nature photonics

LETTERS

https://doi.org/10.1038/s41566-019-0504-5

An integrated silicon photonic chip platform for continuous-variable quantum key distribution

G. Zhang[1,2], J. Y. Haw[3], H. Cai[2], F. Xu[4*], S. M. Assad[3], J. F. Fitzsimons[5], X. Zhou[6], Y. Zhang[7], S. Yu[7], J. Wu[7], W. Ser[1], L. C. Kwek[8*] and A. Q. Liu[1*]

Quantum key distribution (QKD) is a quantum communication technology that promises unconditional communication security. High-performance and cost-effective QKD systems are essential for the establishment of quantum communication networks[1-3]. By integrating all the optical components (except the laser source) on a silicon photonic chip, we have realized a stable, miniaturized and low-cost system for continuous-variable QKD (CV-QKD) that is compatible with the existing fibre optical communication infrastructure[4]. Here, the integrated silicon photonic chip is demonstrated for CV-QKD. It implements the widely studied Gaussian-modulated coherent state protocol that encodes continuous distributed information on the quadrature of laser light[5,6]. Our proof-of-principle chip-based CV-QKD system is capable of producing a secret key rate of 0.14 kbps (under collective attack) over a simulated distance of 100 km in fibre, offering new possibilities for low-cost, scalable and portable quantum networks.

QKD has been successfully demonstrated in various platforms such as fibre optical communication, free-space communication and satellites[1]. Silicon photonic technology enables on-chip QKD with many advantages[3]. Over the past few years, different substrates have been explored for chip-level integration of QKD[3]. Indium phosphide (InP)[7], lithium niobate ($LiNbO_3$)[8] and potassium titanyl phosphate (KTP)[9] have been used to fabricate on-chip lasers and fast modulators. Silica offers low-loss delay lines and fibre-chip couplers, but lacks rapid modulation[10,11]. Silicon relies on well-established microfabrication techniques and is ideally suited for both on-chip photonic components[12–14].

There are two main categories of QKD systems, namely discrete-variable QKD (DV-QKD) and CV-QKD. Fibre-based DV-QKD has been demonstrated in up to around 400-km ultra-low-loss fibre[15,16]. The key rate is around the kbps level at 100 km distance, as reported in ref. [16]. Several DV-QKD protocols, including encoding on photon polarization[17], spatial dimensions[18] and time bins[19], have been demonstrated on silicon wafers. To detect photons on-chip, superconducting nanowire-based single-photon detectors with detection efficiencies up to 90% are integrated on-chip[20,21]. Compared with DV-QKD, CV-QKD is more suitable for photonic chip integration due to its compatibility with existing telecom technologies[22,23]. A fibre-based CV-QKD system showed a secure key rate of about 1 kbps at 80 km transmission distance in 2013[24], and the distance was further pushed to over 100 km by controlling the excess noise[25]. Very recently, several on-chip quantum entropy sources based on the detection of phase fluctuations[26–28] and vacuum fluctuations[29] were reported. The chip-based homodyne detector showed a gain of 4.5 kV A^{-1} with 150-MHz bandwidth[29].

Here we report a Gaussian-modulated coherent state CV-QKD protocol on an integrated silicon photonic chip. The on-chip integration (Supplementary Fig. 1) increases the stability and scalability of all the optical components, reduces the cost, and extends the applicability of photonic chips to CV-QKD and potentially to other quantum communication protocols.

Figure 1 shows a schematic of the silicon photonic CV-QKD chip. In the transmitter chip (Alice), a 1,550-nm continuous-wave laser is coupled into the waveguide with a grating coupler. The first modulator serves as an attenuator to control the input laser intensity. A 1:99 directional coupler splits the input laser into two paths, with the weaker one as signal and the stronger one as the local oscillator (LO). The signal path is modulated with an amplitude modulator (AM) and a phase modulator (PM) to generate a series of coherent state $|x_A + ip_A\rangle$, where x_A and p_A are random numbers with a Gaussian distribution. The information is encoded by modulating the continuous light signal on the sideband ranging from 1–10 MHz (refs. [30,31]). A digital filter and demodulator extract the information from one of the sideband frequencies. To keep the relative phase between the signal path and the LO path after transmission, the modulated signal and LO are multiplexed into two orthogonal polarization states with a two-dimensional grating coupler. After the signal is transmitted over a line with a transmittance T, the receiver (Bob) first compensates the polarization drift with a polarization controller followed by demultiplexing of the signal and the LO with another two-dimensional grating coupler. Unlike previous protocols that require an ultra-high (60–80 dB) intensity difference between the signal and the LO[24], our design only requires a 35-dB extinction ratio because the information is encoded on the sideband frequency that is the a.c. component of the signal light. Finally, Bob arbitrarily measures quadrature x or p with the homodyne detector and filters out the required frequency. The security of CV-QKD is guaranteed by the Heisenberg uncertainty principle between the x and p quadratures. Because the two quadratures do not commute, the eavesdropper's (Eve) attempt to measure one quadrature would result in noise in the other, which implies that the amount of

