Integrated Silicon Photonics for High-Speed Quantum Key Distribution

P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O’Brien, and M. G. Thompson
1 Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK
2 Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, BS8 1UB, UK

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 miniaturisation, 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.

Quantum technologies are rapidly developing and have the potential to revolutionise 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 towards 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 GHz 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 utilise 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 of slow, but ideal, TOPMs alongside fast, but non-ideal, CDMs utilised for QKD state preparation at GHz speeds. We then use this technique to demonstrate three implementations of high-speed low-error QKD (Figure 1): chip-to-chip Coherent One Way (COW) QKD, polarisation 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 (QBER) as low as 1.01% over 20 km of fibre, experimentally demonstrating the feasibility of high-speed QKD integrated circuits based on standard silicon photonic fabrication.

Figure 1 shows the three different silicon photonic devices which use a combination of TOPMs and CDMs to prepare and modulate QKD states. As illustrated in Figure 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 ($\Delta T$). The TOPMs were designed in silicon-on-insulator using doped resistive heating in the waveguide slab. This design provides ohmic electrical characteristics ($\sim 6.14 \, k\Omega$ for a 150 $\mu$m length) and a $2\pi$ voltage of $\sim 24 \, V$.

The TOPMs are limited in bandwidth ($\sim$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 Figure 2 (b), and employ carrier injection or depletion techniques.

Carrier depletion modulation induces a phase by reducing the carriers occupying the region which 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 of carriers. Figure 2 (b) plots the extracted relationship between voltage, phase, and transmission for a 1.5 mm modulator ($\sim$5 dB loss at 0 V), illustrating that the induced phase saturates below $\pi$ 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 minimise this effect. By using the TOPMs to bias the circuits in a favourable operating regime, and limiting the modulation depth required for each individual CDM, we mitigate these negative characteristics for both pulse modulation and state preparation.

Utilising this technique, we demonstrate the pulse modulation of coherent light using a Mach-Zehnder interferometer (MZI) including both TOPMs and CDMs, as illustrated in Figure 1 (a). The TOPMs provide a DC offset to minimise one of the MZI output intensities. Consequently, small changes in one of the CDMs’ phases will cause a large change in intensity of this output arm with a high extinction ratio of $\sim$25 dB without requiring a full $\pi$ phase change. The $\sim$3 dB bandwidth of the CDM changes with the biasing conditions, and was estimated at $\sim$10 GHz and produced $\sim$175 ps full-width-half-maximum (FWHM) pulses. This allows operation of the devices for use in the Coherent-One-Way (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$_2$N$_y$ receiver device from Ref. [16] as illustrated in Figure 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 fibre-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 to security of the channel.

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 Figure 1 (d), we start by preparing the state $|+i\rangle$ (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 minimising the phase dependent transmission across all four BB84 states and allowing state preparation with non-ideal phase modulators.

The technique can be applied to polarisation encoding as illustrated in Figure 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 $|+i\rangle$ 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-polarisation converter [23].

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

Polarisation encoded systems are commonly used in free-space links owing to the non-birefringent nature of the atmosphere. However, in fibre-based networks the birefringence of the fibre induces a time-dependent polarisation 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 fibre optics is a much more stable degree of freedom. Here we show 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 Figure 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 $|1\rangle$ is encoded by a photon
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 fibre losses; however, the data shown with asterisks was collected using a 20 km fibre spool as the quantum channel. (a) Raw and secure key rates using the chip to implement the COW QKD protocol, as illustrated in Figure 1 (a). The system operates with a 1.72 GHz clock-rate with a QBER of 1.01% and estimated secure key rate of 916 kbps over a 20 km fibre. (b) Raw and secure key rates using the chip to produce polarisation encoded BB84 states, as illustrated in Figure 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 a 20 km fibre. (c) Histogram measurements of the time-bin encoded BB84 state preparation and measurement, as illustrated in Figure 1 (c).

in the first or second time-bin, respectively, and $|+\rangle$ and $|−\rangle$ encoded by a photon in a superposition of the first and second time-bin with 0 and $\pi$ 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 is 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 every time-bin contains equal photon amplitudes exiting the device. The inside of the AMZI includes TOPMs which 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 to select the first or second time-bin coupled into a single fibre output.

A second identical chip [pictured at the bottom right of Figure 1 (c)] is used as a receiver circuit with a matched AMZI used to passively select basis measurements before the output is fibre 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.

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 $\sim25$ 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 estimated asymptotic secure key rate of 916 kbps over a 20 km fibre, following the upper-bound security proof against collective attacks of Branciard et al. [22].

