Letter

ADVANCED PHOTONICS

Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution

Xiaodong Zheng,[a,†] Peiyu Zhang,[a,†] Renyou Ge,[b,†] Liangliang Lu,[a,†] Guanglong He,[a,†] Qi Chen,[a,†] Fangchao Qu,[a] Labao Zhang,[a,*] Xinlun Cai,[b,*] Yanqing Lu,[a] Shining Zhu,[a] Peiheng Wu,[a] and Xiao-Song Ma[a,*]

[a]Nanjing University, National Laboratory of Solid-state Microstructures, School of Physics, Research Institute of Superconducting Electronics, School of Electronic Science and Engineering, College of Engineering and Applied Sciences, Collaborative Innovation Center of Advanced Microstructures, Nanjing, China

[b]Sun Yat-sen University, State Key Laboratory of Optoelectronic Materials and Technologies, School of Electronics and Information Technology, Guangzhou, China

Abstract. Integrated photonics provides a route to both miniaturization of quantum key distribution (QKD) devices and enhancing their performance. A key element for achieving discrete-variable QKD is a single-photon detector. It is highly desirable to integrate detectors onto a photonic chip to enable the realization of practical and scalable quantum networks. We realize a heterogeneously integrated, superconducting silicon-photonic chip. Harnessing the unique high-speed feature of our optical waveguide-integrated superconducting detector, we perform the first optimal Bell-state measurement (BSM) of time-bin encoded qubits generated from two independent lasers. The optimal BSM enables an increased key rate of measurement-device-independent QKD (MDI-QKD), which is immune to all attacks against the detection system and hence provides the basis for a QKD network with untrusted relays. Together with the time-multiplexed technique, we have enhanced the sifted key rate by almost one order of magnitude. With a 125-MHz clock rate, we obtain a secure key rate of 6.166 kbps over 24.0 dB loss, which is comparable to the state-of-the-art MDI-QKD experimental results with a GHz clock rate. Combined with integrated QKD transmitters, a scalable, chip-based, and cost-effective QKD network should become realizable in the near future.

Keywords: quantum key distribution; hybrid photonics; single-photon detector; Bell-state measurement; time-multiplexing.

Received Jun. 17, 2021; revised manuscript received Sep. 27, 2021; accepted for publication Sep. 29, 2021; published online Oct. 30, 2021.

[DOI: 10.1117/1.AP.3.5.055002]

1 Introduction

Quantum key distribution (QKD) employs the laws of quantum physics to provide information-theoretical security for key exchange.[1–5] Despite the substantial progress in the past 35 years, practical implementations of QKD still deviate from ideal descriptions in security proofs, mainly due to potential side-channel attacks. For instance, a series of loopholes have been identified due to the imperfections of measurement devices.[6–9] Inspired by the time-reversed entanglement-based QKD, measurement-device-independent QKD (MDI-QKD), which removes all detector side attacks, has been proposed.[10,11] Instead of relying on the trusted nodes of traditional QKD protocols, MDI-QKD requires only a central node (Charlie) to perform a Bell-state measurement (BSM). The correlations between the two senders (Alice and Bob) can be obtained from the BSM results. Importantly, even if Charlie is not trusted, one can still guarantee the security of the MDI-QKD as long as Charlie can project his two photons onto Bell states. The outstanding features of MDI-QKD invite global experimental efforts, which

*Address all correspondence to Labao Zhang, lzhang@nju.edu.cn; Xinlun Cai, caixlun5@mail.sysu.edu.cn; Xiao-Song Ma, xiaosong.ma@nju.edu.cn

†These authors contributed equally to this work.

are mainly based on bulk/fiber components.[12–20] Despite the additional BSM by Charlie, the key rate[17] and the communication distance[18] of MDI-QKD can be comparable with those of traditional QKD. Furthermore, the star-like topology of the MDI-QKD quantum network is naturally suited for the metropolitan network with multiple users.[21–23] Recently, the generalization of the MDI protocol to multipartite schemes has been investigated.[24–26] It has been shown that the performance of the multipartite schemes can be advantageous to iterative use of independent bipartite protocols.[26]

From the perspectives of hardware, recent developments involve particular integrated photonic devices for QKD, including on-chip encoders based on silicon modulators,[27–31] on-chip transmitters including lasers, photodiodes, modulators based on indium phosphide,[32,33] and decoders based on silicon oxynitride[34] and silicon dioxide,[35] as well as integrated silicon-photonic chips for continuous-variable (CV) QKD.[36,37] The notion of MDI has also been extended to CV protocols[38] and can be applied for multipartite metropolitan networks with a considerable rate.[39] Most of the components used in QKD, including lasers, modulators, and passive components [such as beam splitters (BSs) and attenuators] are widely used in classical optical communication systems and are not specifically designed for QKD. In addition, single-photon detectors are indispensable for discrete-variable QKD systems, because the senders' pulses have to have a mean photon number of <1 to guarantee communication security. So far, a single-photon detector integrated chip platform has not been employed in an MDI-QKD system. In this work, we report the realization of a heterogeneously integrated, superconducting silicon-photonic chip, and its application for MDI-QKD.