[1]School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, Singapore. [2]Institute of Microelectronics, A*STAR, Singapore, Singapore. [3]Centre for Quantum Computation and Communication Technology, The Australian National University, Canberra, Australian Capital Territory, Australia. [4]Shanghai Branch, National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Shanghai, China. [5]Singapore University of Technology and Design, Singapore, Singapore. [6]State Key Laboratory of Optoelectronic Materials and Technologies, Sun Yat-sen University, Guangzhou, China. [7]State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing, China. [8]Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore.
*e-mail: feihuxu@ustc.edu.cn; cqtklc@nus.edu.sg; eaqliu@ntu.edu.sg

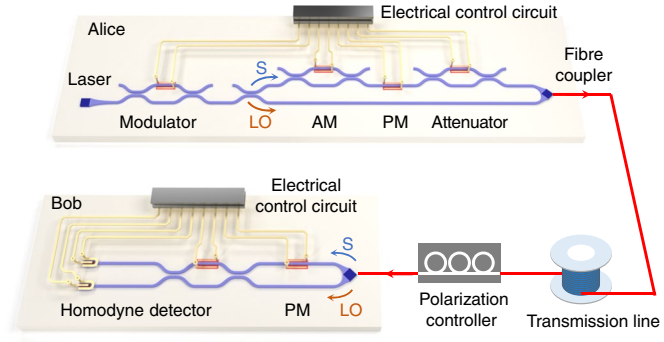

Fig. 1 | Schematic of the CV-QKD system. The system built on silicon photonic chips contains two parties, Alice and Bob, which are used as the transmitter and receiver. Alice's side consists of several AMs, PMs, attenuators and grating couplers, which can modulate the signal (S) and multiplex the signal with the LO in two orthogonal polarization states. Bob demultiplexes and detects the signal with the receiver chip.

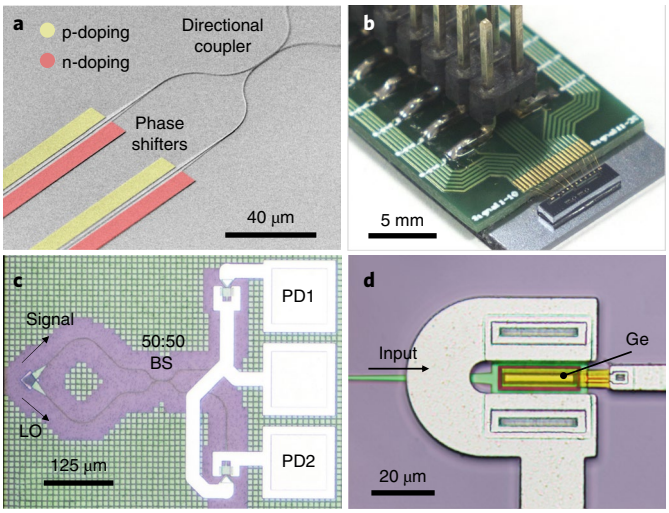

Fig. 2 | Scanning electron microscopy and optical microscopy images of the QKD chip. a, Scanning electron microscopy image of part of the AM structure, including the p–i–n phase shifter and directional couplers. **b**, QKD chip packaged with a PCB board. **c**, Optical microscopy image of the on-chip homodyne detector, which is also the receiver chip. The signal from two PDs is subtracted and amplified. **d**, Enlarged optical microscopy image of the on-chip germanium PD.

information leaked to Eve is bound by the noise level detected by Alice and Bob.

