



## Article

# Performance Improvement of Discretely Modulated Continuous-Variable Quantum Key Distribution with Untrusted Source via Heralded Hybrid Linear Amplifier

Kunlin Zhou <sup>1,†</sup>, Xuelin Wu <sup>1,2,\*,†</sup>, Yun Mao <sup>3,\*</sup>, Zhiya Chen <sup>1</sup>, Qin Liao <sup>4</sup>  and Ying Guo <sup>3,\*</sup> 

<sup>1</sup> School of Traffic and Transportation Engineering, Central South University, Changsha 410083, China; yingguo1001@foxmail.com (K.Z.); chzy@csu.edu.cn (Z.C.)

<sup>2</sup> Jiangsu Key Construction Laboratory of IoT Application Technology, Taihu University, Wuxi 214064, China

<sup>3</sup> School of Automation, Central South University, Changsha 410083, China

<sup>4</sup> College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China; llqqlq@hnu.edu.cn

\* Correspondence: wuxl@wxu.edu.cn (X.W.); k40669115@outlook.com (Y.M.); yingguo@csu.edu.cn (Y.G.)

† These authors contributed equally to this work.

Received: 1 July 2020; Accepted: 7 August 2020; Published: 12 August 2020

**Abstract:** In practical quantum communication networks, the scheme of continuous-variable quantum key distribution (CVQKD) faces a challenge that the entangled source is controlled by a malicious eavesdropper, and although it still can generate a positive key rate and security, its performance needs to be improved, especially in secret key rate and maximum transmission distance. In this paper, we proposed a method based on the four-state discrete modulation and a heralded hybrid linear amplifier to enhance the performance of CVQKD where the entangled source originates from malicious eavesdropper. The four-state CVQKD encodes information by nonorthogonal coherent states in phase space. It has better transmission distance than Gaussian modulation counterpart, especially at low signal-to-noise ratio (SNR). Moreover, the hybrid linear amplifier concatenates a deterministic linear amplifier (DLA) and a noiseless linear amplifier (NLA), which can improve the probability of amplification success and reduce the noise penalty caused by the measurement. Furthermore, the hybrid linear amplifier can raise the SNR of CVQKD and tune between two types of performance for high-gain mode and high noise-reduction mode, therefore it can extend the maximal transmission distance while the entangled source is untrusted.

**Keywords:** untrusted source; discrete modulation; heralded hybrid linear amplifier

## 1. Introduction

Quantum key distribution (QKD) allows two legitimate parties to share the secure key string over an insecure quantum channel [1–5]. The continuous-variable QKD (CVQKD) is one of alternative protocols of QKD, can provide higher detection efficiencies than original discrete-variable QKD (DVQKD) [6–12]. Furthermore, using the laser to generate the entangled source makes it easier to integrate with existing fiber network systems. However, compared with the DVQKD, the CVQKD has one of fatal disadvantages, which is the short secure transmission distance [11,13,14], especially if the entangled source is untrusted [15]. In fact the safety of CVQKD protocol has been proved where the entangled source is originated from the malicious eavesdropper [15], and it still can distill a positive key rate. However, the performance of this protocol is not great in terms of secret key rate and transmission distance, and thus could restrict the practical application of CVQKD in development. One of the main reasons for the short transmission distance of CVQKD is that traditional Gaussian modulation CVQKD

cannot maintain relatively high reconciliation efficiency in long-distance transmission, but discretely the modulation scheme can solve this problem even better than using error correcting code [16]. The four-state discretely modulation scheme produces four nonorthogonal coherent states in phase space and thus it can randomly select those coherent states by different quadrature to encode information rather than using the  $\hat{x}$  and  $\hat{p}$  quadratures themselves. Due to the fact that, the received coherent state will be easier to distinguish with a traditional Gaussian counterpart. That is the reason why the discrete modulation scheme can reach relative longer transmission distance even at very low SNR [16].

The penalty noise caused by detector in Bob side will also directly affect the transmission distance performance of CVQKD protocol where the entanglement source is untrusted. In practice, the intrinsic disadvantage of the receiver's apparatus, such as the efficiency of detector and the electrical noise referred by measurement, will decrease the secret key rate and thus shorten the transmission distance. In fact, optical amplifiers can solve such problem, for instance, the noiseless linear amplifier (NLA) is one of existing methods to overcome this limitation of detector. It can compensate the noise penalty and thus preserve the signal-to-noise ratio (SNR) [17–21]. However, the CVQKD scheme with non-traditional light source modulation and non-Gaussian operation, such as the discrete or unimentional modulation and photon subtraction operation, cannot directly implement via NLA. To overcome this problem, the measurement-based NLA (MB-NLA) has been proposed [22,23], which installs a dual homodyne detection ahead of NLA. The MB-NLA not only solve the application problem of NLA in CVQKD scheme with non-Gaussian modulation, but also can simulate the action of post-selection with amplifier. Furthermore, the quantum filter induced by the MB-NLA can simply model an appropriate postprocessing [24,25]. Although MB-NLA has the advantages mentioned above, its property of post-selective restricts it in point-to-point application such as CVQKD. To overcome this defect, the hybrid amplifier has been proposed, which concatenates a deterministic linear amplifier (DLA) behind the MB-NLA to form a feed-forward loop [25]. Due to the installation of the DLA, the amplification function uncertainty caused by NLA has been solved [24]. Furthermore, the DLA also can compensate the degeneration of SNR caused by NLA. It is worth noting that DLA can be divided into a phase-sensitive amplifier (PSA) and phase-insensitive amplifier (PIA) [26,27]. If Bob adopts heterodyne measurement, we only can deploy PIA as the DLA, on the contrary, it can deploy PSA [28,29].

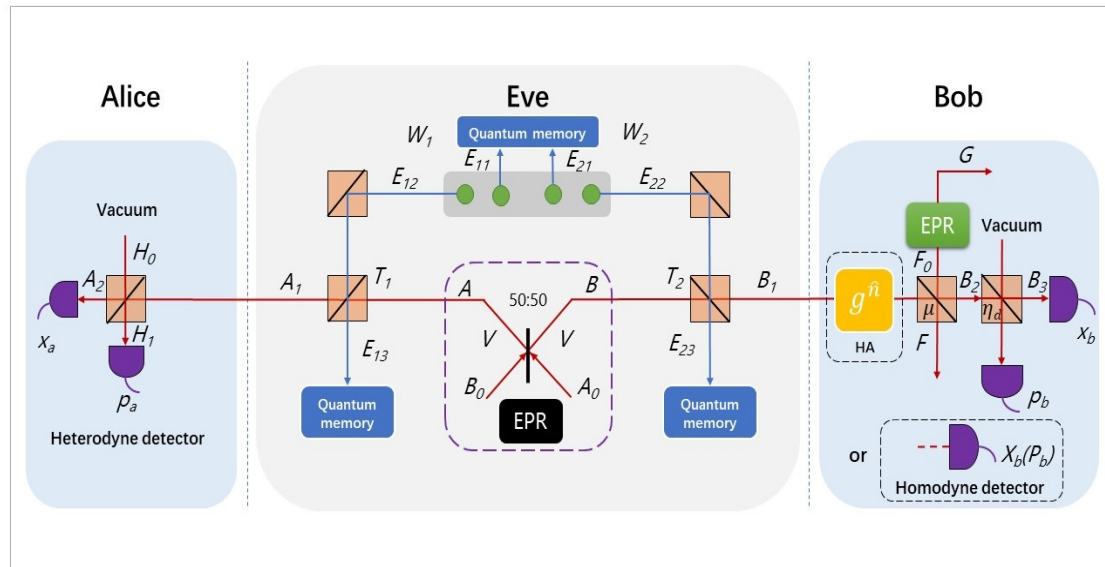
From the inspiration of the discrete modulation and hybrid amplifier mentioned above, in this paper, we proposed a scheme of discretely modulated CVQKD with hybrid amplifier to improve the performance of CVQKD with untested entangled source. Here, the four-state discrete modulation can improve the transmission distance of CVQKD even on the low SNR. Moreover, a hybrid amplifier deployed on the Bob side can reduce the influence of electrical noise caused by the detection and thus further enhance the transmission distance and secret key rate. The hybrid amplifier not only integrates the advantages of MB-NLA and DLA, but also provides a fully tunable gain for NLA and DLA. The proposed scheme outperforms the classical Gaussian modulation CVQKD with untested source in terms of the key rate, and also transcends the traditional discrete modulation CVQKD with untested source in terms of the maximal transmission distance.

