Metropolitan Quantum Key Distribution with Silicon Photonics

Darius Bunandar,[1,2,*] Anthony Lentine,[2] Catherine Lee,[1,3] Hong Cai,[2] Christopher M. Long,[2] Nicholas Boynton,[2] Nicholas Martinez,[2] Christopher DeRose,[2] Changchen Chen,[1] Matthew Grein,[3] Douglas Trotter,[2] Andrew Starbuck,[2] Andrew Pomerene,[2] Scott Hamilton,[3] Franco N. C. Wong,[1] Ryan Camacho,[4] Paul Davids,[2] Junji Urayama,[2] and Dirk Englund[1]

[1]*Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[2]*Sandia National Laboratories, Albuquerque, New Mexico 87123, USA*
[3]*MIT Lincoln Laboratory, Lexington, Massachusetts 02421, USA*
[4]*Electrical and Computer Engineering Department, Brigham Young University, Provo, Utah 84602, USA*

(Received 30 August 2017; revised manuscript received 2 March 2018; published 6 April 2018)

Photonic integrated circuits provide a compact and stable platform for quantum photonics. Here we demonstrate a silicon photonics quantum key distribution (QKD) encoder in the first high-speed polarization-based QKD field tests. The systems reach composable secret key rates of 1.039 Mbps in a local test (on a 103.6-m fiber with a total emulated loss of 9.2 dB) and 157 kbps in an intercity metropolitan test (on a 43-km fiber with 16.4 dB loss). Our results represent the highest secret key generation rate for polarization-based QKD experiments at a standard telecom wavelength and demonstrate photonic integrated circuits as a promising, scalable resource for future formation of metropolitan quantum-secure communications networks.

DOI: 10.1103/PhysRevX.8.021009 Subject Areas: Photonics, Quantum Information

I. INTRODUCTION

Quantum key distribution (QKD) remains the only quantum-resistant method of sending secret information at a distance [1,2]. The first QKD system ever devised used polarization of photons to encode information [3,4]. QKD has since progressed rapidly to several deployed systems that can reach point-to-point secret key generation rates in upwards of 100 kbps [5–8] and to other photonic degrees of freedom: time [9–12], frequency [13–16], phase [17], quadrature [18–21], and orbital angular momentum [22]. While polarization remains an attractive choice for free-space QKD due to its robustness against turbulence [23–28], polarization is commonly thought to be unstable for fiber-based QKD. For this reason, there has been strong interest in translating the polarization QKD components into photonic integrated circuits (PICs), which provide a compact and phase-stable platform capable of correcting for polarization drifts in the channel. Recently, silicon-based polarization QKD encoders were used for laboratory QKD demonstrations [29,30], but their performance advantage over standard telecommunication components has yet to be demonstrated. Here we report the first field tests using a high-speed silicon photonics-based encoder for polarization-encoded QKD.

The silicon photonics platform allows for the integration of multiple high-speed photonic operations into a single compact circuit [31–34]. Operating at gigahertz bandwidth, a silicon photonics polarization QKD encoder can correct for polarization drifts with typical millisecond timescales in a metropolitan-scale fiber link. Furthermore, silicon nanophotonic devices are compatible with the existing complementary metal-oxide-semiconductor (CMOS) processes that have enabled monolithic integration of photonics and electronics, possibly leading to future widespread utilization of QKD.

The QKD encoder demonstrated here is manufactured using a CMOS-compatible process. The encoder combines a 10-Gbps Mach-Zehnder modulator (MZM) with interleaved grating couplers, which convert the polarization of a photon in an optical fiber into the path the photon takes in the integrated circuit, and vice versa. The high-speed polarization control is enabled by electro-optic carrier depletion modulation within the MZM [35]. We show the performance of the device in a local field test and an intercity field test. With a clock rate of 625 MHz, we generated secret keys at a rate of 1.039 Mbps and observed a bit error rate of 2% in the local test between two neighboring buildings connected by a 103.6-m fiber (with an additional 9 dB emulated loss). In the 43-km (16.4-dB

*dariusb@mit.edu

channel loss) intercity test between the cities of Cambridge and Lexington, we generated secret keys at a rate of 157 kbps and observed a bit error rate 2.8%. Both QKD operations are demonstrated to be secure against collective attacks in a composable security framework with a tight security parameter of $\varepsilon_{\text{sec}} = 10^{-10}$. Our results demonstrate how silicon photonics—supported by the currently existing CMOS technology—can pave the way for a high-speed metropolitan-scale quantum communication network.

II. SILICON PHOTONICS ENCODER

Our QKD encoder and its cross section are shown in Figs. 1(a)–1(c). Light is coupled in and out of the encoder using a standard fiber V-groove array of 250-μm pitch. Owing to the large index contrast between the silicon layer and the buried oxide, the encoder is compact within a total area of 0.75×1.5 mm^2. Polarization grating couplers are used to convert between polarization encoding in the input-output fibers and path encoding within the PIC. The unitary transformation is similar to that of a polarizing beam splitter (PBS). Within the PIC, the photons' paths—and their relative phases—are manipulated using a MZM with two internal and two external electro-optic phase modulators, which in turn manipulate the photon polarization in the output fiber.

The input polarization grating coupler separates light from the horizontal and vertical polarizations onto two different paths, both in the transverse-electric (TE) polarization: with its electric field oscillating parallel to the chip surface [36]. Any light inadvertently converted into the transverse-magnetic (TM) polarization in these waveguides is greatly attenuated by the phase modulators, which strongly support higher transmission in TE polarization over TM polarization. The grating coupler is a square array of holes, with 20 holes of lattice period of 575 nm in each direction. We measured ~10 dB loss through the grating coupler at our operating wavelength of 1480 nm. Although this loss is higher than that of typical silicon-on-insulator grating couplers at ~3 dB [37], the polarization grating coupler is suitable as an encoder for a QKD transmitter, where an average photon number per pulse of less than one is required for secure key distribution.

The electro-optic phase modulators in the MZM are based on depletion-mode free-carrier dispersion from a doped *p-i-n* junction superimposed on the optical mode [38,39]. The overlap between the optical mode and the free carriers results in free-carrier refraction [40], which can be controlled with gigahertz rf signals to achieve high-speed phase modulation.

The polarization states generated by the silicon photonics encoder have a purity of 1.000 ± 0.005, measured using a polarimeter. In Fig. 1(d), the relative phases of the internal phase shifters ($\Delta\theta$) as well as the relative phases of the external phase shifters ($\Delta\phi$) are swept with a reverse bias voltage between 0 and 8 V. For this voltage range, the polarization states lie on the surface of the Bloch sphere, indicating that they remain pure throughout.

