Sibson, P., Kennard, J. E., Stanisic, S., Erven, C., O'Brien, J. L., & Thompson, M. G. (2017). Integrated silicon photonics for high-speed quantum key distribution. Optica, 4(2), 172-177. DOI: 10.1364/OPTICA.4.000172

optica

Integrated silicon photonics for high-speed quantum key distribution

Philip Sibson,[1,3] Jake E. Kennard,[1] Stasja Stanisic,[1,2] Chris Erven,[1] Jeremy L. O'Brien,[1] and Mark G. Thompson[1,*]

[1]Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol BS8 1UB, UK
[2]Quantum Engineering Center for Doctoral Training, School of Physics & Department of Electrical and Electronic Engineering, University of Bristol, BS8 1UB, UK
[3]e-mail: philip.sibson@bristol.ac.uk
*Corresponding author: mark.thompson@bristol.ac.uk

Received 28 July 2016; revised 20 October 2016; accepted 15 November 2016 (Doc. ID 272445); published 24 January 2017

Integrated photonics offers great potential for quantum communication devices in terms of complexity, robustness, and scalability. Silicon photonics in particular is a leading platform for quantum photonic technologies, with further benefits of miniaturization, cost-effective device manufacture, and compatibility with CMOS microelectronics. However, effective techniques for high-speed modulation of quantum states in standard silicon photonic platforms have been limited. Here we overcome this limitation and demonstrate high-speed low-error quantum key distribution modulation with silicon photonic devices combining slow thermo-optic DC biases and fast (10 GHz bandwidth) carrier-depletion modulation. The ability to scale up these integrated circuits and incorporate microelectronics opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secured communications.

OCIS codes: (130.0130) Integrated optics; (060.5565) Quantum communications; (270.5568) Quantum cryptography.
https://doi.org/10.1364/OPTICA.4.000172

1. INTRODUCTION

Quantum technologies are rapidly developing and have the potential to revolutionize the fields of computing and telecommunications. They have major implications for the security of many of our conventional cryptographic techniques, which are known to be insecure against a quantum computer [1]. Fortunately, quantum key distribution (QKD) provides a highly secure approach to sharing random encryption keys by transmitting single photons [2]. Although QKD has advanced from simple proof-of-principle experiments toward robust long-term demonstrations [3–6], it has still not obtained wide-scale adoption.

Integrated photonics provides a stable, compact, and robust platform to implement complex photonic circuits amenable to mass-manufacture, and therefore provides a compelling technology for optical quantum information devices [7]. Silicon photonics, in particular, is a leading platform for quantum photonic technologies with the promise of high density integration, mature fabrication processing, and compatibility with microelectronics [8]. Silicon has been used to demonstrate sources of quantum light, manipulation and transmission of quantum information, and integration with single-photon detectors [9–11]. It has also been used in classical computing and communications for modulation, transceivers [12], and a recent demonstration of optical interconnects alongside electronic microprocessor technology [13].

The appeal of this platform has led to integrated photonic technologies increasingly being deployed in the development of practical QKD systems. Demonstrations include integrated "client" chips for reference-frame-independent QKD [14], planar waveguide components in transmitters and receivers [15], and chip-to-chip QKD using gigahertz clocked indium phosphide transmitters and silicon oxynitride receivers [16].

However, high-speed modulation of quantum states in standard silicon photonic fabrication has been limited. With no natural electro-optic non-linearity, many silicon quantum photonic experiments instead utilize slow thermo-optic phase modulators (TOPMs) for high-fidelity state preparation. Carrier-injection or carrier-depletion modulators (CDMs) offer high-speed operation, but incur phase-dependent loss and saturation [17], which are detrimental in quantum applications where state preparation has stringent requirements.

