PHOTONICS Research

Resource-efficient quantum key distribution with integrated silicon photonics

Kejin Wei,[1,4,†] Xiao Hu,[2,†] Yongqiang Du,[1] ⓘ Xin Hua,[2,3] Zhengeng Zhao,[1] Ye Chen,[1] Chunfeng Huang,[1] and Xi Xiao[2,3,5]

[1]Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning 530004, China
[2]National Information Optoelectronics Innovation Center (NOEIC), Wuhan 430074, China
[3]State Key Laboratory of Optical Communication Technologies and Networks, China Information and Communication Technologies Group Corporation (CICT), Wuhan 430074, China
[4]e-mail: kjwei@gxu.edu.cn
[5]e-mail: xxiao@wri.com.cn
[†]These authors contributed equally to this work.

Integrated photonics provides a promising platform for quantum key distribution (QKD) system in terms of miniaturization, robustness, and scalability. Tremendous QKD works based on integrated photonics have been reported. Nonetheless, most current chip-based QKD implementations require additional off-chip hardware to demodulate quantum states or perform auxiliary tasks such as time synchronization and polarization basis tracking. Here, we report a demonstration of resource-efficient chip-based BB84 QKD with a silicon-based encoder and a decoder. In our scheme, the time synchronization and polarization compensation are implemented relying on the preparation and measurement of the quantum states generated by on-chip devices; thus, we need no additional hardware. The experimental tests show that our scheme is highly stable with a low intrinsic quantum bit error rate of 0.50% ± 0.02% in a 6 h continuous run. Furthermore, over a commercial fiber channel up to 150 km, the system enables the realization of secure key distribution at a rate of 866 bit/s. Our demonstration paves the way for a low-cost, wafer-scale manufactured QKD system.   © 2023 Chinese Laser Press

https://doi.org/10.1364/PRJ.482942

1. INTRODUCTION

Quantum key distribution (QKD) has been believed as a promising tool providing theoretic information security without any restrict on the eavesdropper's computing power. Since the first QKD scheme, named BB84 protocol [1], was proposed by Bennett and Brassard in 1984, QKD has attracted a lot of interests and achieved a rapid development. So far, several QKD theoretical schemes have been proposed to improve performance or enhance security [2–9]. Experimentally, QKD has been widely implemented toward long distances [10], GHz repetition rates [11,12], field tests [13], and large-scale networks [14,15]. The recording transmission distance of QKD was pushed up to 830 km installed fiber [16]. Recently, important breakthroughs were achieved in the demonstration of device-independent QKD [17–19]. Recent researches have focused on making QKD systems simpler, more compact, and lower-cost for widespread deployment [20,21].

Integrated photonics is a natural solution to realize miniature QKD [22,23]. In particular, QKD chips relying on well-established integrated techniques have been fabricated to realize key QKD devices [24–28]. The reliability of chip-based QKD devices has also been demonstrated by implementing several QKD protocols, including decoy-state BB84 [27,29–35], high dimensions [36,37], continuous variables [38], and measurement-device-independent QKD [39–42]. These achievements open the way to implant QKD into telecommunication networks. See Ref. [43] for a recent review for advance in chip-based QKD.

Until now, however, chip-based QKD experiments have two substantial limitations. First, although remarkable advances in quantum integrated devices enable chip-based demonstration of QKD, it requires additional off-chip hardware to perform auxiliary tasks in the process. For example, in a recently reported multichip QKD system [44], the time synchronization between Alice and Bob is realized using an additional classical light synchronization setup. In the photonics polarization decoder presented in Ref. [34], a bulk fiber-based polarization controller is used to track polarization basis and to compensate polarization drift.

Second, despite that standard silicon photonic fabrication provides a feasible way to realize mutlifunctional devices for manipulation of quantum states, it is hard to fabricate some integrated components for quantum applications. For example,

some prior works involving chip-based polarization-encoding systems still use discrete optics devices to demodulate the quantum states due to the difficulty of achieving integrated polarization manipulation devices [29,31,33,40]. Hence, building a fully deployed QKD system is still challenging.

In this work, we present a resource-efficient chip-based polarization-encoding QKD scheme in which key distribution and all auxiliary tasks are realized using the same chip devices. The scheme is implemented using a chip-based encoder and a decoder that are manufactured by a standard Si photonic platform. The time synchronization and polarization drift compensation are performed exploiting a qubit-based method, which relies on the quantum states generated by the chip devices. The scheme experimentally shows an average quantum bit error rate (QBER) of 0.50% ± 0.02% and high stability in the 6 h continuous operation. Furthermore, we successfully generate secure bits over different fiber channel lengths, up to 150 km fiber spool with a finite key rate of 866 bit/s. This study paves the way for low-cost, wafer-scale manufactured QKD systems and provides a promising solution for making chip-based systems simple.

2. SETUP

Our chip-based BB84 QKD system is schematically shown in Fig. 1. Alice prepares decoy-state BB84 polarization states on a chip-based transmitter and distributes the states to Bob, who possesses a chip-based receiver, via an optical fiber link.

Alice generates low-jitter phase-randomized light pulses at a repetition rate of 50 MHz and a center wavelength of 1550 nm. The generated pulses are coupled into a Si photonic encoder chip [see Fig. 1(b)], which integrates together an intensity modulator (IM) and a path-to-polarization modulator (Pol-M).

The components consist of interferometric structures, which exploit standard building blocks offered by the commercial fabrication foundry. The multimode interference (MMI) couplers act as symmetric beam splitters, and the thermo-optics phase shifters (PSs) with ∼5 kHz bandwidth and the carrier-depletion modulators (CDMs) with ∼5 GHz bandwidth act as phase modulators.

The first interferometric structure, realizing a Mach–Zehnder interferometer (MZI), is used to realize an IM. The IM is used to generate different intensities, one intensity μ for signal state and another one ν for decoy state. The ratio μ/ν is set by both DC-bias of the PSs and the RF signals sent to the CDMs of the MZI.

The output of IM is connected to Pol-M, which functions by means of a path-to-polarization converter. The structure combines an inner MZI with two external CDMs, ending in a two-dimensional grating coupler (2-D). The 2-D, acting as a polarization rotator combiner, converts the path-encoding information at each arm of the MZI into polarization-encoding information at the output. The Pol-M enables the preparation of the four BB84 polarization states, $|\psi\rangle = (|H\rangle + e^{i\theta}|V\rangle)/\sqrt{2}, \theta \in \{0, \pi/2, \pi, 3\pi/2\}$, where $\theta \in \{0, \pi\}$ ($\theta \in \{\pi/2, 3\pi/2\}$) represents the states in Z (X) basis. More details about chip design as well as work principle can be found in Ref. [33].

