An Integrated Silicon Photonic Chip Platform for Continuous-Variable Quantum Key Distribution

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

[1]*School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798*

[2]*Centre for Quantum Computation and Communication Technology, The Australian National University, Canberra, Australian Capital Territory 2601, Australia*

[3]*Institute of Microelectronics, A*STAR, Singapore 138634*

[4]*Shanghai Branch, National Laboratory for Physical Sciences at the Microscale, University of Science and Technology of China, Shanghai 201315, China*

[5]*Singapore University of Technology and Design, Singapore 138682.*

[6]*State Key Laboratory of Optoelectronic Materials and Technologies, Sun Yat-sen University, Guangzhou 510275, China*

[7]*State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[8]*Centre for Quantum Technologies, National University of Singapore, Singapore 117543*

[†] *Corresponding Author:* feihuxu@ustc.edu.cn, cqtklc@nus.edu.sg, eaqliu@ntu.edu.sg

To realize a miniaturized and low-cost quantum key distribution (QKD) system on an integrated photonic chip is challenging yet highly coveted for the development of quantum networks[1-3]. Continuous-variable QKD (CV-QKD) is particularly suitable for cost-effective photonic integration due to its compatibility with existing fiber optical communication technology[4]. In this paper, an integrated silicon photonic chip that implements the Gaussian-modulated coherent state protocol for CV-QKD[5, 6] is demonstrated. All required components, except the laser, are integrated on the silicon photonic chip. 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 fiber, offering new possibilities for low-cost, scalable and portable quantum networks.

Quantum key distribution (QKD) is an emerging technology that applies fundamental quantum mechanic theories to realize unconditional communication security[1, 2]. QKD has been successfully demonstrated in various platforms such as fiber optical communication, free-space communication and satellite[2]. Silicon photonic technology enables on-chip QKD with many unprecedented advantages[3, 7]. Over the past few years, different substrates have been explored for chip-level integration of QKD[3]. Indium phosphide (InP)[8], lithium niobate ($LiNbO_3$)[9] and potassium titanyl phosphate (KTP)[10] have been used to fabricate on-chip lasers and fast modulators. Silica[11, 12] offer low-loss delay line and fiber-chip coupler, but lack rapid modulation. Silicon relies on well-established microfabrication techniques and is ideally suited for both on-chip photonic components.

There are two major categories of QKD systems, namely discrete-variable (DV-QKD) and continuous-variable QKD (CV-QKD). Fiber-based DV-QKD has been

demonstrated up to around 400-km ultra-low loss fiber[13, 14]. The key rate is around kbps level at 100 km distance, as reported in ref[14]. Several DV-QKD protocols, including encoding on photon polarization[15], spatial dimension[16] and time bin[17], 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[18, 19]. Compare to DV-QKD, CV-QKD is more suitable for photonic chip integration due to its compatibility with existing telecom technologies[20, 21]. A fiber-based CV-QKD system showed a secure key rate of about 1 kbps at 80 km transmission distance in 2013[22], and the distance was further pushed to over 100 km by controlling the excess noise[23]. Very recently, several on-chip quantum entropy sources based on the detection of phase-fluctuation[24-26] and vacuum fluctuation[27] were reported. The chip-based homodyne detector showed a gain of 4.5 kV/A with 150-MHz bandwidth[27].

In this paper, we report a Gaussian-modulated coherent states CV-QKD protocol on an integrated silicon photonic chip. The on-chip integration increases the stability and scalability of all optical components, reduces the cost, and extends the applicability of photonic chip to CV-QKD and potentially other quantum communication protocols.

Figure 1 shows the schematics of the silicon photonic CV-QKD chip. In the transmitter chip (Alice), a 1550-nm continuous wave (CW) 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[28, 29]. 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 (2D) 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 2D grating coupler. Unlike previous protocols with requires an ultra-high (60-80 dB) intensity difference between the signal and the LO[22, 30], our design only requires a 35-dB extinction ratio because the information is encoded on the sideband frequency which is the AC 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, eavesdropper's (Eve) attempt to measure one quadrature would result in noise in the other, which implies that the amount of information leaked to Eve is bound by the noise level detected by Alice and Bob.

Figure 2a illustrates the Mach-Zehnder interferometer (MZI) structure designed as the amplitude modulator. The photo of the transmitter chip packaged with PCB is shown in Figure 2b. Figure 3a demonstrates that the amplitude and phase modulators 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 the modulator.

