Entropy **2015**, *17*, 4547-4562; doi:10.3390/e17074547

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Noiseless Linear Amplifiers in Entanglement-Based Continuous-Variable Quantum Key Distribution

Yichen Zhang [1], Zhengyu Li [2], Christian Weedbrook [3], Kevin Marshall [4], Stefano Pirandola [5], Song Yu [1,*] and Hong Guo [1,2]

[1] State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2] State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics Engineering and Computer Science, Center for Quantum Information Technology and Center for Computational Science and Engineering, Peking University, Beijing 100871, China

[3] QKD Corp., 60 St. George St., Toronto, M5S 1A7, Canada

[4] Department of Physics, University of Toronto, Toronto, M5S 1A7, Canada

[5] Department of Computer Science, University of York, Deramore Lane, York YO10 5GH, UK

* Author to whom correspondence should be addressed; E-Mail: yusong@bupt.edu.cn.

Academic Editor: Jay Lawrence

Received: 27 March 2015 / Accepted: 23 June 2015 / Published: 26 June 2015

Abstract: We propose a method to improve the performance of two entanglement-based continuous-variable quantum key distribution protocols using noiseless linear amplifiers. The two entanglement-based schemes consist of an entanglement distribution protocol with an untrusted source and an entanglement swapping protocol with an untrusted relay. Simulation results show that the noiseless linear amplifiers can improve the performance of these two protocols, in terms of maximal transmission distances, when we consider small amounts of entanglement, as typical in realistic setups.

Keywords: quantum key distribution; continuous-variable quantum key distribution; noiseless linear amplifiers

---

1. Introduction

Quantum key distribution (QKD) [1,2] is the most practical application in the field of quantum information and enables two distant parties, Alice and Bob, to establish a secret key through

insecure quantum and classical channels. The continuous-variable version of quantum key distribution (CV-QKD) [3–5], an alternative to single-photon-based QKD, has attracted much attention in the past few years [5,6], mainly because it does not require single-photon sources or detectors. The Gaussian-modulated CV-QKD protocols based on coherent states [7–9] have been experimentally demonstrated [6,10–12] and have been shown to be secure against arbitrary attacks in the asymptotic [13] and finite-size regimes [14]. Two-way protocols [15–18] and thermal-state protocols [19–21] have been also designed.

However, there still exists a gap between the theoretical security analyses and the practical implementations. Such real-life implementations of CV-QKD systems may contain overlooked imperfections, which might not have been accounted for in the theoretical security proofs, and may provide security loopholes. Recently, various attacks have been proposed and closed, such as wavelength attacks [22–24], calibration attacks [25] and local oscillator fluctuation attacks [26]. One approach to overcome device imperfections is by characterizing the whole practical system and to consider all of the existing loopholes. Although some potential loopholes have been discovered and then closed using this approach, it is difficult to find all of the loopholes in practical CV-QKD systems, because the number of loopholes is theoretically infinite.

Another approach is by establishing a full device-independent CV-QKD protocol like its discrete-variable counterpart [27], which is based on the violation of a Bell inequality [28]. Recently, there has been work to build various device-independent CV-QKD protocols, including schemes which are both one-sided [29] and fully device independent [30]. The goal of full device-independent QKD is the removal of the requirement that Alice and Bob need to trust their devices.

In this paper, we consider two kinds of entanglement-based CV-QKD protocols in untrusted scenarios: an entanglement distribution protocol with an untrusted source and an entanglement swapping protocol with an untrusted relay. The latter protocol is inspired by [31] and corresponds to the entanglement-based version of the CV-QKD protocols described in [32–35]. In particular, we consider a symmetric formulation where the two legitimate partners both modify their data during the classical data post-processing stage.

To improve the maximal transmission distances of these two schemes, we consider the use of two noiseless linear amplifiers (NLAs) [36], one at Alice's side and one at Bob's side. We show that the practical example of the CV-QKD protocol with an untrusted source, *i.e.*, the entanglement-in-the-middle protocol [37], improves by placing two NLAs at the output of the quantum channel at both Alice's and Bob's side. Additionally, the maximal transmission distances of the untrusted relay scheme are also improved using this same method. Previously, a similar method had only been analysed for the case of the one-way CV-QKD protocol [38–40]. These improvements are found in the regime of small entanglement, which is typical in realistic implementations. It is also found that placing only one NLA at the non-reconciliation side (Alice's side for reverse reconciliation and Bob's side for direct reconciliation) has a greater improvement than placing it at the opposite side.

