Int J Theor Phys (2016) 55:1156–1166
DOI 10.1007/s10773-015-2757-1

Improving Continuous-Variable Quantum Key Distribution Using the Heralded Noiseless Linear Amplifier with Source in the Middle

Jianwu Liang[1] · Jian Zhou[1] · Jinjing Shi[1] · Guangqiang He[2] · Ying Guo[1]

Received: 10 March 2015 / Accepted: 16 June 2015 / Published online: 11 August 2015

Abstract We characterize the efficiency of the practical continuous-variable quantum key distribution (CVQKD) while inserting the heralded noiseless linear amplifier (NLA) before detectors to increase the secret key rate and the maximum transmission distance in Gaussian channels. In the heralded NLA-based CVQKD system, the entanglement source is only placed in the middle while the two participants are unnecessary to trust their source. The intensities of source noise are sensitive to the tunable NLA with the parameter g in a suitable range and can be stabilized to the suitable constant values to eliminate the impact of channel noise and defeat the potential attacks. Simulation results show that there is a well balance between the secret key rate and the maximum transmission distance with the tunable NLA.

Keywords Continuous-variable · Quantum key distribution · Noiseless linear amplifier · Source in the middle

1 Introduction

Quantum key distribution (QKD) [1–5] can provide an interesting approach for two participants, Alice and Bob, to communicate secretly over insecure quantum channels. Different from the discrete-variable quantum key distribution (DVQKD) [6, 7], the continuous-variable QKD (CVQKD) [8] offers high detection efficiencies, off-the-shelf lasers for sources, and hence has a prospect of the high rate secure key distribution.

✉ Jinjing Shi
sjjgz2009@gmail.com; shijinjing@csu.edu.cn

[1] School of Information Science & Engineering, Central South University, Changsha 410083, China

[2] State Key Lab of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200030, China

Conventionally, the usage of Gaussian resources, operations, and measurements offers a simple way of analyzing the security of the CVQKD [29–32] protocols. In contrast to Alice being the source of the entanglement protocol [27], an idea of having Eve being the source (EBTS) was put forward to keep the high secret-key rate and defend the attack performed by the eavesdropper, Eve [9]. Namely, Eve was placed in the middle between Alice and Bob and was given full control of the creation of the Gaussian entangled resource. Using the previous analytical techniques, a secure key can still be generated between Alice and Bob [10].

Recently, it has been demonstrated that noiseless linear amplifier (NLA) can be properly applied in the CVQKD protocol to improve the maximum transmission distance [11]. According to the characteristics of the one-way NLA-based CVQKD [11], it is expected that the inserted NLA [12–14] can be elegantly applied before detectors to improve the maximum transmission distance of the CVQKD with the entanglement in the middle (EITM). In the NLA-EITM-based CVQKD protocol, the parameter of the tunable NLA can be achieved from balancing between the secret-key rate and the maximal transmission distance with post-selection approach [15].

In this approach, we focus on the use of the heralded NLA that is inserted before detectors to dynamically balance between the secret key rate and the maximal transmission distance of the EITM-based CVQKD protocol, which contributes to better performances defend against losses or noises and has attracted much attention recently [9]. Compared to other optical amplifiers, such as the probabilistic NLA which amplifies the amplitude of a coherent state to achieve the original level of noise [12], the effect on the maximum transmission distance is apparent because it is the tuned parameter g rather than the success rate of the NLA has a main influence on it. Furthermore, the effect of a probabilistic NLA on the secret-key rate may be not obvious as the success rate of the NLA is always lower than $1/g^2$. Consequently, it is useful for the practical NLA-EITM-based CVQKD by compensating the effect of the noises or losses in imperfect quantum channels [16] as they usually play a key role in increasing the maximum transmission distance of quantum communications.

This paper is structured as follows. In Section 2, the NLA-EITM-based CVQKD protocol is described for a quantum network, where an entangled Gaussian resource is placed in the middle between Alice and Bob. Then the equivalent parameters of the NLA-EITM-based CVQKD protocol is calculated with the post-selection approach. In Section 3, the secret key rates of the protocols with and without NLA are compared for performance analysis while balancing the secret key rate and the maximum transmission distance. Finally, the conclusion is drawn in Section 4.

2 The NLA-EITM-Based CVQKD Protocol

In order to show the effect of the heralded NLA on the EITM-based CVQKD, we suggest an NLA-EITM-based network system with the tunable NLA being inserted before detectors using direct reconciliation.

