LETTER | MARCH 12 2025

On-chip quantum key distribution over field-deployed fiber using lithium niobate photonic circuit

Hyungjun Heo ; Min Ki Woo; Chang-Hoon Park ; Hyeong-Soon Jang ; Hyeon Hwang; Hansuek Lee ; Min-Kyo Seo ; Sangin Kim ; Hyounghan Kwon ; Hojoong Jung ; Sang-Wook Han

APL Photonics 10, 031301 (2025)
https://doi.org/10.1063/5.0223694

On-chip quantum key distribution over field-deployed fiber using lithium niobate photonic circuit

Cite as: APL Photon. 10, 031301 (2025); doi: 10.1063/5.0223694
Submitted: 17 June 2024 • Accepted: 24 February 2025 •
Published Online: 12 March 2025

Hyungjun Heo,[1,2] Min Ki Woo,[2] Chang-Hoon Park,[2] Hyeong-Soon Jang,[2,3] Hyeon Hwang,[4] Hansuek Lee,[4,5] Min-Kyo Seo,[4] Sangin Kim,[3] Hyounghan Kwon,[2,6] Hojoong Jung,[2,a)] and Sang-Wook Han[2,6,a)]

AFFILIATIONS

[1] Technological Convergence Center, Korea Institute of Science and Technology (KIST), Seoul 02792, South Korea
[2] Center for Quantum Technology, Korea Institute of Science and Technology (KIST), Seoul 02792, South Korea
[3] Department of Electrical and Computer Engineering, Ajou University, Suwon 16499, South Korea
[4] Department of Physics, Korea Advanced Institute of Science and Technology (KAIST), Daejeon 34141, South Korea
[5] Graduate School of Nanoscience and Technology, Korea Advanced Institute of Science and Technology (KAIST), Daejeon 34141, South Korea
[6] Division of Quantum Information, KIST School, Korea University of Science and Technology, Seoul 02792, South Korea

[a)] Authors to whom correspondence should be addressed: hojoong.jung@kist.re.kr and swhan@kist.re.kr

ABSTRACT

Quantum key distribution (QKD) systems have proven their theoretically unconditional security by quantum mechanics, but the scalability and cost barriers limit the rapid growth of the QKD system industry. The integration of QKD systems on chips has enabled their widespread adoption in secure quantum communication technologies, but the optimized platforms and designs are still being studied. Herein, we fabricated monolithic quantum photonic circuits for the BB84 QKD protocol using thin-film lithium niobate (TFLN), which enables flexible design in organizing both active and passive elements on one chip based on its superior material properties. The proposed circuit design for both transmitter and receiver parts are identical, which facilitates stable operation and mass production. Using our device, we demonstrated QKD over a field-deployed quantum channel, and its performance is comparable to state-of-the-art. This result proved the potential of TFLN for quantum communication technology.

I. INTRODUCTION

With demonstrated quantum advantages in cryptographic communication, computing, and metrology, research on quantum science has now been expanding to quantum engineering and quantum industries.[1–3] Quantum key distribution (QKD) is a quantum technology that is closest to the realization of quantum industries owing to its robust implementation and unconditional security guaranteed by the physical laws of quantum mechanics.[4–7] Despite rapid advancements in QKD systems based on fiber or free-space optics, the bulky footprint and limited scalability of conventional optics severely hinder the wide dissemination of QKD systems. In contrast, quantum photonic integrated circuits (PICs) offer key advantages, including miniaturization, stability, high-speed operation, and scalability, making them a promising alternative to traditional systems.[8,9]

Integrated QKD systems have been developed significantly, enabling not only discrete variable QKD protocols, such as BB84, Coherent One-Way (COW), and Differential Phase-Shift (DPS),[10–22] but also continuous variable QKD, such as Gaussian-modulated coherent-state (GMCS),[23,24] using various materials, including Si, InP, SiO_2, SiN, and SiON, depending on the encoding and decoding methods. Those mature material platforms barely satisfy the high-speed modulation and low optical loss requirements simultaneously owing to their inherent material properties that limit the circuit design flexibility. Therefore, transmitters and receivers have been fabricated independently on different material platforms with specialized and limited functions to meet distinct requirements. For instance, Si and InP have been used for transmitter components requiring fast active modulation to encode quantum key states through phase and intensity modulation, and SiN, SiON, SiO_2, and laser writing materials have been used for receiver components requiring low optical losses for the accurate detection of single-photon levels. However, these material combinations require a precise control of key state synchronization and individual chip packaging, which are big burdens for multi-network quantum communication and mass production.

Recently, thin-film lithium niobate (TFLN) has achieved wafer-level production while maintaining the excellent material properties of bulk lithium niobate, such as a wide bandgap (~4 eV) and large electro-optic coefficients (r_{33} = 32 pm/V; r_{13} = 10 pm/V).[25,26] Research on photonic integrated circuits (PICs) has been actively pursued on TFLN platforms, leading to the development of various high-performance optical components. Correspondingly, researchers have thoroughly investigated TFLN platforms and demonstrated various types of notable optical components, such as high-performance electro-optic modulators with a bandwidth exceeding 100 GHz,[27–29] ultralow loss optical waveguides with a propagation loss under 0.027 dB/cm,[30,31] broadband frequency combs,[32–34] highly efficient wavelength converters,[35] and photon-pair sources,[36,37] just to name a few examples.

The various active and passive functionalities of these components provide high degrees of freedom in the optical circuit design, which make it a highly promising material platform for critical components in the QKD system. In addition, the successful heterogeneous integration of TFLN photonic circuits with InP-based lasers[38] and superconducting nanowire single-photon detectors (SNSPDs) utilizing NbTiN[39,40] has been achieved. Although these advancements have considerably enhanced the potential of TFLN as QKD platforms, TFLN photonic circuits for QKD systems composed of transmitters and receivers are yet to be explored.

In this work, we demonstrated the potential of TFLN as a QKD chip with optical delay lines, as well as a high-speed modulator that addresses a significant challenge faced by other photonic platforms: achieving both low-loss (0.13 dB/cm) and high-speed (~10 MHz) modulation capabilities within a single chip. The propagation loss of our chip is smaller than the silicon shallow-ridge waveguides loss of 0.27 dB/cm,[41] and the modulation speed is significantly faster than that of the fast SiN thermo-optic phase shifters (~100 kHz).[42] This unique strength of TFLN makes it an attractive choice for QKD systems.

