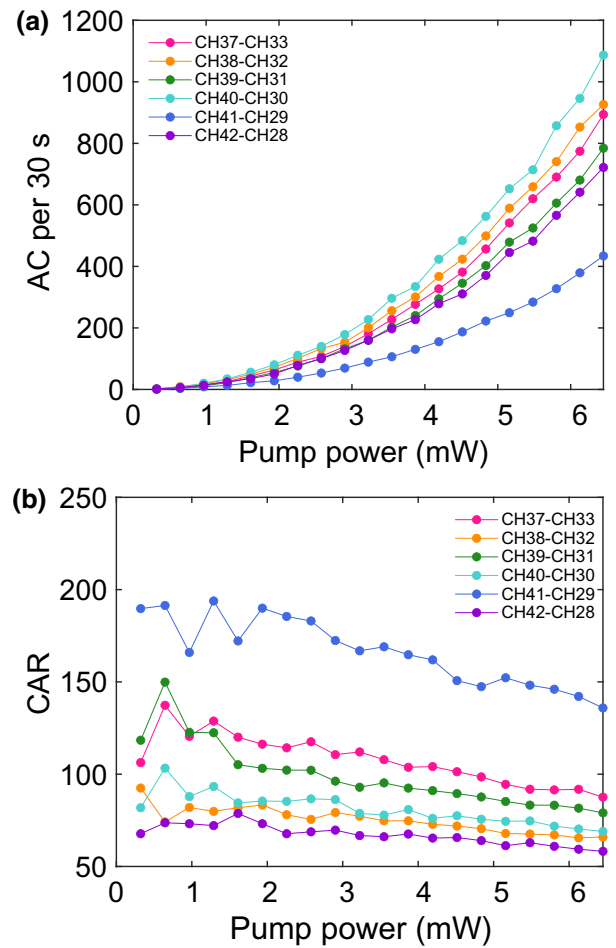

FIG. 7. (a) Accidental coincidences (AC) and (b) coincidence to accident ratio (CAR) as a function of the injected pump power for all six selected photon pairs.

advancements of SiN fabrication technology, it is possible to integrate wavelength demultiplexing/multiplexing module onto the same chip of the source, which will largely reduce the complexity and the optical connection losses of the off-chip, individual optical components. This work paves the way for providing a turn-key solution of the large-scale entanglement-based QN.

APPENDIX A: CHARACTERIZATION OF MICRORING RESONATORS

To characterize the MRR, we measure the transmission spectrum ranging from 1500 to 1600 nm, as shown in Fig. 6(a).

The inset shows an enlarged view of a resonant mode around the pump wavelength (CH35) with a FWHM of 5.2 pm, or 649 MHz. Figure 6(b) shows the FSR and the quality factors (Q) of each resonant mode. We obtain 128 cavity resonance modes and the averaged FSR is 97.8 GHz, which is sufficiently close to the standard 100 GHz DWDM filters and offers a plentiful selection of possible photon pairs at telecom-band. The averaged measured Q factor is about 3.1×10^5.

Then we characterized the photon pair generated from the MRR. The coincidence counts (CC) in Fig. 2(b) is obtained by taking a window with a center at zero relative delay and a width of 2.5 ns from the histogram of coincidence counts (such as the histogram shown in the inset of Fig. 2(b) with a temporal resolution of 156.25 ps), and

TABLE I. The coherence time of the single photons, bandwidth, pair generation rate (PGR), calculated loss and calculated time jitter of all six selected photon pairs without interferometers and partial WDM network.

Channel pairs	Coherence time (ps)	Bandwidth (MHz)	PGR (s^{-1} mW^{-2})	PGR (s^{-1} mW^{-2} MHz^{-1})	Loss (dB)	Jitter (ps)
CH37-CH33	250.8	634.7	7.22×10^3	11.4	−10.29	138.3
CH38-CH32	234.4	678.9	8.70×10^3	12.8	−11.22	133.9
CH39-CH31	245.0	649.7	7.27×10^3	11.2	−10.82	136.4
CH40-CH30	254.6	625.2	9.55×10^3	15.3	−11.00	127.0
CH41-CH29	242.2	657.1	7.92×10^3	12.1	−11.12	139.8
CH42-CH28	244.6	650.7	9.51×10^3	14.6	−11.85	128.1

summing all the counts in this window. Accidental coincidences (AC) is the average of the counts in all other 2.5 ns windows except the previous one in the histogram. Coincidence-to-accidental ratio (CAR) is defined as CC divided by AC. Figure 7 shows the AC and CAR as a function of injected pump power. At low pump power, the CAR is mainly limited by the dark count of the detector. As the pump power increases, the multipair generation increases, which leads to a reduction in the CAR. Taking the pair of channels CH37 and CH33 as an example, we obtain a maximum CAR of 137 when the pump power is 0.64 mW, and the CAR is 95 when the pump power is 5 mW.

The measured coincidence count curve is the convolution of the signal/idler temporal correlation function $g_{s,i}^{(2)}(t)$ and the response function of the whole detection system $h(t)$ [47]. The signal/idler temporal cross-correlation function is given as $g_{s,i}^{(2)}(\Delta t) \propto 1/\tau_c \exp(-|\Delta t|/\tau_c)$ [29], and the response of the whole detection system can be modeled using a Gaussian function $h(\Delta t) \propto \exp\left(-(\Delta t)^2/\sigma^2\right)$ [47]. Here Δt is the time delay, τ_c is the coherence time of the single photons and σ is the time jitter of the detection system (including SNSPD and time-tagger unit). In Fig. 8, we compare the fitting results without (a) and with (b) considering the broadening due to the jitter of the detection system. After considering the time jitter, we obtained an average coherence time of 245.2 ps and an average bandwidth of 649.4 MHz, which is in good agreement with the linewidth of the MRR. Detailed data of all six pairs of photons are listed in Table I.