Figure 2a illustrates the Mach–Zehnder interferometer structure designed as the AM. The photo of the transmitter chip packaged with a printed circuit board (PCB) is shown in Fig. 2b. Figure 3a demonstrates that the AM and PM have a 90% switching time of 2.5 ns, which corresponds to a 200-MHz modulation frequency. Limited by the detector bandwidth, the system is designed to operate between 1–10 MHz, right within the range of both the modulators. The cross-modulation of the AM and the PM was also measured to confirm that the two modulators did not affect each other (Supplementary Fig. 2).

The displaced coherent state is measured by the balanced homodyne detector, integrated on the receiver chip. The homodyne detector consists of a 50:50 beam splitter (BS) and two photodiodes (PD) as shown in Fig. 2c,d. The signals from the two PDs

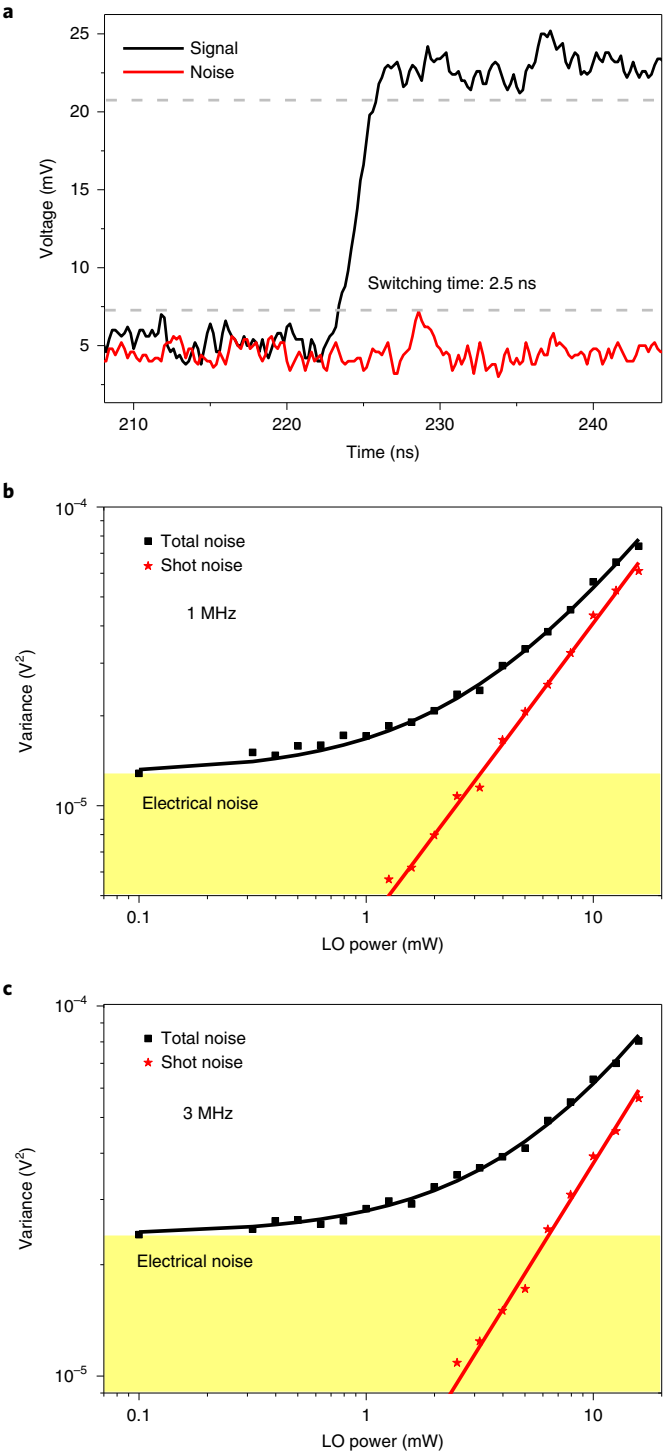

Fig. 3 | Chip performance analysis. a, Switching speed of the modulator, where the grey lines indicate 10% and 90% of the peak-to-peak value. **b**,**c**, Total noise variance and fitted shot noise for the homodyne detector with different input LO power levels at the 1 MHz (**b**) and 3 MHz (**c**) bands. The red and black lines are the theoretical fitting curves for the data points.