The proposed integrated QKD chip design allows the device to function as either a transmitter or a receiver with an identical design. This design reduces the complexity of the control element in the system and improves the operational stability. Moreover, the use of identical transmitters and receivers is favorable to high yields and mass production. Finally, using the QKD chips based on TFLN, we implemented the BB84 protocol using time-bin and phase states in a 32.16-km field-deployed quantum channel with a quantum bit error rate (QBER) of 0.58% and a secure key rate (SKR) of 0.77 × 10^{-4} per pulse. The performance of individual components in our system may fall slightly short of the state-of-the-art TFLN. However, we believe that these results will serve as a cornerstone in demonstrating the feasibility of integrated QKD systems by fully leveraging the potential of the TFLN platform.

II. RESULTS

A. On-chip QKD system over field-deployed quantum channel

Figure 1(a) presents a schematic of the on-chip QKD system using monolithic TFLN photonic circuits. Here, twin chips for the transmitter and receiver parts denoted as Alice and Bob, respectively, were connected using the fiber quantum channel. The photodetector (PD) connected to Alice provides feedback on the laser source intensity, and the polarization controllers (PCs) placed before Alice, Bob, and the SNSPD define the polarization at each part, ensuring optimal device performance. A complete on-chip photonic QKD system is prepared by combining four Laser Diodes (LDs) and SNSPDs through optical fibers. The TFLN-based QKD chip, which has a small chip area of 8 × 4 mm^2 [Fig. 1(b)], was fabricated by monolithic integration of a low-loss waveguide and a fast electro-optic modulator [Fig. 1(c); see Sec. IV for details of the fabrication procedure].

Utilizing these TFLN photonic integrated circuits, we demonstrated the BB84 QKD protocol using a field-test channel of 32.16 km. Figure 1(d) shows a deployment map of this quantum channel between the Center for Quantum Information (CQI) laboratory and Sungkyunkwan University (SKK Univ), including three Korea Telecom (KT) nodes compatible with commercial networks provided by the KT company. The measurement setups of Alice and Bob were located in separate rooms within the CQI laboratory, as shown in the inset of Fig. 1(d) (see the supplementary material Fig. 1 for details). The quantum channel has a dark count of 120 counts/s and a total transmission loss of 11.5 dB, which exceeds the conventional fiber loss (0.2 dB/km) owing to the fiber coupling losses at seven nodes during a round trip. The QKD demonstration was successful, with a QBER of 0.58% and a SKR of 0.77 × 10^{-4} per pulse. We calculated the SKR based on two-decoy-state[43,44] using an asymptotic analysis (see Sec. IV for further details regarding the analysis).

B. TFLN photonic circuits

The proposed TFLN photonic circuit consists of various functional elements, including a 50:50 splitting 2 × 2 beam splitter (BS), a 4 × 2 BS, an optical delay line (ODL), a phase modulator (PM), and a cascaded intensity modulator (IM), as indicated by the yellow dashed boxes in Fig. 2(a). These elements function optimally for transverse electric (TE) waves. The 2 × 2 BS is linked to the 4 × 2 BS through two distinct paths: PM and ODL. When the chip is used as Bob, the injected light from port 1 is divided into four ports (ports 3–6) to detect the four quantum states in the BB84 protocol. For Alice, the injected light from ports 4 and 5 passed through an asymmetric Mach–Zehnder interferometer (AMZI), which consists of an ODL and PM. Ports 3 and 6 are exclusively linked to the ODL and PM paths, respectively, via 50:50 multimode interference (MMI) splitters, which are parts of the 4 × 2 BS. The path to port