2 Schematic of a Time-Multiplexed MDI-QKD

We use time-bin qubits to encode bit information, which are well suited for fiber-based quantum communication due to their immunity to random polarization rotations in fibers. The conceptual scheme of our experiment is shown in Fig. 1(a). Alice and Bob encode keys with time-bin qubits using modulated weak coherent pulse sets. In Pauli Z-basis, the time-bins are encoded as the early $|e\rangle$ and the late $|l\rangle$ for bit values of 0 and 1, respectively. The temporal separation between $|e\rangle$ and $|l\rangle$ is Δt. In Pauli X-basis, the keys are encoded as the coherent superposition states between $|e\rangle$ and $|l\rangle$: $|+\rangle = (|e\rangle + |l\rangle)/\sqrt{2}$ and $|-\rangle = (|e\rangle - |l\rangle)/\sqrt{2}$, representing bit values of 0 and 1, respectively. The Z-basis code is used for key exchange, and the X-basis code is for error detection. These encoded time-bin qubits are then sent to Charlie, who performs the BSM on the incoming time-bin qubits using a BS and two single-photon detectors (D_1 and D_2).[10,11] Using linear optical elements, the success probability of BSM is bounded by 50%.[40] For projective measurements, optimal BSM corresponds to distinguish two out of four Bell states. Although time-bin qubits are well suited for fiber-based quantum communication, optimal BSM for time-bin qubits has yet to be realized. The bottleneck so far has been the lack of high-speed single-photon detectors.[33,41,42] The BSM scheme for time-bin qubits is shown in the inset of Fig. 1(a). The coincidence counts between two different detectors at different time bins correspond to coincidence counts between $|e\rangle_{D_1}$ (D_1 detects a photon at an early bin, red) and $|l\rangle_{D_2}$ (D_2 detects a photon at a late bin, red), or coincidence counts between $|l\rangle_{D_1}$ and $|e\rangle_{D_2}$. Such coincidence detection projects two photons onto $|\Psi^-\rangle = (|el\rangle - |le\rangle)/\sqrt{2}$, which is the common scenario realized in most of the time-bin BSM schemes.[14,33,42] In order to achieve optimal BSM, we also need to detect $|\Psi^+\rangle = (|el\rangle + |le\rangle)/\sqrt{2}$ by measuring the coincidence counts of one detector at different time bins, corresponding to the coincidence detection between $|e\rangle_{D_1}$ and $|l\rangle_{D_1}$, or $|e\rangle_{D_2}$ and $|l\rangle_{D_2}$. This particular BSM requires high-speed single-photon detection, able to detect consecutive photons separated by Δt. The unique design of the waveguide-integrated superconducting nanowire single-photon detector (SNSPD) provides a short recovery time (<10 ns) for single-photon detection, enabling us to perform time-bin-encoded optimal BSM between two independent lasers for the first time. Note that if we only use one set of time-bin qubits, the system repetition rate will be limited to $1/(2\Delta t)$.

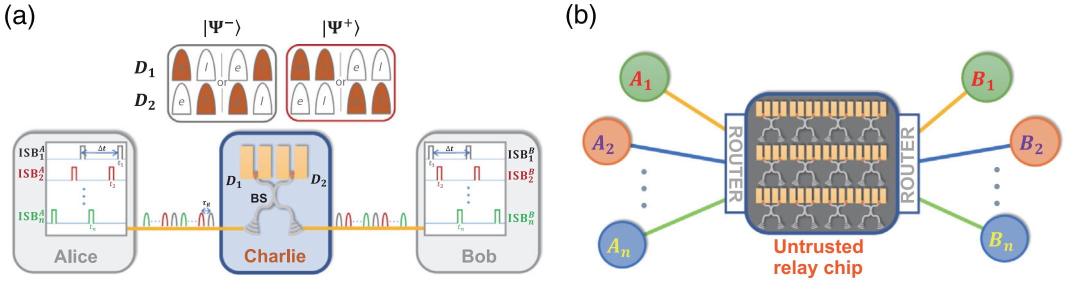

Fig. 1 Schematic of a time-multiplexed MDI-QKD and a star-like MDI-QKD network. (a) Schematic of a time-multiplexed MDI-QKD with optimal BSM. Alice and Bob send time-bin encoded qubits to Charlie for exchanging keys. By detecting the coincidence (red) between the early (e) and late (l) pulses with two detectors (D_1 and D_2), or with one detector (D_1 or D_2). Charlie projects two incoming photons onto $|\Psi^-\rangle$ or $|\Psi^+\rangle$ to facilitate the key exchanges between Alice and Bob. The full-recovery time of the single-photon detector sets the lower limit of the temporal separation (Δt) between e and l pulses for realizing optimal BSM. We insert ISBs between e and l for realizing time-multiplexing and hence increase the key rate by reducing the bin separation from Δt to τ_R. (b) A star-like MDI-QKD network with the untrusted relay server. A series of Alice ($A_1, A_2, \dots, A_n$) and Bob ($B_1, B_2, \dots, B_n$) prepare modulated weak coherent pulses and send to the routers. Two routers select a pair of Alice and Bob and send their pulses to an untrusted relay server controlled by Charlie.

In order to maximize the channel efficiency, we use time-multiplexed encoding to insert independent sets of bins ($\mathrm{ISB}_2^A, \ldots, \mathrm{ISB}_n^A$ and $\mathrm{ISB}_2^B, \ldots, \mathrm{ISB}_n^B$) between the $|e\rangle$ and $|l\rangle$ bins of ISB_1^A and ISB_1^B. Therefore, the system repetition rate will be greatly increased to $1/(2\tau_R)$, where τ_R is the time difference between t_1 and t_2. By harnessing the optimal BSM and time-multiplexing, the key rate generation is enhanced by an order of magnitude compared to the system without using these two techniques. Consequently, our key rate is comparable to the state-of-the-art MDI-QKD experimental results with a GHz clock rate, as detailed later.