The PGR can be calculated by $\text{PGR} = S_s S_i / R_c$, and the loss can be derived by $\text{Loss} = R_c / \sqrt{S_s S_i}$, where S_s (S_i) is the single counts of signal (idler) due to SFWM, and R_c is the coincidence count. It can be found that the calculated PGR is different for different channel pairs, which may come from the nonideal dispersion engineering and high-order mode-crossing [53] of MRR. This can also be seen in the transmission spectrum of MRR with nonuniform extinction ratio in Fig. 6(a). We estimate an average PGR for each pair of photons to be 8.3×10^3 s^{-1} mW^{-2} (ranging from 7.22×10^3 s^{-1} mW^{-2} to 9.55×10^3 s^{-1} mW^{-2} for different pairs), or 12.9 s^{-1} mW^{-2} MHz^{-1} (ranging

from 11.2 s^{-1} mW^{-2} MHz^{-1} to 15.3 s^{-1} mW^{-2} MHz^{-1} for different pairs) after dividing by the bandwidth, as listed in the Table I. The PGR of different channel pairs together
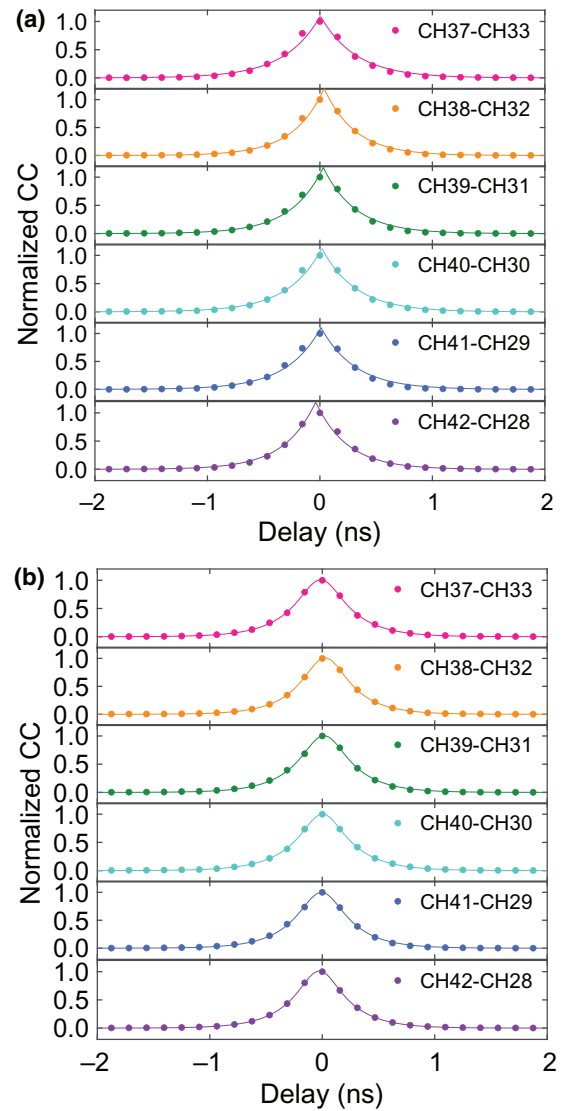
FIG. 8. Comparison of the fitting results of using (a) $\frac{A}{\tau_c} \exp\left(-\frac{|\Delta t|}{\tau_c}\right)$ and (b) $\frac{A}{\tau_c} \exp\left(-\frac{|\Delta t|}{\tau_c}\right) * \exp\left(-\frac{(\Delta t)^2}{\sigma^2}\right)$.
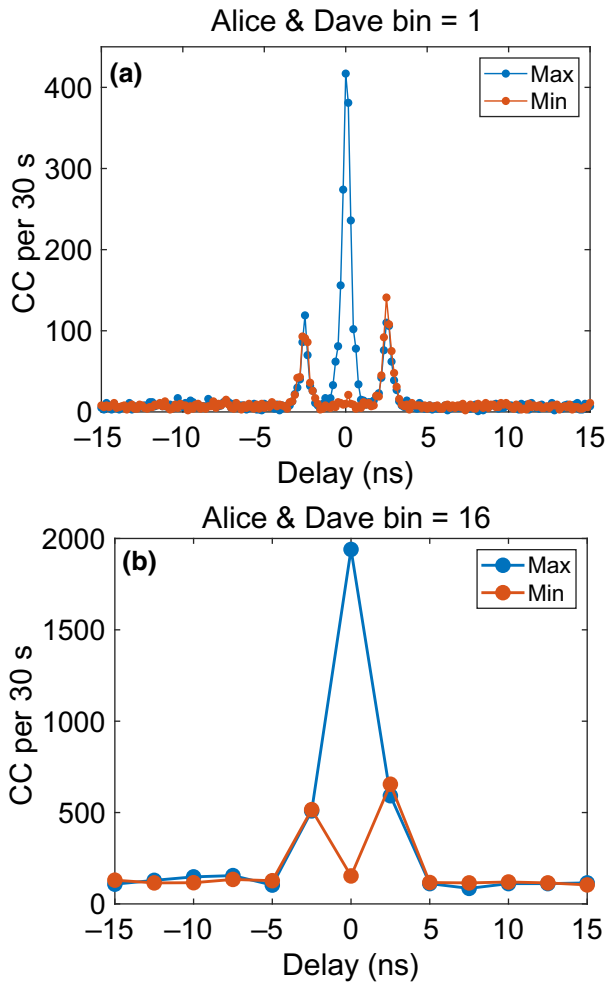
FIG. 9. The coincidence histograms of the maximum (blue) and minimum (orange) points of the interference curve between Alice and Dave, with the time-bin size of (a) is 0.15625 ns, and the time-bin size of (b) is 2.5 ns.