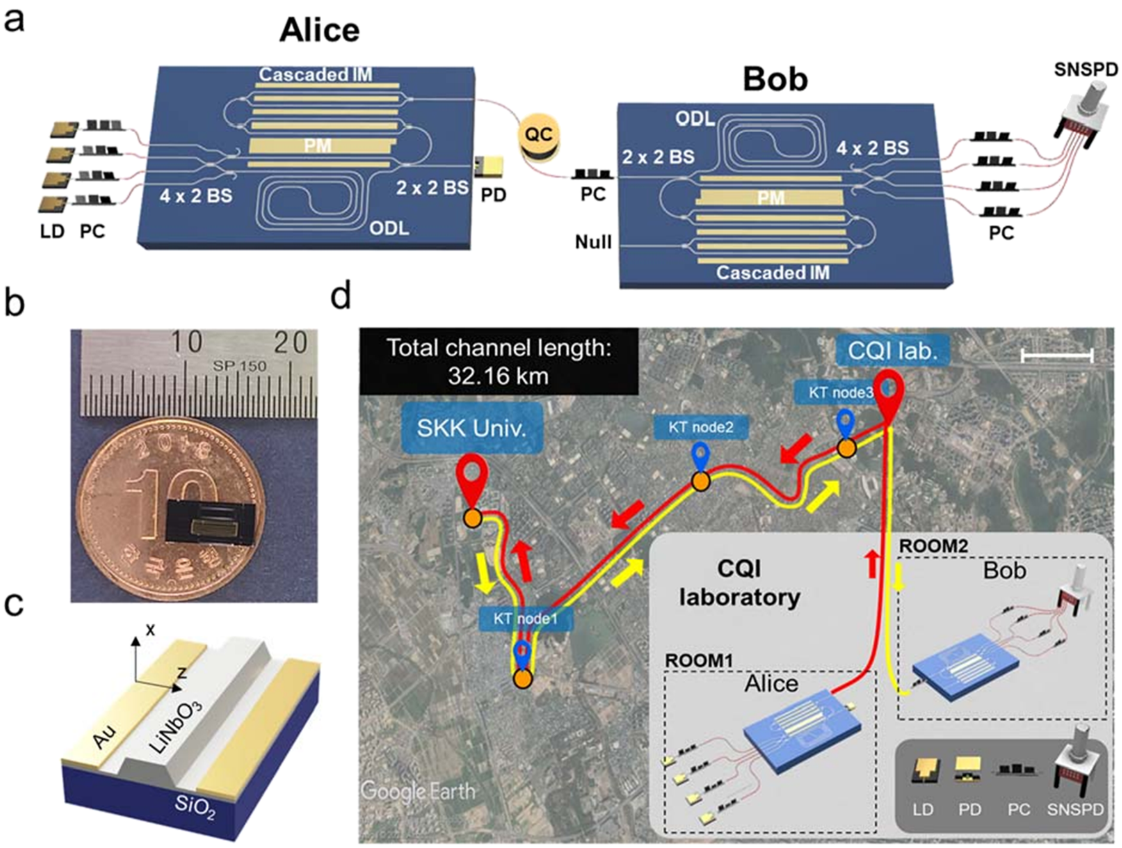

FIG. 1. Schematic of the integrated QKD system based on TFLN photonic circuits. (a) Schematic of the integrated QKD system. The integrated QKD system implements the BB84 protocol and consists of two TFLN photonic circuits, a quantum channel (QC), off-chip LDs, and SNSPDs. The transmitter and receiver are identical and denoted as Alice and Bob, respectively. (b) Optical image of the TFLN photonic chip with dimensions of 8 × 4 mm^2. (c) Schematic of the x-cut TFLN waveguide and Au electrodes. The waveguides and electrodes are aligned perpendicular to the z axis (corresponding to a crystallographic c-axis of LiNbO3). (d) Map of the quantum test channel deployment arranged to travel 32.16 km between the CQI laboratory of the Korea Institute of Science and Technology (KIST) and SKK Univ. The measurement setups of Alice and Bob are located in different rooms within the CQI laboratory. Map data: 37°16′52.93″N and 127°00′24.28″E. Google Earth, November 11, 2022. March 4, 2023, 2022; Maxar Technologies. Scale bar: 1 km.

2 has a cascaded IM, which modulates the light intensity for decoy-state generation and provides feedback on the encoded key-state intensity at Alice's end. The PM is used to stabilize our QKD system by compensating for the phase drift during operation (See the supplementary material Fig. 3 for details).

First, we investigated the passive optical characteristics of the photonic circuits. In Fig. 2(b), the transmission spectra at ports 3–6 are plotted when a tunable continuous-wave (CW) laser is injected into port 1. Ports 3 and 6 present transmittances through the ODL and PM paths, respectively. The transmittances of the two ports differ by less than 1 dB, even though the ODL is 7.8 cm longer than the PM path, corresponding to a time delay of 570 ps. This low loss matches well with the estimated optical propagation loss of ~0.13 dB/cm based on the micro-ring intrinsic quality factor of 3.15 × 10^6 (see the supplementary material Fig. 2 for details). The AMZI interferences were observed at ports 4 and 5 with a free spectral range of 1.75 GHz and an extinction ratio exceeding 20 dB. Despite the complex noise from the Mach–Zehnder interferometer (MZI), the sum of the transmissions of ports 4 and 5 was approximately flat [cyan line in Fig. 2(b)] and ~0.8 dB lower than the sum of output powers at ports 3 and 6 [not shown in Fig. 2(b)] across the measured wavelengths, which is from an additional MMI insertion loss to port 4 or 5. Considering the loss of ODL (L_{ODL}) and MMI (L_{MMI}) is less than 1 and 0.8 dB, respectively, the total element loss in the receiver chip can be estimated. As there are four ways from input port 1 to output ports 3–6, (ports 1–3: L_{ODL} + 2·L_{MMI}, ports 1–4: L_{ODL} + 3·L_{MMI}, ports 1–5: 3·L_{MMI}, and ports 1–6: 2·L_{MMI}), the total element loss would be $(2 \cdot L_{ODL} + 10 \cdot L_{MMI})/4 \leq 2.5$ dB.

The total transmittance of ports 3–6 was −14.35 ± 0.23 dB [black line in Fig. 2(b)], including coupling loss, delay line, and MMI losses. Most of the reduction in the total transmission is caused by coupling losses between the optical fiber and the chip. The proposed TFLN optical rib-waveguide has a smaller optical mode area (<0.7 μm^2) compared to the lensed fiber's mode area (~4.9 μm^2). This significant mode mismatch leads to a fiber-to-chip coupling loss of 6.5 dB/facet. If the coupling loss is ~13 dB, the element loss