3 Integrated Relay Server for MDI-QKD Based on Superconducting Silicon Photonics

Our heterogeneously integrated, superconducting silicon-photonic platform provides a server architecture for realizing a multiple-user trust-node-free quantum network with a fully connected bipartite-graph topology. As shown in Fig. 1(b), modulated weak coherent pulses are prepared by Alices ($A_1, A_2, \ldots, A_n$) and Bobs ($B_1, B_2, \ldots, B_n$) and are sent to the routers. Two routers select the pair of the communicating Alice and Bob and send their pulses to an untrusted relay server controlled by Charlie. At Charlie's station, a chip with multiple low-dead-time,[43] low-timing-jitter,[44] and high-efficiency detectors in conjunction with low-loss silicon photonics[45] is used to realize the BSM. This configuration allows any user at Alice's side to communicate with any user at Bob's side and hence to realize a fully connected bipartite quantum network.

The schematic of our experimental setup is shown in Fig. 2(a). Alice (Bob) chops the CW laser operated at about 1536.47 nm into the desired pulse sequences. The pulse is about 370 ps wide and separated by 12 ns at a rate of 41.7 MHz rate (1/24 ns). Z-basis (X-basis) states are generated by chopping the laser into $|e\rangle$ or (and) $|l\rangle$ states with intensity modulators (IMs). The average photon numbers per pulse in the two bases are about the same. The resulting pulses are sent into a phase modulator (PM) with (without) π-phase shift for the generation of $|-\rangle$ ($|+\rangle$) states. The electrical signals applied to the modulators are generated by an arbitrary waveform generator [not shown in Fig. 2(a)]. An additional 50:50 BS combined with a power sensor (PS) is employed to monitor the long-term stability of laser power in each encoder.

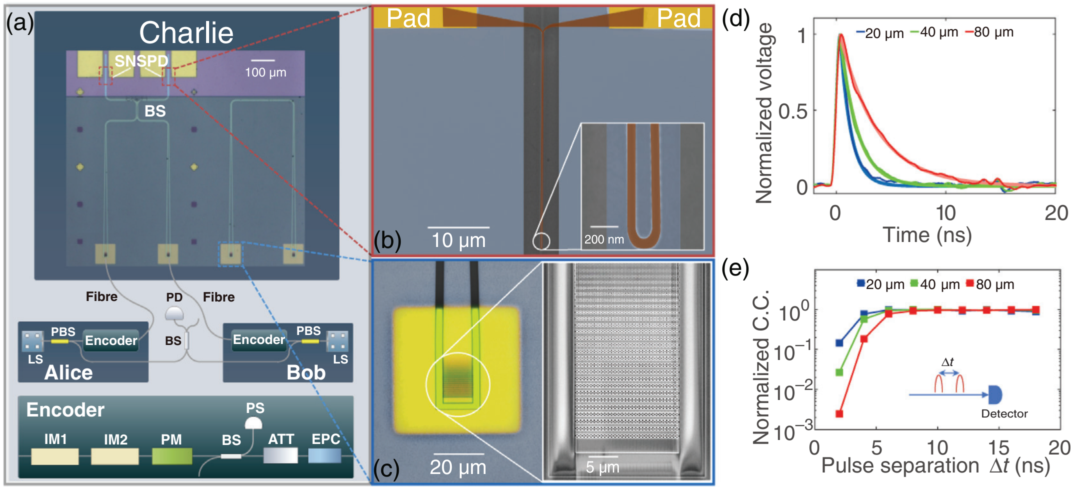

Fig. 2 Experimental device and setup. (a) Schematic of the experiment setup. Alice (Bob) employs a CW laser as the LS and encodes the keys into optical pulses with an encoder module. In this module, one intensity modulator (IM1) chops out early ($|e\rangle$) and late ($|l\rangle$) temporal modes to generate time-bin qubits with a 370 ps duration and separated by 12 ns with a 41.7 MHz repetition rate. IM2 implements intensity modulation for the decoy-state protocol. A PM applies a π-phase to the late temporal modes for $|-\rangle$ and 0-phase for $|+\rangle$ in X-basis. This PM also implements the phase randomization required for MDI-QKD. A variable attenuator prepares weak coherent pulses and simulates the propagation loss in fibers. An EPC adjusts the polarization of the input pulses. The pulses travel through fibers and are coupled into the integrated chip of the relay server (Charlie) for BSM. On the chip, we use a multi-mode interferometer acting as a 50:50 BS and two SNSPDs. (b) False-color scanning electron micrograph (SEM) of the SNSPD. A 80-nm-wide, 80-μm-long U-shaped NbN nanowire is integrated on a 500-nm-wide silicon optical waveguide and connected with two gold pads for electrical readout. The inset shows the zoomed part of the nanowire. (c) Optical and SEM graphs of the high-efficiency photonic-crystal grating coupler with a back-reflected mirror. (d) The averaged amplified response pulses of the 80-nm-wide SNSPD with different lengths. The 1/e-decay time of different SNSPDs is obtained by fitting: 20 μm to 0.96 ns; 40 μm to 1.56 ns; 80 μm to 3.39 ns. (e) Normalized coincidence counts of one detector consecutively detecting both early and late time bins as a function of time separation Δt between them. PBS, polarization beam splitter; PD, photodiode; PS, power sensor; and EPC, electrical polarization controller.

One of the most important requirements of MDI-QKD is to obtain high-quality two-photon Hong–Ou–Mandel (HOM) interference on the integrated relay server. To achieve that, it is necessary for Alice and Bob to generate indistinguishable weak-coherent pulses. The interfering pulses have to be indistinguishable in all degrees of freedom (DOFs), including spectrum, time, and polarization. For the spectrum DOF, Alice's and Bob's unmodulated pulses pass through polarization beam splitters (PBSs), with one of the outputs connected with a 50:50 BS for frequency beating. From the beating signal, we feedback onto one of the lasers and regulate the frequency difference of these two lasers to be within 10 MHz (see Supplementary Material for details). For the polarization DOF, two electrical polarization controllers (EPCs) are used to optimize the polarization of both pulses before they are coupled into Charlie's chip. For the temporal DOF, we adjust the relative electrical delay between Alice's and Bob's IMs to ensure that their pulses arrive at the chip simultaneously. Attenuators are used to adjust the average photon number per pulse and simulate the loss of the communication channels.