This paper is structured as follows. In Section 2, we introduce the scheme design for four-state discrete modulation CVQKD with untested source involving the hybrid amplifier. In Section 3, we demonstrate the secret key rate for the proposed scheme. In Section 4, we analyze the results of its performance. In Section 5, we provide a conclusion.

## 2. Discretely Modulated CVQKD with Untested Source via Hybrid Amplifier

In this paper, we consider to integrate a hybrid amplifier at Bob side in discretely modulated CVQKD scheme with untested source and thus leading to the performance improvement of transmission distance at low SNR. In this section, we will introduce the Alice side, Eve side, and Bob side according to the order from left to right in Figure 1, namely, the four-state discrete modulation

will be introduced at first, next we consider about the CVQKD scheme with untested source model, and the last part is the description of hybrid amplifier.



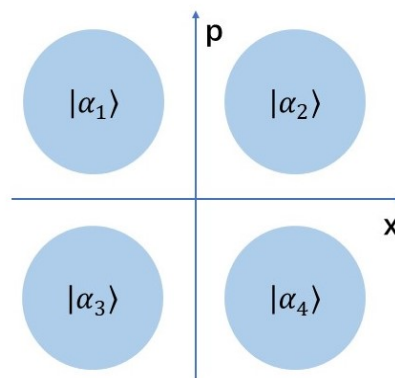
**Figure 1.** (Color online) Schematic of the entangled source in middle (ESIM) CVQKD using a hybrid amplifier. In the entanglement-based model, Alice detects one of the EPR states by heterodyne detector and the hybrid linear amplifier is installed before Bob uses either the homodyne or heterodyne detector to measure the other half of EPR states. Eve’s attack consists of two entangling cloner attacks on either side of the source. The yellow box of  $g^{\hat{n}}$  shows the hybrid linear amplifier.

### 2.1. Deploying a Four-State Discrete Modulation at Alice Side

We first begin by introducing the four-state discrete modulation scheme. The four-state protocol is belonged to the discrete modulation protocol. In the discrete modulation CVQKD, Alice produces  $N$  coherent states at phase space with

$$|\alpha_k^N\rangle = |\alpha e^{\frac{i2k\pi}{N}}\rangle. \quad (1)$$

For the four-state protocol, we only prepare four coherent states at phase space (see the Figure 2) [12], namely, here we have  $|\alpha_k^N\rangle = |\alpha e^{\frac{i(2k+1)\pi}{4}}\rangle$ ,  $k \in \{0, 1, 2, 3\}$ , and  $\alpha$  is a positive parameter and relates to the modulation variance with  $\alpha = \sqrt{\frac{V_M}{2}}$ .



**Figure 2.** (Color online) Four-state discrete modulation in phase space.

In the scheme of prepare-and-measure (PM), Alice randomly selects one of coherent state  $|\alpha_k^4\rangle, k \in \{0, 1, 2, 3\}$ , and transmits it to Bob by quantum channel with transmission efficiency  $T$  and excess noise  $\epsilon$ . Bob use detector to measure the received coherent states with detection efficiency  $T_d$  and electronics noise  $v_{el}$ . The mixture of four coherent state received by Bob can be denoted as

$$\rho_{4c} = \frac{1}{4} \sum_{k=0}^3 |\alpha_k^4\rangle \langle \alpha_k^4|. \quad (2)$$

At the equivalent scheme of entanglement-based (EB), we can more convenient to calculate the secret key rate. First, the  $\rho_{4c}$  is transformed to

$$\rho_{4c} = \text{tr}_A(|\Phi\rangle \langle \Phi|), \quad (3)$$

the mixture coherent state can be diagonalized and thus rewritten as the following form,

$$\rho_{4c} = \mu_0 |\phi_0\rangle \langle \phi_0| + \mu_1 |\phi_1\rangle \langle \phi_1| + \mu_2 |\phi_2\rangle \langle \phi_2| + \mu_3 |\phi_3\rangle \langle \phi_3|, \quad (4)$$

here

$$\mu_{0,2} = \frac{1}{2} e^{-\alpha^2} [\cosh(\alpha^2) \pm \cos(\alpha^2)], \quad (5)$$

$$\mu_{1,3} = \frac{1}{2} e^{-\alpha^2} [\sinh(\alpha^2) \pm \sin(\alpha^2)], \quad (6)$$

and

$$|\phi_k\rangle = \frac{e^{-\frac{\alpha^2}{2}}}{\sqrt{\mu_k}} \sum_{n=0}^{\infty} \frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}} (-1)^n |4n+k\rangle. \quad (7)$$

Then, we purify the system by the Schmidt decomposition

$$|\Phi\rangle = \frac{1}{2} \sum_{k=0}^3 |\psi_k\rangle |\alpha_k\rangle, \quad (8)$$

where the non-Gaussian (NG) state  $|\psi_k\rangle$  can be expressed as

$$|\psi_k\rangle = \frac{1}{2} \sum_{m=0}^3 e^{-i(1+2k)m(\frac{\pi}{4})} |\phi_m\rangle. \quad (9)$$

## 2.2. Eve Producing the Untrusted Entanglement Source

In practice, we need to consider any possible scenarios like that Eve that could have controlled the entangled source and generate it to any state. In this case, we first assume that Eve adopts Gaussian modulation and compare its performance to discrete modulation counterpart. That is because the Gaussian state can produce the maximum Shannon mutual information. In Gaussian attack, Eve perfectly uses its own quantum channel to replace the quantum channel which is placed between Alice and Bob. The loss channels are simulated by two independent beam splitters with transmissions  $T_1$  and  $T_2$  [12]. Note that if there is a symmetric transmission ( $T_1 = T_2$ ), it can be considered as entangled source in middle (ESIM) CVQKD protocol, and if these two transmissions are asymmetric with  $T_1 = 1$  ( $T_1 \neq T_2$ ), it can be recovered to the traditional CVQKD protocol where entangled source is generated at Alice or Charlie. In this case, we hypothesize entangled source is generated by Eve, but Eve is close to Alice side. Here, we have the distance between Alice and Eve with  $L_1$  and Eve between Bob with  $L_2$ , therefore the channels transmissions can be rewritten as  $T_1 = 10^{-0.02L_1}$ ,  $T_2 = 10^{-0.02L_2}$ , and thus  $T = T_1 T_2$ .

Eve's Einstein–Podolsky–Rosen (EPR) state  $|\psi\rangle_{AB}$  is created by two single-mode squeezed states,  $|z\rangle$  and  $|-z\rangle$  with

$$|z\rangle_i = \hat{O}_i |z|0\rangle, \quad (10)$$

here  $\hat{O}_i(z)$  is the squeezing operator and can be expressed with

$$\hat{O}_i(z) = \exp\left[-\frac{z}{2}(\hat{a}_i^{\dagger 2} - \hat{a}_i^2)\right], \quad (11)$$

where  $\hat{a}_i$  and  $\hat{a}_i^{\dagger}$  represent the creation and annihilation operation, and  $z$  is the squeezing parameter. The combining two single-mode squeezed states ( $\hat{z}_{A_0}$  and  $\hat{z}_{B_0}$ ) become a EPR state  $|\psi\rangle_{AB}$  by a 50:50 beam splitter. We can denote each entangled mode ( $\hat{X}_A$  and  $\hat{X}_B$ ) as

$$\hat{X}_A = \frac{(\hat{z}_{A_0} + \hat{z}_{B_0})}{\sqrt{2}}, \quad (12)$$

$$\hat{X}_B = \frac{(\hat{z}_{A_0} - \hat{z}_{B_0})}{\sqrt{2}}. \quad (13)$$

The EPR state  $|\psi\rangle_{AB}$  can be represent as

$$|\psi\rangle = \hat{O}_{AB}(-z)|0\rangle_A|0\rangle_B = \delta \sum_{n=0}^{\infty} \lambda^n |n, n\rangle, \quad (14)$$

where  $\hat{O}_{AB}$  represents a squeezing operator on two modes (modes  $A$  and  $B$ ),  $\hat{O}_{AB}(z) = \exp[-z(\hat{a}_A^{\dagger}\hat{a}_B^{\dagger} - \hat{a}_A\hat{a}_B)]$ ,  $\lambda = \sqrt{\frac{V-1}{V+1}}$ , here  $V$  is variance of two modes and  $\delta = \sqrt{1-\lambda^2}$ . Then, we assume that Eve performs the best collective Gaussian attack on the entangled source modes. The entangling cloner, a common collective Gaussian attack, is used to prepare two ancilla modes,  $\hat{X}_{E_1}$  and  $\hat{X}_{E_2}$ , from an entangled Gaussian state with symmetrized variance ( $W_1 = W_2$ ). In each pulse, Eve stores modes  $E_{11}$  and  $E_{21}$  in her quantum memory and injects the other two modes  $E_{12}$  and  $E_{22}$  into the beam splitter, thus obtains the output modes  $E_{13}$  and  $E_{23}$ . In the end of protocol, Eve measures the quadratures of  $E_{11}$  and  $E_{21}$  to obtain the communication information between Alice and Bob.