are subtracted and amplified using a two-stage transimpedance amplifier operating at 1–10 MHz, which defines the bandwidth of the homodyne detector. The transimpedance gain is 10^5 V A^{-1}. The common mode rejection ratio is 25 dB (Supplementary Fig. 3). A homodyne detector must be able to distinguish the shot noise of the LO light from the electronic background noise, because CV-QKD

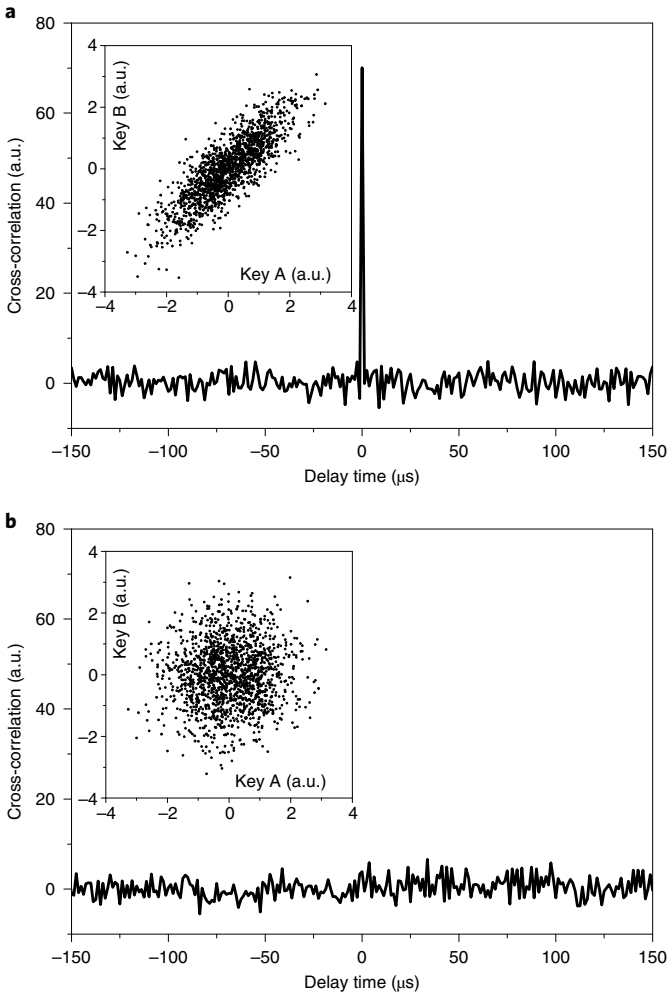

Fig. 4 | Key distribution test. a,**b**, Cross-correlation results of Bob's measurement result and Alice's modulation on corresponding quadratures (**a**) and different quadratures (**b**). The insets show the correlated Gaussian keys in the two different situations.

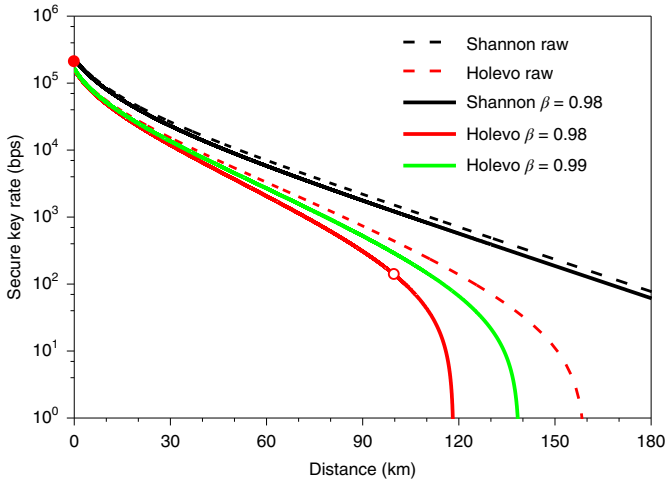

Fig. 5 | Secure key rate analysis. The secure key rate under individual attack (black line) and collective attack (red line). Considering a practical case, the reconciliation efficiencies of 0.98 and 0.99 are used to calculate the effective key rate after the reconciliation process. The red filled dot near 0 km represents the experimental key rate with a 2-m fibre link, while the open circle at 100 km represents the simulated key rate with a high-efficiency reconciliation protocol.

