On-Chip Continuous-Variable Quantum Key Distribution(CV-QKD) and Homodyne Detection

Y. Shen[1,*], L. Cao[2,1,*], X. Y. Wang[1], J. Zou[1], W. Luo[1], Y. X. Wang[1,3], H. Cai[4], B. Dong[5], X. S. Luo[5], W. J. Fan[1†], L. C. Kwek[1,6†], A. Q. Liu[1†]

[1]*Quantum Science & Engineering Centre, Nanyang Technological University, 50 Nanyang Avenue, Singapore 637553, Singapore*
[2]*School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China*
[3]*School of Optoelectronic Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China*
[4]*Institude of Microelectronics, A*STAR, 2 Fusionopolis Way, Singapore 138634, Singapore*
[5]*Advanced Micro Foundry Pte Ltd, 11 Science Park Road, Singapore 117685, Singapore*
[6]*Centre for Quantum Technologies, National University of Singapore,3 Science Drive 2, Singapore 117543, Singapore*
[*]*Y. Shen and L. Cao have equal contribution.*
†Email Address: ewjfan@ntu.edu.sg; cqtklc@nus.edu.sg; eaqliu@ntu.edu.sg

Abstract: An on-chip continuous-variable quantum key distribution(CV-QKD) system is integrated using silicon photonics fabrication process and demonstrates the capability of transceiving Gaussian-modulated coherent states and homodyne detection.

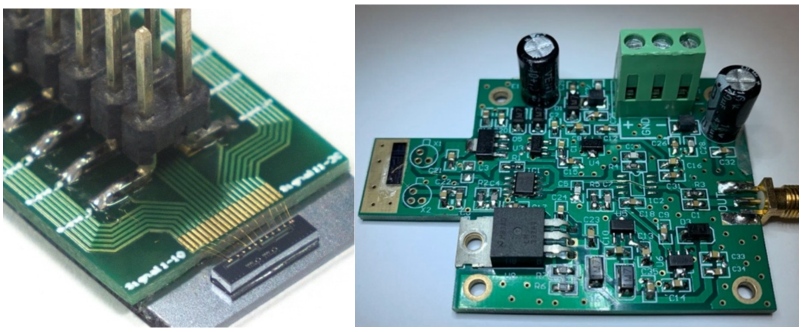
OCIS codes: (270.5568) quantum cryptography; (270.5585) quantum information and processing

Introduction

CV-QKD has been explored as an efficient approach to share secret keys between two parties with high security promised by the law of quantum mechanics[1]. It has been shown that the CV-QKD has the potential advantage for chip integration since successful experimental demonstration of the Gaussian-modulated coherent states (GMCS) protocol[2]. In the protocol, the key information is encoded by Alice in the two quadratures(amplitude and phase) of coherent states which are Gaussian distributed, and subsequently performed shot-noise-limited homodyne detection by Bob[3]. In this paper, an integrated silicon photonic chip for Gaussian-modulated coherent states CV-QKD protocol is designed and tested. This chip-based solution integrates state-of-art components including thermo-optic modulators, carrier injection/depletion modulators, 2D grating fiber-to-chip couplers, 50:50 beam splitters, Germanium photodiodes with high responsivity and a low-noise transimpedance amplifier. A proof-of-principle test is conducted, which shows the secure key rate can reach 0.83 Mbit/s in a 2 m fiber and 2.3 kbit/s at a fiber length of 100 km.

Design and theoretical analysis

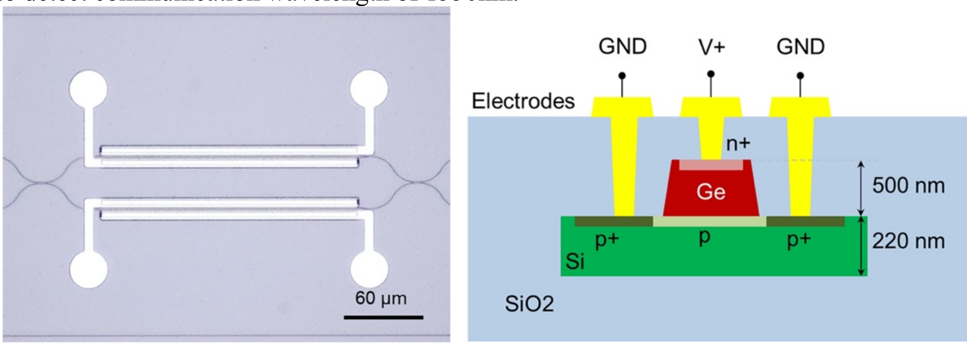
Figure 1 shows the image of the chip packaged to a control PCB and the PCB layout of transimpedance amplifier for receiver chip. 1550-nm wavelength laser is coupled to the transmitter chip via a grating coupler. Then the laser passes a 1:99 beam splitter. The weaker portion is the signal and the stronger portion is the local oscillator. The signal light is randomly modulated to get a Gaussian distribution on both x and p quadrature. The signal and local oscillator are multiplexed in polarization by a 2D grating coupler and transmitted in a single mode fiber. After the transmission fiber, the polarization drift is compensated by a polarization controller and then coupled back to the receiver chip. On receiver chip, the 2D grating coupler demultiplexes the signal and local oscillator. Then another phase modulator is used to randomly select the measured quadrature. Then both signal and local oscillator goes to a balanced homodyne detector. The photocurrents generated in the two photodiodes are subtracted and amplified using a transimpedance amplifier with high sensitivity, ultra-low electrical noise and 10MHz bandwidth. Due to the random Poissonian statistic of photons, the output of the detector will add up the shot noise in the input field while cancelling out classical fluctuations.