All the operation of Alice's devices, including triggering the laser and applying voltage on the IM and Pol-M, is controlled by arbitrary waveform generators (AWGs) and homemade time delay generators (Delayer). Alice's encoding pulses are sent to the silicon-based measurement setup in Bob.

The transmitted signals are coupled into Bob's decoder chip [see Fig. 1(c)] via spot-size converter (SSC). The decoder chip then converts the polarization-encoding photons to the
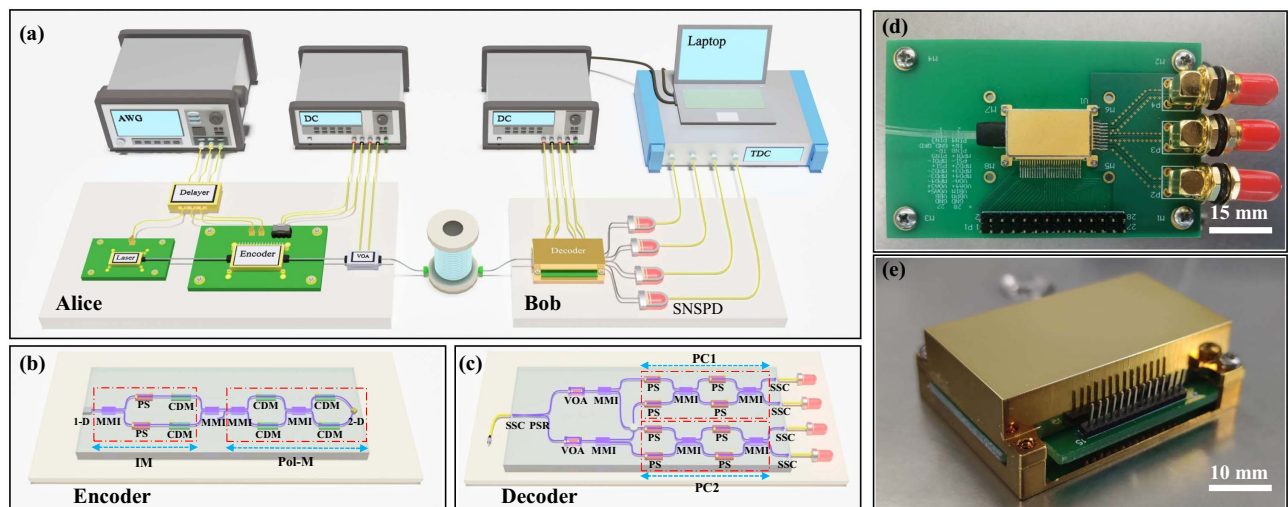

Fig. 1. Silicon-based QKD system. (a) Schematic of the QKD setup. Laser, laser diode; Encoder, silicon chip integrating an intensity modulator and a polarization state modulator; VOA, variable optical attenuator; Decoder, polarization state demodulation chip; SNSPD, superconducting nanowire single photon detector; TDC, time digital converter; AWG, arbitrary waveform generator; DC, programmable DC power supply; Delayer, home-made time delay generator. (b) Schematic of the encoder. MMI, multimode interferometer; PS, thermo-phase shifter; CDM, carrier-depletion modulator; 1-D, one-dimensional grating coupler; 2-D, two-dimensional grating coupler; IM, intensity modulator; Pol-M, polarization modulator. (c) Schematic of the decoder. SSC, spot-size converter; PSR, polarization splitter-rotator. (d) Picture of the packaged encoder chip soldered to the external control board. (e) Picture of the packaged decoder chip soldered to the external control board.

on-chip path encoding via a polarization splitter-rotator (PSR). Therefore, these photons passively choose the measurement bases of Z or X via a symmetric MMI. The quantum measurement in Z (X) base is constituted by a polarization controller measurement state PC1 (PC2). Each PC contains two MMIs and four thermal PSs. By fine-tuning the applied voltages, supplied by a DC power supply, on PSs, the PC1 and PC2 constitute the quantum measurement in Z and X basis, respectively. Further information about the principle of the polarization state analysis by the decoder chip for the BB84 protocol can be found in Ref. [45].

After configuring the measurement basis in PCs, the photons are detected by four commercial superconducting nanowire single photon detectors (SNSPDs, Photon Technology Co., Ltd.). The SNSPDs are cooled down to 2.1 K and have an detection efficiency of around 75%, dead time of ~40 ns, time jitter of ~70 ps, and dark counts of ~25 Hz. The detection events are registered using a high-speed time tagger (Timetagger20, Swabian Instruments). The local clock reference for Bob is generated by using the internal clock in the time digital converter (TDC). A laptop then reads the TDC data and processes it for time synchronization and polarization drift compensation. The encoder is triggered by a programmable DC power supply.

The encoder and decoder chips are fabricated using stand silicon photonics foundry services with an in-house design. The encoder and decoder have a footprint size of 6 mm × 3 mm and 1.6 mm × 1.7 mm, respectively. The encoder chip is butterfly packaged with a total volume of 20 mm × 11 mm × 5 mm and then soldered to a standard 9 cm × 7 cm printed circuit board, as shown in Fig. 1(d). The decoder chip is packaged using a chip-in-board assembly with a total volume of 3.95 cm × 2.19 cm × 0.90 cm, as shown in Fig. 1(e). With a dedicated layout, the chip is easily assembled by a commercial foundry, providing a low-cost, portable, stable, and miniaturized device. Details for the encoder and decoder chip designs and fabrications can be found in Appendix A.

Different from the conventional optical or electrical time synchronization methods, we apply a qubit-based method to synchronize two remote users' clocks. This method enables synchronizing the clocks using the transmitted quantum signal states. This means that our setup does not require a synchronization subsystem, which normally consists of a pulsed laser and a photonic detector, as utilized in pioneering works [46–48]. We remark that removing the synchronization subsystem is extremely crucial for building a fully chip-based QKD system since the development of an on-chip laser source remains a great challenge on Si photonics research [49].

The main goal of the time synchronization is to recover the specific frequency of the qubits arriving at the detectors and the time-offset of corresponding qubits between Alice and Bob. The main idea of our algorithm is similar to a recently proposed Qubit4Sync algorithm [50] except the method of recovering the absolute time-offset; instead of implementing public periodic-correlation codes in the first L states, we divide those codes into single bits and then periodically and cyclically embed them in prepared states. The detailed description of our synchronization method is presented in Appendix B. Here, we describe the main features of our algorithm as follows.