uses the constant shot noise as a reference to normalize the signals and to detect potential eavesdroppers. The total noise of the homodyne detector is measured as a function of LO power at 1 MHz and 3 MHz bands as shown in Fig. 3b,c, respectively. The fitted shot noise has a linear relationship with the LO power. When the LO power is higher than 10 mW, the shot noise is at least 5 dB higher than the electronic background noise. This difference is referred to as shot noise clearance. The homodyne detection efficiency is calculated as $\eta = \eta_{PD}\eta_{vis}^2 = 0.498$, where η_{PD} is the quantum efficiency of the PD and η_{vis} is the visibility.

The QKD transmitter chip is calibrated using an off-chip detector with a fibre polarization controller, which has a 2-m fibre link in between. The quadrature selection is achieved by maximizing the cross-modulation peak-to-peak difference. Both the output signal and the input signal for x and p quadrature modulation are recorded, and the data are collected for 4 ms with a sampling frequency of 25 MHz. The output signal on Bob's side is synchronized with Alice's modulation signal by measuring their cross-correlation. Figure 4a shows the normalized cross-correlation measurement between the homodyne detector output and the corresponding modulation signal. Figure 4b shows the cross-correlation between the homodyne detector output and the other modulation signal. The differences between the two cross-correlations are more than 10-fold. The small correlation with the different quadrature is due to the phase noise between the signal and the LO, which is one of the main contributions to the excess noise. All signals are synchronized based on the cross-correlation and passed through a digital bandpass filter between 2.8 and 3.2 MHz (see Supplementary Fig. 4 for full noise spectra). Next, the filtered signals are demodulated and down-sampled to 0.8 Mbps to generate a set of correlated Gaussian keys that are shown in the insets of Fig. 4a,b with Alice's key as the x coordinate and Bob's key as the y coordinate. These plots confirm that Bob's key only correlates to one of Alice's keys with the same measured quadrature. Information reconciliation is then applied to the correlated Gaussian key (see Methods).

The secure key rate at a longer distance is calculated based on the assumption of individual attack and collective attack under the trusted device scenario, which means an eavesdropper cannot access the noise from Bob's apparatus[22]. The total losses consist of the losses on the transmission line and Bob's equipment while the losses on Alice's side do not affect the final security key. The homodyne detection efficiency is $\eta = 0.498$. The 5-dB loss of Bob's chip is considered as an additional 68.3% drop in efficiency. The total excess noise is $\varepsilon = 0.0934$ shot-noise units (SNU) at a modulation variance of $V_{mod} = 7.07$ SNU and $T = 1$. Detector electrical noise is $v_{el} = 0.0691$ SNU. Symbol rate is SR = 0.8 Mbps. With these data, the secure key rate of the current CV-QKD system is estimated. The Shannon raw key rate and Holevo raw key rate are given as the dashed lines in Fig. 5. Considering a more practical situation, the reconciliation efficiencies $\beta = 0.98$ and 0.99 are chosen[32,33], which represent the case that we have achieved and the state-of-the-art case, respectively. The corresponding Shannon effective key rate and Holevo effective key rate are shown as the solid lines in Fig. 5 (see Supplementary Figs. 5 and 6 for a detailed analysis).

We performed an experiment to demonstrate CV-QKD over a 2-m fibre link. To generate secret keys, the slice reconciliation and low-density parity check (LDPC) error correction are performed on the measured data. The resulting secret key rate is 0.25 Mbps, which is shown as the filled dot in Fig. 5. Furthermore, to prove the capability for long-distance CV-QKD, we simulated the total noise

χ_{tot} and obtained that the SNR = 0.028 (see Methods, where SNR is the signal-to-noise ratio) by considering a 16-dB loss (equivalent to 100 km ultra-low-loss fibre with 0.16 dB km^{-1}). For such a low SNR, we developed a rate-adaptive reconciliation protocol based on multidimensional reconciliation and multi-edge type LDPC codes (see Supplementary Information). A high reconciliation efficiency of 97.99% was achieved, and the expected secret key rate is 0.14 kbps, which is indicated as the open circle in Fig. 5. Our system is comparable to state-of-the-art DV-QKD and CV-QKD systems in terms of performance and has a smaller size and potential for chip integration and mass production.