These pulses are then sent to Charlie's relay server chip, which is mounted on a nanopositioner in a closed-cycle cryostat with a base temperature of 2.1 K. We show the U-shape waveguide-integrated SNSPD in Fig. 2(b) in which the superconducting nanowire (80-nm-wide, 80-μm-long) is highlighted in red and the silicon optical waveguide (500 nm-wide) is shown in blue. Figure 2(c) shows the scanning electron microscope image of the photonic-crystal grating coupler,[46,47] which couples light from the fiber array to the chip. We obtain coupling loss from the reference device, which is at the right side of the main device.[48] The grating coupler with a back-reflected mirror offers a coupling loss of ~2.24 dB at a wavelength of 1536 nm. The main device has two identical grating couplers, coupling Alice's and Bob's pulses from fiber to chip. Silicon optical waveguides guide the pulses to a multi-mode interference (MMI) coupler, which acts as a 50:50 BS. At the output of the MMI, two waveguide-integrated SNSPDs work simultaneously for detecting photons. Both SNSPDs are biased with constant voltage sources and connected with electronic readout circuitries. In Fig. 2(d), we show the electrical signals of waveguide-integrated SNSPDs with different nanowire lengths. The decay time of SNSPD is directly proportional to the kinetic inductance of the nanowire. Shorter detectors exhibit lower kinetic inductance and therefore have shorter decay times, resulting in faster detector recovery.[49] However, for traditional normal-incidence SNSPDs, the shorter nanowire length leads to lower detection efficiency, because it is necessary to fabricate large-area meander nanowire to match the optical modes from fibers to obtain high detection efficiency. Therefore, it is hard to simultaneously obtain low dead time and high detection efficiency with the traditional design. In our work, we use the evanescent coupling between the optical waveguide and superconducting nanowire to circumvent this trade-off. Therefore, we are able to obtain low dead time as well as high on-chip detection efficiency. To further quantitatively characterize the efficiency of our SNSPDs for projecting two photons onto $|\Psi^+\rangle$, we measure the normalized coincidence counts of one detector consecutively detecting both early and late time bins as a function of the time separation Δt between them. The experimental results are shown in Fig. 2(e). The detection probability is significantly decreased when the time separation is smaller than the dead time and is fully recovered for separation larger than 12 ns. Based on these results, the dead time of the SNSPD we use in our QKD system is about 3.4 ns for the 1/e-delay time, and we set the time separation between $|e\rangle$ and $|l\rangle$ to be 12 ns. This short time separation not only allows high-speed detection but also greatly simplifies frequency stabilization of the light source (LS). For a traditional normal-incidence SNSPD that limits 75 ns time-bin separation,[50] a 185-kHz frequency difference between two lasers can result in a 5-deg phase error, which is technologically challenging and not practical. By contrast, for our waveguide-integrated SNSPD, the frequency-stabilization requirement is only 1.2 MHz for achieving the same phase error, which is significantly more feasible in practice.

4 Optimal Bell-State Measurement for Time-Bin Qubits

In Figs. 3(a) and 3(b), we show the two-photon coincidence counts with optimal BSM as a function of the relative electronic delays between Alice's and Bob's pulse sequence in which Charlie projects the two photons sent by Alice and Bob onto $|\Psi^-\rangle$ and $|\Psi^+\rangle$, respectively. The dependence of the coincidence counts on the delay is a result of BSM, showing the coherent two-photon superposition. Due to the symmetry of $|\Psi^-\rangle$ and $|\Psi^+\rangle$, when Alice and Bob send the same states in X-basis, $|++\rangle$ or $|--\rangle$, we obtain the destructive/constructive interference patterns for the BSM results of $|\Psi^-\rangle/|\Psi^+\rangle$, as shown by the blue dots in Figs. 3(a) and 3(b). When Alice and Bob send the orthogonal states in X-basis, $|+-\rangle$ or $|-+\rangle$, we obtain the inverse results, as shown by the red dots in Figs. 3(a) and 3(b). [The logic of coincidence detection for $|\Psi^-\rangle$ and $|\Psi^+\rangle$ is shown in the inset of Fig. 1(a).]

We obtain secure keys from the Z-basis measurements and verify the reliability of the QKD system in X-basis.[18] To quantify the performance of the system, we analyze the quantum bit error rate (QBER). For instance, Alice and Bob exchange their keys conditionally on Charlie obtaining $|\Psi^-\rangle/|\Psi^+\rangle$ from his BSM, when Alice and Bob send the same/orthogonal states. For X-basis, the probability of Charlie obtaining a coincidence at two subsequent time bins with time separation Δt is $P_X^-(t, t+\Delta t)/P_X^+(t, t+\Delta t)$. We then obtain the QBER in X-basis ($\mathrm{QBER}_X^{|\Psi^-\rangle}/\mathrm{QBER}_X^{|\Psi^+\rangle}$) based on[51]

$$\mathrm{QBER}_X^{|\Psi^-\rangle} = \frac{P_X^-(t, t+\Delta t)}{P_X^+(t, t+\Delta t) + P_X^-(t, t+\Delta t)}, \tag{1}$$

$$\mathrm{QBER}_X^{|\Psi^+\rangle} = \frac{P_X^+(t, t+\Delta t)}{P_X^+(t, t+\Delta t) + P_X^-(t, t+\Delta t)}, \tag{2}$$

$$\mathrm{QBER}_Z^{|\Psi^\pm\rangle} = \frac{P_Z^-(t, t+\Delta t)}{P_Z^+(t, t+\Delta t) + P_Z^-(t, t+\Delta t)}. \tag{3}$$

