Energy-Time Entanglement Based Dispersive Optics Quantum Key Distribution over Optical Fibers of 20 km

Xu Liu[1,2], Xin Yao[1,2], Heqing Wang[3], Hao Li[3], Lixing You[3], and Yidong Huang[1,2] , Wei Zhang[1,2, *]

[1]*Beijing National Research Center for Information Science and Technology (BNRist), Beijing Innovation Center for Future Chips, Electronic Engineering Department, Tsinghua University, Beijing 100084, China*

[2]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*

[3]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*

** zwei@tsinghua.edu.cn*

Abstract: An energy-time entanglement based dispersive-optics quantum key distribution is demonstrated experimentally over 20 km optical fibers, in which photon pairs are generated by spontaneous four wave mixing in a silicon waveguide.

OCIS codes: (270.5565) Quantum communication, (270.5585) Quantum information and processing

1. Introduction

Dispersive optics QKD (DO-QKD) protocol attracts much attention recently. By introducing normal and anomalous dispersion components at Alice and Bob side, security test can be realized by measurements of unbiased time-frequency bases, which has been proved to be secure against collective attacks [1]. From the point of implementation, DO-QKD can be realized in either prepare-and-measurement (P&M) [2] or entanglement-based way [3]. The P&M version of DO-QKD protocols have been demonstrated by field experiments with high key rate of 1.2 Mbps over optical fibers of 43km [2]. On the other hand, the entanglement-based way has inherent random local results and correlated outcomes. If swapped with high fidelity at quantum repeater nodes, photonic entanglement could be extended over long distances, possibly to a global. However, entanglement-based DO-QKD was only demonstrated by short fiber links and the key rates were relatively low [3]. In this work, we experimentally realized the entanglement-based DO-QKD over optical single mode fibers (SMFs) of 20 km. Energy-time entangled photon pairs were used in this experiment, which were generated by a SFWM quantum light source based on a silicon waveguide. The keys were generated by high dimensional time encoding. The bin sifting process was optimized by a three level structure, which significantly reduced the raw bit error rate (BER) due to timing jitters of detectors and electronics. A raw key generation rate of nearly 120kbps was achieved, with a low BER of 0.5%.

2. The Experiment and Results

The experimental setup is shown in Fig. 1(a). Energy-time entangled photon pairs are generated through SFWM in a piece of silicon waveguide. The idler photons of entangled photons are sent to Bob via SMFs of 20 km. A dispersive compensation module (DCM) is utilized to compensate the chromatic dispersion introduced by the SMFs. At each side, a 50:50 fiber coupler routes photons into two paths randomly. In one path, photons are detected directly, which corresponds to the time basis, and the arrival times are mainly used for key generation. In the other path, photons are detected after a normal dispersion (ND) or anomalous dispersion (AD) module (±1800 ps/nm), which corresponds to the frequency basis. The recorded single photon events under frequency basis and a part of events under time basis are utilized for joint measurement of time-frequency covariance matrix to bound Eve's Holevo information, which is responsible for the security test. Four NbN superconducting nanowire single-photon detectors (SNSPDs, provided by SIMIT, CAS, China) were used in this experiment. Their detection efficiencies ~50% at 1550nm, with dark-count rates of 100 counts per second and average timing jitters of 80ps full width at half maximum (FWHM). Single photon events were precisely recorded by time-to-digital converters (TDC, PicoQuant HydraHarp 400) at a 1 ps resolution and sent to computers for data processing.

The results of photon coincidences between Alice and Bob are shown in Fig. 2, under four basis combinations at Alice and Bob sides. Eve's attack on the time information would broaden the correlations shown in Fig. 2(d). Based on the time events measured by time bases and frequency bases, joint measurement of time-frequency covariance matrix (TFCM) is calculated and evaluated to bound Eve's Holevo information for the security test.

