entropy

MDPI

Article

Performance Improvement of Plug-and-Play Dual-Phase-Modulated Quantum Key Distribution by Using a Noiseless Amplifier

Dongyun Bai, Peng Huang *, Hongxin Ma, Tao Wang and Guihua Zeng *

State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China; bdy1993@sjtu.edu.cn (D.B.); x1992mhx@gmail.com (H.M.); tonystar@sjtu.edu.cn (T.W.)

* Correspondence: huang.peng@sjtu.edu.cn (P.H.); ghzeng@sjtu.edu.cn. (G.Z.); Tel.: +86-021-3420-4361 (P.H.); +86-021-3420-4361 (G.Z.)

Received: 9 August 2017; Accepted: 13 October 2017; Published: 20 October 2017

Abstract: We show that the successful use of a noiseless linear amplifier (NLA) can help increase the maximum transmission distance and tolerate more excess noise of the plug-and-play dual-phase-modulated continuous-variable quantum key distribution. In particular, an equivalent entanglement-based scheme model is proposed to analyze the security, and the secure bound is derived with the presence of a Gaussian noisy and lossy channel. The analysis shows that the performance of the NLA-based protocol can be further improved by adjusting the effective parameters.

Keywords: plug-and-play dual-phase-modulated; noiseless linear amplifier (NLA); quantum key distribution

1. Introduction

Quantum information science involves a variety of fields such as quantum cryptography [1], quantum teleportation [2] and quantum communication [3]. The quantum key distribution (QKD) protocol is one of the most feasible and practical applications of quantum information, which allows the two remote parties, normally known as Alice and Bob, to generate and establish a series of secure keys through an insecure quantum channel controlled by an eavesdropper called Eve [4]. The generated key can then be applied in other cryptographic protocols to improve the security. Several achievements have been made in both discrete-variable (DV) QKD [5,6] and continuous-variable (CV) QKD [7,8] in recent years. CVQKD has been promoted as an alternative to DVQKD because it provides higher key distribution rates compared to its DV counterpart [9]. However, the security of QKD lies in the idea that any perturbation on quantum signals will surely introduce some noise, which limits the maximum transmission distance in the quantum channel between the two legitimate parties.

In recent decades, numerous experiments on both DVQKD [9,10] and CVQKD [11,12] have been carried out. In the CVQKD field, generally, the experiments were demonstrated based on the one-way Gaussian-modulated coherent-states (GMCS) scheme. In the one-way experiments, quantum signals obtained from the coherent state were transmitted with a strong local oscillator (LO) over a noisy and lossy optical-fiber channel [13], and the quantum signals were transmitted only once. A recent demonstration of one-way GMCS CVQKD has been achieved over 150 km of optical fiber by controlling excess noise [12]. However, the ignorance of the nonlocal arrangement of LO will lead to wavelength attacks [14], calibration attacks [15] and LO fluctuation attacks [16], which are all related to the loopholes of LO. Therefore, self-referenced CVQKD without sending an LO is proposed, and it can effectively remove the loopholes introduced by the LO transmission [17]. Nevertheless, in the real-life experiments, it is a hard problem to realize content detection for two separate lasers, since

the frequency instability, the fluctuation of the polarizations and the phase drifts caused by phase transmission [18] of the two lasers will ruin the homodyne detection.

In contrast to the above schemes, the plug-and-play configuration [19] can generate a local LO with a single laser source for the two legitimate parties. Unfortunately, the plug-and-play protocol shows higher sensitivity to excess noise compared with one-way GMCS QKD and suffers from Trojan-horse attack [20]. More recently, a plug-and-play CVQKD protocol based on dual-phase-modulated coherent states (DPMCS) [21] is proposed and experimentally demonstrated over a 20-km fiber. This plug-and-play DPMCS protocol can solve the loopholes associated with transmitting LO, as well as remove the instability from the polarization drifts. From the experiment results, this proposed protocol can derive security bounds against collective attacks and provide greater flexibility of shot-noise-limited measurement by controlling the light power of the Local LO. However, in the practical experiments, the excess noise in plug-and-play DPMCS CVQKD is larger than that in normal one-way GMCS CVQKD, and thus, the secure transmission distance is limited to some extent.

In this paper, we consider using a heralded noiseless linear amplifier (NLA) [22] before the homodyne detection as a way to develop the robustness of the plug-and-play DPMCS protocol against noises and losses. Ordinary linear amplifiers can recover classical signals effectively, but when dealing with quantum signals, they only provide limited advantages, as amplification is bound to retain the original signal to noise ratio [23,24]. The probabilistic NLA can amplify the amplitude of a coherent state while obtaining the initial level of noise [25]. The successful running of NLA can compensate the influence of losses and noises, and therefore, it could be used to improve the performance of CVQKD [26]. The availability of NLA has been demonstrated in one-way CVQKD experiments over the last few years, which have provided a solid proof-of-principle. A more practical method of implementing NLA in the CVQKD protocol just by post-selection of the measurements has been proposed [27], which allows one to avoid physical implementation with NLA. A recent research work also shows that a heralded noiseless amplification can be used in a two-way protocol [28].

The question arises whether the sophisticated NLA can be applied to the plug-and-play DPMCS protocol to improve the whole performance. Here, we address this problem, by investigating the most general NLA device. We can obtain the equivalent parameters of the plug-and-play DPMCS and then transferring the situation based on reformulated entanglement-based version (EB) into that without the NLA to compute the secret-key rate. Due to the non-deterministic nature of the NLA, the security proofs with the NLA before homodyne detection are similar to those relevant protocols with secure post-selection. Subsequently, we can find that inserting the NLA can truly help improve the maximum transmission distance of the plug-and-play DPMCS CVQKD while tolerating more excess to some extent.

The paper is organized as follows. In Section 2, we first review the prepare-and-measure (P&M)-based and EB version of the plug-and-play DPMCS CVQKD protocol and the derivation of the expressions of its secret-key rate. In Section 3, the most general NLA is inserted before the homodyne detector, and then, we calculate the equivalent parameters, based on the transmission channel of our protocol. In Section 4, the secret-key rates are computed with the NLA and without the NLA in the plug-and-play DPMCS, and we make the analysis of the performance improvement. Finally, we come to the conclusion and provide discussions in Section 5.