In addition, the phase difference of two subsequent time bins induced by frequency difference is

$$\theta = 2\pi\Delta\omega\Delta t = 2\pi(\omega_a - \omega_b)\Delta t = 2\pi c\Delta t\frac{|\lambda_a - \lambda_b|}{\lambda_a\lambda_b}, \tag{4}$$

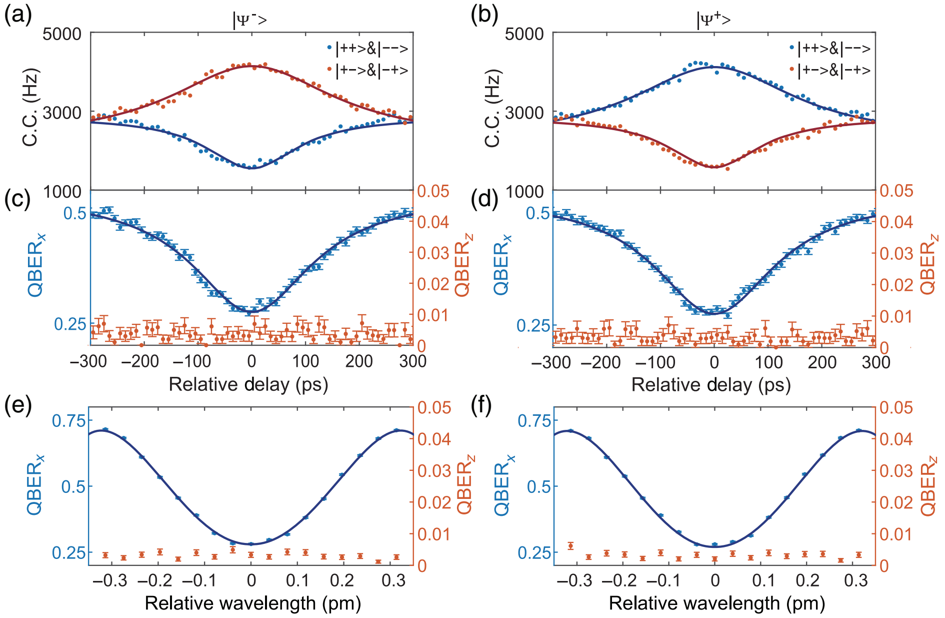

Fig. 3 Experimental results of optimal BSM and QBER. (a) BSM results of $|\Psi^-\rangle$. When Alice and Bob send the same states ($|++\rangle/|--\rangle$, blue dots), or different states ($|+-\rangle/|-+\rangle$, red dots), we obtain destructive and constructive interference in coincidence counts as functions of relative temporal delay, respectively. (b) BSM results of $|\Psi^+\rangle$. Note that the correlations between Alice and Bob are inverted comparing to $|\Psi^-\rangle$. (c), (d) The QBER in X-basis (blue) and Z-basis (red) for $|\Psi^-\rangle$ and $|\Psi^+\rangle$, respectively. (e), (f) The measured QBER in X-basis and Z-basis as a function of the wavelength detuning between two lasers for two different Bell states.

where c is the speed of light and ω_a (ω_b) and λ_a (λ_b) are the laser's frequency and wavelength of Alice (Bob), respectively. $P_X^-(t,t+\Delta t)/P_X^+(t,t+\Delta t)$ can be written as

$$P_X^{\pm}(t,t+\Delta t) = 1 \pm V \exp\left[-\tau^2\left(c\frac{|\lambda_a-\lambda_b|}{\lambda_a\lambda_b}\right)^2\right]\cos\theta, \tag{5}$$

where V is the visibility and τ is the coincidence window.

As for Z-basis, QBER$_Z$ always have the same formula for $|\Psi^-\rangle/|\Psi^+\rangle$. In Figs. 3(c) and 3(d), we show the measured QBER$_X^{|\Psi^-\rangle}$ and QBER$_X^{|\Psi^+\rangle}$ (blue) as functions of time delays between Alice and Bob, which show the minimum close to 0.25 at the zero time delay. For Z-basis, the measured QBER$_Z^{|\Psi^{\pm}\rangle}$ (red) are close to zero, showing the high quality of our system. In Figs. 3(e) and 3(f), we vary the relative central wavelength between Alice's and Bob's lasers. Also, we show the results for QBER$_X^{|\Psi^-\rangle}$ and QBER$_X^{|\Psi^+\rangle}$ as functions of the relative wavelength, respectively. The experimental data (blue dots) agree well with the theoretical prediction (blue curves).