Here we show an approach to overcome the limitations of saturation and phase-dependent loss of high-speed CDMs in standard silicon photonic fabrication. First we describe a combination

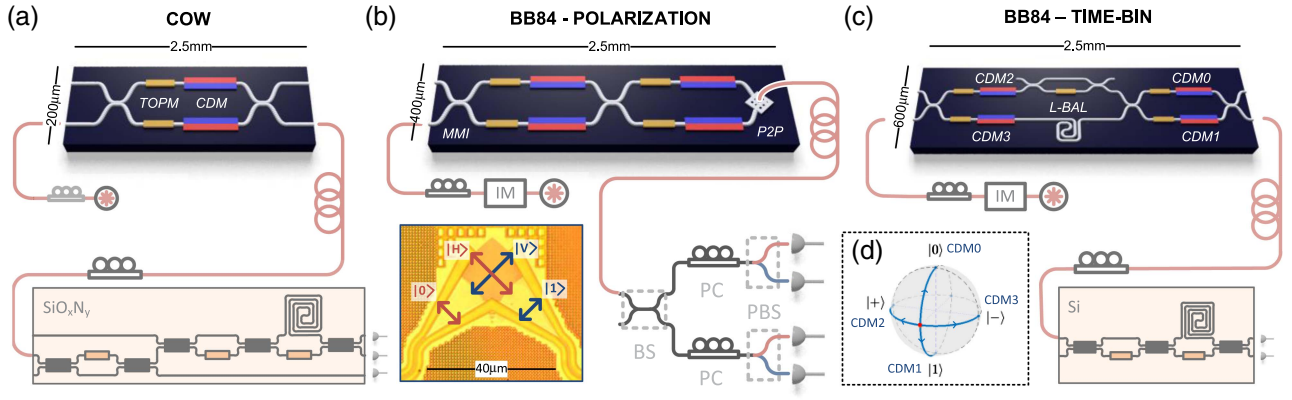

Fig. 1. Integrated silicon photonic devices for QKD: (a) coherent-one-way: a balanced Mach–Zehnder interferometer (MZI) comprising two multimode interference (MMI) devices acting as beam splitters, with phase modulation from thermo-optic phase modulators (TOPMs) and carrier-depletion modulators (CDMs), allows for the encoding of quantum information in path, or pulse modulation. (b) Polarization encoded BB84: combining the two paths of the MZI with a two-dimensional grating coupler allows for the conversion from path encoded information to polarization encoded information (P2P), suitable for communication in free space. (c) Time-bin encoded BB84: an unbalanced asymmetric MZI (AMZI) allows for encoding in time by temporally separating weak coherent pulses into two time intervals using an on-chip delay of 1.5 ns. The extra loss this incurs is balanced by an MZI used as a tunable beam splitter on the opposing arm. The last beam splitter in the AMZI is replaced with another MZI that allows for the selection of time-bin $|0\rangle$ and $|1\rangle$ states. DC offsets are provided by the TOPMs and fast modulation by four CDMs. (d) Illustrated Bloch sphere highlighting the DC offset at $|+\mathrm{i}\rangle$ (red dot), set by the TOPMs. Each CDM is only required to modulate up to $\pi/2$ to permit the encoding of each BB84 state.

of slow, but ideal, TOPMs alongside fast, but non-ideal, CDMs utilized for QKD state preparation at gigahertz speeds. We then use this technique to demonstrate three implementations of high-speed low-error QKD (Fig. 1): chip-to-chip coherent one-way (COW) QKD, polarization encoded BB84, and time-bin encoded BB84 [18] state preparation. We achieve estimated asymptotic secret key rates of up to 916 kbps and quantum bit error rates (QBERs) as low as 1.01% over 20 km of fiber, experimentally demonstrating the feasibility of high-speed QKD integrated circuits based on standard silicon photonic fabrication.

2. SILICON PHOTONIC PHASE MODULATION

Figure 1 shows the three different silicon photonic devices that use a combination of TOPMs and CDMs to prepare and modulate QKD states. As illustrated in Fig. 2(a), the TOPMs allow for almost ideal state preparation with a phase relationship proportional to the square of the voltage (V^2) and no change in transmission (ΔT). The TOPMs were designed in silicon-on-insulator using doped resistive heating in the waveguide slab. This design provides ohmic electrical characteristics (~6.14 kΩ for a 150 μm length) and a 2π voltage of ~24 V.