### 2.3. Implementing a Hybrid Linear Amplifier at Bob Side

First, we introduce the conceptual layout of our scheme, and in order to overcome the post-selective nature and thus promote the point-to-point application for traditional linear amplifier, we set a feed-forward loop outputted to a quantum state instead of the original state as follows [24],

$$\hat{\rho}_{out} = Z \text{Tr}_v\{\hat{D}_{g_D} g_N^{\hat{n}} \hat{\rho}_{in} \otimes |0\rangle\langle 0|_v g_N^{\hat{n}} \hat{D}_{g_D}^{\dagger}\}. \quad (15)$$

where the  $Z$  is the normalization factor and the operators  $\hat{D}_{g_D}$  and  $g_N^{\hat{n}}$  are used to model the action of NLA and DLA. In addition, the input coherent state can be written as

$$\hat{\rho}_{in} = \frac{1}{\pi} \frac{1-\lambda^2}{\lambda^2} \int d^2\alpha e^{-\frac{1-\lambda^2}{\lambda^2}|\alpha|^2} |\alpha\rangle\langle\alpha|. \quad (16)$$

here the  $\lambda$  ( $0 \leq \lambda < 1$ ) relates to the variance of coherent states with  $V$ . Due to the operations of NLA and DLA, the variance has been changed to

$$V = \frac{1+\lambda^2}{1-\lambda^2} \implies V_g = \frac{1+g_N^2\lambda^2}{1-g_N^2\lambda^2}. \quad (17)$$

The mean variance of two quadratures of the electric field can be written as

$$\langle \hat{X} \rangle = \hat{a} + \hat{a}^{\dagger}, \quad (18)$$

$$\langle \hat{P} \rangle = -i(\hat{a} - \hat{a}^{\dagger}). \quad (19)$$

when the signal feed through the hybrid amplifier, the expectation of the measurable value  $\hat{M} = (\hat{a}, \hat{a}^\dagger)$  is further amplified by DLA, and the outcomes can be expressed as

$$\hat{a}_{out} = \hat{a}_{in} g_D + \hat{a}_{int}^\dagger \sqrt{g_D^2 - 1}, \quad (20)$$

$$\hat{a}_{out}^\dagger = \hat{a}_{in}^\dagger g_D + \hat{a}_{int} \sqrt{g_D^2 - 1}. \quad (21)$$

So that, according to above Equations (18)–(21), we can give the corresponding outcome quadratures of amplitude and phase as

$$\langle \hat{X} \rangle_{out} = \langle \hat{X} \rangle_{in} g_N g_D, \quad (22)$$

$$\langle \hat{P} \rangle_{out} = \langle \hat{P} \rangle_{in} g_N g_D. \quad (23)$$

In this proposed scheme, we take the GG02 protocol [2] (the GG02 protocol is a fundamental CVQKD protocol) as usual but add a hybrid amplifier at Bob side, so that the secure key rate should depend on the covariance matrix with presence of the hybrid amplifier. However, the output of the linear hybrid amplifier remains in the Gaussian regime, therefore we use an equivalent channel to replace the previous one (Figure 3). Here, the corresponding system parameters are changed from  $(|\lambda\rangle, T_1, T_2, \epsilon, \chi)$  to  $(|\zeta\rangle, \eta_1, \eta_2, \epsilon_{gn}, \chi_{gd})$ , those equivalent parameters are listed below,

$$\zeta = \lambda \sqrt{\frac{(g_N^2 - 1)(\epsilon - 2)T - 2}{(g_N^2 - 1)\epsilon T - 2}}, \quad (24)$$

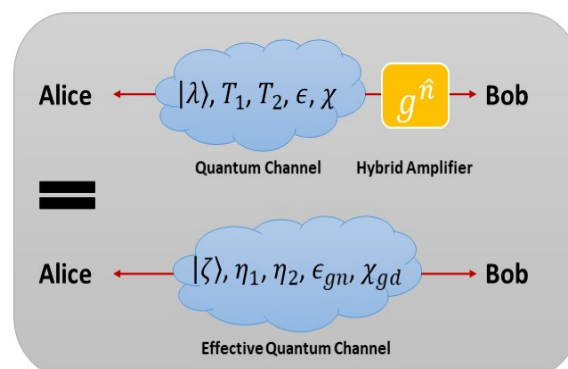
$$\eta = \frac{g_N^2 T}{(g_N^2 - 1)T[\frac{1}{4}(g_N^2 - 1)(\epsilon - 2)\epsilon T - \epsilon + 1] + 1}, \quad (25)$$

$$\epsilon_{gN} = \epsilon - \frac{1}{2}(g_N^2 - 1)(\epsilon - 2)\epsilon T, \quad (26)$$

$$\chi_{hom}^{gD} = \frac{(1 - T_d) + v_{el}}{g_D T_d}, \quad (27)$$

and

$$\chi_{het}^{gD} = \frac{1 + (1 - T_d) + 2v_e + (g_D - 1)T_d}{g_D T_d}. \quad (28)$$



**Figure 3.** (Color online) An EPR state  $|\lambda\rangle$  sent through a Gaussian quantum channel with transmittance  $T_1, T_2$ , excess noise  $\epsilon$ , and detection-added noise  $\chi$  has been replaced by an EPR state  $|\zeta\rangle$  sent through a Gaussian quantum channel with transmittance  $\eta_a, \eta_2$ , excess noise  $\epsilon_{gn}$ , and detection-added noise  $\chi_{gd}$ , but without the hybrid amplifier.



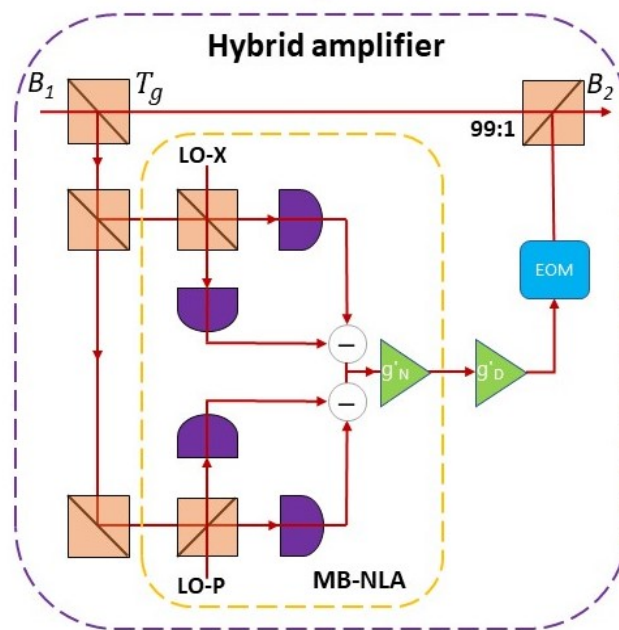
Finally, we present the equivalent experimental layout for our scheme. As mentioned above, we consider applying a hybrid linear amplifier at Bob's station (as shown in Figure 4). The input mode  $B_1$  is first fed through a beam splitter with transmissivity  $T_g = (g_N/g_D)^2$ , here  $g_N$  and  $g_D$  represent gains of NLA and DLA, respectively. After that, the reflected mode is fed through a measurement-based noiseless linear amplifier (MB-NLA), which consists by a dual-heterodyne detection and a noiseless linear amplifier. Here, one of the heterodyne detectors is used to measure the  $X$  quadrature of the coherent state, and other one measures the  $P$  quadrature. The MB-NLA has some special features, including a probabilistic of Gaussian filter and rescaling of amplifier gain factors. Here, the rescaling of gain NLA is given as  $g'_N = \frac{1}{g_N}$ , and thus the success probability of Gaussian filter is given as [25,30]

$$P(\alpha_m) = \begin{cases} \exp(|\alpha_m|^2 - |\alpha_c|^2)[1 - (g_N)^2], & |\alpha_m| \leq \alpha_c \\ 1, & |\alpha_m| > \alpha_c \end{cases} \quad (29)$$

The measurement outcomes of the dual-heterodyne detection is applied as [23]

$$\alpha_m = \frac{x_m + ip_m}{\sqrt{2}}, \quad (30)$$

and  $\alpha_c$  represents a tunable cut-off parameter, which directly determines the success probability of the protocol and how closely the MB-NLA approximates to an ideal NLA ( $\alpha_c > 0$ ). In this scheme, we couple a DLA before the MB-NLA to further improve the probability of success by  $g'_D = \sqrt{2(g_D^2 - 1)}$ . Finally, the output signal feeds through an elector-optic modulator (EOM) and a beam splitter with transmissivity 99:1.