2.1 The EITM-based CVQKD

In the EITM-based CVQKD, an entangled Gaussian resource is placed in the middle between two participants, i.e., Alice and Bob, as shown in Fig. 1. The entangled source with variance V (potentially created by the entrusted participant) is placed in the middle between Alice and Bob, as shown in Fig. 1. Eve's attack consists of two entangling cloner

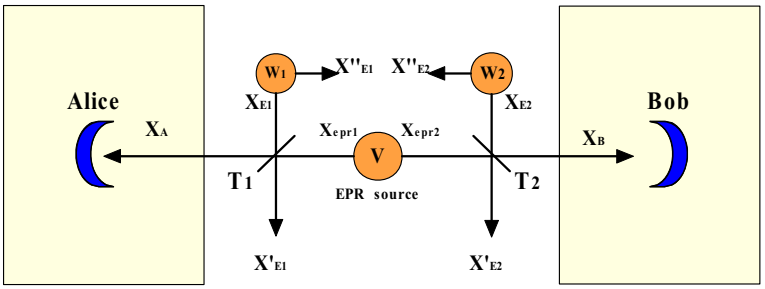

Fig. 1 Schematic of the EITM-based CVQKD protocol

attacks on each side of the source. Without loss of generality, Alice performs heterodyne detection while Bob performs homodyne detection with direct reconciliation since the calculations for reverse reconciliation can be derived automatically. The source is employed by Alice and Bob to generate a secure key for encryption [1]. In principle, this source could be created by the third party, say Charlie, while installing an entangled source between two participants in a quantum network. However, we can assume that Eve could also create this entangled state. The entangled source is assumed to be Gaussian due to the fact that a Gaussian state can maximize the Shannon mutual information and a Gaussian attack can maximize Eve's extractable information from an eavesdropping point of view [17, 18]. In the attack, Eve perfectly replaces quantum channels between Alice and Bob with her own quantum channels, where the loss is simulated by two separate beam splitters with symmetric transmissions T_1 and T_2, i.e., T_1=T_2. Eve's Einstein-Podolsky-Rosen (EPR) state has two entangled modes, i.e., X_{epr1} (sent to Alice) and X_{epr2} (sent to Bob), which is created by combining two orthogonal squeezed states X_{s1} and X_{s2} on a 50 : 50 beam splitter given by

$$X_{epr1} = (X_{s1} + X_{s2})/\sqrt{2}, \tag{1}$$

and

$$X_{epr2} = (X_{s1} - X_{s2})/\sqrt{2}. \tag{2}$$

Assume V is the symmetrized variance of two entangled modes and Eve's attack is perfect, i.e. $V := V(X_{epr1}) = V(X_{epr2})$. It is interesting to note that taking $T_1 = 1$, it becomes the conventional CVQKD where Alice creates the entangled state safely at her station. Eve performs a collective Gaussian attack on each of these beam splitters [17–19], which is the strongest attack according to the principle of quantum physics [20–22]. In addition, entangling cloner is one of the most commonly used collective Gaussian attack [23, 24]. This attack consists of Eve preparing (for each of the two beam splitter attacks) ancilla modes X_E and X''_E from an entangled Gaussian state with variance W. She keeps one mode X''_E and injects another mode X_E into the unused port of the beam splitter, leading to the output mode X'_E. These operations are repeated identically and independently for each of the signal modes sent out to Alice and Bob. The output modes are stored in a quantum computer and detected collectively at the end of the protocol with the final measurement being optimized on the basis of Alice and Bob's classical communications.

The secret-key rate of the EITM-based CVQKD protocol can be derived for direct reconciliation as follows

$$K = rS(A : B) - S(A : E), \tag{3}$$

where $S(A:B)$ (or $S(A:E)$) is the mutual information between Alice and Bob (or Alice and Eve) and r represents reconciliation efficiency [9]. Alice's heterodyne detector and Bob's homodyne detector are assumed to be perfect and their covariance matrix is characterized by [25]

$$\gamma_{AB} = \begin{pmatrix} aI & cZ \\ cZ & bI \end{pmatrix}, \tag{4}$$

where I and Z are general Pauli matrices, $a = T_1V + (1-T_1)W_1$, $b = T_2V + (1-T_2)W_2$, and $c = \sqrt{T_1T_2(V^2-1)}$ [9]. It forms the basis for most of our analysis, which takes the situation Eve being in the middle into account. The mutual information between Alice and Bob for coherent states is given by

$$S(A:B) = \frac{1}{2}\log_2\left(\frac{a+1}{a+1-c^2/b}\right). \tag{5}$$

Subsequently, we obtain $S(E) = G[(\lambda_1-1)/2] + G[(\lambda_2-1)/2]$ [8], where