with the different insertion loss of different wavelength channels, resulting in the different coincidence counts of the six channel pairs show in Fig. 2(b).
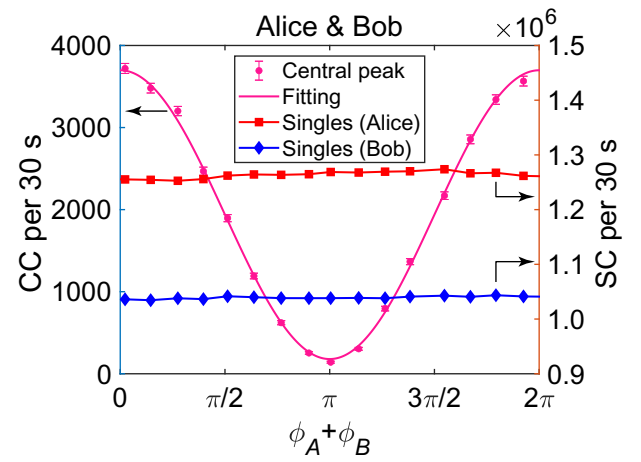

FIG. 10. Coincidence count of the central peak and single count of the output of each interferometer as a function of the phase $\phi_s + \phi_i$ for Alice and Bob.

APPENDIX B: RESULTS OF ENTANGLEMENT DISTRIBUTION FOR SIX PAIRS OF USERS

In order to conveniently determine the phase $\phi_s + \phi_i$, the two-photon interference fringes shown in Figs. 4(a)–4(f) is measured by keep the idler's phase zero while tuning the phase of the signal. The results show that the visibility (calculated from raw data) of different user pairs varies from $85.56 \pm 1.37\%$ (Alice-Dave) to $92.70 \pm 0.70\%$ (Alice-Bob). We tested the total loss from chip to SNSPD for each wavelength channel with classical laser and power meter, and the results showed that the higher the total loss of signal and idler, the lower the interference visibility between the corresponding user pairs. Note that each user received three wavelength channels and shared one and only one pair of correlated photons with any other user, and coincidences between uncorrelated photons contributes to the accidental coincidences. After subtracting the measured accidental coincidence, the net visibilities are found to be varies from $96.70 \pm 0.65\%$ to $99.83 \pm 0.13\%$, as listed in Table II.

TABLE II. The brightness detected between users, the total loss of different wavelength channels, and the corresponding raw (net) visibilities without (with) subtraction of accidental coincidences.

User	ITU Channels	Detected Brightness (s^{-1} mW^{-2} MHz^{-1})	Total Loss (dB) Signal	Idler	Visibility Raw	Net
Alice & Bob	CH37-CH33	0.78×10^{-2}	-14.29	-13.20	$92.70 \pm 0.70\%$	$99.53 \pm 0.17\%$
Alice & Chloe	CH38-CH32	0.58×10^{-2}	-14.90	-13.12	$90.50 \pm 0.90\%$	$97.67 \pm 0.44\%$
Alice & Dave	CH39-CH31	0.40×10^{-2}	-15.27	-15.30	$85.56 \pm 1.37\%$	$96.70 \pm 0.65\%$
Bob & Chloe	CH40-CH30	0.46×10^{-2}	-14.03	-14.01	$91.89 \pm 0.94\%$	$99.83 \pm 0.13\%$
Bob & Dave	CH41-CH29	0.47×10^{-2}	-13.86	-14.67	$91.25 \pm 0.97\%$	$98.93 \pm 0.32\%$
Chloe & Dave	CH42-CH27	0.44×10^{-2}	-14.29	-14.56	$89.48 \pm 1.10\%$	$96.87 \pm 0.59\%$