**Figure 4.** (Color online) The heralded hybrid linear amplifier is applied at Bob side. The mode  $B_1$  first goes through into a beam splitter with transmissivity  $T_g$ , then the reflected mode goes through into the MB-NLA concatenated by a dual-heterodyne detection and NLA. Here, the dual-heterodyne detection is used to measure the  $X$  and  $P$  quadrature of the reflected mode, respectively. After that we set a DLA and an elector-optic modulator (EOM) to dispose the amplified signal pulse and output mode  $B_2$  by a beam splitter with transmissivity 99:1.

Notice that the performance of our hybrid amplifier depends on the respective gain of two different amplifiers. A relatively larger NLA gain cloud increases the signal-to-noise ratio (SNR),

but also leads to a lower success probability. In contrast, a relatively larger DLA gain would increase the success probability, but will also bring the added noise.

### 3. Simulation of the Secret Key Rate

In this section, we will demonstrate the calculation process of the asymptotic secret key rate for traditional Gaussian modulation and discrete modulation. The traditional Gaussian modulation scheme is based on two quantum states (coherent or squeezed states) and two measurement methods (homodyne or heterodyne detection). The discrete modulation scheme is based on coherent state four-state modulation and homodyne detection.

#### 3.1. The Gaussian Modulation with Untested Source via Hybrid Amplifier Scheme

In the Gaussian modulation scheme, we will mainly introduce calculation of direct reconciliation, and for the reverse reconciliation the calculation process can be simply derived from the covariance matrix  $\Gamma_{A_2B_2}$  by switching  $a$  and  $b$ . The secret key rate is defined as [2]

$$K = \beta I(A_2 : B_3) - \chi_E, \quad (31)$$

here  $\beta$  represents the reconciliation efficiency and  $I(A_2 : B_3)$  is the Shannon mutual information between Alice and Bob [31]; furthermore, the  $\chi_E$  is Eve's mutual information connected between Eve and Alice for direct reconciliation or between Eve and Bob for reverse reconciliation. When we consider the situation of untested entangled source CVQKD protocol with hybrid amplifier at Bob side, the covariance matrix of the Gaussian state  $\zeta_{A_2B_3}$  is given by (notice that here we assume that Alice and Bob both have deployed the ideal detectors)

$$\Gamma_{A_2B_3} = \begin{pmatrix} aI & c\sigma_z \\ c\sigma_z & bI \end{pmatrix},$$

where  $I$  and  $\sigma_z$  are the Pauli matrices  $a = \eta_1 V + (1 - \eta_1)W_1$ ,  $b = \eta_2 V + (1 - \eta_2)W_2$ , and  $c = \sqrt{\eta_1} \sqrt{\eta_2} \sqrt{V^2 - 1}$ ; therefore, the covariance matrix  $\Gamma_{A_2B_3}$  can be rewritten as

$$\begin{pmatrix} \eta_1 V + (1 - \eta_1)W_1 I & \sqrt{\eta_1} \sqrt{\eta_2} \sqrt{V^2 - 1} \sigma_z \\ \sqrt{\eta_1} \sqrt{\eta_2} \sqrt{V^2 - 1} \sigma_z & \eta_2 V + (1 - \eta_2)W_2 I \end{pmatrix},$$

here  $W_i = \eta_i \chi_{line} / (1 - \eta_i)$  ( $i = 1, 2$ ) and  $\chi_{line} = (1 - \eta_i) / (\eta_i + \epsilon_{gn})$  represents the added noise inputted by Gaussian channel. We first introduce the case of squeezed states with homodyne or heterodyne detection. In this case, when Bob adopts homodyne measurement, the mutual information between Alice and Bob can be defined as [2]

$$I(A_2 : B_3)_{hom}^S = \frac{1}{2} \log_2 \left( \frac{a}{a - c^2/b} \right), \quad (32)$$

with heterodyne measurement the mutual information is given as

$$I(A_2 : B_3)_{het}^S = \frac{1}{2} \log_2 \left( \frac{a}{a - (c^2/(b+1))} \right). \quad (33)$$

Then, we will introduce the Eve's mutual information, namely, the  $\chi_E$  mentioned in Equation (31). Here,

$$\chi_E = S(E) - S(E|A), \quad (34)$$

and it has the same calculation process for both homodyne and heterodyne detections. Due to the direction reconciliation implemented in this scheme, which only depends on the measurement results



with Alice but not Bob. Furthermore, Eve provides a purification for Alice and Bob's matrix, so that we can rewrite  $S(E)$  as

$$S(AB) = G[(\lambda_1 - 1)/2] + G[(\lambda_2 - 1)/2]. \quad (35)$$

Here,  $G(x) = (x + 1)\log_2(x + 1) - x\log_2 x$ , thus the symplectic eigenvalues are represented as

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B^2}]. \quad (36)$$

where  $A = a^2 + b^2 - 2c^2$  and  $B = ab - c^2$ , then Eve uses the same purification for Alice and Bob's matrix, thus we can rewrite  $S(E|A)$  as  $S(B|A)$ . Here,  $S(B|A) = G[(\lambda_3 - 1)/2]$  and  $\lambda_3 = \sqrt{b(b - (c^2/a))}$ . Therefore, we now can calculate the secret key rate mentioned in Equation (31).

Next, when Alice adopts coherent state, the mutual information for Alice and Bob with homodyne and heterodyne detections are given by

$$I(A_2 : B_3)_{hom}^C = \frac{1}{2} \log_2 \left( \frac{a + 1}{a + 1 - c^2/b} \right), \quad (37)$$

$$I(A_2 : B_3)_{het}^C = \log_2 \left( \frac{b + 1}{b + 1 - c^2/(a + 1)} \right). \quad (38)$$

in the case of coherent state with homodyne detection and heterodyne detection, the  $S(E)$  mentioned in Equation (34) is same with the counterpart of squeezed state, but the  $S(E|A)$  is replaced by  $S(BC|A)$  and expressed as follows,

$$S(BC|A) = G[(\lambda_4 - 1)/2] + G[(\lambda_5 - 1)/2], \quad (39)$$

here

$$\lambda_{4,5}^2 = \frac{1}{2}[C_{hom} \pm \sqrt{C_{hom}^2 - 4D_{hom}}]. \quad (40)$$

where, in the case of homodyne detection, the  $C_{hom}$  and  $D_{hom}$  can be denoted as

$$C_{hom} = \frac{A\chi_{hom}^{gD} + V\sqrt{B} + \eta(V + \chi_{line})}{\eta(V + \chi_{tot})}, \quad (41)$$

$$D_{hom} = \sqrt{B} \frac{V + \sqrt{B}\chi_{hom}^{gD}}{\eta(V + \chi_{tot})}. \quad (42)$$

For the heterodyne case, the symplectic eigenvalues 6 and 7 can be expressed as

$$\lambda_{6,7}^2 = \frac{1}{2}[C_{het} \pm \sqrt{C_{het}^2 - 4D_{het}}], \quad (43)$$

and  $C_{het}$  and  $D_{het}$  are denoted as follows,

$$C_{het} = \frac{A(\chi_{het}^{gD})^2 + B + 1 + 2\chi_{het}^{gD}[V\sqrt{B} + \eta(V + \chi_{line})] + 2\eta(V^2 - 1)}{[\eta(V + \chi_{tot})]^2}, \quad (44)$$

$$D_{het} = \left( \frac{V + \sqrt{B}\chi_{het}^{gD}}{\eta(V + \chi_{tot})} \right)^2. \quad (45)$$

$\chi_{line} = 1/\eta - 1 + \varepsilon$  is shot noise units and  $\chi_{tot} = \chi_{line} + \chi_h/\eta$  is channel total noise, here  $\chi_h$  is detection added noise mentioned in Equations (27) and (28) with  $\chi_{hom}^{gD}$  and  $\chi_{het}^{gD}$ . We can now plot the final secret key rate for both the Gaussian modulation squeezed state and coherent state.