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x, \tag{6}$$

and the symplectic eigenvalues $\lambda_{1,2}$ are calculated as

$$\lambda_{1,2}^2 = \frac{1}{2}\left[\Delta \pm \sqrt{\Delta^2 - 4D^2}\right], \tag{7}$$

with $\Delta = a^2 + b^2 - 2c^2$ and $D = ab - c^2$. To create a coherent state, Alice performs heterodyne detection on her mode using a $50:50$ beam splitter (BS), which introduces vacuum noise denoted by system C. The operation on the initial correlation matrix $\gamma_{A_0C_0B}$ can be described by the symplectic transformation $\gamma_{ACB} = [S_{AC}^{BS} \otimes I_B]^T \gamma_{A_0C_0B}[S_{AC}^{BS} \otimes I_B]$ [2]. Using the purification approach, we have $S(E|A) = S(BC|A)$ since the system BCE is pure after Alice's measurement. The correlation matrix of the system BC which is relevant to Alice's measurement is calculated to be

$$\gamma_{BC}^{x_a} = \begin{pmatrix} b - c^2/(a+1) & 0 & \sqrt{2}c/(a+1) & 0 \\ 0 & b & 0 & -c/\sqrt{2} \\ \sqrt{2}c/(a+1) & 0 & 2a/(a+1) & 0 \\ 0 & -c/\sqrt{2} & 0 & (a+1)/2 \end{pmatrix}. \tag{8}$$

After that, the conditional von Neumann entropy can be calculated as $S(BC|A) = G[(\lambda_3-1)/2] + G[(\lambda_4-1)/2]$, where

$$\lambda_{3,4}^2 = \frac{1}{2}\left[A \pm \sqrt{A^2 - 4B}\right], \tag{9}$$

with $A = (a + bD + \Delta)/(a+1)$ and $B = D(b+D)/(a+1)$. Finally, we can calculate $S(E:A) = S(E) - S(E|A)$, and hence achieve the secret key rate K from (3).

2.2 The Tunable NLA-EITM-Based CVQKD

We assume that Alice, Bob and Eve operate as usually while Alice and Bob insert the tunable NLA in their detection stages, as shown in Fig. 2. The entangled source with variance V is placed between Alice and Bob while Eve implements two entangling cloner attacks on each side of the source. Alice and Bob select the successful run of amplification after their detections. Only the events that corresponding to the successful amplifications will be used for extracting a secret key [11]. Since the output of the tunable NLA remains in the Gaussian regime, the equivalent parameters of a coherent state sent in a Gaussian noisy channel can

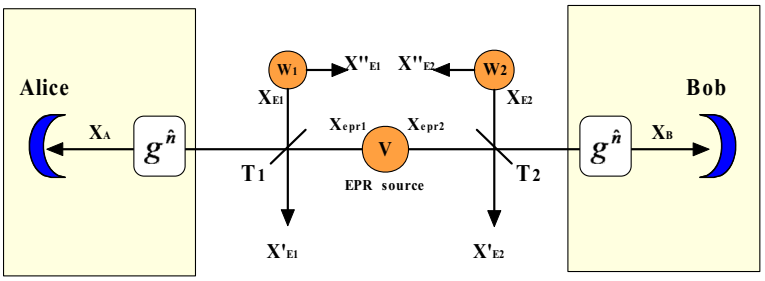

Fig. 2 Schematic of the NLA-EITM-based CVQKD protocol with the tunable NLA before detectors

be similarly derived. It is shown that the covariance matrix $\gamma_{AB}(\lambda, T, W)$($\lambda$ is the parameter of coherent state, T is the transmittance, W is the variance of attack) of the amplified state is equal to the covariance matrix $\gamma_{AB}(\zeta, \eta, N, g = 1)$, which describes an equivalent system with a coherent state parameter ζ sent through a channel with transmittance η and the variance of attack N without using the tunable NLA.

When the input state, i.e., $\hat{\rho}_{th}(\lambda_{ch}) = (1 - \lambda_{ch}^2)\Sigma_{n=0}^{\infty}\lambda_{ch}^{2n}|n\rangle\langle n|$($\lambda_{ch}$ is the parameter of thermal state), is displaced by $\beta = \beta_x + i\beta_y$, the output is described as

$$\hat{\rho} = \hat{D}(\beta)\hat{\rho}_{th}(\lambda_{ch})\hat{D}(-\beta). \tag{10}$$