The TOPMs are limited in bandwidth (~kHz) and therefore inappropriate for the fast modulation required in communications. Silicon also has no natural $\chi^{(2)}$ non-linearity, and therefore the high-speed electro-optic effect cannot be used. An approach to overcome this in standard silicon photonic platforms is to use doped waveguide sections as shown in Fig. 2(b), and employ carrier injection or depletion techniques.

Carrier-depletion modulation induces a phase by reducing the carriers occupying the region that overlaps with the optical mode. This is achieved by reverse biasing a p–n junction formed by doping p and n regions in the core of the silicon waveguide. The depletion of carriers in the waveguide decreases the absorption of the waveguide and induces an optical phase change [19]; however, this effect saturates as the waveguide becomes fully depleted

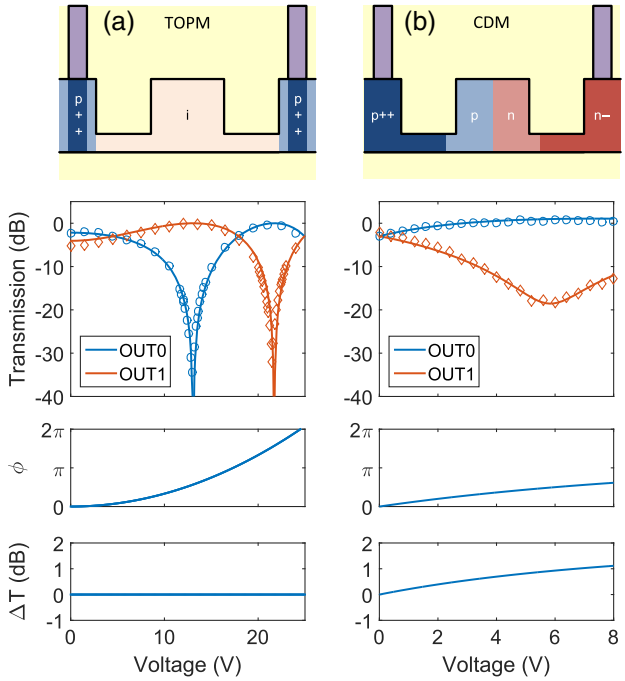

Fig. 2. Thermo-optic and carrier-depletion phase modulation in silicon photonics fabricated with standard doping processes [20]. (a) Cross section of the thermo-optic phase modulation waveguide with $p++$ doping in the waveguide slab and intrinsic (i) silicon waveguide core, followed by the power measured at the two outputs of an MZI, the fitted quadratic phase (ϕ) relationship, and the change in transmission (ΔT) as a function of the applied voltage (V). (b) Cross section of the carrier-depletion phase modulator with p and n doping in the waveguide core, followed by the power measured at the two outputs of an MZI (with an additional TOPM providing a $\pi/2$ offset or initially equal intensity outputs), the fitted phase (ϕ) relationship illustrating saturation, and the change in transmission (ΔT) as a function of the applied voltage (V).

of carriers. Figure 2(b) plots the extracted relationship between voltage, phase, and transmission for a 1.5 mm modulator (~5 dB loss at 0 V), illustrating that the induced phase saturates below π over 8 V while the transmission continues to increase.

The phase-dependent loss characteristics and saturation of the CDMs can severely reduce operational fidelity. This is especially damaging for quantum applications where requirements are often more stringent than many classical applications. Here we describe a combination of thermal and carrier depletion modulators to minimize this effect. By using the TOPMs to bias the circuits in a favorable operating regime, and limiting the modulation depth required for each individual CDM, we mitigate these negative characteristics for both pulse modulation and state preparation.