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 Figure 2c. The signals from the two PDs 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. The homodyne detector must be able to distinguish the shot noise of the LO light from the electronic background noise, because CV-QKD uses the constant shot noise as a reference to normalize the signals and 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 Figs. 3b and 3c, 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 the shot noise clearance (SNC). The homodyne detection efficiency is calculated as $\eta = \eta_{PD}\eta_{vis}^2 = 0.498$, where η_{PD} is the quantum efficiency of photodiode and η_{vis} is the visibility.

The QKD transmitter chip is calibrated using an off-chip detector with a fiber polarization control. 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 of 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. Next, the filtered signals are demodulated and downsampled to 0.8 Mbps to generate a set of correlated Gaussian key, that are shown in the insets of Figure 4a and 4b with Alice's key as *x*-coordinate and Bob's key as *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 lab[20]. The total losses consist of the losses on the transmission line and Bob's equipment while the losses on the Alice side do not affect the final security key. The homodyne detection efficiency is measured to be η = 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 ε = 0.0934 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 line in Figure 5. Considering a more practical situation, the reconciliation efficiency β = 0.98 and 0.99 is chosen[31, 32], which represents the case we have achieved and the state-of-the-art case. The

corresponding Shannon effective key rate and Holevo effective key rate are shown as the solid line in Figure 5.

We performed an experiment to demonstrate CV-QKD over a 2-m fiber 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 a solid dot in Figure 5. Furthermore, to prove the capability for long-distance CV-QKD, we simulated the total noise χ_{tot} and obtain that SNR = 0.028 (see Methods), by considering a 16-dB loss (equivalent to 100 km ultra-low-loss fiber with 0.16 dB/km). In such a low SNR, we developed a rate-adaptive reconciliation protocol based on multidimensional reconciliation and multi-edge type LDPC codes (see Supplementary). A high reconciliation efficiency of 97.99% was achieved, and the expected secret key rate is 0.14 kbps, which is indicated as a circle in Figure 5. Our system is comparable to the state-of-the-art DV-and CV-QKD systems in terms of performance and has a smaller size and potential for chip-integration and mass production.

In conclusion, this is the first time that the silicon photonic chip has been used 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 on-chip laser source. Well-Characterized noise sources and careful modeling may mitigate the impact of excess noise from experimental imperfection and improve the secret key rates[23, 33]. Some recently developed self-referenced CV-QKD protocols suggest that the LO could be generated locally at Bob's side, which would significantly improve the security of current CV-QKD system[30]. Our

robust and inexpensive photonic chip can promote real-world applications of on-chip hybrid quantum-classical communication for advanced communication network.

Methods

Experimental setup. The source was a 1550-nm laser with 12 dBm power from Santec TSL-510 tunable laser. After a polarization controller, the laser was coupled to the photonic chip. The AM and PM were then performed by applying two white noise signals from HP 33120A arbitrary waveform generator. 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 environment heat fluctuation 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 analyzed 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 signal-to-noise ratio (SNR) of the transmission. Here, under the pure lossy channel assumption, the SNR of the transmission was defined as

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

where V_{mod} is the modulation variance and χ_{tot} is the total added noise between Alice and Bob. Two post processing protocols are 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 fiber transmission distance, the slice reconciliation and low-density parity check (LDPC) error correction are performed on the measured data. The resulting secure fraction was 0.516 bits/symbol. With a low SNR (SNR = 0.028), which corresponded to a 100-km simulated transmission distance, we had 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/ symbol.

Acknowledgment

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), the Singapore National Research Foundation under its Environmental & Water Technologies Strategic Research Programme (1102-IRIS-05-02) & (1102-IRIS-05-05), which is administered by the Environment & Water Industry Programme Office (EWI) of the PUB, National Natural Science Foundation of China (Grants No. 61771443), Thousand Young Talent Program of China and Australian Research Council (ARC) under the Centre of Excellence for Quantum Computation and Communication Technology (project number CE110001027).

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.Q.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 works. 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.

References

1. Scarani, V. et al. The security of practical quantum key distribution. *Rev Mod Phys* **81**, 1301-1350 (2009).
2. Lo, H.K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat Photonics* **8**, 595-604 (2014).
3. Orieux, A. & Diamanti, E. Recent advances on integrated quantum communications. *J Optics-Uk* **18**, 083002 (2016).
4. Diamanti, E., Lo, H.K., Qi, B. & Yuan, Z.L. Practical challenges in quantum key distribution. *Npj Quantum Inform* **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. Huang, J.G. et al. Torsional frequency mixing and sensing in optomechanical resonators. *Appl Phys Lett* **111**, 111102 (2017).