For the polarisation and time-bin BB84 QKD protocols, we model and fit the data from our TOPMs and CDMs in Figure 2 (a) and (b), resulting in an expected state preparation fidelity of 99.5%, which yields an expected QBER of $\leq1.1\%$. This is equivalent to a 19.5 dB extinction ratio between measuring the state $|ψ_i\rangle$ and its orthogonal counterpart $|ψ^*_i\rangle$ (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 polarisation encoding and using the passive fibre-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 fibre using a non-phase randomised weak coherent BB84 secu-
rity 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 Figure 3 (c). Analysing these measurements, we observe a low QBER of \( \sim 2.1\% \) 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 minimising the fibre-to-chip coupling loss (currently \( \sim 4.5\, \text{dB} \)) 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 \( > 3\, \text{dB} \). As we implement a passive basis selection scheme there is not a need for fast modulation on the receiver, and removing the \( p-n \) carrier depletion modulators would further decrease absorption by \( \sim 5\, \text{dB} \) per modulator.

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 (\( \sim 10\, \text{GHz} \)), 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, polarisation 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 fibre 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 combining 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 \( \text{SiO}_2\text{N}_x \)) 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 the use of 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 polarisation and micro-ring resonators for pulse modulation.

Acknowledgments

The authors thank IMEC for the fabrication of the integrated photonic silicon devices and LioniX for the fabrication of the silicon oxynitride receiver.

This work was supported by the Engineering and Physical Sciences Research Council (EPSRC), The European Research Council (ERC), FP7 Action: Beyond the Barriers of Optical Integration (BBOI), and the UK Quantum Communications Hub. J.L.O’B. acknowledges a Royal SocietyWolfson 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).
[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. Fujiiwara, M. Sasaki, and A. J. Shields, “High speed prototype quantum key distribution system and long term field trial,” Opt. Exp., vol. 23, no. 6, pp. 7583–7592, 2015.

[6] M. Sasaki, M. Fujiiwara, 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 Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 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, devices & systems, vol. 5, no. 2, pp. 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,” Selected Topics in Quantum Electronics, IEEE Journal of, vol. 20, no. 4, pp. 405–416, 2014.

[9] J. W. Silverstone, D. Bonneau, J. L. O’Brien, and M. G. Thompson, “Silicon Quantum Photonics,” IEEE Journal of Selected Topics in Quantum Electronics, vol. 22, no. 6, pp. 1–13, 2016.

[10] W. H. P. Pernice, C. Schuck, O. Minacena, M. Li, G. N. Golsman, A. V. Sergienko, and H. X. Tang, “High-speed and high-efficiency traveling wave single-photon detectors embedded in nanophotonic circuits.” Nature communications, vol. 3, p. 1325, jan 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.” Nature communications, vol. 6, 2015.

[12] C. R. Doerr, “Silicon photonic integration in telecommunications,” Frontiers in Physics, vol. 3, p. 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. Asanovi, R. J. Ram, M. A. Popovi, and V. M. Stojanovi, “Single-chip microprocessor that communicates directly using light,” Nature, vol. 528, no. 7583, pp. 534–538, 2015.

[14] P. Zhang, K. Aungskunsiri, E. Martín-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., vol. 112, no. 13, p. 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,” Quantum Electronics, IEEE Journal of, vol. 48, no. 4, pp. 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 preprint arXiv:1509.00768, September 2015.

[17] G. T. Reed, G. Mashanovich, F. Gardes, and D. Thompson, “Silicon optical modulators,” Nature photonics, vol. 4, no. 8, pp. 518–526, 2010.

[18] C. H. Bennett, “Quantum cryptography: Public key distribution and coin tossing,” in Proceedings of IEEE International Conference on Computer Systems and Signal Processing, pp. 175–179, 1984.

[19] Z. Fang and C. Z. Zhao, “Recent progress in silicon photonics: a review,” ISRN Optics, vol. 2012, 2012.

[20] P. P. Absil, P. De Heyn, H. Chen, P. Verheyen, G. Lepage, M. Pantouvakis, 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,” in Proc. SPIE 9367, p. 93670V, International Society for Optics and Photonics, 2015.

[21] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, “Fast and simple one-way quantum key distribution,” Appl. Phys. Lett., vol. 87, no. 19, p. 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., vol. 10, no. 1, p. 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, vol. 3, no. 4, pp. 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 Journal of Physics, vol. 11, no. 4, p. 045015, 2009.

[25] H.-K. Lo and J. Preskill, “Security of Quantum Key Distribution using Weak Coherent States with Non-Random Phases,” Quantum Information and Computation, vol. 7, no. 5&6, pp. 431–458, 2007.

[26] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” Phys. Rev. A, vol. 72, p. 012326, July 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 Photonics Technol. Lett., vol. 26, no. 23, pp. 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,” Optics express, vol. 17, no. 6, pp. 4752–4757, 2009.

[29] D. Liang and J. E. Bowers, “Recent progress in lasers on silicon,” Nature Photonics, vol. 4, no. 8, pp. 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,” Nature Photonics, vol. 7, no. 3, pp. 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 preprint arXiv:1606.04407, June 2016.