3. PULSE MODULATION—COW

Utilizing this technique, we demonstrate the pulse modulation of coherent light using a Mach–Zehnder interferometer (MZI) including both TOPMs and CDMs, as illustrated in Fig. 1(a). The TOPMs provide a DC offset to minimize one of the MZI output intensities. Consequently, small changes in one of the CDMs' phases will cause a large change in the intensity of this output arm with a high extinction ratio of ~25 dB without requiring a full π phase change. The −3 dB bandwidth of the CDM changes with the biasing conditions, and was estimated at ~10 GHz and produced ~175 ps full-width-half-maximum (FWHM) pulses. This allows operation of the devices for use in the COW QKD protocol.

COW is a distributed-phase-reference scheme [21] that transmits pulses in pairs, encoding $|0\rangle$ in the first bin and $|1\rangle$ in the second. Here we modulate an external CW laser (1550 nm) to generate pulses in these time-bins and generate a key from the unambiguous time of arrival of the single photons in each time-bin pair. Security of the channel is maintained by measuring the visibility from interfering successive photon pulses, when the pattern of state $|1\rangle$ followed by state $|0\rangle$ occurs, at the receiver [22]. A decoy state, with photon pulses in each time-bin ($|0\rangle$ and $|1\rangle$), is included to increase the probability of occupied successive pulses, allowing a more accurate measurement of the interference, and to detect photon-number-splitting attacks.

We perform chip-to-chip COW QKD using the integrated SiO_xN_y receiver device from Ref. [16] as illustrated in Fig. 1(a). The receiver uses a reconfigurable thermo-optic MZI to route a larger proportion of the input signal directly to a single-photon detector for key generation. The fiber-coupled superconducting nanowire single-photon detectors are biased to ~40% system detection efficiency and dark count rates of ~500 cps per detector. A smaller proportion of the signal is routed to an asymmetric MZI (AMZI) with a 580 ps delay line for the visibility measurement to verify the security of the channel.

4. POLARIZATION ENCODING—BB84

Extending this approach also allows the state preparation of the four BB84 states [18]. Figure 1(b) illustrates slow TOPMs inside and outside an MZI that apply a static phase offset, while we use the non-ideal but fast CDMs in both arms to apply small state-dependent modulations. As shown in Fig. 1(d), we start by preparing the state $|+\mathrm{i}\rangle$ (red dot on the Bloch sphere), using the TOPMs as a DC offset, with near unit fidelity. We then use four non-ideal CDMs (two inside and two outside of the MZI) to prepare any of the four BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ by shifting each of the fast CDMs by $\pi/2$, respectively. This approach limits each CDM to a $\pi/2$ phase shift, thus minimizing the phase-dependent transmission across all four BB84 states and allowing state preparation with non-ideal phase modulators.

The technique can be applied to polarization encoding as illustrated in Fig. 1(b). We couple an intensity modulated (IM) laser to launch 175 ps FWHM optical pulses into a path encoded MZI. Applying static biases to the TOPMs in the MZI prepares the $|+\mathrm{i}\rangle$ state, and using each of the CDMs generates one of the four BB84 states as above. Finally this path encoded state is combined on a 2D grating coupler that acts as a path-to-polarization converter [23].

A fiber-based receiver [shown under the transmitter chip in Fig. 1(b)] was constructed to decode and measure the output polarization states. It consisted of a 50:50 beam splitter (BS) to passively choose the measurement basis, with one arm connected to a polarization beam splitter (PBS) to measure $|0\rangle$ and $|1\rangle$, and one arm coupled to a PBS to measure $|+\rangle$ and $|-\rangle$. Polarization controllers (PCs) were then used to set the measurement bases in each arm. Finally, the outputs were coupled to superconducting nanowire single-photon detectors.

5. TIME-BIN ENCODING—BB84

Polarization encoded systems are commonly used in free-space links owing to the non-birefringent nature of the atmosphere. However, in fiber-based networks the birefringence of the fiber induces a time-dependent polarization rotation on any transmitted qubits, requiring active compensation to maintain reference frame alignment [24]. Instead, encoding qubits in time and phase, so-called time-bin encoding, when transmitting over fiber optics is a much more stable degree of freedom. Here we show that the combined TOPM and CDM approach for state preparation described above can be translated to the equivalent time-bin encoded device.