Our approach first computes the frequency from the time-of-arrival measurements based on fast Fourier transform. To recover the absolute time-offset, Alice prepares a random qubit string, which is periodically and cyclically embedded with several public known bits from periodic-correlation codes with a length of L. Then each bit, according to a preset ratio M, is sequentially inserted into random encode bits. For example, supposing that $M = 9{:}1$, every 10 bits contain 9 random bits that are embedded with a single bit from periodic-correlation codes of length L. When the L bits are consumed, the periodic-correlation codes are cyclically reused. By correlating these periodic-correlation codes with the one received by Bob, it is possible to distinguish which state received by Bob is the first one sent by Alice. The absolute time-offset of the first qubit can be obviously derived. This is the typical frame-synchronization technique used in digital communication systems [51].

Our algorithm periodically inserts the synchronization string in the random data stream so that Bob can execute the qubit synchronization algorithm at any time and quickly reestablish synchronization when the system is out of step. This allows the system to continuously accumulate the bit string for a long time up to 6 h.

After recovery time synchronization, we can further perform polarization compensation using a shared qubit string. We note that, due to the environmental disturbance, the polarization state of the transmitted photon is rotating unpredictably along fiber channel. This polarization variation would lead to a mismatch between Alice and Bob's reference frames and result in a high QBER and low secure key rate. To eliminate it, a polarization compensation subsystem, which typically includes an auxiliary laser and several electronic polarization controllers, must be utilized.

In our scheme, since the POVMs in the Z and X bases are set by actively tuning PSs at the stages of PC1 or PC2, this enables the polarization basis tracking and, hence, allows our system to compensate polarization rotation.

Here, similar to the work in Refs. [20,52], we use a qubit-based polarization compensation method that employs a shared qubit string. The shared qubit strings are generated using the chip-based transmitter and receiver; hence, it does not need additional hardware. The idea is that Bob directly evaluates the QBER in Z and X basis from the public string after performing the time synchronization process. The estimated QBERs are then put into an optimization algorithm (based on gradient descent algorithm), which is running in Bob's laptop. The laptop then adjusts the applied voltages of PS in PC1 and PC2 using a programmable linear DC source. Taking advantage of the gradient descent optimization algorithm, the voltages applied on PSs in PC1 and PC2 are tuned in real time to suppress QBER. The process is continuously running until the estimated QBER is lower than the preset threshold.

3. EXPERIMENTAL RESULTS

A. Characterization of Components

We first experimentally characterize each component in the encoder chip. At a frequency of 50 MHz, the IM provides a static extinction ratio (ER) of approximately 27 dB and a dynamic ER of approximately 18 dB, which meets the require-

ment of the one-decoy method [53]. The produced polarization states are analyzed with the decoder by Bob. The PCs are calibrated to Z (X) basis. We obtain an average polarization ER of ~23 dB. The performance of the chip ensures realizing a low-error, high-rate QKD system.

The 3 dB bandwidths of CDM and PS, which are key parameters evaluating the performance of the IM, Pols and PC, are measured. The 3 dB bandwidth of CDM is tested by measuring the eye diagram, and a value of approximately 10 GHz is obtained, which is consistent with design. The 3 dB bandwidth of PSs is approximately 3 kHz. This value ensures that the decoder has a fast polarization tracking speed in field-buried and aerial fibers.

The total loss of the decoder chip is approximately 4.6 dB. The source of loss includes coupling-in and -out loss (~3 dB), as well as on-chip device propagation loss (~1.6 dB). The MMI and waveguide bends contribute mostly to the propagation loss. The loss in the decoder chip reduces the probability of detecting photons, thus compromising the secure bit rate of the QKD system.

B. Intrinsic QBER and Stability

We first report the intrinsic QBER and stability of our QKD setup, which gives a quantitative first look of the performance of our setup. Furthermore, the characterization is crucial to predict the secure key rate under different channels or detector technologies. We first remove the fiber spool and then send a sequence of qubits prepared using the method described in Section 2. The total length of periodic-correlation codes $L = 5 \times 10^4$ and the ratio M is set to 9:1. The transmitted states are analyzed, including time synchronization performance as well as QBER estimation, using the measurement devices in Bob. The intensity of signal μ is set to a constant value of 0.5. The experimental results are shown in Fig. 2, which shows, in a 6 h testing time, an average $QBER_z$ is measured to be 0.78% ± 0.02% for the Z basis, while for X basis, the average $QBER_x$ is 0.22% ± 0.04%. The total QBER for both two bases is 0.50% ± 0.02%. These results demonstrate

the low intrinsic QBER and high stability of our setup. Due to different applied voltages on CDMs for the preparation of the four polarization states, the phase-dependent loss characteristics and saturation of the CDMs result in a discrepancy in the QBERs of Z and X. Since the data are contentiously collected, these results demonstrate the time synchronization method works well in a long-time run.

C. Polarization Compensation of 50 km Fiber Spool

To test the performance of the polarization compensation method, we continuously run the system with a 50 km fiber spool channel. We exploit a fiber polarization scrambler, of which the applied voltages are step-by-step increased 1 V every 5 min, to mimic the polarization rotation of photons in long fiber spool. With our polarization feedback algorithm, we are able to compensate the polarization drifting to a low QBER within 1 min. For comparison, we also measure the QBERs without activating the polarization feedback.

The experimental results are shown in Fig. 3. It can be observed that, for 2.4 h continuous run, due to the polarization drift introduced by the environmental distance and polarization scrambler, the QBERs for Z and X basis gradually increase to 50% without active polarization feedback. In this stage, no secure key bits can be extracted. In contrast, with our polarization feedback process, the QBERs keep stable and stay at a low level of around 0.85% for 2.4 h run.