This state would be received by Bob if he obtains Alice's measurement results. It can be decomposed on an ensemble of coherent states using P function [26]

$$\hat{\rho} = \int P(\alpha)|\alpha\rangle\langle\alpha|d\alpha, \tag{11}$$

where $P(\alpha) = \frac{e^{|\alpha|^2}}{\pi^2}\int e^{|u|^2}\langle -u|\hat{\rho}|u\rangle e^{u^*\alpha - u\alpha^*}du$ [11]. Straightforward calculations show that

$$\langle -u - \beta|\hat{\rho}_{th}(\lambda_{ch})|u - \beta\rangle = (1 - \lambda_{ch}^2)e^{-|u|^2(1+\lambda_{ch}^2)-|\beta|^2(1-\lambda_{ch}^2)+(u\beta^* - u^*\beta)(1-\lambda_{ch}^2)}. \tag{12}$$

Therefore we achieve $P(\alpha_x + i\alpha_y) = p(\alpha_x) * p(\alpha_y)$ with

$$p(\alpha_\varsigma) = \frac{1}{\sqrt{\pi}}\sqrt{\frac{1 - \lambda_{ch}^2}{\lambda_{ch}^2}}e^{-\frac{1-\lambda_{ch}^2}{\lambda_{ch}^2}(\alpha_\varsigma - \beta_\varsigma)^2}, \tag{13}$$

for $\varsigma \in \{x, y\}$. In the absence of thermal noise, i.e., $\lambda_{ch} = 0$, the expression $p(\alpha_\varsigma)$ in (13) becomes proportional to a Dirac distribution $\delta(\alpha_\varsigma - \beta_\varsigma)$.

The successful amplification can be ideally described by an operator $\hat{C} = g^{\hat{n}}$, where $\hat{n}$ is the number operator in the Fock basis. The yielded state has to be normalized, but the norm is not the success probability of the transformation since $\hat{C}$ is unbounded. Namely, the amplification of a coherent state $|\alpha\rangle$ leads to another coherent state proportional to $|g\alpha\rangle$, i.e.,

$$\hat{C}|\alpha\rangle = e^{\frac{|\alpha|^2}{2}(g^2-1)}|g\alpha\rangle. \tag{14}$$

Since $\hat{C}$ is linear, the amplification of $\hat{\rho}$ can be derived directly as follows

$$\hat{\rho}' = \hat{C}\hat{\rho}\hat{C} = \int P(\alpha)e^{|\alpha|^2(g^2-1)}|g\alpha\rangle\langle g\alpha|d\alpha. \tag{15}$$

By introducing the change of variable $u = g\alpha$, we obtain

$$\hat{\rho}' \propto \int P(u/g) e^{\frac{g^2-1}{g^2}|u|^2} |u\rangle\langle u| du. \tag{16}$$

As before, it is easy to see that $P(u/g) = p(u_x/g)p(u_y/g)$. Since $|u|^2 = |u_x|^2 + |u_y|^2$, we consider the scenario

$$P(u_x/g) e^{\frac{g^2-1}{g^2}u_x^2} = \frac{1}{\sqrt{\pi}} \sqrt{\frac{1-\lambda_{ch}^2}{\lambda_{ch}^2}} e^{-\frac{1-\lambda_{ch}^2}{\lambda_{ch}^2}\left(\frac{u_x}{g}-\beta_x\right)^2 + \frac{g^2-1}{g^2}u_x^2}. \tag{17}$$

The argument of the exponential can be easily put in the following form [11]

$$\begin{aligned} &-\frac{1-\lambda_{ch}^2}{\lambda_{ch}^2}\left(\frac{u_x}{g}-\beta_x\right)^2 + \frac{g^2-1}{g^2}u_x^2 = \\ &-\frac{1-g^2\lambda_{ch}^2}{g^2\lambda_{ch}^2}\left(u_x - \beta_x g \frac{1-\lambda_{ch}^2}{1-g^2\lambda_{ch}^2}\right)^2 - \beta_x^2 \frac{(1-g^2)(1-\lambda_{ch}^2)}{1-g^2\lambda_{ch}^2}. \end{aligned} \tag{18}$$

Therefore, up to a global unimportant normalization factor independent of the variable integrated α or u, the expression in (18) corresponds to a thermal state $\hat{\rho}_{th}(g\lambda_{ch})$ displaced by $\frac{g(1-\lambda_{ch}^2)}{1-g^2\lambda_{ch}^2}\beta$. Then we can conclude that

$$\hat{\rho} \propto \hat{D}(\tilde{g}\beta)\hat{\rho}_{th}(g\lambda_{ch})\hat{D}(-\tilde{g}\beta), \tag{19}$$

where $\tilde{g} = \frac{g(1-\lambda_{ch}^2)}{1-g^2\lambda_{ch}^2}$. In order to keep a physical interpretation, we note that the tuned parameter g must satisfy the constraint $g\lambda_{ch} < 1$ [11].

