entropy

MDPI

Article

Improving the Performance of Continuous-Variable Measurement-Device-Independent Quantum Key Distribution via a Noiseless Linear Amplifier

Fan Jing, Weiqi Liu *, Lingzhi Kong and Chen He *

College of Information Science and Technology, Northwest University, Xi’an 710127, China;
jingfan1217@163.com (F.J.); konglingzhi@stumail.nwu.edu.cn (L.K.)
* Correspondence: vickylwq1991@nwu.edu.cn (W.L.); chenhe@nwu.edu.cn (C.H.)

Abstract: In the continuous variable measurement-device-independent quantum key distribution (CV-MDI-QKD) protocol, both Alice and Bob send quantum states to an untrusted third party, Charlie, for detection through the quantum channel. In this paper, we mainly study the performance of the CV-MDI-QKD system using the noiseless linear amplifier (NLA). The NLA is added to the output of the detector at Charlie’s side. The research results show that NLA can increase the communication distance and secret key rate of the CV-MDI-QKD protocol. Moreover, we find that the more powerful the improvement of the performance with the longer gain of NLA and the optimum gain is given under different conditions.

Keywords: CV-MDI-QKD; NLA; the performance

check for updates

Citation: Jing, F.; Liu, W.; Kong, L.; He, C. Improving the Performance of Continuous-Variable Measurement-Device-Independent Quantum Key Distribution via a Noiseless Linear Amplifier. *Entropy* **2021**, *23*, 1691. https://doi.org/10.3390/e23121691

Academic Editor: Ángel S. Sanz

Received: 16 November 2021
Accepted: 14 December 2021
Published: 16 December 2021

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the development of photoelectric technology, many physical phenomena of quantum theory [1] have been verified through observation, which attracts many researchers to consider its application. Quantum key distribution (QKD) [2,3] is one of the applications, in which two trusted communication parties (Alice and Bob) are allowed to exchange the cryptographic key through a quantum channel at the existence of eavesdropping. Its theoretical unconditional security is guaranteed by the laws of Heisenberg’s uncertainty principle [4] and no-clone theory [5,6]. The QKD protocols are mainly divided into the following two categories: the discrete variable quantum key distribution (DVQKD) [7–10] and the continuous variable quantum key distribution (CVQKD) [11–15]. In theory, the unconditional security of QKD has been proven [16–22].

However, the deviation between the theoretical assumption and the actual implementation will effect the performance and may lead to a loophole in the practical system that could be used by Eve to intercept key information without being discovered. The loopholes involve the the laser source [23–25], the local oscillator [26,27], the beam splitter (BS) [28–30], the basis choice [31], and the detector [32–37]. Nowadays, researchers have proposed the CV-MDI-QKD protocol [38–40], which can defend all detector side channels. In the CV-MDI-QKD protocol, Alice and Bob each generate an Einstein–Podolsky–Rosen (EPR) state, and both of them send one mode of the EPR state to an untrusted third party, Charlie, for detection through the quantum channel. After the CV-MDI-QKD protocol was put forward, it was well analyzed in theory and demonstrated in experiments. However, the shortcomings of the communication distance and secret key rate of the CV-MDI-QKD system are still a problem.

In this paper, facing the above problem, the NLA is induced to improve the performance of the CV-MDI-QKD system. The amplification performance of the NLA is better because it can mechanically amplify the amplitude of the coherent state while retaining the excess noise at the initial level [41–43]. Thus, when only considering its successful runs, the NLA can compensate the effect of losses and could therefore be useful for quantum communication [44]. So, in theory, the NLA can greatly improve the signal-to-noise ratio of the transmission signal, so that the performance of the system can be improved. Here, we consider that we can add two NLAs to the output ports of two homodyne detectors on Charlie's side. We find that the communication distance and secret key rate of the NLA-based CV-MDI-QKD system have been improved.

The structure of this paper is as follows. In Section 2, we first introduce the CV-MDI-QKD protocol, and then the CV-MDI-QKD protocol with NLA is investigated. Then, the performance of the CV-MDI-QKD protocol with NLA is analyzed in Section 3. Finally, we conclude the paper in Section 4.

2. The Scheme of CV-MDI-QKD with NLA

The equivalent entanglement-based (E&B) model of the CV-MDI-QKD protocol is shown in Figure 1. Alice prepares an EPR state, keeps one of its mode A_1, and sends the other mode A_2 to Charlie by channel A. Bob also prepares another EPR state and keeps the mode B_1, and the mode B_2 is also sent to Charlie by channel B. Then, Charlie will obtain the quadratures X_C and P_D via homodyne detectors after interfering with the received modes A_2' and B_2' through a 50:50 BS. Then, X_C and P_D pass through their respective amplifiers. After being amplified by NLA, we record the measurement results $\{X_C', P_D'\}$, which will be announced by Charlie.

