Improvement of No-Switching Continuous-Variable Quantum Key Distribution System by Using a Practical Noiseless Linear Amplifier

Yi-Chen Zhang, Song Yu, Wanyi Gu*

State Key Laboratory of Information Photonics and Optical Communications,
Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: yusong@bupt.edu.cn.

Abstract

We propose a practical modified no-switching continuous-variable quantum key distribution system to improve the secret key rate over long transmission distance by inserting a practical noiseless linear amplifier at the output of quantum channel.

1. Introduction

Quantum key distribution (QKD) [1] is one of the most practical applications in the field of quantum information and is able to establish a secure key between two legitimate partners (usually called Alice and Bob). Continuous-variable quantum key distribution (CV-QKD) [2] has attracted much attention in the past few years [1–3] mainly because it uses only requires off-the-shelf standard telecom components.

The first CV-QKD protocol based on the Gaussian modulation of coherent states and homodyne detection was proposed in 2002 [4]. Shortly afterward, another coherent state protocol was proposed, known as no-switching protocol, where homodyne detection is replaced by heterodyne detection [5]. This enables the honest parties to exploit both quadratures in the distribution of the secret key [2]. However, the practical application of no-switching CV-QKD protocol is limited to much shorter distance and less key rates. The main reason is that the reconciliation efficiency of correlated Gaussian variables is quite low, especially when the transmission distance is very long.

To improve the secret key rate and maximal transmission distance of practical no-switching CV-QKD system, in this paper, we consider putting a heralded noiseless linear amplifier (NLA) at the output of quantum channel. Previously this had only been analyzed for the case of switching schemes [6]. The modified system with a practical NLA of gain g can increase the maximum transmission distance by $100\log_{10}g$ km. Furthermore, a critical point is given to separate the enhanced and degenerative region of the modified system, which will be useful and instructive for the usage of practical NLA to achieve the optimal performance in a practical scenario.

2. Modified No-Switching CV-QKD System by Using a Practical NLA

In this section, we firstly describe the prepare-and-measure (PM) and entanglement-based (EB) version of the modified-switching protocol. Then, the secure bound of the protocol under collective attack is given in detail. Finally, we provide the results of simulations to compare the performances of the protocol with or without a practical NLA.

2.1 The PM and EB description of the modified protocol

In the PM version of the modified system (see Fig. 1 (a)), Alice generates two Gaussian random real number (a_x, a_p) from independent distribution of variance V_A ($V_A = V - 1$). Alice first sends a coherent state centered in (a_x, a_p) to Bob and Bob uses a practical NLA to amplifier the state he receives. As illustrated in Fig. 1, the imperfections of a NLA contain detection inefficiency η_D and heralded single photon source (HSPS) [7]. Bob then measures both x and p. After Bob has received all the pulses, the two partners proceed with the post-processing which consists of sifting, reverse reconciliation and privacy amplification.

The PM version of the modified system can be reformulated in EB version (see Fig. 1 (b)). Alice initially prepares an EPR pair (EPR with variance V), measures one mode A_1 with heterodyne detection and sends the other mode A_2 to Bob through the channel. Then Bob uses a practical NLA to amplifier the mode he receives and measures both x and p. Although the EB version does not correspond to the actual implementation, it is fully equivalent to the PM

978-1-4673-5225-3/14/$31.00 ©2014 IEEE

version from the secure point of view, and it provides a powerful description of establishing security proof [4, 8].