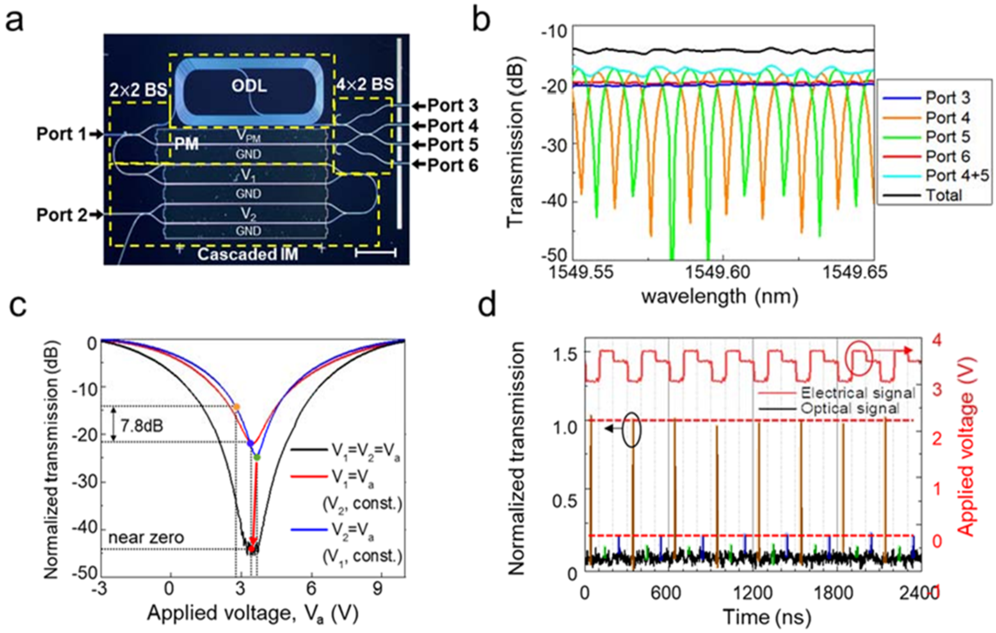

FIG. 2. Characterization of elements in the TFLN QKD chip. (a) Optical microscopic image of the fabricated QKD chip. Scale bar: 1 mm. (b) Transmission spectra of the passive on-chip optical elements. The CW laser is injected into port 1 and propagates through the 2 × 2 BS, the AMZI composed of an ODL and PM, and the 4 × 2 BS. The transmission spectra are recorded at ports 3–6 and are indicated by solid blue, orange, green, and red lines, respectively. The corresponding ports 1–6 are denoted in (a). (c) Modulated transmission of the cascaded IMs. The orange, blue, and green circles on the solid blue line indicate the three modulation levels of the lower IM (V_2) for the signal, weak, and vacuum decoy states, respectively. (d) Normalized transmission of the modulated pulses from port 2 to port 6 for the decoy states generation. According to the periodic modulation of the IM, the pulsed laser intensity exhibits stable repetition at three distinct levels: signal (orange), weak (blue), and vacuum (green). The solid red line indicates the voltage applied to the lower IMs, corresponding to the same-colored circles shown in (c).

is ~1.35 dB, which is within the reasonable range of on-chip element losses (<2.5 dB). It is noteworthy that the transmission of each port maintains an appropriate intensity ratio within the measured wavelength region, although light passes through multiple elements comprising the MMI and ODL. The relatively high coupling losses can be mitigated using advanced techniques such as inverse tapering or multi-layer tapering.[45,46] In a recent parallel study, we have reported ~1 dB/facet coupling loss by forming a 3D structure at the chip edge,[47] which will be applied to the next version QKD chips.

Next, cascaded IMs were tested to generate decoy signals. Figure 2(c) shows the normalized transmission from port 2 to port 6 as a function of the applied voltage (V_a) on each electrode. The solid red and blue lines correspond to the modulated transmission when electrical biases, V_1 and V_2, were applied to the upper and lower IMs in Fig. 2(a), respectively. While one IM was tested, another IM is set for the maximum transmission. By simultaneous modulating both IMs, a high extinction ratio of more than 45 dB was achieved (black solid line). To realize the decoy protocol, we generated the signal (μ = 0.6), weak (υ = 0.1), and vacuum decoy states using the lower IM. The intensity of the input pulse laser with a repetition rate of 10 MHz and a pulse width of 120 ps was modulated as depicted in Fig. 2(d). The orange, blue, and green peaks are modulated pulses attenuated using the IM as indicated by the same-colored circles in Fig. 2(c). The orange and blue pulses were used as the signal and weak decoy states, whereas the vacuum (green) state can be further attenuated using the upper IM and additional equipment.

C. On-chip quantum key states encoding and decoding

The TFLN QKD chip realized the BB84 protocol using four quantum key states based on time-bin (Z-basis) and phase (X-basis). We defined early and late signals as |0> and |1> states in the Z-basis, respectively, and the X-basis states are defined as follows: |+> = |0 > + |1> and |−> = |0> − |1>. Figure 3(a) shows the simplified schematics of our QKD system [Fig. 1(a)] that generate and detect the four key states. Before the field test, we verified key states encoding and decoding using a weak pulsed laser. First, we measured the photon counts at the output port of the Alice chip when each input laser was on, and Fig. 3(b) shows the histogram results with an integration time of 1 s. Four input lasers correspond to four states expressed with different colors: red, |0>; blue, |1>; orange, |+>; and green, |−>. The detected photons were clearly synchronized with a time interval of 570 ps between early and late photons, as indicated by the red dotted lines. Here, the PM is not used for key state encoding but rather for the phase reference frame agreement between Alice and Bob chips.

Next, the four key states sent from the Alice part via the quantum channel were decoded at the Bob part. Figure 3(c) presents SPD 1 and 4 measurements for Z-basis (|0>, |1>) inputs and SPD

