Practical Security of Continuous-Variable Quantum Key Distribution with Imperfect Random Basis-Choice Operations

Weiqi Liu,[1, 2] Yingming Zhou,[2] Jinye Peng,[1] Peng Huang,[2, *] and Guihua Zeng[2, 1, †]

[1] *College of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, China*
[2] *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

Generally, continuous-variable quantum key distribution (CVQKD) schemes need random basis-choice operations with homodyne detector to measure one of two quadratures, i.e., position and momentum quadratures. However, we find that the basis-choice oprations may become imperfect in practical applications due to the imperfections of the digital to analog convertor and the phase modulator. This imperfection will decrease the lower bound of secret key rate and leave security loopholes when the legitimate communicators do not aware the imperfection. Here we analyze the security of CVQKD system induced by the imperfection of the basis-choice operations and suggest possible countermeasures.

Continuous-variable quantum key distribution enables Alice and Bob to share a secret key, which allows them to communicate with full security[1]. One of the most favourable CVQKD protocols is the Gaussian-modulated coherent state (GMCS) protocol[2]. In the GMCS CVQKD schemes, bases choice are the necessary procedure[3], in which Bob randomly modulates 0 or $\frac{\pi}{2}$ on the phase modulator to measure either quadrature of the received quantum state with the homodyne detector. However, in practical system, because of the imperfections of the digital to analog convertor and the phase modulator, the real phase values applied to the system θ' may be not equal to the expected phase values θ (0 or $\frac{\pi}{2}$) of the bases choice, which will introduce the imperfections to the basis-choice operations.

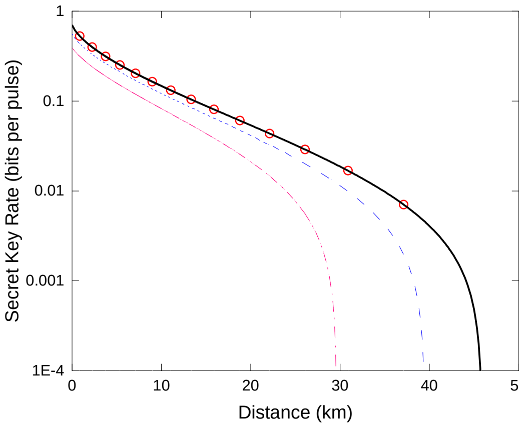

FIG. 1. The secret key rate as a function of the transmission distance for different degrees of imperfection of basis-choice operations (perfect bases choice corresponds to $\kappa = 1$). The curves from right to the left represent the secret key rate for $\kappa = 1.0$, 0.999, and 0.997, respectively. The red marked curve represents the effect of eliminating the imperfections of the basis-choice operations by our phase compensation algorithm.

We find that the imperfect basis-choice operations will increase the excess noise and decrease the secret key rate of the CVQKD system. To demonstrate the effects, we plot the secret key rates of the system under collective attacks with finite-size effect in Fig.1. The degree of imperfection of basis-choice operations is weighted by the parameter $\kappa = (E[\cos\delta\theta])^2$, where E denotes the expectation and $\delta\theta = |\theta' - \theta|$. Moreover, when Alice and Bob do not aware the imperfection, they will directly mislead the estimation of channel excess noise. Then they fail to fully discard the information obtained by Eve and will induce a loophole to the involved CVQKD system.

Actually, the imperfection induced by the random basis choice operation is equivalent to adding a random small phase shift in the CVQKD system. To resist this imperfection, a phase compensation algorithm may be effective, in which the variation of the phase shifts should be less than the inaccuracy of the algorithm. We test our phase compensation algorithm [4] in practice, the precision can reach 0.1° per frame, which represents $\kappa \doteq 1$ nearly corresponding to the perfect bases choice. Recently, we further suppress the phase error to 0.01° per frame[5]. Thus our algorithm can well meet the requirement of eliminating the imperfections of the bases choice. In addition, we propose an alternative CVQKD scheme using continuous random bases choice[6], in which Bob randomly measures the quadratures depending on a continuous random phase θ (from 0 to 2π). It is also helpful for resisting this imperfection and meanwhile decrease the complexity of implementations.

[1] C. Weedbrook, *et al.* Rev. Mod. Phys. 84, 621 (2012).

[2] F. Grosshans, and P. Grangier, Phys. Rev. Lett. 88, 057902 (2002).

[3] F. Grosshans, G. Van Assche, J. Wenger, *et al.* Nature 501, 238-241 (2003).

[4] D. Huang, P. Huang, D. Lin, *et al.* Sci. Rep. 6, 19201 (2016).

[5] Y. Zhou, W. Liu, T. Wang, *et al.* (submitted to the Qcrypt 2017).

[6] W. Liu, J. Peng, P. Huang, *et al.* Opt. Express (under review).

[*] huang.peng@sjtu.edu.cn
[†] ghzeng@sjtu.edu.cn