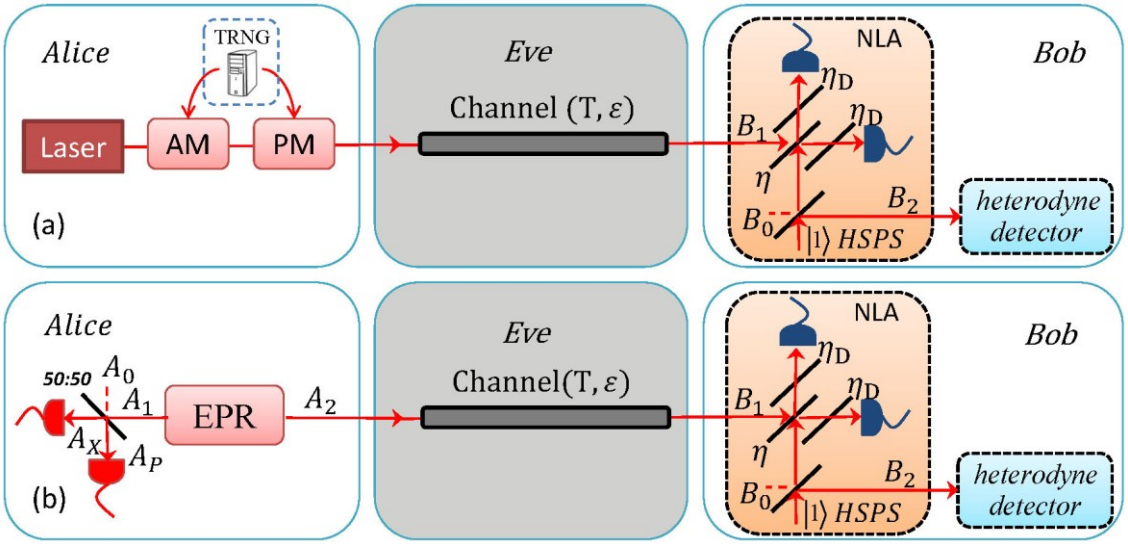

Fig. 1: (a) Prepare-and-measure scheme of the modified no-switching CV-QKD system with a practical noiseless linear amplifier (NLA). The practical realization of the NLA needs a heralded single photon source (HSPS), which is split by an asymmetric beam splitter ($\eta < 0.5$) [7]. The red and blue detectors represent homodyne and single photon detection respectively. (b) The equivalent entanglement-based scheme of the modified system.

2.2 Secure bound of the modified protocol

A practical NLA can in principle probabilistic amplify the amplitude of a coherent state while retaining the initial level of the noise [6, 7]. The successful amplification can be described by an operator $\hat{C}=g^{\hat{n}}$, where $\hat{n}$ is the number operator and g is the gain of a NLA. When a NLA succeeds amplifying a coherent state [6]

$$\hat{C}|\alpha\rangle = g^{\hat{n}}|\alpha\rangle = e^{\frac{|\alpha|^2}{2}\left(g^2-1\right)}|g\alpha\rangle \tag{1}$$

The inefficient detector can be modeled by a beam splitter with transmittance η_D combined with a perfect detector (see Fig. 1). Furthermore, the trigger probability $P_{trigger}$ of HSPS will reduce the total successful probability of NLA. To increase the trigger probability $P_{trigger}$, one can use a non-degenerated PDC source to produce the HSPS, which is $\Sigma_{n=0}^{\infty} x^n/(1+x)^{n+1}|n\rangle|n\rangle$, where x and η_T are the intensity and the detection efficiency of the heralding signal. The total successful probability of the practical NLA is $P_{success}^{total} = P_{success}^{efficiency}(\eta_D) \cdot P_{trigger}$, where the successful probability of the NLA and the corresponding trigger probability are [7]

$$\begin{cases} P_{success}^{efficiency}(\eta_D) = e^{-\eta\mu}\eta_D\left[\eta + \mu\left(1-\eta\eta_D\right)\right] \\ P_{trigger} = \sum_{n=0}^{\infty}\frac{x^n}{(1+x)^{n+1}}\left[1-\left(1-\eta_T\right)^n\right] = 1-\frac{1}{1+\eta_T x} \end{cases} \tag{2}$$

where μ and η represent the intensity of the input state into NLA and the transmittance of the beam splitter.

We now derive security bound of the modified direct reconciliation CV-QKD protocol. When Alice and Bob use reverse reconciliation, the secret key rate is given by

$$K = P_{success}^{total} \cdot \left[\beta I(a:b) - S(b:E)\right] \tag{3}$$

where $\beta \in [0,1]$ is the reconciliation efficiency, $I(a:b)$ is the classical mutual information between Alice and Bob $I(a:b)=0.5\log V_{Ax}-0.5\log V_{Ax|Bx}$ and $S(b:E)$ is the quantum mutual information between Bob and Eve $S(b:E)=S(\rho_E)-\iint p(x_{Bx})p(p_{Bp})S(\rho_E^{xBx,PBp})dx_{Bx}dx_{Bp} \leq x_{BE}$ [8], where $V_{Ax}=0.5(V_A+1)$, $V_{Ax|Bx}$ is the variance of mode A_x conditioned on Bob's data, $p(xB_x)$ is the probability density function of the measurement output and $S(\rho)$ is the von Neumann entropy of the quantum state ρ [8].

2.3 Numerical simulation and discussion

In the following, the performance of the modified system is compared with the original one. The parameters that will affect the secret key rate and transmission distance are the reconciliation efficiency β = 0.948, the variance of Alice's modulation V_A-1, the transmission efficiency T ,excess noise ε = 0.15 and successful probability of a NLA $P_{success}^{total}$, the intensity and the detection efficiency of the heralding signal $\eta_T = x$ = 0.1, which are standard in one-way CV-QKD experiments and practical NLA experiments [3, 6, 7].