2. Plug-and-Play DPMCS Scheme

2.1. The Model of Plug-and-Play DPMCS Scheme

Generally, in the one-way protocol, Alice prepares the Gaussian signals and sends the signals together with the LO to Bob. The plug-and-play DPMCS protocol aims to overcome some limitations in the normal one-way GMCS protocol, and we first describe the physical models of the proposed plug-and-play DPMCS CVQKD scheme with the untrusted coherent source in the middle under the prepare-and-measure (P&M) and the equivalent entanglement-based (EB) schemes. With the P&M

model illustrated in Figure 1, we can depict the scheme as follows. Alice uses the laser source to generate a strong LO and the classical light via a beam splitter. Then, Alice sends the classical light regarded as an ideal coherent source with shot noise $(\delta X_s, \delta P_s)$ without Gaussian modulation through the optical fiber to Bob. Under the realistic assumption, Eve can control the classical light, and this would inevitably increase excess noise. In this scenario, the untrusted source noise is characterized by introducing a PIA (phase-insensitive amplifier) [29] with a gain of G ($G \geq 1$), in order to model the intervention by Eve. The source noise induced by G can be measured carefully using a practical detector at Bob's side. The quadratures $(\delta X_A, \delta P_A)$ denoting the untrusted coherent source transmitted from Alice to Bob can be described as:

$$\begin{aligned} \delta X_A &= \sqrt{G}\delta X_s + \sqrt{G-1}\delta X_I, \\ \delta P_A &= \sqrt{G}\delta P_s + \sqrt{G-1}\delta P_I. \end{aligned} \tag{1}$$

where $(\delta X_s, \delta P_s)$ satisfy $\langle(\delta X_s)^2\rangle = \langle(\delta P_s)^2\rangle = 1$ (in shot noise units) and (X_I, P_I) denotes an idle input ideally in a vacuum state with a noise variance V_I. Then, Bob uses a dual-phase-modulation scheme to prepare the coherent state, and Bob generates two random Gaussian numbers X_B and P_B of mean value zero and variances V_B. The coherent state $(\delta X_A, \delta P_A)$ is dual-phase-modulated by using two polarization-independent phase modulators installed in a perpendicular position to compensate for the birefringence of the transmission medium automatically. The prepared quadratures sent from Bob to Alice are:

$$\begin{aligned} X &= X_B + \delta X_A, \\ P &= P_B + \delta P_A. \end{aligned} \tag{2}$$

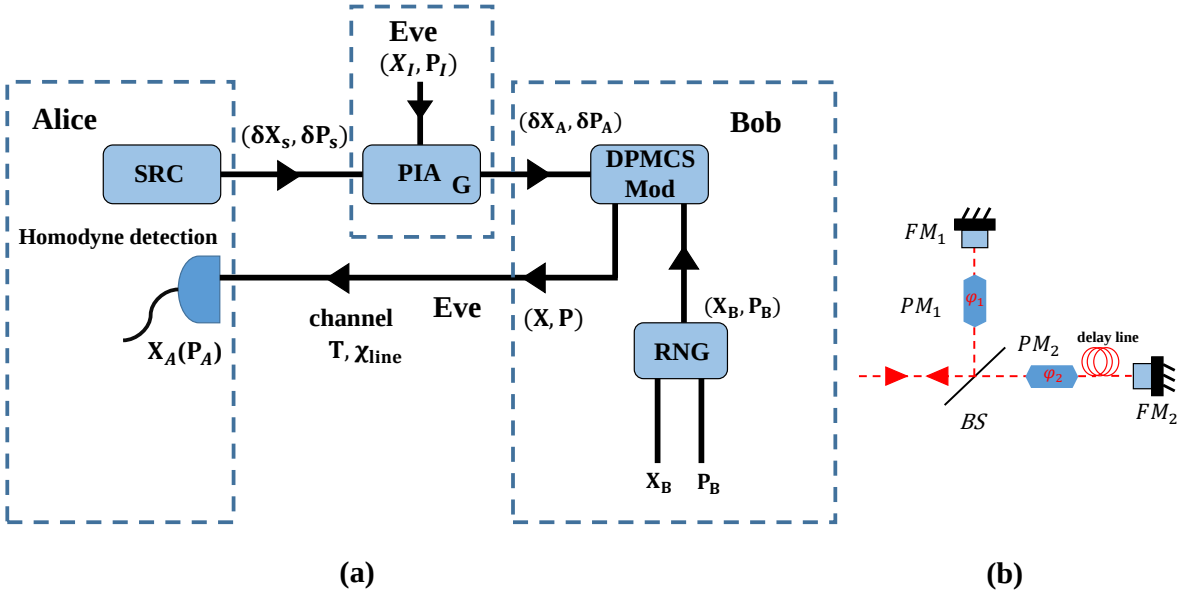

Figure 1. (**a**) The prepare-and-measure (P&M) scheme of the plug-and-play dual-phase-modulated coherent states (DPMCS) protocol with the untrusted laser coherent source. A phase-insensitive amplifier (PIA) can amplify both quadratures symmetrically, while the input noise will increase as the result of the coupling process to internal modes. A PIA can be ideally described as a nondegenerate optical parametric amplifier. RNG is random number generator. (**b**) The dual-phase-modulated scheme. FM, Faraday mirror; PM, phase modulator; BS, beam splitter.

The modulated random input from RNG satisfies the Gaussian distribution, so the variances of X and P satisfy:

$$\langle X^2 \rangle = \langle P^2 \rangle = V + \xi_s, \tag{3}$$

where $V = V_B + 1$, $\xi_s = G - 1 + (G-1)V_I$ and V_I can be set to one (in shot noise units) to model a vacuum state. Bob sends the prepared coherent state to Alice through a quantum channel with a transmittance efficiency T and excess noise ε_c; the channel-added noise referred to the channel input can be expressed as $\chi_{line} = 1/T - 1 + \epsilon_c$ (in shot-noise units). In this scheme, Alice uses homodyne detection to randomly measure one of the two quadratures. A practical homodyne detector for Alice can be modeled with the electrical noise V_{el} and an efficiency η_A. Therefore, the detection-added noise referred to Alice's input can be expressed in shot-noise units as $\chi_{hom} = [(1-\eta_A) + V_{el}]/\eta_A$. Then, the total added-noise can be denoted as $\chi_{tot} = \chi_{line} + \chi_{hom}/T$. The following procedures such as classical reverse reconciliation and privacy amplification are similar to those in the normal one-way GMCS protocols.

After analyzing the P&M scheme above, the equivalent EB scheme is derived in Figure 2 with homodyne detections. We should remark that the optimality of a Gaussian attack is guaranteed under a general collective attack. In the EB scheme, Alice's detector efficiency can be modeled by a beam splitter (BS) with transmission efficiency η_A and an Einstein–Podolsky–Rosen (EPR) state ρ_{GH_0} with a variance V_d coupled to the BS. V_d is valued as $V_d = \eta_A \chi_{hom}/(1-\eta_A) = (1-\eta_A+V_{el})/(1-\eta_A)$ when Alice uses homodyne detection to correspond with the P&M detection-added noise. When Bob's detection and the EPR state are hidden in the black box, Eve cannot distinguish which scheme is applied between the P&M scheme and the EB scheme to ensure safety. It should be mentioned here when $G = 1$, the noise $\xi_s = 0$, so in this situation, the plug-and-play DPMCS EB scheme can be regarded as a typical GMCS EB scheme.