FIG. 12. The measurement setup for quantum key distribution using BBM92 protocol with PID module included. Here Z and X represent two sets of measurement bases Z ($0 / \pi$) and X ($\frac{\pi}{2} / \frac{3\pi}{2}$). The black arrows represent the direction of the reference light, and the red arrows represent the direction of the signal/idler. Abbreviations of components: BS, beam splitter; PD, power detector; PS, phase shifter; CIR, circulator; WDM, wavelength division multiplexer; SNSPD, superconducting nanowire single-photon detector.
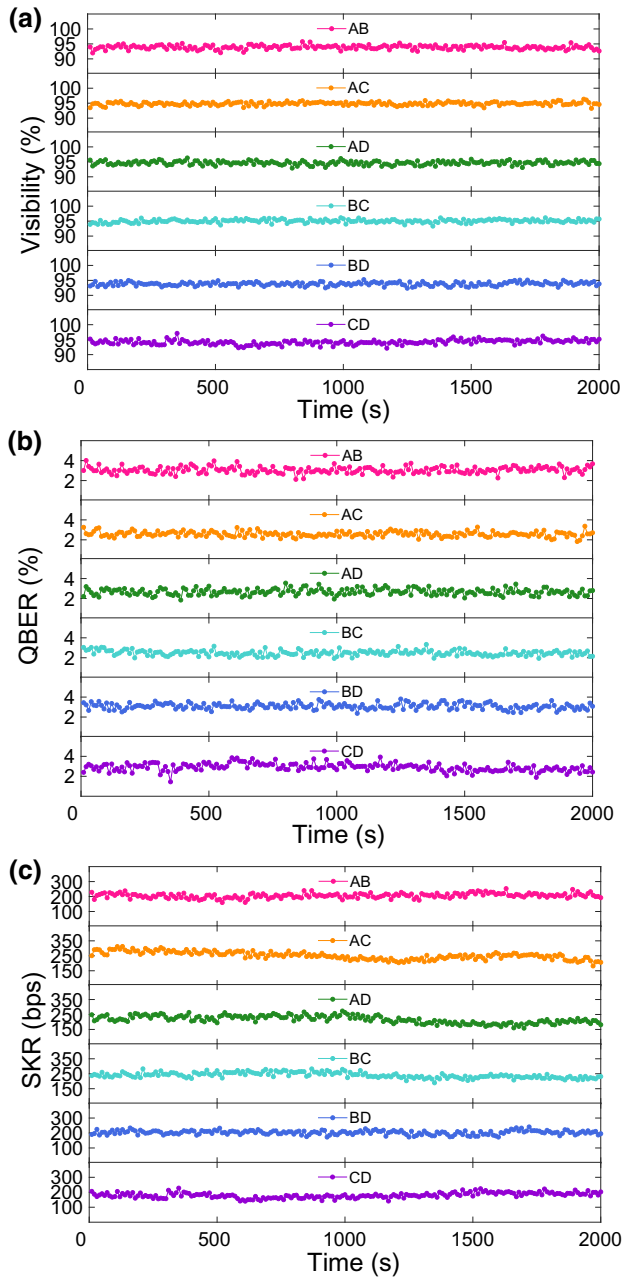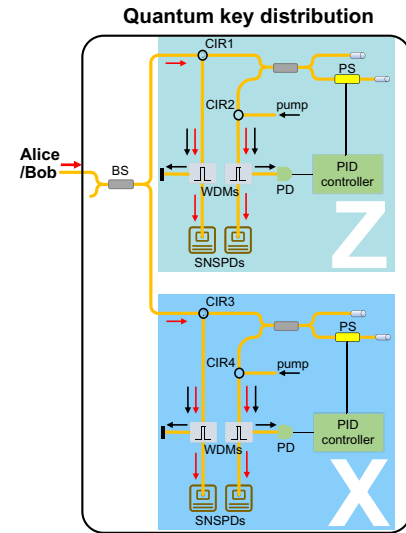
FIG. 11. The stability of (a) visibility, (b) quantum bit error rate (QBER), and (c) secure key rate (SKR) over time without the use of PID module.

Let us take the interference curve between Alice and Dave shown in Fig. 1(c) as an example, and the corresponding coincidence histograms of the maximum (blue) and minimum (orange) points are shown in Fig. 9. The left and right figures are the same set of data, with the time-bin size of Fig. 9(a) being 0.15625 ns and the time-bin size of Fig. 9(b) being 2.5 ns. The middle point of the two curves in Fig. 9(b) shows a maximum count of 1940 and a minimum count of 151, which corresponds to a raw visibility of 85.6%. The side peaks correspond to

the non-interfering terms in typical Franson interferometer (see the main text for details). The accidental coincidence is obtained by taking the average of the other 10 points except the 3 middle points. The averaged accidental coincidence counts calculated by the two curves are 117 and 120, respectively. After subtracting the respective accidental coincidences, we obtain a net visibility of 96.7%, proving the presence of high-quality Bell nonlocality between users. However, we would like to emphasize that in the later BBM92 QKD experiment, no accidental coincidence counts were subtracted.

Figure 10 shows the coincidence count and single count of Alice and Bob as a function of the phase $\phi_A + \phi_B$, where the fluctuation of single counts is less than 0.8%. The comparison demonstrates that single-photon coherence is suppressed because the time difference between the two arms of the Franson interferometer ($\Delta T = 2.5$ ns) is larger than the coherence time of the single photons ($\tau_c \sim 250$ ps).

APPENDIX C: RESULTS OF QUANTUM KEY DISTRIBUTION WITHOUT PID MODULE

We tested 2000 s of quantum key distribution (QKD) between all six pairs of entangled photon (or channels). Figure 11 shows the overall qubit error rate (QBER) between 2.57% and 3.09%, and the averaged SKR between 180 and 251 Hz. The results are summarized in Table III.
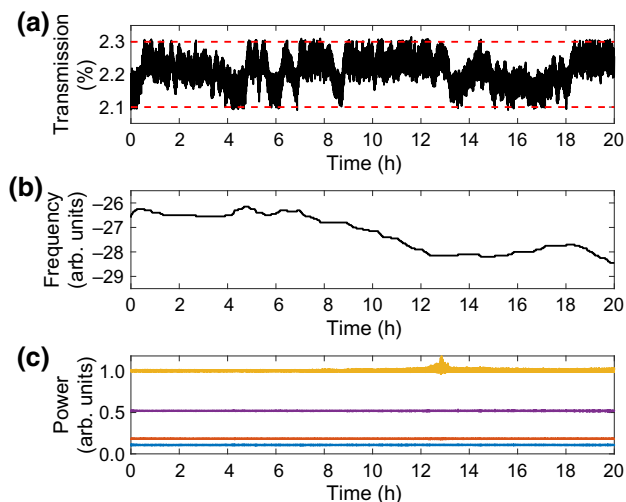
FIG. 13. (a) The stability of pump transmission at resonance wavelength, (b) the tuning of pump frequency during feedback control, and (c) the stability of the output pump power (phase) of the four PID phase-locking modules used in quantum key distribution.

