

Article

Continuous-Variable Quantum Key Distribution Based on Heralded Hybrid Linear Amplifier with a Local Local Oscillator

Yin Li, Yijun Wang, Yun Mao *, Weishao Peng *, Di Jin * and Ying Guo 

School of Automation, Central South University, Changsha 410083, China; liyin@csu.edu.cn (Y.L.); xxywyj@csu.edu.cn (Y.W.); yingguo@csu.edu.cn (G.Y.)

* Correspondence: sduoying@gmail.com (Y.M.); pws315@csu.edu.cn (W.P.); dijin95@csu.edu.cn (D.J.)

Abstract: An improved continuous variable quantum key distribution (CVQKD) approach based on a heralded hybrid linear amplifier (HLA) is proposed in this study, which includes an ideal deterministic linear amplifier and a probabilistic noiseless linear amplifier. The CVQKD, which is based on an amplifier, enhances the signal-to-noise ratio and provides for fine control between high gain and strong noise reduction. We focus on the impact of two types of optical amplifiers on system performance: phase sensitive amplifiers (PSA) and phase insensitive amplifiers (PIA). The results indicate that employing amplifiers, local local oscillation-based CVQKD systems can enhance key rates and communication distances. In addition, the PIA-based CVQKD system has a broader application than the PSA-based system.

Keywords: continuous-variable quantum key distribution; optical amplifier; local local oscillator



Citation: Li, Y.; Wang, Y.; Mao, Y.; Peng, W.; Jin, D.; Guo, Y. Continuous-Variable Quantum Key Distribution Based on Heralded Hybrid Linear Amplifier with a Local Local Oscillator. *Entropy* **2021**, *23*, 1395. <https://doi.org/10.3390/e23111395>

Academic Editors: Stefano Olivares, Marcin Jarzyna and Vladyslav Usenko

Received: 12 September 2021
Accepted: 20 October 2021
Published: 24 October 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

Quantum key distribution (QKD) provides a secret key sharing method guaranteed by quantum mechanics for trusted communication parties, namely Alice and Bob, in the presence of potential eavesdroppers [1–3]. Currently, there are two methods available for key distribution: discrete variable (DV) QKD [4,5] and continuous variable (CV) QKD [6–9]. Among them, the CVQKD has two main advantages. On the one hand, it circumvents the drawbacks of single-photon counting. On the other hand, it ensures that standard optical communication components are compatible [10,11]. The unconditional security of CVQKD has been established in the information-theoretical in both the asymptotic case [12,13] and the finite-size regime [14–16] to against general collective eavesdropping attacks.

The strong local oscillator (LO) for coherent detection as an important part of the CVQKD system can be employed as a filter to effectively suppress noise. However, the imperfections of the actual CVQKD system have led to potential loopholes and endangered the security of the communication system. Since Eve performs intercept-resend attacks by manipulating the LO, almost all of the attacks are related to the LO [17–21]. The CVQKD system based on local local oscillation (LLO), for example, prevents LO-related attacks by sending LO directly to the receiving end [22–25].

The transmission distance of CVQKD is currently limited compared to discrete variable systems, making it unsuitable for long-distance distribution. In the detection process, a heralded noiseless linear amplifier (NLA) is an excellent instrument for strengthening the amplitude of the coherent state while keeping the starting noise level low [26–29]. The practicality of this device has been proven in recent years, providing convincing evidence of the theory [30–35]. Furthermore, in Bob's quadrature measurement, the defects associated with practical detectors cause a secret key rate constraint [36]. To compensate for this weakness, optical amplifier compensation technology offers a viable solution that can also improve transmission distance in specific situations [37–39].

We propose a CVQKD scheme based on LLO in this paper by placing an HLA at the detection end, which consists of a predictive measurement (MB)-based NLA and an

optimal deterministic linear amplifier (DLA) that can amplify the amplitude of the coherent state while maintaining low noise and a high success rate. The signal-to-noise ratio is amplified by the NLA part, while the signal and success probability are amplified by the DLA part. In addition, we take into account the NLA’s restrictions. The addition of a hybrid amplifier to the LLO-based CVQKD protocol efficiently increases the key rate and the maximum secure transmission distance according to simulation results.

The paper is organized as follows. In Section 2, we describe the LLO-CVQKD system based on optical amplifiers. In Section 3, we conduct a theoretical analysis of excess noise. We performed a detailed analysis in Section 4, comparing the performance of practical systems that implement two different types of optical amplifiers. Finally, we conclude the paper in Section 5.