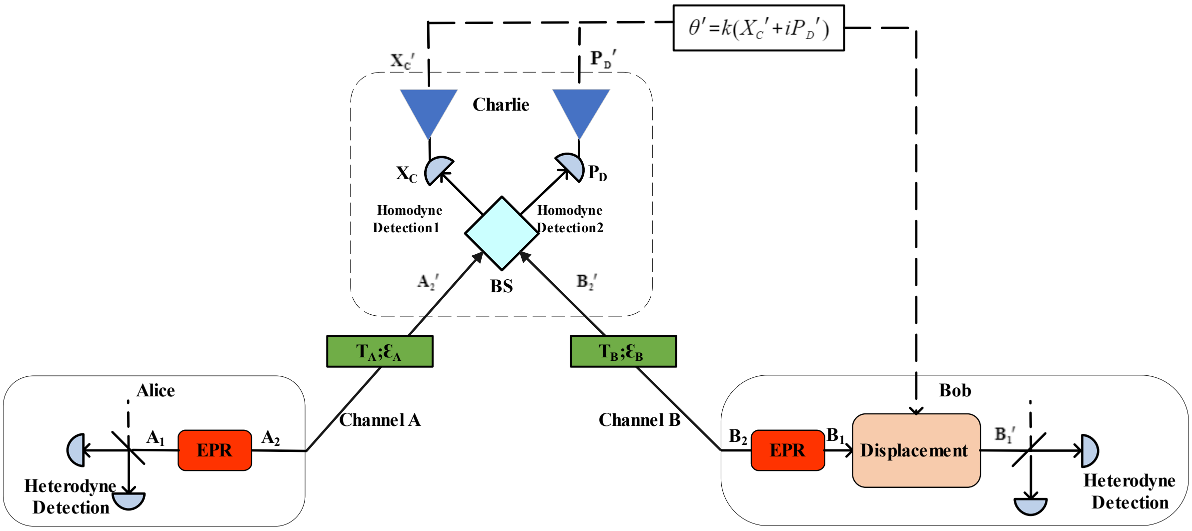

Figure 1. The EB scheme of the CV-MDI-QKD system with the noiseless linear amplifier. T_A and ϵ_A are the transmittance and excess noise of channel A, respectively. T_B and ϵ_B are the transmittance and excess noise of channel B, respectively. BS is the beam splitter with the splitting ratio 50:50.

After Alice and Bob receive the measurement results announced by Charlie, Bob performs the displacement operation $D(\theta')$ on the mode B_1 and obtains the mode B_1', where $\theta' = k(X_C' + iP_D')$ and k is the gain coefficient of the displacement operation. Then, Alice and Bob measure states A_1 and B_1', respectively, via heterodyne detector. Finally, they obtain the data $\{X_A', P_A'\}$, $\{X_B', P_B'\}$. If we assume that Bob's EPR state preparation and displacement operation are untrusted, then the protocol could be seen as the well-known one-way CVQKD protocol using coherent states and heterodyne detection [45].

Moreover, due to the presence of Charlie in the CV-MDI-QKD system, there are two situations. Firstly, the symmetrical situation is that the distance L_{AC} between Alice and Charlie is equal to the distance L_{BC} between Bob and Charlie, i.e., $L_{AC} = L_{BC}$. In this case, the secure communication distance is relatively short due to the excess noise in the channel. Secondly, the asymmetrical case is that the third-party is infinitely close to Bob, that is, $L_{BC} = 0$. In this case, the communication distance is significantly higher than the symmetrical case. Therefore, in this paper, we only consider the secret key rate in the asymmetric case.

Assuming that there is such an equivalent in Figure 2, i.e., the modulation variance of the CV-MDI-QKD system without NLA is $V(\lambda) = \frac{1+\lambda^2}{1-\lambda^2}$, the channel transmittance is T, and the channel excess noise ϵ can be equivalent to the modulation variance of the NLA-based CV-MDI-QKD system, which is $V(\lambda_d) = \frac{1+\lambda_d^2}{1-\lambda_d^2}$, and the channel transmittance and excess noise are T_d and ϵ_d, respectively. Considering a thermal state $\hat{\rho}_{th}(\lambda_{ch}) = (1-\lambda_{ch}^2)\sum_{n=0}^{\infty}\lambda_{ch}^{2n}|n\rangle\langle n|$ with variance $\frac{1+\lambda_{ch}^2}{1-\lambda_{ch}^2}$ and the displacement $\beta = \beta_x + i\beta_y$, the displaced input thermal state can be given by:

$$\hat{\rho} = \hat{D}(\beta)\hat{\rho}_{th}(\lambda_{ch})\hat{D}(-\beta) \tag{1}$$

When the input thermal state is amplified successfully by NLA, the thermal state $\hat{\rho}$ will be transformed into:

$$\hat{\rho'} = \hat{D}(g'\beta)\hat{\rho}_{th}(g\lambda_{ch})\hat{D}(-g'\beta) \tag{2}$$

where the variance is $\frac{1+g^2\lambda_{ch}^2}{1-g^2\lambda_{ch}^2}$. Here, g' is $g\frac{1-\lambda_{ch}^2}{1-(g\lambda_{ch})^2}$, we set the parameter g to satisfy $g\lambda_{ch} < 1$, λ_{ch} is the compressibility of the incident thermal state, and the displacement of the thermal state is $g'\beta$ after the amplification of NLA. The related parameters are given by:

$$\begin{aligned}
\lambda_d &= \lambda\sqrt{\frac{(g^2-1)(\epsilon-2)T-2}{(g^2-1)\epsilon T-2}} \\
T_d &= \frac{g^2 T}{(g^2-1)T[\frac{1}{4}(g^2-1)(\epsilon-2)\epsilon T-\epsilon+1]} \\
\epsilon_d &= \epsilon - \frac{1}{2}(g^2-1)(\epsilon-2)\epsilon T
\end{aligned} \tag{3}$$

where g is the amplification gain of NLA. The amplification effect of NLA on the system is essential to amplify the quantum state transmitted in the channel. As we all know, when the coherent state transmits in the channel, it will be interfered by the excess noise of the channel. Then, it will be regarded as a displacement thermal state. The NLA's effect on this displaced thermal state can be described by Equation (3) when it is successfully amplified. However, the above equation only considers the amplification effect of the quantum state transmitted in the channel when the NLA amplification is successfully amplified. The successful amplification of NLA is actually probabilistic. Therefore, we must also consider the impact of NLA probabilistic amplification on the EPR state [45].

