The Improvement of Security for Continuous-Variable Quantum Key Distribution with Imperfect Phase Modulation

Zhengwen Cao[1]*, Chenhao Zhang[1], Geng Chai[1]

◆Background

The Phase Modulator (PM) is a piece of the necessary equipment in the practical application1 of continuous variable quantum key distribution (CVQKD) system. However, in the actual experiment, the phase modulators may receive some interference resulting a drift in the modulation voltage leads to the phase modulation errors.

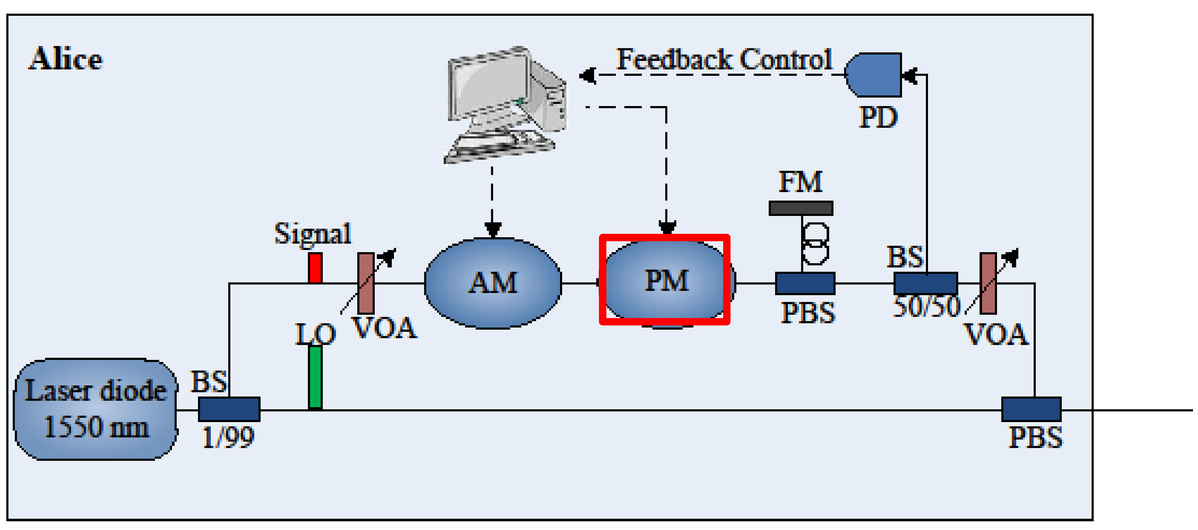

FIG. 1 The experimental setup of the CVQKD system at Alice's side.

◆Objective

We study the security of the CVQKD system with imperfect PM and research the differences of CVQKD system security under different noise models and find a method to contain the modulation noise in CVQKD system.

◆Content

Based on the EB model, we use the ideal parameters and real parameters to calculate the influence of phase modulation errors on the security of the system, and We analyze the secret key rate and the secure distance with imperfect PM in two noise module. Moreover, we show the influence of this imperfect device on the performance of the system and propose a method to contain the modulation noise in CVQKD system.

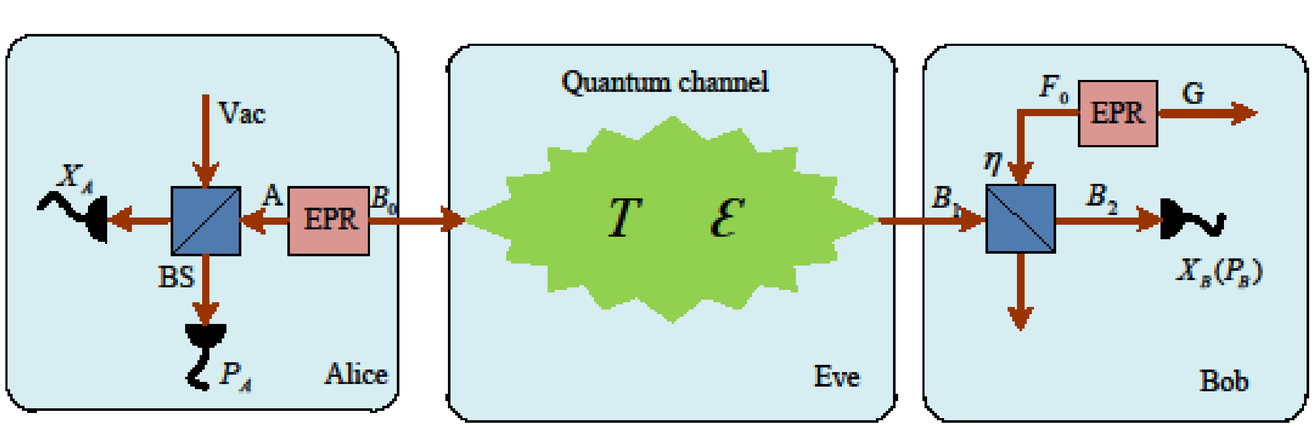

FIG. 2 EB model of CVQKD using homodyne detector.

◆Conclusion

We use two different noise models to simulate the secret key rate and the secure distance with imperfect PM. Obviously, the system security will be affected by phase noise. And we find the deviations will become greater with the increase of the phase noise. More importantly, we find the results of the two models are quite different. Alice and Bob may misestimate the security of the system by choosing channel noise module.

We also analyse the relation in two models between the secret key rate and the variance of the modulation noise. Under different transmission distances, the tolerance of the modulation noise module to the modulated noise is obviously higher than that of the channel noise module. In other words, the channel noise model overestimates the attacker's ability.

We propose a method to contain the modulation noise in CVQKD system. we can determined the drift of the phase modulator only by using raw signal data.We can use this method to solve this phase drift problem instead of using the phase compensation method.

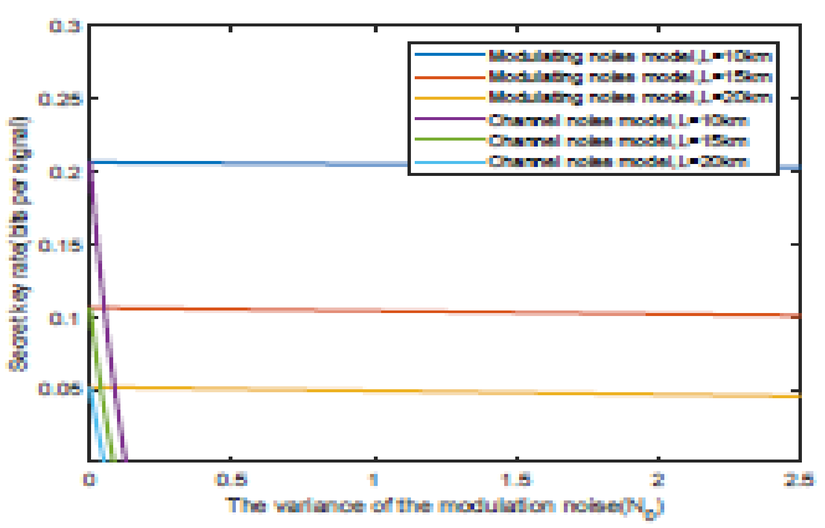

FIG. 3 The secret key rate and the variance of modulation noise with imperfect PM. (Va = 19,η = 0.6025, β = 0.89, vel=0.0423 , ε = 0.02,L represent the transmission distances.)

1. School of Information Science and Technology, Northwest University, Xi'an, 710127, China.

caozhw@nwu.edu.cn