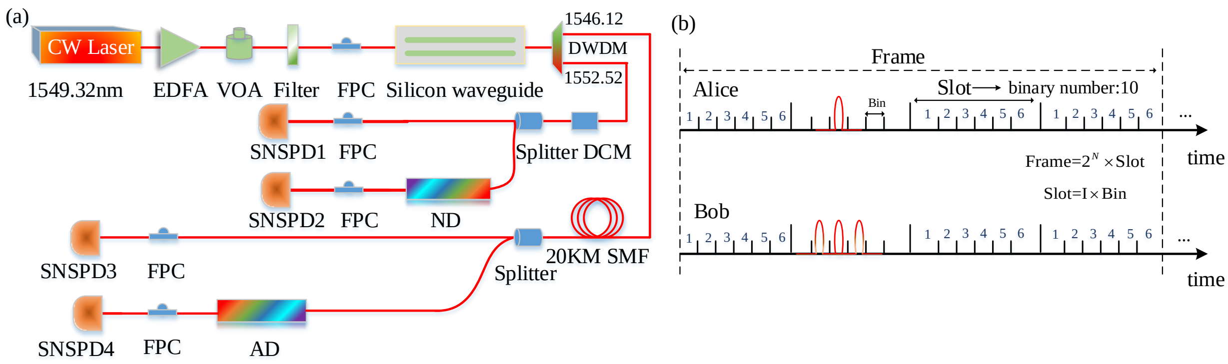

Fig. 1. (a) Schematic of entanglement-based DO-QKD setup; (b) Example of bin sifting method.

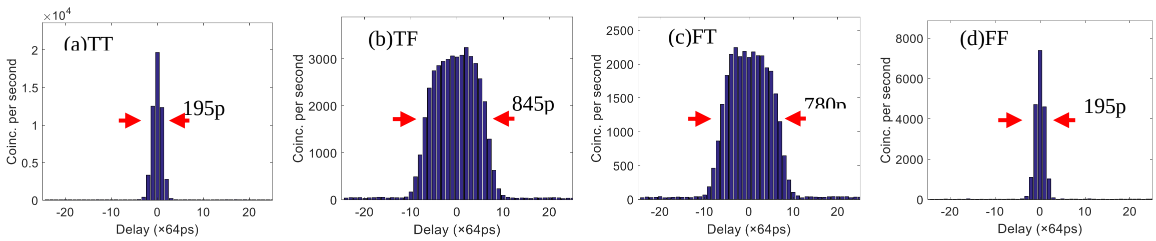

Fig.2 Photon coincidences between Alice and Bob under four basis combinations. T represents the time base; F represents the frequency base.

Alice and Bob built their distilled keys from correlated events acquired both in the time basis. In order to acquire high key generation rate, we sliced the single photon events in large alphabet way to get more information from each coincidence. Fig.1(b) shows the sketch of the bin sifting process, which has three levels. The bin sifting process was optimized under different bin width and division number. As a result, a raw key rate of 120kbps with BER of 0.5% was achieved under bin=65ps, I=9, and N=4.11. After further post processing for error correction and private amplification, the final secret key rate is about 100kbps.

3. Conclusion

In this work, we experimentally demonstrated the energy-time entanglement based DO-QKD over optical fibers of 20km, in which the energy-time entangled photon pairs were generated by SFWM in a piece of silicon waveguide. The bin sifting process was optimized by a three level structure, as a result, the BER was significantly reduced to about 0.5% under a raw key rate of ~120kbps. The whole system is secured by nonlocal dispersion cancellation based on dispersive optics.

4. Acknowledgments

This work was supported by the National Key R&D Program of China under Contract No. 2017YFA0303704 and No. 2017YFA0304000; the National Natural Science Foundation of China under Contract No. 61575102, No. 91750206 and No. 61621064; Tsinghua National Laboratory for Information Science and Technology.

5. References

[1] Mower, J., Z. Zhang, P. Desjardins, et al., “High-dimensional quantum key distribution using dispersive optics,” Physical Review A **87**, 062322 (2013).

[2] Lee. C., Darius. B., Z. Zhang, et al., “High-rate field demonstration of large-alphabet quantum key distribution,” arXiv (2016).

[3] Lee, C., Z. Zhang, G.R. Steinbrecher, et al., “Entanglement-based quantum communication secured by nonlocal dispersion cancellation,” Physical Review A **90**, 062331 (2014).