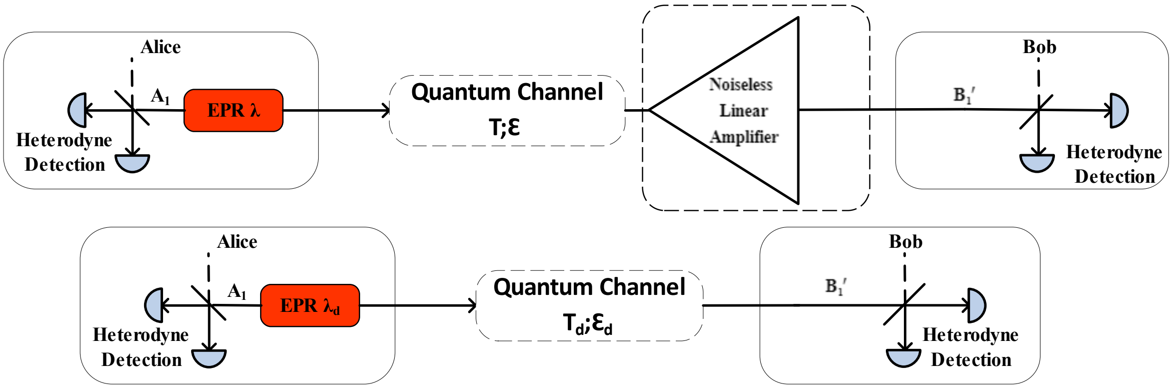

Figure 2. The equivalent method is used to analyze the CV-MDI-QKD system with NLA.

In general, the thermal state ρ can be regarded as the superposition of countless coherent states and can be expressed $\hat{\rho} = \int P(\alpha)|\alpha\rangle\langle\alpha|d\alpha$. The equation can be used in the EB model, and $P(\alpha)$ represents the probability of the coherent state $|\alpha\rangle$ being transmitted to Bob through the channel. If we selectively amplify the coherent state $|\alpha\rangle$ in the channel and only retain the successfully amplified state, that is, the non-uniform shielding of the EPR state, we will obtain a new thermal state finally. The corresponding entanglement parameter λ_d is given as follows:

$$\lambda_d = \frac{\lambda}{\sqrt{1 - T\lambda^2(g^2 - 1)}} \tag{4}$$

Furthermore, only considering the case when the coherent state is successfully amplified by NLA, the other two equivalent parameters T_d and ϵ_d will be recalculated. The EPR state is always prepared by Alice, and Alice obtains the result of the heterodyne detection α_A in one mode $|\lambda\rangle$ of the EPR state, the amplitude of which is proportional to $\lambda\alpha_A$. This coherent state is sent to Bob through a quantum channel with a transmittance T, which transforms its amplitude to $\propto \sqrt{T}\lambda\alpha_A$. The displacement thermal state β can thus be taken as:

$$\beta = \sqrt{T}\lambda\alpha_A \tag{5}$$

After being amplified by the NLA, the displacement thermal state β becomes:

$$\sqrt{T}\lambda\alpha_A \rightarrow g\frac{1 - \lambda_{ch}^2}{1 + (g\lambda_{ch})^2}\sqrt{T}\lambda\alpha_A \tag{6}$$

When the modulation variance on Alice's side $V_A = 0$, the variance of the thermal state will be equal to the variance at Bob's side, where ϵ is the excess noise of the CV-MDI-QKD system channel. That is:

$$\frac{1 + \lambda_{ch}^2}{1 - \lambda_{ch}^2} = 1 + T\epsilon \Rightarrow \lambda_{ch}^2 = \frac{T\epsilon}{T\epsilon + 2} \tag{7}$$

After the NLA's amplification, the parameter λ_{ch} will be changed to $g\lambda_{ch}$ and then:

$$\lambda_{ch}^2 = \frac{T\epsilon}{T\epsilon + 2} \rightarrow \lambda_{ch}'^2 = g^2\frac{T\epsilon}{T\epsilon + 2} \tag{8}$$

Finally, we consider the action of the NLA when Bob does not have any knowledge of Alice's measurement result. In this case, Bob's state is regarded as a thermal state $\hat{\rho}(\lambda_d) = (1 - \lambda_d^2)\sum_{n=0}^{\infty}\lambda_d^{2n}|n\rangle\langle n|$, where the variance is:

$$V(\lambda_d) = \frac{1 + \lambda_d^2}{1 - \lambda_d^2} = TV_A + T\epsilon + 1 \tag{9}$$

According to Equation (9) and based on the analysis above, we know that the parameter λ_d will change to $g\lambda_d$ after NLA, and the following equation will be obtained:

$$\lambda_d^2 = \frac{\lambda^2 T(2 - \epsilon) + T\epsilon}{2 - 2\lambda^2(1 - T) + T\epsilon(1 - \lambda^2)} \rightarrow \lambda_d'^2 = g^2\frac{\lambda^2 T(2 - \epsilon) + T\epsilon}{2 - 2\lambda^2(1 - T) + T\epsilon(1 - \lambda^2)} \tag{10}$$