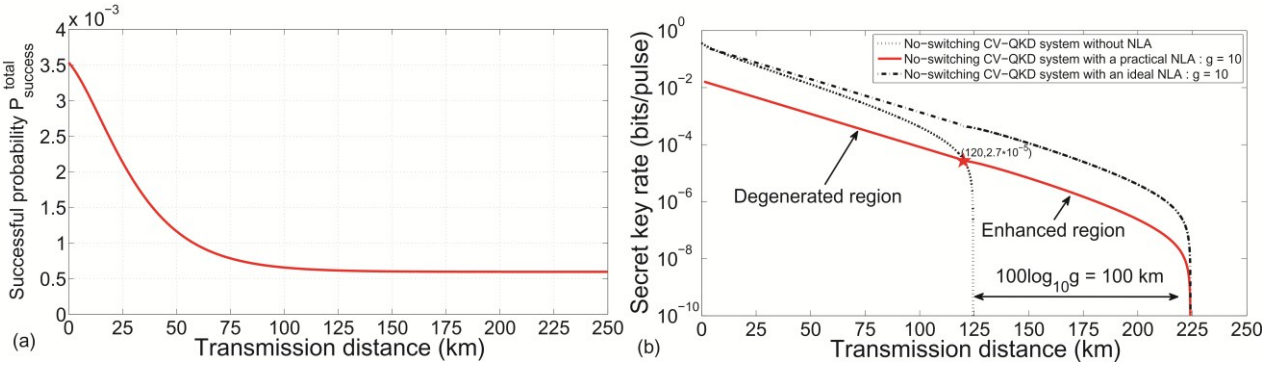

Fig. 2: (a) The successful probability of a practical NLA $P_{success}^{total}$, against the transmission distance. (b) The lower bound of the secret key rate of the practical modified no-switching CV-QKD system with an ideal (η_D=1, $P_{trigger}$=1) or a practical NLA (η_D=0.15, $P_{trigger} \neq 1$) for g = 10 and that of the original system without a NLA against the transmission distance in km. In the simulations, V_A=4.706, β=0.948, ε=0.04, $\eta_T = x$ = 0.1, $P_{success}^{total} = P_{success}^{efficiency}(\eta_D) \bullet P_{trigger}$.

As illustrated in Fig. 2 (a), we calculate the successful probability of a practical NLA against the transmission distance, which determines the successful probability of amplifying the coherent state throughout the channel. Furthermore, the secure bound of the practical modified no-switching CV-QKD system with an ideal or a practical NLA for g = 10 and that of the original system without a NLA against the transmission distance are shown in Fig. 2 (b). One can find that the maximum transmission distance is increased by $100\log_{10}g$ km by using a practical NLA with gain g.This result does not depend on $P_{success}^{total}$. The larger the gain of the NLA, the longer the secure transmission distance we can achieve .We also observe the practical NLA may not work for the whole distance. There is an enhanced region and a degenerative region. If the transmission distance is smaller than D about 120 km (g = 10), the usage of the NLA does not improve the performance of the system in terms of the secret key rates. However, if transmission distance goes beyond D, the performance of the modified system is better than without using a practical NLA. Thus, the critical point D is very significant for practical implementations of CV-QKD system.

3. Conclusion

In this paper, we analyze the no-switching CV-QKD system modified by inserting a practical NLA at the output of the quantum channel. We find that the maximum transmission distance of the modified protocol can be increased by the $100\log_{10}g$ km by using a practical NLA with gain g. A critical point is given to separate the enhanced and degenerative region, which will be useful and instructive for experiment.

4. Acknowledgment

This work was supported in part by the National Basic Research Program of China (973 Pro-gram) under Grant 2012CB315605 and 2014CB340102, in part by the National Natural Science Foundation under Grant 61271191 and 61271193, and in part by the Fundamental Re-search Funds for the Central Universities.

5. References

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution", Rev. Mod. Phys. **81**, 1301-1350 (2009).

2. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, S. Lloyd, "Gaussian quantum information", Rev. Mod. Phys. **84**, 621-669 (2012).

3. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution", Nat. Photon. **7**, 378-381 (2013).

4. F. Grosshans, P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States", Phys. Rev. Lett. **88**, 057902 (2002).

5. C. Weedbrook, A. M. Lance, W. P.Bowen, T. Symul, T. C. Ralph, P. K. Lam, "Quantum cryptography without switching", Phys. Rev. Lett. **93**, 170504, 2004.

6. R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, R. Tualle-Brouri, "Improving the maximum transmission distance of continuous variable quantum key distribution using a noiseless amplifier", Phys. Rev. A **86**,012327 (2012).

7. F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, P. Grangier, "Implementation of a Nondeterministic Optical Noiseless Amplifier", Phys. Rev. Lett. **104**, 123603 (2010)

8. M. A. Nielsen, I. L. Chuang, "Quantum computation and quantum information", Cambridge university press (2010).