Asynchronous continuous-variable quantum key distribution against practical attacks

Peng Huang,[1,*] Tao Wang,[1] and Guihua Zeng[1,†]

[1] *Center of Quantum Sensing and Information Processing (QSIP), State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiao Tong University, Shanghai 200240, China*

We develop here an asynchronous countermeasure strategy against the practical attack in continuous-variable quantum key distribution (CVQKD) without structural modifications. In particular, two countermeasures are proposed by adding peak-valley seeking and Gaussian postselection steps in conventional data postprocessing procedure. The analysis shows that the peak-valley seeking method naturally makes the schemes immune to all known types of calibration attacks even when Eve simultaneously performing wavelength or LO fluctuation attacks and exhibits simpler implementation and better performance than the known countermeasures. Meanwhile, the proposed schemes are secure against all known types of practical attacks.

Recently, several practical attacks on continuous-variable quantum key distribution (CVQKD) are proposed based on faking the estimated value of channel excess noise to hide the intercept-and-resend eavesdropping strategy, including the local oscillator (LO) fluctuation, calibration, wavelength and saturation attacks. However, the known countermeasures against all these practical attacks will inevitably increase the complexity of the implementation of CVQKD and lead to attenuation of the signal and thus reduction of secret key rate.

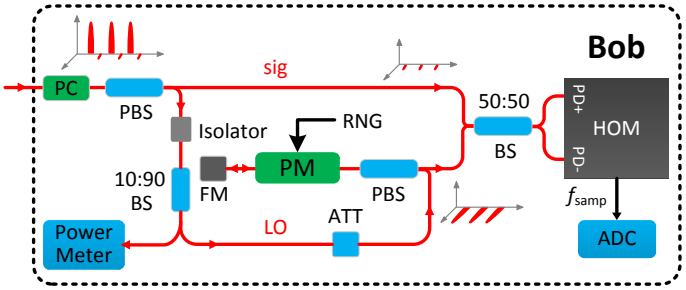

FIG. 1. Countermeasure against practical attacks with power meter based on peak-valley seeking and Gaussian postselection.

We develop here a countermeasure strategy relying on the improvement of data postprocessing procedure without any structural modification of conventional Gaussian-modulated coherent-state (GMCS) CVQKD scheme [1]. In particular, two practical countermeasures are proposed by adding the peak-valley seeking and Gaussian postselection steps in conventional data postprocessing procedure. The structure of the first countermeasure is same as the conventional GMCS CVQKD scheme in [1], which is depicted in Fig.1. Bob oversamples the analog pulse with an asynchronous clock and picks the solitary peak or valley points with the largest absolute values in every period of the analog pulses with sorting algorithm. These data will be then processed by discarding the uncorrected one to form the sifted key data and further processed by Gaussian postselection to resist the saturation attacks [2]. Noted here the trigger clock regeneration part in Bob's side is unnecessary, and the estimated shot noise can always match with the one in the output result of homodyne detection. So all the time-shift calibration and saturation attacks are invalid. The secret key rate of the proposed countermeasure under collective attack will be higher than the known countermeasures [3, 4] (see [5] for details).

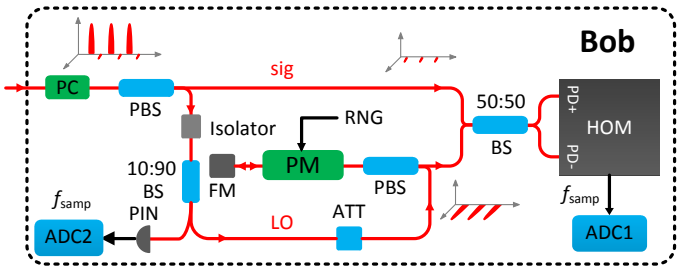

FIG. 2. Countermeasure against practical attacks with dual-sampling measurement based on peak-valley seeking and Gaussian postselection.

Actually, the finite sampling bandwidth effects will lead to LO calibration attacks, since the shot noise is overestimated and then deduces incorrect estimations of transmission efficiency and excess noise. So we develop another countermeasure based on dual-sampling method in Fig.2, which can be used in peak-valley seeking step to further resist this LO calibration attacks arising from the finite bandwidth effects (see [5] for details).

[1] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).
[2] H. Qin, R. Kumar, and R. Alléaume, Phys. Rev. A **94**, 012325 (2016).
[3] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).
[4] J. Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z. Q. Yin, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Phys. Rev. A **89**, 032304 (2014).
[5] P. Huang, J. Huang, T. Wang, H. Li, D. Huang, and G. Zeng, Phys. Rev. A **95**, 052302 (2017).

* huang.peng@sjtu.edu.cn

† ghzeng@sjtu.edu.cn