By Equations (8) and (10), we can obtain:

$$\begin{aligned} T_d &= \frac{4Tg^2}{[T\epsilon(1 - g^2) + 2]^2} \\ \epsilon_d &= \epsilon - \frac{1}{2}T(g^2 - 1)\epsilon^2 \end{aligned} \tag{11}$$

When the parameters of the CV-MDI-QKD system λ, T, and ϵ are replaced by the improved channel equivalent parameter λ_d, T_d, and ϵ_d, we can find that the signal-to-noise ratio of system will be improved. There are also some limitations we should pay attention to in the developed method provided above. When we calculate the secret key rate after the equivalent channel, the equivalent parameters must satisfy the following relationship: $0 < \lambda_d < 1$, $0 \leq T_d < 1$, $\epsilon_d \geq 0$. We put this restriction into Equation (11). Then, we can obtain the following restriction:

$$g_{max}(\lambda, T, \epsilon) = Min(\sqrt{1 + \frac{1-\lambda}{T\lambda^2}}, \frac{-1 + \sqrt{4 + 4\epsilon(2 + T\epsilon)}}{\sqrt{T}\epsilon}) \tag{12}$$

According to Equation (12), we can obtain an upper bound of the parameter g of the NLA. As shown in Figure 3, the maximum value g_{max} of NLA with channel loss is plotted under different values of the entanglement coefficient, i.e., $\lambda = 0.7, 0.8, 0.9$. The result shows that the gain g of the NLA is limited to a small rang at the short communication distance, but when the communication distance is long, the gain of the NLA will increase quickly. In addition, the smaller the entanglement coefficient is, the greater the gain will be under the same communication distance.

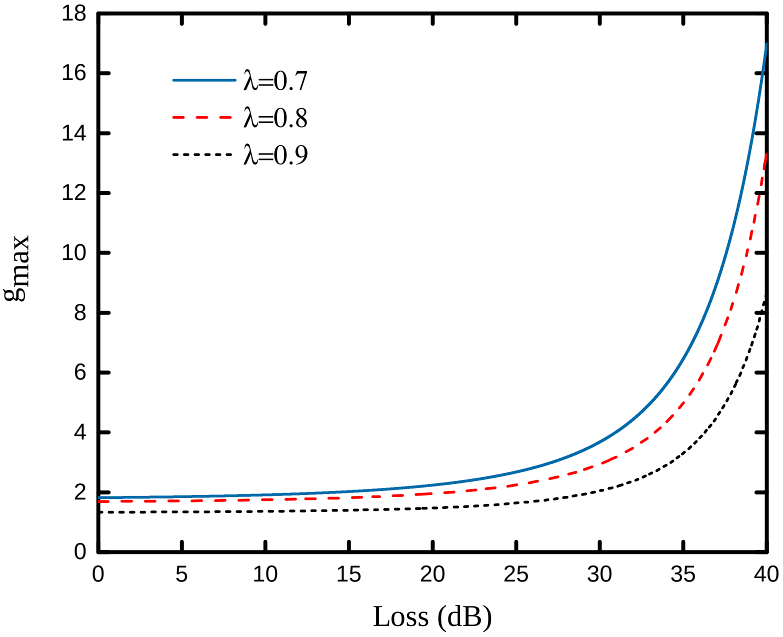

Figure 3. The maximum value g_{max} of NLA gain is a function of channel loss (dB). The curve from top to bottom is $\lambda = 0.7, 0.8, 0.9$. The excess noise is $\epsilon_A = \epsilon_B = 0.001$.

3. The Secret Key Rate of the CV-MDI-QKD System with NLA

In the previous chapter, we introduced the amplification performance of NLA in detail, the equivalent parameters of channel transmittance and excess noise of the CV-MDI-QKD system with NLA are obtained. Then, we will calculate the secret key rate of the CV-MDI-QKD system with NLA, and the performance of the system will be simulated.

Assuming that the quantum channel parameters transmittance between Alice (Bob) and Charlie are $T_A = 10^{-aL_{AC}/10}$ ($T_B = 10^{-aL_{BC}/10}$), here, the quantum channel losses are $a = 0.2$ dB/km. The excess noise is $\epsilon_A(\epsilon_B)$ correspondingly. After performing the quantum channel equivalent, the covariance matrix of $\rho^{NLA}_{A_1B'_1}$ has the following form:

$$\gamma_{A_1B'_1} = \begin{bmatrix} a\mathbb{I}_2 & c\sigma_z \\ c\sigma_z & b\mathbb{I}_2 \end{bmatrix} = \begin{bmatrix} V(\lambda_d)\mathbb{I}_2 & \sqrt{T_d[(V(\lambda_d))^2 - 1)}\sigma_z \\ \sqrt{T_d[(V(\lambda_d))^2 - 1)}\sigma_z & T_d(V(\lambda_d) + \chi_{tot})\mathbb{I}_2 \end{bmatrix} \tag{13}$$

