nature photonics

SUPPLEMENTARY INFORMATION

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

In the format provided by the authors and unedited.

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]*

[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

Supplementary Information

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

Chip Fabrication. As shown in Figure S1, three consecutive deep-UV lithography steps and reactive-ion etching processes formed the silicon waveguide (with a width of 450 nm), grating coupler and rib structures. Boron and phosphorous doping were then performed, with an impurity concentration of approximately 10^{20} cm^{-3}. After patterning the waveguide structure, the waveguide surface was doped with boron with a 10^{19} cm^{-3} concentration. Then, a 500-nm germanium layer was epitaxially grown on top of the waveguide structure. The top of the germanium was doped with phosphorous to form a p-i-n junction in the vertical direction, resulting in the on-chip PD. After covering the silicon structures with 2-um thickness silicon dioxide (SiO_2), the via hole structures were etched on the SiO_2 layer for electrical connection. Then, a 750-nm thick aluminium layer was deposited and patterned as the conduction layer, which acted as the electrical connections for active control.

Cross modulation. To precisely modulate the signal, the cross-modulation of the AM and the PM was measured to confirm that the two modulators did not affect each other. A sine wave of 5-MHz frequency was added on the AM and 6-MHz was added on the PM. The output signal spectrum from the homodyne detector was monitored while the LO phase was scanned by another PM.

The result in the top graph of Figure S2a shows that the power root-mean-square (RMS) at 5 MHz and 6 MHz, which corresponds to the AM and PM modulation signal. The difference between these two signals is shown in the bottom graph of Figure S2a. The difference between the maximum and minimum is more than 40 dB, which proves that the AM signal and PM signal has more than 40dB isolation between each other and precisely

reflects the added modulation signal. The maximum and minimum point is also used to choose the measured quadrature. The difference is measured before and after each measurement to confirm there is no significant signal drift. Figure S2b shows the spectrum from 4.5 to 6.5 MHz at 1.1 V and 2 V modulation power respectively, which correspond to the maximum and minimum point marked with dash lines in Figure S2a.

Receiver common mode rejection ratio. The common mode rejection ratio of the homodyne detector is also tested. Figure S3 shows the spectrum output when the LO beam is modulated with a 7 MHz sine wave. The two curves show the balanced and unbalanced results, which are achieved by switching one of the PDs in on- or off-state, respectively. The RMS has 25 dB difference in these two states, which indicates that the homodyne detector is well balanced and capable of reducing the classical noise in the LO beam by 25 dB.

System noise analysis. Figure S4 shows the different noise spectra in the system. The oscilloscope noise is at about -120 dBm, and the electronic noise of the detector is approximately 30 dB higher. The shot noise is 5-10 dB higher than the electronic background noise, which corresponds to a 5-10 dB signal to noise ratio at the 1-10MHz band. White noise from the function generator is used to modulate the signal randomly as required by the protocol. By switching on the modulation, the measured output is 10 dB higher than the shot noise, which is referred to as a 10 SNU modulation.

Homodyne detection. The output current i of the homodyne detector is obtained by subtracting signals from the two balanced PDs, which can be expressed as

$$i \propto 2E_{LO}(E_S^X \cos\phi_{LO} + E_S^P \sin\phi_{LO}) \quad (1)$$

where E_{LO} is the amplitude of the LO beam and ϕ_{LO} is its phase relative to the signal beam. E_S^X and E_S^P are the amplitudes of the signal light projecting to x and p quadratures, respectively. When $\phi_{LO} = 0$, the output is only proportional to E_S^X, and when $\phi_{LO} = \pi/2$, the output is proportional to E_S^P. Thus, the x or p quadratures of the signal light can be measured by tuning the phase of the LO light.

Secure Key Rate Analysis. Following the optimality of Gaussian collective attacks on the Gaussian CV-QKD, the CV-QKD system can be fully characterized by the modulation variance $V_{mod} = V - 1$, channel transmission T and the excess noise ε[1-4]. These parameters were sufficient to estimate the secret key rate. By considering the source of noise, the total noise can be categorized into two parts, which can be expressed as $\chi_{tot} = \chi_{ch} + \chi_{det}/T$. The channel added noise $\chi_{ch} = 1/T - 1 + \varepsilon$ consists of the channel loss and excess noise, which is all the noise added before Bob. The homodyne detector added noise is expressed as $\chi_{det} = (1 + v_{el})/\eta - 1$, where v_{el} is the electronic noise of Bob's equipment and η is homodyne detection efficiency. The noise source is clarified so that another assumption can be made, which is the so-called "Loose Security Assumption" or "Trusted-device Scenario," which means an eavesdropper cannot have access to the noise χ_{det} from the instrument in Bob's lab.