In conclusion, we have reported here the use of a silicon photonic chip for CV-QKD. All components except the laser source, including the modulators, multiplexers and homodyne detectors, are integrated on a silicon photonic chip. Future demonstrations will focus on full-system integration with the on-chip laser source. Well-characterized noise sources and careful modelling may mitigate the impact of excess noise from experimental imperfections and improve the secret key rates[25,34]. Some recently developed self-referenced CV-QKD protocols suggest that the LO could be generated locally at Bob's side, which would substantially improve the security of current CV-QKD systems[35]. Our robust and inexpensive photonic chip can promote real-world applications of on-chip hybrid quantum–classical communication for advanced communication networks.

Online content

Any methods, additional references, Nature Research reporting summaries, source data, statements of code and data availability and associated accession codes are available at https://doi.org/10.1038/s41566-019-0504-5.

Received: 11 October 2018; Accepted: 4 July 2019;
Published online: 12 August 2019

References

1. Lo, H. K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **8**, 595–604 (2014).
2. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
3. Orieux, A. & Diamanti, E. Recent advances on integrated quantum communications. *J. Opt.* **18**, 083002 (2016).
4. Diamanti, E., Lo, H. K., Qi, B. & Yuan, Z. L. Practical challenges in quantum key distribution. *npj Quant. Inf.* **2**, 16025 (2016).
5. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
6. Grosshans, F. et al. Quantum key distribution using Gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
7. Sibson, P. et al. Chip-based quantum key distribution. *Nat. Commun.* **8**, 13984 (2017).
8. Zhang, P. et al. Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client. *Phys. Rev. Lett.* **112**, 130501 (2014).
9. Tanzilli, S. et al. On the genesis and evolution of integrated quantum optics. *Laser Photon. Rev.* **6**, 115–143 (2012).
10. Politi, A., Cryan, M. J., Rarity, J. G., Yu, S. Y. & O'Brien, J. L. Silica-on-silicon waveguide quantum circuits. *Science* **320**, 646–649 (2008).
11. Davis, K. M., Miura, K., Sugimoto, N. & Hirao, K. Writing waveguides in glass with a femtosecond laser. *Opt. Lett.* **21**, 1729–1731 (1996).
12. Huang, J. G. et al. Torsional frequency mixing and sensing in optomechanical resonators. *Appl. Phys. Lett.* **111**, 111102 (2017).
13. Shi, Y. Z. et al. Sculpting nanoparticle dynamics for single-bacteria-level screening and direct binding-efficiency measurement. *Nat. Commun.* **9**, 815 (2018).
14. Shi, Y. et al. Nanometer-precision linear sorting with synchronized optofluidic dual barriers. *Sci. Adv.* **4**, eaao0773 (2018).
15. Boaron, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).
16. Yin, H. L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
17. Ma, C. X. et al. Silicon photonic transmitter for polarization-encoded quantum key distribution. *Optica* **3**, 1274–1278 (2016).
18. Ding, Y. H. et al. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quant. Inf.* **3**, 25 (2017).
19. Sibson, P. et al. Integrated silicon photonics for high-speed quantum key distribution. *Optica* **4**, 172–177 (2017).
20. Najafi, F. et al. On-chip detection of non-classical light by scalable integration of single-photon detectors. *Nat. Commun.* **6**, 5873 (2015).
21. Pernice, W. H. P. et al. High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits. *Nat. Commun.* **3**, 1325 (2012).
22. Lodewyck, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**, 042305 (2007).
23. Ziebell, M. et al. Towards on-chip continuous-variable quantum key distribution. In *Conf. Lasers Electro-Optics (CLEO) Europe* JSV-4.2 (Optical Society of America, 2015).
24. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photon.* **7**, 378–381 (2013).
25. Huang, D., Huang, P., Lin, D. K. & Zeng, G. H. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **6**, 19201 (2016).
26. Rude, M. et al. Interferometric photodetection in silicon photonics for phase diffusion quantum entropy sources. *Opt. Express* **26**, 31957–31964 (2018).
27. Raffaelli, F. et al. Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip. *Opt. Express* **26**, 19730–19741 (2018).
28. Abellan, C. et al. Quantum entropy source on an InP photonic integrated circuit for random number generation. *Optica* **3**, 989–994 (2016).
29. Raffaelli, F. et al. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. *Quantum Sci. Technol.* **3**, 025003 (2018).
30. Lance, A. M. et al. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.* **95**, 180503 (2005).
31. Shen, Y., Zou, H. X., Tian, L. A., Chen, P. X. & Yuan, J. M. Experimental study on discretely modulated continuous-variable quantum key distribution. *Phys. Rev. A* **82**, 022317 (2010).
32. Wang, X. Y., Zhang, Y. C., Yu, S. & Guo, H. High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code. *Sci. Rep.* **8**, 10543 (2018).
33. Milicevic, M., Feng, C., Zhang, L. M. & Gulak, P. G. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. *npj Quant. Inf.* **4**, 21 (2018).
34. Jouguet, P., Kunz-Jacques, S., Diamanti, E. & Leverrier, A. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A* **86**, 032309 (2012).
35. Qi, B., Lougovski, P., Pooser, R., Grice, W. & Bobrek, M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X* **5**, 041009 (2015).