where II_2 is the 2×2 identity matrix and σ_z is the Pauli matrix $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. χ_{tot} represents the total noise at the input of the channel, $\chi_{tot} = \chi_{line} + \frac{2\chi_{hom}}{T}$, χ_{hom} represents the noise of the homodyne detector, $\chi_{hom} = \frac{1+v_{el}}{\eta} - 1$, χ_{line} represents the noise of the quantum channel, and $\chi_{line} = \frac{1}{T} - 1 - \epsilon'$. Here, ϵ' refers to the equivalent excess noise of the equivalent one-way protocol, which can be calculated by:

$$\epsilon' = 1 + \chi_A + \frac{T_B(\chi_B - 1)}{T_A} + \frac{1}{T_A}(\frac{\sqrt{2}}{k}\sqrt{V_B - 1} - \sqrt{T_B}\sqrt{V_B + 1})^2 \tag{14}$$

where $\chi_A = \epsilon_A - 1 + \frac{1}{T_A}, \chi_B = \epsilon_B - 1 + \frac{1}{T_B}$ and when we set $k = \sqrt{\frac{2(V_B - 1)}{T_B(V_B + 1)}}$, we will obtain:

$$\epsilon' = \epsilon_A + \frac{1}{T_A}[2 + T_B(\epsilon_B - 2)] \tag{15}$$

Considering collective attack,the secret key rate of the CV-MDI-QKD protocol with NLA under finite-size effect can be defined as follows [46]:

$$K_{finite} = P_{nla}[\frac{n}{N}(\beta I_{AB} - \chi_{BE} - \Delta(n))] \tag{16}$$

where P_{nla} is the probability of successful amplification of the NLA and $P_{nla} = 1/g^2$, N is the length of valid data collected, n is the data length used for the final key rate generation, $m = N - n$ is the data length for parameter estimation, β is the efficiency of reverse reconciliation, $\Delta(n)$ is a function related to privacy enhancement, and $\Delta(n) = 7\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}}$, where $\bar{\epsilon}$ means the smoothing parameter.

Moreover, I_{AB} is the Shannon mutual information between Alice and Bob, which can be written as:

$$I_{AB} = 2 \times \frac{1}{2}\log_2\frac{V_A}{V_{A|B}} = \log_2\frac{a+1}{a+1-c^2/(b+1)} \tag{17}$$

where $V = V_A + 1$. From Equation (9), we can obtain the modulation variance $V_A = \frac{V(\lambda)-1-T\epsilon}{T}$, where λ is substituted with the equivalent λ_d.

In addition, the maximum information χ_{BE} that Eve can eavesdrop from Bob is limited by the Holevo quantity:

$$\chi_{BE} = S(\rho_E) - \int dm_B p(m_B) S(\rho_E^{m_B}) \tag{18}$$

where m_B represents Bob's measurement results, $p(m_B)$ represents the measured probability density, $\rho_E^{m_B}$ represents Eve's state under Bob's measurement, and $S(\rho)$ represents the von Neumann entropy of the quantum state ρ. Since Eve can purify the system $\rho_{A_1B_1'}$, we can obtain $S(\rho_E) = S(\rho_{A_1B_1'})$. Therefore, χ_{BE} can be expressed as:

$$\chi_{BE} = S(\rho_{A_1B_1'}) - S(\rho_{A_1}^{m_{B_1'}}) \tag{19}$$

where $\rho_{A_1B_1'}$ and $\rho_{A_1}^{m_{B_1'}}$ are the covariance matrices of $\gamma_{A_1B_1'}$ and $\gamma_{A_1}^{m_{B_1'}}$, respectively. $S(\rho_{A_1B_1'})$ is the function of the symplectic eigenvalues $\lambda_{1,2}$ of $\gamma_{A_1B_1'}$, which can be expressed as:

$$S(\rho_{A_1B_1'}) = G(\frac{\lambda_1 - 1}{2}) + G(\frac{\lambda_2 - 1}{2}) \tag{20}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and the symplectic eigenvalues $\lambda_{1,2}$ is:

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}] \tag{21}$$

and

$$
\begin{aligned}
A &= a^2 + b^2 - 2c^2 \\
B &= (ab - c^2)^2
\end{aligned}
\tag{22}
$$

Moreover, $S(\rho_{A_1}^{m_{B'_1}})$ is the function of the symplectic eigenvalues λ_3 of $\gamma_{A_1}^{m_{B'_1}}$, which will be given by:

$$S(\rho_{A_1}^{m_{B'_1}}) = G(\frac{\lambda_3 - 1}{2}) \tag{23}$$

the symplectic eigenvalues λ_3 is

$$\lambda_3 = a - \frac{c^2}{b+1} \tag{24}$$

To demonstrate the influence of the NLA on the secret key rate of the CV-MDI-QKD system, we simulate the relationship between the secret key rate of the system and the communication distance under different NLA gains in Figure 4. Here, we choose the optimal entanglement coefficient $\lambda = 0.7$ and consider that Charlie's detectors are perfect, that is, $\chi_{tot} = \chi_{line}$. Among all curves, the black curve with gain $g = 1$ represents the secret key rate of the original CV-MDI-QKD protocol. We can see that its performance is worse than the CV-MDI-QKD protocol with NLA in the same communication distance. Moreover, the result shows that after adding NLA to the CV-MDI-QKD system, the communication distance is longer than that of the original protocol. Furthermore, the communication distance and the secret key rate of the system will increase significantly with the increase in the NLA' s gain.