D. QKD Secure Key Rate for Different Fiber Channel Lengths

Using the described setup, we perform a series of one-decoy QKD experiments with different fiber spool lengths of 50 km, 100 km, and 150 km. To get a better performance, we perform a full optimization of the implementation parameters for the one decoy-state protocol [54]. For example, in the scenario of 100 km, the intensities of the signal states and decoy state are chosen to be $\mu = 0.565$ and $\nu = 0.143$, respectively. The
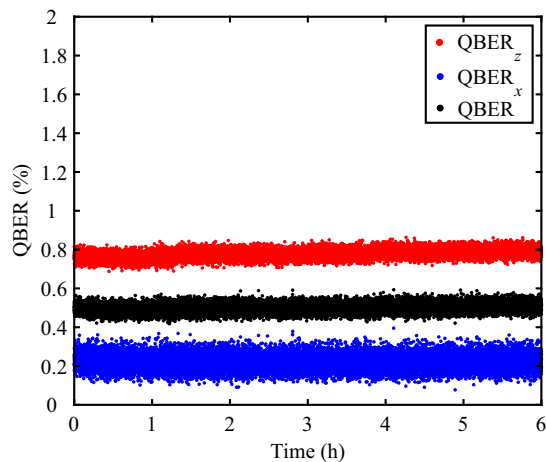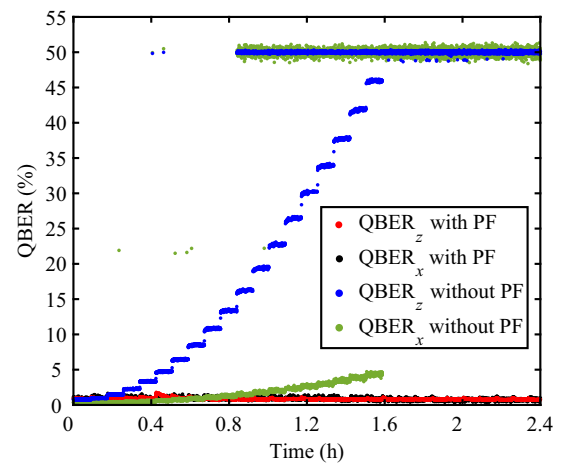
Fig. 2. QBER on Z (X) basis of the system without active feedback over 6 h. The red (blue) points represent the quantum bit error in Z (X) basis. Each point is refreshed every 1 s.

Fig. 3. QBER measurements for a 50 km fiber channel over 2.4 h operation. During the measurement process, an increased voltage at a step of 1 V is applied to the fiber scrambler every 5 min to mimic the polarization drift of the fiber channel. The black (red) and green (blue) dots represent the measured $QBER_x$ ($QBER_z$) with and without polarization feedback (PF), respectively. With the PF, $QBER_x =$ 0.86% ± 0.17% and $QBER_z$ is 0.84% ± 0.13%.

Table 1. Overview of Experimental Parameters and Performances for Different Distances[a]

L (km)	Loss (dB)	μ	ν	n_z	t (s)	τ_b (ns)	QBER$_z$	ϕ_z^U	$s_{z,1}^L$	SKR (bit/s)
50	9.957	0.568	0.144	10,241,262	42.3	$20.0 \pm 5.4 \times 10^{-9}$	0.653%	0.0224	5,280,589	8.96×10^4
100	18.857	0.565	0.143	10,021,841	317.8	$20.0 \pm 1.2 \times 10^{-8}$	0.764%	0.0177	5,155,932	1.18×10^4
150	28.992	0.564	0.142	10,078,187	3640.4	$20.0 \pm 1.9 \times 10^{-7}$	1.358%	0.0270	5,317,027	8.66×10^2

[a]L and loss are the channel length and channel loss, respectively. μ (ν) is the intensity of the signal (decoy) state, n_z is the amount of data accumulated on the Z basis, t is the total accumulated time, τ_b is the period measured by Bob, QBER$_z$ is quantum bit error rate of Z basis, ϕ_z^U is the upper bound of phase error rate, $s_{z,1}^L$ is the lower bound for measuring single-photon events in the Z basis, and SKR is the final secure key rate.

probabilities of sending out the signal state μ and choosing the bases Z are $P_\mu = 0.798$ and $P_z = 0.944$, respectively. At Bob's side, the probabilities of choosing the measurement basis in Z and X are permanently set to be equal due to the balanced MMI used in the decoder.

For each distance, the total length of periodic-correlation codes is of 5×10^4, and the ratio M is set to 9:1. We continuously accumulate the detection numbers n_z of approximately 10^7 and perform the finite key analysis using [53]

$$R \leq (s_{z,0}^L + s_{z,1}^L(1 - h(\phi_z^U)) - \text{leak}_{EC}$$
$$- 6\log_2(19/\epsilon_{sec}) - \log_2(2/\epsilon_{cor}))/t, \qquad (1)$$

where t is the time duration of each acquisition, $s_{z,0}^L$ is the lower bound of the detector event received by Bob when Alice sends a vacuum state in Z basis, and $s_{z,1}^L$ is the lower bound of the detection event, given that Alice only sends a single-photon state in the Z-basis. ϕ_z^U is the upper bound of the phase error rate, leak$_{EC}$ is the number of bits consumed for error correction, and ϵ_{sec} and ϵ_{cor} are the parameters used to evaluate secrecy and correctness, respectively. The $h(x)$ denotes the Shannon binary information function.

An overview of experimental parameters and performances for different distances is listed in Table 1. The experimental results are also plotted in Fig. 4. It can been seen that we successfully run QKD up to 150 km; with a continuous accumulated time of 3640.4 s, a finite key rate of 866 bit/s is obtained. These results also demonstrate that our qubit-based synchronization and polarization compensation methods work well even in a high loss fiber channel and a long running time. The detailed experimental results are listed in Appendix C.
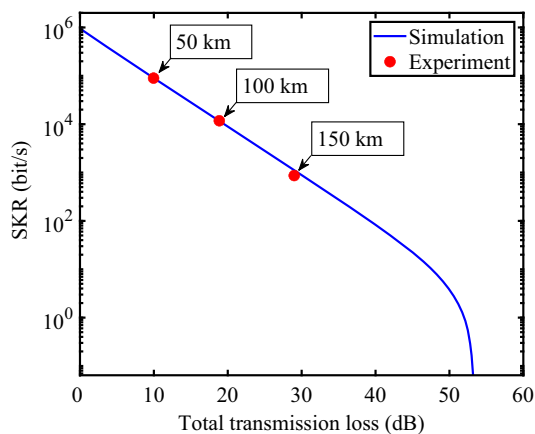

Fig. 4. Secure key rates with different transmission loss. The blue line represents the simulation results based on our experimental parameters, and the red dots represent the experimental results.

4. DISCUSSION

We have demonstrated a resource-efficient fully chip-based BB84 QKD scheme. The scheme implemented the time synchronization and polarization compensation using on-chip devices, which generates also secure keys for quantum communication. The system can distill a finite key secure bit rate of 866 bit/s over up to 150 km fiber spool. Limited by the driving circuit, which only supplies maximum peak-to-peak voltage $V_{pp} = 10$ V at a repetition rate of 50 MHz, the current system works at a repetition rate of 50 MHz and has a relatively low key rate. The obtained key rate can be further increased by using a state-of-the-art high-speed modulator driving circuit [55]. The presented system can be further integrated with the laser based on wire-bounding or the hybrid integration technologies [56,57], which contributes to a compact chip-scale QKD transmitter. Since CDMs are used to modulate the phase, it inevitably introduces the phase-dependent losses. To solve this problem, a polarization-loss-tolerant protocol [58,59] can be incorporated into our work, or novel phase modulation schemes provided in Refs. [28,48,60] can be employed. This work paves the way for a low-cost, robust wafer-scale manufactured QKD system and provides a promising scheme for developing simple chip-based systems.