The mutual information between Alice and Bob I_{AB} is given by

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} = \frac{1}{2}\log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}} \,, \tag{2}$$

where $V_B = \eta T(V + \chi_{tot})$ is the variance obtained by Bob and $V_{B|A} = \eta T(1 + \chi_{tot})$ is the conditional variance of Bob's measurement regarding Alice's sending. Then Eve's information in the reverse reconciliation protocol is given by

$$I_{BE} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|E}} = \frac{1}{2}\log_2 \frac{\eta T(V + \chi_{tot})}{\frac{1}{\eta(\frac{1}{T(1/V + \chi_{ch})} + \chi_{det})}} \,. \tag{3}$$

The Holevo information between Eve and Bob is given by $\chi_{BE} = S_E - S_{E|B}$, where S_E is the von Neumann entropy for Eve's measurement and can be calculated from the symplectic eigenvalue $\lambda_{1,2}$ of the covariance matrix

$$\gamma_{AB} = \begin{pmatrix} V \cdot I_2 & \sqrt{T\left(V^2 - 1\right)} \cdot \sigma_z \\ \sqrt{T\left(V^2 - 1\right)} \cdot \sigma_z & T(V + \chi_{ch}) \cdot I_2 \end{pmatrix} = \begin{pmatrix} a \cdot I_2 & c \cdot \sigma_z \\ c \cdot \sigma_z & b \cdot I_2 \end{pmatrix} \tag{4}$$

where I_2 is the two-dimensional identity matrix and σ_z is the Pauli-z matrix. The symplectic eigenvalue can be calculated by

$$\lambda_{1,2} = \frac{1}{2}\left(\sqrt{(a + b)^2 - 4c^2} \pm (b - a)\right) \,. \tag{5}$$

The entropy $S_{E|B}$ is calculated from the same covariance matrix after a projection caused by Bob's homodyne detection. The new symplectic eigenvalue $\lambda_{3,4}$ is given by

$$\lambda_{3,4} = \sqrt{\frac{1}{2}\left(\alpha \pm \sqrt{\alpha^2 - 4\beta}\right)} \,, \tag{6}$$

with

$$\begin{cases} \alpha = \dfrac{a(ab-c^2)+b+(a^2+b^2-2c^2)\chi_{det}}{b+\chi_{det}}, & \text{(7a)} \\ \beta = \dfrac{a(ab-c^2)+(ab-c^2)^2\chi_{det}}{b+\chi_{det}} \ . & \text{(7b)} \end{cases}$$

The Holevo information is given by

$$\chi_{BE} = g\left(\frac{\lambda_1-1}{2}\right)+g\left(\frac{\lambda_2-1}{2}\right)-g\left(\frac{\lambda_3-1}{2}\right)-g\left(\frac{\lambda_4-1}{2}\right), \quad (8)$$

where $g(x) = (x+1)\log_2(x+1) - x\log_2 x$.

The secure key rate is calculated under the assumption of individual attack and collective attack[1, 2]. The coherent attack is the most potent attack, but it was proven not more efficient than collective attacks for Gaussian modulated CV-QKD protocol[5, 6]. Therefore, the secure key rate calculation based on collective attack assumption could provide unconditional security. The asymptotic secure key fraction (bits/symbol) against the individual attack and the collective attack, which are referred to as Shannon key rate and Holevo key rate, is $r_{individual}^{asymptotic} \geq I_{AB} - I_{BE}$ and $r_{collective}^{asymptotic} \geq I_{AB} - \chi_{BE}$, respectively. I_{AB} and I_{BE} are the mutual information shared between Alice & Bob and between Bob & Eve respectively. χ_{BE} is the Holevo information between Eve & Bob. The secure key rate K is given by $K = SR \cdot r$, where SR is the symbol rate in the unit of symbols/s.

Above analysis has not considered the effect of all the post-processing. A practical data reconciliation method requires more bits to be exchanged than the theoretical limit. Also, some bits are used for system calibration and parameter estimation, which also cannot be used in final key extraction. Thus, a more practical secure key rate is given by $K_{individual,practical}^{asymtotic} = SR(1-FER)(1-\nu)(\beta I_{AB} - I_{BE})$ and $K_{collective,practical}^{asymtotic} = SR(1-FER)(1-\nu)(\beta I_{AB} - \chi_{BE})$, where SR is the symbol rate, FER is the frame-error-

rate, υ is the fraction of bits that cannot be used to distil the final key and β is the reconciliation efficiency.