This paper is organized as follows. In Section 2, we introduce the two entanglement-based CV-QKD protocols. In Section 3, we show that we can improve the performance of these protocols by using NLAs. Our conclusions are drawn in Section 4.

2. Entanglement-Based CV-QKD Protocols

In this section, we begin by describing the two entanglement-based CV-QKD protocols: entanglement-based protocols with an untrusted source and entanglement-based protocol with an untrusted relay, which can also be thought of as entanglement distribution and entanglement swapping protocols, respectively. We then outline the secret key rates for these protocols in the presence of collective Gaussian attacks.

2.1. Entanglement Distribution: Entanglement-Based Protocols with an Untrusted Source

The schematic of the entanglement-based CV-QKD protocol with an untrusted source is illustrated in Figure 1 and can be described as follows:

Step 1: The untrusted third party, Charlie, initially prepares an entangled source. He sends one mode A_1 to Alice through Channel 1 and sends the other mode B_1 to Bob through Channel 2, where Eve may perform her attack.

Step 2: Alice and Bob perform either a homodyne (switching) (Hom) or a heterodyne (no switching) (Het) measurement on the received modes A_2 and B_2. Once Alice and Bob have collected a sufficiently large set of correlated data, they proceed with classical data post-processing, namely error reconciliation and privacy amplification. The reconciliation can be performed in one of two ways: either direct reconciliation (DR) [7] or reverse reconciliation (RR) [8].

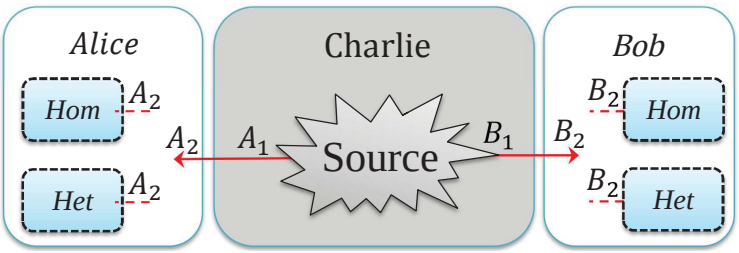

Figure 1. Schematic of the continuous-variable version of quantum key distribution (CV-QKD) protocols with an untrusted source. Both the entangled Gaussian source and the quantum channels are fully controlled by Eve. However, Eve has no access to the apparatuses in Alice's and Bob's stations. Alice and Bob can perform either homodyne (Hom) or heterodyne (Het) detection, using either direct or reverse reconciliation.

Since the untrusted Charlie could be completely controlled by the eavesdropper, the original source $\rho_{A_1B_1}^{(n)}$ (where n denotes the number of quantum signals exchanged during the protocol) is not important to Alice and Bob. What matters is the final state $\rho_{A_2B_2}^{(n)}$ before their measurements. Here, we assume that the final state $\rho_{A_2B_2}^{(n)}$ is a 'collective source' to simplify the problem, which means Alice and Bob get the same quantum state $\rho_{A_2B_2}$ each time, so that $\rho_{A_2B_2}^{(n)} = \rho_{A_2B_2}^{\otimes n}$. The asymptotic secret key rates K_{DR} for direct reconciliation and K_{RR} for reverse reconciliation are given by [41]:

$$\begin{cases} K_{DR} = \beta I(A:B) - \chi(A:E) \\ K_{RR} = \beta I(A:B) - \chi(B:E) \end{cases}, \tag{1}$$

where $\beta \in [0,1]$ is the reconciliation efficiency, $I(A:B)$ is the classical mutual information between Alice and Bob, $\chi(A:E)$ and $\chi(B:E)$ are the Holevo quantities [42]:

$$\begin{cases} \chi(A:E) = S(\rho_E) - \sum_x p(x) S(\rho_{E|x}) \\ \chi(B:E) = S(\rho_E) - \sum_y p(y) S(\rho_{E|y}) \end{cases}, \tag{2}$$

where $S(\rho)$ is the von Neumann entropy of the quantum state ρ, x and y are Alice's and Bob's measurement results obtained with probability $p(x)$ and $p(y)$, $\rho_{E|x}$ and $\rho_{E|y}$ are the corresponding state of Eve's ancillas and $\rho_E = \sum_x p(x) \rho_{E|x}$ and $\rho_E = \sum_y p(y) \rho_{E|y}$ are Eve's average states for DRand RR, respectively. Unless both Alice and Bob performed heterodyne measurements, they first apply a sifting process, where they compare the chosen measurement quadrature ($\hat{x}$ or $\hat{p}$) and only keep the data for which the quadratures match. Here, we use x and y to represent Alice's and Bob's measurement results, respectively, for both homodyne and heterodyne measurements.