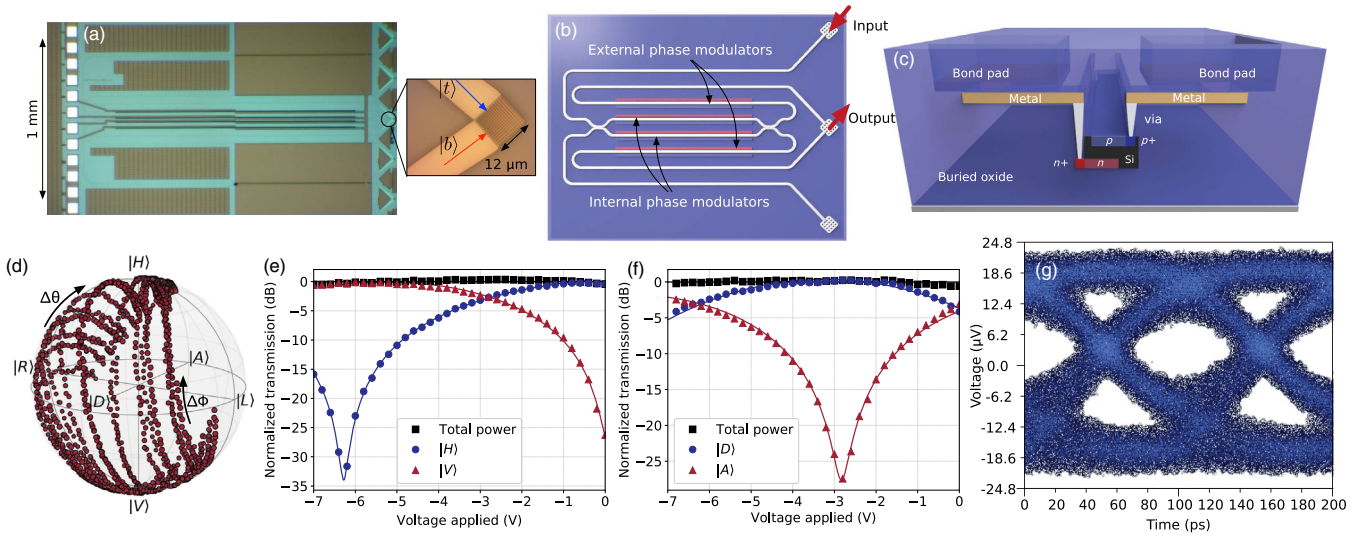

FIG. 1. (a) Optical micrograph of the silicon photonics encoder, along with a scanning electron micrograph of the polarization grating coupler. Only the inner three polarization grating couplers are parts of the encoder operation; the outer two couplers are present to help alignment with a fiber V-groove array. (b) Schematic diagram of the MZM encoder. The device uses two internal and two external electro-optic phase modulators, each of length 1.5 mm. (c) Schematic of the cross-sectional layer stack of the encoder. (d) Bloch sphere representation of the polarization states generated by the encoder as the internal ($\Delta\theta$) and the external ($\Delta\phi$) phase modulators are biased. (e),(f) Polarization modulation with the silicon photonics polarization modulator as measured in the two relevant bases. Polarization extinction ratio of more than 25 dB can be typically achieved. Negative voltage denotes reverse bias with regards to the doped *p-i-n* junction. Measurements in the Z basis and X basis are shown in (e) and (f), respectively. (g) Eye diagram of 10-Gbps polarization modulation in the Z basis: on state corresponds to $|V\rangle$ and off state corresponds to $|H\rangle$.

The Bennett-Brassard 1984 (BB84) QKD protocol [3] requires Alice to prepare three quantum states: two eigenstates of Z and an eigenstate of X [41,42]. Alice randomly chooses the basis she prepares in. When the Z basis is selected, Alice prepares either $|0_z\rangle = |H\rangle$ or $|1_z\rangle = |V\rangle$ with equal probabilities of $1/2$. Otherwise, when the X basis is selected, Alice prepares the state $|0_x\rangle = |D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$.

We prepared the three quantum states at high fidelity, as shown in Figs. 1(e) and 1(f), with a polarization extinction ratio better than 25 dB, which is required for low-error QKD operations. The internal and external phase modulators were configured to produce the state $(|t\rangle + |b\rangle)/\sqrt{2}$, which we take to be $|0_z\rangle$. rf signals of differing voltages were applied to one of the external phase modulators to generate $(|t\rangle + e^{i\phi}|b\rangle)/\sqrt{2}$, where ϕ is the applied phase shift. All of the three BB84 states can be generated by applying the phase shifts $\phi = 0$, $\pi/2$, and π. The polarization states were measured using a PBS followed by two InGaAs photodiodes. A polarization controller before the PBS allowed measurements in the two BB84 bases: the Z basis and the X basis.

As shown in the eye diagram in Fig. 1(g), the phase modulators allowed us to generate the polarization states at 10 Gbps. These measurements were acquired by using an inline polarizer placed at the output of the encoder that converts the polarization state $|V\rangle$ into an on state and the polarization state $|H\rangle$ into an off state. When the encoder was modulated at 6 Gbps or lower, not a single error was observed for a 5-min operation. At a 10-Gbps data rate, as shown here, we measured a low error rate of 9.0×10^{-10} s^{-1}.

III. FIELD TESTS

We performed two QKD field tests: a local test and an intercity test. Figure 2 shows a map of the greater Boston area, identifying the locations of Alice and Bob, together with the experimental setups implementing the asymmetric polarization-based BB84 protocol. Alice, located in the Compton Laboratories at MIT for both field tests, prepares the three polarization BB84 states at random. Bob measures in either the Z basis or the X basis using four superconducting nanowire single-photon detectors (SNSPDs) at a different location for each field test. He is located in the

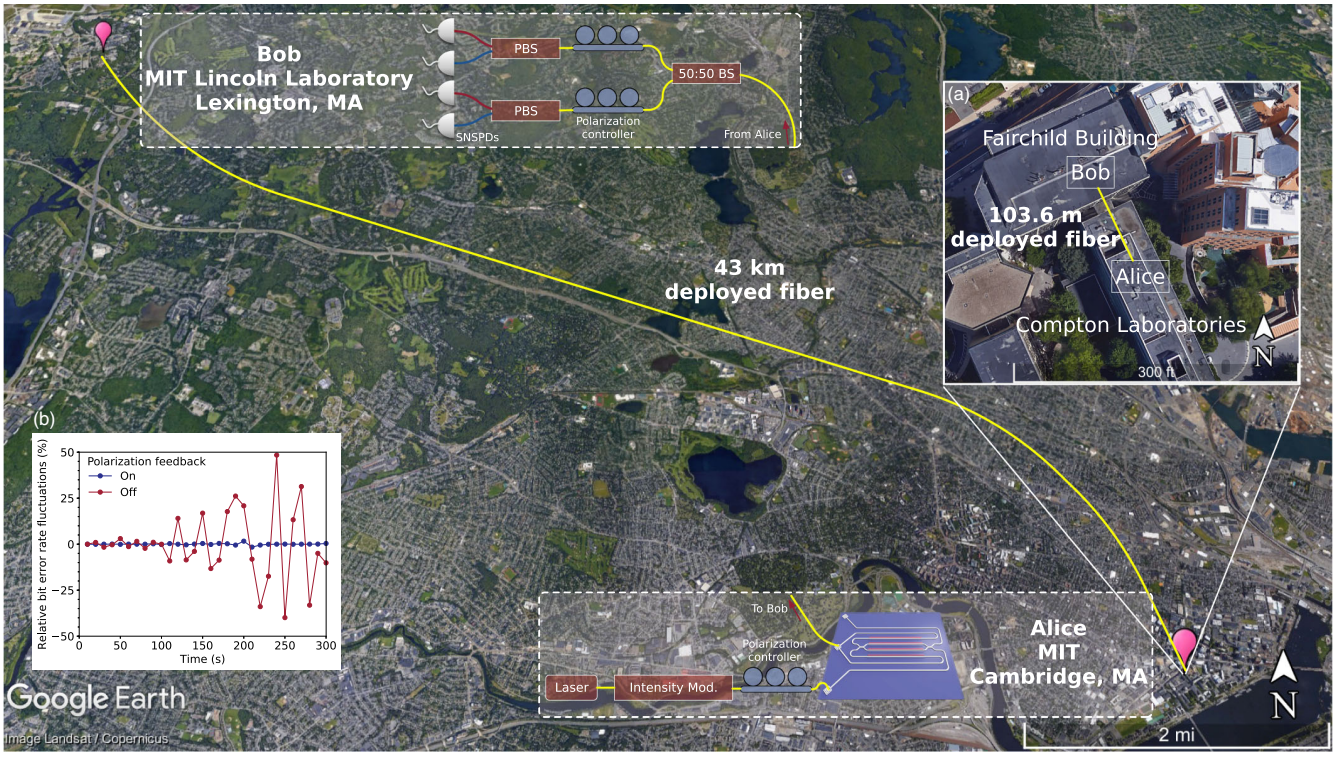

FIG. 2. Aerial view of the intercity QKD field test. Alice is located at Massachusetts Institute of Technology (MIT) in Cambridge and Bob is located at MIT Lincoln Laboratory in Lexington. Although the point-to-point distance between the two stations is ~18 km, they are connected by a 43-km dark fiber link. Alice consists of an attenuated laser source, an intensity modulator, and the silicon photonics polarization encoder. Bob consists of two polarizing beam splitters (PBSs) followed by four superconducting nanowire single-photon detectors (SNSPDs). Insets: (a) Close-up aerial view of the local QKD field test, where Alice and Bob are located in two adjacent MIT buildings connected by a 103.6-m deployed dark fiber link. Alice's and Bob's setups are the same as the ones used in the intercity test. (b) Fluctuations on the bit error rate with and without polarization feedback control, relative to the starting bit error rate. Imagery ©2017 Google. Map data from Google, Landsat/Copernicus.

Fairchild Building for the local test and at MIT Lincoln Laboratory in Lexington for the intercity test. Bob makes his basis choices using the polarization controller placed before each PBS.

Alice creates (not phase randomized) attenuated laser pulses of width 800 ps at 1480 nm [43] with a 625-MHz repetition rate. The pulses are modulated into the three BB84 polarization states by the silicon photonics encoder. Alice first calibrates for the polarization rotation through the channel, and dc reverse voltage biases are applied to the encoder such that the state $|D\rangle$ is generated by default. To generate the states $|H\rangle$ and $|V\rangle$, Alice applies synchronized rf pulses with a full width at half maximum of 400 ps. Phase randomization is achieved on the silicon photonics chip by applying a random, common phase offset on both external phase shifters [44]. To maximize the length of secret keys generated, Alice chooses to prepare either in the Z basis with a probability of $15/16$ or in the X basis with a probability of $1/16$.