As shown in Figure S5, the effect of modulation variance V_{mod}, channel transmittance T and the excess noise ε to the final secret fraction is calculated. The calculation is under the assumption of collective attack and a reconciliation efficiency of 0.98 is considered. The secret fraction r in the unit of bits/symbol indicates how much secret keys can be extracted from one Gaussian symbol. The secret fraction as a function of excess noise ε from 0.07 to 0.25 and transmittance T from 0 to 1 is shown, in Figure S5a. The modulation variance is $V_{mod} = 7$. When $r < 0$, it means no secure key can be extracted from the key distribution process, which is marked in a yellow shade. The result shows that lower the excess noise, higher the secure key fraction. When excess noise $\varepsilon = 0.25$, the minimum transmittance acceptable is about $T = 0.6$, which reaches the limitation for our fibre-chip coupler. Thus, $\varepsilon < 0.25$ is a requirement for our photonic chip. The secret fraction r at $V_{mod} = 2$ to 15, $T = 0$ to 1 and $\varepsilon = 0.1$ is shown in Figure S5b. At the low-loss and short-distance scenario ($T > 0.3$), the secret fraction r increases when V_{mod} increases. Higher modulation variance could significantly increase the secure key fraction. However, at the high-loss and long-distance region (Transmittance < 0.3), there is an optimum modulation variance available, as shown in the inset of Figure S5b. The maximum secure key fraction and minimum acceptable transmittance occur at a modulation variance of about $V_{mod} = 6$, where the limitation for transmittance is $T = 0.016$. The loss we consider here is all contributing to channel loss, which can convert to fibre distance (0.16-0.2 dB/km). The corresponding maximum transmission distance is about 100 km. The parameters tested in our experiment are summarized in Table S1. The secret fraction at different reconciliation

Table S1 Summary of characterized parameters.

Parameters	Value	Experimental/ Theoretical
Detector quantum efficiency	0.59	Experimental
Homodyne detection efficiency	0.498	Experimental
Electrical noise (SNU)	0.069	Experimental
Total excessive noise (SNU)	0.094	Experimental
Modulation variance (SNU)	7.07	Experimental
Operation band (MHz)	3	Experimental
Loss at receiver (dB)	5	Experimental
Fiber loss (dB/km)	0.16	Theoretical
Reconciliation efficiency	0.98	Experimental

efficiency is also calculated. As shown in Figure S6a, the theoretical limit for transmission distance is about 160 km. Considering a reconciliation efficiency of 0.95-0.99, the ultimate transmission distance could achieve 60-140 km.

Information reconciliation. A full demonstration of CV-QKD including the post-processing part was presented. The efficiency of the protocol only depends on the signal-to-noise ratio (SNR) of the transmission. Here, under the pure lossy channel assumption, the SNR of the transmission can be calculated as

$$SNR = \frac{V_{mod}}{1 + \chi_{tot}}. \tag{9}$$

The SNR as a function of transmission distance is shown in Figure S6b. Due to the different optimum SNR for different post-processing protocols, two different protocols are implemented targeting both the high SNR and low SNR scenario. At high SNR scenario (SNR = 2.20), which corresponded to the 2-m transmission distance, the slice reconciliation

and low-density parity check (LDPC) error correction are performed on the real data. The resulting secure fraction is 0.516 bits/symbol. At low SNR scenario (SNR = 0.028), which corresponding to a 100-km transmission distance (0.16 dB/km loss), we developed a rate-adaptive reconciliation protocol based on multidimensional reconciliation and multi-edge type LDPC codes[7, 8]. A reconciliation efficiency of 97.99% is achieved. The resulting secure fraction was 1.8×10^{-4} bits/ symbol.

At 0 km transmission distance, the slice reconciliation and LDPC error correction are performed. Bob uses a slice function $S(x')$ to map one of his key x' into an m bits binary string $\left(S_1(x'), S_2(x'), \ldots, S_m(x')\right)$. The domain for Bob's key is divided into $t = 2^m$ intervals by $\tau_0, \ldots, \tau_t$, where $\tau_0 = -\infty$ and $\tau_t = \infty$. Each interval a with $(x': \tau_a \leq x' < \tau_{a+1})$ is mapped to a m bits binary string $binary(a)$. Alice on the other side, tries to guess Bob's binary string $S(x')$ based on her key x, using the slice estimator $\hat{S}$. The output from slice estimator is a binary string given by

$$\left(\hat{S}_1(x), \hat{S}_2\left(x, \hat{S}_1(x)\right), \ldots, \hat{S}_m\left(x, \hat{S}_1(x), \ldots, \hat{S}_{m-1}(x)\right)\right). \quad (10)$$

The digits are calculated one by one with a recursion. The estimation for next digits is based on not only the key x Alice owns but also the estimation of all the previous digits. The mutual information shared here is $I(X, X') = 0.839$ bits/symbol. Here a 5-bits slice function is used, where the optimized interval is shown in Table S2. The optimized slice

Table S2 Optimized slice interval.