### 3.2. The Discrete Modulation with Untested Source via Hybrid Amplifier Scheme

In the discrete modulation scheme, we mainly consider direct reconciliation with the coherent state scheme. The secret key rate is also same as Equation (31), but due to the state  $\zeta_{A_2B_3}^{DM}$  is not Gaussian anymore, and we should replace the Gaussian state  $\zeta_{A_2B_3}$  to  $\zeta_{A_2B_3}^{DM}$  as follows,

$$\Gamma_{A_2B_3}^{DM} = \begin{pmatrix} a_{DM}I & c_{DM}\sigma_z \\ c_{DM}\sigma_z & b_{DM}I \end{pmatrix},$$

here  $a_{DM} = \eta_1 a_0 + (1 - \eta_1)W_1$ ,  $b_{DM} = \eta_2 b_0 + (1 - \eta_2)W_2$ , and  $c_{DM} = \sqrt{\eta}c_0$ , the  $a_0, b_0$  and  $c_0$  can express as following

$$a_0 = 1 + 2\alpha^2, \quad (46)$$

$$b_0 = 1 + 2\alpha^2, \quad (47)$$

$$c_0 = 2\alpha^2 \sum_{k=0}^3 \mu_{k-1}^{3/2} \mu_k^{-1/2}. \quad (48)$$

where  $\alpha = \sqrt{\frac{V_M}{2}}$  and  $V_M = V - 1$ ; the mutual information between Alice and Bob is also the same with Gaussian counterpart in Equation (37), but the  $\chi_E$  has been changed,  $\chi_E = S(E) - S(E|A)$ , here the  $S(E)$  can be denoted as

$$S(E) = S(AB) = G[(\lambda_1^{DM} - 1)/2] + G[(\lambda_2^{DM} - 1)/2]. \quad (49)$$

Here  $G(x) = (x + 1)\log_2(x + 1) - x\log_2 x$ , thus the symplectic eigenvalues are represented as

$$\lambda_{1,2}^{DM} = \sqrt{\frac{1}{2}(A_{DM} \pm \sqrt{A_{DM}^2 - 4B_{DM}^2})}, \quad (50)$$

with  $A_{DM} = a_{DM}^2 + b_{DM}^2 - 2c_{DM}^2$  and  $B_{DM} = a_{DM}b_{DM} - c_{DM}^2$ , furthermore the  $S(E|A)$  is also replaced by  $S(BC|A)$

$$S(BC|A) = G[(\lambda_3^{DM} - 1)/2] + G[(\lambda_4^{DM} - 1)/2], \quad (51)$$

with

$$\lambda_{3,4}^{DM} = \sqrt{\frac{1}{2}[C_{hom}^{DM} \pm \sqrt{(C_{hom}^{DM})^2 - 4D_{hom}^{DM}}]}. \quad (52)$$

Here,  $C_{hom}^{DM}$  and  $D_{hom}^{DM}$  can be denoted as

$$C_{hom}^{DM} = \frac{A_{DM}\chi_{hom}^{gD} + V\sqrt{B_{DM}} + \eta(V + \chi_{line})}{\eta(V + \chi_{tot})}, \quad (53)$$

$$D_{hom}^{DM} = \sqrt{B_{DM}} \frac{V + \sqrt{B_{DM}}\chi_{hom}^{gD}}{\eta(V + \chi_{tot})}. \quad (54)$$

In the case of heterodyne detection, the symplectic eigenvalues are expressed as

$$\lambda_{5,6}^{DM} = \sqrt{\frac{1}{2}[C_{het}^{DM} \pm \sqrt{(C_{het}^{DM})^2 - 4D_{het}^{DM}}]}, \quad (55)$$

and

$$C_{het}^{DM} = \frac{A_{DM}(\chi_{het}^{gD})^2 + B_{DM} + 1 + 2\chi_{het}^{gD}[V\sqrt{B_{DM}} + \eta(V + \chi_{line})] + 2\eta(V^2 - 1)}{[\eta(V + \chi_{tot})]^2}, \quad (56)$$

$$D_{het}^{DM} = \left[ \frac{V + \sqrt{B_{DM} \chi_{het}^{g_D}}}{\eta(V + \chi_{tot})} \right]^2. \quad (57)$$

Finally, we can plot the secret key rate for proposed scheme in terms of discrete modulation.

#### 4. Performance Analysis and Results Discussion

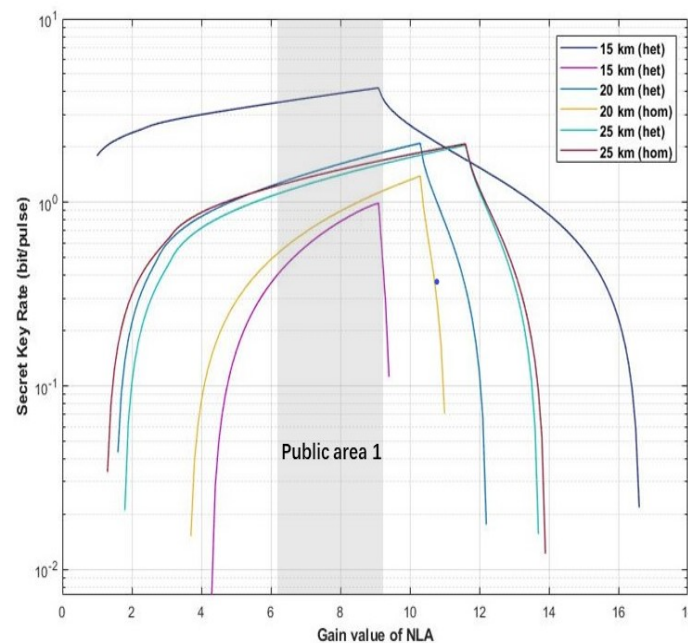
In the process of parameter setting of the hybrid amplifier, an appropriate gain value of the amplifier will directly determine the final performance of the scheme. As the main function of DLA is to improve the functional uncertainty caused by NLA, its gain value does not significant improvement for the performance of proposed scheme. Therefore, we mainly discuss the optimal range of NLA gain first. As shown in Figures 5–7, here we set the tunable distance to derive the optimal range for  $g_N$  in our proposed scheme. The parameters are set as fixed value with  $g_D = 12$ ,  $\eta = 1$ ,  $\varepsilon = 0.01$ , and  $V_M = 0.3$ .

In the first scenario, we set different distance with  $d = 15$  km,  $d = 20$  km, and  $d = 25$  km. As shown in Figure 5, the public zone 1 highlighted with light gray denotes that two kinds of proposed scheme can obtain relative higher secret key rate in this gain value range of  $g_N$  ( $6.1 \leq g_N \leq 8.6$ ).

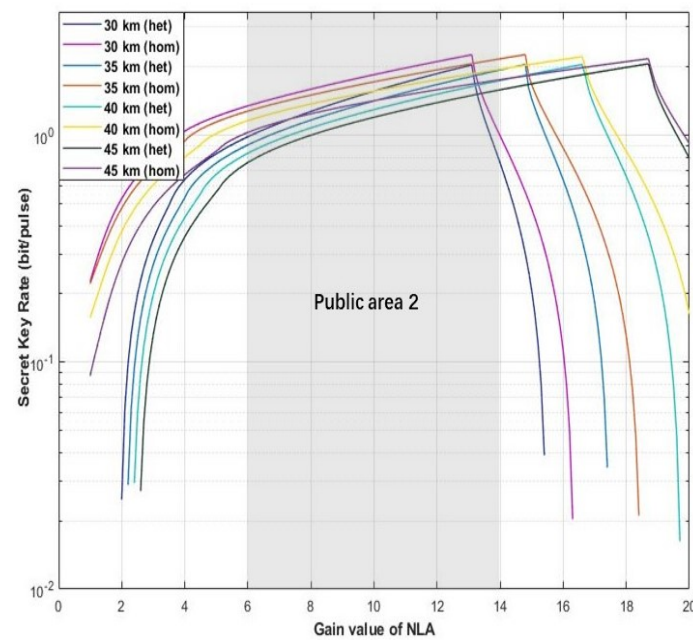
In the second scenario, we have different distance values with  $d = 30$  km,  $d = 35$  km,  $d = 40$  km, and  $d = 45$  km. The public zone 2 has been highlighted with light gray in Figure 6, which represents our proposed schemes can obtain relative higher secret key rate in this gain range with NLA ( $6 \leq g_N \leq 14$ ).