5 Enhancing Key Rate with Time-Multiplexing

Although the full-recovery time of the detector determines the time-bin separation to be 12 ns, we can harness the time-multiplexed technique by inserting more pairs of time-bin pulses to enhance the key rate. This is particularly useful in high-loss communication applications. As shown in the insets of Fig. 4(a), we insert up to five bins within 12 ns with an equal temporal separation of 2 ns. By combining this

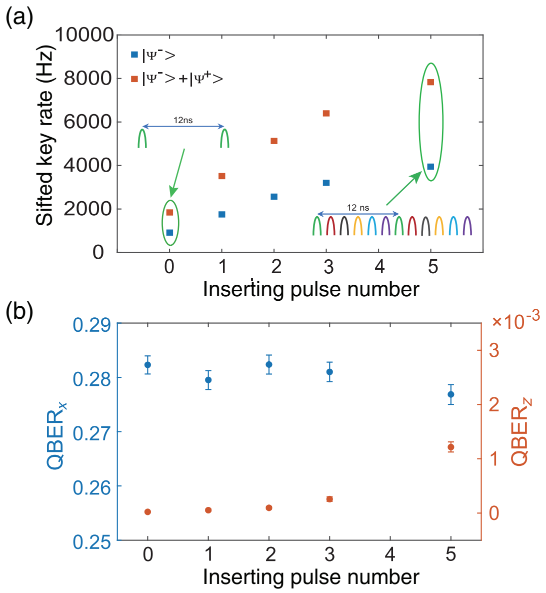

Fig. 4 Enhanced key rate by time-multiplexing. (a) The sifted key rate as a function of the inserted pulse number within the full-recovery time of SNSPD (12 ns). Red squares are the results of optimal BSM and blue squares are the results of $|\Psi^-\rangle$ only measurement. To compare fairly, in all the results presented here, Alice and Bob send the weak coherent pulses with the average photon number of 0.66 per pulse, and the total loss is 35.0 dB (including chip insertion loss ~4.5 dB). (b) QBER$_X$ and QBER$_Z$ versus inserting pulse number, indicating that time-multiplexing has little influence on error rate.

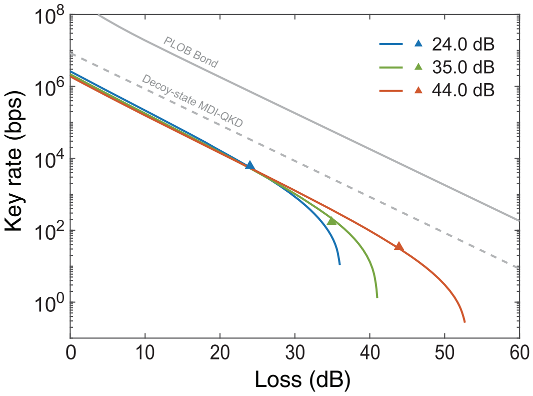

Fig. 5 The key rate at different losses including chip insertion loss. The solid lines show theoretical simulations and the triangle symbols show experimental results with a loss of 24.0, 35.0, and 44.0 dB, respectively. For different losses, the parameters (the intensities, s, μ, ν, and the probabilities of intensities, P_s, P_μ, P_ν) are different (see Supplementary Material for detailed parameters of theoretical simulations). The gray solid line: PLOB bond[55] and the gray dotted line: decoy-state MDI-QKD are numerical simulations (see Supplementary Material for details).

time-multiplexed technique and optimal BSM, we enhance the sifted key rate by almost an order of magnitude. At the same time, these two techniques have little impact on QBER$_X$ and QBER$_Z$, as shown in Fig. 4(b).

We demonstrate a complete MDI-QKD system including decoy states and phase randomization for guaranteeing the security[13–20,52,53] with our heterogeneously integrated, superconducting silicon-photonic platform. We use a four-intensity encoding protocol[52] with three intensities (μ, ν, o) in the X-basis for decoy-state analysis and one intensity (s) in the Z-basis for key generation. Finite-key effects are considered in the secure-key-rate analysis with a failure probability of 10^{-10}.[54] For statistical fluctuations, we use the joint constraints where the same observables are combined and treated together[52] (see Supplementary Material for details).

In this part of the experiment, we evenly insert two more pairs of time-bin qubits within 12 ns separation. Therefore, the effective clock rate of our system is tripled to 125 MHz (1/8 ns). The secure key rates for different losses are shown in Fig. 5. With the 125 MHz clock rate, we obtain the key rate of 6.166 kbps at the loss of 24.0 dB. This loss includes chip insertion loss ~4.5 dB. The actual transmission loss is about 19.5 dB, which corresponds to 98 km standard fiber. To the best of our knowledge, this is the highest secure key rate obtained experimentally with ~20 dB transmission loss in MDI-QKD, which is highly relevant in the context of a metropolitan quantum network without detector vulnerabilities. Furthermore, we obtain the secure key rates of 170 and 34 bps with total losses of about 35.0 and 44.0 dB. We emphasize that our secure key rates with the 125 MHz clocked system are very close to the best MDI-QKD experiments with a GHz clock rate.[31,56] In contrast with the GHz clock rate MDI-QKD experiments, our system does not require the complicated injection locking technique, which significantly reduces the complexity of the transmitter (see Table S1 in the Supplementary Material for detailed comparison).

6 Conclusion

We have demonstrated the first integrated relay server for MDI-QKD with a heterogeneous superconducting silicon-photonic chip. The excellent optical and electronic performance of this chip not only facilitates the experimental high-visibility HOM interference and low QBER, but also allows us to perform optimal BSM for time-bin qubits for the first time. Our work shows that integrated quantum-photonic chips provide not only a route to miniaturization but also significantly enhance the system performance more than traditional platforms. Our chip-based relay server can also be employed in twin-field QKD (TF-QKD),[57] which can overcome the rate-distance limit of QKD without quantum repeaters. TF-QKD is indispensable in long-distance intercity communication links. Moreover, the chip-based relay server with the MDI-QKD protocol presented in this work could be an ideal solution for a scalable trust-node-free metropolitan quantum network. Using more advanced waveguide-integrated SNSPDs,[45] one can further improve the integrated server with a high detection efficiency, low timing jitter, and high repetition rate. Combined with photonic-chip transmitters,[31,33] a fully chip-based, scalable, and high-key-rate MDI-QKD metropolitan quantum network should be realized in the near future.