Acknowledgements

This work was supported by the Singapore Ministry of Education (MOE) Tier 3 grant (MOE2017-T3-1-001), the Singapore National Research Foundation (NRF) National Natural Science Foundation of China (NSFC) joint grant (NRF2017NRF-NSFC002-014) and the Singapore National Research Foundation under the Competitive Research Program (NRF-CRP13-2014-01).

Author contributions

G.Z., L.C.K. and A.Q.L. jointly conceived the idea. G.Z. and H.C. designed and fabricated the silicon photonic chip. G.Z., Y.Z., S.Y., J.W., W.S., F.X. and X.Z. performed the experiments. J.Y.H., S.M.A., J.F.F. and L.C.K. assisted with the theory. All authors contributed to the discussion of experimental results. F.X., L.C.K. and A.Q.L. supervised and coordinated all the work. G.Z., F.X., L.C.K. and A.Q.L. wrote the manuscript with contributions from all co-authors.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information is available for this paper at https://doi.org/10.1038/s41566-019-0504-5.

Reprints and permissions information is available at www.nature.com/reprints.

Correspondence and requests for materials should be addressed to F.X., L.C.K. or A.Q.L.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Methods

Experimental set-up. The source was a 1,550-nm laser with 12 dBm power from a Santec TSL-510 tunable laser. After travelling through a polarization controller, the laser was coupled to the photonic chip. The amplitude and phase modulation were then performed by applying two white noise signals from two HP 33120A arbitrary waveform generators. The white noise frequency could reach up to 10 MHz. For the current proof-of-principle testing, the LO phase tuning was also conducted on the same chip. An off-chip homodyne detector was used to assist the measurement of excess noise and modulation variance from Alice's chip. A Peltier device together with a Thorlab TED200C temperature controller was used to stabilize the temperature of the entire chip, which would reduce the noise from the heat fluctuations in the environment and heat crosstalk on the chip. The output from the homodyne detector was monitored in both time and frequency domains on a Tektronix MDO4104B-3 oscilloscope. The data were analysed offline using MATLAB.

Information reconciliation. A full demonstration of CV-QKD including the post-processing was presented. The efficiency of the protocol only depended on the SNR of the transmission. Here, under the pure lossy channel assumption, the SNR of the transmission was defined as

$$\mathrm{SNR} = \frac{V_{\mathrm{mod}}}{1+\chi_{\mathrm{tot}}}$$

where V_{mod} is the modulation variance and χ_{tot} is the total added noise between Alice and Bob. Two post-processing protocols were implemented to generate the secret key in the second stage. The selection of the protocol is based on the SNR of the transmission. With a high SNR (SNR = 2.20), which corresponded to a 2-m fibre transmission distance, the slice reconciliation and LDPC error correction were performed on the measured data. The resulting secure fraction was 0.516 bits per symbol. With a low SNR (SNR = 0.028), which corresponded to a 100-km simulated transmission distance, we developed a rate-adaptive reconciliation protocol based on multidimensional reconciliation and multi-edge-type LDPC codes. A reconciliation efficiency of 97.99% was achieved. The resulting secure fraction was 1.8×10^{-4} bits per symbol.

Data availability

The data that support the plots within this paper and other findings of this study are available from the corresponding authors upon reasonable request.