The imperfection of the visibility mainly comes from the limited extinction ratio and isolation of the WDM filter, the phase drifts of the interferometer, and the imperfect polarization adjustment.

APPENDIX D: STABILITY OF OUR SYSTEM

Although all interferometers are entirely buried in quartz sand and wrapped with a thick insulating layer, the phase of the interferometer will still drift slightly due to the sensitivity of the phase to temperature, affecting the duration of QKD. For the long-term operation of the whole setup, we have made some experimental technical efforts. We added PID phase-locking module based on the original interferometers as shown in Fig. 12. Specifically, a portion of the pump from Fig. 1(a) is split by the beam splitter and then injected into the interferometers through a circulator as reference light for actively stabilizing the phase by using a PID controller. An additional circulator is added to the input of each interferometer to acquire two-port data. The
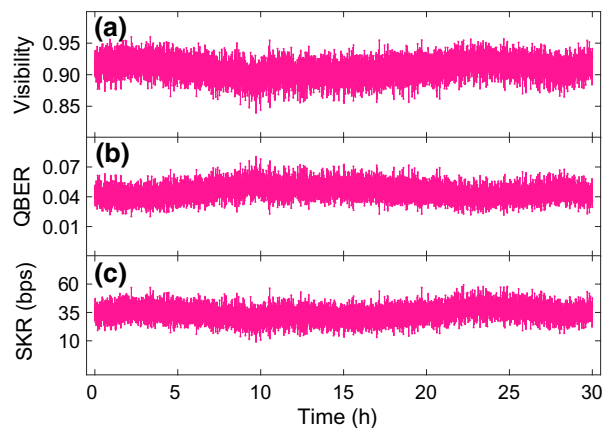

FIG. 14. (a) Visibility, (b) quantum bit error rate (QBER), and (c) secure key rate (SKR) over time for Alice and Bob with PID phase-locking module included. Each data point stands for a 10 s average value.

excess pump photons are filtered by the WDMs and the desired signal/idler photons are selected for photon detection. The reflected pump power is monitored by a power detector whose output electrical signal is connected to a PID controller (Toptica DigiLock-110/PID-110), which is used to adjust the phase shifter, and actively stabilizes the phase of the interferometer. Alice and Bob have a total of four interferometers, so a total of four such PID modules are required. We define the initial phase of Alice's first interferometer as the zero phase point, whereas the phases of the other three interferometers are determined by their respective interference results. After that, the relative phase of the measurement base Z ($0 / \pi$) and X ($\pi/2 / 3\pi/2$) are determined and then locked by the PID modules.

At the same time, to maintain the stability of the MRR resonance, we added a thermoelectric cooler and NTC thermistor at the bottom of the chip, and both were connected to a temperature controller (Thorlabs TED4015). However, due to the instability of the temperature of the laboratory, we found that the resonance of the MRR will shift slightly over time. To solve this problem, we developed a feedback control system to move the pump

TABLE III. The measured total sifted key, the average interference visibility during key distribution, the average quantum bit error rate (QBER), and the average SKR between four users in 2000 s.

User	Total sifted key (2000 s)	Visibility	QBER	SKR (bit/s or bps)
Alice & Bob	7.28×10^5	$93.89 \pm 0.66\%$	$3.06 \pm 0.33\%$	206
Alice & Chloe	8.12×10^5	$94.85 \pm 0.53\%$	$2.57 \pm 0.26\%$	252
Alice & Dave	7.13×10^5	$94.65 \pm 0.64\%$	$2.67 \pm 0.32\%$	217
Bob & Chloe	7.60×10^5	$95.04 \pm 0.53\%$	$2.48 \pm 0.27\%$	240
Bob & Dave	7.22×10^5	$93.82 \pm 0.59\%$	$3.09 \pm 0.29\%$	203
Chloe & Dave	6.18×10^5	$94.18 \pm 0.77\%$	$2.91 \pm 0.38\%$	180

TABLE IV. Comparison of sources used in different multiuser QKD platforms based on BBM92 protocol.