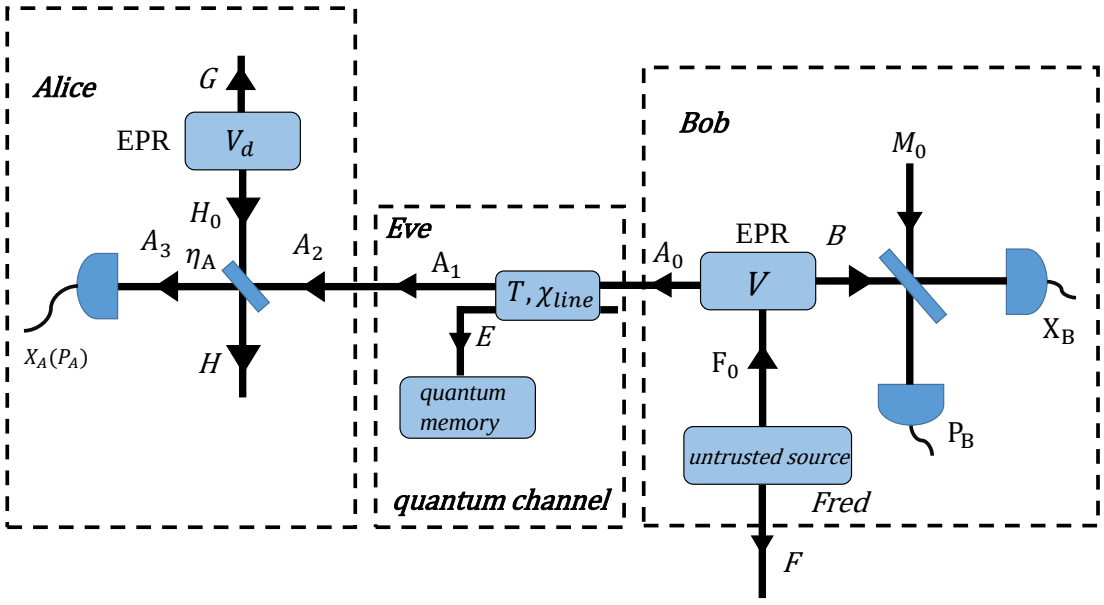

Figure 2. The schematic of the equivalent entanglement-based scheme of the plug-and-play DPMCS protocol. Although Eve has no access to the users' apparatus, the source is regarded to be equivalently controlled in the plug-and-play protocol. Eve can either control Fred or not, to derive a tight secure bound, and Fred will be assumed to be controlled by Eve instead of a mere neutral party. EPR, Einstein–Podolsky–Rosen.

2.2. Calculation of Secret-Key Rate with Reverse Reconciliation

In the above part, we analyzed the plug-and-play DPMCS in detail, and in this part, we will analyze the secret-key rate based on the EB protocol with reverse reconciliation. As mentioned before, to derive a tight security bound, Fred is assumed to be controlled by Eve, which means Eve may acquire some extra secret-key information. What should be further pointed out is that Bob might prepare an impure state; thus, the security bound is a lower and tight bound under Gaussian attack. As we did in the one-way GMCS scheme, the secret-key rate against collective attacks [30] can be calculated as:

$$\Delta I = \beta I_{AB} - \chi_{AE}. \tag{4}$$

where β is the reconciliation efficiency, I_{AB} is the Shannon mutual information between the two legitimate parties and χ_{AE} represents the maximum information Eve could get from Alice. It should be mentioned here that the security proofs show that the derived bounds in the collective attacks remain asymptotically valid for arbitrary coherent attacks, and therefore, the results in this paper are valid for both collective attacks and coherent attacks. The mutual information between Alice and Bob when Alice uses homodyne detection can be calculated as:

$$I_{AB}^{hom} = \frac{1}{2}\log_2\frac{V_A}{V_{A|B}} = \frac{1}{2}\log_2\frac{V+\xi_s+\chi_{tot}}{1+\xi_s+\chi_{tot}}. \tag{5}$$

where the variance measured by Alice $V_A = \eta_A T(V+\xi_s+\chi_{tot})$ and the conditional variance $V_{A|B} = \eta_A T(1+\xi_s+\chi_{tot})$. V, ξ_s, χ_{tot} and χ_{line} take the corresponding forms in the above part. Using the fact that Eve can purify the system ρ_{BFA_1E} and Alice's measurement can purify the system ρ_{FBEHG}, with the fact that $S(\rho_{FBEHG}^{m_A})$ is independent of m_A for Gaussian protocols and the global pure state will collapse to ρ_{FBEHG}, the maximum information available to Eve on Alice is bounded by the Holevo quantity [31]. We can derive the form as:

$$\begin{aligned}
\chi_{AE}^{hom} &= S(\rho_E) - \int dm_A p(m_A) S(\rho_E^{m_A}), \\
&= S(\rho_{BFA_1E}) - S(\rho_{FBEHG}^{m_A}), \\
&= \sum_{i=1}^{2} G(\frac{\lambda i - 1}{2}) - \sum_{i=3}^{5} G(\frac{\lambda_i - 1}{2}).
\end{aligned} \tag{6}$$

where m_A is the measurement of Alice and in the homodyne detection, and it can be $m_A = x_A$ or $m_A = p_A$ ($dm_A = dx_A$ or $dm_A = dp_A$). $\rho_E^{m_A}$ is the eavesdropper's conditional state on Alice. S is the Neumann entropy of the quantum state ρ, and $p(m_A)$ is the probability of Alice's measurement. $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. $\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix γ_{BFA_1E}, which characterizes the state ρ_{FBA_1E}, and $\lambda_{3,4,5}$ represent the symplectic eigenvalues of the covariance matrix $\gamma_{FBEHG}^{m_A}$ characterizing the state $\rho_{FBEHG}^{m_A}$ after Alice's projective measurement. The covariance matrix γ_{BFA_1E} has the following expression due to its dependence on the system including Bob and the lossy and noisy quantum channel.

$$\gamma_{BFA_1E} = \begin{bmatrix} V \cdot I_2 & \sqrt{T(V^2-1)} \cdot \sigma_z \\ \sqrt{T(V^2-1)} \cdot \sigma_z & T(V+\xi_s+\chi_{line}) \cdot I_2 \end{bmatrix}, \tag{7}$$

where I_2 is the 2×2 unit matrix and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. The symplectic eigenvalues of the above covariance matrix can be expressed in the form as:

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}], \tag{8}$$

where *A and* B can be expressed as:

$$\begin{aligned} A &= V^2(1-2T)+2T+T^2(V+\xi_s+\chi_{line})^2, \\ B &= T^2(1+V\chi_{line}+V\xi_s)^2. \end{aligned} \tag{9}$$

The covariance matrix $\gamma^{m_A}_{FBEHG}$ can be expressed as:

$$\gamma^{m_A}_{FBEHG} = \gamma_{FBEHG} - \sigma^T_{FBEHGA_3} H_{hom} \sigma_{FBEHGA_3}. \tag{10}$$

In the above equation, $H_{hom} = (X\gamma_{A_3}X)^{MP}$ stands for the homodyne detection on mode A_3; here, $X = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and Moore–Penrose pseudo-inverse of a matrix MP. The matrices γ_{A_3}, γ_{FBEHG}, γ_{FBEHGA_3} can be all obtained from the decomposition of the covariance matrix:

$$\gamma_{FBEHGA_3} = \begin{bmatrix} \gamma_{FBEHG} & \sigma^T_{FBEHGA_3} \\ \sigma_{FBEHGA_3} & \gamma_{A_3} \end{bmatrix}. \tag{11}$$

can be derived with appropriate rearrangements of columns and lines from the matrix describing the system $FBEA_3HG$ (Figure 3):

$$\gamma_{FBEA_3HG} = (Y^{BS})^T[\gamma_{FBA_1E} \oplus \gamma_{H_0G}]Y^{BS}. \tag{12}$$