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

9. 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).

10. Tanzilli, S. et al. On the genesis and evolution of Integrated Quantum Optics. *Laser Photonics Rev* **6**, 115-143 (2012).

11. 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).

12. Davis, K.M., Miura, K., Sugimoto, N. & Hirao, K. Writing waveguides in glass with a femtosecond laser. *Opt Lett* **21**, 1729-1731 (1996).

13. Boaron, A. et al. Secure Quantum Key Distribution over 421 km of Optical Fiber. *Phys Rev Lett* **121** (2018).

14. Yin, H.L. et al. Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber. *Phys Rev Lett* **117**, 190501 (2016).

15. Ma, C.X. et al. Silicon photonic transmitter for polarization-encoded quantum key distribution. *Optica* **3**, 1274-1278 (2016).

16. Ding, Y.H. et al. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *Npj Quantum Inform* **3**, 25 (2017).
17. Sibson, P. et al. Integrated silicon photonics for high-speed quantum key distribution. *Optica* **4**, 172-177 (2017).
18. Najafi, F. et al. On-chip detection of non-classical light by scalable integration of single-photon detectors. *Nat Commun* **6**, 5873 (2015).
19. 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).
20. Lodewyck, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys Rev A* **76**, 042305 (2007).
21. Ziebell, M. et al. in The European Conference on Lasers and Electro-Optics JSV_4_2 (2015).
22. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat Photonics* **7**, 378-381 (2013).
23. Huang, D., Huang, P., Lin, D.K. & Zeng, G.H. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci Rep-Uk* **6**, 19201 (2016).
24. Rude, M. et al. Interferometric photodetection in silicon photonics for phase diffusion quantum entropy sources. *Opt Express* **26**, 31957-31964 (2018).
25. 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).

26. Abellan, C. et al. Quantum entropy source on an InP photonic integrated circuit for random number generation. *Optica* **3**, 989-994 (2016).
27. 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).
28. Lance, A.M. et al. No-switching quantum key distribution using broadband modulated coherent light. *Phys Rev Lett* **95**, 180503 (2005).
29. 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).
30. 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).
31. 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-Uk* **8**, 10543 (2018).
32. Milicevic, M., Feng, C., Zhang, L.M. & Gulak, P.G. Key reconciliation with low-density parity-check codes for long-distance quantum cryptography. *arXiv preprint arXiv:1702.07740* (2017).
33. 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).

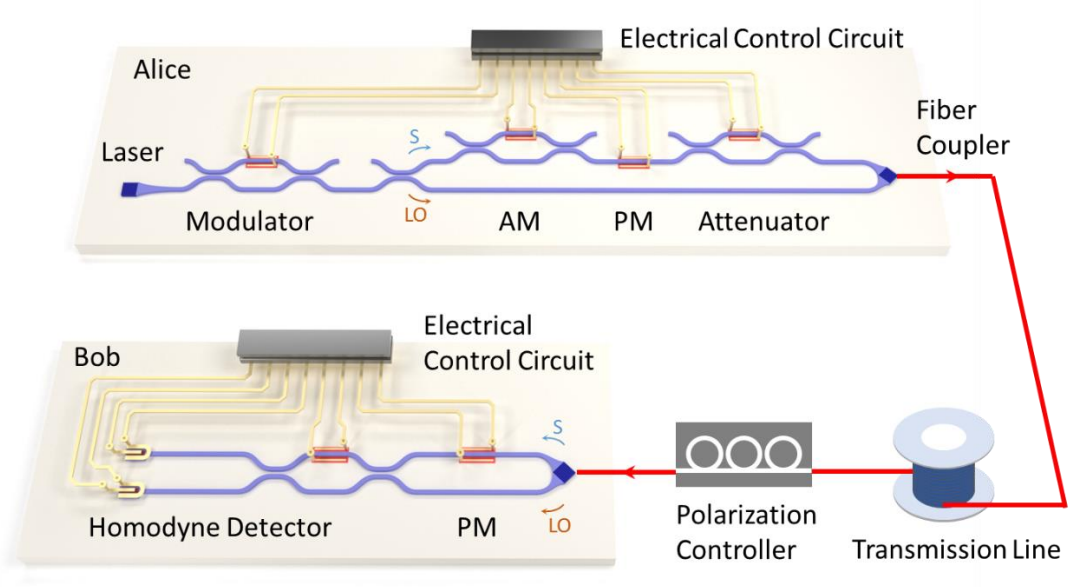

Figure 1 | Schematics of the CV-QKD system. The system built on silicon photonic chips contains two parties, Alice and Bob, which are used as the transmitter and receiver. Alice side consists of several amplitude modulators (AM), phase modulators (PM), attenuators and grating couplers, which can modulate the signal (S) and multiplex signal with the local oscillator (LO) in two orthogonal polarization states. Bob demultiplexes and detects the signal with the receiver chip.