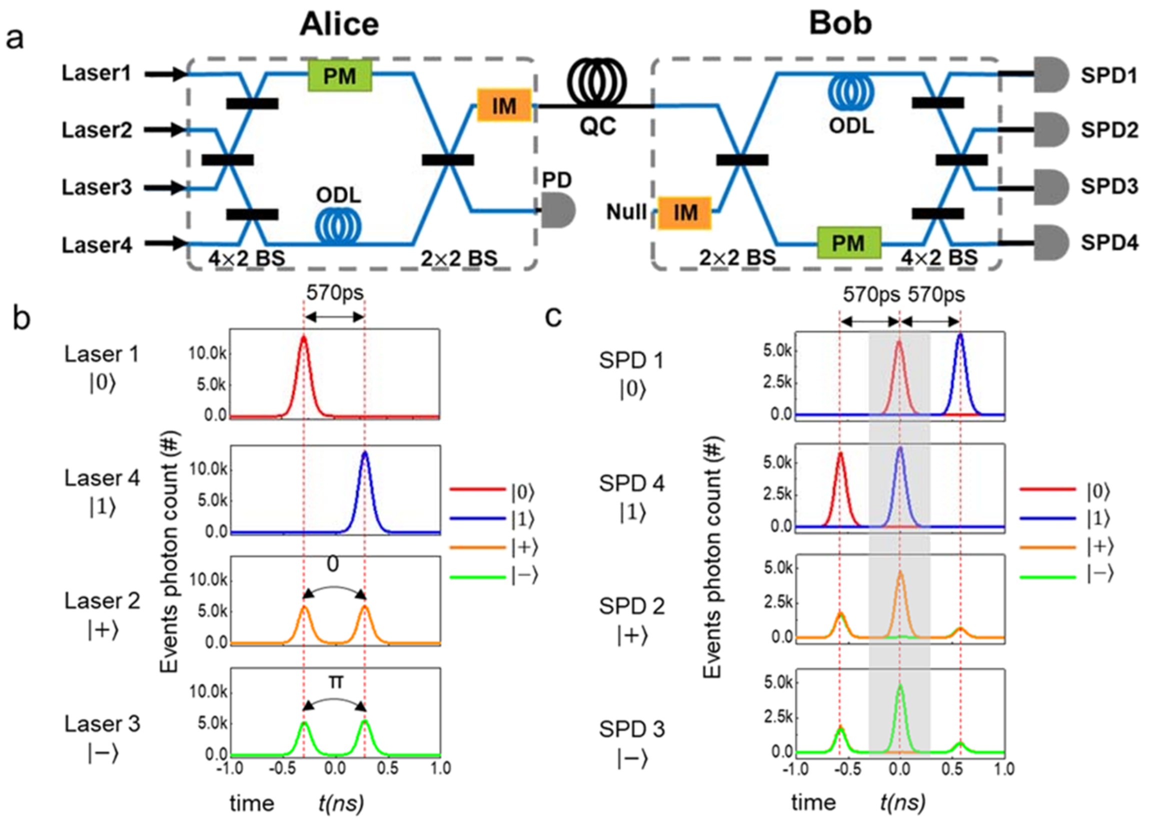

FIG. 3. BB84 protocol using passive encoding and decoding. (a) Schematic of the photonic circuit of the proposed BB84 protocol. For generating keys, each state is passively encoded (decoded) by selecting an input (output) port. (b) Measurement histograms of the encoded states at the Alice output port. We encode the quantum states based on two orthogonal bases using phase and time-bin. The |0> and |1> states represent the early and late time-bins, respectively, and the |+> and |−> states have 0 and π phase differences between the early and late time-bins, respectively. (c) Measurement histograms of the decoded states at the Bob output ports. Sift keys are generated by the photons detected at mid-timing (gray-shaded area) when Alice and Bob select the same basis.

2 and 3 measurements for X-basis (|+>, |−>) inputs. Considering the incremental loss by Bob's chip, the detection integration time was increased to 60 s. From the measurement results, we only use the photons detected during the mid-timing (the gray-shaded area) as sift keys. The lateral peaks of |0> and |1> states are vulnerable to time-shift attacks,[48] and the lateral peaks of |+> and |−> states are not suitable for secret key generation. They are inevitable extra losses in the QKD system and reduce the secure key rate (SKR).

A distinct detection histogram at the mid-timing allows accurate determination of the key state only when the detector set and key basis are matched (SPDs 1 and 4: Z-basis; SPDs 2 and 3: X-basis). The key state cannot be determined when an unmatched basis is detected because the detection information is not enough to distinguish the Alice state, which is not illustrated in the graph here. In this way, when Alice and Bob select the same laser and SPD set, they both know that the key states are |0>, |1>, |+> or |−>, which become the quantum keys they share. Conversely, if different bases are selected, the key states cannot be determined, and the corresponding keys are discarded.

Note that even after passing through the quantum channel and Bob chip, the clear synchronization still remained at the early, mid, and late timings (red dotted lines) with an interval of 570 ps, which aids in simplifying the system's control units. This is due to the equal length of the ODL in Alice and Bob owing to the same design and the same fabrication process in the same batch, which is critical for stable and accurate QKD operation. The asymmetry in the lateral peaks at SPD2 and SPD3 is mainly from the optical losses in the delay lines located in the transmitter and receiver chips. The signal of the late-lateral peak (right) undergoes greater attenuation compared to the fast-lateral peak (left), as it passes through two optical delay lines (7.8 × 2 cm^2).

D. Experimental demonstration of on-chip QKD

Figures 4(a) and 4(b) show ideal statistical results and measurement results of the four quantum key states recorded over the field-deployed quantum channel shown in Fig. 1(d), and the corresponding values are listed in Table I (See the supplementary material for further details of the overall flow). In Table I, the measurement probability of each detector is at mid-timing, and the ideal values are in the round brackets. When Alice's chosen basis matches with Bob's detected basis, they probabilistically generate sifted keys