Here, γ_{FBA_1E} is given in Equation (7), and γ_{H_0G} is the matrix that describes the EPR state of variance v_d used to model the homodyne detector's electronic noise. The matrix can be written as:

$$\gamma_{H_0G} = \begin{bmatrix} v_d \cdot I_2 & \sqrt{(v_d^2-1)} \cdot \sigma_z \\ \sqrt{(v_d^2-1)} \cdot \sigma_z & v_d \cdot I_2 \end{bmatrix}. \tag{13}$$

where v_d is mentioned before as $v_d = (1-\eta_A+v_{el})/(1-\eta_A)$. The matrix Y^{BS} describes the beam splitter transformation, which models the inefficiency of the homodyne detector on acting mode A_2 and H_0. It can be written as:

$$\begin{aligned} Y^{BS} &= I_F \oplus I_B \oplus Y^{BS}_{A_2H_0} \oplus I_G \\ Y^{BS}_{A_2H_0} &= \begin{bmatrix} \sqrt{\eta_A} \cdot I_2 & \sqrt{1-\eta_A} \cdot I_2 \\ -\sqrt{1-\eta_A} \cdot I_2 & \sqrt{\eta_A} \cdot I_2 \end{bmatrix}. \end{aligned} \tag{14}$$

Till now, we get all the elements to calculate the symplectic eigenvalues $\lambda_{3,4,5}$, and they are given by expressions with homodyne detection as:

$$\lambda^2_{3,4} = \frac{1}{2}[C_{hom} \pm \sqrt{C^2_{hom} - 4D_{hom}}], \lambda_5 = 1, \tag{15}$$

where:

$$\begin{aligned} C_{hom} &= \frac{A\chi_{hom} + V\sqrt{B} + T(V+\xi_s+\chi_{line})}{T(V+\xi_s+\chi_{tot})} \\ D_{hom} &= \frac{V\sqrt{B} + B\chi_{hom}}{T(V+\xi_s+\chi_{tot})}. \end{aligned} \tag{16}$$

where χ_{line} and χ_{hom} can be expressed as:

$$\chi_{hom} = \frac{(1-\eta_A)+v_{el}}{\eta_A}. \tag{17}$$

$$\chi_{tot} = \chi_{line} + \frac{\chi_{hom}}{T}. \tag{18}$$

Using the related equations above, we can calculate the asymptotic lower bound of the secret-key rates in Equation (4) against collective attacks.

3. Channel Equivalence of Plug-and-Play DPMCS CVQKD with NLA

From the above section, we have analyzed the security of the plug-and-play DPMCS CVQKD scheme with its equivalent EB scheme. In this section, we use the most general NLA before Alice's homodyne detection in our scheme shown in Figure 3. In this new version of the scheme, Alice and Bob implement the plug-and-play DPMCS protocol, while Alice adds an NLA before her homodyne detection to her stage; here, we assume Alice's homodyne detector is perfect ($\eta_A = 1$ and $V_{el} = 0$), and all the rest of our calculations are based on this condition. Then, only the events in accord with a successful amplification can be used to extract the secret-key rate, which can be regarded as similar to those protocols with suitable post-selection.

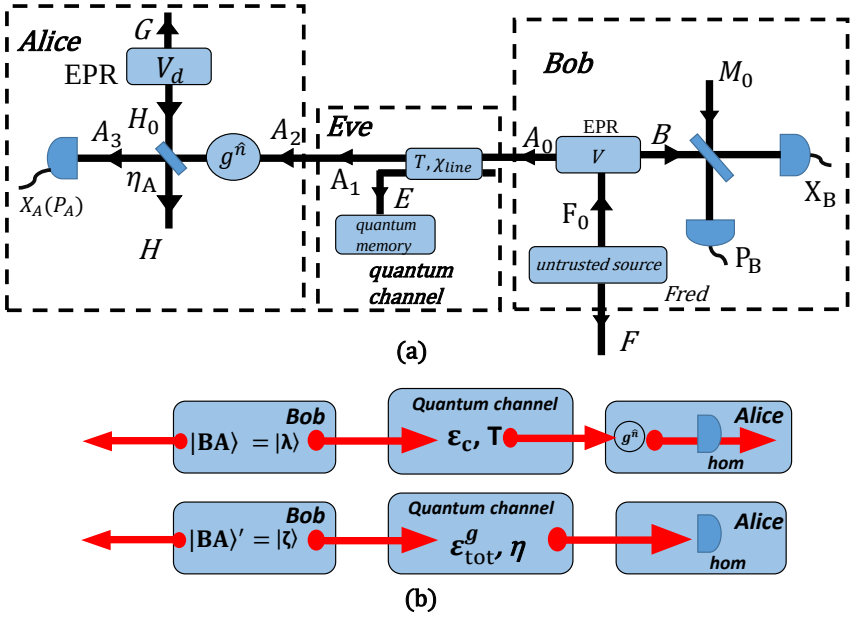

Figure 3. (**a**) Plug-and-play DPMCS scheme with the noiseless linear amplifier (NLA) before Alice's homodyne detection. Eve uses the EPR states to perform the collective attack, and Fred might be controlled by Eve. (**b**) The basic equivalent protocol with and without the NLA. The lower bound of the secret-key rate corresponding to the successful amplification in the protocol $(\lambda, \varepsilon_c, T)$ and the virtually equivalent protocol $(\zeta, \varepsilon^g_{tot}, \eta)$.

Since the plug-and-play protocol is quite similar to the one-way protocol with the noisy and lossy Gaussian quantum channel and the output of the NLA remains in the Gaussian regime, it is reasonable for us to derive the equivalent parameters ζ, ε^g_{tot}, η of the state sent from Bob to Alice to help us keep the same average value and variance, thus finally obtaining the secret-key rates.

Firstly, to simplify the model, the input state $\hat{\rho}$ is a thermal state before Alice's homodyne detector, which can be expressed as $\hat{\rho_{th}}(\lambda_{ch}) = (1-\lambda_{ch}^2)\sum_{n=0}^{\infty}\lambda_{ch}^{2n}|n><n|$ with variance $V(\lambda) = \frac{1+\lambda^2}{1-\lambda^2}$. Then, the state is displaced by $\alpha = \alpha_x + i\alpha_y$, and it comes out as:

$$\hat{\rho} = \hat{D}(\alpha)\hat{\rho}_{th}(\lambda_{ch})\hat{D}(-\alpha) \tag{19}$$