In the final scenario, the distance value are given as  $d = 90$  km,  $d = 95$  km, and  $d = 100$  km. Our proposed scheme can reach the relative higher secret key rate in the public zone 3, which has been shown in Figure 7 with the gain value range ( $7.5 \leq g_N \leq 20$ ).

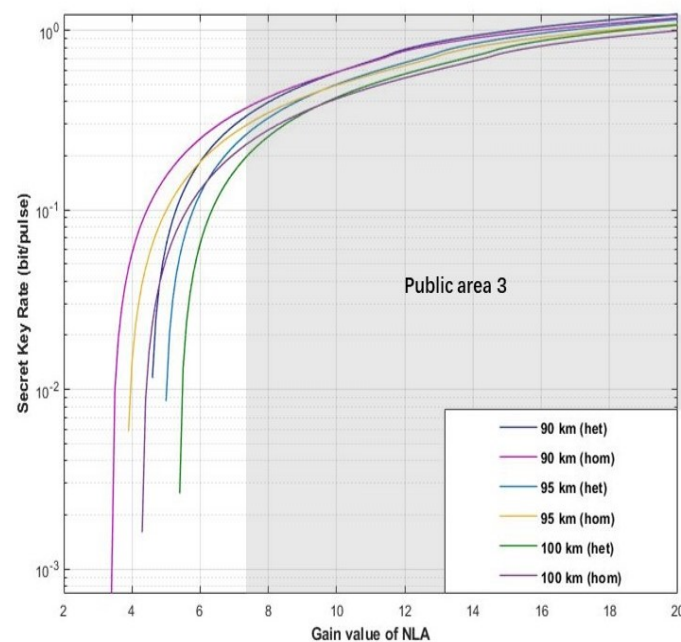
Therefore, considering the above three scenarios, we can get the overlapping area ( $7.5 \leq g_N \leq 8.6$ ) in Figure 8, which represents the optimal gain range for proposed scheme.



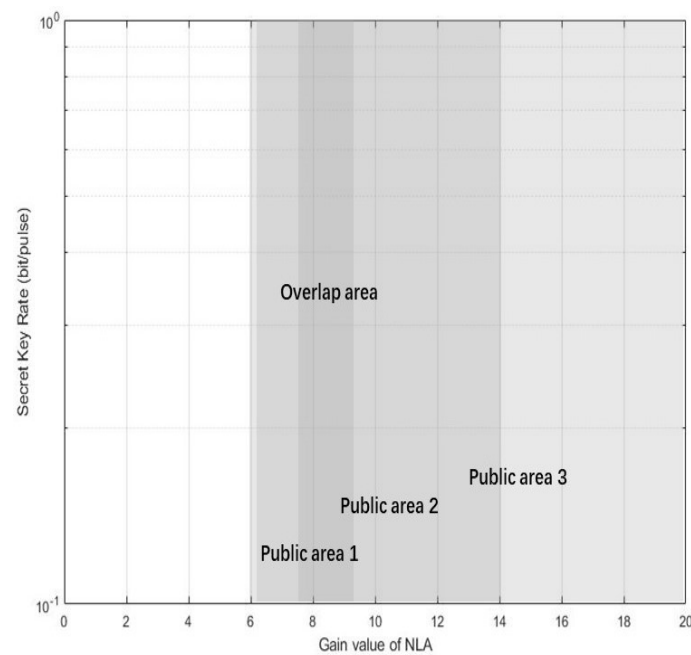
**Figure 5.** (Color online) The optimal value range for  $g_{NLA}$ . The X-coordination and Y-coordination represent gain value of NLA and secret key rate, respectively. The figure shows that the proposed scheme with different detector (homodyne detector and heterodyne detector) can obtain relative higher secret key rate in the public area 1. Here, the distance be set as 15, 20, and 25 km. Moreover, the fixed parameter values are set with  $g_D = 12$ ,  $\eta = 1$ ,  $\varepsilon = 0.01$ , and  $V_M = 0.3$ .



**Figure 6.** (Color online) The optimal value range for  $g_{NLA}$ . The X-coordination and Y-coordination represent the gain value of NLA and secret key rate, respectively. The figure shows that the proposed scheme with different detectors (homodyne detector and heterodyne detector) can obtain relative higher secret key rate in the public area 2. Here, the distance be set as 30, 35, 40, and 45 km. Moreover, the fixed parameter values are set with  $g_D = 12$ ,  $\eta = 1$ ,  $\varepsilon = 0.01$ , and  $V_M = 0.3$ .

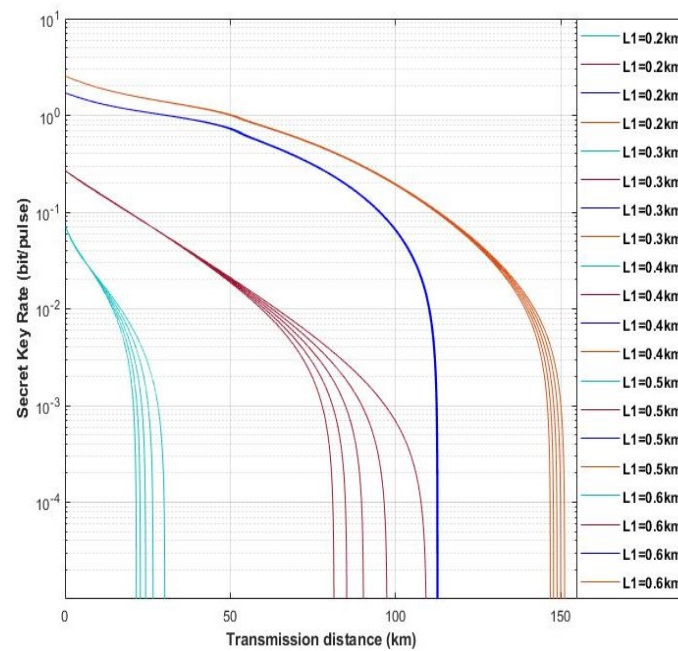


**Figure 7.** (Color online) The optimal value range for  $g_{NLA}$ . The X-coordination and Y-coordination represent gain value of NLA and secret key rate, respectively. The figure shows that the proposed scheme with different detector (homodyne detector and heterodyne detector) can obtain relative higher secret key rate in the public area 3. Here, the distance be set as 90, 95, and 100 km. Moreover, the fixed parameter values are set with  $g_D = 12$ ,  $\eta = 1$ ,  $\varepsilon = 0.01$ , and  $V_M = 0.3$ .

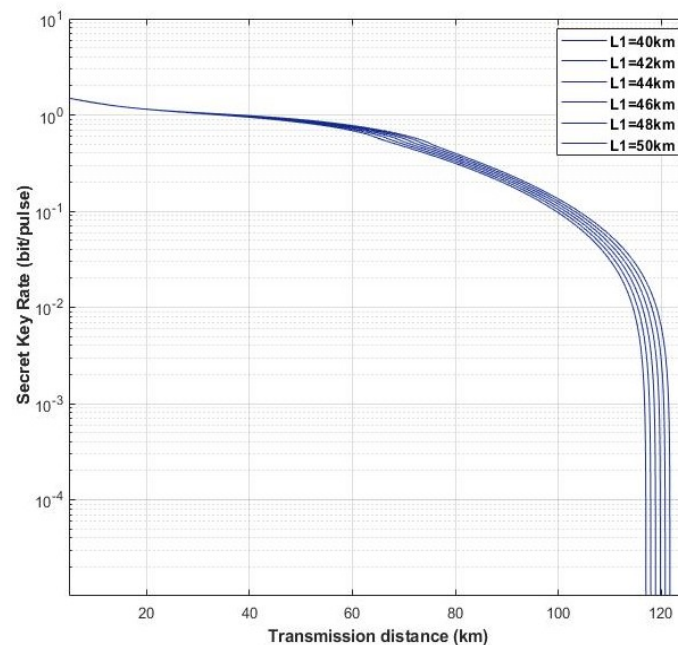


**Figure 8.** (Color online) Considering the above three public areas denoted in Figures 5–7, we get the overlapping region in this figure, which represents the optimal gain value range of proposed scheme.