Note that these secret key rates could be modified to take finite-size effects into consideration. For simplicity, here we only consider the asymptotic secret key rates, *i.e.*, achieved in the limit of infinite rounds of the protocol. Firstly, Eve is able to purify the whole system $\rho_{A_2B_2}$ to maximize her information, *i.e.*, we have $S(\rho_E) = S(\rho_{A_2B_2})$. Secondly, after Alice's projective measurement resulting in x, the system ρ_{B_2E} is pure, so that $S(E|x) = S(B_2|x)$ for DR and $S(E|y) = S(A_2|y)$ for RR. Thus, $\chi(A:E)$ and $\chi(B:E)$ become:

$$\begin{cases} \chi(A:E) = S(\rho_{A_2B_2}) - \sum_x p(x) S(\rho_{B_2|x}) \\ \chi(B:E) = S(\rho_{A_2B_2}) - \sum_y p(y) S(\rho_{A_2|y}) \end{cases}. \tag{3}$$

In practical experiments, we calculate the covariance matrix $\gamma_{A_2B_2}$ of correlated variables from randomly-chosen samples of measurement data. According to the optimality of collective Gaussian attacks [43,44], we therefore assume that the final state $\rho_{A_2B_2}$, shared by Alice and Bob, is Gaussian to minimize the final secret key rates. If the entangled source is Gaussian, one can show that there exists a Gaussian channel mapping the initial state to the final state: this means that there exists a Gaussian attack that is optimal [43,44]. If the entangled source is non-Gaussian, it is an open question whether the optimal attack is Gaussian or not. However, whether Eve's attack is Gaussian or not, we can always bound the information available to Eve by assuming the final state is Gaussian.

Thus, the entropies $S(\rho_{A_2B_2})$, $\sum_x p(x) S(\rho_{B_2|x})$ and $\sum_y p(y) S(\rho_{A_2|y})$ can be calculated using the covariance matrices $\gamma_{A_2B_2}$ characterizing the state $\rho_{A_2B_2}$, $\gamma_{B_2|x}$ characterizing the state $\rho_{B_2|x}$ and $\gamma_{A_2|y}$ characterizing the state $\rho_{A_2|y}$. The Holevo quantities become:

$$\begin{cases} \chi(A:E) = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) \\ \chi(B:E) = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right) \end{cases}, \tag{4}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, $\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix $\gamma_{A_2B_2}$ and λ_3, λ_4 are the symplectic eigenvalues of the covariance matrices $\gamma_{B_2|x}$ and $\gamma_{A_2|y}$ [5].

In particular, a practical example of the CV-QKD protocol with an untrusted source is the entanglement-in-the-middle protocol [37], in which the source is assumed to be a two-mode squeezed vacuum state. The latter numerical simulations are also based on this specific example.

2.2. Entanglement Swapping: Entanglement-Based Protocol with an Untrusted Relay

The schematic of the entanglement-based CV-QKD protocol with an untrusted relay is shown in Figure 2a. This is inspired by the scheme of [31] and represents a modified entanglement-based version of the CV-QKD protocols proposed by [32–35]. It can be described as follows:

Step 1: Alice and Bob both generate an Einstein–Podolsky–Rosen (EPR), states EPR_1 and EPR_2, respectively, with variances V_A and V_B and they keep modes A_2 and B_2 at their respective sides. Then, they send their other modes A_1 and B_1 to the untrusted third party (Charlie) through two different quantum channels with lengths L_{AC} and L_{BC}.

Step 2: Charlie combines the received two modes A_1' and B_1' onto a beam splitter (50:50), where we label output modes of the beam splitter as C and D. Charlie then measures the x-quadrature of mode C and the p-quadrature of mode D using homodyne detectors and publicly announces the measurement results x_C, p_D to Alice and Bob through classical channels. After the measurements of modes C and D, the two initially independent modes A_2 and B_2 get entangled if channel noise is not too strong.