τ_{16}	$\tau_{17}, -\tau_{15}$	$\tau_{18}, -\tau_{14}$	$\tau_{19}, -\tau_{13}$	$\tau_{20}, -\tau_{12}$	$\tau_{21}, -\tau_{11}$	$\tau_{22}, -\tau_{10}$	$\tau_{23}, -\tau_{9}$
0	0.131	0.263	0.397	0.533	0.673	0.816	0.966
$\tau_{24}, -\tau_{8}$	$\tau_{25}, -\tau_{7}$	$\tau_{26}, -\tau_{6}$	$\tau_{27}, -\tau_{5}$	$\tau_{28}, -\tau_{4}$	$\tau_{29}, -\tau_{3}$	$\tau_{30}, -\tau_{2}$	$\tau_{31}, -\tau_{1}$
1.12	1.29	1.47	1.67	1.89	2.16	2.48	2.95

efficiency is calculated to be $\beta_{slice} = 99.5\%$. Based on the calculation, the mutual information contained in each slice is [0 0.001 0.011 0.191 0.632]. Thus, the first four bits are publicly disclosed to assist the reconciliation of the last digit with only 0.207 bits of information disclosed. LDPC binary error correction protocol is then used on the last bit to correct all the errors. The last bit has an error rate of $e = 0.0299$ and can be treated as a binary symmetric channel (BSC). A LDPC code with code rate $r = 0.78$ is applied to the data with a block size of 10000. Based on a testing of 100 blocks, the resulting frame error rate (FER) is 40% with 128 average decoding iterations. The final secret fraction at 0 km is 0.516 bits/symbol.

At 100 km transmission distance, high-efficiency post processing at low SNR is a significant step to push the limit. We developed the rate-adaptive reconciliation protocol based on multidimensional reconciliation and multi-edge type LDPC codes[7, 8].

Multidimensional reconciliation converts the correlated gaussian keys shared by Alice and Bob into a correlated bit string. Alice and Bob first combine d consecutive gaussian variables they shared into two series of d-dimensional vectors $\boldsymbol{X} \sim \mathcal{N}(0,1)^d$ and $\boldsymbol{Y} \sim \mathcal{N}(0,1+\sigma^2)^d$. The vectors distribute uniformly near a n-dimensional unit hypersphere. Thus, the distance and distinguishability of each vector are maximized comparing to the 1-dimensional case. The effect of noise on the low amplitude gaussian variables measurement is significantly reduced. Bob then choose a random codeword $\boldsymbol{U} \in \left\{-\frac{1}{\sqrt{d}}, \frac{1}{\sqrt{d}}\right\}^d$ and send the rotation $\boldsymbol{R} = \boldsymbol{U} \cdot \boldsymbol{X}^{-1}$ to Alice through the public channel. Alice calculates the codeword $\boldsymbol{V}$ with the help of the gaussian keys she held as $\boldsymbol{V} = \boldsymbol{R} \cdot \boldsymbol{Y}$. The resulting codeword $\boldsymbol{V}$ is a noisy version of $\boldsymbol{U}$, which can be modelled as a virtual binary-input additive white Gaussian noise channel (BIAWGNC). Because the multiplication and

division operator are only defined in d = 1, 2, 4, 8 dimensions, the maximum of 8-dimensional reconciliation is considered.

Multi-edge type LDPC codes are used to correct the error between $\boldsymbol{U}$ and $\boldsymbol{V}$, which is a high-efficiency error correction codes perform very close to Shannon limit. At low SNR scenario, the code words typically have a length of $n = 10^6$. Bob first generates a set random bits $\boldsymbol{S}$ of length $k < n$ and encodes it based on the LDPC parity check matrix $\boldsymbol{H}$. The resulting codewords $\boldsymbol{C}$ of length n has (n - k) bits of redundant parity bits. Then Bob calculates the bitwise XOR result $\boldsymbol{I} = XOR(\boldsymbol{C}, \boldsymbol{U})$ and sends publicly to Alice as the side information. Next, Alice attempt to recover Bob's code words $\boldsymbol{C'}$ using the side information $\boldsymbol{I}$ by $C_i' = (-1)^{I_i} \cdot V_i$, with i = 1, 2, … , n. The noisy code words $\boldsymbol{C'}$ is in the form of Log-Likelihood Ratios (LLR). Based on the known variance of the channel noise, Alice uses belief propagation LDPC decoding algorithm to get the estimation of $\widehat{\boldsymbol{S}}$ and $\widehat{\boldsymbol{C}}$. If the decoding is successful, which means $\widehat{\boldsymbol{S}} = \boldsymbol{S}$, the binary key $\boldsymbol{U}$ can be calculated as $\boldsymbol{U} = XOR(\widehat{\boldsymbol{C}}, \boldsymbol{I})$. The randomness of $\boldsymbol{U}$ and $\boldsymbol{S}$ ensured that the transmission of $\boldsymbol{R}$ and $\boldsymbol{I}$ over the public channel during the two steps does not reveal any additional information about the secret key.