(a) (b)

Fig. 1. (a) image of the chip packaged to a control PCB. (b) PCB of transimpedance amplifier for receiver chip

Figure 2(a) shows the fabricated carrier injection amplitude modulator based on MZI structure. The phase modulation is placed on both of the MZI arm to provide a balanced optical path. The structure could be designed as a p-n or p-i-n modulator, only depends on the doping process. The device is capable of operating at the whole C+L band. And with 100 MHz achievable modulation frequency, it is fully capable in our QKD application in 1-10 MHz band. Figure 2(b) shows the cross-section schematic of the Germanium photodiode. The Ge photodiode is designed and fabricated with a vertical p-i-n structure, with 500nm of Ge material epitaxially grown on top of the Si layer. Due to a smaller bandgap energy of Ge compared to Si, the Ge photodiode is ideal for SOI platform and is tuned to detect communication wavelength of 1550nm.



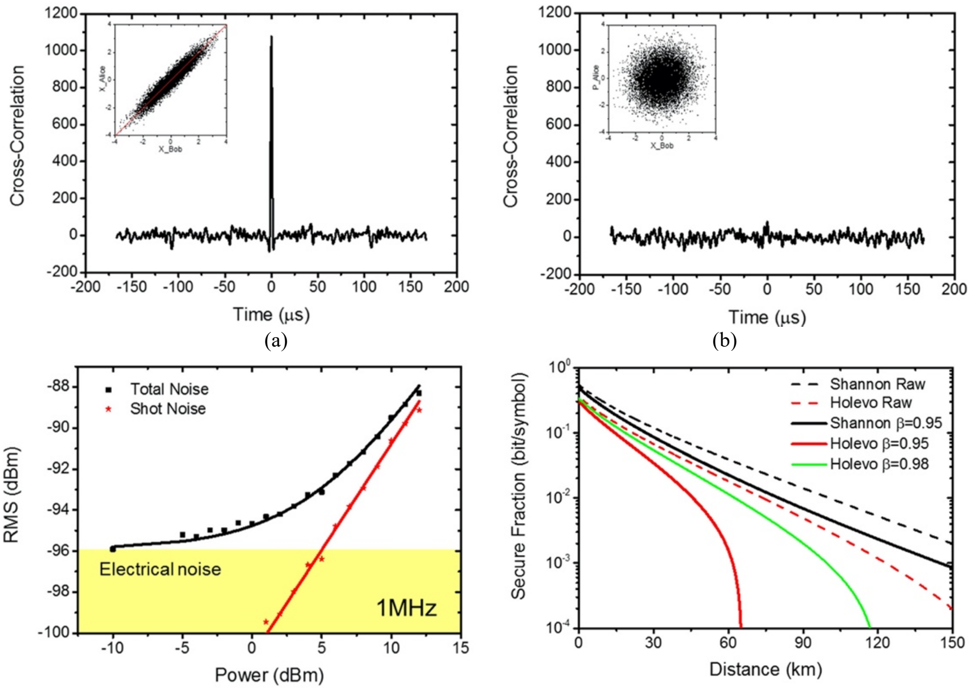
(a) (b)

Fig. 2. (a) microscope image of carrier injection Mach-Zehnder modulator, (b) cross-section of on-chip Germanium photodiode

Results and discussions

A characterization experiment is conducted for transmitting and receiving Gaussian-modulated coherent states and the fidelity of the homodyne detection is evaluated. Figure 3(a) and (b) shows the normalized cross-correlation measurement result between the x quadrature (and the p quadrature) modulation signal and the homodyne detector output while the homodyne detector is fixed to measure the x quadrature. The peak value of the cross-correlation has about 10-times difference. A strong correlation when the measuring quadrature match, while a poor correlation when the measuring quadrature are orthogonal is observed, which indicate the chip is fully capable of quadrature selection.

Figure 3(c) shows the result of homodyne detection, indicating a shot noise level 7 dB above the electronic noise level at 3 MHz modulation, which is adequate for successful extraction of quadrature information. In the experiment, the detector is capable of extinguishing shot noise up to 15 MHz of modulation. In Figure 3(d), with 3 MHz symbol rate, the effective Holevo secure key rate at $\beta = 0.98$ can reach 0.83 Mbits/s at 0 km and 2.3 kbits/s at 100 km fiber length.



(c) (d)

Figure 3. Cross-correlation between homodyne output with (a) corresponding quadrature, (b) different quadrature, (c) shot noise RMS at homodyne detector output as a function of input laser power, (d) the secure key fraction(bits/symbol) with 3MHz symbol rate.

Conclusions

In conclusion, a proof of principle test of CV-QKD on integrated silicon photonic chip is performed. The calculated secure key rate can reach 0.83 Mbit/s in a 2 m fiber and 2.3 kbit/s at a fiber length of 100 km. The balanced homodyne detector achieves a shot noise clearance of 7 dB, the operation range reaches 15 MHz when the power of local oscillator is above 5dBm. Such on-chip system with high performance will push forward the scalability and practical implementation of CV-QKD as an important building block.

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) and National Natural Science Foundation of China (NSFC) joint grant (NRF2017NRF-NSFC002-014).

References

[1] D. Eleni, and A. Leverrier. “Distributing secret keys with quantum continuous variables: principle, security and implementations.” Entropy 17, 6072-6092 (2015).
[2] G. Zhang, J. Y. Haw, H. Cai, et. al, “An integrated silicon photonic chip platform for continuous-variable quantum key distribution.” Nat. Photonics, 10.1038/s41566-019-0504-5 (2019)
[3] C. Weedbrook, S. Pirandola, et. al, “Gaussian quantum information.” Rev. Mod. Phys. 84, 621 (2012).