Let us derive the parameters β and λ_{ch} corresponding to the entanglement-based protocol presented in (19). When Alice obtains the results α_A for her heterodyne measurement on one mode of the EPR state $|\lambda\rangle$, another mode is projected on a coherent state with an amplitude proportional to $\lambda\alpha_A$. This state is then sent through the quantum channel with transmittance T, which transforms its amplitude to be proportional to $\sqrt{T}\lambda\alpha_A$. Thus the displacement β can be taken as

$$\beta = \sqrt{T}\lambda\alpha_A. \tag{20}$$

The variance $\frac{1+\lambda_{ch}^2}{1-\lambda_{ch}^2}$ of the thermal state corresponds to Bob's variance $T + (1-T)W$ for $V_A = 0$, i.e.,

$$\frac{1+\lambda_{ch}^2}{1-\lambda_{ch}^2} = T + (1-T)W, \tag{21}$$

and hence

$$\lambda_{ch}^2 = \frac{T + (1-T)W - 1}{T + (1-T)W + 1}. \tag{22}$$

Finally, the action of the NLA in (19) on a displaced thermal state given by (20) and (22) induces the transformations as follows

$$\sqrt{T}\lambda\alpha_A \to g\frac{1-\lambda_{ch}^2}{1-g^2\lambda_{ch}^2}\sqrt{T}\lambda\alpha_A, \tag{23}$$

$$\frac{T + (1-T)W - 1}{T + (1-T)W + 1} \to g^2 \frac{T + (1-T)W - 1}{T + (1-T)W + 1}. \tag{24}$$

In what follows, we consider the effect of the tunable NLA when Bob has no idea about Alice's measurement result. In such a case, Bob's state is a thermal state $\hat{\rho}_B = (1-\lambda^{*2})\Sigma_{n=0}^{\infty}(\lambda^*)^{2n}|n\rangle\langle n|$, whose variance is given by γ_{AB}, i.e.,

$$\frac{1+\lambda^{*2}}{1-\lambda^{*2}} = TV + (1-T)W, \tag{25}$$

from which we obtain

$$\lambda^{*2} = \frac{TV + (1-T)W - 1}{TV + (1-T)W + 1}. \tag{26}$$

Since the tunable NLA always transforms a thermal state with parameter λ^* into another thermal state with parameter $g\lambda^*$, it shows that the tunable NLA performs the transformation as follows

$$\frac{TV + (1-T)W - 1}{TV + (1-T)W + 1} \to g^2 \frac{TV + (1-T)W - 1}{TV + (1-T)W + 1}. \tag{27}$$

According to above-mentioned analysis, the effective parameters ζ, η and N can be derived from

$$\sqrt{\eta}\zeta = g\frac{1-\lambda_{ch}^2}{1-g^2\lambda_{ch}^2}\sqrt{T}\lambda, \tag{28}$$

$$\frac{\eta + (1-\eta)N - 1}{\eta + (1-\eta)N + 1} = g^2 \frac{T + (1-T)W - 1}{T + (1-T)W + 1}, \tag{29}$$

and

$$\frac{\eta\frac{1+\zeta^2}{1-\zeta^2} + (1-\eta)N - 1}{\eta\frac{1+\zeta^2}{1-\zeta^2} + (1-\eta)N + 1} = g^2 \frac{T\frac{1+\lambda^2}{1-\lambda^2} + (1-T)W - 1}{T\frac{1+\lambda^2}{1-\lambda^2} + (1-T)W + 1}. \tag{30}$$

Taking for $W = 1$, we achieve

$$\zeta = \lambda\sqrt{1 + (g^2-1)T}, \eta = \frac{g^2 T}{1 + (g^2-1)T}, N = 1. \tag{31}$$

It is obvious that the parameters ζ, η, N correspond to the parameters λ, T, W, respectively. In the light of the equivalent parameters with the constraints $0 < \zeta < 1$, $0 < \eta < 1$ and $N \geq 1$, we get the maximum value of the gain g_{max} given by

$$g_{max}(T, W) = \sqrt{\frac{-2\sqrt{\frac{(W^2-1)(T-1)^2}{T}} + 4T\sqrt{\frac{(W+1)T}{W-1}} + ((W+1)T - W + 1)(W+1)(T-1)}{((W+1)T - W + 1)^2}}. \tag{32}$$

We obtain the relationship between W and ϵ due to the attacks hidden in the noises, i.e., $(1-T)W = 1 - T + T\epsilon$. The channel loss L will change the channel transmission T to $T = 10^{-L/10}$. Then the function of $g_{max}(L, \epsilon)$ is acquired, as shown in Fig. 3. It is helpful for us to find the optimal parameter g according to the values of L and ϵ. Making use of these parameters, we can calculate the secret-key rate as a function of the transmission distance, which will be analyzed in next section.