At about 100 km transmission distance, the SNR decreased to 0.028, which is suitable for the rate-adaptive reconciliation protocol[7, 8]. The maximum reconciliation efficiency of 97.99% is achieved using the parity check matrix with a code rate of 0.02. Thus, as shown in Figure S6a, the maximum transmission distance of about 120 km could achieve. Besides, the speed of the error correction can reach 30.39 Mbits/s on an NVIDIA TITAN Xp GPU by multiple codewords decoding simultaneously[9].

References

1. Lodewyck, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**, 042305 (2007).
2. Laudenbach, F. et al. Continuous-Variable Quantum Key Distribution with Gaussian Modulation--The Theory of Practical Implementations. *arXiv preprint arXiv:1703.09278* (2017).
3. 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).
4. Madsen, L.S., Usenko, V.C., Lassen, M., Filip, R. & Andersen, U.L. Continuous variable quantum key distribution with modulated entangled states. *Nat. Commun.* **3**, 1083 (2012).
5. Garcia-Patron, R. & Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
6. Navascues, M., Grosshans, F. & Acin, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **97**, 190502 (2006).
7. Wang, X.Y. et al. Efficient Rate-Adaptive Reconciliation for Continuous-Variable Quantum Key Distribution. *Quantum Inf. Comput.* **17**, 1123-1134 (2017).
8. Zhang, Y. et al. Continuous-variable QKD over 50 km commercial fiber. *Quantum Sci. Technol.* **4**, 035006 (2019).

9. 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).

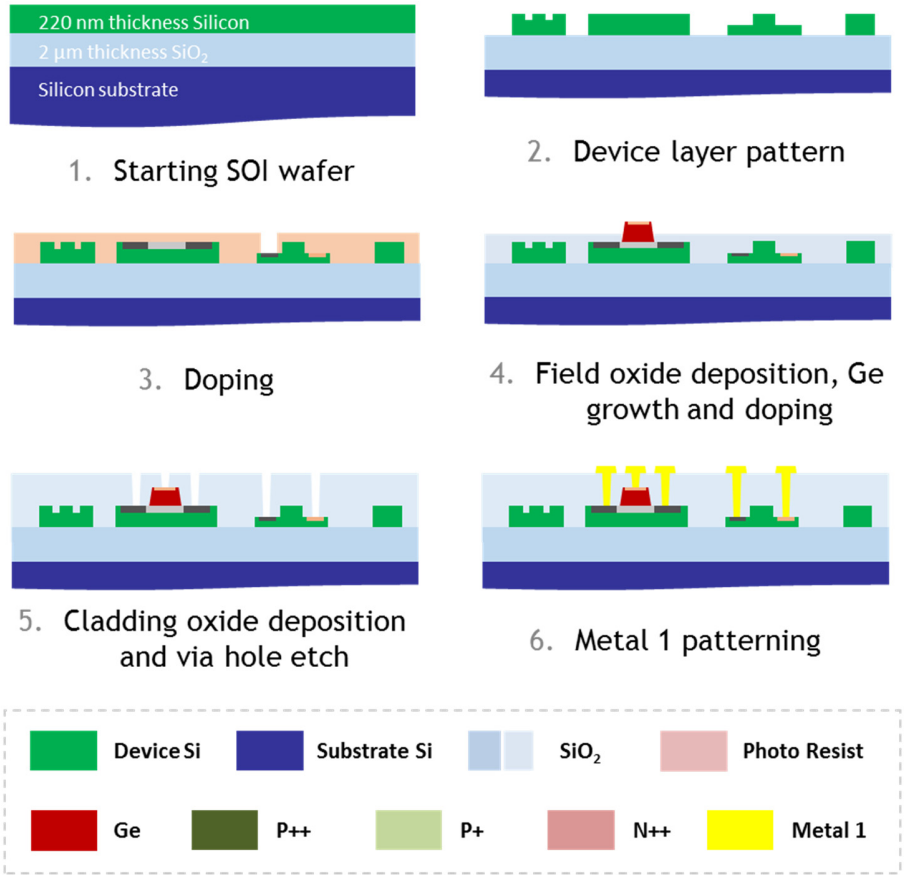

Figure S1 | Fabrication process flow.