Acknowledgments

We would like to thank R. Chen and A. Miller for helpful discussions. This research was supported by the National Key Research and Development Program of China (Nos. 2017YFA0303704, 2019YFA0308700, and 2017YFA0304002), the National Natural Science Foundation of China (Nos. 11690032, 11321063, and 12033002), the NSFC-BRICS (No. 61961146001), the Leading-Edge Technology Program of Jiangsu Natural Science Foundation (No. BK20192001), and the Fundamental Research Funds for the Central Universities.

References

1. H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science* **283**(5410), 2050–2056 (1999).
2. N. Gisin et al., "Quantum cryptography," *Rev. Mod. Phys.* **74**(1), 145–195 (2002).
3. V. Scarani et al., "The security of practical quantum key distribution," *Rev. Mod. Phys.* **81**(3), 1301–1350 (2009).
4. F. Xu et al., "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.* **92**(2), 025002 (2020).
5. S. Pirandola et al., "Advances in quantum cryptography," *Adv. Opt. Photonics* **12**(4), 1012–1236 (2020).
6. V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A* **74**(2), 022313 (2006).
7. Y. Zhao et al., "Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A* **78**(4), 042333 (2008).
8. L. Lydersen et al., "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nat. Photonics* **4**(10), 686–689 (2010).
9. M. Elezov et al., "Countermeasure against bright-light attack on superconducting nanowire single-photon detector in quantum key distribution," *Opt. Express* **27**(21), 30979–30988 (2019).
10. S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.* **108**(13), 130502 (2012).

11. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.* **108**(13), 130503 (2012).
12. A. Rubenok et al., "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Phys. Rev. Lett.* **111**(13), 130501 (2013).
13. Y. Liu et al., "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.* **111**(13), 130502 (2013).
14. Y.-L. Tang et al., "Measurement-device-independent quantum key distribution over 200 km," *Phys. Rev. Lett.* **113**(19), 190501 (2014).
15. Z. Tang et al., "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Phys. Rev. Lett.* **112**(19), 190503 (2014).
16. C. Wang et al., "Phase-reference-free experiment of measurement-device-independent quantum key distribution," *Phys. Rev. Lett.* **115**(16), 160502 (2015).
17. L. Comandar et al., "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nat. Photonics* **10**(5), 312–315 (2016).
18. H.-L. Yin et al., "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.* **117**(19), 190501 (2016).
19. C. Wang et al., "Measurement-device-independent quantum key distribution robust against environmental disturbances," *Optica* **4**(9), 1016–1023 (2017).
20. H. Liu et al., "Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels," *Phys. Rev. Lett.* **122**(16), 160501 (2019).
21. B. Fröhlich et al., "A quantum access network," *Nature* **501**(7465), 69–72 (2013).
22. R. J. Hughes et al., "Network-centric quantum communications with application to critical infrastructure protection," arXiv:1305.0305 (2013).
23. Y.-L. Tang et al., "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X* **6**(1), 011024 (2016).
24. Y. Fu et al., "Long-distance measurement-device-independent multiparty quantum communication," *Phys. Rev. Lett.* **114**(9), 090501 (2015).
25. C. Zhu, F. Xu, and C. Pei, "W-state analyzer and multi-party measurement-device-independent quantum key distribution," *Sci. Rep.* **5**(1), 17449 (2015).
26. F. Grasselli, H. Kampermann, and D. Bruß, "Conference key agreement with single-photon interference," *New J. Phys.* **21**(12), 123002 (2019).
27. Y. Ding et al., "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," *npj Quantum Inf.* **3**(1), 25 (2017).
28. D. Bunandar et al., "Metropolitan quantum key distribution with silicon photonics," *Phys. Rev. X* **8**(2), 021009 (2018).
29. C. Ma et al., "Silicon photonic transmitter for polarization-encoded quantum key distribution," *Optica* **3**(11), 1274–1278 (2016).
30. P. Sibson et al., "Integrated silicon photonics for high-speed quantum key distribution," *Optica* **4**(2), 172–177 (2017).
31. K. Wei et al., "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," *Phys. Rev. X* **10**(3), 031030 (2020).
32. C. Agnesi et al., "Hong–Ou–Mandel interference between independent III–V on silicon waveguide integrated lasers," *Opt. Lett.* **44**(2), 271–274 (2019).
33. H. Semenenko et al., "Chip-based measurement-device-independent quantum key distribution," *Optica* **7**(3), 238–242 (2020).
34. P. Sibson et al., "Chip-based quantum key distribution," *Nat. Commun.* **8**(1), 13984 (2017).
35. C.-Y. Wang et al., "Integrated measurement server for measurement-device-independent quantum key distribution network," *Opt. Express* **27**(5), 5982–5989 (2019).
36. G. Zhang et al., "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nat. Photonics* **13**(12), 839–842 (2019).
37. J. F. Tasker et al., "Silicon photonics interfaced with integrated electronics for 9 GHz measurement of squeezed light," *Nat. Photonics* **15**(1), 11–15 (2021).
38. S. Pirandola et al., "High-rate measurement-device-independent quantum cryptography," *Nat. Photonics* **9**(6), 397–402 (2015).
39. C. Ottaviani et al., "Modular network for high-rate quantum conferencing," *Commun. Phys.* **2**(1), 118 (2019).
40. J. Calsamiglia and N. Lütkenhaus, "Maximum efficiency of a linear-optical Bell-state analyzer," *Appl. Phys. B* **72**(1), 67–71 (2001).
41. J. A. W. van Houwelingen et al., "Quantum teleportation with a three-Bell-state analyzer," *Phys. Rev. Lett.* **96**(13), 130502 (2006).
42. F. Samara et al., "Entanglement swapping between independent and asynchronous integrated photon-pair sources," *Quantum Sci. Technol.* **6**, 045024 (2021)
43. W. H. Pernice et al., "High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits," *Nat. Commun.* **3**(1), 1325 (2012).
44. B. Korzh et al., "Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector," *Nat. Photonics* **14**(4), 250–255 (2020).
45. S. Ferrari, C. Schuck, and W. Pernice, "Waveguide-integrated superconducting nanowire single-photon detectors," *Nanophotonics* **7**(11), 1725–1758 (2018).
46. Y. Ding et al., "Fully etched apodized grating coupler on the SOI platform with −0.58 dB coupling efficiency," *Opt. Lett.* **39**(18), 5348–5350 (2014).
47. Y. Luo et al., "Low-loss two-dimensional silicon photonic grating coupler with a backside metal mirror," *Opt. Lett.* **43**(3), 474–477 (2018).
48. A. Gaggero et al., "Amplitude-multiplexed readout of single photon detectors based on superconducting nanowires," *Optica* **6**(6), 823–828 (2019).
49. A. J. Kerman et al., "Kinetic-inductance-limited reset time of superconducting nanowire photon counters," *Appl. Phys. Lett.* **88**(11), 111116 (2006).
50. R. Valivarthi et al., "Efficient Bell state analyzer for time-bin qubits with fast-recovery WSi superconducting single photon detectors," *Opt. Express* **22**(20), 24497–24506 (2014).
51. J. Jin et al., "Two-photon interference of weak coherent laser pulses recalled from separate solid-state quantum memories," *Nat. Commun.* **4**(1), 2386 (2013).
52. Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," *Phys. Rev. A* **93**(4), 042324 (2016).
53. Z. Zhang et al., "Improved key-rate bounds for practical decoy-state quantum-key-distribution systems," *Phys. Rev. A* **95**(1), 012333 (2017).
54. M. Curty et al., "Finite-key analysis for measurement-device-independent quantum key distribution," *Nat. Commun.* **5**(1), 3732 (2014).
55. S. Pirandola et al., "Fundamental limits of repeaterless quantum communications," *Nat. Commun.* **8**(1), 15043 (2017).
56. R. I. Woodward et al., "Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers," *npj Quantum Inf.* **7**(1), 58 (2021).
57. M. Lucamarini et al., "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature* **557**(7705), 400–403 (2018).