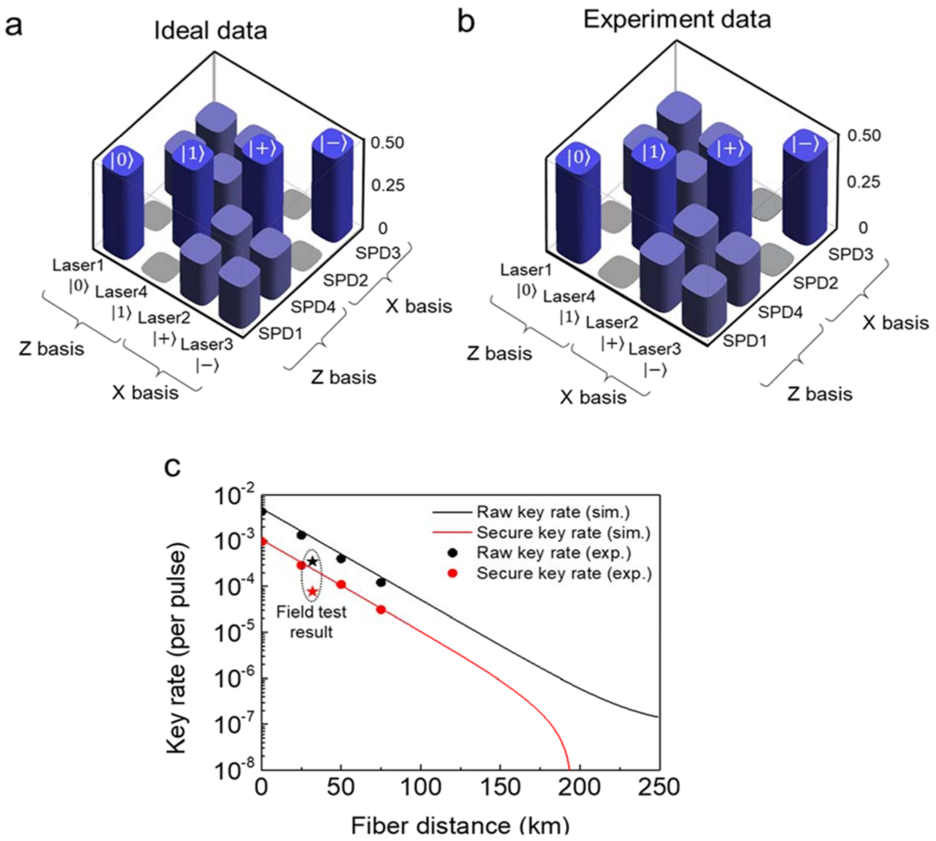

FIG. 4. Simulation and experiment results of on-chip QKD. (a) Probability distributions of the received key states in the ideal case and (b) measured data in the field. Almost identical graphs show the successful QKD demonstration in the real environment. (c) Experimental and calculated key rates per pulse. The fiber distance is emulated using a variable optical attenuator. The black and red colors represent the raw and SKRs, respectively. The solid lines, circles, and stars are the numerical simulation, lab test, and field test results, respectively. The SKR at the actual field test (red star) is lower than the simulation or lab test results owing to the coupling losses at the multi-node for commercial networks on the field-deployed quantum channel, as shown Fig. 1(d).

TABLE I. Measurement probability distributions.

	SPD 1 |0>	SPD 4 |1>	SPD 2 |+>	SPD 3 |−>
Laser 1	46.68%	0.01%	25.95%	27.36%
|0>	(50%)	(50%)	(25%)	(25%)
Laser 4	0.01%	51.36%	24.94%	23.69%
|1>	(0%)	(50%)	(25%)	(25%)
Laser 2	26.85%	25.64%	47.10	0.41%
|+>	(25%)	(25%)	(50%)	(0%)
Laser 3	22.58%	23.74%	0.23%	53.45%
|−>	(25%)	(25%)	(0%)	(50%)

associated with the laser and detector number. The QBER of the sifted keys was 0.58%, with 0.14% for the Z-basis and 1.10% for the X-basis. In our passive encoding and decoding scheme, the low QBER was maintained by the phase reference frame calibration using the feedback control with a PM element in the Bob chip. In addition, the on-chip interferometer including the optical delay line without active control is relatively insensitive to the environment and exhibits inherent stability. This is especially beneficial for Z-basis, which shows a much lower QBER than X-basis. As a result, the measurement probabilities match well with the ideal's ones, which proves the accurate operation of our QKD system in the field.

To estimate the key-rate dependence on the channel distance, we measured the SKR by emulating the channel distance using a variable optical attenuator with an assumed optical fiber loss of 0.2 dB/km. Figure 4(c) shows the simulation, lab test, and field test results for the raw key rate and SKR. The emulated lab experiment results, denoted by the black and red circles in Fig. 4(c), show good agreement with the numerical simulation results. The parameters adopted for the simulation are as follows: the same decoy state as used in the experiment; a SNSPD (Single Quantum Eos) detection efficiency of 80%; a dark count rate of 120 cps; a QBER of 0.58%; and Bob's chip transmission of 1.84% ± 0.19%. Based on the simulation results, the proposed QKD system guarantees secure communication at a distance more than 150 km using conventional fibers. The key rates of the actual field test (black and red stars) are lower than the lab experiment results, which is due to the coupling losses at the seven nodes in the quantum channel, as shown in Fig. 1(d).

In order to increase the SKR and secure communication distance, the system loss needs to be minimized. Currently, the fiber-to-chip interface loss is dominant, and the improved coupling efficiency will increase the photon counts, key rate, and the communication distance. In addition, only mid-timing signals were used for secure key generation to avoid the time-shift attack, which results in the information loss at early or late timings. We expect that design improvement can resolve this issue and enhance the system efficiency. The pulse laser in this experiment has a repetition rate of 10 MHz considering our system speed. We used the time-correlated single-photon counting unit (PicoHarp 300) and the SNSPD unit (EOS800CS) having dead times of 90 and 30 ns, respectively. Thus, we limited the operation speed to 10 MHz to focus on proving the possibility of TFLN PICs for QKD application. As our system loss is relatively high, the mean photon number per pulse is much less than one. Therefore, the QKD operation speed can be increased simply by using high speed laser.

III. CONCLUSION

In conclusion, we fabricated the TFLN QKD chip and demonstrated the BB84 protocol using the commercial fiber networks. The high $\chi^{(2)}$ nonlinearity and low optical loss of TFLN allow a high degree of freedom in the device design and fabrication, which enables both active and passive components on a single chip with a size of 8 × 4 mm^2. Our QKD chip can encode and decode synchronized key states without active control of timing and phase, and the same chip can be used for either Alice or Bob owing to the twin-configuration, which supports mass production and commercialization. The passive components including AMZI and multiple MMI beam splitters exhibit accurate path and timing control, which result in clear generation and detection of quantum key states. The IM and PM active components provide decoy state generation and feedback control to maintain the system stable.

The field test using the deployed optical fiber of 32.16 km was successful with a QBER of 0.58% and a SKR of 0.77×10^{-4} per pulse. The measured quantum key state distributions are very close to the ideal case, which proves our well-functioning device. The simulation and emulated experiment results of SKR match well, and the little offset with the field test is due to the deployed fiber coupling losses at nodes. The TFLN QKD chips for the BB84 protocol can be further developed for comprehensive QKD systems, such as plug-and-play QKD or measurement device-independent QKD applications.[49,50] Integration with lasers and SNSPDs is also crucial for high-efficient, high-speed, and mobile QKD systems.[17,20,39] With proven fundamental building blocks for quantum photonics, the TFLN device can be utilized in other quantum applications, such as quantum computing, in the near future.

IV. METHODS

A. Sample fabrication

We used commercial x-cut TFLN wafers composed of 600 nm-thick $LiNbO_3$ on 4.7 μm-thick SiO_2 on a Si substrate from NanoLN. First, we patterned a photonic integrated circuit design on the TFLN wafer using E-beam lithography after spin-coating of the hydrogen silsesquioxane (FOX-16) resist with a thickness of 800 nm. Inductively coupled plasma-reactive ion etching (Oxford Plasmalab 100) with Ar was used to etch the patterned sample, and the re-deposition residue was removed by cleaning with a KOH solution at 80 °C. The etching depth was 400 nm, and the sidewall angle was ~70°. Electrode patterns were formed through photolithography and a lift-off process. An e-beam evaporator was used to deposit Ti and Au with thicknesses of 10 and 100 nm, respectively. The electrodes were oriented perpendicular to the z axis, which corresponds to the crystallographic c-axis of $LiNbO_3$, to utilize the highest electro-optic coefficient (r_{33}). Finally, the TFLN wafer was annealed at 600 °C for 1 h.