For the local test, Alice sends her prepared states to Bob through a 103.6-m fiber link connecting the two laboratories. The loss through the link is 0.2 dB, and we emulated longer fiber distances by installing a variable optical attenuator before the channel. For the intercity test on deployed fiber connecting Cambridge and Lexington, the optical path length is 43 km long with 16.4-dB loss.

Bob detects the pulses he receives in either of the two bases with 50% probability to maximize the number of security-check events when the key-generating detectors are saturated. For the local test, Bob uses four individual WSi SNSPDs, each with a quantum efficiency greater than 85%, a timing resolution of ∼250 ps, a background dark count rate of ∼1000 counts/s, and a saturation count rate of $\sim 5 \times 10^6$ counts/s. For the intercity test, Bob uses four NbN SNSPD systems, each consisting of four interleaved NbN nanowires with a single optical fiber input with a quantum efficiency of 60%. Because only two out of the four interleaved nanowire outputs were used (due to the limited number of time-to-digital converter channels), the effective quantum efficiency was 30%. The timing resolution was ∼50 ps, the background dark count rate was ∼1000 counts/s, and the saturation count rate was $\sim 200 \times 10^6$ counts/s.

Alice and Bob only generate secret keys when both parties choose the Z basis. The quantum bit error rate e_{bit} is measured by checking the number of bits that have been flipped between their raw bit strings. On the other hand, the upper bound to the quantum phase error rate e_{ph}^U can be estimated from X-basis events along with the mismatched-basis events, where Alice and Bob choose different preparation and measurement bases (see Appendix A) [41,42].

An automated polarization feedback system is placed in the intercity channel between Alice and Bob, which can drift significantly on the timescale of the experiment. To correct for the drift, Alice sends a series of calibration signals and optimizes her dc voltage biases such that the error rate on both measurement bases is kept low. Single-photon detectors with good detection efficiency, such as the SNSPD systems above, are helpful for obtaining reliable error signals when optimizing for the voltage biases. As seen in Fig. 2(b), the relative fluctuations of e_{bit} (relative to its starting value) are limited to 2% with feedback, and to about 50% without feedback.

IV. COMPOSABLE SECRET KEY GENERATION

Figure 3 shows the performance of the QKD encoder in both field tests, in terms of the observed secret key rate (SKR), e_{bit}, and e_{ph}^U. For clarity, we plotted the SKRs against the channel loss and the equivalent fiber distance assuming an optimistic fiber loss of 0.2 dB/km. We kept the number of pulses sent from Alice to Bob at $N = 2.81 \times 10^{11}$ to maintain a uniform collection time of 450 s for each experiment, and analyzed the composable security

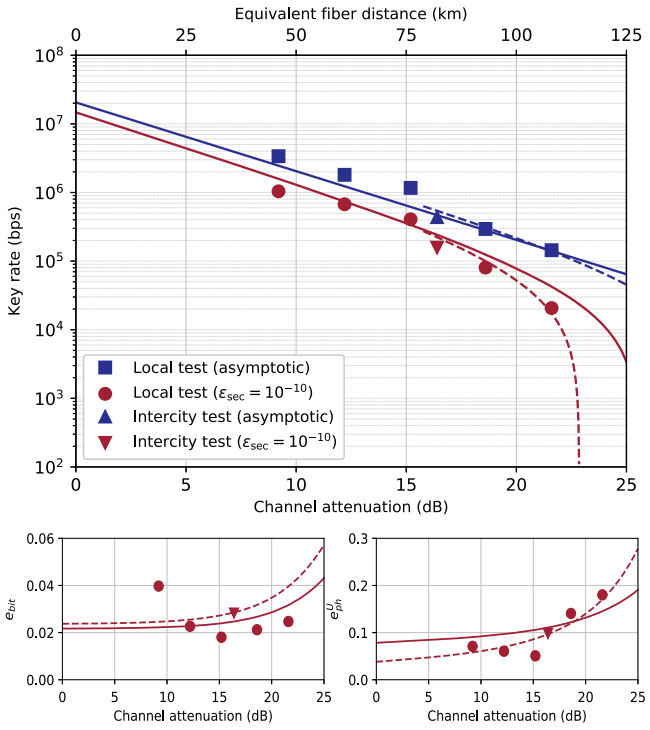

FIG. 3. Top: Experimental SKRs at different channel losses. The (blue) squares and upright triangles are asymptotic SKRs for the local test and the 43-km metropolitan intercity test, respectively. Similarly, the (red) circles and inverted triangles are the SKRs calculated within the composable security framework with $\varepsilon_{\mathrm{sec}} = 10^{-10}$ for the local test and the metropolitan field test, respectively. In the local tests, a variable attenuator is used to provide higher attenuation beyond the channel's 0.2-dB loss. Solid and dashed lines correspond to numerical simulations of the SKRs for the local test and the intercity test, respectively. Bottom: Bit error rate (e_{bit}) and upper bound to the phase error rate (e_{ph}^U) against channel attenuation. The symbols used here are the same as the ones above.

with a small security parameter of $\varepsilon_{\text{sec}} = 10^{-10}$—making use of the novel Chernoff bound recently proposed in Ref. [45].

For the local test, at a total channel attenuation of 9.2 dB, we obtained a SKR of 1.039 Mbps using mean photon numbers of 0.12, 0.012, and 0.003 for the signal and the two decoy states, chosen with probabilities 2/3, 2/9, and 1/9, respectively. The mean photon numbers were kept low to avoid detector saturation. The total channel attenuation was further increased from 9.2 to 21.2 dB to simulate longer fiber distances. We observed an average e_{bit} of ∼2%, except for the lowest channel attenuation where e_{bit} is higher at 3.97% as the WSi detectors are saturated. As expected from theoretical simulations, the upper bound to the phase error rate e_{ph}^{U} increased from 7.09% to 18.01% as we increased the channel attenuation.

For the metropolitan intercity test, we obtained a SKR of 157 kbps using mean photon numbers 0.5, 0.03, and 0.015 for the signal and the decoy states with the same probabilities as above. Here the mean photon numbers could be chosen higher while being well under the NbN detector systems' saturation point. We observed an e_{bit} of 2.82% and an e_{ph}^{U} of 9.81% in this 43-km experiment.

V. DISCUSSION AND OUTLOOK

To illustrate the progress entailed by our results, we summarize our work in Table I along with recent demonstrations of high-speed polarization-based QKD and other discrete-variable QKD field tests. Our work represents the highest observed SKR for any polarization-based QKD operations at comparable channel losses, and it performs comparably to other state-of-the-art QKD field demonstrations. It is also the first demonstration of the asymmetric loss-tolerant BB84 QKD protocol with guaranteed security against collective attacks [42]. The silicon photonics platform has enabled us to design a compact encoder with high-speed and high-fidelity operations using a CMOS-compatible process. This points to the possibility of low-cost and resilient QKD transmitters for metroscale quantum-secure networks.

PICs offer opportunities for further integration for both the transmitter and the receiver and for closing possible security flaws and side-channel attacks. Dense wavelength-division multiplexing has been one major thrust in classical communications, and a compact solution is available in silicon photonics by using an array of add-drop ring resonators [48,49]. This scheme can be integrated with our current QKD encoder design with only minimal changes in the footprint. Furthermore, single photon detectors have been integrated into silicon photonics [50], showing the possibility of a compact QKD receiver.

Moreover, the configurability of the silicon photonics platform allows for complex monitoring circuits that protect against side-channel attacks [51]. For example, a Trojan horse attack can be thwarted by placing watchdog detectors in our silicon photonics chip [52,53]. Possible detector vulnerabilities, such as the detector blinding attack

TABLE I. Comparison of high-rate polarization-based QKD experiments and other high-rate discrete-variable QKD field tests.