This would be the state received when Alice knows Bob's heterodyne measurement results. As discussed in detail in [22], when the state passes through the NLA, we can conclude that the state is transformed into:

$$\hat{\rho}' = \hat{D}(\tilde{g}\alpha)\hat{\rho}_{th}(g\lambda_{ch})\hat{D}(-\tilde{g}\alpha). \tag{20}$$

where $\tilde{g}$ equals $g\frac{1-\lambda_{ch}^2}{1-g^2\lambda_{ch}^2}$. The parameter g should satisfy $g\lambda_{ch} < 1$ to keep the system's physical interpretation. Let us find the the values of α and λ_{ch} corresponding to the equivalent EB scheme in the above parts. When Bob encodes the Gaussian variables and obtains the results β_B after heterodyne detection on one mode of the EPR mode $|BA\rangle = |\lambda\rangle$, the second mode is projected on a coherent state with an amplitude proportional to $\lambda\beta_B$. Additionally, when the second state is sent through the quantum channel of transmittance T, the displacement α can be taken as:

$$\alpha = \sqrt{T}\lambda\beta_B. \tag{21}$$

From the last section, we can clearly see the incoming state before Alice's homodyne detector with the variance $TV_B + 1 + T\xi_s + T\epsilon_c$. Then, the variance $\frac{1+\lambda_{ch}^2}{1-\lambda_{ch}^2}$ of the thermal state corresponds to Alice's variance when $V_B = 0$ can be expressed as:

$$\begin{aligned} \frac{1+\lambda_{ch}^2}{1-\lambda_{ch}^2} &= 1 + T(\xi_s + \epsilon_c) \\ \Rightarrow \lambda_{ch}^2 &= \frac{T(\xi_s+\epsilon_c)}{2+T(\xi_s+\epsilon_c)}. \end{aligned} \tag{22}$$

Next, the action of the NLA on a displaced thermal state given in Equation (20) produces the transformation:

$$\begin{aligned} \sqrt{T}\lambda\beta_B &\xrightarrow{NLA} g\frac{1-\lambda_{ch}^2}{1-g^2\lambda_{ch}^2}\sqrt{T}\lambda\beta_B \\ \frac{T(\xi_s+\epsilon_c)}{T(\xi_s+\epsilon_c)+2} &\xrightarrow{NLA} g^2\frac{T(\xi_s+\epsilon_c)}{2+T(\xi_s+\epsilon_c)}. \end{aligned} \tag{23}$$

The next step is to think about the action of the NLA when Alice does not have any knowledge of Bob's measurement. In such a situation, her state is a thermal state $\hat{\rho_B} = (1-\lambda^{*2})\sum_{n=0}^{\infty}(\lambda^*)^{2n}|n><n|$, and we can obtain:

$$\begin{aligned} \frac{1+\lambda^{*2}}{1-\lambda^{*2}} &= 1 + TV_B + T(\xi_s+\epsilon_c), \\ \Rightarrow \lambda^{*2} &= \frac{T(2\lambda^2 + (\xi_s+\epsilon_c)(1-\lambda^2))}{2-2\lambda^2-\lambda^2T(\xi_s+\epsilon_c-2)+T(\epsilon_c+\xi_s)}. \end{aligned} \tag{24}$$

where $V_B = V - 1 = \frac{1+\lambda^2}{1-\lambda^2} - 1$. Since the NLA always transform a thermal state with a gain of g, we can derive:

$$\frac{T(2\lambda^2 + (\xi_s+\epsilon_c)(1-\lambda^2))}{2-2\lambda^2-\lambda^2T(\xi_s+\epsilon_c-2)+T(\xi_s+\epsilon_c)} \xrightarrow{NLA} g^2\frac{T(2\lambda^2 + (\xi_s+\epsilon_c)(1-\lambda^2))}{2-2\lambda^2-\lambda^2T(\xi_s+\epsilon_c-2)+T(\xi_s+\epsilon_c)}. \tag{25}$$

Now, all the equations required to resolve the equivalent expression of the effective parameters ζ, ϵ_{tot}^{g}, η are obtained. Using the equations above, those parameters should satisfy:

$$\sqrt{\eta}\zeta = g\frac{1-\lambda_{ch}^2}{1-g^2\lambda_{ch}^2}\sqrt{T}\lambda. \tag{26}$$

$$\frac{\eta\epsilon_{tot}^{g}}{\eta\epsilon_{tot}^{g}+2} = g^2\frac{T(\xi_s+\epsilon_c)}{T(\xi_s+\epsilon_c)+2}. \tag{27}$$

$$\frac{\eta(2\zeta^2+\epsilon_{tot}^{g}(1-\zeta^2))}{2-2\zeta^2-\zeta^2\eta(\epsilon_{tot}^{g}-2)+\eta\epsilon_{tot}^{g}} = g^2\frac{T(2\lambda^2+(\xi_s+\epsilon_c)(1-\lambda^2))}{2-2\lambda^2-\lambda^2T(\xi_s+\epsilon_c-2)+T(\xi_s+\epsilon_c)}. \tag{28}$$

This system can be resolved and the solution can be expressed as below:

$$\begin{aligned}
\zeta &= \lambda\sqrt{\frac{T(g^2(\xi_s+\epsilon_c-2)-(\xi_s+\epsilon_c-2))-2}{\eta(g^2-1)(\xi_s+\epsilon_c)-2}},\\
\eta &= g^2\frac{T}{T(g^2-1)(\frac{1}{4}T(\xi_s+\epsilon_c)(g^2-1)(\xi_s+\epsilon_c-2)+1-(\xi_s+\epsilon_c))+1},\\
\epsilon_{tot}^{g} &= (\xi_s+\epsilon_c)-\frac{1}{2}(\xi_s+\epsilon_c)T(g^2-1)(\xi_s+\epsilon_c-2).
\end{aligned} \tag{29}$$

Then, we should pay attention to the effective parameters satisfying $0 \le \lambda < 1, 0 \le \eta < 1$, so we can obtain:

$$0 \le \lambda < \left(\sqrt{\frac{T(g^2(\xi_s+\epsilon_c-2)-(\xi_s+\epsilon_c-2))-2}{T(g^2-1)(\xi_s+\epsilon_c)-2}}\right)^{-1}. \tag{30}$$

Then, we can derive the maximum gain g_{max} for those physical-value parameters as:

$$g_{max} = \sqrt{\frac{(\xi_s+\epsilon_c)(T(\xi_s+\epsilon_c-4)+2)+4\sqrt{\frac{T(\xi_s+\epsilon_c-2)+2}{\xi_s+\epsilon_c}}-2\sqrt{(\xi_s+\epsilon_c)(T(\xi_s+\epsilon_c-2)+2)}+4T-4}{T(\xi_s+\epsilon_c-2)^2}}. \tag{31}$$

After deriving these results, we must consider the validity of these expressions. Firstly, these parameters naturally degenerate to the real physical parameters without the NLA where $g = 1$,

$$g = 1 \Rightarrow \zeta = \lambda, \eta = T, \epsilon_{tot}^{g} = \xi_s + \epsilon_c. \tag{32}$$

Then, when there is no excess noise ($\xi_s + \epsilon_c = 0$), they match the similar results in previous outcomes:

$$\epsilon_{tot}^{g} = 0 \Rightarrow \zeta = \lambda\sqrt{1+(g^2-1)T}, \eta = \frac{g^2T}{1+g^2T-T}, \epsilon^{g} = 0. \tag{33}$$

Through complex calculations, we can use the equivalent parameters to calculate and compare the secret-key rate ΔI_{NLA} with and without an ideal NLA in the next section.