3 Performance Analysis

The secret-key rate of the non-NLA-EITM-based CVQKD protocol without using the NLA is given by $K(\lambda, T, W)$ in (3). By multiplying the secret-key rate for successful amplifications $K(\zeta, \eta, N)$ with the success probability P_{ss}, the secret-key rate K_{NLA} of the

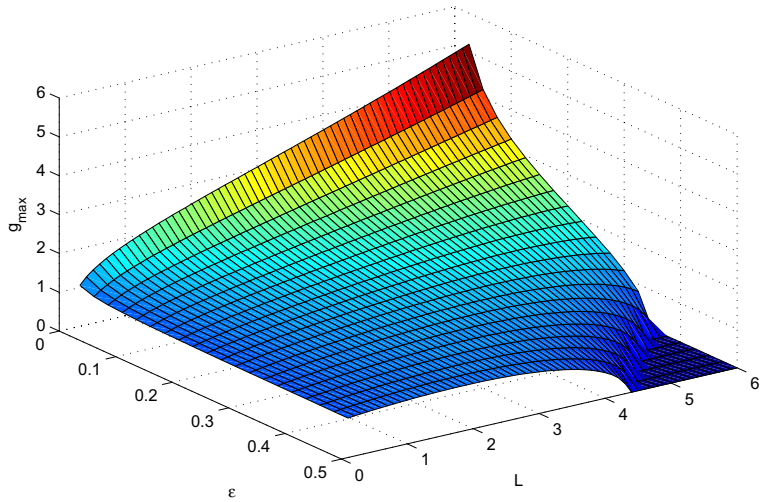

Fig. 3 Maximum value of the gain g_{max} as a function of the losses and noise. Maximum value g_{max} rises with the increase of the loss while the noise has a negative effect on the g_{max}

NLA-EITM-based CVQKD protocol can be derived. For the simple analysis, it can be assumed that the tunable NLA has a sufficient dynamics to neglect distortions and hence P_{ss} is constant. This is a reasonable assumption since in that case the optimal value of V is not infinite for the constraint $r < 1$. In addition, the precise value of P_{ss} depends on practical implementations and is not important in this work. It acts only as a scaling factor and does not change the fact that a zero secret-key rate can become positive with the tunable NLA. Then we get the secret-key rate given by

$$K_{NLA} = P_{ss} K(\zeta, \eta, N). \tag{33}$$

The success probability P_{ss} for the tunable NLA with gain g is bounded by $1/g^2$, which will be used for the NLA-EITM-based CVQKD protocol.

Using the above-derived parameters, the secret-key rates of the NLA-EITM-based protocol can be acquired in simulations over a lossy channel. We consider a simple case that Alice performs heterodyne detection while Bob performs homodyne detection for coherent states. The parameter η can be calculated with the help of λ and g, and the value λ is selected as small as possible due to the constraint of η. Furthermore, the value λ that satisfies the constraint $V = \frac{1+\lambda^2}{1-\lambda^2}$ should be taken large enough to achieve the high secret key rate. Simulations show that this protocol performs well for the given parameters $W = 1$, $V = 1.13$, $\epsilon = 0.005$, and $r = 0.95$. In addition, we let $T = 10^{-aS/10}$, where S denotes the transmission distance and $a = 0.2$ dB/km is the optical fibre channel loss coefficient.

We illustrate the secret key rates (bit/pulse) of the EITM-based protocol as functions of transmission distance (km) in Fig. 4. The full line indicates the secret-key rate for the EITM-based protocol without using the NLA [9], while the dashed and dotted lines indicate that of the protocol with the inserted NLA for $g = 2$ and $g = 3$, respectively. Compared with the non-NLA-EITM-based protocol, the maximum transmission distance of the NLA-EITM-based protocol is more than 30 kilometers for $g = 2$ before the secret key rate decreases rapidly, as shown in Fig. 4. Furthermore, taking a larger parameter for $g = 3$, the maximum transmission distance of the NLA-EITM-based protocol can be increased by