Moreover, the effect of the reverse reconciliation efficiency on the system is shown in Figure 5. We plot the relationship between the secret key rate and the communication distance with different reverse reconciliation efficiency and the NLA's gain. The result shows that the influence of the reverse reconciliation efficiency on the communication distance is relatively small when the gain of the NLA becomes larger. In short-distance communication, the greater the gain of NLA, the smaller the impact of the reverse reconciliation efficiency on the secret key rate.

Finally, to investigate the best gain to maximize the secret key rate of the CV-MDI-QKD system with NLA, we simulate the maximized secret key rate as a function of the gain of NLA. Assuming that the secure communication distance of the CV-MDI-QKD system is 60 km, we can see that the secret key rate of the system does not increase with the increase in the NLA's gain but has a maximum in Figure 6. The reason for this is that there is a successful amplification probability of NLA is $P_{nla} = 1/g^2$. With the increase in the NLA's gain, the secret key rate will reach the optimal value with a certain gain, and then the secret key rate will drop rapidly. The best gain under different modulation variances is also given by Figure 6, and it can be seen that the smaller the modulation variance, the greater the optimal gain required.

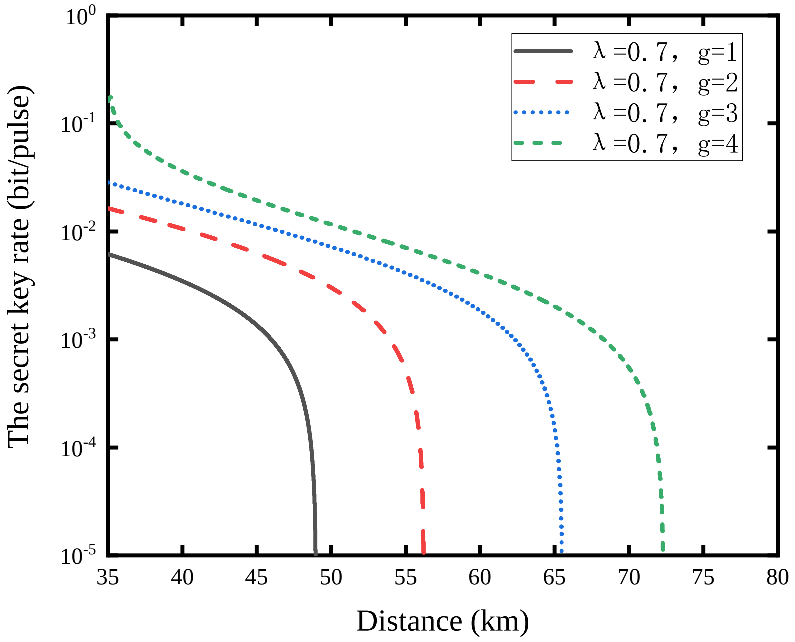

Figure 4. The secret key rate as a function of the communication distance. The entanglement coefficient $\lambda = 0.7$ and g is the gain of NLA. The other parameters are $\epsilon_A = \epsilon_B = 0.002$, $v_{el} = 0, \eta = 1$, and $\beta = 0.98$.

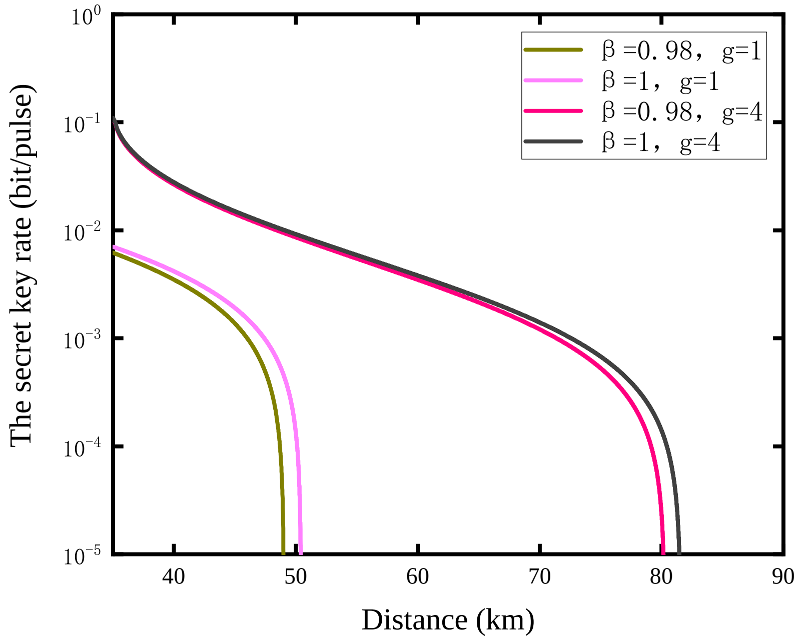

Figure 5. The secret key rate is a function of communication distance under different the efficiencies of reverse reconciliation and the gain of NLA. In the NLA-based CV-MDI-QKD protocol, when $g = 4$, the reverse reconciliation efficiency has little effect on the secret key rate of the system. The other parameters are $\lambda = 0.7, \epsilon_A = \epsilon_B = 0.002$, and $v_{el} = 0, \eta = 1$.