2. Description of the LLO-CVQKD Scheme Based on Optical Amplifiers

In this section, we introduce the LLO-CVQKD scheme by using heralded HLA. As shown in Figure 1, Alice randomly chooses two Gaussian random variables (with a mean of zero and a variance of V_A), generates a coherent state to modulate the continuous waves emitted by the laser [40,41]. An arbitrary phase rotation is generated by a quantum channel to change the states. To restore the original signal, a relatively strong phase reference pulse is alternately sent with the quantum signal. The beam then passes through the optical channel. At Bob’s side, a heralded HLA is placed in the signal beam to improve system performance. Besides, Bob performs optical heterodyne detection to measure quadrature x and p .

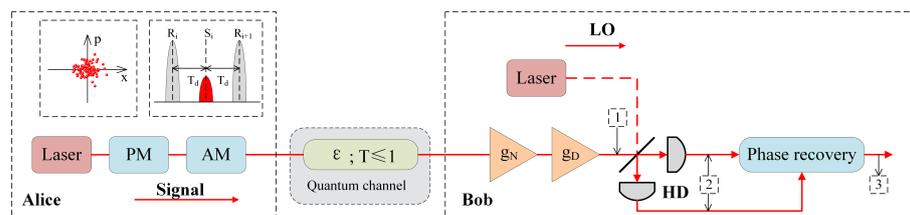


Figure 1. System layout of LLO-CVQKD scheme based on a heralded HLA. The signal light is in red (gray) solid line, and the local oscillator light is in red (gray) dashed line. LO, local oscillator; AM, amplitude modulator; PM, phase modulator; HD, heterodyne detection.

2.1. Amplifier Compensation Scheme

The above-mentioned heralded HLA is composed of a MB-NLA and an optimal DLA. In theory, NLA can increase the amplitude of the coherent state while keeping the original noise level constant [26]. The output after an initial channel and NLA action, given any quantum state $\hat{\rho}_{in} = \int d^2\gamma P_{in}(\gamma)|\gamma\rangle\langle\gamma|$, can be represented as

$$\hat{\rho}_{out}^{NLA} \propto \int d^2\gamma P_{in}(\gamma)\hat{\sigma}(\gamma)e^{|\gamma|^2 T \frac{(g_N^2-1)(1-\lambda_{ch}^2)}{1-g_N^2\lambda_{ch}^2}}, \tag{1}$$

where g_N describes the operator of NLA. The initial channel transforms the coherent state of the mean amplitude γ into the thermal state of the parameter λ_{ch} and the average amplitude $\sqrt{T}\gamma$. The displaced thermal state can be expressed by

$$\hat{\sigma}(\gamma) = \hat{D}(g_N\sqrt{T}\gamma)\hat{\rho}_{th}(g_N\lambda_{ch})\hat{D}^\dagger(g_N\sqrt{T}\gamma), \tag{2}$$

of parameter $g\lambda_{ch}$ and mean amplitude $g_N\sqrt{T}\gamma$, where the gain \tilde{g} is given by

$$\tilde{g}_N = g_N \frac{1 - \lambda_{ch}^2}{1 - g_N^2 \lambda_{ch}^2}. \tag{3}$$

We mainly consider two modes of DLA, phase-sensitive amplifiers (PSA) and phase-insensitive amplifiers (PIA) [42–45]. PSA ideally allows noiseless amplification of a selected

quadrature. The structure of PSA is shown in Figure 2a. X_B^i and P_B^i correspond to the outputs at point i in Figure 1. The output of the amplifier is written as

$$\begin{bmatrix} X_B^0 \\ P_B^0 \end{bmatrix} = \begin{bmatrix} \sqrt{g_D} & 0 \\ 0 & 1/\sqrt{g_D} \end{bmatrix} \begin{bmatrix} X_A \\ P_A \end{bmatrix} \tag{4}$$

where g_D is the amplifier coefficient of DLA. Besides, the noise introduced by the real amplifier is ignored here.

PIA is a non-degenerate optical parametric amplifier whose structure is shown in Figure 2b. It consists of a noiseless amplifier and a two-mode squeezed vacuum (EPR) state of variance N_{EPR} , which is used to simulate the inherent noise of the amplifier. The output of PIA is written as

$$\begin{bmatrix} X_B^0 \\ P_B^0 \end{bmatrix} = \begin{bmatrix} X_A & X_I \\ P_A & P_I \end{bmatrix} \begin{bmatrix} \sqrt{g_D} \\ \sqrt{g_D - 1} \end{bmatrix}, \tag{5}$$

where I is an idler mode that is ideally in a vacuum state or in a state featuring a noise variance $V_I = N_{EPR} > 1$.

