Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution

Jian-Yu Guan,[1,2] Zhu Cao,[3] Yang Liu,[1,2] Guo-Liang Shen-Tu,[1,2] Jason S. Pelc,[4] M. M. Fejer,[4] Cheng-Zhi Peng,[1,2] Xiongfeng Ma,[3,*] Qiang Zhang,[1,2,†] and Jian-Wei Pan[1,2]

[1]Department of Modern Physics and Nation al Laboratory for Physical Sciences at Microscale, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 23002 6, China

[2]CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

[3]Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China

[4]Edward L. Ginzton Laboratory, Stanford University, Stanford, California 94305, USA

Abstract:

A safety quantum key distribution must take bit error and phase error into account. In common QKD protocols and security analysis, phase error has certain relation with bit error. So there will be a threshold, when bit error exceeds it, no secure key can be distilled. For example, BB84 protocol cannot tolerate bit error more than 11% with the Shor-Preskill security proof [1] [2]. Recently, a novel protocol called round-robin differential phase-shift QKD [3] is proposed. It encodes bit information on phases of L pulses, bounds phase error from other aspects, and thus can tolerate much higher bit error. The theoretical limitation is 50%.

However, the protocol need a variable delay, which can switch between L (here L is a parameter of the protocol) kinds of delays. Realistic delay cannot benefit both low insertion loss and high changing speed. Due to the raw protocol is hard to achieve experimentally, we give a passive version which is friendly to experiment and easy to adjust and optimize the L. In our protocol, variable delay is replaced by two-photon interference, the position of two clicks will give an equivalent delay L. So a simple beam splitter and a local reference beam can achieve the passive variable delay.

We also do experiment to principally demonstrate the passive protocol. Without phase-locking, the bit error exceeds 25%, however, optimizing some parameters can bound the phase error to a very low level, thus secure keys can still be distilled. That is, our passive protocol can experimentally tolerate such a high bit error. We finally get a key rate more than 50bps in 53km distance, with bit error 31.2%, while no QKD protocols before can tolerate such a high bit error.

In the future, with application of phase-locking technology, we can remove the 25% base error, and dramatically improve the final key rate.

Reference:

[1] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (200

[2] H.-K. Lo and H. F. Chau, Science 283, 2050 (1999) .

[3] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature (London) 509, 475 (2014)