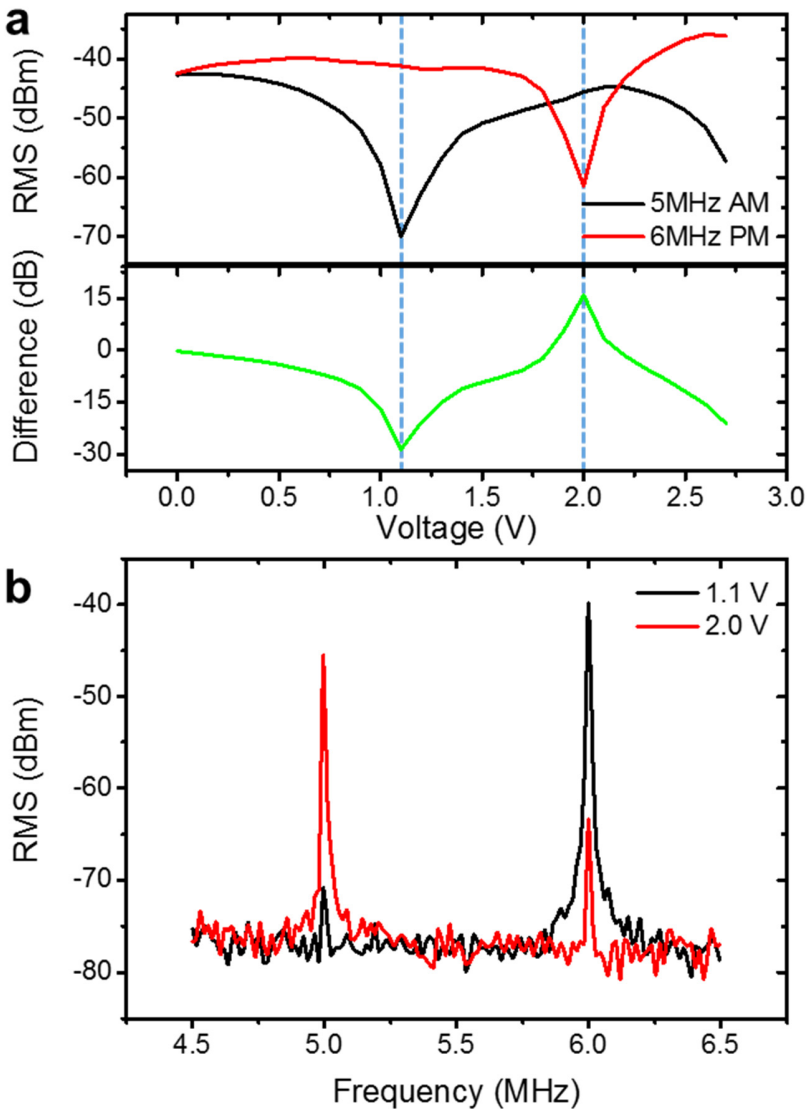

Figure S2 | Amplitude and phase modulator cross modulation. a Cross-modulation measurement of AM and PM. AM is modulated at 5 MHz and PM at 6 MHz. The power of these two frequencies is monitored when scanning the LO phase by adding voltage on PM. The difference between these two powers is shown in the bottom graph. **b** Measured frequency spectrum at maximum and minimum cross-modulation difference, which are marked with a dashed line in **a**.