Reference	Clock rate (MHz)	λ (nm)	Fiber length (km)	Loss (dB)	SKR (kbps)	SKR normalized to 10 dB (kbps)	Finite key ε_{sec}	Protocol	Notes
[46]	1000	850	4.2	9.24	130	109	Assumes asymptotic	B92	Polarization, APDs, VCSELs
[47]	625	850	1	2.2	2100	349	Assumes asymptotic	B92	Polarization, APDs, VCSELs
[29]	10	1550	⋯	0.0	0.95	0.10	Assumes asymptotic	BB84	Polarization, APDs, Si PIC
[30]	1000	1550	20	4.0	329	83	Assumes asymptotic	BB84	Polarization, SNSPDs, Si PIC
[5]	1000	1550	50†	14.5	304	857	Assumes asymptotic	BB84	Time bin, APDs, long term
[6]	1000	1547.72	22†	12.6	230	419	Assumes asymptotic	BB84	Time bin, APDs, long term
[7]	1000	1550.92 1550	45†	14.5	300	846	10^{-10}	BB84	Time bin, APDs, long term
This work	625	1480	0.1† + attenuator	9.2	1039	864	10^{-10}	BB84	Polarization, SNSPDs, Si PIC
			43†	16.4	157	685			

†Dagger (†) represents a deployed fiber link. For each experiment, we also note the choice of photonic encoding, the choice of single-photon detectors used, the use of integrated optics, and whether the trial was continuously operating for more than 24 h. VCSELs, vertical-cavity surface-emitting lasers; APDs, avalanche photodiodes; SNSPDs, superconducting nanowire single-photon detectors.

[54,55], can be eliminated using the measurement-device-independent (MDI) configuration [9,56,57].

PICs also offer new opportunities of quantum sources for QKD applications. Heterogeneous bonding of active laser III–V materials, such as indium phosphide (InP), onto the silicon photonics QKD encoder would enable a fully integrated silicon photonics QKD transmitter along with the light source [58–61]. QKD transmitters based on InP have been demonstrated [12]. Furthermore, the PIC platform allows for the construction of identical ring resonators of quality factor above 10^7 with lithographic precision [62]. The ring resonators, when operated as add-drop filters for broadband light sources based on spontaneous emissions whose phases are intrinsically random, can generate lithographically defined indistinguishable light for MDI QKD. Recent demonstrations of efficient spontaneous four-wave mixing with silicon ring resonators also promise the possibility of identical integrated single-photon sources for MDI QKD [63–65].

In conclusion, we have demonstrated short-range and metroscale QKD field tests using a silicon photonics chip, reaching secret key rates of 1.039 Mbps and 157 kbps, respectively. These are the first polarization-based QKD field tests on deployed fiber links, which were typically deemed too unstable for high-fidelity transmission of polarization states. The PIC platform provides a compact and phase-stable platform for high-speed QKD that is well suited for further scaling by wavelength division multiplexing.

ACKNOWLEDGMENTS

We thank Evan Gabhart (MIT), Zheshen Zhang (MIT), Nicholas Harris (MIT), and P. Ben Dixon (MIT Lincoln Laboratory) for their helpful suggestions and discussion. We also acknowledge the assistance of Di Zhu (MIT), Cheng Peng (MIT), and Tsung-Ju Lu (MIT) in electrically packaging the silicon photonic integrated circuit. D. E., D. B., C. C., and F. N. C. W. acknowledge support from the Office of Naval Research CONQUEST program. D. E. and D. B. also acknowledge support from the Air Force Office of Scientific Research program FA9550-16-1-0391, supervised by Gernot Pomrenke, and from Samsung Advanced Institute of Technology Global Research Outreach program. We thank the anonymous reviewers for their suggestions to improve the decoy state analysis with novel Chernoff bound methods and to consider the realization of phase-encoded BB84 QKD protocol using our silicon photonics QKD encoder. This work was partly supported by the U.S. Department of Energy through the Sandia Enabled Communications and Authentication Network using Quantum Key Distribution (SECANT QKD) Grand Challenge, and performed, in part, at the Center for Integrated Nanotechnologies, an Office of Science User Facility operated for the U.S. Department of Energy Office of Science. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under Contract No. DE-NA0003525. This material is based upon work supported by the Office of the Assistant Secretary of Defense for Research and Engineering under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Assistant Secretary of Defense for Research and Engineering.

Note added.—Recently, we became aware of another polarization-based QKD encoder using polarization grating coupler that was developed independently [30].

APPENDIX A: PROTOCOL DESCRIPTION

We consider an asymmetric three-state BB84 protocol. In particular, Alice randomly selects to prepare a qubit in either the Z basis or the X basis with probabilities p_Z^A and $p_X^A = 1 - p_Z^A$, respectively. Similarly, Bob independently and randomly chooses to measure in either of the two bases with probabilities p_Z^B and $p_X^B = 1 - p_Z^B$. In our experiments, $p_Z^A = 15/16$, $p_X^A = 1/16$, $p_Z^B = 1/2$, and $p_X^B = 1/2$. The mean photon number of each laser pulse in the experiment is chosen randomly from three different settings: μ_1, μ_2, μ_3. They satisfy the relation $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geq 0$.

(1) *Preparation.*—For each laser pulse, Alice randomly chooses the mean photon number $\langle N \rangle \in \{\mu_1, \mu_2, \mu_3\}$ with probabilities p_{μ_1}, p_{μ_2}, and $p_{\mu_3} = 1 - p_{\mu_1} - p_{\mu_2}$, respectively. Alice then selects the basis $a \in \{Z, X\}$ with probabilities p_Z^A and $p_X^A = 1 - p_Z^A$, respectively. If she has selected the Z basis, then she randomly sends either $|0_z\rangle = |H\rangle$ or $|1_z\rangle = |V\rangle$ to Bob with equal probabilities. If the X basis was selected, she sends the $|0_x\rangle = |D\rangle$ to Bob. She records the bit value of the state she has sent in x.

(2) *Measurement.*—Bob measures the signals he received in the measurement basis $b \in \{Z, X\}$ with probabilities p_Z^B and $p_X^B = 1 - p_Z^B$, respectively. Bob performs the measurements with four single-photon detectors (one per basis). He then records his measurement as one of the four possible outcomes: $\{0, 1, \varnothing, \perp\}$. 0 and 1 are the bit values (H and V in the Z basis, and D and A in the X basis), $\varnothing$ represents no detection, and $\perp$ represents a double detection. Bob records the outcome in y, and he assigns a random bit value if a double detection is observed.

(3) *Basis reconciliation and sifting.*—Alice and Bob announce their bases and intensity choices over an

authenticated public channel. They then place their records into one of the following sets:

(a) key-generation sets:
$\mathcal{Z}_\mu = \{i|a_i = b_i = Z, \langle N_i\rangle = \mu, y_i \neq \varnothing\}$;
(b) security-check sets:
$\mathcal{X}_\mu = \{i|a_i = b_i = X, \langle N_i\rangle = \mu, y_i \neq \varnothing\}$;
(c) mismatched-basis sets:
$\mathcal{Z}^j\mathcal{X}^k_\mu = \{i|a_i = Z, b_i = X, \langle N_i\rangle = \mu, x_i = j, y_i = k\}$.

Steps 1–3 are repeated until the size of each set has reached a certain length previously agreed by both parties. Alice and Bob generate a raw key pair $(\mathbf{Z}_A, \mathbf{Z}_B)$ by choosing a random sample from the set $\mathcal{Z} = \cup_\mu \mathcal{Z}_\mu$. Following Ref. [66], we generate secret keys from all intensity settings.

(4) *Parameter estimation.*—Alice and Bob then compute the bounds to the number of vacuum and single-photon events within the set $\mathcal{Z}$ using the security-check sets and the mismatched-basis sets. Next, they estimate the number of phase errors within the single-photon events, and check if the phase error rate $e^U_{\rm ph}$ is less than the predetermined threshold value $e_{\rm phase,tol}$. If $e^U_{\rm ph} > e_{\rm phase,tol}$, then they abort the protocol, otherwise they proceed.

(5) *Postprocessing.*—Alice and Bob perform error correction for $(\mathbf{Z}_A, \mathbf{Z}_B)$ over their authenticated public channel, revealing $\lambda_{\rm EC}$ bits. To verify that they have identical secret keys, they compute a two-universal hash function that publishes $\lceil \log_2 1/\varepsilon_{\rm cor}\rceil$ bits. If the protocol passes all the above steps, they then perform privacy amplification to extract a secret key pair $(\mathbf{K}_A, \mathbf{K}_B)$ with each key of length ℓ bits.