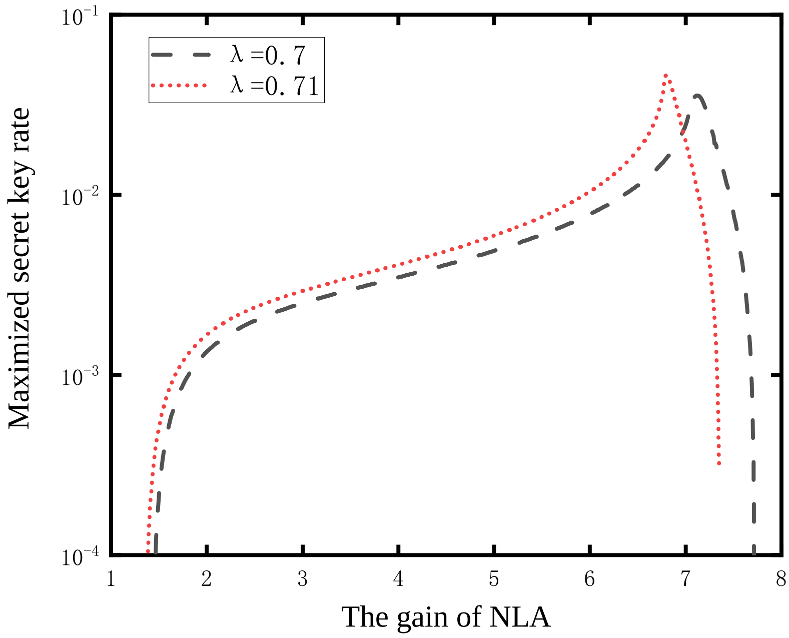

Figure 6. Maximized secret key rate as a function of the gain of NLA, with a probability of success $P_{nla} = 1/g^2$. The black dotted curve represent the secret key rate of the NLA-based CV-MDI-QKD protocol with $\lambda = 0.7$, and the red curve represents the secret key rate of the NLA-based CV-MDI-QKD protocol with $\lambda = 0.71$.

4. Conclusions

In this paper, we induced an NLA into the traditional CV-MDI-QKD protocol to improve the communication distance and the secret key rate of the system. The NLA is added to the output of the detector at Charlie's side first, and then, to investigate the performance of the system with NLA, we equate the E-B model of the CV-MDI-QKD system with NLA to the one-way CV-QKD protocol for which both Alice and Bob use heterodyne detectors and perform some related simulations. The research results show that NLA can increase the communication distance and secret key rate of the CV-MDI-QKD protocol. However, the secret key rate will reach the optimal value with a certain gain, and then the secret key rate will drop rapidly with the increase in the NLA's gain since there is a successful amplification probability of NLA. Moreover, we find that the influence of the reverse reconciliation efficiency on the communication distance is relatively small when the gain of the NLA becomes larger.

Author Contributions: Conceptualization, F.J. and L.K.; methodology, W.L.; software, C.H.; validation, F.J., L.K. and W.L.; formal analysis, F.J.; investigation, L.K.; resources, W.L.; data curation, F.J.; writing—original draft preparation, F.J.; writing—review and editing, W.L.; visualization, L.K.; supervision, C.H.; project administration, W.L.; funding acquisition, W.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grants No. 62001383) and the Shaanxi Provincial Department of Education 2019 Special Scientific Research Plan (Natural Science Special Project), 19JK0847.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

Acknowledgments: The author thanks the anonymous reviewers for their critical appraisal and constructive recommendations.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ghirardi, G.C.; Grassi, R.; Michelini, M. *Thinking Physics for Teaching*; Springer: Milan, Italy, 1995; pp. 329–334.
2. Soujaeff, A.; Nishioka, T.; Hasegawa, T.; Takeuchi, S.; Matsui, M. Quantum key distribution at 1550 nm using a pulse heralded single photon source. *Opt. Exp.* **2007**, *15*, 726–734. [CrossRef] [PubMed]
3. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [CrossRef]
4. Loeb, A.L. The Heisenberg Uncertainty Principle. *Am. J. Phys.* **1963**, *12*, 945. [CrossRef]
5. Shokeir, H. Increasing the Bit Density of a Quantum-Confinement Physically Unclonable Function. Master's Thesis, Master of Science, Lancaster University, Lancaster, UK, 2017.
6. Goorden, S.A.; Horstmann, M.; Mosk, A.P.; Škorić, B.; Pinkse, P.W.H. Quantum-secure authentication of a physical unclonable key. *Optica* **2014**, *1*, 421–424. [CrossRef]
7. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
8. Bennett, C.H.; Bessette, F.; Brassard, G.; Salvail, L.; Smolin, J.A. Experimental Quantum Cryptography. *J. Cryptol.* **1992**, *5*, 3–28. [CrossRef]
9. Wang, J.Y.; Yang, B.; Liao, S.K.; Zhang, L.; Shen, Q.; Hu, X.F.; Wu, J.C.; Yang, S.J.; Jiang, H.; Tang, Y.L. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nat. Photonics* **2013**, *7*, 387–393. [CrossRef]
10. Chong, S.K.; Hwang, T. Quantum key agreement protocol based on BB84. *Opt. Commun.* **2010**, *283*, 1192–1195. [CrossRef]
11. Walk, N.; Ralph, T.C.; Symul, T.; Ping, K.L. Security of Continuous Variable Quantum Cryptography. *Phys. Rev. A* **2013**, *87*, 20303. [CrossRef]
12. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **1999**, *61*, 022309. [CrossRef]
13. Grosshans, F.; Assche, G.V.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef]
14. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
15. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.; Ralph, T.; Shapiro, J.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2011**, *84*, 621–669. [CrossRef]
16. Berta, M.; Christandl, M.; Colbeck, R.; The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **2010**, *6*, 659–662. [CrossRef]
17. Jain, N.; Stiller, B.; Khan, I.; Makarov, V.; Marquardt,C.; Leuchs,G. Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse. *Phys. Rev. A* **2009**, *80*, 84–85.
18. Renner, R.; Cirac, J.I.; de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Phys. Rev. Lett.* **2009**, *102*, 110504. [CrossRef]
19. Leverrier, A. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.* **2013**, *110*, 030502. [CrossRef]
20. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 7. [CrossRef]
21. Leverrier, A. Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction. *Phys. Rev. Lett.* **2017**, *118*, 200501. [CrossRef] [PubMed]
22. Liu, W.Q.; Peng, J.Y.; Peng, H.; Duan, H.; Zeng, G.H. Monitoring of continuous-variable quantum key distribution system in real environment. *Opt. Exp.* **2017**, *25*, 19429. [CrossRef]
23. Bugge, A.N.; Sauge, S.; Ghazali, A.M.M.; Skaar, J.; Lydersen, L.; Makarov, V. Laser Damage Helps the Eavesdropper in Quantum Cryptography. *Phys. Rev. Lett.* **2014**, *112*, 070503. [CrossRef]
24. Huang, A.Q.; Navarrete, Á.; Sun, S.H.; Chaiwongkhot, P.; Curty, M.; Makarov, V. Laser-Seeding Attack in Quantum Key Distribution. *Phys. Rev. Appl.* **2019**, *12*, 064043. [CrossRef]
25. Huang, A.Q.; Li, R.; Egorov, V.; Tchouragoulov, S.; Kumar, K.; Makarov, V. Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution. *Phys. Rev. Appl.* **2020**, *13*, 034017. [CrossRef]
26. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313. [CrossRef]
27. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **2013**, *88*, 022339. [CrossRef]
28. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Liang, L.M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A* **2013**, *87*, 052309. [CrossRef]
29. Huang, J.Z.; Weedbrook, C.; Yin, Z.Q.; Wang, S.; Li, H.W.; Chen, W.; Guo, G.C.; Han, Z.F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329. [CrossRef]