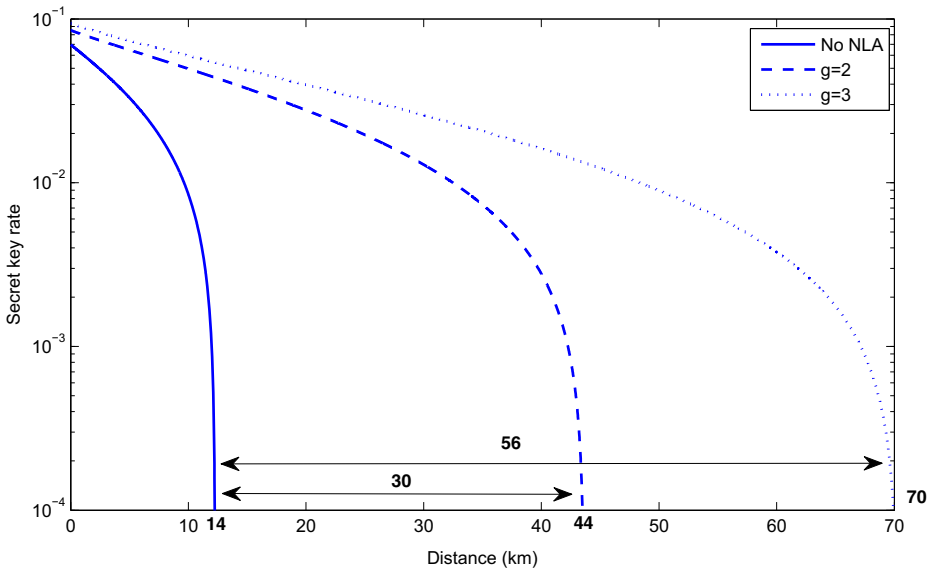

Fig. 4 Maximized secret-key rates as a function of the distance. The horizontal axis shows distance and longitudinal axis key rate

almost 56 kilometers. It is interesting to note that the secret key rate decreases slowly before the transmission distance approaches to 70 kilometers. Also, there is a well balance between the secret key rate and the maximal transmission distance for the parameter g of the tunable NLA. Namely, the larger value g means the higher secret key rate and the longer maximal transmission distances as well. Of course, the NLA-EITM-based protocol performs much better than that of the non-NLA-EITM-based protocol in terms of both the secret key rate and the maximal transmission distance.

We note that here the above-mentioned results are not the exact secret key rate and maximal transmission distance of the implemental protocol in practice, but only an illustration of the effect of the NLA on the EITM-based CVQKD [28]. The reason is that the NLA-added noise can be manipulated adaptively for the optimization referring to participants' detections, which enhance the performance in implementation procedures [10]. Furthermore, the case of the NLA-EITM-based CVQKD may be similarly done by the receiver (Bob) of reverse reconciliation to enhance the efficiency of the related CVQKD, which can be analyzed in a similar way. Therefore, the simulation results are just for the preliminary analysis and the rigorous analysis of the proposed NLA-EITM-based CVQKD protocol needs to be further investigated in our future work.

4 Conclusions

A novel NLA-EITM-based CVQKD protocol with the tunable heralded NLA inserting before each receiving terminal is proposed to to balance between the secret key rate and the maximal transmission distance. It has been demonstrated that the inserted NLA in the EITM-based CVQKD protocol can increase the maximum transmission distance by

$20\log_{10}g$ dB of losses, which is compared with the non-NLA-EITM-based CVQKD protocol. In this protocol, the tunable NLA increases the maximum distance by about 30 kilometers, which is equivalent to 6 dB of losses even for a small gain $g = 2$. As mentioned above, two tunable NLAs can be respectively inserted in the NLA-EITM-based CVQKD protocol which means the increased distance is doubled.

Acknowledgments This work was supported by the National Natural Science Foundation of China (Grant Nos. 61272495, 61379153, 61401519), the Research Fund for the Doctoral Program of Higher Education of China (Grant Nos. 20130162110012), the Program for New Century Excellent Talents in University of Ministry of Education of China (NCET-11-0510).