APPENDIX B: SECURITY ANALYSIS

We consider the loss-tolerant asymmetric BB84 protocol in the composable security framework [41,42]. A QKD protocol is considered to be secure if it is both correct and secret. The protocol is secret when the pair of keys $\mathbf{K}_A$ and $\mathbf{K}_B$ are identical except for some small probability $\varepsilon_{\rm cor}$; i.e., $\Pr[\mathbf{K}_A \neq \mathbf{K}_B] = \varepsilon_{\rm cor}$. The probability $\varepsilon_{\rm cor}$ is determined by the failure probability of the two-universal hash function. Furthermore, the protocol is secret if the quantum state $\rho_{K_A E}$ that describes the correlation between Alice's key and Eve's quantum system is $\varepsilon_{\rm sec}$ close to $\omega_{K_A} \otimes \rho_E$, where ω_{K_A} describes a uniform distribution of all bit strings. In other words,

$$\frac{1}{2}\|\rho_{K_A E} - \omega_{K_A} \otimes \rho_E\| \leq \varepsilon_{\rm sec}. \tag{B1}$$

Within this composable security framework, the secret key length is

$$\ell \geq \left\lfloor m^L_0 + m^L_1[1 - h(e^U_{\rm ph}) - \xi h(e_{\rm bit})] - \log_2\frac{4}{\varepsilon^2_{\rm sec}} - \log_2\frac{2}{\varepsilon_{\rm cor}}\right\rfloor, \tag{B2}$$

where h is the binary entropy function, and m^L_0 and m^L_1 are the lower bounds to the number detections due to vacuum and single photons, respectively. $e^U_{\rm ph}$ is an upper bound to the phase error rate, which can be computed using the methods outlined in Ref. [42]. $e_{\rm bit}$ is the quantum bit error rate for the key-generating basis, and ξ represents the error correction inefficiency—set at 1.15 for our calculations. For simplicity, we set all 17 failure probabilities related to estimating m^L_0, m^L_1, and $e^U_{\rm ph}$ as $\varepsilon = \varepsilon^2_{\rm sec}/17$.

APPENDIX C: IMPROVED DECOY STATE ANALYSIS

We take advantage of the improved decoy state analysis [45] and apply them to obtain the security quantities m^L_0, m^L_1, and $e^U_{\rm ph}$ [42].

1. Lower bound on vacuum contributions

We wish to calculate the value of m^L_0 which is the *observed* lower bound on the number of events where (i) Alice generates a vacuum state with the signal intensity setting μ_1 in the Z basis and (ii) Bob detects in the Z basis.

First, let $\langle m_0\rangle^L$ be the lower bound on the *average* number of such events:

$$\langle m_0\rangle^L = \frac{p_{\mu_1} e^{-\mu_1}}{\mu_2 - \mu_3}\left(\frac{\mu_2 e^{\mu_3}}{p_{\mu_3}}\langle Z\rangle^L_{\mu_3} - \frac{\mu_3 e^{\mu_2}}{\mu_2}\langle Z\rangle^U_{\mu_2}\right), \tag{C1}$$

where the parameter $\langle Z\rangle^{L(U)}_{\mu_i}$ is defined as the lower (upper) bound on the *expectation value* of the number of detection events when Alice chooses the basis setting Z at intensity μ_i and Bob chooses the basis setting Z.

Alice and Bob, given the *observed value* $|Z|_{\mu_i}$, can calculate the confidence interval of the underlying expectation value with the failure probability ε. Using the Chernoff bound for independent Bernoulli binary random variables $\chi_j \in \{0, 1\}$, and defining $\chi = \sum^n_{j=1}\chi_j \equiv |Z|_{\mu_i}$ and $\langle\chi\rangle \equiv \langle Z\rangle_{\mu_i}$, we obtain

$$\begin{aligned}\Pr[|Z|_{\mu_i} > (1+\delta^L)\langle Z\rangle_{\mu_i}] &< g(\delta^L, \langle Z\rangle_{\mu_i}),\\ \Pr[|Z|_{\mu_i} < (1-\delta^U)\langle Z\rangle_{\mu_i}] &< g(-\delta^U, \langle Z\rangle_{\mu_i}),\end{aligned} \tag{C2}$$

where $g(\delta, \langle\chi\rangle) \equiv [(e^\delta)/(1+\delta)^{1+\delta}]^{\langle\chi\rangle}$. We further define $\langle Z\rangle^L_{\mu_i} \equiv |Z|_{\mu_i}/(1+\delta^L)$ and $\langle Z\rangle^U_{\mu_i} \equiv |Z|_{\mu_i}/(1-\delta^U)$, such that the two equations [Eq. (C2)] above can be interpreted as the probabilities that the expectation value deviates from the confidence interval. We desire the two probabilities to be small, i.e., upper bounded by some small failure probability ε.

The confidence interval of the expectation value is then obtained by (numerically) solving

$$g(\delta^L, \langle Z\rangle_{\mu_i}) = \frac{\varepsilon}{2} \quad \text{and} \quad g(-\delta^U, \langle Z\rangle_{\mu_i}) = \frac{\varepsilon}{2} \tag{C3}$$

for δ^L and δ^U. For large values of $\langle Z\rangle^L_{\mu_i} \geq 6\beta = -6\ln(\varepsilon/2)$ (which is the case in our measurements), the solutions are approximately [45]

$$\delta^L = \delta^U \approx \frac{3\beta + \sqrt{\beta^2 + 8\beta|Z|_{\mu_i}}}{2(|Z|_{\mu_i} - \beta)}, \tag{C4}$$

from which Alice and Bob can estimate the lower (upper) bound $\langle Z\rangle^{L(U)}_{\mu_i}$.

From here, we can obtain a second confidence interval for the observed value m_0 using the symmetric Chernoff bound:

$$\Pr\left[|m_0 - \langle m_0\rangle| \geq \delta\langle m_0\rangle\right] \leq 2e^{-\delta^2\langle m_0\rangle/(2+\delta)} = \varepsilon, \tag{C5}$$

which can be rewritten to

$$\Pr\left[m_0^L \leq m_0 \leq m_0^U\right] > 1 - \varepsilon, \tag{C6}$$

for

$$m_0^L \equiv (1-\delta)\langle m_0\rangle, \quad m_0^U \equiv (1+\delta)\langle m_0\rangle, \quad \delta = \frac{\beta + \sqrt{\beta^2 - 8\beta\langle m_0\rangle}}{2\langle m_0\rangle}. \tag{C7}$$

However, since Alice and Bob can estimate only the confidence interval of the expectation value $\langle n_0(a^xb^y)\rangle \in [\langle n_0(a^xb^y)\rangle^L, \langle n_0(a^xb^y)\rangle^U]$, they can only obtain worse *observed* lower bound:

$$m_0^L = (1-\delta)\langle n_0(a^xb^y)\rangle^L, \quad \delta = \frac{\beta + \sqrt{\beta^2 - 8\beta\langle m_0\rangle^L}}{2\langle m_0\rangle^L}. \tag{C8}$$

2. Lower bound on single-photon contributions

Alice and Bob also need to obtain m_1^L, which is the *observed* lower bound on the number of events where (a) Alice generates a single-photon state with the signal intensity setting μ_1 in the Z basis and (b) Bob detects in the Z basis.

Let $\langle m_1\rangle^L$ be the lower bound on the *average* number of such events, then

$$\langle m_1\rangle^L = \frac{p_{\mu_1}\mu_1^2 e^{-\mu_1}}{(\mu_2-\mu_3)(\mu_1-\mu_2-\mu_3)}\left[\frac{e^{\mu_2}}{p_{\mu_2}}\langle Z\rangle^L_{\mu_2} - \frac{e^{\mu_3}}{p_{\mu_3}}\langle Z\rangle^U_{\mu_3} + \frac{\mu_2^2-\mu_3^2}{\mu_1^2}\frac{e^{\mu_1}}{p_{\mu_1}}(\langle m_0\rangle^L - \langle Z\rangle^U_{\mu_1})\right]. \tag{C9}$$

It is then straightforward to use the Chernoff bound analyses outlined in Appendix C 1 to obtain the value of m_1^L.

3. Upper bound on phase error rate

To place an upper bound to the phase error rate (e^U_{ph}), Alice and Bob need to find the lower and upper bounds to $\langle a^xb^y;k\rangle$ [42] which are the *mean* number of events where (a) Alice generates a k-photon state (with $k \in \{0,1\}$) with the signal intensity setting μ_1 in the basis setting $a \in \{Z,X\}$ to encode bit value $x \in \{0,1\}$ and (b) Bob measures bit $y \in \{0,1\}$ using basis setting $b \in \{Z,X\}$.

These quantities are labeled as $\underline{\text{Decoy}}_k(ax,by)$ and $\overline{\text{Decoy}}_k(ax,by)$ in Ref. [42].