Note: During the preparation of this manuscript, the authors noticed that a related work which presented a high-speed integrated QKD system [61] has been released. Although both works involve the chip-based QKD system, there are several differences. First, in contrast to the use of a time-bin encoding scheme, our work employs a polarization encoding scheme, which does not require the maintenance of interferometric stability that would be necessary in time-bin encoding. Additionally, polarization encoding is also a favored choice for the deployment of quantum networks and free-space QKD, especially for ground-to-satellite QKD.

Second, the receiver chip in Ref. [61] was fabricated on an aluminum borosilicate glass process platform, whereas we use CMOS-compatible silicon photonics technology, which has advantages of high-density integration and mature fabrication processing. Third, Ref. [61] realized synchronization by using classical communication between two field-programmable gate arrays (FPGAs), while our work uses a low-cost and efficient qubit synchronization approach.

APPENDIX A: ENCODER AND DECODER DESIGN AND FABRICATION

The encoder chip has a device footprint of 3 mm × 6 mm. The device is fabricated on a high-resistance silicon-on-insulator wafer with a 220 nm thick silicon layer and 3 μm thick buried oxide. The width of the routing silicon waveguide was 450 nm.

The light was coupled in/out of the device via 1-D and 2-D grating coupler, respectively. The 2 × 2 MMI couplers were designed as around 8 μm × 60 μm to get a nearly balanced splitting ratio. All the thermal-optical PSs are identical with a length of 260 μm, which efficiently result in a static extinction of around 28 dB when implemented in MZIs. Note that, in the experiment, only one PS on one arm in each MZI was active, and the other PS was designed for the compensation of 0.05 dB loss.

All CDMs are identical as well. The active CDMs have a length of about 3 mm. The doping concentration of the P- and N-type region is about 8×10^{17} cm^{-3} [62]. Intermediate P+ and N+ doping regions of concentrations of 3×10^{18} cm^{-3} are added 220 nm away from the PN junction to reduce the series resistance and optical loss. The two PN junctions of CDMs are connected in series to form a push–pull configuration, which is beneficial to decreasing the capacitance and improving the impedance matching. Experimentally, the MZIs were biased with PSs, the CDMs inside MZIs were operated at high-speed with ground-signal-ground (GSG) traveling wave electrode. The estimated 3 dB bandwidth of the device was around 20 GHz. The half-wave voltage was smaller than 6 V. The aluminum DC pad pitch was about 150 μm. The pad area was about 80 μm × 100 μm.

The decoder chip has a device footprint of 1.6 mm × 1.7 mm. The device is fabricated on a standard silicon-on-insulator wafer with a 220 nm silicon layer and a 3 μm buried silica oxide layer. The width of the single-mode silicon waveguide was 450 nm.

The light is coupled into/out of the device via an SSC with a taper length of approximately 100 μm and then split and converted into transverse electric (TE) modes using a compact PSR [63]. The PSR comprises the following two functional parts: TM$_0$–TE$_n$ mode converter and TE$_n$–TE$_0$ mode converter. The ERs of TM$_0$ and TE$_0$ modes of PSR are more than 17 dB over a wavelength range from 1520 to 1620 nm. The principle of the TM$_0$–TE$_n$ mode converter is the mode hybridization of the tapered rib waveguides, while the TE$_n$–TE$_0$ mode converter, acting as a PSR, is realized through the beam shaping method. The further details of operation principle can be found in Refs. [63] and [64]. The variable optical attenuators (VOAs) function based on the forward carrier injection PIN junction, and the value of attenuation is increasing with the applied voltage. The length of the VOA is approximately 200 μm. The 1 × 2 MMI and 2 × 2 MMI couplers are designed to be approximately 4 μm × 14 μm and 8 μm × 60 μm, respectively, to obtain a balanced splitting ratio. All eight PSs are identical, with a length of 260 μm, which efficiently results in a static extinction of approximately 28 dB when implemented in MZIs. Notably, in real-time, only one PS on one arm in each MZI was active, and the other PS is designed for the compensation of a 0.05 dB loss. The pitch of the aluminum DC pad is approximately 150 μm. The pad area is approximately 80 μm × 100 μm.

APPENDIX B: QUBIT-BASED SYNCHRONIZATION METHOD

Here we describe our qubit-based synchronization method in detail. The main goal of the time synchronization is to recover
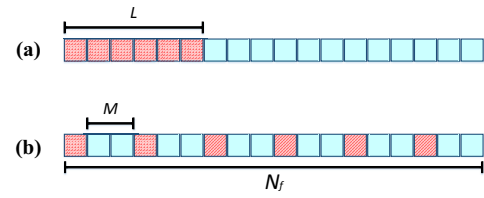

Fig. 5. The way Alice sends a synchronization string is shown. The red and blue squares represent single bits of the synchronization and random string, respectively. (a) Qubit4Sync. Alice first sends a synchronous string of length L and then sends a random string for QKD. (b) Our method. Alice divided the synchronization string of length L into L single bits, and each bit is followed with M random bits to form a block. L blocks build the synchronization frame of length $N_f = (M + 1)L$, which contains the complete synchronization string.

the specific frequency of the qubits arriving at the detectors and the time-offset of corresponding qubits between Alice and Bob. The main idea of our algorithm is similar to a recently proposed Qubit4Sync algorithm [50] except for the way of placing the correlation codes, aiming at recovering the absolute time-offset. Suppose that Alice sends a qubit string that consists of several qubit frames with a length of N_f. We define L as the total length of the synchronization string s^A in each frame. In the Qubit4Sync algorithm, as shown in Fig. 5(a), public periodic-correlation codes are encoded in the first L states; in contrast, the codes with a length L are divided into single bits and are then periodically embedded in prepared states in our method, as shown in Fig. 5(b). The detailed process is explained as follows.

As shown in Fig. 5(b), Alice first generates correlation codes s^A of length L and then divides them into L single bits. Each bit is then connected with M random bits. These qubit strings are sent to Bob via a lossy channel. Bob performs time synchronization based on the received qubits. That is, Bob needs to determine the expected time of arrival t_a^e, which can be expressed as

$$t_a^e = t_0 + n_a \tau^B + \epsilon_a, \quad n_a \in \mathbb{N}, \tag{B1}$$

where n_a is the order number of the sent qubit in Alice's raw key, a denotes the ath detection, t_0 is the initial time-offset, and ϵ_a is a variable satisfying normal distribution, whose expectation value is zero and variance is σ^2.