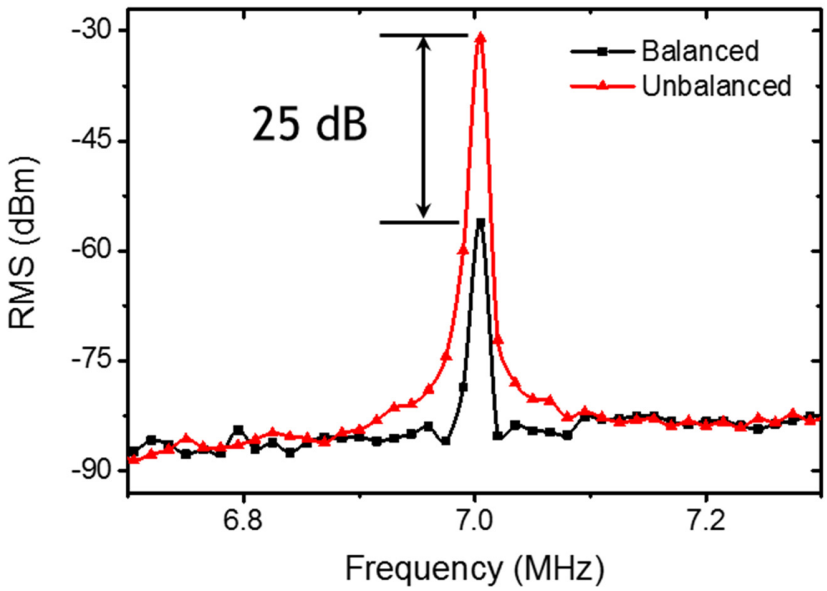

Figure S3 | Common mode rejection ratio of the homodyne detector. PD signal balance test when LO is modulated at 7 MHz and no signal is presented.

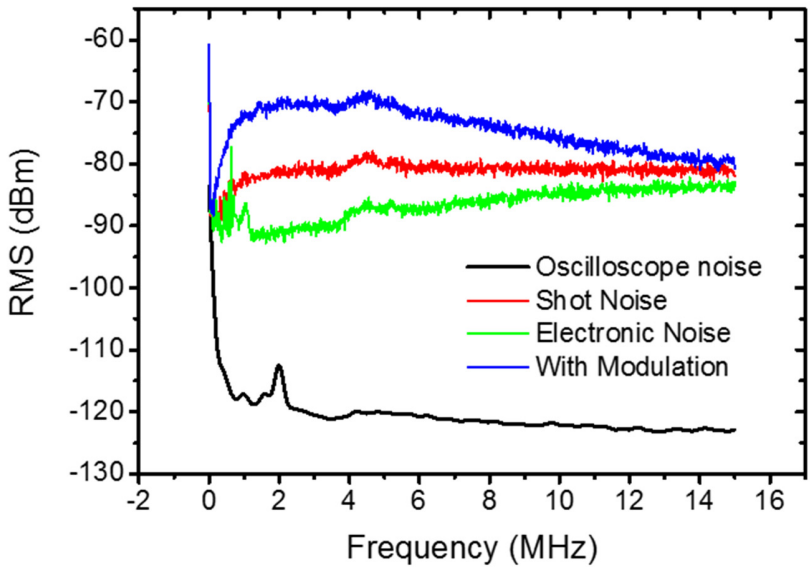

Figure S4 | System noise analysis. The noise power spectrum of the oscilloscope, electronic noise, shot noise and when the signal is modulated at 10-shot-noise-unit (SNU).

