Practical security of a chip-based continuous-variable quantum key distribution system

Lang Li, Peng Huang,* Tao Wang, and Guihua Zeng†
Center for Quantum Sensing and Information Processing,
State Key Laboratory of Advanced Optical Communication Systems and Networks,
Shanghai Jiao Tong University, Shanghai 200240,
People's Republic of China and Shanghai Research Center for Quantum Sciences,
Shanghai 201315, People's Republic of China

A chip-based continous-variable quantum-key-distribution (CVQKD) system with a high practical confidentiality performance is crucial for constructing quantum metropolitan communication networks, but imperfections in the chip-based modulation will threaten the practical security of the chip-based CVQKD system. In this paper, we combine the plasma dispersion effect of free carriers to model the carrier fluctuations and reveal the essential mechanism of carrier fluctuations' influence on the system. The simulations show that the chip-based CVQKD system may face potential loophole threats or its performance will dramatically decrease under different carrier fluctuations.Moreover, two preliminary defense strategies are proposed to completely solve the practical security problems commonly induced by modulators in general chip-based CVQKD systems. This work proposes a set of modeling and analysis methods for general chip-based CVQKD systems' modulators, which provides constructive methods to build the chip-based CVQKD system with more rigorous practical security.

Recently, the continuous-variable quantum key distribution based on the Gaussian modulation coherent state protocol has been initially verified on a silicon-based chip platform[1]. In recent years, research on the imperfections that may be used by a third-party attacker Eve has been widely studied, such as the local oscillator(LO) fluctuation, calibration, wavelength and saturation attacks,etc. Unfortunately, there has not been any research on the practical security of the chip-based CVQKD system.

The practical security of the chip-based CVQKD system may be affected, since the imperfections of silicon-based MZI modulator such as the imperfect Gaussian property of the modulation voltage, the difference of carrier concentration diffusion performance of the modulator,etc. We creatively combine the plasma dispersion effect of free carriers to model the carrier fluctuations and reveal the essential mechanism of the carrier fluctuations. The simulations verify that the chip-based CVQKD system will face potential loophole threats under positive fluctuations of the practical concentration changes of carriers(see FIG.1 for details) or its performance will dramatically decrease under negative one.

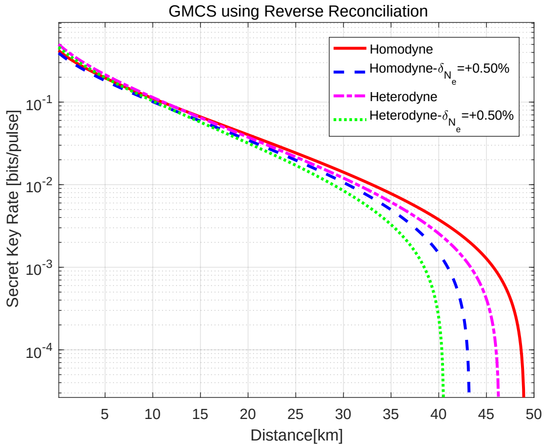

FIG. 1. Estimated and practical secret key rate(bits/pulse) vs Distance(km) with a carrier fluctuation $\delta_{N_e} = +0.50\%$ under the asymptotic condition of infinite sampling. i.e. estimated one under BHD(solid line), practical one under BHD(dashed line), estimated one under balanced heterodyne detector(dashdotted line), and practical one under balanced heterodyne detector(dotted line).

We proposed defense method called the maximum carrier fluction deviation method without changing the system structure. Additionally, dynamic random carrier fluctuaion calibration defense method based on deep neural network is proposed to accurately estimate δ_{N_e} and further adjust the modulation voltage through an adaptive feedback system to achieve perfect Gaussian modulation(see [2] for details).

[1] Zhang, G, et al. Nat. Photonics **13**, 839 (2019).

[2] L.Li, et al. Phys. Rev. A **103**, 032611 (2021).

* huang.peng@sjtu.edu.cn

† ghzeng@sjtu.edu.cn