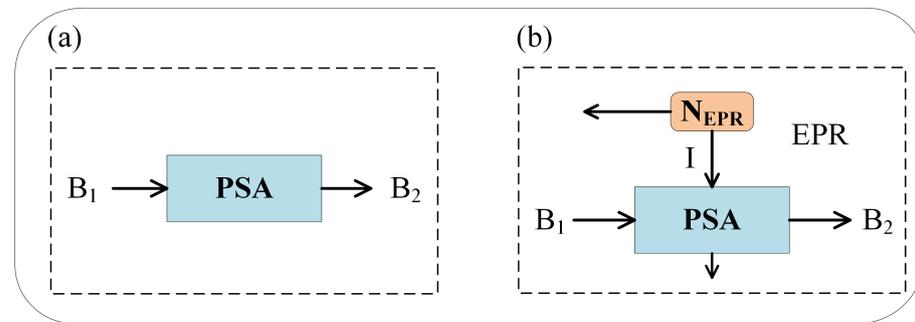


Figure 2. Two different amplifier model. (a) Model for a phase-sensitive amplifier. (b) Model for a phase-insensitive amplifier.

2.2. Phase Recovery Scheme

Bob’s measurement results are described by

$$\begin{bmatrix} X_B^1 \\ P_B^1 \end{bmatrix} = \begin{bmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{bmatrix} \begin{bmatrix} X_B^0 \\ P_B^0 \end{bmatrix} + \begin{bmatrix} N_X \\ N_P \end{bmatrix}, \tag{6}$$

where φ respects the phase drift in a quantum channel. N_X and N_P are independent and identically distributed (i.i.d.) Gaussian noises.

Assuming that the channel drift is known, Bob’s measurement can be corrected as

$$\begin{bmatrix} X_B^2 \\ P_B^2 \end{bmatrix} = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} \begin{bmatrix} X_B^1 \\ P_B^1 \end{bmatrix}, \tag{7}$$

Based on PSA scheme, the final output can be obtained according to Equations (4), (6) and (7), which can easy to show

$$\begin{bmatrix} X_B^2 \\ P_B^2 \end{bmatrix} = \begin{bmatrix} \sqrt{g_D} & 0 \\ 0 & 1/\sqrt{g_D} \end{bmatrix} \begin{bmatrix} X_A \\ P_A \end{bmatrix} + \begin{bmatrix} N'_X \\ N'_P \end{bmatrix}, \tag{8}$$

where noise terms can be expressed as

$$\begin{bmatrix} N'_X \\ N'_P \end{bmatrix} = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} \begin{bmatrix} N_X \\ N_P \end{bmatrix}. \tag{9}$$

Based on PIA scheme, the final output can be obtained according to Equations (5)–(7), which can easily show

$$\begin{bmatrix} X_B^2 \\ P_B^2 \end{bmatrix} = \sqrt{g_D} \begin{bmatrix} X_A \\ P_A \end{bmatrix} + \begin{bmatrix} N_X' \\ N_P' \end{bmatrix}, \quad (10)$$

where noise terms can be described by

$$\begin{bmatrix} N_X' \\ N_P' \end{bmatrix} = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} \begin{bmatrix} N_X \\ N_P \end{bmatrix} + \sqrt{g_D - 1} \begin{bmatrix} X_I \\ P_I \end{bmatrix}. \quad (11)$$

Next, calculate the phase shift. Assume that the phase drift is slow enough to remain constant over the frame time of ΔT . Since Alice alternately sends the quantum signal and the reference pulse, the phase shift of the signal pulse can be calculated from the phase shift of the reference pulse [46]. The phase of the reference pulse can be expressed as

$$\varphi_R^i = -\tan^{-1} \frac{P_R^i}{X_R^i}. \quad (12)$$

The phase shift of the signal pulse can be calculated as

$$\varphi_S^i = \frac{\varphi_R^i + \varphi_R^{i+1}}{2} = \varphi_R^i + 2\pi f_d T_d, \quad (13)$$

where $f_i = (\varphi_R^{i+1} - \varphi_R^i / 4\pi T_d)$ is the frequency difference between two adjacent reference pulsed lasers in a short time.

3. Excess Noise Analysis

The excess noise analysis of the LLO CV-QKD system based on the heralded HLA is shown in this section. Although the signal's pulse phase was approximated using the reference pulse phase in the preceding section, it was not exact enough, and there were inaccuracies. In the phase recovery phase, the excess noise induced by the uncertainty of φ can be described as

$$\varepsilon_\varphi = V_A \sigma_\varphi, \quad (14)$$

where σ_φ is the variance of noise generated by the uncertainty of phase φ . The noise variance σ_φ is expressed as

$$\sigma_\varphi = \frac{1}{2} \{ \langle (\Delta\varphi_S T_d)^2 \rangle + \langle (\Delta\varphi_L T_d)^2 \rangle \}, \quad (15)$$