A schematic of the integrated circuit used to produce time-bin qubits is illustrated in Fig. 1(c). An external laser (1550 nm) is intensity modulated (IM) to generate weak coherent pulses (350 ps FWHM), which are coupled into the silicon chip containing an AMZI with a 1.5 ns delay line to separate photon pulses into one of two time-bins. Here, $|0\rangle$ and $|1\rangle$ are encoded by a photon in the first or second time-bin, respectively, and $|+\rangle$ and $|-\rangle$ are encoded by a photon in a superposition of the first and second time-bin with 0 and π relative phase, respectively. In future designs, the external $LiNbO_3$ IM can be replaced with an on-chip MZI as demonstrated in the COW protocol, as they showed comparable performance with extinction ratios of 25–30 dB. Although the modulation bandwidth and loss performance of the on-chip MZI are inferior to the external $LiNbO_3$ IM (10 GHz rather than 40 GHz bandwidth, and 5 dB loss rather than 4 dB insertion loss), they are still sufficient for QKD and gain the important advantage of monolithic integration in a standard silicon photonic platform.

An MZI is included in the top arm and contains a TOPM to apply a loss balancing correction to ensure each time-bin contains equal photon amplitudes exiting the device. The inside of the AMZI includes TOPMs that can control the DC relative phase between the separate pulses and CDMs to alternate between the $|+\rangle$ and $|-\rangle$ states. The final beam splitter of the AMZI is replaced with a further MZI, with the TOPMs biasing an equal superposition of the two time-bins, and the two CDMs used

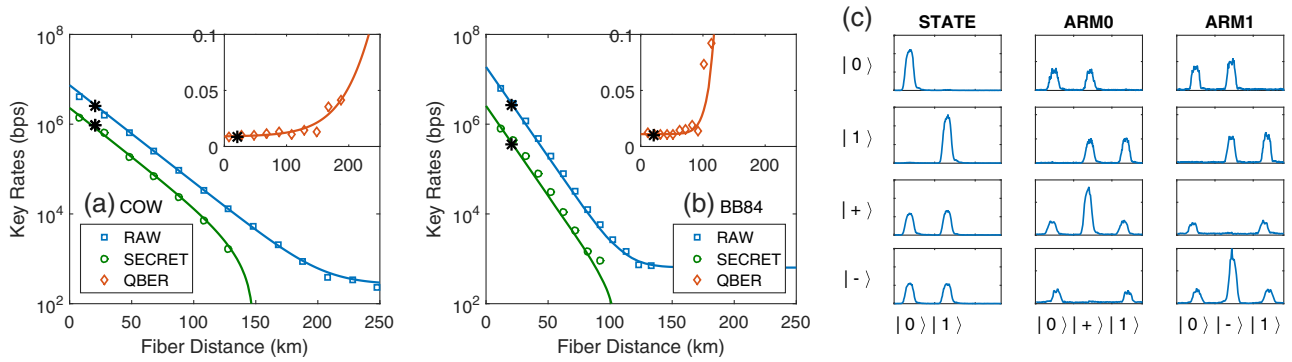

Fig. 3. Estimated secret key rates: the main data sets (squares, circles, and diamonds) were collected by emulating a quantum channel with the use of a variable optical attenuator and assuming standard fiber losses; however, the data shown with asterisks was collected using a 20 km fiber spool as the quantum channel. (a) Raw and secure key rates using the chip to implement the COW QKD protocol, as illustrated in Fig. 1(a). The system operates with a 1.72 GHz clock-rate with a QBER of 1.01% and an estimated secure key rate of 916 kbps over a 20 km fiber. (b) Raw and secure key rates using the chip to produce polarization encoded BB84 states, as illustrated in Fig. 1(b). We measure a low QBER of 1.1% while the transmitter is operated with a 1 GHz clock-rate, which yields an estimated secure key rate of 329 kbps over 20 km. (c) Histogram measurements of the time-bin encoded BB84 state preparation and measurement, as illustrated in Fig. 1(c).

to select the first or second time-bin coupled into a single fiber output.