Xiaodong Zheng is a PhD student working under the supervision of Xiao-Song Ma at the School of Physics of Nanjing University (NJU). Currently, he is working on superconducting nanowire single-photon detection and quantum key distribution.

Peiyu Zhang received her MS degree from NJU in 2020. Currently, she is working on optical communication.

Renyou Ge received his PhD from Sun Yat-sen University in 2021. Currently, he is working on integrated optical devices.

Liangliang Lu received his BS degree from Guangzhou University in 2009 and his PhD from NJU in 2015. He worked as a researcher at the School of Physics of NJU from 2017 to 2020 and joined the School of Physical Science and Technology at Nanjing Normal University in November 2020. His research area is integrated photonic quantum information processing, including quantum simulation, quantum key distribution, and nonlinear optics.

Guanglong He is a PhD student working under the supervision of Labao Zhang at the School of Electronic Science and Engineering of NJU. Currently, he is working on superconducting nanowire single-photon detectors.

Qi Chen is a PhD student working under the supervision of Labao Zhang at the School of Electronic Science and Engineering of NJU. Currently, he is working on superconducting nanowire single-photon detectors.

Fangchao Qu received his MS degree from NJU in 2020. Currently, he is working on integrated circuits.

Labao Zhang received his PhD from NJU, Nanjing, China, in 2010. He is currently a professor at NJU. His current research interests include the phenomena and the physics of nanostructured superconductors.

Xinlun Cai received his PhD in electrical and electronics engineering from the University of Bristol, Bristol, UK, in 2012. He is currently a professor at the School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, China. His research is mainly focused on optical communication and photonic integrated devices.

Yanqing Lu received his BS and PhD degrees from NJU, Nanjing, China, in 1991 and 1996, respectively. He has 5 years of experience in the U.S. and China telecom industries. He designed and developed a serial of liquid-crystal-based fiber-optic devices with his colleagues, which include variable optical attenuators, variable Mux/Demux, and DWDM wavelength blockers. He is currently a Changjiang distinguished professor at NJU. His research interests include liquid crystal photonics, nonlinear optics, and quantum optics.

Shining Zhu is a professor at the School of Physics and a principal investigator at the National Laboratory of Solid State Microstructures, NJU, Nanjing, China. He is an academician of the Chinese Academy of Sciences (CAS) and a fellow of Optical Society of America, Chinese Optical Society, and American Physical Society, respectively. His research interests include microstructured functional materials, nonlinear optics, laser physics, quantum communication, and integrated quantum optics.

Peiheng Wu received his PhD in physics from NJU, Nanjing, China, in 1961. He has been a professor at NJU, since 1985 and an academician at the CAS, Beijing, China, since 2005. From January 2001 to July 2001, he was a professor with RIEC, Tohoku University, Sendai, Japan. His research interests include superconducting electronics, high-frequency techniques, and their applications.

Xiao-Song Ma received his BS degree from NJU in 2003 and his PhD from the University of Vienna in 2010. He worked as a postdoc fellow at the University of Vienna and Yale University from 2010 to 2015. He joined the School of Physics at NJU as a professor in 2015. His research interests include quantum communication, quantum network, quantum simulation and computation, solid-state quantum memory, and integrated photonic quantum technologies.