B. Two-decoy state

The decoy state effectively deals with the photon number splitting attack, where an eavesdropper captures photons within a quantum channel in the system using weak coherent pulses. In this paper, the theoretical background of the decoy state was referred to asymptotic analysis of Ref. 43. Briefly reviewing the formulas from the reference, the SKR per laser pulse obtained from the two-decoy protocol is given as

$$R \geq q\{-Q_\mu f(E_\mu)\mathrm{H}_2(E_\mu) + Q_1^L[1 - \mathrm{H}_2(e_1^U)]\},$$

where $q = 1/2$ is the basis reconciliation factor; the signal gain is $Q_\mu = Y_0 + 1 - e^{-\eta\mu}$, i.e., the ratio of Bob's detections to pulses sent by Alice is calculated accounting for an average photon number μ and total detection probabilities (η); Y_0 is the detection yield when there are 0 photons or dark count; total detection probability is calculated by $\eta = t_{bob} \times t_{channel} \times \eta_{detector}$, where t_{bob} is the transmission of Bob's chip, $t_{channel}$ is the transmission of the link channel between Alice and Bob, $\eta_{detector}$ is the detector efficiency; E_μ is the QBER for signal pulses; $f(E_\mu) = 1.2$ is the assumed error correction efficiency for practical error correction codes; $\mathrm{H}_2(x) = -x\log_2(x) - (1 - x)\log_2(1 - x)$ is the binary Shannon entropy function; and Q_1^L and e_1^U are the estimated gain lower bound and error rate upper bound, respectively, for single-photon pulses. In the two decoys with weak and vacuum states,

$$Q_1 \geq Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - Y_0 \frac{\mu^2 - \nu^2}{\mu^2}\right),$$

$$e_1 \leq e_1^U = \frac{Q_\mu E_\mu - e_0 Y_0 e^{-\mu}}{Q_1^L},$$

where the background error rate is $e_0 = 0.5$ (random background is assumed).

For decoy state generation, we choose average photon numbers of 0.6, 0.1, and 0 for the signal (μ), weak-decoy state (υ), and vacuum state with probabilities of 0.8, 0.15, and 0.05, respectively. According to the experimental results, SNSPD (Single Quantum, Eos800CS) detection efficiency ($\eta_{detector}$) is 80%, the dark count rate is 120 cps, the QBER is 0.58%, and the Bob part chip transmission (t_{bob}) is 1.84% ± 0.19%. By applying these parameters, the SKR value is theoretically simulated as a function of the quantum channel distance.

SUPPLEMENTARY MATERIAL

See the supplementary material for the measurement setup, propagation loss estimation, phase stabilization using phase modulator feedback control, and passive encoding and decoding BB84 protocol.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF) (Grant Nos. 2021M1A2A2043892 and 2022M3K4A1097119), the Institute for Information and Communications Technology Promotion (IITP) (Grant Nos. 2020-0-00947, 2020-0-00890, and RS-2023-00222863), the National Research Council of Science and Technology (NST) (Grant No. CAP21034-000), the Commercialization Promotion Agency for R&D Outcomes (COMPA) (Grant No. 2022SCPO_B_0210), the KREONET Advanced Research Program Grant from KISTI, and the KIST research program (Grant Nos. 2E33541 and 2E33571). We acknowledge Hyun-Joon Shin, a member of the Center for Bionics, Korea Institute of Science and Technology, for the provision of experimental equipment.

AUTHOR DECLARATIONS

Conflict of Interest

The authors have no conflicts to disclose.

Author Contributions

H.H., M.-K.W., C.-H.P, and H.-S.J. designed the device and evaluated the data. H.H. and H.-S.J. fabricated the samples and conducted the experiments. S.K., M.-K.S., H.L., and H.H contributed to the analysis and discussion of the results. H.J. and S.-W.H. supervised the research and experiments. H.H., M.-K.W., C.-H.P, H.K., and H.J. contributed to the writing of the manuscript. All authors contributed to the discussion and manuscript revision.

Hyungjun Heo: Conceptualization (lead); Data curation (lead); Writing – original draft (lead); Writing – review & editing (lead). **Min Ki Woo**: Conceptualization (equal); Data curation (equal). **Chang-Hoon Park**: Conceptualization (equal); Data curation (equal). **Hyeong-Soon Jang**: Data curation (supporting). **Hyeon Hwang**: Data curation (supporting). **Hansuek Lee**: Data curation (supporting); Funding acquisition (supporting); Writing – review & editing (supporting). **Min-Kyo Seo**: Data curation (supporting); Funding acquisition (supporting); Writing – review & editing (supporting). **Sangin Kim**: Funding acquisition (supporting). **Hyounghan Kwon**: Writing – original draft (supporting); Writing – review & editing (supporting). **Hojoong Jung**: Conceptualization (equal); Funding acquisition (equal); Supervision (equal); Writing – original draft (equal); Writing – review & editing (equal). **Sang-Wook Han**: Conceptualization (equal); Funding acquisition (equal); Supervision (equal); Writing – review & editing (equal).

DATA AVAILABILITY

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

REFERENCES

[1] G. Moody *et al.*, "2022 roadmap on integrated quantum photonics," J. Phys.: Photonics **4**, 012501 (2022).

[2] E. Pelucchi *et al.*, "The potential and global outlook of integrated photonics for quantum technologies," Nat. Rev. Phys. **4**, 194–208 (2021).

[3] J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson, "Integrated photonic quantum technologies," Nat. Photonics **14**, 273–284 (2019).

[4] S. K. Liao *et al.*, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).

[5] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**, 595–604 (2014).

[6] V. Scarani *et al.*, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).

[7] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).

[8] L.-C. Kwek *et al.*, "Chip-based quantum key distribution," AAPPS Bull. **31**, 15 (2021).

[9] Q. Liu *et al.*, "Advances in chip-based quantum key distribution," Entropy **24**, 1334 (2022).