where $\langle (\Delta\varphi_S T_d)^2 \rangle$ and $\langle (\Delta\varphi_L T_d)^2 \rangle$ are the phase noise of signal light and auxiliary light, respectively. T_d represents the time interval between the signal pulse and the reference pulse (see Figure 1). Assuming that the laser phase at $t = 0$ is φ_0 , the phase noise $\varphi(t)$ can be modeled as a Gaussian random variable with a mean of 0 and a variance of

$$\langle (\Delta\varphi_S t)^2 \rangle = \frac{2t}{\alpha}, \quad (16)$$

where $\alpha \simeq \frac{1}{\pi\Delta f}$ respects the coherence time of the laser. Δf is the linewidth of α .

4. Security Analysis

This section will analyze the impact of the amplifier on the performance of the LLO-CVQKD system. Our simulation is based on the security of GMCS QKD system given in Refs. [14,47].

An NLA-based CV-QKD system with a variance $V(\delta) = \frac{1+\delta^2}{1-\delta^2}$, channel transmittance $T = 10^{-\alpha L/10}$, and excess noise ε can be transformed into another typical CV-QKD system with variance $V(\delta_N) = \frac{1+\delta_N^2}{1-\delta_N^2}$, channel transmittance T_N , excess noise ε_N , and loss coefficient

$\alpha = 0.2 \text{ dBkm}^{-1}$. The parameter expression that has been equivalently converted is as follows:

$$\begin{aligned} \delta_N &= \delta \sqrt{\frac{(g_N^2 - 1)(\epsilon - 2)T - 2}{(g_N^2 - 1)\epsilon T - 2}}, \\ T_N &= \frac{g^2 T}{(g_N^2 - 1)T[\frac{1}{4}(g_N^2 - 1)(\epsilon - 2)\epsilon T - \epsilon + 1] + 1}, \\ \epsilon_N &= \epsilon - \frac{1}{2}(g^2 - 1)(\epsilon - 2)\epsilon T. \end{aligned} \tag{17}$$

When the parameters in the CVQKD system above satisfy a specified condition, the system can be viewed as equivalent. The limitations are written as

$$0 \leq \delta_N < 1 \Rightarrow 0 \leq \delta < \left(\sqrt{\frac{(g_N^2 - 1)(\epsilon - 2)T - 2}{(g_N^2 - 1)\epsilon T - 2}}\right)^{-1}. \tag{18}$$

Figure 3 shows the limitations of VA taking under various settings when the excess noise is equal to 0.01. In addition the success probability of the amplifier is taken into account. According to Ref. [27], the upper bound on the amplifier success probability is

$$P_{\text{success}} \leq \frac{1}{g_N^2}. \tag{19}$$

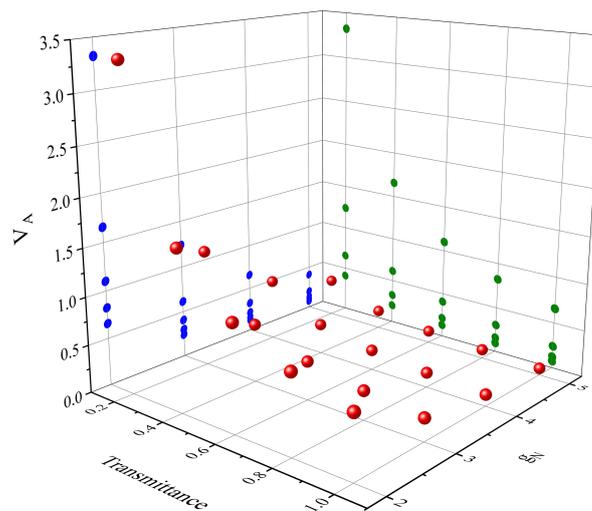


Figure 3. Maximum value of the modulation variance. Five cases at different transmittance (from $T = 0.2$ to 1 in steps of 0.2) and four amplification factor of NLA (from $g_N = 2$ to 5 in steps of 1) are investigated.

The secure key rate with finite-size effect is given by

$$R = \frac{n P_{\text{success}}}{N} [\beta I_{AB} - \chi_{BE} - \Delta(n)], \tag{20}$$

where I_{AB} is defined as the Shannon mutual information of Alice and Bob, χ_{BE} respects the upper bound of the Holevo information between Eve and Bob, $\Delta(n)$ is related to the security of the privacy amplification and β is the reconciliation efficiency. The privacy amplification $\Delta(n)$ is given by

$$\Delta(n) \equiv (2 \dim \mathcal{H}_X + 3) \sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n} (1 + \epsilon_{PA}), \tag{21}$$

where $\bar{\epsilon}$ and ϵ_{PA} are the smoothing parameter and failure probability of the privacy amplification, respectively. \mathcal{H}_X is the Hilbert space corresponding to the variable X used in the raw key. The square-root term in $\Delta(n)$ actually corresponds to the pace with which the smooth min-entropy of an independently and identically distributed (i.i.d.) state approaches the von Neumann entropy. Indeed, the smooth min-entropy of an i.i.d. state is identical to its von Neumann entropy only at the asymptotic limit. The second term is proportional to the privacy amplification procedure’s failure probability.