Moreover, we find that the distance between Alice and Eve ( $L_1$ ) can also influence the performance of our scheme. In Figure 9, here we set different distances,  $L_1$ , to observe the schemes performance with  $L_1 = 0.2$  km,  $L_1 = 0.3$  km,  $L_1 = 0.4$  km,  $L_1 = 0.5$  km, and  $L_1 = 0.6$  km. The fixed parameters are set with  $g_N = 8$ ,  $g_D = 12$ ,  $\eta = 1$ ,  $\varepsilon = 0.01$ , and  $V_M = 0.3$ . As shown in Figure 9, the light blue solid lines and red solid lines represent four-state discrete modulation with untested source via heterodyne detection and homodyne detection, respectively. Furthermore, the dark blue solid lines and orange solid lines denote four-state discrete modulation with untested source via hybrid amplifier by heterodyne and homodyne detection, respectively. We can find that with the increasing of  $L_1$  the maximum transmission distance of all schemes is increasing, and the increasing of scheme with four-state untested source via homodyne detection is the most obvious, which is almost catching up the scheme with four-state untested source by hybrid amplifier via heterodyne detection. However, when the distance exceeds 0.6 ( $L_1 > 0.6$  km), the four-state with untested source schemes are on longer to generate the secret key rate, and it has the same situation with the counterpart schemes of hybrid amplifier in  $L_1 > 50$  km and  $L_1 > 2$  km, respectively (as shown in Figures 10 and 11). Therefore, in our scheme we set the distance between Alice and Eve with  $L_1 = 0.5$ .

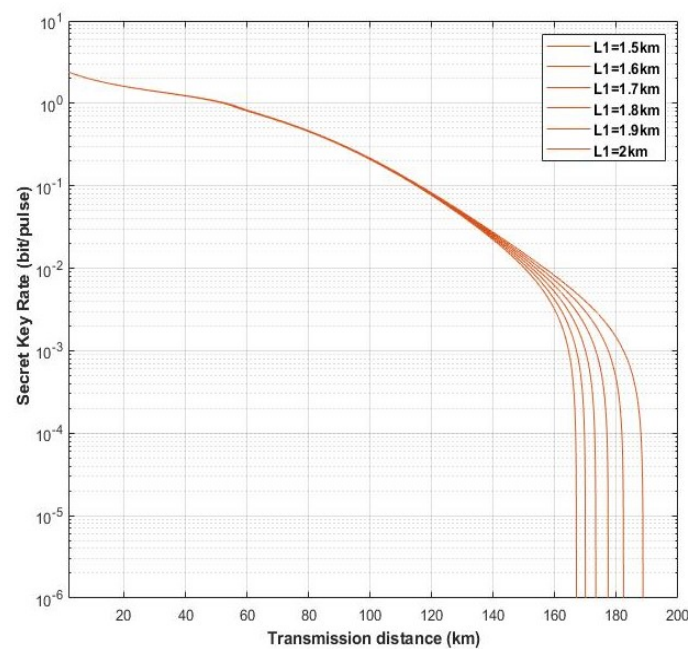


**Figure 9.** (Color online) The performance of proposed schemes for different  $L_1$ . The fixed parameters are set with  $g_N = 8$ ,  $g_D = 12$ ,  $\eta = 1$ ,  $\varepsilon = 0.01$ , and  $V_M = 0.3$ . Here, the light blue solid lines and red solid lines express the scheme without hybrid amplifier, moreover dark blue solid lines and orange lines represent the scheme with hybrid amplifier.



**Figure 10.** (Color online) The performance of schemes with four-state untested source via hybrid amplifier and heterodyne detection in different  $L_1$ . The fixed parameters are set with  $g_N = 8$ ,  $g_D = 12$ ,  $\eta = 1$ ,  $\varepsilon = 0.01$ , and  $V_M = 0.3$ .





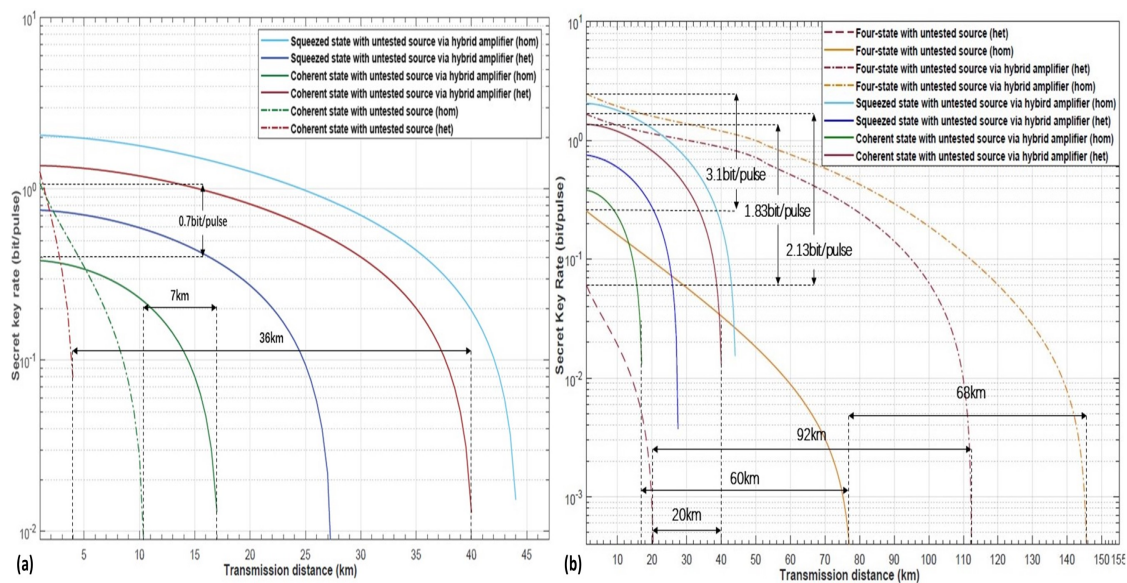
**Figure 11.** (Color online) The performance of schemes with four-state untested source via hybrid amplifier and homodyne detection in different  $L_1$ . The fixed parameters are set with  $g_N = 8$ ,  $g_D = 12$ ,  $\eta = 1$ ,  $\varepsilon = 0.01$ , and  $V_M = 0.3$ .

Based on the calculation process in the previous section, we show the performances of various protocols over the lossy quantum channel. According to different modulation methods, we divide these protocols into two categories that includes the protocol based on Gaussian modulation and discrete modulation. For these schemes, we set the entanglement source in untested side, and implement a hybrid amplifier at Bob side. In the case of Gaussian modulation we have the squeezed-state with homodyne and heterodyne detection, or, equivalently, coherent-state with homodyne and heterodyne detection (in Figure 12a). In the scenario of discrete modulation, we select coherent-state with homodyne and heterodyne detection (in Figure 12b). The dashed lines in Figure 12a indicate the scheme without hybrid amplifier, and the solid lines denote the scheme implemented hybrid amplifier. Where the red dashed line indicates that the scheme by coherent state with untested source and heterodyne detection is far behind its corresponding scheme with hybrid amplifier, and the red solid line, in terms of transmission distance by 36 km. Furthermore, although the scheme of coherent state with untested source via hybrid amplifier homodyne detection (the green solid line) has lower initial secret key rate than its counterpart (the green dashed line), its transmission distance has been increased 7 km compared to the same scheme without hybrid amplifier (the green dashed line). The squeezed state with untested source via hybrid amplifier schemes are indicated as a dark blue solid line and light blue solid line, respectively; here, the scheme with homodyne detection (the light blue solid line) reaches the maximal transmission distance of approximately 45 km, and the scheme of heterodyne detection (the dark blue solid line) reaches it in 17 km. Therefore, in the case of the scheme adopting traditional Gaussian modulation, the hybrid amplifier is helpful in improving the transmission distance indeed.

Next, Figure 12b will show the performance result for Gaussian modulation and discrete modulation schemes. In Figure 12b, the dot-dashed lines represent the discrete modulation with untested source via hybrid amplifier, corresponding to the original schemes that did not adopt the hybrid amplifier, marked with red dashed line and yellow solid line, respectively. The remaining schemes are the Gaussian modulation with untested source and hybrid amplifier. We can see the detailed relationship between each line of the scheme, and find that the scheme of classical four-state modulation with untested source heterodyne detection has poorer performance than the same scheme



with Gaussian modulation adopted hybrid amplifier, in terms of transmission distance (20 km behind) and initial secret key rate (1.83 bit per pulse behind). However, after being amplified by the hybrid amplifier, the four-state modulation with heterodyne detection scheme, the red dot-dashed line, has better transmission distance performance by 72 km ahead than the Gaussian modulation (red solid line) and 92 km ahead than the unamplified scheme (red dashed line). The scheme of four-state modulation untested source via hybrid amplifier and homodyne detection, the yellow dot-dashed line, reaches the maximal transmission distance with over 146 km. It is 68 km beyond the scheme of discrete modulation unadopted hybrid amplifier (the yellow solid line), and 128 km ahead the scheme of Gaussian modulation with hybrid amplifier. All the simulation results show that even if the entangled source is untested, the discrete modulation with four-state modulation has better performance in key rate and transmission distance than the scheme with Gaussian modulation.