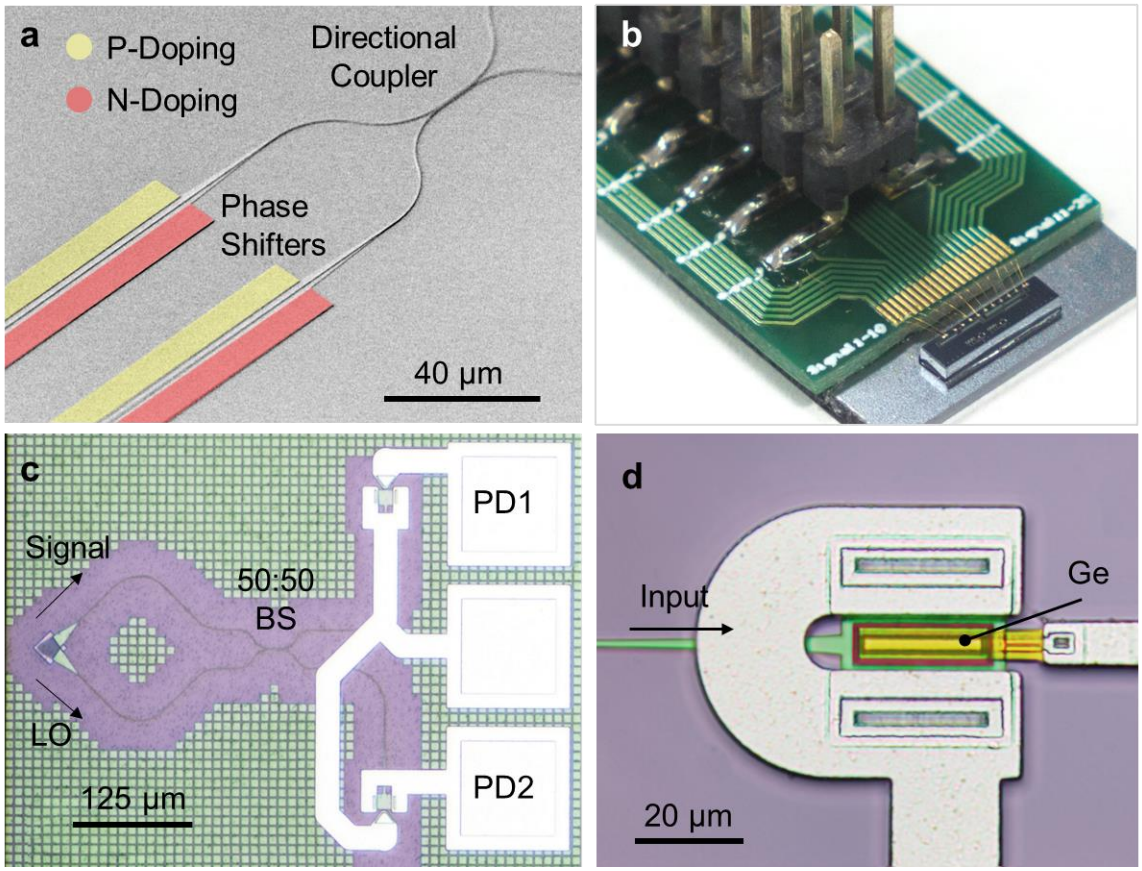

Figure 2 | SEM and microscopic photos of the QKD chip. (a) SEM of part of the amplitude modulator structure, including the p-i-n phase shifter and directional couplers. **(b)** QKD chip packaging with PCB board. **(c)** Microscopic photo of the on-chip homodyne detector, which is also the receiver chip. The signal from two photodiodes (PD) is subtracted and amplified. **(d)** Enlarged microscopic photo of the on-chip germanium PD.