	Platform	Material	Source size	CMOS compatible?	Linewidth per frequency mode (GHz)	Spectrum bandwidth (nm)
Wengerowsky *et al.* [16]	Free-space	MgO:PPLN	4 cm long	No	100	~ 60 (Fig. 3 of Ref. [16])
Joshi *et al.* [17]	Free-space	MgO:PPLN	4 cm long	No	100	~ 60 (SM of Ref. [17])
Fitzke *et al.* [20]	Fiber-coupled	PPLN	N.A.	No	25, 50, 100	~ 75 (Section A of Ref. [20])
This work	Chip-integrated	Si_3N_4	460 μm diameter	Yes	0.65	~ 35 (Hundreds in Ref. [15,32,33])

wavelength to follow the resonance drift of the MRR resonance. In the upper panel of Fig. 13, we show the pump transmission at the resonant wavelength, which is kept at the minimum level ($2.2 \pm 0.1\%$ of the input power, and the upper and lower bounds are marked with red dashed lines). In order to maintain this resonance condition, we adaptively tune the pump frequency, as shown in the middle panel of Fig. 13. The range of the y-axis is about 150 MHz. The lower panel of Fig. 13 shows the variation of the pump power output from the four interferometers with time under the active control of the PID phase-locking module, which indicates that the phases of the four interferometers have good stability.

Figure 14 shows the long-running performance of quantum key distribution between Alice and Bob. In Fig. 14(a) we show the entanglement visibility with an average value of $90.98 \pm 1.61\%$, and in Fig. 14(b) we show the QBER with an average value $4.51 \pm 0.80\%$. Within an integration time of 30 h, we obtain a total security key of 3.68×10^6 bits. This corresponds to an average SKR [51,52] of 34 bits/s, as shown in Fig. 14(c). Note that due to the residual pump photons, the QBER is higher than that when the PID module is not added. At the same time, due to the extra loss brought by WDMs, the SKR is lower than that without the PID module included.

APPENDIX E: SECURITY OF OUR SYSTEM

Entanglement-based QKD has inherent source-independent security and is therefore immune to source-targeted attacks [51,54]. Therefore, one usually considers the effect of detection attacks for entanglement-based QKD, such as detector-related attack [55–57], wavelength-dependent attack [58], and spatial-mode attack [59]. Note that most of these attacks have been studied in Ref. [60]. Here we only consider the potential attacks coming from different physical implementations between ours and those in Ref. [60]. For the detector efficiency mismatch attack, we use SNSPDs in our system and they are in work the free-running mode. Hence, Eve cannot employ the detector efficiency mismatch attack. For the blinding attack, it has been shown that by implementing an active antilatching system for SNSPDs, monitoring the comparator pulse shape and implementing postprocessing key extraction, one can resolve the blinding attack [61]. For the beam-splitter attack, we do use a 1×2 beam splitter to randomly select the measurement basis in our QKD system. However, the photons generated by our MRR source inherently have narrow linewidths (~ 650 MHz), so the wavelength dependence of the beam splitter's splitting ratio within this range can be ignored.

TABLE V. Performance comparison of QKD systems on different multiuser QKD platforms based on BBM92 protocol.

	Protocol	Basis	Number of users	SKR (bps)	QBER
Wengerowsky *et al.* [16]	BBM92	Polarization	4 (fully connected)	$3 \sim 15$ (estimated by authors)	N.A.
Joshi *et al.* [17]	BBM92	Polarization	8 (fully connected)	$58 \sim 304$ (in-laboratory) $0.5 \sim 51.8$ (city-wide) (calculated from SM)	$3\% \sim 6\%$ (estimated from SM)
Fitzke *et al.* [20]	BBM92	Time-bin	4 (pairwise connected)	42/29 (in-laboratory) 6/102 (field test)	2.41%/2.36% (in-laboratory) 4.5%/2.6% (field test)
This work	BBM92	Energy-time	4 (fully connected)	$180 \sim 252$ (in-laboratory)	$2.5\% \sim 3.1\%$

APPENDIX F: COMPARISON WITH OTHER QUANTUM NETWORKS BASED ON BBM92 PROTOCOL

Recently, several platforms that use wavelength division multiplexing schemes to realize multiuser QNs have been presented [16–20] and some of these platforms have already been implemented in real-world scenarios. Here, we compare the performance of sources used by different platforms based on the BBM92 protocol in Table IV, and compare the performance of the QKD system of these platforms in Table V.

---

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[2] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, Quantum computers, Nature **464**, 45 (2010).

[3] V. Giovannetti, S. Lloyd, and L. Maccone, Advances in quantum metrology, Nat. Photonics **5**, 222 (2011).

[4] R. Thew, A. Acín, H. Zbinden, and N. Gisin, Experimental realization of entangled qutrits for quantum communication, Quantum Info. Comput. **4**, 93 (2004).

[5] A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson, Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities, Nat. Phys. **7**, 677 (2011).

[6] D. Richart, Y. Fischer, and H. Weinfurter, Experimental implementation of higher dimensional time–energy entanglement, Appl. Phys. B **106**, 543 (2012).

[7] X.-L. Wang, X.-D. Cai, Z.-E. Su, M.-C. Chen, D. Wu, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, Quantum teleportation of multiple degrees of freedom of a single photon, Nature **518**, 516 (2015).

[8] C. Schaeff, R. Polster, M. Huber, S. Ramelow, and A. Zeilinger, Experimental access to higher-dimensional entangled quantum systems using integrated optics, Optica **2**, 523 (2015).

[9] M. Kues, C. Reimer, P. Roztocki, L. R. Cortés, S. Sciara, B. Wetzel, Y. Zhang, A. Cino, S. T. Chu, B. E. Little, D. J. Moss, L. Caspani, J. Azaña, and R. Morandotti, On-chip generation of high-dimensional entangled quantum states and their coherent control, Nature **546**, 622 (2017).