4. Increase of the Maximum Transmission Distance

In Section 2, we have analyzed the DPMCS scheme and obtained the secret-key rate analysis. In Section 3, we get our needed parameters to calculate the secret-key rate with the NLA. The secret-key rate comparison must be performed in a given channel with fixed transmittance T and total excess noise ϵ_{tot}, which cannot be controlled by the two legitimate parties. Bob is allowed to optimize his modulation variance V_B in order to maximize the secret-key rates, for the modulation cannot be infinite. Here, we come to the successful amplification of the NLA with the probability P_{ssf}. The precise value of the P_{ssf} depends on practical implementations. Since we only care about the maximum distance and endurable excess noise, the precise value of the P_{ssf} is not crucial to our study because the NLA cannot

transform a negative secret-key into a positive one. We can assume P_{ssf} is constant and reaches the upper limitation of $1/g^2$ [22] when the NLA has a sufficient dynamics to neglect distortions. Therefore,

$$\Delta I_{NLA} = P_{ssf}\Delta I(\eta, \epsilon_{tot}^{g}). \tag{34}$$

Before calculation, let us find out if the maximum gain of NLA g_{max} only depends on T, ξ_s and ϵ_c from Equation (31); we give the relationship in Figure 4 between the g_{max} and the channel losses in dB, while the parameter ϵ_c is 0.04, which is achievable from previous experiments [32]. The parameter g_{max} here means the maximum gain to satisfy the physical meaning constraints $0 \leq \eta < 1$, and all the equivalent parameters take physical values.

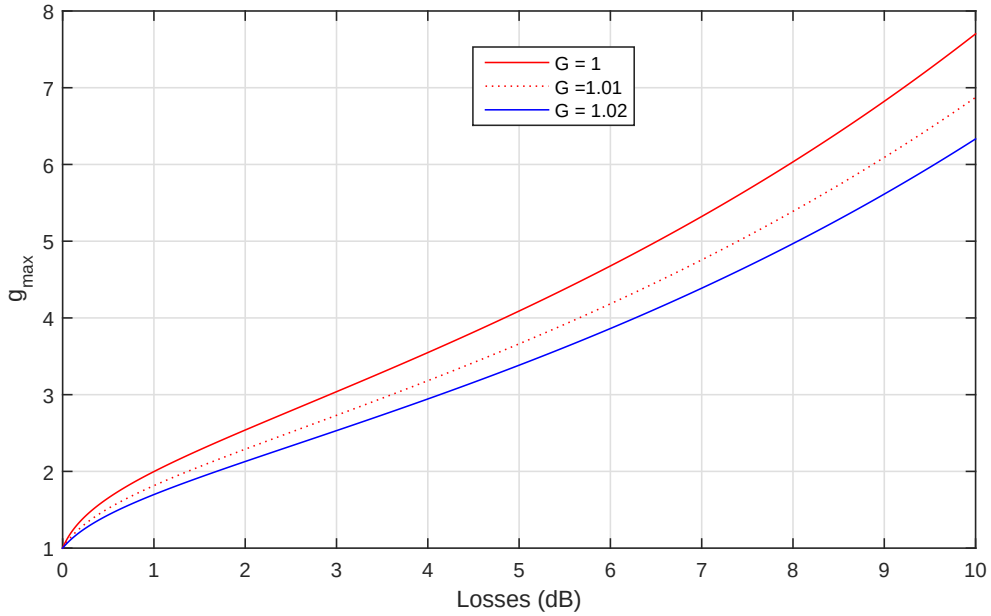

Figure 4. In the curve, g_{max} against the losses in dB, where $\epsilon_c = 0.04$, $V_I = 1$ represents that the noise variance of the PIA in Figure 1 is one (in shot-noise units); G has different values of 1, 1.01, 1.02. We can clearly see g_{max} increase with the increase of the losses.

From the illustration, we cannot use a fixed g_{max} to match every value of T. For instance, in the above illustration, when the loss is 0 dB, which means the transmittance T is one, g_{max} can be derived as one, which means the NLA cannot be used in the channel with no losses. However, for general strong losses, g_{max} is large enough, and the NLA has a sufficient dynamics; thus, we can use the NLA with constant g to help us to improve the performance of the plug-and-play DPMCS CVQKD scheme.

The simulations of ΔI and ΔI_{NLA} with the same parameter transmittance T and excess noise ϵ_c are shown in Figure 5. We can see that the secret-key rates with the NLA of gain g remain positive for losses, which can be maximally improved by $\Delta_{\sum} = 20\log_{10}g = 9.5$ dB. Here, we briefly calculate this result. The transmittance T with the NLA of gain g can be transformed into $T_{NLA} = T/g^2$ of high losses. When calculating the maximum distance, we set the maximum losses with positive secret-key rates to zero, which can be derived as:

$$10^{\frac{-m}{10}} = g^2 10^{\frac{-M}{10}} \tag{35}$$

where M and m represent the maximum losses when the secret-key rates remain positive with and without the NLA. After calculation, we could obtain $M - m = 20\log_{10}g$.

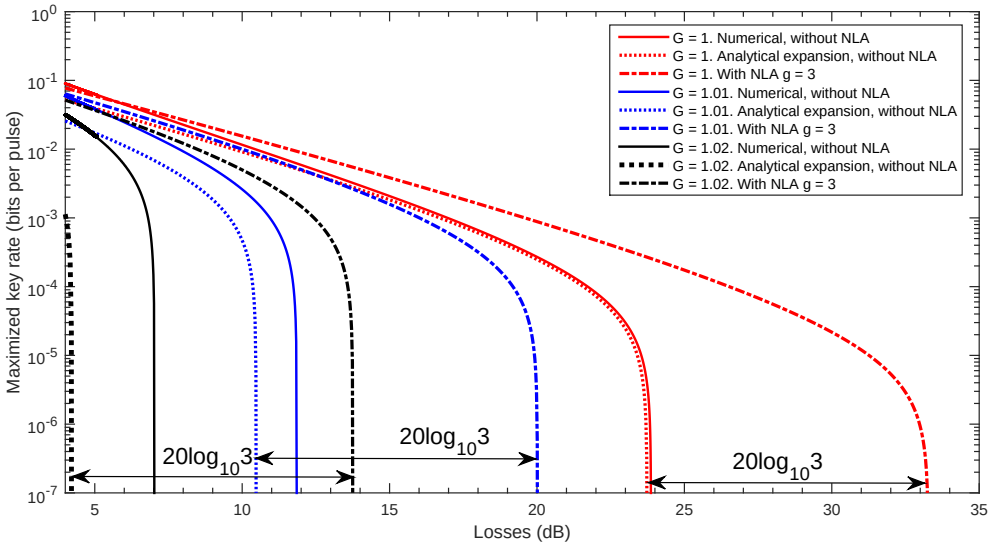

Figure 5. Maximized secret-key rates against losses in dB units. The maximization is performed in different ξ_s, which is determined by the eavesdropper. Due to the probability of success $1/g^2$, it is reasonable for us to keep the information on its positivity. The parameters needed are as below: $\beta = 0.9$, $V = 3.3$, $\epsilon_c = 0.04$. From left to right, the dashed, solid and dash-dotted lines represent the analytical series expansion without NLA, the numerical expansion without NLA and using the NLA corresponding to the secret-key rates for $G = 1, 1.01, 1.02$.