The Shannon mutual information of Alice and Bob, as well as the Holevo information of Eve and Bob, differ depending on the amplifier type. The CVQKD scheme based on PSA is first studied. The detection-added noise of quadrature X and P is considered separately, as shown below

$$\begin{aligned} \chi_{PSA}^x &= \frac{1 + (1 + \eta) + 2\vartheta_{el}}{g_D \eta}, \\ \chi_{PSA}^p &= \frac{g_D(1 + (1 + \eta) + 2\vartheta_{el})}{\eta}, \end{aligned} \tag{22}$$

where ϑ_{el} is the detector electronics noise, η is detector efficiency. The total noise is defined as

$$\chi_{tot}^{x,p} = \chi_{line} + \chi_{PSA}^{x,p}, \tag{23}$$

where $\chi_{line} = 1/T_N - 1 + \epsilon_N$ is the total channel-added noise. The Shannon mutual information of Alice and Bob is written by [48]

$$I_{AB} = \log_2 \frac{V_B}{V_{B|A}}, \tag{24}$$

where $V_B = \frac{\eta T_N}{2} [(V_N + \chi_{tot}^x)(V_N + \chi_{tot}^p)]^{1/2}$, and $V_{B|A} = \frac{\eta T_N}{2} [(1 + \chi_{tot}^x)(1 + \chi_{tot}^p)]^{1/2}$. The Holevo information between Eve and Bob is defined as [12,13]

$$\chi_{BE} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^5 G\left(\frac{\lambda_i - 1}{2}\right), \tag{25}$$

where $G(x) = (x + 1)\log_2(x + 1) - x\log_2 x$. The symplectic eigenvalues $\lambda_{1,2}$ are given by

$$\lambda_{1,2} = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}], \tag{26}$$

where $A = V_N^2(1 - 2T_N) + 2T_N + T_N^2(V_N + \chi_{line})^2$ and $B = T_N^2(V\chi_{line} + 1)^2$. The symplectic eigenvalues $\lambda_{3,4}$ are expressed as

$$\lambda_{3,4} = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}], \tag{27}$$

where

$$C_{PAS} = \frac{A\chi_{PSA}^x\chi_{PSA}^p + B + 1 + (\chi_{PSA}^x + \chi_{PSA}^p)(V_N\sqrt{B} + T_N(V_N + \chi_{line})) + 2T_N(V_N^2 - 1)}{(T_N(V_N + \chi_{tot}^x))(T_N(V_N + \chi_{tot}^p))}, \tag{28}$$

and

$$D_{PSA} = \left(\frac{V_N + \sqrt{B}\chi_{PSA}^x}{T_N(V_N + \chi_{tot}^x)}\right)\left(\frac{V_N + \sqrt{B}\chi_{PSA}^p}{T(V_N + \chi_{tot}^p)}\right). \tag{29}$$

The last eigenvalue is $\lambda_5 = 1$.

Then, the LLO-CVQKD scheme based on PIA is analyzed. The detection-added noise is shown as

$$\chi_{PIA} = \frac{1 + (1 - \eta) + 2\vartheta_{el} + N_{EPR}(g - 1)\eta}{g\eta}, \tag{30}$$

where N_{EPR} is the variance of the EPR state to model the amplifier’s inherent noise. A similar change was made to the Shannon information. We now have

$$\begin{aligned} V_B &= \eta T_N(V + \chi_{tot})/2, \\ V_{B|A} &= \eta T_N(1 + \chi_{tot})/2. \end{aligned} \tag{31}$$

χ_{BE} is calculated from

$$\chi_{BE} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^7 G\left(\frac{\lambda_i - 1}{2}\right), \tag{32}$$

The parameters $(\lambda_{1,2,3,4})$ are calculated according to Equations (26) and (27), while $\lambda_{5,6,7} = 1$. The parameters $(\lambda_{3,4})$ are calculated from

$$C_{PIA} = \frac{A\chi_{PIA}^2 + B + 1 + 2\chi_{PIA}(V_N\sqrt{B} + T_N(V_N + \chi_{line})) + 2T_N(V_N^2 - 1)}{(T_N(V_N + \chi_{tot}))^2}, \tag{33}$$

and

$$D_{PIA} = \left(\frac{V_N + \sqrt{B}\chi_{PIA}}{T_N(V_N + \chi_{tot})}\right)^2. \tag{34}$$

The secret key rate as a function of transmission distance is shown in Figure 4 using HLA with PSA. For simulation, the parameters stated in Table 1 are utilized, which is in accordance with the most advanced experimental methods [22,24]. The secure communication distance increases as the amplifier coefficient g_N and g_D increases when the modulation variance $V_A = 0.6$. In terms of both key rate and distance, NLA-based schemes perform better than PSA-based systems. When the solution is based on HLA, the performance is optimal.