**Figure 12.** (Color online) Panel (a) shows the relationship between the transmission distance and secret key rate. It demonstrates the maximal transmission distance for the scheme with Gaussian modulation. Here, the parameters are set as  $g_N = 8$ ,  $g_D = 12$ ,  $\eta = 1$ ,  $\varepsilon = 0.01$ , and  $V_M = 0.3$ . The dot-dash lines in the figure represent Gaussian modulation with an untested source. Furthermore, the solid lines represent Gaussian modulation with untested source via hybrid amplifier. Panel (b) also shows the relationship between transmission distance and secret key rate. Here, the parameters are also set as  $g_N = 8$ ,  $g_D = 12$ ,  $\eta = 1$ ,  $\varepsilon = 0.01$ , and  $V_M = 0.3$ . In panel (b), the green, dark blue, red, and light blue solid lines represent the Gaussian modulation with untested source via hybrid amplifier. Furthermore, the red dash line and yellow solid line represent the four-state discrete modulation with untested source. The red dot-dash line and yellow dot-dash line denote our proposed scheme (four-state discrete modulation with untested source via hybrid amplifier).

## 5. Conclusions

In this paper, we proposed a scheme of four-state discrete modulation with hybrid amplifier to improve the performance of traditional Gaussian modulation CVQKD while the entangle source is untested. The hybrid amplifier is composed of a MB-NLA and a DLA in series. Due to deployment of the MB-NLA, the noise penalty caused by the detector in the Bob side can be compensated. Moreover, the adoption of DLA compensated the problem of SNR degeneration and amplification probability caused by NLA. The numerical simulations show that our proposed scheme can improve the maximal transmission distance in the four-state modulation CVQKD and Gaussian modulation CVQKD for both homodyne and heterodyne detection, where the entangled source is untested. In terms of possible future research, it could be focusing to implement the hybrid amplifier in Alice and Bob side.

**Author Contributions:** Data curation, X.W.; investigation, K.Z.; resources, Q.L.; software, Y.M.; supervision, Z.C. and Y.G. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was supported by the National Natural Science Foundation of China (Grant No.61871407), National Key R & D Project (No. 2018YFB0704000), Hunan Provincial Natural Science Foundation of China (Grant No. 2020JJ5088), and the Fundamental Research Funds for the Central Universities (No. 531118010371).

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

## References

1. Brassard, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
2. Gisin, N.; Grégoire, R.; Tittel, W. Quantum Cryptography. *Rev. Mod. Phys.* **2002**, *74*, 154–195. [\[CrossRef\]](#)
3. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [\[CrossRef\]](#)
4. Bang, J.Y.; Berger, M.S. Quantum Mechanics and the Generalized Uncertainty Principle. *Phys. Rev.* **2006**, *74*, 125012. [\[CrossRef\]](#)
5. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.; Dušek, M.; Lütkenhaus, N.; Peev, M. The Security of Practical Quantum Key Distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [\[CrossRef\]](#)
6. Pirandola, S.; Ottaviani, C.; Spedalieri, G. High-rate measurement-device-independent quantum cryptography. *Nat. Photonics* **2015**, *9*, 397–402. [\[CrossRef\]](#)
7. Ma, X.C.; Sun, S.H.; Jiang, M.S. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **2013**, *89*, 23–35. [\[CrossRef\]](#)
8. Lance, A.M.; Symul, T.; Sharma, V. No-Switching Quantum Key Distribution using Broadband Modulated Coherent Light. *Phys. Rev. Lett.* **2005**, *95*, 0503. [\[CrossRef\]](#)
9. Huang, P.; Fang, J.; Zeng, G. State-discrimination attack on discretely modulated continuous-variable quantum key distribution. *Phys. Rev. A* **2014**, *89*, 2330. [\[CrossRef\]](#)
10. 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* **2012**, *86*, 022338. [\[CrossRef\]](#)
11. Leverrier, A.; Grangier, P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. *Phys. Rev. A* **2011**, *83*, 2312. [\[CrossRef\]](#)
12. Leverrier, A.; Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **2009**, *102*, 0504. [\[CrossRef\]](#) [\[PubMed\]](#)
13. Ma, X.F.; Qi, B.; Zhao, Y.; Lo, H.K. Practical Decoy State for Quantum Key Distribution. *Phys. Rev. A* **2005**, *72*, 012326. [\[CrossRef\]](#)
14. Zhao, Y.; Qi, B.; Ma, X.F.; Lo, H.K.; Qian, L. Experimental Quantum Key Distribution with Decoy States. *Phys. Rev. Lett.* **2006**, *96*, 070502. [\[CrossRef\]](#)
15. Weedbrook, C. Continuous-Variable Quantum Key Distribution with Entanglement in the Middle. *Phys. Rev. A* **2012**, *87*, 1110–1116. [\[CrossRef\]](#)
16. Leverrier, A.; Grangier, P. Erratum: Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. *Phys. Rev. Lett.* **2011**, *106*, 259902. [\[CrossRef\]](#)
17. Rémi, B.; Leverrier, A.; Barbieri, M. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A* **2012**, *86*, 2327.
18. Wang, T.; Song, T. Improving the maximum transmission distance of continuous-variable quantum key distribution with noisy coherent states using a noiseless amplifier. *Phys. Lett. A* **2014**, *378*, 2808–2812. [\[CrossRef\]](#)
19. Weedbrook, C.; Lance, A.M.; Bowen, W.P. Quantum cryptography without switching. *Phys. Rev. Lett.* **2004**, *93*, 0504. [\[CrossRef\]](#)
20. Weedbrook, C.; Lance, A.M.; Bowen, W.P. Coherent state quantum key distribution without random basis switching. *Phys. Rev. A* **2006**, *73*, 2316. [\[CrossRef\]](#)
21. García-Patrón, R.; Cerf, N.J. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.* **2009**, *102*, 0501. [\[CrossRef\]](#)
22. Qi, B.; Zhao, Y.; Ma, X.F.; Lo, H.K.; Qian, L. Dual detectors scheme in practical quantum key distribution systems. *Phys. Rev. A* **2007**, *75*, 2304. [\[CrossRef\]](#)

23. Zhao, J.; Haw, J.Y.; Symul, T. Characterization of a measurement-based noiseless linear amplifier and its applications. *Phys. Rev. A* **2017**, *96*, 2319. [[CrossRef](#)]
24. Jie, Z.; Josephine, D.; Yan, H.J. Quantum enhancement of signal-to-noise ratio with a heralded linear amplifier. *Optica* **2017**, *4*, 1421.
25. Haw, J.Y.; Zhao, J.; Dias, J. Surpassing the no-cloning limit with a heralded hybrid linear amplifier for coherent states. *Nat. Commun.* **2016**, *7*, 13222. [[CrossRef](#)] [[PubMed](#)]
26. Takada, A.; Imajuku, W. Amplitude noise suppression using a high gain phase sensitive amplifier as a limiting amplifier. *Electron. Lett.* **1996**, *32*, 677–679. [[CrossRef](#)]
27. Yoshikawa, J.I.; Miwa, Y.; Filip, R. Demonstration of reversible phase-insensitive optical amplifier. *Phys. Rev. A* **2011**, *83*, 4861–4865. [[CrossRef](#)]
28. Müller, C.R.; Wittmann, C.; Marek, P.; Filip, R.; Marquardt, C.; Leuchs, G.; Andersen, U.L. Probabilistic cloning of coherent states without a phase reference. *Phys. Rev. A* **2011**, *86*, 18515–18524. [[CrossRef](#)]
29. Zhang, Y.C.; Li, Z.; Weedbrook, C. Improvement of two-way continuous-variable quantum key distribution using optical amplifiers. *J. Phys. B At. Mol. Opt. Phys.* **2014**, *47*, 5501. [[CrossRef](#)]
30. Ralph, T.C.; Lund, P.A. Nondeterministic Noiseless linear amplification of quantum systems. *Am. Inst. Phys. Conf.* **2009**, *1110*, 155–160.
31. Shannon, C.E.; Syst, B. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423. [[CrossRef](#)]



© 2020 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 (<http://creativecommons.org/licenses/by/4.0/>).