There are some other points we need to address from Figure 5. From the simulations, the parameter ξ_s to model Fred's behaviors can affect the transmission distance, and we see that with the increased $\xi_s = (G-1) + (G-1)V_I$, the maximal transmission distance will decrease. Additionally, when ξ_s is zero, the numerical curve is in great agreement with the analytical series expansion curve without NLA; however, with the increase in ξ_s, we can clearly see the departure between the numerical curve and the analytical series expansion curve without NLA. The reason can be explained as the increase in G reduces the maximum transmission, as well as it breaks the high-loss condition, which can be regarded as the main reason. Therefore, to improve the performance, it is reasonable for us to reduce the influence controlled by Fred when we use our plug-and-play DPMCS scheme with the NLA.

The other important quality for the plug-and-play DPMCS scheme with the NLA is the tolerable excess noise. The maximum tolerable excess noise against losses for our proposed protocol by using an NLA with gain $g = 2$ and $g = 3$ is shown in Figure 6, where we can also get the maximal excess noise against losses without the NLA.

Here, we do not compare the maximum tolerable excess noise when $G = 1.02$ (refers to $\xi_s = 0.04$) because from Figure 5, we can see its analytical expansion secret-key rates drop to zero quickly within the loss around 4 dB, which cannot satisfy the high-loss condition, so it is not necessary for us to draw its illustration to prove our conclusion. From the scene where $G = 1.01$, we can clearly see that the NLA can help to tolerate more excess noise, and with increased g, the maximum tolerable excess noise will increase, as well. We can also see that the permitted maximum losses can be maximally extended as $20\log_{10} g$ dB with the NLA in the analytical expansion.

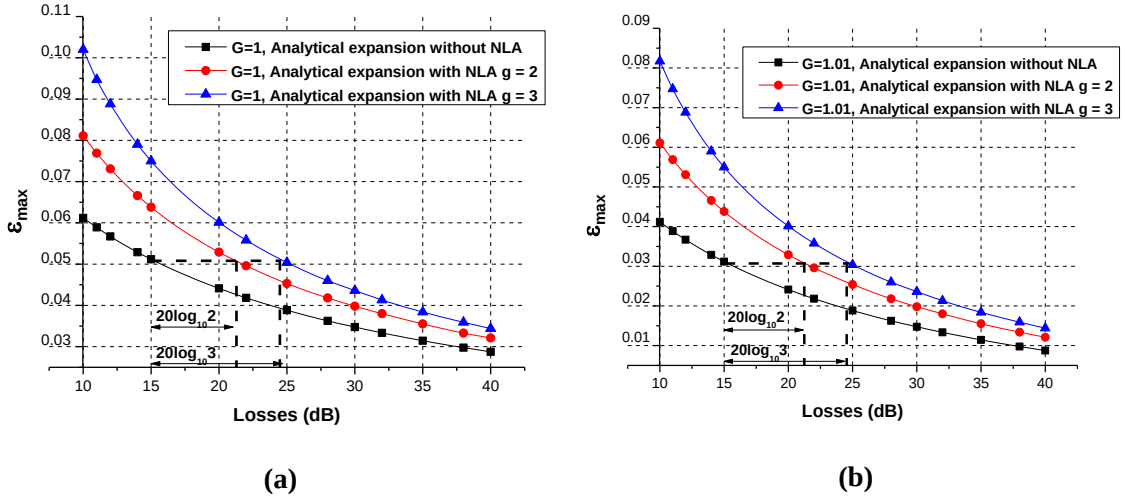

Figure 6. Maximum excess noise in analytical expansion against losses when the secret-key rates are positive. (**a**) represents $G = 1$ with and without NLA. (**b**) represents $G = 1.01$ with and without NLA. The curves only depend on the positivity of the secret-key rates rather than the success probability. We can see that NLA can help tolerate more excess noise in high losses.

Finally, we come to the optimal parameters analysis. Here, we consider the parameters including reverse reconciliation efficiency β, the variance V_B and the gain of NLA g. From Figure 7a, we can clearly see with the increase of β that the maximized secret-key rates will also increase. However, the parameter ξ_s introduced by Fred can affect the secret-key rates, and we can see when $\xi_s = 0$, the minimum value of β for positive secret-key rates is around 0.8 while the minimum value is around 0.87 when $\xi_s = 0.02$ when the loss is 16 dB and the gain g is three. Physically, ξ_s, here introduced by Fred referring to the increased excess noise, corresponds to the imperfections of the coherent states of the signal source. From Figure 7b, the increased variance V_B can help increase the maximized secret-key rates when V_B reaches a certain value, but beyond that value, the secret-key rates will drop and even become negative when V_B is too large. Therefore, there exists an optimal variance V_B to obtain the maximized secret-key rates, and from Figure 7, we can see that the optimal V_B is almost the same as the increased gain g of the NLA.

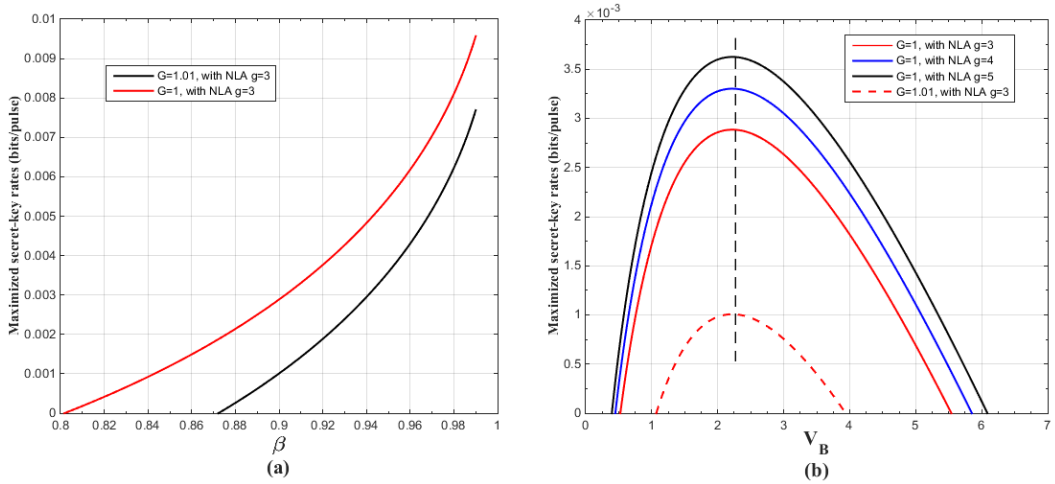

Figure 7. Maximized secret-key rates against reverse reconciliation efficiency β and the variance V_B. In (**a**), the excess noise ϵ_c is 0.04; the loss is 16 dB; λ is optimized in accord with β from [22]. In (**b**), the excess noise ϵ_c is 0.04; the loss is 16 dB; and the reverse reconciliation is 0.9. In both (**a**,**b**), ξ_s introduced by Fred will affect the secret-key rates.

From Figure 8, we can see that the NLA can help increase the secret-key rates when the gain g is up to a certain value, but beyond that certain value, the secret-key rates will drop and even become negative when g is too large. So there exists an optimal value g, and the optimal value of g slightly increases with the excess noise ξ_s. The reason can be mainly explained by the fact that when g is too large, the effective excess noise ϵ_{tot}^{g} would be too large from Equation (29), though the transmittance η is higher, to give a positive secret-key rate. Furthermore, when ξ_s is introduced by Fred, the maximized secret-key rates and the positive range will both decrease.