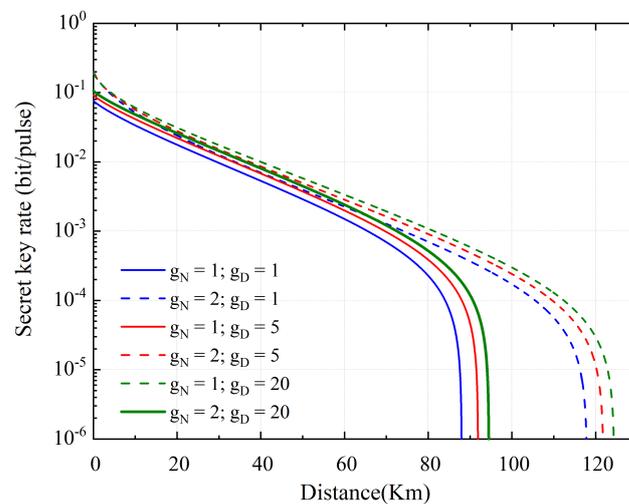


Figure 4. The secret key rate as a function of transmission distance based on PSA. Blue line, red line, and green line correspond, respectively, to a value of the amplifier coefficient of $g_D = 1$ (initial), $g_D = 5$, and $g_D = 20$. Full lines and dashed lines correspond to two cases where the number of g_N links is 1 and 2, respectively.

The secret key rate as a function of transmission distance is plotted in Figure 5 using HLA with PIA. The PIA-based LLO-CVQKD is similar to the psa-based LLO-CVQKD. The system performance improves as the amplification parameters are increased. When N_{EPR} is increased, however, the system performance degrades due to an increase in the introduced noise.

Table 1. The parameters to simulate the secret key rate.

Parameter	Value	Description
V_A	0.6	Modulation variance
β	98%	Reconciliation efficiency
η	0.6	Detector efficiency
ν_{el}	0.05	Detector noise
σ_φ	0.04	Phase noise variance
$\bar{\epsilon}, \epsilon_{PA}$	10^{-20}	Security parameter
N	10^{10}	Total photons
$\frac{n}{N}$	$\frac{1}{2}$	Photon ratio used for key

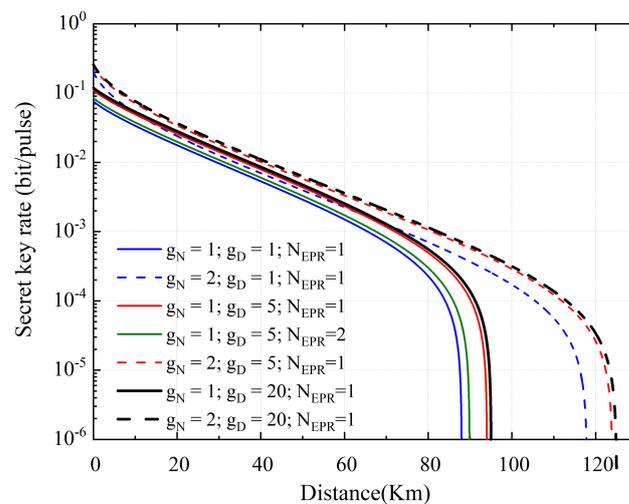


Figure 5. The secret key rate as a function of transmission distance based on PIA. Blue line, red line, and black line correspond, respectively, to a value of the amplifier coefficient of $g_D = 1$ (initial), $g_D = 5$, and $g_D = 20$. The green line represents the case of $N_{EPR} = 2$. Full lines and dashed lines correspond to two cases where the number of g_N links is 1 and 2, respectively.

5. Conclusions

In this study, we offer a practical LLO-CVQKD system based on an HLA, which consists of an MB-NLA and a DLA, with the latter compensating for the former’s signal-to-noise ratio degradation. Two HLA schemes based on two separate DLAs, a phase-sensitive amplifier and a phase-insensitive amplifier, were analyzed to verify system performance. The system’s noise was initially studied, with all conceivable consequences taken into account. Following that, simulations were run to determine the situations under which the NLA is applicable. Finally, the system’s performance was assessed utilizing two alternative amplifier methods. The results demonstrated that HLAs based on various forms of DLA can help improve system performance. Furthermore, when compared to the PSA-based scheme, the PIA-based strategy performs better. Because the majority of the simulation parameters were derived from existing experiments, our research was extremely practical.