30. Kunz-Jacques, S.; Jouguet, P. Robust shot-noise measurement for continuous-variable quantum key distribution. *Phys. Rev. A* **2015**, *91*, 022307. [CrossRef]
31. Liu, W.Q.; Peng, J.Y.; Qi, J.; Cao, Z.W.; He, C. Imperfect basis choice in continuous-variable quantum key distribution. *Laser Phys. Lett.* **2020**, *17*, 055203. [CrossRef]
32. Cives-Esclop, A.; Luis, A.; Sánchez-Soto, L.L. Unbalanced homodyne detection with a weak local oscillator. *Opt. Commun.* **2000**, *175*, 153–161. [CrossRef]
33. Kühn, B.; Vogel, W. Unbalanced Homodyne Correlation Measurements. *Phys. Rev. Lett.* **2016**, *116*, 163603. [CrossRef]
34. Huang, Y.; Zhang, Y.; Xu, B.;Huang, L.; Yu, S. A modified practical homodyne detector model for continuous-variable quantum key distribution: Detailed security analysis and improvement by the phase-sensitive amplifier. *J. Phys. B-At. Mol. Opt. Phys.* **2020**, *54*, 015503. [CrossRef]
35. Almeida, M.; Pereira, D.; Facão, M.; Pinto, A. N.; Silva, N.A. Impact of imperfect homodyne detection on measurements of vacuum states shot noise. *Opt. Quantum Electron.* **2020**, *52*, 503. [CrossRef]
36. Wallentowitz, S.; Vogel, W. Unbalanced homodyning for quantum state measurements. *Phys. Rev. A* **1996**, *53*, 4528. [CrossRef]
37. Silva, N.A.; Pereira, D.; Muga, N.J.; Pinto, A.N. Practical imperfections affecting the performance of CV-QKD based on coherent detection. In Proceedings of the 2020 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 19–23 July 2020; pp.1–4.
38. Li, Z.; Zhang, Y.; Xu, F.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052301. [CrossRef]
39. Papanastasiou, P.; Ottaviani, C.; Pirandola, S. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Phys. Rev. A* **2017**, *96*, 4. [CrossRef]
40. Tang, Z.; Liao, Z.; Xu, F.; Qi, B.; Qian, L.; Lo, H.K. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2014**, *112*, 190503. [CrossRef]
41. Ralph, T.C.; Lund, A.P. Nondeterministic noiseless linear amplification of quantum systems. *Am. Inst. Phys.* **2009**, *1110*, 155–160.
42. Blandino, R.; Leverrier, A.; Barbieri, M.; Etesse, J.; Tualle-Brouri, R. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A* **2014**, *86*, 1.
43. Levenson, J.A.; Abram, I.; Rivera, T.; Grangier, P. Reduction of quantum noise in optical parametric amplification. *JOSA B* **1993**, *10*, 2233–2238. [CrossRef]
44. Ralph, T.C. Quantum error correction of continuous-variable states against gaussian noise. *Phys. Rev. A* **2011**, *84*, 022339. [CrossRef]
45. Li, Y.; Huang, P.; Li, D.; Zhou, Y.; Zeng, G. Security analysis of practical continuous-variable quantum key distribution using a heralded noiseless amplifier. *Int. J. Theor. Phys.* **2019**, *58*, 2392–2406. [CrossRef]
46. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343. [CrossRef]