We first describe how Bob recovers the clock time τ^B from the received signal. Bob performs a fast Fourier transform of the
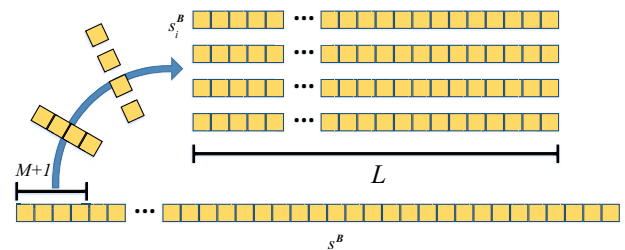

Fig. 6. Schematic of reverse-processing s^B. Bob's string s^B is divided into L blocks of length $M + 1$ and reshaped into an $(M + 1) \times L$ matrix. Each row of the matrix reconstructs a bit string s_i^B.

time-of-arrival signal. Similar to Ref. [50], we sample the time of the received signal with a sampling rate of $4/\tau^A$, where τ^A is the clock time of Alice for sending the light pulse. The number of samples for the fast Fourier transform is set to $N_s = 10^6$. At this stage, Bob gets a primary estimation τ_0^B of τ^B with an error of approximately $4\tau^A/N_s$. To get a more accurate value, the sampled signals are then fed into the least trimmed squares algorithm to get an accurate clock time, which satisfies

$$\frac{1}{D}\sum_{b=1}^{D}|\mathcal{E}_a^I(b)|^2 \simeq \sigma^2. \tag{B2}$$

Here $\mathcal{E}_a = t_a^m - t_a^e$ indicates the time-interval error, t_a^m is the measured time of arrival with $a \geq 1$, in Bob site, and $\mathcal{E}_a^I(b) = \mathcal{E}_{a+b} - \mathcal{E}_a$ denotes the time-interval error between two different detections a and $a + b$. $\mathcal{E}_a^I(b)$ can help Bob measure the accuracy of the period recovery.

Now we describe how to calculate the time-offset t_0 from the detections. It should be known that, once τ^B is identified, Bob has the correct index difference $n_{a+1} - n_a$. Due to the losses of channel, it is unlikely that the first photon in the pulse is detected by Bob. So Bob makes a first guess t_0^A about the value of t_0, where t_0^A is regarded as Bob's first detection as well as the first pulse sent by Alice.

In order to precisely determine t_0, Bob should calculate the correlation between the received signal and the public synchronization string s^A. The synchronization string is only encoded on the Z basis, and we assign the values $+1$ and -1 to the H and V state, respectively. Once the period τ^B is determined, Bob makes a first guess of t_0 and then extracts the detection for generating a string s^B with values $+1$, -1, and 0, in which the value of 0 denotes no detection or a detection in X basis. Note that s^B has a length of N_f. Evidently, s^B must contain the detections of a complete synchronization string of length L.

As shown in Fig. 6, Bob can reversely process s^B according to the frame structure shown in Fig. 5(b). Bob first separates the detection string s^B into L blocks of length $M + 1$ and then fits them into an $(M + 1) \times L$ matrix. Each row of the matrix constructs a string s_i^B with a length of L, where $i \in \{1, 2, ..., M + 1\}$. By calculating the cross correlation

between the s^A and s_i^B, Bob can determine the optimal detection string $s_{i_{\text{opt}}}^B$, which offers a maximum value of cross correlation. The cross correlation calculation between $s_{i_{\text{opt}}}^B$ and s^A can be accelerated using the matrix manipulation described in Ref. [50]. With the optimal value of the cross correlation, an accurate time-offset between Alice and Bob can be defined as illustrated in Ref. [50]. For a good offset recovery, the length of s^A should satisfy the following inequality: $\sqrt{L\eta} \geq 10$, where η is the total transmittance. When the system has a very high channel loss, we also can overcome the loss by repeating synchronization string detections. This avoids increasing the length L of the synchronization string. The efficiency of QKD can further improved by using a shorter length of s^A; however, to ensure the correct execution of the synchronization algorithm, it cannot be indefinitely diluted. This is determined by two factors: the time duration of system frequency stability and the total transmission loss.

APPENDIX C: DETAILED EXPERIMENTAL RESULTS

Table 2 shows the detailed experimental results.

Author Contributions. K. W. designed and developed the experiment. X. Hu, X. Hua, and X. X. developed the device design and fabrication. K. W., Y. D., Z. Z., C. H., and Y. C. implemented the experiment and evaluated the data. K. W. and X. X. supervised the research and experiment. All authors contributed to the writing of the paper.

Disclosures. The authors declare no conflicts of interest.

Table 2. Experimental Parameters and Results[a]

L (km)	Loss (dB)	μ	ν	P_μ	P_ν	P_z	P_x	Ratio	n_z	t (s)	τ_b (ns)	QBER$_z$
50	9.957	0.568	0.144	0.799	0.201	0.944	0.056	1:9	10,241,262	42.3	$20.0 \pm 5.4 \times 10^{-9}$	0.653%
100	18.857	0.565	0.143	0.798	0.202	0.944	0.056	1:9	10,021,841	317.8	$20.0 \pm 1.2 \times 10^{-8}$	0.764%
150	28.992	0.564	0.142	0.798	0.202	0.944	0.056	1:9	10,078,187	3640.4	$20.0 \pm 1.9 \times 10^{-7}$	1.358%

L (km)	$n_{z,\mu}$	$m_{z,\mu}$	$n_{x,\mu}$	$m_{x,\mu}$	$n_{z,\nu}$	$m_{z,\nu}$	$n_{x,\nu}$	$m_{x,\nu}$	ϕ_z^u	$s_{z,1}^L$	l	SKR (bit/s)
50	9,628,161	62,566	575,986	3379	613,101	4387	35,863	236	0.0224	5,280,589	3,787,713	8.96×10^4
100	9,419,400	70,873	557,703	2576	602,441	5644	35,140	200	0.0177	5,155,932	3,742,736	1.18×10^4
150	9,456,469	126,891	577,883	4653	621,718	9973	37,593	334	0.0270	5,317,027	3,152,614	8.66×10^2