In addition, we supplemented the scheme in Refs. [28,29]. Ref. [28] proposes a basic CVQKD scheme for Gaussian modulated coherent states based on hybrid amplifiers. Ref. [29] proposes a CVQKD scheme based on a four-state modulation scheme using a hybrid amplifier under seawater channel conditions. Our scheme is mainly based on the improvement of Ref. [28]. We mainly analyze the performance of the HLA scheme in the case of local local oscillation. Furthermore, the effective case of HLA is analyzed.

Author Contributions: Conceptualization, Y.W.; data curation, W.P.; formal analysis, Y.M.; investigation, Y.L.; methodology, Y.M.; resources, Y.W.; software, Y.L.; supervision, Y.G.; validation, Y.G.; visualization, W.P.; writing—original draft, Y.L.; writing—review and editing, D.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the National Natural Science Foundation of China (Grant Nos. 61871407, 61801522).

Data Availability Statement: The data used are included in the article.

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

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [[CrossRef](#)]
2. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [[CrossRef](#)]
3. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **2020**, *12*, 1012–1236. [[CrossRef](#)]
4. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [[CrossRef](#)]
5. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2014**, *8*, 595–604. [[CrossRef](#)]
6. Braunstein, S.L.; van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513–577. [[CrossRef](#)]
7. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621–669. [[CrossRef](#)]
8. Huang, D.; Huang, P.; Lin, D.; Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **2016**, *6*, 19201. [[CrossRef](#)]
9. Zhong, H.; Zou, S.; Huang, D.; Guo, Y. Continuous-variable quantum key distribution coexisting with classical signals on few-mode fiber. *Opt. Express* **2021**, *29*, 14486–14504. [[CrossRef](#)]
10. Weedbrook, C.; Lance, A.M.; Bowen, W.P.; Symul, T.; Ralph, T.C.; Lam, P.K. Quantum Cryptography Without Switching. *Phys. Rev. Lett.* **2004**, *93*, 170504. [[CrossRef](#)]
11. Guo, Y.; Xie, C.; Liao, Q.; Zhao, W.; Zeng, G.; Huang, D. Entanglement-distillation attack on continuous-variable quantum key distribution in a turbulent atmospheric channel. *Phys. Rev. A* **2017**, *96*, 022320. [[CrossRef](#)]
12. García-Patrón, R.; Cerf, N.J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [[CrossRef](#)]
13. Navascués, M.; Grosshans, F.; Acín, A. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [[CrossRef](#)]
14. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343. [[CrossRef](#)]
15. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.B.; Tomamichel, M.; Werner, R.F. Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks. *Phys. Rev. Lett.* **2012**, *109*, 100502. [[CrossRef](#)] [[PubMed](#)]
16. Leverrier, A. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Phys. Rev. Lett.* **2015**, *114*, 070501. [[CrossRef](#)]
17. 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](#)]
18. 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](#)]
19. 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](#)]
20. 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](#)]
21. Qin, H.; Kumar, R.; Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *94*, 012325. [[CrossRef](#)]
22. Qi, B.; Lougovski, P.; Pooser, R.; Grice, W.; Bobrek, M. Generating the Local Oscillator “Locally” in Continuous-Variable Quantum Key Distribution Based on Coherent Detection. *Phys. Rev. X* **2015**, *5*, 041009. [[CrossRef](#)]
23. Soh, D.B.S.; Brif, C.; Coles, P.J.; Lütkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar, M. Self-Referenced Continuous-Variable Quantum Key Distribution Protocol. *Phys. Rev. X* **2015**, *5*, 041010. [[CrossRef](#)]
24. Huang, D.; Huang, P.; Lin, D.; Wang, C.; Zeng, G. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.* **2015**, *40*, 3695–3698. [[CrossRef](#)] [[PubMed](#)]
25. Wu, X.; Wang, Y.; Guo, Y.; Zhong, H.; Huang, D. Passive continuous-variable quantum key distribution using a locally generated local oscillator. *Phys. Rev. A* **2021**, *103*, 032604. [[CrossRef](#)]
26. Ralph, T.C.; Lund, A.P. Nondeterministic Noiseless Linear Amplification of Quantum Systems. *AIP Conf. Proc.* **2009**, *1110*, 155–160. [[CrossRef](#)]
27. 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. A* **2012**, *86*, 012327. [[CrossRef](#)]