Step 3: Bob displaces the mode B_2 to B_3 by the operation $\hat{D}(\beta)$ and gets $\hat{\rho}_{B_3} = \hat{D}(\beta)\hat{\rho}_{B_2}\hat{D}^{\dagger}(\beta)$, where $\hat{\rho}_B$ represents the density matrix of mode B, $\beta = g(X_C + iP_D)$, $\hat{D}(\beta) = e^{\beta\hat{a}^{\dagger} - \beta^{*}\hat{a}}$ ($\hat{a}^{\dagger}$ and $\hat{a}$ are the creation and annihilation operators, respectively), and g represents the gain of the displacement. Then Bob measures the mode B_3 to get the final data $\{x_B, p_B\}$ using heterodyne detection. Alice also measures the mode A_2 to get the final data $\{x_A, p_A\}$, again using heterodyne detection.

Step 4: Once Alice and Bob have collected a sufficiently large set of correlated data, they use an authenticated public channel to do parameter estimation from a randomly-chosen sample of final data from $\{x_A, p_A\}$ and $\{x_B, p_B\}$. Then, Alice and Bob proceed with classical data post-processing to distil a secret key. The reconciliation can also be done in two ways: either DR or RR.

Note that we can put the displacement operator at each side rather than placing it only at Bob's side, which now makes the protocol symmetric (see Figure 2b). This symmetry allows the CV-QKD protocol with an untrusted relay to have a similar structure with the entanglement-in-the-middle protocol. In this modified protocol, Alice and Bob displace the modes A_2 and B_2 by the operators $D(\alpha_1)$ and $D(\alpha_2)$, resulting in $\rho_{A_3} = D(\alpha_1)\rho_{A_2}D^{\dagger}(\alpha_1)$ and $\rho_{B_3} = D(\alpha_2)\rho_{B_2}D^{\dagger}(\alpha_2)$, where $\alpha_1 = -g_A(X_C - iP_D)/2$, $\alpha_2 = g_B(X_C + iP_D)/2$, and g_A, g_B represents the gain of the displacements at Alice's and Bob's side, respectively.

Note that these protocols can completely defeat side-channel attacks provided that Alice and Bob use quantum memories in their private spaces, which is discussed in detail in [31]. From this point of view, this makes the CV-QKD protocol with an untrusted relay more secure. The secret key rate for these protocols against a collective attack is similar to Equation (1) and can be found in [32,33] in detail. See [34] for an unconditional security analysis against the most general coherent attacks.