[a]L and loss are the channel lengths and channel losses, respectively. μ (ν) is the intensity of the signal (decoy) state, P_μ (P_ν) is the selection probability of the signal (decoy) state, P_z (P_x) is the probability of choosing Z (X) basis, n_z is the amount of data accumulated on the Z basis, t is the total accumulated time of measurement, ratio denotes the ratio between the number of qubits for synchronization and that of random polarization states of four BB84 polarizations, τ_b is the period measured by Bob, $n_{z,\mu}$ ($n_{x,\mu}$) is the raw count measured under Z (X) basis for the signal state, $n_{z,\nu}$ ($n_{x,\nu}$) is the raw count measured for the decoy state under Z (X) basis, $m_{z,\mu}$ ($m_{x,\mu}$) is the error count measured under Z (X) basis for the signal state, $m_{z,\nu}$ ($m_{x,\nu}$) is the error count measured for the decoy state under Z (X) basis, QBER$_z$ is quantum bit error rate of Z basis, ϕ_z^U is the upper bound of phase error rate, $s_{z,1}^L$ is the lower bound for measuring single-photon events in the Z-basis, l is the secret key length, and SKR is the final secure key rate.

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 175–179.
2. S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," Phys. Rev. Lett. **108**, 130502 (2012).
3. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
4. T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," Nature **509**, 475–478 (2014).
5. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).
6. X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," Phys. Rev. X **8**, 031043 (2018).
7. M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," npj Quantum Inf. **5**, 64 (2019).
8. X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," Phys. Rev. A **98**, 062323 (2018).
9. R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y. Z. Tan, R. Wolf, V. Scarani, and C. C. W. Lim, "Device-independent quantum key distribution with random key basis," Nat. Commun. **12**, 2880 (2021).
10. A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," Phys. Rev. Lett. **121**, 190502 (2018).
11. A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 GHz time-bin quantum key distribution," Appl. Phys. Lett. **112**, 171108 (2018).
12. F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Performance and security of 5 GHz repetition rate polarization-based quantum key distribution," Appl. Phys. Lett. **117**, 144003 (2020).
13. M. Avesani, L. Calderaro, G. Foletto, C. Agnesi, F. Picciariello, F. B. L. Santagiustina, A. Scriminich, A. Stanco, F. Vedovato, M. Zahidy, G. Vallone, and P. Villoresi, "Resource-effective quantum key distribution: a field trial in Padua city center," Opt. Lett. **46**, 2848–2851 (2021).
14. J. F. Dynes, A. Wonfor, W. W. S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J. P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," npj Quantum Inf. **5**, 101 (2019).
15. 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**, 214–219 (2021).
16. S. Wang, Z. Q. Yin, D. Y. He, W. Chen, R. Q. Wang, P. Ye, Y. Zhou, G. J. Fan-Yuan, F. X. Wang, Y. G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G. C. Guo, and Z. F. Han, "Twin-field quantum key distribution over 830-km fibre," Nat. Photonics **16**, 154–161 (2022).
17. W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, "Toward a photonic demonstration of device-independent quantum key distribution," Phys. Rev. Lett. **129**, 050502 (2022).
18. D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y. Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J. D. Bancal, "Experimental quantum key distribution certified by Bell's theorem," Nature **607**, 682–686 (2022).
19. W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C. W. Lim, and H.

Weinfurter, "A device-independent quantum key distribution system for distant users," Nature **607**, 687–691 (2022).
20. C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Foletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, and P. Villoresi, "Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder," Optica **7**, 284–290 (2020).
21. D. Ma, X. Liu, C. Huang, H. Chen, H. Lin, and K. Wei, "Simple quantum key distribution using a stable transmitter-receiver scheme," Opt. Lett. **46**, 2152–2155 (2021).
22. J. W. Silverstone, D. Bonneau, J. L. O'Brien, and M. G. Thompson, "Silicon quantum photonics," IEEE J. Sel. Top. Quantum Electron. **22**, 390–402 (2016).
23. J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson, "Integrated photonic quantum technologies," Nat. Photonics **14**, 273–284 (2019).
24. F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. Matthews, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," Quantum Sci. Technol. **3**, 025003 (2018).
25. S. Gyger, J. Zichi, L. Schweickert, A. W. Elshaari, S. Steinhauer, S. F. Covre da Silva, A. Rastelli, V. Zwiller, K. D. Jöns, and C. Errando-Herranz, "Reconfigurable photonics with on-chip single-photon detectors," Nat. Commun. **12**, 1408 (2021).
26. F. Beutel, H. Gehring, M. A. Wolff, C. Schuck, and W. Pernice, "Detector-integrated on-chip QKD receiver for GHz clock rates," npj Quantum Inf. **7**, 40 (2021).
27. F. Beutel, F. Brückerhoff-Plückelmann, H. Gehring, V. Kovalyuk, P. Zolotov, G. Goltsman, and W. H. P. Pernice, "Fully integrated four-channel wavelength-division multiplexed QKD receiver," Optica **9**, 1121–1130 (2022).
28. P. Ye, W. Chen, Z.-H. Wang, G.-W. Zhang, Y.-Y. Ding, G.-Z. Huang, Z.-Q. Yin, S. Wang, D.-Y. He, W. Liu, G.-C. Guo, and Z.-F. Han, "Transmittance-invariant phase modulator for chip-based quantum key distribution," Opt. Express **30**, 39911–39921 (2022).
29. C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, "Silicon photonic transmitter for polarization-encoded quantum key distribution," Optica **3**, 1274–1278 (2016).
30. P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," Nat. Commun. **8**, 13984 (2017).
31. D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X **8**, 021009 (2018).
32. T. K. Paraïso, I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, "A modulator-free quantum key distribution transmitter chip," npj Quantum Inf. **5**, 42 (2019).
33. M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," npj Quantum Inf. **7**, 93 (2021).
34. G. Zhang, Z. Zhao, J. Dai, S. Yang, X. Fu, and L. Yang, "Polarization-based quantum key distribution encoder and decoder on silicon photonics," J. Lightwave Technol. **40**, 2052–2059 (2021).
35. X. Li, L.-L. Wang, J.-S. Zhang, W. Chen, Y. Wang, D. Wu, and J.-M. An, "Quantum key distribution transmitter chip based on hybrid-integration of silica and lithium niobates," Chin. Phys. B **31**, 064212 (2022).
36. Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," npj Quantum Inf. **3**, 25 (2017).
37. M. Zahidy, Y. Liu, D. Cozzolino, Y. Ding, T. Morioka, L. K. Oxenløwe, and D. Bacco, "Photonic integrated chip enabling orbital angular momentum multiplexing for quantum communication," Nanophotonics **11**, 821–827 (2022).