References

1. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dusek, M., Lutkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301 (2009)
2. Zhang, H., Fang, J., He, G.: Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers. Phys. Rev. A **86**, 022338 (2012)
3. Qian, Y., Shen, Z., He, G., Zeng, G.: Quantum-cryptography network via continuous-variable graph states. Phys. Rev. A **86**, 052333 (2012)
4. Ma, X.-C., Sun, S.-H., Jiang, M.-S., Gui, M., Liang, L.-M.: Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. Phys. Rev. A **89**, 042335 (2014)
5. Zhang, Y.-C., Li, Z., Song, Y., Wanyi, G., Peng, X., Guo, H.: Continuous-variable measurement-device-independent quantum key distribution using squeezed states. Phys. Rev. A **90**, 052325 (2014)
6. Bennett, C.H., Brassard, G.: Proceedings of IEEE International Conference Computers, System and Signal Processing, pp. 175–179. IEEE, New York (1984)
7. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145 (2002)
8. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N.J., R.lph, T.C., Shapiro, J.H., Lloyd, S.: Gaussian quantum information. Rev. Mod. Phys. **84**, 621 (2012)
9. Weedbrook, C.: Continuous-variable quantum key distribution with entanglement in the middle. Rev. Mod. Phys. **87**, 022308 (2013)
10. Garcia-Patron, R.: Ph.D. thesis, Universite Libre de Bruxelles, Bruxelles (2007)
11. Blandino, R., Leverrier, A., Barbieri, M., Etesse, J., Grangier, P., Tualle-Brouri, R.: Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. Phys. Rev. **86**, 012327 (2012)
12. Ralph, T.C., Lund, A.P.: Nondeterministic noiseless linear amplification of quantum systems. In: Lvovsky, A. (ed.) Quantum Communication Measurement and Computing Proceedings of 9th International Conference, pp. 155–160. AIP Conf. Proc. No. 1110, AIP, New York (2009). arXiv:0809.0326
13. Ferreyrol, F., Blandino, R., Barbieri, M., Tualle-Brouri, R., Grangier, P.: Experimental realization of a nondeterministic optical noiseless amplifier. Phys. Rev. A **83**, 063801 (2011)
14. Zavatta, A., Fiurasek, J., Bellini, M.: A quantum delivery note. Nature Photon. Lett. **5**, 52 (2011)
15. Walk, N., Ralph, T.C., Symul, T., Lam, P.K.: Security of continuous-variable quantum cryptography with Gaussian postselection. Phys. Rew. A **87**, 020303(R) (2013)
16. Ralph, T.C.: Quantum error correction of continuous-variable states against Gaussian noise. Phys. Rev. A **84**, 022339 (2011)
17. Navascués, M., Acín, A.: Security bounds for continuous variable quantum key distribution. Phys. Rev. Lett. **94**, 020505 (2005)
18. Garcéa-Patrín, R., Cerf, N.J.: Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys. Rev. Lett. **97**, 190503 (2006)
19. Pirandola, S., Braunstein, S.L., Lloyd, S.: Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. Phys. Rev. Lett. **101**, 200504 (2008)
20. Renner, R., Cirac, J.I.: de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Phys. Rev. Lett. **102**, 110504 (2009)
21. Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. **88**, 057902 (2002)
22. Grosshans, F., Assche, G., Wenger, J., Brouri, R., Cerf, N.J., Grangier, P.: Quantum key distribution using gaussian-modulated coherent states. Nature (London) **421**, 238 (2003)

23. Grosshans, F., Cerf, N.J., Wenger, J., Tualle-Brouri, R., Grangier, Ph.: Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quantum Inf. Comput. **3**, 535 (2003)
24. Häseler, H., Moroder, T., Lütkenhaus, N.: Testing quantum devices: Practical entanglement verification in bipartite optical systems. Phys. Rev. A **77**, 032303 (2008)
25. Weedbrook, C., Lance, A.M., Bowen, W.P., Symul, T., Ralph, T.C., Lam, P.K.: Quantum cryptography without switching. Phys. Rev. Lett. **93**, 170504 (2004)
26. Gerry, C.C., Knight, P.L.: Introductory quantum optics. Cambridge University Press, Cambridge (2005)
27. Walk, N., Ralph, T.C.: Gaussian post-selection for continuous variable quantum cryptography, quantum physics. arXiv:1206.0936v2 [quant-ph] 6 Jun 2012
28. Fossier, S., Diamanti, E., Debuisschert, T., Tualle-Brouri, R., Grangier, P.: Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. J. Phys. B: Mol. Opt. Phys. **42**, 114014 (2009)
29. He, G., Zhu, J., Zeng, G.: Quantum secure communication using continuous variable Einstein-Podolsky-Rosen correlations. Phys. Rev. A **73**, 012314 (2006)
30. Huang, P., He, G., Fang, J., Zeng, G.: Performance improvement of continuous-variable quantum key distribution via photon subtraction. Phys. Rev. A **87**, 012317 (2013)
31. Wang, X.-Y., Bai, Z.-L., Wang, S.-F., Li, Y.-M., Peng, K.-C.: Four-state modulation continuous variable quantum key distribution over 30 km fibre and analysis of excess noise. Chin. Phys. Lett. **30**(1), 010305 (2013)
32. Wang, X.-Y., Bai, Z.-L., Du, P.-Y., Li, Y.-M., Peng, K.-C.: Ultrastable fiber-based time-domain balanced homodyne detector for quantum communication. Chin. Phys. Lett. **29**(12), 124202 (2012)