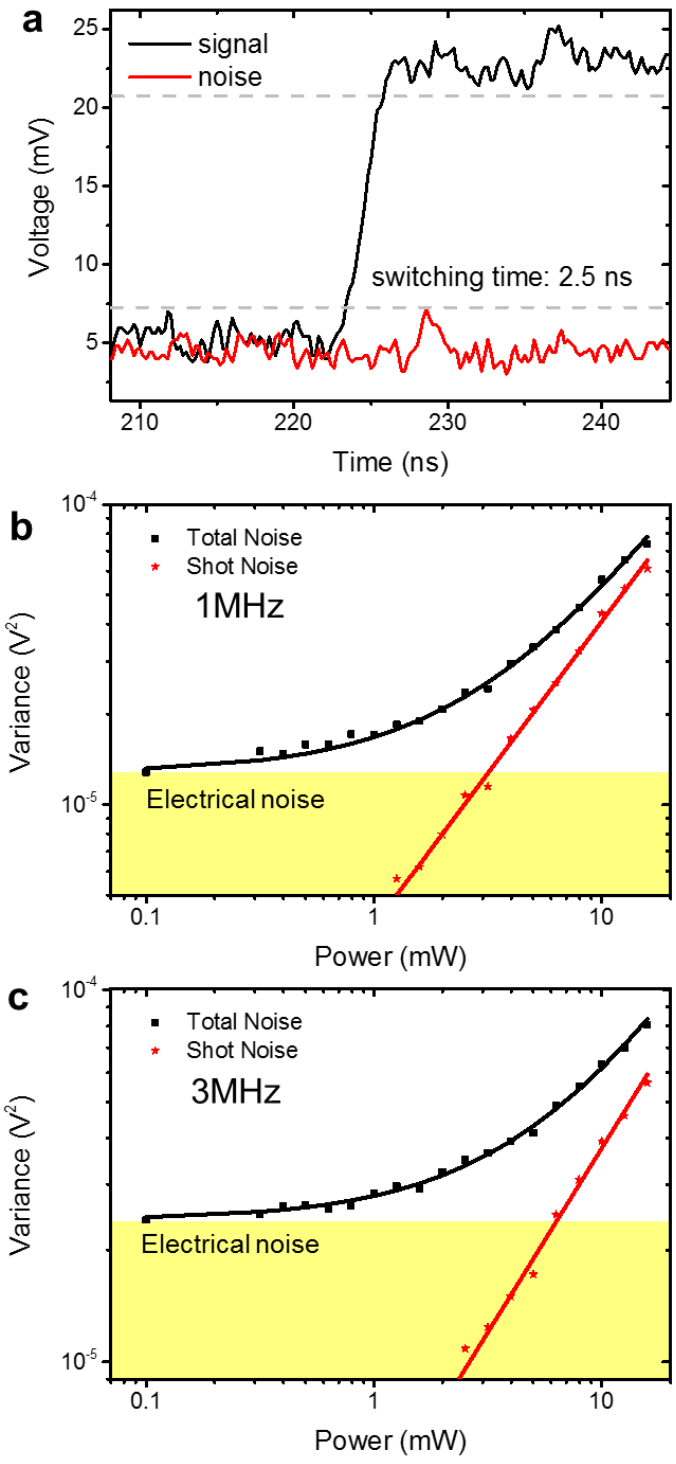

Figure 3 | Chip performance analysis. (a) Switching speed of the modulator. **(b)** Total noise variance and fitted shot noise for the homodyne detector with different input LO power level at the 1 MHz band and **(c)** 3 MHz band.