28. Zhou, J.; Shi, R.; Feng, Y.; Shi, J.; Guo, Y. Enhancing continuous variable quantum key distribution with a heralded hybrid linear amplifier. *J. Phys. A Math. Theor.* **2019**, *52*, 245303. [[CrossRef](#)]
29. Xiang, Y.; Wang, Y.; Ruan, X.; Zuo, Z.; Guo, Y. Improving the discretely modulated underwater continuous-variable quantum key distribution with heralded hybrid linear amplifier. *Phys. Scr.* **2021**, *96*, 065103. [[CrossRef](#)]
30. Ferreyrol, F.; Barbieri, M.; Blandino, R.; Fossier, S.; Tualle-Brouri, R.; Grangier, P. Implementation of a Nondeterministic Optical Noiseless Amplifier. *Phys. Rev. Lett.* **2010**, *104*, 123603. [[CrossRef](#)]
31. Ferreyrol, F.; Blandino, R.; Barbieri, M.; Tualle-Brouri, R.; Grangier, P. Experimental realization of a nondeterministic optical noiseless amplifier. *Phys. Rev. A* **2011**, *83*, 063801. [[CrossRef](#)]
32. Barbieri, M.; Ferreyrol, F.; Blandino, R.; Tualle-Brouri, R.; Grangier, P. Nondeterministic noiseless amplification of optical signals: a review of recent experiments. *Laser Phys. Lett.* **2011**, *8*, 411–417. [[CrossRef](#)]
33. Zavatta, A.; Fiurášek, J.; Bellini, M. A high-fidelity noiseless amplifier for quantum light states. *Nat. Photonics* **2011**, *5*, 52–56. [[CrossRef](#)]
34. Xiang, G.Y.; Ralph, T.C.; Lund, A.P.; Walk, N.; Pryde, G.J. Heralded noiseless linear amplification and distillation of entanglement. *Nat. Photonics* **2010**, *4*, 316–319. [[CrossRef](#)]
35. Usuga, M.A.; Müller, C.R.; Wittmann, C.; Marek, P.; Filip, R.; Marquardt, C.; Leuchs, G.; Andersen, U.L. Noise-powered probabilistic concentration of phase information. *Nat. Physics* **2010**, *6*, 767–771. [[CrossRef](#)]
36. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **2000**, *61*, 022309. [[CrossRef](#)]
37. Leonhardt, U.; Paul, H. High-Accuracy Optical Homodyne Detection with Low-Efficiency Detectors: “Pre-amplification” from Antisqueezing. *Phys. Rev. Lett.* **1994**, *72*, 4086–4089. [[CrossRef](#)]
38. Levenson, J.A.; Abram, I.; Rivera, T.; Fayolle, P.; Garreau, J.C.; Grangier, P. Quantum optical cloning amplifier. *Phys. Rev. Lett.* **1993**, *70*, 267–270. [[CrossRef](#)]
39. Bencheikh, K.; Lopez, O.; Abram, I.; Levenson, J.A. Improvement of photodetection quantum efficiency by noiseless optical preamplification. *Appl. Phys. Lett.* **1995**, *66*, 399–401. [[CrossRef](#)]
40. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [[CrossRef](#)]
41. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [[CrossRef](#)]
42. Caves, C.M. Quantum limits on noise in linear amplifiers. *Phys. Rev. D* **1982**, *26*, 1817–1839. [[CrossRef](#)]
43. Fasel, S.; Gisin, N.; Ribordy, G.; Scarani, V.; Zbinden, H. Quantum Cloning with an Optical Fiber Amplifier. *Phys. Rev. Lett.* **2002**, *89*, 107901. [[CrossRef](#)] [[PubMed](#)]
44. Ou, Z.Y.; Pereira, S.F.; Kimble, H.J. Quantum noise reduction in optical amplification. *Phys. Rev. Lett.* **1993**, *70*, 3239–3242. [[CrossRef](#)] [[PubMed](#)]
45. Levenson, J.A.; Abram, I.; Rivera, T.; Grangier, P. Reduction of quantum noise in optical parametric amplification. *J. Opt. Soc. Am. B* **1993**, *10*, 2233–2238. [[CrossRef](#)]
46. Qi, B.; Huang, L.L.; Qian, L.; Lo, H.K. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **2007**, *76*, 052323. [[CrossRef](#)]
47. 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 At. Mol. Opt. Phys.* **2009**, *42*, 114014. [[CrossRef](#)]
48. Lodewyck, J.; Bloch, M.; García-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Debuisschert, T.; Cerf, N.J.; Tualle-Brouri, R.; McLaughlin, S.W.; et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **2007**, *76*, 042305. [[CrossRef](#)]