Let $|a^xb^y|_{\mu_i}$ be the *observed* number of events where Alice prepares bit x in basis setting a and Bob detects bit y in basis setting b. Then, we can obtain bounds on the mean vacuum and single-photon contributions $\langle a^xb^y;k\rangle$ using similar equations to Eqs. (C1) and (C9):

$$\begin{aligned}
\langle a^xb^y;0\rangle^L &= \frac{p_{\mu_1}e^{-\mu_1}}{\mu_2-\mu_3}\left(\frac{\mu_2 e^{\mu_3}}{p_{\mu_3}}\langle a^xb^y\rangle^L_{\mu_3} - \frac{\mu_3 e^{\mu_2}}{\mu_2}\langle a^xb^y\rangle^U_{\mu_2}\right),\\
\langle a^xb^y;1\rangle^L &= \frac{p_{\mu_1}\mu_1^2 e^{-\mu_1}}{(\mu_2-\mu_3)(\mu_1-\mu_2-\mu_3)} \times \left[\frac{e^{\mu_2}}{p_{\mu_2}}\langle a^xb^y\rangle^L_{\mu_2} - \frac{e^{\mu_3}}{p_{\mu_3}}\langle a^xb^y\rangle^U_{\mu_3} + \frac{\mu_2^2-\mu_3^2}{\mu_1^2}\frac{e^{\mu_1}}{p_{\mu_1}}(\langle a^xb^y;0\rangle^L - \langle a^xb^y\rangle^U_{\mu_1})\right],
\end{aligned} \tag{C10}$$

and

$$\langle a^xb^y;1\rangle^U = \frac{p_{\mu_1}\mu_1 e^{-\mu_1}}{\mu_2-\mu_3}\left[\frac{e^{\mu_2}}{p_{\mu_2}}\langle a^xb^y\rangle^U_{\mu_2} - \frac{e^{\mu_3}}{p_{\mu_3}}\langle a^xb^y\rangle^U_{\mu_3}\right]. \tag{C11}$$

To obtain the lower and upper bounds to the mean, i.e., $\langle a^xb^y\rangle^{L(U)}_{\mu_i}$, we can repeat the analysis in Sec. C 1 after redefining $\chi = \sum_{j=1}^n \chi_j \equiv |a^xb^y|_{\mu_i}$ and $\langle\chi\rangle \equiv \langle a^xb^y\rangle_{\mu_i}$.

APPENDIX D: EXPERIMENTAL RAW COUNTS

The observed raw counts are tabulated in Table II.

TABLE II. Experimental raw counts observed during the local tests and the 43-km intercity test. The heading $|a^x b^y|_{\mu_i}$ refers to the recorded number of events where Alice prepares bit x with basis choice $a \in \{Z,X\}$ and Bob detects bit y with basis choice $b \in \{Z,X\}$.

Channel and loss	μ_i	$\lvert Z^0Z^0\rvert_{\mu_i}$	$\lvert Z^1Z^0\rvert_{\mu_i}$	$\lvert Z^0Z^1\rvert_{\mu_i}$	$\lvert Z^1Z^1\rvert_{\mu_i}$	$\lvert Z^0X^0\rvert_{\mu_i}$	$\lvert Z^1X^0\rvert_{\mu_i}$	$\lvert X^0X^0\rvert_{\mu_i}$	$\lvert Z^0X^1\rvert_{\mu_i}$	$\lvert Z^1X^1\rvert_{\mu_i}$	$\lvert X^0X^1\rvert_{\mu_i}$
Local	0.12	6.44×10^8	2.68×10^7	2.49×10^7	5.77×10^8	2.92×10^8	3.04×10^8	7.38×10^7	3.18×10^8	2.40×10^8	3.80×10^6
9.2 dB	0.012	2.40×10^7	3.96×10^5	3.68×10^5	2.11×10^7	1.08×10^7	1.13×10^7	2.79×10^6	1.14×10^7	8.48×10^6	1.07×10^5
	0.003	2.51×10^6	4.79×10^4	3.89×10^4	2.22×10^6	1.16×10^6	1.21×10^6	3.04×10^5	1.24×10^6	9.21×10^5	1.38×10^4
Local	0.12	3.05×10^8	6.47×10^6	7.52×10^6	2.90×10^8	1.35×10^8	1.45×10^8	3.59×10^7	1.45×10^8	1.23×10^8	1.48×10^6
12.2 dB	0.012	1.06×10^7	1.36×10^5	1.60×10^5	1.02×10^7	4.89×10^6	5.22×10^6	1.31×10^6	5.17×10^6	4.35×10^6	5.65×10^4
	0.003	1.13×10^6	2.35×10^4	2.13×10^4	1.03×10^6	5.12×10^5	5.60×10^5	1.37×10^5	5.51×10^5	4.75×10^5	8.99×10^3
Local	0.12	1.57×10^8	2.55×10^6	3.10×10^6	1.49×10^8	7.05×10^7	7.51×10^7	1.87×10^7	7.42×10^7	6.29×10^7	7.55×10^5
15.2 dB	0.012	6.80×10^6	8.90×10^4	1.01×10^5	6.34×10^6	3.06×10^6	3.25×10^6	8.02×10^5	3.20×10^6	2.71×10^6	3.56×10^4
	0.003	6.24×10^5	2.08×10^4	1.67×10^4	5.68×10^5	2.90×10^5	2.98×10^5	7.32×10^4	3.08×10^5	2.72×10^5	6.85×10^3
Local	0.12	7.67×10^7	9.43×10^5	1.88×10^6	6.34×10^7	3.08×10^7	3.08×10^7	7.52×10^6	2.53×10^7	2.03×10^7	1.82×10^5
18.2 dB	0.012	2.70×10^6	5.78×10^4	1.80×10^5	2.32×10^6	1.49×10^6	1.50×10^6	3.11×10^5	8.81×10^5	7.06×10^5	4.75×10^3
	0.003	2.76×10^5	1.85×10^4	7.31×10^4	2.76×10^5	3.32×10^5	3.34×10^5	5.31×10^4	9.26×10^4	7.21×10^4	1.34×10^3
Local	0.12	3.72×10^7	4.46×10^5	1.05×10^6	3.07×10^7	1.58×10^7	1.58×10^7	3.71×10^6	1.22×10^7	9.75×10^6	8.37×10^4
21.2 dB	0.012	1.58×10^6	4.35×10^4	1.67×10^5	1.41×10^6	1.07×10^6	1.07×10^6	2.08×10^5	5.11×10^5	4.20×10^5	4.37×10^3
	0.003	1.72×10^5	1.97×10^4	7.42×10^4	2.00×10^5	2.80×10^5	2.86×10^5	4.47×10^4	5.84×10^4	4.46×10^4	1.28×10^3
Intercity	0.5	1.47×10^8	4.31×10^6	2.89×10^6	1.08×10^8	4.24×10^7	4.79×10^7	1.03×10^7	4.85×10^7	3.38×10^7	5.03×10^5
16.4 dB	0.03	3.51×10^6	1.88×10^5	1.15×10^5	2.22×10^6	8.94×10^5	1.08×10^6	2.35×10^5	1.30×10^6	6.74×10^5	1.20×10^4
	0.015	6.85×10^5	6.75×10^4	4.76×10^4	4.98×10^5	2.05×10^5	2.43×10^5	4.93×10^4	2.38×10^5	1.52×10^5	4.14×10^3

APPENDIX E: POLARIZATION-MODE-EFFICIENT BB84 QKD WITH PHASE ENCODING

The same silicon photonics polarization QKD encoder can be converted to realize polarization-mode-efficient BB84 QKD with phase encoding [67]. In this scheme, Alice encodes information in the phase of two consecutive photon pulses in *both* polarizations. In this regard, the QKD scheme is polarization-mode efficient because both modes are used, and two bits of information can be generated per transmission through the quantum channel.