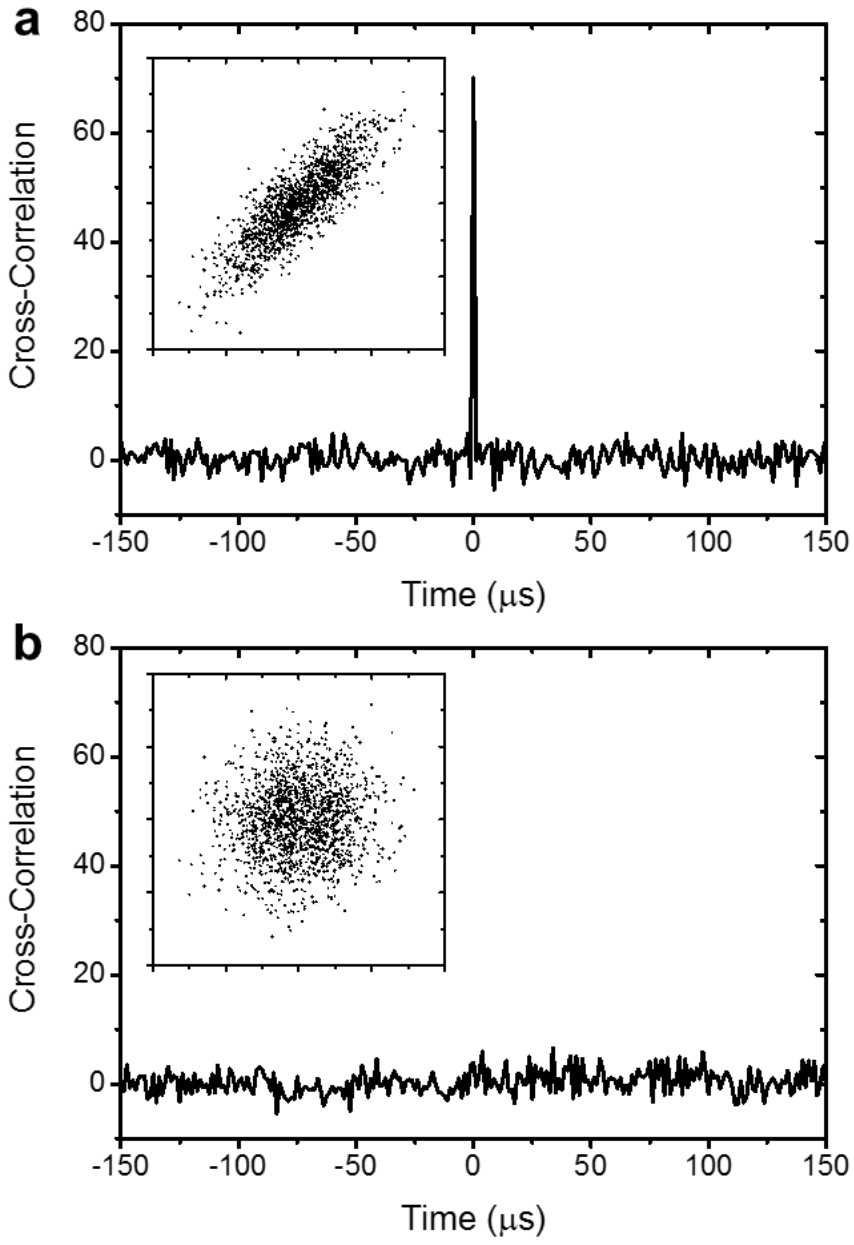

Figure 4 | Key distribution test. Cross-correlation result of Bob's measurement result and Alice's modulation on **(a)** corresponding quadrature **(b)** different quadrature. The inset shows the correlated gaussian key in two different situations.

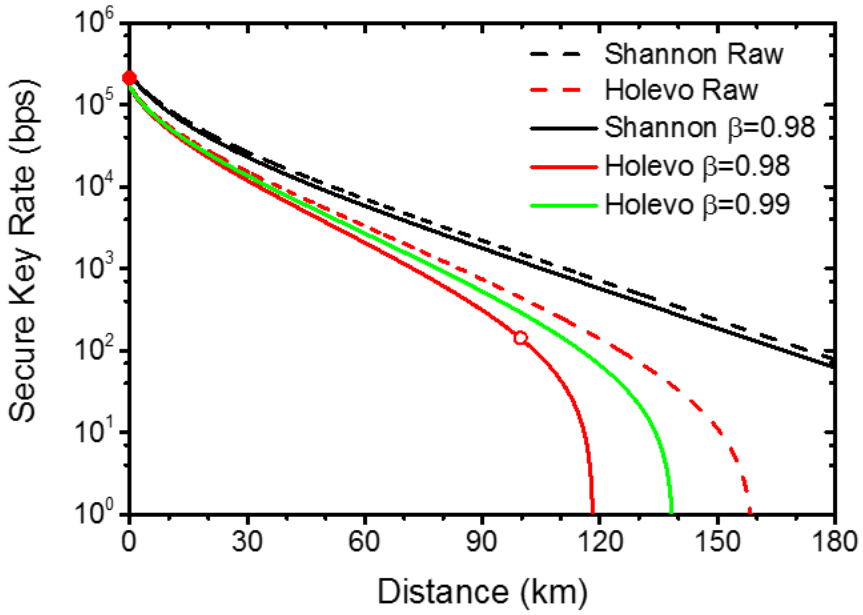

Figure 5 | Secure Key rate analysis. The secure key rate under individual attack (black line) and collective attack (red line). Considering a practical case, the reconciliation efficiency of 0.98 and 0.99 is used to calculate the effective key rate after the reconciliation process. The solid dot near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