38. G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," Nat. Photonics **13**, 839–842 (2019).

39. L. Cao, W. Luo, Y. X. Wang, J. Zou, R. D. Yan, H. Cai, Y. Zhang, X. L. Hu, C. Jiang, W. J. Fan, X. Q. Zhou, B. Dong, X. S. Luo, G. Q. Lo, Y. X. Wang, Z. W. Xu, S. H. Sun, X. B. Wang, Y. L. Hao, Y. F. Jin, D. L. Kwong, L. C. Kwek, and A. Q. Liu, "Chip-based measurement-device-independent quantum key distribution using integrated silicon photonic systems," Phys. Rev. Appl. **14**, 011001 (2020).

40. K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," Phys. Rev. X **10**, 031030 (2020).

41. W. Li, V. Zapatero, H. Tan, K. Wei, H. Min, W.-Y. Liu, X. Jiang, S.-K. Liao, C.-Z. Peng, M. Curty, F. Xu, and J.-W. Pan, "Experimental quantum key distribution secure against malicious devices," Phys. Rev. Appl. **15**, 034081 (2021).

42. X. Zheng, P. Zhang, R. Ge, L. Lu, G. He, Q. Chen, F. Qu, L. Zhang, X. Cai, Y. Lu, S. Zhu, P. Wu, and X. Ma, "Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution," Adv. Photon. **3**, 055002 (2021).

43. Q. Liu, Y. Huang, Y. Du, Z. Zhao, M. Geng, Z. Zhang, and K. Wei, "Advances in chip-based quantum key distribution," Entropy **24**, 1334 (2022).

44. T. K. Paraïso, T. Roger, D. G. Marangon, I. De Marco, M. Sanzaro, R. I. Woodward, J. F. Dynes, Z. Yuan, and A. J. Shields, "A photonic integrated quantum secure communication system," Nat. Photonics **15**, 850–856 (2021).

45. Y. Du, X. Zhu, X. Hua, Z. Zhao, X. Hu, Y. Qian, X. Xiao, and K. Wei, "Silicon-based decoder for polarization-encoding quantum key distribution," Chip **2**, 100039 (2023).

46. D. Bacco, I. Vagniluca, B. Da Lio, N. Biagi, A. Della Frera, D. Calonico, C. Toninelli, F. S. Cataliotti, M. Bellini, L. K. Oxenløwe, and A. Zavatta, "Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area," EPJ Quantum Technol. **6**, 5 (2019).

47. J.-Q. Geng, G.-J. Fan-Yuan, S. Wang, Q.-F. Zhang, Y.-Y. Hu, W. Chen, Z.-Q. Yin, D.-Y. He, G.-C. Guo, and Z.-F. Han, "Coexistence of quantum key distribution and optical transport network based on standard single-mode fiber at high launch power," Opt. Lett. **46**, 2573–2576 (2021).

48. W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Q. Li, Y. Liu, Q. Zhang, C.-Z. Peng, L. You, F. Xu, and J.-W. Pan, "High rate quantum key distribution exceeding 110 M b s⁻¹," Nat. Photonics **17**, 416–421 (2023).

49. Y. Han, H. Park, J. Bowers, and K. M. Lau, "Recent advances in light sources on silicon," Adv. Opt. Photon. **14**, 404–454 (2022).

50. L. Calderaro, A. Stanco, C. Agnesi, M. Avesani, D. Dequal, P. Villoresi, and G. Vallone, "Fast and simple qubit-based synchronization for quantum key distribution," Phys. Rev. Appl. **13**, 054041 (2020).

51. A. de Lind van Wijngaarden and T. Willink, "Frame synchronization using distributed sequences," IEEE Trans. Commun. **48**, 2127–2138 (2000).

52. Y.-Y. Ding, W. Chen, H. Chen, C. Wang, Y.-P. Li, S. Wang, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, "Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits," Opt. Lett. **42**, 1023–1026 (2017).

53. D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state QKD protocol," Appl. Phys. Lett. **112**, 171104 (2018).

54. Z. Li and K. Wei, "Improving parameter optimization in decoy-state quantum key distribution," Quantum Eng. **2022**, 9717591 (2022).

55. X. Liu, M.-Q. Huang, H. Min, G. Jin, X. Jiang, and C.-Z. Peng, "A 5 GHz and 7.5 V multi-amplitude modulator driving circuit for practical high-speed quantum key distribution," Rev. Sci. Instrum. **91**, 024705 (2020).

56. H. Semenenko, P. Sibson, M. G. Thompson, and C. Erven, "Interference between independent photonic integrated devices for quantum key distribution," Opt. Lett. **44**, 275–278 (2019).

57. C. Agnesi, B. Da Lio, D. Cozzolino, L. Cardi, B. Ben Bakir, K. Hassan, A. Della Frera, A. Ruggeri, A. Giudice, G. Vallone, P. Villoresi, A. Tosi, K. Rottwitt, Y. Ding, and D. Bacco, "Hong–Ou–Mandel interference between independent III–V on silicon waveguide integrated lasers," Opt. Lett. **44**, 271–274 (2019).

58. C. Li, M. Curty, F. Xu, O. Bedroya, and H.-K. Lo, "Secure quantum communication in the presence of phase- and polarization-dependent loss," Phys. Rev. A **98**, 042324 (2018).

59. C. Huang, C. Yen, L. Jin, M. Geng, J. Wang, Z. Zhang, and K. Wei, "Experimental secure quantum key distribution in the presence of polarization-dependent loss," Phys. Rev. A **105**, 012421 (2022).

60. P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," Optica **4**, 172–177 (2017).

61. R. Sax, A. Boaron, G. Boso, S. Atzeni, A. Crespi, F. Grünenfelder, D. Rusca, A. Al-Saadi, D. Bronzi, and S. Kupijai, "High-speed integrated QKD system," arXiv, arXiv:2211.11560 (2022).

62. M. Li, L. Wang, X. Li, X. Xiao, and S. Yu, "Silicon intensity Mach–Zehnder modulator for single lane 100 Gb/s applications," Photon. Res. **6**, 109–116 (2018).

63. D. Chen, M. Liu, Y. Zhang, L. Wang, X. Hu, P. Feng, X. Xiao, and S. Yu, "C + L band polarization rotator-splitter based on a compact S-bend waveguide mode demultiplexer," Opt. Express **29**, 10949–10957 (2021).

64. D. Chen, X. Xiao, L. Wang, W. Liu, Q. Yang, and S. Yu, "Highly efficient silicon optical polarization rotators based on mode order conversions," Opt. Lett. **41**, 1070–1073 (2016).