[10] D. Bunandar *et al.*, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X **8**, 021009 (2018).

[11] C. Ma *et al.*, "Silicon photonic transmitter for polarization-encoded quantum key distribution," Optica **3**, 1274–1278 (2016).

[12] T. K. Paraïso *et al.*, "A modulator-free quantum key distribution transmitter chip," npj Quantum Inf. **5**, 42 (2019).

[13] T. K. Paraïso *et al.*, "A photonic integrated quantum secure communication system," Nat. Photonics **15**, 850–856 (2021).

[14] G. Zhang *et al.*, "Polarization-based quantum key distribution encoder and decoder on silicon photonics," J. Lightwave Technol. **40**, 2052–2059 (2022).

[15] R. Sax *et al.*, "High-speed integrated QKD system," Photonics Res. **11**, 1007–1014 (2023).

[16] W. Li *et al.*, "High-rate quantum key distribution exceeding 110 Mb s^{-1}," Nat. Photonics **17**, 416–421 (2023).

[17] P. Sibson *et al.*, "Chip-based quantum key distribution," Nat. Commun. **8**, 13984 (2017).

[18] J. Dolphin *et al.*, "A hybrid integrated quantum key distribution transceiver chip," npj Quantum Inf. **9**, 84 (2023).

[19] R. Terhaar *et al.*, "Ultrafast quantum key distribution using fully parallelized quantum channels," Opt. Express **31**, 2675–2688 (2023).

[20] 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).

[21] J. You, Y. Wang, Q. Han, and J. An, "Silica-silicon based planar lightwave circuit quantum key distribution decoding chip for multi-protocol," Opt Laser. Technol. **145**, 107505 (2022).

[22] K. Wei *et al.*, "Resource-efficient quantum key distribution with integrated silicon photonics," Photonics Res. **11**, 1364–1372 (2023).

[23] G. Zhang *et al.*, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," Nat. Photonics **13**(12), 839–842 (2019).

[24] Y. Bian *et al.*, "Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip," Appl. Phys. Lett. **124**, 17 (2024).

[25] A. Boes *et al.*, "Lithium niobate photonics: Unlocking the electromagnetic spectrum," Science **379**, eabj4396 (2023).

[26] D. Zhu *et al.*, "Integrated photonics on thin-film lithium niobate," Adv. Opt. Photonics **13**, 242–252 (2021).

[27] M. He *et al.*, "High-performance hybrid silicon and lithium niobate Mach–Zehnder modulators for 100 Gbit s^{-1} and beyond," Nat. Photonics **13**, 359–364 (2019).

[28] M. Li *et al.*, "Lithium niobate photonic-crystal electro-optic modulator," Nat. Commun. **11**, 4123 (2020).

[29] C. Wang *et al.*, "Integrated lithium niobate electro-optic modulators operating at CMOS-compatible voltages," Nature **562**, 101–104 (2018).

[30] B. Desiatov, A. Shams-Ansari, M. Zhang, C. Wang, and M. Lončar, "Ultra-low-loss integrated visible photonics using thin-film lithium niobate," Optica **6**, 380–384 (2019).

[31] A. Shams-Ansari *et al.*, "Reduced material loss in thin-film lithium niobate waveguides," APL Photonics **7**, 081301 (2022).

[32] Y. He *et al.*, "Self-starting bi-chromatic $LiNbO_3$ soliton microcomb," Optica **6**, 1138–1144 (2019).

[33] A. Shams-Ansari *et al.*, "Thin-film lithium-niobate electro-optic platform for spectrally tailored dual-comb spectroscopy," Commun. Phys. **5**, 88 (2022).

[34] C. Wang *et al.*, "Monolithic lithium niobate photonic circuits for Kerr frequency comb generation and modulation," Nat. Commun. **10**, 978 (2019).

[35] C. Wang *et al.*, "Ultrahigh-efficiency wavelength conversion in nanophotonic periodically poled lithium niobate waveguides," Optica **5**, 1438–1441 (2018).

[36] J. Lu *et al.*, "Periodically poled thin-film lithium niobate microring resonators with a second-harmonic generation efficiency of 250,000%/W," Optica **6**, 1455–1460 (2019).

[37] R. Luo *et al.*, "On-chip second-harmonic generation and broadband parametric down-conversion in a lithium niobate microresonator," Opt. Express **25**, 24531–24539 (2017).

[38] A. Shams-Ansari *et al.*, "Electrically pumped laser transmitter integrated on thin-film lithium niobate," Optica **9**, 408–411 (2022).

[39] E. Lomonte *et al.*, "Single-photon detection and cryogenic reconfigurability in lithium niobate nanophotonic circuits," Nat. Commun. **12**, 6847 (2021).

[40] A. A. Sayem, R. Cheng, S. Wang, and H. X. Tang, "Lithium-niobate-on-insulator waveguide-integrated superconducting nanowire single-photon detectors," Appl. Phys. Lett. **116**, 151102 (2020).

[41] P. Dong *et al.*, "Low loss shallow-ridge silicon waveguides," Opt. Express **18**(14), 14474–14479 (2010).

[42] R. Pradip *et al.*, "Fast thermo-optic switching on silicon nitride platform through parity-time symmetry breaking," arXiv:2408.15139 (2024).

[43] Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim, "Experimental comparison between one-decoy and two-decoy implementations of the Bennett–Brassard 1984 quantum cryptography protocol," Phys. Rev. A **93**, 012322 (2016).

[44] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005).

[45] L. He *et al.*, "Low-loss fiber-to-chip interface for lithium niobate photonic integrated circuits," Opt. Lett. **44**(9), 2314–2317 (2019).

[46] C. Hu *et al.*, "High-efficient coupler for thin-film lithium niobate waveguide devices," Opt. Express **29**(4), 5397–5406 (2021).

[47] H.-S. Jang *et al.*, "Fabrication of a 3D mode size converter for efficient edge coupling in photonic integrated circuits," Opt. Express **33**(4), 6909–6917 (2025).

[48] 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).

[49] C. H. Park *et al.*, "2 × N twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing," npj Quantum Inf. **8**, 48 (2022).

[50] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).