A second identical chip [pictured at the bottom right of Fig. 1(c)] is used as a receiver circuit with a matched AMZI used to passively select basis measurements before the output is fiber coupled and measured with superconducting nanowire single-photon detectors. The phase decoding AMZI overlaps successive time-bins creating three possible time-slots within which to detect photons. Phase information is interfered in the middle time-slot allowing measurements in the $\{|+\rangle, |-\rangle\}$ basis, whereas time-of-arrival information in the first and third time-slots allows measurement in the $\{|0\rangle, |1\rangle\}$ basis.

6. RESULTS

Figure 3 illustrates the results from our three implementations of high-speed low-error QKD with integrated silicon photonics. Figure 3(a) shows the raw and secret key rates, and the QBER from the system performing the COW QKD protocol. Here, pulse modulation provides 175 ps FWHM pulses with a high ~25 dB extinction ratio between bright and empty pulses. The system operates with a 1.72 GHz clock-rate (or 0.86 GHz system-rate, as one state is sent every two clock cycles) with a QBER of 1.01% and an estimated asymptotic secure key rate of 916 kbps over a 20 km fiber, following the upper-bound security proof against collective attacks of Branciard *et al.* [22].

For the polarization and time-bin BB84 QKD protocols, we model and fit the data from our TOPMs and CDMs in Figs. 2(a) and 2(b), resulting in an expected state preparation fidelity of 99.5%, which yields an expected QBER of ≤1.1%. This is equivalent to a 19.5 dB extinction ratio between measuring the state $|\psi\rangle_i$ and its orthogonal counterpart $|\overline{\psi}\rangle_i$ (e.g., measuring $|1\rangle$ when preparing $|0\rangle$ or measuring $|-\rangle$ when preparing $|+\rangle$).

Figure 3(b) shows the measured raw and secret key rates as well as the QBER from operating the transmitter for polarization encoding and using the passive fiber-based receiver detection scheme described. We measure a low QBER of 1.1% while the transmitter is operated with a 1 GHz clock-rate, which yields an estimated asymptotic secure key rate of 329 kbps over a 20 km fiber using a non-phase randomized weak coherent BB84 security proof without decoy states against general attacks [25]. The rate and maximum secure distance could be increased drastically with the addition of an extra integrated intensity modulator to produce decoy states [26].

Finally, measurements of the time-bin encoded states, using a second identical chip as the receiver circuit as described above, are shown in Fig. 3(c). Analyzing these measurements, we observe a low QBER of ~2.1% for this proof-of-principle demonstration of time-bin encoded BB84 state preparation. Future systems will benefit from a dedicated low-loss silicon receiver circuit by minimizing the fiber-to-chip coupling loss (currently ~ – 4.5 dB) and reducing the loss incurred in the on-chip delay; e.g., reducing the 1.5 ns delay used here to the 600 ps used in COW would increase transmission by >3 dB. As we implement a passive basis selection scheme there is not a need for fast modulation on the receiver, and removing the *p*–*n* CDMs would further decrease absorption by ~5 dB per modulator.

7. DISCUSSION

In conclusion, this work experimentally demonstrates the feasibility of high-speed QKD transmitters in CMOS-based silicon photonic integrated circuits. In particular, we show an approach to overcome the problems of high-fidelity state preparation when using non-ideal fast modulation in standard silicon photonic fabrication. Using a combination of slow, but ideal, TOPMs alongside high-bandwidth (~10 GHz), but non-ideal, CDMs, we demonstrate QKD state preparation and pulse modulation. We show three successful implementations: time-bin encoded BB84 state preparation and measurement, polarization encoded BB84 (1 GHz clock-rate, 1.1% QBER, 329 kbps estimated asymptotic secret key rate), and pulse modulation for COW QKD (1.72 GHz clock-rate, 1.01% QBER, 916 kbps estimated asymptotic secure key rate) over a 20 km fiber link.