Figure 4 shows a schematic of the phase-encoded QKD system. Alice controls the intensity of the weak coherent pulse in each polarization using an intensity modulator, which controls the mean number of photons entering the chip, and two internal phase modulators, which distribute the photons between the horizontal and vertical polarization modes. Adjusting the intensity modulator and the internal

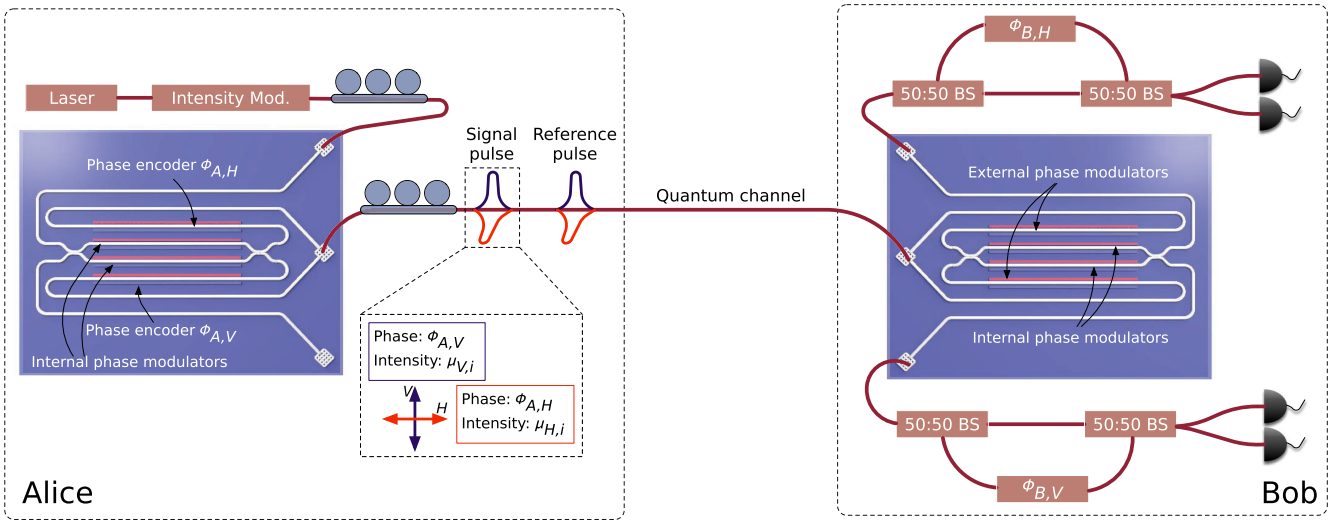

FIG. 4. Schematic diagram of polarization-mode-efficient phase-encoded BB84 QKD which encodes information in both polarizations using the silicon photonics QKD encoder. Alice encodes information in both polarization modes using a single silicon photonics encoder. Bob, on the other hand, uses another copy of the silicon photonics chip to undo the polarization unitary transformation of the channel. At each output, he detects using an unbalanced Mach-Zehnder interferometer terminated by two single-photon detectors.

phase modulators at every clock cycle allows Alice to change the intensity of each polarization pulse ($\mu_{H,i}$ and $\mu_{V,i}$, where $i \in \{1,2,3\}$ is the three decoy state intensities) for decoy state modulation. For every clock cycle, two pulses are generated—a reference pulse (weak or strong) and a signal pulse—in both polarizations. She then encodes her bit choice and basis choice by independently choosing the relative phases $\phi_{A,H}$ and $\phi_{A,V}$ between the two horizontal and vertical pulses, respectively. Each relative phase is encoded using one of the two external phase modulators. Referring to Fig. 4, the relative phase $\phi_{A,H}$ is encoded using the top external phase modulator and $\phi_{A,V}$ is encoded using the bottom external phase modulator. Choosing the relative phase $\{0,\pi\}$ and $\{\pi/2, 3\pi/2\}$ corresponds to bit values $\{0,1\}$ in the Z and X basis, respectively. Phase randomization is achieved by applying a random phase offset on both the reference and signal pulses—chosen independently for each polarization. Since each orthogonal polarization mode is modulated independently of each other, we can consider each mode being an independent quantum channel.

The quantum channel, in addition to loss, applies a drifting polarization unitary transformation. Bob uses another copy of the silicon photonics chip to undo the unitary transformation of the channel, such that Alice's horizontal pulses exits the chip through the top grating coupler and Alice's vertical pulses through the bottom grating coupler. (Bob also has to correct for possible polarization drifts of the channel using his silicon chip.) For each polarization, Bob detects the signals using an unbalanced Mach-Zehnder interferometer, which interferes the reference pulse and the signal pulse. Bob chooses his detection basis by either applying a 0-phase shift on $\phi_{B,H/V}$ for the Z basis or a $\pi/2$-phase shift on $\phi_{B,H/V}$ for the X basis. The pulses would arrive at Bob's detectors in three different time slots: early, middle, and late. Bob keeps only the middle clicks which are produced from the interference.

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

[2] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The Security of Practical Quantum Key Distribution*, Rev. Mod. Phys. **81**, 1301 (2009).

[3] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Experimental Quantum Cryptography*, J. Cryptol. **5**, 3 (1992).

[5] M. Sasaki, *Field Test of Quantum Key Distribution in the Tokyo QKD Network*, Opt. Express **19**, 10387 (2011).

[6] K.-i. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, *Maintenance-Free Operation of WDM Quantum Key Distribution System through a Field Fiber over 30 Days*, Opt. Express **21**, 31395 (2013).

[7] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, *High Speed Prototype Quantum Key Distribution System and Long Term Field Trial*, Opt. Express **23**, 7583 (2015).

[8] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. B. Dixon, F. N. C. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, *High-Rate Field Demonstration of Large-Alphabet Quantum Key Distribution*, arXiv:1611.01139.

[9] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W. -B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, *Quantum Key Distribution without Detector Vulnerabilities Using Optically Seeded Lasers*, Nat. Photonics **10**, 312 (2016).

[10] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, *Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre*, Nat. Photonics **9**, 163 (2015).

[11] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, *Measurement-Device-Independent Quantum Key Distribution over 200 km*, Phys. Rev. Lett. **113**, 190501 (2014).

[12] 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).

[13] C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R. D. Horansky, V. B. Verma, A. E. Lita, R. P. Mirin, F. Marsili, M. D. Shaw, S. W. Nam, G. W. Wornell, F. N. C. Wong, J. H. Shapiro, and D. Englund, *Entanglement-Based Quantum Communication Secured by Nonlocal Dispersion Cancellation*, Phys. Rev. A **90**, 062331 (2014).

[14] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, *Large-Alphabet Quantum Key Distribution Using Energy-Time Entangled Bipartite States*, Phys. Rev. Lett. **98**, 060503 (2007).

[15] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong, *Photon-Efficient Quantum Key Distribution Using Time-Energy Entanglement with High-Dimensional Encoding*, New J. Phys. **17**, 022002 (2015).

[16] J. Nunn, L. J. Wright, C. Söller, L Zhang, I. A. Walmsley, and B. J. Smith, *Large-Alphabet Time-Frequency Entangled Quantum Key Distribution by Means of Time-to-Frequency Conversion*, Opt. Express **21**, 15959 (2013).

[17] K. Inoue, E. Waks, and Y. Yamamoto, *Differential Phase Shift Quantum Key Distribution*, Phys. Rev. Lett. **89**, 037902 (2002).

[18] L. Zhang, C. Silberhorn, and I. Walmsley, *Secure Quantum Key Distribution Using Continuous Variables of Single Photons*, Phys. Rev. Lett. **100**, 110504 (2008).

[19] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, *Field Test of a Continuous-Variable Quantum Key Distribution Prototype*, New J. Phys. **11**, 045023 (2009).

[20] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, *Experimental Demonstration of Long-Distance Continuous-Variable Quantum Key Distribution*, Nat. Photonics **7**, 378 (2013).

[21] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, *High-Rate Measurement-Device-Independent Quantum Cryptography*, Nat. Photonics **9**, 397 (2015).

[22] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, *Higher-Dimensional Orbital-Angular-Momentum-Based Quantum Key Distribution with Mutually Unbiased Bases*, Phys. Rev. A **88**, 032305 (2013).

[23] A. Sergienko, A. Migdall, and R. Datla, in *Proceedings of the Quantum Electronics and Laser Science Conference* (Optical Society of America, Washington, DC, 1997), p. QME1.

[24] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, *Practical Free-Space Quantum Key Distribution over 1 km*, Phys. Rev. Lett. **81**, 3283 (1998).

[25] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon, and Y. Yamamoto, *Secure Communication: Quantum Cryptography with a Photon Turnstile*, Nature (London) **420**, 762 (2002).

[26] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, *Practical Free-Space Quantum Key Distribution over 10 km in Daylight and at Night*, New J. Phys. **4**, 43 (2002).

[27] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, *Free-Space Quantum Key Distribution by Rotation-Invariant Twisted Photons*, Phys. Rev. Lett. **113**, 060503 (2014).

[28] J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein, *Free-Space Quantum Key Distribution to a Moving Receiver*, Opt. Express **23**, 33437 (2015).

[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 (2016).

[30] 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 (2017).

[31] G. T. Reed, G Mashanovich, F. Y. Gardes, and D. J. Thomson, *Silicon Optical Modulators*, Nat. Photonics **4**, 518 (2010).

