An integrated photonic chip of measurement-device independent quantum key distribution (MDI-QKD)

Cao, Lin; Luo, Wei; Wang, Yun Xiang; Zou, Jun; Yan, Ru Dai; Cai, Hong; Hu, Xiao Long; Jiang, Cong; Zhou, Xiao Qi; Sun, Shi Hai; Wang, Xiang Bin; Jin, Yu Feng; Kwek, Leong Chuan; Liu, Ai Qun

2020

Cao, L., Luo, W., Wang, Y. X., Zou, J., Yan, R. D., Cai, H., Hu, X. L., Jiang, C., Zhou, X. Q., Sun, S. H., Wang, X. B., Jin, Y. F., Kwek, L. C. & Liu, A. Q. (2020). An integrated photonic chip of measurement-device independent quantum key distribution (MDI-QKD). 2020 Conference on Lasers and Electro-Optics (CLEO).
https://dx.doi.org/10.1364/CLEO_QELS.2020.FF3C.2

<https://hdl.handle.net/10356/151452>

https://doi.org/10.1364/CLEO_QELS.2020.FF3C.2

© 2020 The Author(s). All rights reserved. This paper was published in 2020 Conference on Lasers and Electro-Optics (CLEO) and is made available with permission of The Author(s).

Downloaded on 26 Apr 2023 20:00:34 SGT

An Integrated Photonic Chip of Measurement-Device-Independent Quantum Key Distribution (MDI-QKD)

L. Cao^{1,2*}, W. Luo^{2*}, Y. X. Wang^{2,3*}, J. Zou², R. D. Yan², H. Cai⁴, X. L. Hu⁵, C. Jiang⁵, X. Q. Zhou⁶
S. H. Sun^{7†}, X. B. Wang^{5†}, Y. F. Jin¹, L. C. Kwek^{2,8†} and A. Q. Liu^{2†}

¹School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China

²Quantum Science and Engineering Centre (QSec), Nanyang Technological University, Singapore 639798, Singapore

³School of Optoelectronic Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China

⁴Institute of Microelectronics, A*STAR (Agency for Science, Technology and Research), Singapore 138634, Singapore

⁵State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China

⁶State Key Laboratory of Optoelectronic Materials and Technologies and School of Physics, Sun Yat-sen University, Guangzhou 510275, China

⁷School of Physics and Astronomy, Sun Yat-Sen University, Zhuhai 519082, China

⁸Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore

*These authors contributed equally

†Email Address: shsun@nudan.edu.cn, xbwang@mail.tsinghua.edu.cn, kwekleongchuan@nus.edu.sg and eaqliu@ntu.edu.sg

Abstract: An integrated chip of MDI-QKD system is demonstrated. The system generates a key rate per pulse of 2.923×10^{-6} over a distance corresponding to 50-km optical fibre with 25% detection efficiency. © 2020 The Author(s)

OCIS codes: 270.5565 (Quantum communications), 130.6622 (Subsystem integration and techniques)

Introduction

Quantum key distribution (QKD) offers an unconditional secure method to share secret key between two individuals [1-2]. Among all the QKD protocols currently studied, measurement-device-independent (MDI) QKD is one inherently immune to side-channel attacks targeting the measurement device which can be treated as a black box, or even be operated by eavesdropper [3-4]. However, current MDI-QKD systems use bulky and expensive optical devices, not only limiting the scalability of QKD, but also encountering difficulty in integration with classical fiber-optic communication systems. In this paper, silicon photonic chips for MDI-QKD are designed, fabricated and tested to act as the transmitters and server in a star-shape QKD network. A proof-of-principle demonstration shows the chip-based MDI-QKD system is able to generate a key rate per pulse of 2.923×10^{-6} over a distance corresponding to 50-km optical fibre.

Design and theoretical analysis

Figure 1: (a) Schematic of the chip-based MDI-QKD system comprising two transmitter chips (Alice and Bob) and a receiver chip (Charlie). (b) Packaged chip on a printed circuit board (PCB).

Figure 1 (a) shows the schematic of the chip-based MDI-QKD system, including transmitter chips (Alice and Bob) and a receiver chip (Charlie). In the transmitter chip, a pulse-modulated 1542.3815-nm frequency-locked laser is coupled into the silicon waveguide through a grating coupler. The first Mach-Zehnder interferometer (MZI) modulator modifies the intensity to create signal and decoy states, and another phase modulator implements random modulations of the input pulses. Polarization states of $|H\rangle$, $|V\rangle$, $|+\rangle$ and $|-\rangle$ are encoded by a polarization modulator consisting of an MZI modulator, a path-to-polarization convertor (PPC), and phase shifters at the PPC input arms. Light is coupled out of the chip through an adiabatic tapered waveguide coupler and a lensed fibre. The edge coupler is designed with a cross-section of $200 \text{ nm} \times 220 \text{ nm}$ to minimize the polarization-dependent loss (PDL). After attenuation, the weak coherent pulses from the two transmitter chips reaches the receiver chip (Charlie) via a long-

distance optical fibre. The receiver chip consists of a polarization-independent BS and two PBS. Before entering the receiver chip, the pulses are compensated for polarization drift by polarization controllers in order to maximize the Hong-Ou-Mandel (HOM) interference between the transmitted photons from Alice and Bob chips. Finally, Bell states are measured with single-photon detectors, and all coincidence events for secure key generation are publicly announced. Figure 1 (b) shows the packaged chip on a printed circuit board (PCB).

Results and discussions

Fig. 2: (a) On-chip polarization state preparation. (b) Secure key rates per pulse with different transmission distances.

Figure 2 (a) shows on-chip polarization state preparation. Normalized transmission of the polarization states $|H\rangle$, $|V\rangle$, $|+\rangle$ and $|-\rangle$ is plotted versus voltages applied to the MZI modulator in the polarization modulator. The polarization modulator is capable of providing an extinction ratio over 20 dB. Figure 2 (b) shows secure key rates per pulse with different transmission distances. The black solid line is the theoretical simulation result according to the corresponding experimental conditions using InGaAs/InP single-photon avalanche diodes with a detection efficiency of $\sim 25\%$. The red triangle shows the chip-based MDI-QKD generates a key rate per pulse of 2.923×10^{-6} with a total transmission loss of 10 dB (corresponding to 50-km standard optical fibre). The green dash line and blue dash dot line are simulation results for two different superconducting nanowire single-photon detectors (SNSPD) with a detection efficiency of 53% (SNSPD1) and 85% (SNSPD2), respectively. The results indicate a transmission distance over 120 km for our chip-based MDI-QKD system

Conclusions

An integrated chip of MDI-QKD system is demonstrated for generating polarization-encoded weak coherent states with polarization extinction ratios (PERs) over 20 dB, which is sufficient for low-error MDI-QKD. It is a proof of concept of the silicon photonic chip-based MDI-QKD system that generates a key rate per pulse of 2.923×10^{-6} over a distance corresponding to 50-km optical fibre with 25% detection efficiency, and a predicted distance of 120 km with 85% efficiency. It is a potential application for a fully chip-based MDI-QKD system and hybrid quantum network in the near future.

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).

References

- [1] C. H. Bennett, and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (ed. Goldwasser, S.) 175–179 (IEEE Press, 1984).
- [2] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. 67, 661–663 (1991).
- [3] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. 108, 130503 (2012).
- [4] H. L. Yin, T. Y. Chen, Z. W. Yu, et. al, Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. 117, 190501 (2016).