The modulation bandwidth and estimated secret key rates generated in this demonstration are comparable to previous integrated photonic QKD demonstrations [16], but with less functionality combined on a single device and currently relying on

off-chip laser sources. Future generations of silicon-based chips will benefit from the recent developments of low-loss couplers [27], low-loss delay lines [28], integrated laser sources [29], and integrated single-photon detectors [30], allowing high-performing monolithically integrated transmitter and receiver devices. Performance could be further improved by the functionality demonstrated, such as integrated pulse modulation, intensity modulators for decoy state [26], and attenuation calibration, and by increasing the rates beyond the 10 GHz bandwidth demonstrated here [17]. The ease of fabrication and availability of silicon photonics (in comparison with other integrated photonic platforms such as InP and SiO_xN_y) will also open routes to mass-manufacture using standard CMOS fabrication tools and foundries.

Future demonstrations will require focus on the complete system for autonomous QKD operation deployed in telecommunication networks. This includes the development of real-time basis and bit selection using quantum random numbers, active basis alignment, appropriate error reconciliation, privacy amplification, and finite-key analysis to qualify the security.

Ultimately, integrated silicon photonics will allow the manufacture of quantum communication chips with electronic and photonic processing on a single monolithic device, and the reduced footprint will enable further multiplexing, complexity, and operation with single-photon detection. The ability to scale up these integrated circuits and incorporate microelectronics opens the way to new and advanced integrated quantum communication technologies and larger adoption of quantum-secured communications.

During the preparation of this manuscript, the authors became aware of a complementary demonstration by Ma *et al.* [31] in silicon using carrier-injection *p–i–n* diode phase-shifters to encode BB84 states in polarization and micro-ring resonators for pulse modulation.

Funding. Engineering and Physical Sciences Research Council (EPSRC); European Research Council (ERC); Seventh Framework Programme (FP7) (323734 BBOI); UK Quantum Communications Hub.

Acknowledgment. J.L.O'B. acknowledges a Royal Society Wolfson Merit Award and a Royal Academy of Engineering Chair in Emerging Technologies. M.G.T acknowledges fellowship support from the Engineering and Physical Sciences Research Council (EPSRC, UK). The authors thank IMEC for the fabrication of the integrated photonic silicon devices and LioniX for the fabrication of the silicon oxynitride receiver.

See Supplement 1 for supporting content.