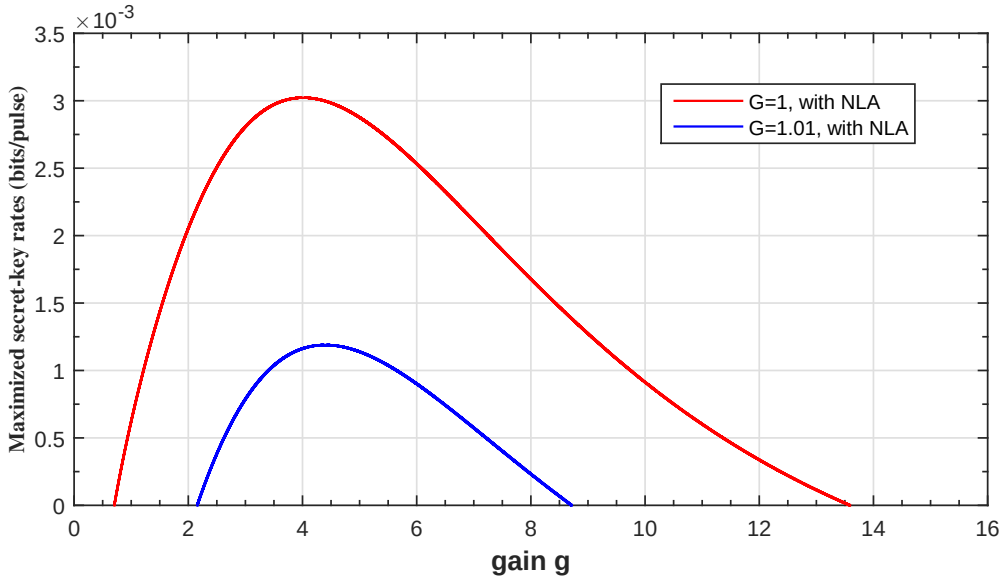

Figure 8. Maximized secret-key rates against the gain g of the NLA. The probability of success is $1/g^2$; the excess noise ϵ_c is 0.04; the loss is 16 dB; and the reverse reconciliation efficiency is 0.9. With the increased g, the secret-key rates will increase to a certain value. Beyond the certain value, the secret-key rates will drop and even become negative.

5. Conclusions and Discussions

In this paper, we have reviewed the plug-and-play DPMCS scheme, and based on its equivalent protocol, we analyze its security. Then, we propose the scheme using a noiseless linear amplifier before the receiver's homodyne detection to improve the performance against losses and noises. Our calculation of the secret-key rates with the NLA is based on an effective system, which is equivalent to the EB-based protocol where the quantum signals are sent through a Gaussian noisy and lossy quantum channel. We demonstrate that the NLA can help increase the distance by the equivalent $20\log_{10}g$ dB of losses, and it may help the scheme to tolerate more excess. However, we should here closely address the noise ξ_s controlled by Fred, which will affect the maximum improved transmission distance to get better performance.

For future work, we will further consider the adjustments of the system parameters and the use of the same NLA before Bob's heterodyne detection to get better performance, as well as keep the symmetry of the whole scheme. Moreover, it should be mentioned here that the gap analysis between practical implementations and theoretical models with NLA should also be considered, and the effects of the imperfections are also influential in our experiments. If more complex parameters are considered, the experimental conditions will deserve more investigation.

Acknowledgments: This work is supported by the National Natural Science Foundation of China (Grant Nos. 61332019, 61671287, 61631014) and the national key research and development program (Grant No. 2016YFA0302600).

Author Contributions: Dongyun Bai designed the conception of the study, accomplished the formula derivation and numerical simulations and drafted the article. Peng Huang gave the general idea of the study, checked the draft and provided feasible suggestions and critical revision of the manuscript. Hongxin Ma gave feasible advice and helped with the calculation. Tao Wang conceived of the study and reviewed relevant studies. Guihua Zeng reviewed relevant studies and literature, conceived of and designed the study and performed critical revision of the manuscript. All authors have read and approved the final manuscript.

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

References

1. Ekert, A.K. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663.
2. Bennett, C.H.; Brassard, G.; Crépeau, C.; Jozsa, R.; Peres, A.; Wootters, W.K. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **1993**, *70*, 1895–1899.
3. Bennett, C.H.; Wiesner, S.J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **1992**, *69*, 2881–2884.
4. 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.
5. Lo, H.-K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2014**, *8*, 595–604.
6. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145.
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.
8. Samuel, L.B.; Peter, V.L. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513.
9. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902.
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.
11. Huang, D.; Lin, D.K.; Huang, P.; Wang, C.; Liu, W.Q.; Fang , S.H.; Zeng, G.H. Continuous-variable quantum key distribution with 1 Mbps secure key rate. *Opt. Express* **2015**, *23*, 17511.
12. Huang, D.; Huang, P.; Lin, D.K.; Zeng, G.H. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **2016**, *6*, 19201.
13. Jouguet, P.; kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **2013**, *7*, 378.
14. 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.
15. 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.
16. 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.
17. 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.
18. Marie, A.; Alléaume, R. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *95*, 012316.
19. Legre, M.; Zbinden, H.; Gisin, N. Implementation of continuous variable quantum cryptography in optical fibres using a go-&-return configuration. *Quantum Inf. Comput.* **2006**, *6*, 326.
20. Jain, N.; Anisimova, E.; Khan, I.; Markarov, V.; Marquardt, C.; Leuchs, G. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.* **2014**, *16*, 123030.
21. Huang, D.; Huang, P.; Wang, T.; Li, H.S.; Zhou, Y.M.; Zeng, G.H. Bass-SIR model for diffusion of new products in social networks. *Phys. Rev. A* **2016**, *94*, 032305.
22. 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*, 012–327.
23. Ferreyrol, F.; Blandino, R.; Barbieri, M.; Tualle-Brouri, R.; Grangier, P. Experimental realization of a nondeterministic optical noiseless amplifier. *Phys. Rev. A* **2011**, *83*, 063–081.
24. Caves, C.M. Quantum limits on noise in linear amplifiers. *Phys. Rev. D* **1982**, *26*, 1817.

25. Ralph, T.C.; Lund, A.P. Nondeterministic noiseless linear amplification of quantum systems. *AIP Conf. Proc.* **2009**, *1110*, 155–160.
26. Ralph, T.C. Quantum error correction of continuous-variable states against Gaussian noise. *Phys. Rev. A* **2011**, *84*, 022339.
27. Fiurášek, J.; Cerf, N.J. Gaussian post-selection and virtual noiseless amplification in continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 060302.
28. Li, C.Y.; Miao, R.H.; Gong, X.B.; Guo, Y.; He, G.Q. Performance Improvement of Two-way Quantum Key Distribution by Using a Heralded Noiseless Amplifier. *Int. J. Theor. Phys.* **2016**, *55*, 2199–2211.
29. 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.
30. Lodewyck, J.; Bloch, M.; Garcá-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.
31. Holevo, A.S.; Sohma, M.; Hirota, O. Capacity of quantum Gaussian channels. *Phys. Rev. A* **1999**, *59*, 1820–1828.
32. Xuan, Q.D.; Zhang, Z.S.; Voss, P.L. A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Opt. Express* **2009**, *17*, 24244.