[10] P. Imany, J. A. Jaramillo-Villegas, O. D. Odele, K. Han, D. E. Leaird, J. M. Lukens, P. Lougovski, M. Qi, and A. M. Weiner, 50-GHz-spaced comb of high-dimensional frequency-bin entangled photons from an on-chip silicon nitride microresonator, Opt. Express **26**, 1825 (2018).

[11] J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson, Multidimensional quantum entanglement with large-scale integrated optics, Science **360**, 285 (2018).

[12] C. Reimer, S. Sciara, P. Roztocki, M. Islam, L. R. Cortés, Y. Zhang, B. Fischer, S. Loranger, R. Kashyap, A. Cino, S. T. Chu, B. E. Little, D. J. Moss, L. Caspani, W. J. Munro, J. Azaña, M. Kues, and R. Morandotti, High-dimensional one-way quantum processing implemented on D-level cluster states, Nat. Phys. **15**, 148 (2019).

[13] L. Lu, L. Xia, Z. Chen, L. Chen, T. Yu, T. Tao, W. Ma, Y. Pan, X. Cai, Y. Lu, Shining Zhu, and Xiao-Song Ma, Three-dimensional entanglement on a silicon chip, NPJ Quantum Inf. **6**, 30 (2020).

[14] C. Joshi, A. Farsi, S. Clemmen, S. Ramelow, and A. L. Gaeta, Frequency multiplexing for quasi-deterministic heralded single-photon sources, Nat. Commun. **9**, 847 (2018).

[15] P. Marin-Palomo, J. N. Kemal, M. Karpov, A. Kordts, J. Pfeifle, M. H. P. Pfeiffer, P. Trocha, S. Wolf, V. Brasch, M. H. Anderson, R. Rosenberger, K. Vijayan, W. Freude, T. J. Kippenberg, and C. Koos, Microresonator-based solitons for massively parallel coherent optical communications, Nature **546**, 274 (2017).

[16] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, An entanglement-based wavelength-multiplexed quantum communication network, Nature **564**, 225 (2018).

[17] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, and R. Ursin, A trusted node–free eight-user metropolitan quantum communication network, Sci. Adv. **6**, eaba0959 (2020).

[18] 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).

[19] 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).

[20] E. Fitzke, L. Bialowons, T. Dolejsky, M. Tippmann, O. Nikiforov, T. Walther, F. Wissel, and M. Gunkel, Scalable network for simultaneous pairwise quantum key distribution via entanglement-based time-bin coding, PRX Quantum **3**, 020341 (2022).

[21] S. Wehner, D. Elkouss, and R. Hanson, Quantum Internet: a vision for the road ahead, Science **362**, eaam9288 (2018).

[22] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han, and G. Guo, Field experiment on a robust hierarchical metropolitan quantum cryptography network, Chin. Sci. Bull. **54**, 2991 (2009).

[23] 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, and A. Zeilinger, The SECOQC quantum key distribution network in Vienna, New J. Phys. **11**, 075001 (2009).

[24] 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. LŁanger, M. Peev, and A. Zeilinger, Field test of quantum key distribution in the Tokyo QKD network, Opt. Express **19,** 10387 (2011).

[25] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, Long-term performance of the SwissQuantum quantum key distribution network in a field environment, New J. Phys. **13,** 123001 (2011).

[26] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature **589,** 214 (2021).

[27] Y. Li, Y. Huang, T. Xiang, Y. Nie, M. Sang, L. Yuan, and X. Chen, Multiuser time-energy entanglement swapping based on dense wavelength division multiplexed and sum-frequency generation, Phys. Rev. Lett. **123,** 250505 (2019).

[28] Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, A 15-user quantum secure direct communication network, Light Sci. Appl. **10,** 183 (2021).

[29] C. Reimer, L. Caspani, M. Clerici, M. Ferrera, M. Kues, M. Peccianti, A. Pasquazi, L. Razzari, B. E. Little, S. T. Chu, D. J. Moss, and R. Morandotti, Integrated frequency comb source of heralded single photons, Opt. Express **22,** 6535 (2014).

[30] F. Mazeas, M. Traetta, M. Bentivegna, F. Kaiser, D. Aktas, W. Zhang, C. A. Ramos, L. A. Ngah, T. Lunghi, É. Picholle, N. Belabas-Plougonven, X. Le Roux, E. Cassan, D. Marris-Morini, L. Vivien, G. Sauder, L. Labonté, and S. Tanzilli, High-quality photonic entanglement for wavelength-multiplexed quantum communication based on a silicon chip, Opt. Express **24,** 28731 (2016).

[31] J. A. Jaramillo-Villegas, P. Imany, O. D. Odele, D. E. Leaird, Z.-Y. Ou, M. Qi, and A. M. Weiner, Persistent energy–time entanglement covering multiple resonances of an on-chip biphoton frequency comb, Optica **4,** 655 (2017).

[32] F. Samara, A. Martin, C. Autebert, M. Karpov, T. J. Kippenberg, H. Zbinden, and R. Thew, High-rate photon pairs and sequential time-bin entanglement with Si_3N_4 microring resonators, Opt. Express **27,** 19309 (2019).

[33] C. Reimer, M. Kues, P. Roztocki, B. Wetzel, F. Grazioso, B. E. Little, S. T. Chu, T. Johnston, Y. Bromberg, L. Caspani, D. J. Moss, and R. Morandotti, Generation of multiphoton entangled quantum states by means of integrated frequency combs, Science **351,** 1176 (2016).