REFERENCES

1. H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**, 595–604 (2014).
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**, 1301–1350 (2009).
3. 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**, 31395–31401 (2013).
4. B. Korzh, N. Walenta, R. Houlmann, and H. Zbinden, "A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator," Opt. Express **21**, 19579–19592 (2013).
5. 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**, 7583–7592 (2015).
6. M. Sasaki, M. Fujiwara, R.-B. Jin, M. Takeoka, H. Endo, K.-I. Yoshino, T. Ochi, S. Asami, and A. Tajima, "Quantum photonic network: concept, basic tools, and future issues," IEEE J. Sel. Top. Quantum Electron. **21**, 49–61 (2015).
7. M. G. Thompson, A. Politi, J. C. Matthews, and J. L. O'Brien, "Integrated waveguide circuits for optical quantum computing," IET Circuits Dev. Syst. **5**, 94–102 (2011).
8. A. E.-J. Lim, J. Song, Q. Fang, C. Li, X. Tu, N. Duan, K. K. Chen, R. P.-C. Tern, and T.-Y. Liow, "Review of silicon photonics foundry efforts," IEEE J. Sel. Top. Quantum Electron. **20**, 405–416 (2014).
9. J. W. Silverstone, D. Bonneau, J. L. O'Brien, and M. G. Thompson, "Silicon quantum photonics," IEEE J. Sel. Top. Quantum Electron. **22**, 1–13 (2016).
10. W. H. P. Pernice, C. Schuck, O. Minaeva, M. Li, G. N. Goltsman, A. V. Sergienko, and H. X. Tang, "High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits," Nat. Commun. **3**, 1325 (2012).
11. 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).
12. C. Doerr, "Silicon photonic integration in telecommunications," Front. Phys. **3**, 37 (2015).
13. C. Sun, M. T. Wade, Y. Lee, J. S. Orcutt, L. Alloatti, M. S. Georgas, A. S. Waterman, J. M. Shainline, R. R. Avizienis, S. Lin, B. R. Moss, R. Kumar, F. Pavanello, A. H. Atabaki, H. M. Cook, A. J. Ou, J. C. Leu, Y.-H. Chen, K. Asanović, R. J. Ram, M. A. Popović, and V. M. Stojanović, "Single-chip microprocessor that communicates directly using light," Nature **528**, 534–538 (2015).
14. P. Zhang, K. Aungskunsiri, E. Martn-López, J. Wabnig, M. Lobino, R. W. Nock, J. Munns, D. Bonneau, P. Jiang, H. W. Li, A. Laing, J. G. Rarity, A. O. Niskanen, M. G. Thompson, and J. L. O'Brien, "Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client," Phys. Rev. Lett. **112**, 130501 (2014).
15. A. Tanaka, M. Fujiwara, K.-I. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, "High-speed quantum key distribution system for 1-Mbps real-time key generation," IEEE J. Quantum Electron. **48**, 542–550 (2012).
16. 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," arXiv:1509.00768 (2015).
17. G. T. Reed, G. Mashanovich, F. Gardes, and D. Thomson, "Silicon optical modulators," Nat. Photonics **4**, 518–526 (2010).
18. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *IEEE International Conference on Computers, Systems, and Signal Processing* (1984), p. 175–179.
19. Z. Fang and C. Z. Zhao, "Recent progress in silicon photonics: a review," ISRN Opt. **2012**, 428690 (2012).
20. P. P. Absil, P. De Heyn, H. Chen, P. Verheyen, G. Lepage, M. Pantouvaki, J. De Coster, A. Khanna, Y. Drissi, D. Van Thourhout, and J. Van Campenhout, "Imec iSiPP25G silicon photonics: a robust CMOS-based photonics technology platform," Proc. SPIE **9367**, 93670V (2015).
21. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," Appl. Phys. Lett. **87**, 194108 (2005).
22. C. Branciard, N. Gisin, and V. Scarani, "Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography," New J. Phys. **10**, 013031 (2008).
23. J. Wang, D. Bonneau, M. Villa, J. W. Silverstone, R. Santagati, 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-to-chip quantum photonic interconnect by path-polarization interconversion," Optica **3**, 407–413 (2016).

24. G. Xavier, N. Walenta, G. V. De Faria, G. Temporão, N. Gisin, H. Zbinden, and J. Von der Weid, "Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation," New J. Phys. **11**, 045015 (2009).
25. H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with non-random phases," Quantum Inf. Comput. **7**, 431–458 (2007).
26. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005).
27. J. Cardenas, C. B. Poitras, K. Luke, L.-W. Luo, P. A. Morton, and M. Lipson, "High coupling efficiency etched facet tapers in silicon waveguides," IEEE Photon. Technol. Lett. **26**, 2380–2382 (2014).
28. J. Cardenas, C. B. Poitras, J. T. Robinson, K. Preston, L. Chen, and M. Lipson, "Low loss etchless silicon photonic waveguides," Opt. Express **17**, 4752–4757 (2009).
29. D. Liang and J. E. Bowers, "Recent progress in lasers on silicon," Nat. Photonics **4**, 511–517 (2010).
30. F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency," Nat. Photonics **7**, 210–214 (2013).
31. C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, H.-K. Lo, and J. K. S. Poon, "Integrated silicon photonic transmitter for polarization-encoded quantum key distribution," arXiv:1606.04407 (2016).