[32] J. Michel, J. Liu, and L. C. Kimerling, *High-Performance Ge-on-Si Photodetectors*, Nat. Photonics **4**, 527 (2010).

[33] J. Leuthold, C. Koos, and W. Freude, *Nonlinear Silicon Photonics*, Nat. Photonics **4**, 535 (2010).

[34] A. E.-J. Lim, T.-Y. Liow, J. Song, C. Li, Q. Fang, X. Tu, N. Duan, K. K. Chen, R. P. C. Tern, C. Peng, B. w. Mun, M. N. Islam, J. S. Park, C. Subbu, and P. G.-Q. Lo, in *Proceedings of the Optical Fiber Communication Conference* (Optical Society of America, Washington, DC, 2014), Vol. 21, p. Th2A.51.

[35] H. Cai, C. M. Long, C. T. DeRose, N. Boynton, J. Urayama, R. Camacho, A. Pomerene, A. L. Starbuck, D. C. Trotter, P. S. Davids, and A. L. Lentine, *Silicon Photonic Transceiver Circuit for High-Speed Polarization-Based Discrete Variable Quantum Key Distribution*, Opt. Express **25**, 12282 (2017).

[36] D. Taillaert, H. Chong, P. I. Borel, L. H. Frandsen, R. M. De La Rue, and R. Baets, *A Compact Two-Dimensional Grating Coupler Used as a Polarization Splitter*, IEEE Photonics Technol. Lett. **15**, 1249 (2003).

[37] D. Taillaert, F. Van Laere, M. Ayre, W. Bogaerts, D. Van Thourhout, P. Bienstman, and R. Baets, *Grating Couplers for Coupling between Optical Fibers and Nanophotonic Waveguides*, Jpn. J. Appl. Phys. **45**, 6071 (2006).

[38] G. T. Reed and A. P. Knights, *Silicon Photonics: An Introduction* (John Wiley & Sons Ltd, Chichester, England, 2004).

[39] T. S. Moss, G. J. Burrell, and B. Ellis, *Semiconductor Opto-Electronics* (Butterworth & Co. Publishers Ltd, London, 1973).

[40] R. A. Soref and B. R. Bennett, *Electrooptical Effects in Silicon*, IEEE J. Quantum Electron. **23**, 123 (1987).

[41] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, *Loss-Tolerant Quantum Cryptography with Imperfect Sources*, Phys. Rev. A **90**, 052314 (2014).

[42] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, *Finite-Key Security Analysis of Quantum Key Distribution with Imperfect Light Sources*, New J. Phys. **17**, 093011 (2015).

[43] We chose the 1480-nm operation wavelength (in the middle of the *S* band) because it is outside of the amplifying window of erbium-doped fiber amplifier (EDFA) which can be pumped at 980 nm. The QKD encoder can then be seamlessly integrated into an operational metropolitan fiber link which typically amplifies classical transmission using an EDFA in the *C* band.

[44] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, *Discrete-Phase-Randomized Coherent State Source and Its Application in Quantum Key Distribution*, New J. Phys. **17**, 053014 (2015).

[45] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, *Improved Key-Rate Bounds for Practical Decoy-State Quantum-Key-Distribution Systems*, Phys. Rev. A **95**, 012333 (2017).

[46] K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller, *A Short Wavelength Gigahertz Clocked Fiber-Optic Quantum Key Distribution System*, IEEE J. Quantum Electron. **40**, 900 (2004).

[47] X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. C. Bienfang, D. Su, R. F. Boisvert, C. W. Clark, and C. J. Williams, *Experimental Study of High Speed Polarization-Coding Quantum Key Distribution with Sifted-Key Rates over Mbit/s*, Opt. Express **14**, 2062 (2006).

[48] R. Ding, Y. Liu, Q. Li, Z. Xuan, Y. Ma, Y. Yang, A. E.-J. Lim, G.-Q. Lo, K. Bergman, T. Baehr-Jones, and Michael Hochberg, *A Compact Low-Power 320-Gb/s WDM Transmitter Based on Silicon Microrings*, IEEE Photonics J. **6**, 1 (2014).

[49] Y. Liu, R. Ding, Y. Ma, Y. Yang, Z. Xuan, Q. Li, A. E.-J. Lim, G.-Q. Lo, K. Bergman, T. Baehr-Jones, and M.

Hochberg, *Silicon Mod-MUX-Ring Transmitter with 4 Channels at* 40 Gb/s, Opt. Express **22**, 16431 (2014).

[50] F. Najafi, J. Mower, N. C. Harris, F. Bellei, A. Dane, C. Lee, X. Hu, P. Kharel, F. Marsili, S. Assefa, K. K. Berggren, and D. Englund, *On-Chip Detection of Non-Classical Light by Scalable Integration of Single-Photon Detectors*, Nat. Commun. **6**, 5873 (2015).

[51] H.-K. Lo, M. Curty, and K. Tamaki, *Secure Quantum Key Distribution*, Nat. Photonics **8**, 595 (2014).

[52] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, *"Plug and Play" Systems for Quantum Cryptography*, Appl. Phys. Lett. **70**, 793 (1997).

[53] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, *Quantum Key Distribution over 67 km with a Plug&Play System*, New J. Phys. **4**, 41 (2002).

[54] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, *Device Calibration Impacts Security of Quantum Key Distribution*, Phys. Rev. Lett. **107**, 110501 (2011).

[55] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination*, Nat. Photonics **4**, 686 (2010).

[56] F. Xu, M. Curty, B. Qi, and H.-K. Lo, *Measurement-Device-Independent Quantum Cryptography*, IEEE J. Sel. Top. Quantum Electron. **21**, 6601111 (2015).

[57] H.-K. Lo, M. Curty, and B. Qi, *Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **108**, 130503 (2012).

[58] D. Liang, G. Roelkens, R. Baets, and J. E. Bowers, *Hybrid Integrated Platforms for Silicon Photonics*, Materials **3**, 1782 (2010).

[59] S. Keyvaninia, G. Roelkens, D. Van Thourhout, C. Jany, M. Lamponi, A. Le Liepvre, F. Lelarge, D. Make, G.-H. Duan, D. Bordel, and J.-M. Fedeli, *Demonstration of a Heterogeneously Integrated III-V/SOI Single Wavelength Tunable Laser*, Opt. Express **21**, 3784 (2013).

[60] M. J. R. Heck, J. F. Bauters, M. L. Davenport, J. K. Doylend, S. Jain, G. Kurczveil, S. Srinivasan, Y. Tang, and J. E. Bowers, *Hybrid Silicon Photonic Integrated Circuit Technology*, IEEE J. Sel. Top. Quantum Electron. **19**, 6100117 (2013).

[61] B. B. Bakir, A. Descos, N. Olivier, D. Bordel, P. Grosse, E. Augendre, L. Fulbert, and J. M. Fedeli, *Electrically Driven Hybrid Si/III-V Fabry-Pérot Lasers Based on Adiabatic Mode Transformers*, Opt. Express **19**, 10317 (2011).

[62] A. Biberman, M. J. Shaw, E. Timurdogan, J. B. Wright, and M. R. Watts, *Ultralow-Loss Silicon Ring Resonators*, Opt. Lett. **37**, 4236 (2012).

[63] N. C. Harris, D. Grassani, A. Simbula, M. Pant, M. Galli, T. Baehr-Jones, M. Hochberg, D. Englund, D. Bajoni, and C. Galland, *Integrated Source of Spectrally Filtered Correlated Photons for Large-Scale Quantum Photonic Systems*, Phys. Rev. X **4**, 041047 (2014).

[64] S. F. Preble, M. L. Fanto, J. A. Steidle, C. C. Tison, G. A. Howland, Z. Wang, and P. M. Alsing, *On-Chip Quantum Interference from a Single Silicon Ring-Resonator Source*, Phys. Rev. Applied **4**, 021001 (2015).

[65] Y.-H. Li, Z.-Y. Zhou, L.-T. Feng, W.-T. Fang, S.-l. Liu, S.-K. Liu, K. Wang, X.-F. Ren, D.-S. Ding, L.-X. Xu, and B.-S. Shi, *On-Chip Multiplexed Multiple Entanglement Sources in a Single Silicon Nanowire*, Phys. Rev. Applied **7**, 064005 (2017).

[66] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, *Concise Security Bounds for Practical Decoy-State Quantum Key Distribution*, Phys. Rev. A **89**, 022307 (2014).

[67] A. Ferenczi, V. Narasimhachar, and N. Lütkenhaus, *Security Proof of the Unbalanced Phase-Encoded Bennett-Brassard 1984 Protocol*, Phys. Rev. A **86**, 042327 (2012).