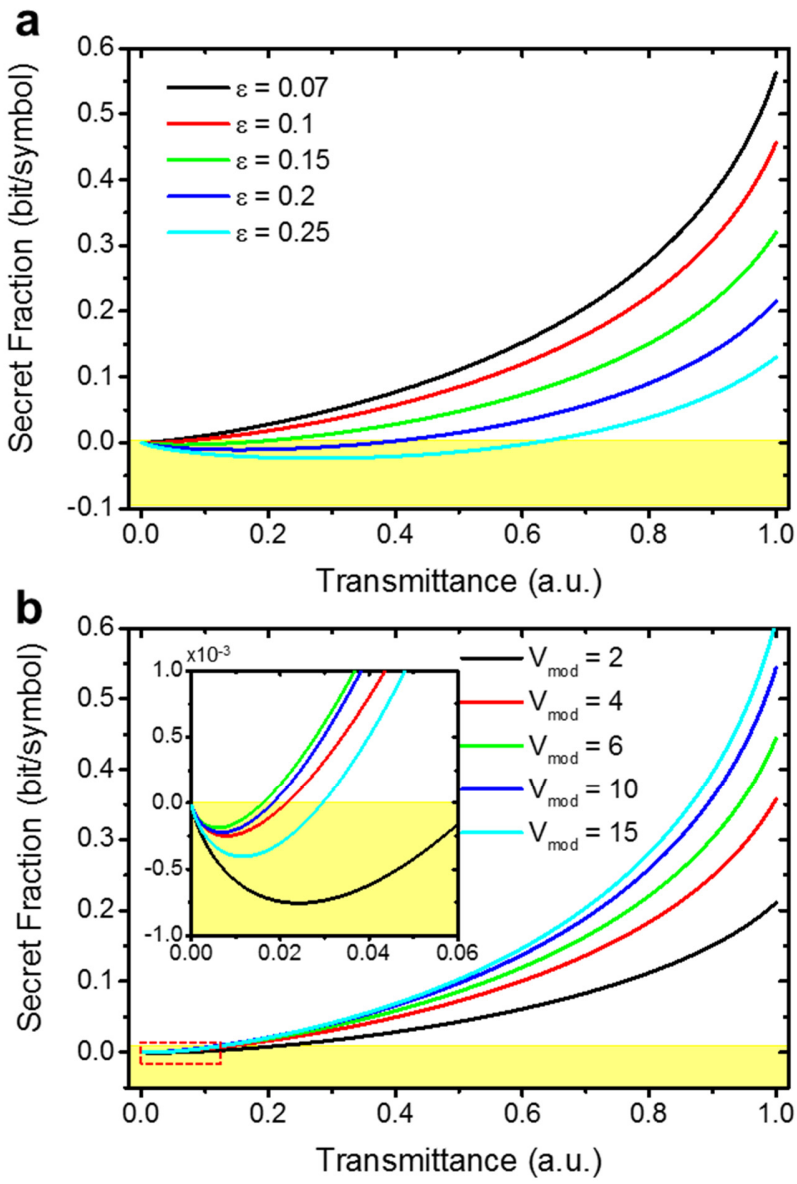

Figure S5 | Secure key rate affect factors. Secure key fraction as a function of transmittance and **a** excess noise **b** modulation variance. The inset is a zoom-in view of the 0 to 0.06 region.

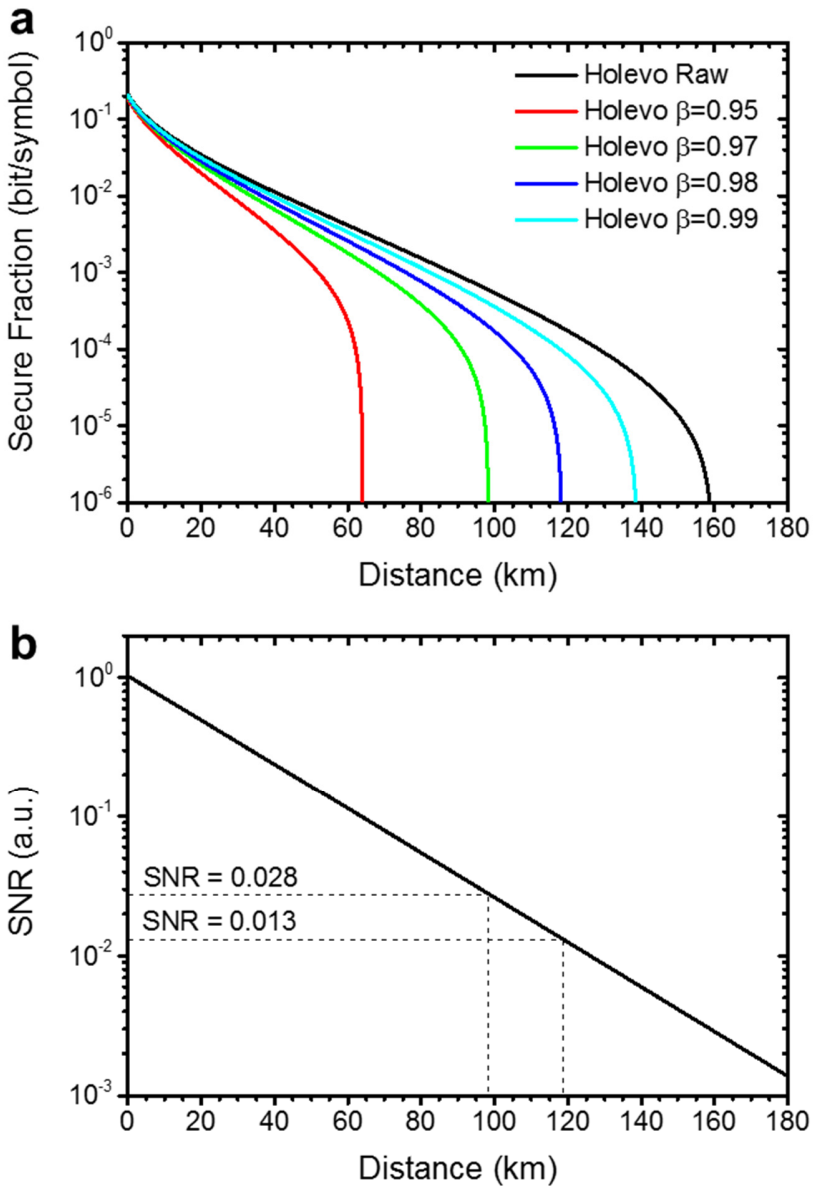

Figure S6 | Reconciliation efficiency and SNR considerations. a The secure fraction as a function of transmission distance. **b** The calculated SNR at different simulated fibre transmission distance.