[34] M. Kues, C. Reimer, J. M. Lukens, W. J. Munro, A. M. Weiner, D. J. Moss, and R. Morandotti, Quantum optical microcombs, Nat. Photonics **13,** 170 (2019).

[35] X. Li, P. L. Voss, J. E. Sharping, and P. Kumar, Optical-Fiber Source of Polarization-Entangled Photons in the 1550 nm Telecom Band, Phys. Rev. Lett. **94,** 053601 (2005).

[36] S. Ramelow, A. Farsi, S. Clemmen, D. Orquiza, K. Luke, M. Lipson, and A. L. Gaeta, Silicon-nitride platform for narrowband entangled photon generation, arXiv:1508.04358 (2015).

[37] F. Samara, N. Maring, A. Martin, A. S. Raja, T. J. Kippenberg, H. Zbinden, and R. Thew, Entanglement swapping between independent and asynchronous integrated photon-pair sources, Quantum Sci. Technol. **6,** 045024 (2021).

[38] Z. Xie, T. Zhong, S. Shrestha, X. Xu, J. Liang, Y.-X. Gong, J. C. Bienfang, A. Restelli, J. H. Shapiro, F. N. C. Wong, and C. W. Wong, Harnessing high-dimensional hyperentanglement through a biphoton frequency comb, Nat. Photonics **9,** 536 (2015).

[39] C. Simon *et al.*, Quantum memories, Eur. Phys. J. D **58,** 1 (2010).

[40] H. Takesue, Y. Tokura, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, and S.-i. Itabashi, Entanglement generation using silicon wire waveguide, Appl. Phys. Lett. **91,** 201108 (2007).

[41] M. Förtsch, J. U. Fürst, C. Wittmann, D. Strekalov, A. Aiello, M. V. Chekhova, C. Silberhorn, G. Leuchs, and C. Marquardt, A versatile source of single photons for quantum information processing, Nat. Commun. **4,** 1818 (2013).

[42] X. Zhang, Y. Zhang, C. Xiong, and B. J. Eggleton, Correlated photon pair generation in low-loss double-stripe silicon nitride waveguides, J. Opt. **18,** 074016 (2016).

[43] X. Lu, S. Rogers, T. Gerrits, W. C. Jiang, S. W. Nam, and Q. Lin, Heralding single photons from a high-Q silicon microdisk, Optica **3,** 1331 (2016).

[44] A. Pasquazi, M. Peccianti, L. Razzari, D. J. Moss, S. Coen, M. Erkintalo, Y. K. Chembo, T. Hansson, S. Wabnitz, P. Del'Haye, Xiaoxiao Xue, Andrew M. Weiner, and Roberto Morandotti, Micro-combs: a novel generation of optical sources, Phys. Rep. **729,** 1 (2018).

[45] J. D. Franson, Bell Inequality for Position and Time, Phys. Rev. Lett. **62,** 2205 (1989).

[46] Y.-H. Li, Z.-Y. Zhou, L.-T. Feng, W.-T. Fang, S.-l. Liu, S.-K. Liu, K. Wang, X.-F. Ren, D.-S. Ding, L.-X. Xu, and B.-S. Shi, On-chip multiplexed multiple entanglement sources in a single silicon nanowire, Phys. Rev. Appl. **7,** 064005 (2017).

[47] Z.-Y. Zhou, D.-S. Ding, Y. Li, F.-Y. Wang, and B.-S. Shi, Cavity-enhanced bright photon pairs at telecom wavelengths with a triple-resonance configuration, JOSA B **31,** 128 (2014).

[48] E. Saglamyurek, J. Jin, V. B. Verma, M. D. Shaw, F. Marsili, S. W. Nam, D. Oblak, and W. Tittel, Quantum storage of entangled telecom-wavelength photons in an erbium-doped optical fibre, Nat. Photonics **9,** 83- (2015).

[49] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett. **23,** 880 (1969).

[50] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography Without Bell's Theorem, Phys. Rev. Lett. **68,** 557 (1992).

[51] X. Ma, C. H. F. Fung, and H.-K. Lo, Quantum key distribution with entangled photon sources, Phys. Rev. A **76,** 012307 (2007).

[52] J. Yin *et al.*, Satellite-to-Ground Entanglement-Based Quantum Key Distribution, Phys. Rev. Lett. **119,** 200501 (2017).

[53] X. Ji, J. K. Jang, U. D. Dave, M. Corato-Zanarella, C. Joshi, A. L. Gaeta, and M. Lipson, Exploiting ultralow loss multimode waveguides for broadband frequency combs, Laser Photonics Rev. **15,** 2000353 (2021).

[54] M. Koashi and J. Preskill, Secure Quantum Key Distribution with an Uncharacterized Source, Phys. Rev. Lett. **90,** 057902 (2003).

[55] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78,** 042333 (2008).

[56] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4,** 686- (2010).

[57] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors, New J. Phys. **13,** 073024 (2011).

[58] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources, Phys. Rev. A **84,** 062308 (2011).

[59] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lutkenhaus, and V. Makarov, Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch, Phys. Rev. A **91,** 062301 (2015).

[60] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, Entanglement-based secure quantum cryptography over 1,120 kilometres, Nature **582,** 501 (2020).

[61] M. Elezov, R. Ozhegov, G. Goltsman, and V. Makarov, Countermeasure against bright-light attack on superconducting nanowire single-photon detector in quantum key distribution, Opt. Express **27,** 30979 (2019).