Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction

Ying Guo,[1, 2] Qin Liao,[1, *] Yijun Wang,[1] Duan Huang,[3, †] Peng Huang,[3] and Guihua Zeng[3]

[1] *School of Information Science & Engineering, Central South University, Changsha 410083, China*
[2] *School of Physics Science and Information Engineering,*
Hunan Normal University, Changsha 410003, China
[3] *State Key Laboratory of Advanced Optical Communication Systems and Networks,*
and Center of Quantum Information Sensing and Processing,
Shanghai Jiao Tong University, Shanghai 200240, China

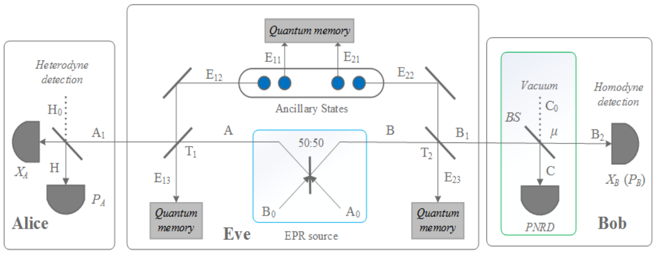

FIG. 1. The non-Gaussian operation in the ESIM-based EB CVQKD. Alice detects one half of EPR state using heterodyne detection while Bob uses homodyne detection to measure another half.

A suitable photon-subtraction operation can be exploited to improve the maximal transmission of continuous-variable quantum key distribution (CVQKD) in point-to-point quantum communication [1, 2]. Unfortunately, photon-subtraction operation faces up to solving the improvement transmission problem of the practical quantum networks, where the entangled source locates in the third part who may be controlled by the malicious eavesdropper instead of in one of the trusted parts, Alice or Bob [3].

In this paper, we show that a solution can come from usage of a non-Gaussian operation, in particular, the photon subtraction operation, which provides a method to enhance the performance of entanglement-based (EB) CVQKD. Photon-subtraction not only can lengthen the maximal transmission distance by increasing the signal-to-noise rate, but also can be easily implemented under existing technologies. As shown in Fig. (1), a source of the two-mode squeezed vacuum state [Einstein-Podolsky-Rosen (EPR) state] is used to create a secure key. Usually, it can be generated by the sender, Alice, or by a third party, say, Charlie, whose security is trustworthy. However, from an eavesdropping point of view, it is necessary to assume that Eve could have controlled the entangled source and could have prepared the arbitrary state. Based on this assumption, we introduce the photon subtraction operation to enhance the performance of entangled-source-in-middle (ESIM)-based CVQKD.

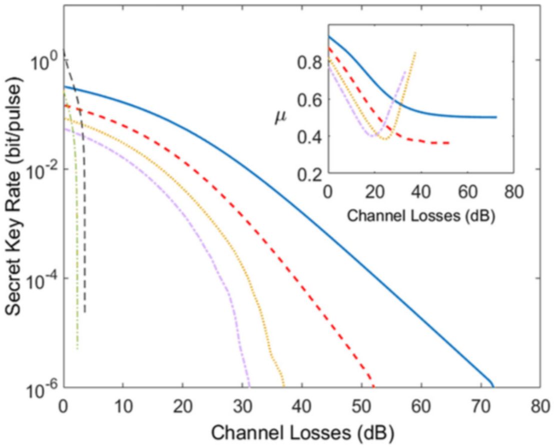

FIG. 2. The secret key rates of the ESIM-based CVQKD as a function of channel loss.

Fig. (2) shows the one of the best performance of our proposed scheme, which can well increase the secure transmission distance in both direct and reverse reconciliation of the EB-CVQKD scheme, even if the entangled source originates from an untrusted part. Moreover, it can defend the inner source attack, which is a specific attack by an untrusted entangled source in the framework of ESIM.

Detailed research can be found in [4].

[1] Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, and H. Guo, Phys. Rev. A **93**, 012310 (2016).

[2] P. Huang, G. He, J. Fang, and G. Zeng, Phys. Rev. A **87**, 012317 (2013).

[3] C. Weedbrook, Phys. Rev. A **87**, 022308 (2013).

[4] Y. Guo, Q. Liao, Y. Wang, D. Huang, P. Huang, and G. Zeng, Physical Review A **95** (2017).

[*] llqqlq@csu.edu.cn

[†] duan.huang@foxmail.com