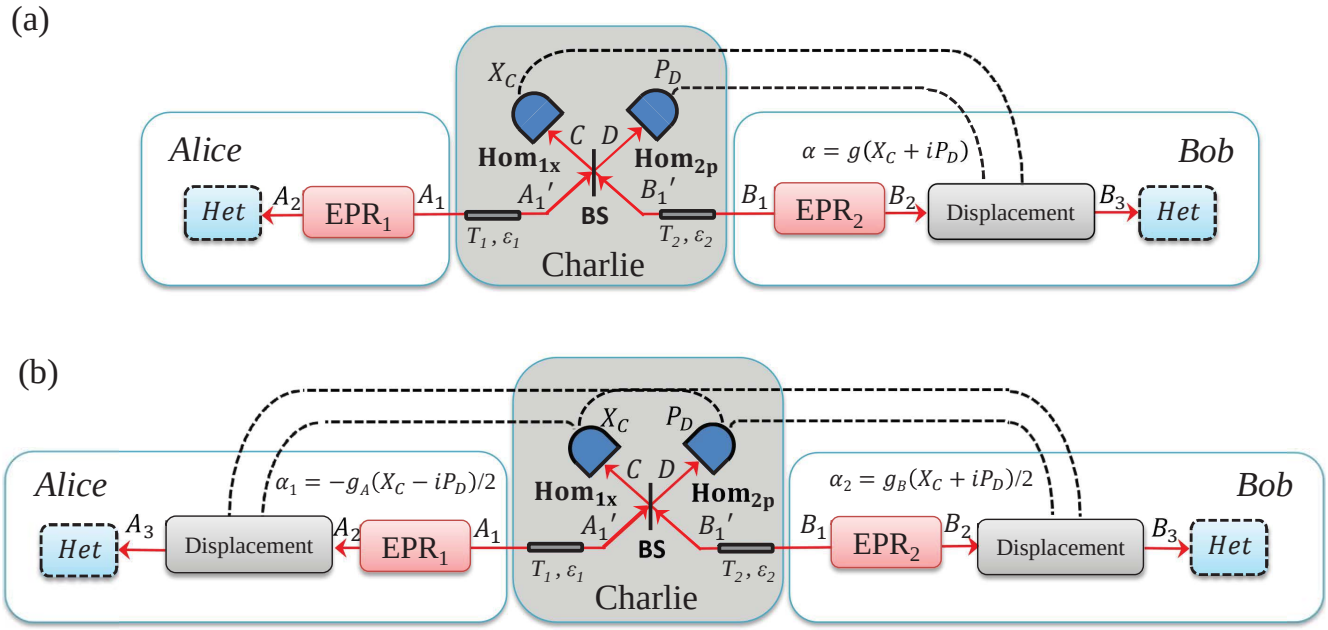

Figure 2. (**a**) Entanglement-based CV-QKD protocol with an untrusted relay where the displacement operator is placed at Bob's side. (**b**) Entanglement-based scheme where the displacement operator is placed at both Alice's and Bob's sides.

3. Improvement Using Noiseless Linear Amplifiers

In this section, we place two noiseless linear amplifiers (NLAs), one at each of Alice's and Bob's side, to improve the performance of the two entanglement-based CV-QKD protocols. We begin by introducing the NLA.

3.1. Noiseless Linear Amplifier

For Gaussian states, an NLA can, in principle, probabilistically increase the signal-to-noise ratio by increasing the mean values of the quadratures while keeping their variances at the initial level [38,45–48]. The amplification can be described by an operator $\hat{C} = g^{\hat{n}}$, where $\hat{n}$ is the number operator in the Fock basis. Such an operator maps $|\alpha\rangle$ into $|g\alpha\rangle$ with a success probability P, *i.e.*,

$$\hat{C}\left(|\alpha\rangle\langle\alpha|\right) = P\,|g\alpha\rangle\langle g\alpha| + (1-P)\,|0\rangle\langle 0|\,, \tag{5}$$

where $g > 1$ is the gain of the amplifier. Only the situations with successful amplification will be used to distil the final secret keys, while the others are discarded.

In a practical experiment, the covariance matrix before passing through two NLAs takes the form γ, which is used to calculate the final secret key rates ($\gamma_{A_2B_2}$ for the entanglement distribution protocols (see Figure 1) and $\gamma_{A_3B_3}$ for the entanglement swapping protocols (see Figure 2b)). Typically, γ can be described by the normal form:

$$\gamma = \begin{bmatrix} a \cdot I_2 & c \cdot \sigma_z \\ c \cdot \sigma_z & b \cdot I_2 \end{bmatrix}, \tag{6}$$

where I_n is the $n \times n$ identity matrix, and σ_z = diag (1, -1).

We then exploit the relationship between the covariance matrix γ and the density matrix $\hat{\rho}$ in the Fock state basis [39]. The Husimi Q-function of the two-mode state can be described as:

$$Q(\mathbf{R}) = \frac{\sqrt{\det \Gamma}}{\pi^2} e^{-\mathbf{R}^T \Gamma \mathbf{R}}, \tag{7}$$

where $\mathbf{R} = (\hat{x}_A, \hat{p}_A, \hat{x}_B, \hat{p}_B)$ and $\Gamma = (\gamma + I_n)^{-1}$. Thus, we can find:

$$\Gamma = \begin{bmatrix} A \cdot I_2 & C \cdot \sigma_z \\ C \cdot \sigma_z & B \cdot I_2 \end{bmatrix}, \tag{8}$$

with new parameters A, B and C, after the application of an NLA on each side. In the Fock basis, the Husimi Q-function is a degenerating function of the density matrix elements. Thus, we can establish a relationship between elements of the covariance matrix Γ and the elements of the normalized density matrix $\sigma_{jk,lm} = \rho_{jk,lm}/\rho_{00,00}$ [49]. Then, the matrix Γ after the two NLAs becomes:

$$\Gamma_{NLA} = \begin{bmatrix} \left(g_1^2\left(A - \frac{1}{2}\right) + \frac{1}{2}\right) \cdot I_2 & g_1 g_2 C \cdot \sigma_z \\ g_1 g_2 C \cdot \sigma_z & \left(g_2^2\left(B - \frac{1}{2}\right) + \frac{1}{2}\right) \cdot I_2 \end{bmatrix}, \tag{9}$$

where g_1 and g_2 are the gains of the NLAs at Alice's and Bob's sides ($g_1 = 1$ or $g_2 = 1$ means there is no NLA). Thus, the covariance matrix γ' after the NLAs can be obtained by:

$$\gamma_{NLA} = (\Gamma_{NLA})^{-1} - I_4. \tag{10}$$

This covariance matrix is used for the calculation of the final key rates in DR and RR, which are reduced according to the total amplification success probability $P_{\text{total}} = P_A P_{B|A}$, where P_A is the success probability of Alice's NLA and $P_{B|A}$ is the success probability of Bob's NLA given that Alice's amplification succeeded. Furthermore, considering the trade-off between the fidelity and the success probability of an NLA, a good estimate of the maximal expected success probability for one NLA is given by [50]:

$$P = \frac{1}{g^{2N}}, \tag{11}$$

where N is the average photon number of the input state (ensemble) of the NLA. Such an NLA can amplify an input coherent $|\alpha\rangle$ to the target output state $|g\alpha\rangle$ with a relatively high fidelity.

3.2. Entanglement-Based Protocol with an Untrusted Source

Using the previous method, we can derive the final covariance matrix $\gamma_{A_3B_3}$ to calculate the secret key rate. As shown in Figure 3, we consider a specific example of an entanglement-based protocol with an untrusted source: the EPR in the middle scheme [37]. This security analysis and latter numerical simulations of this scheme are based on the two independent entangling cloner attacks. This is the most common example of a collective Gaussian attack [51]. Alice and Bob both add an NLA before their detectors, which here are assumed to be perfect for simplicity [38,45,46].

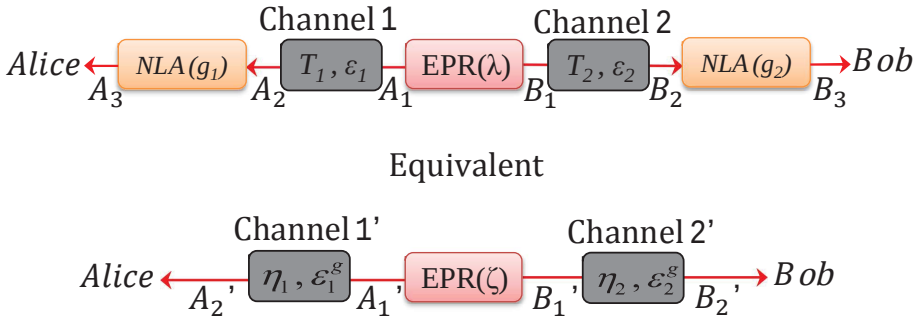

Figure 3. Entanglement-in-the-middle protocol. Equivalent channels and squeezing: an Einstein–Podolsky–Rosen (EPR) state λ sent through two Gaussian channels of transmittance T_1, T_2 and excess noise ε_1, ε_2, followed by two successful noiseless linear amplifiers (NLAs), has the same final covariance matrix with a state ς sent through two Gaussian channels of transmittance η_1, η_2 and excess noise ε_1^g, ε_2^g, without two NLAs.

We can look for equivalent parameters of an EPR state sent through two lossy and noisy Gaussian channels. The covariance matrix $\gamma'_{AB}(\lambda, T_1, \varepsilon_1, g_1, T_2, \varepsilon_2, g_2)$ of the amplified state with an EPR parameter λ passing through two channels of transmittance T_1, T_2, and excess noise $\varepsilon_1, \varepsilon_2$ followed by two gain efficiencies g_1, g_2, is equal to the covariance matrix $\gamma_{AB}(\varsigma, \eta_1, \varepsilon_1^g, g_1 = 1, \eta_2, \varepsilon_2^g, g_2 = 1)$ of an equivalent system with an EPR parameter ς, sent through two channels with parameters η_1, ε_1^g and η_2, ε_2^g, without using NLAs. These parameters are given by:

$$\begin{cases} \varsigma = \lambda\sqrt{\frac{\left[\left(g_1^2-1\right)(\varepsilon-2)T-2\right]\cdot\left[\left(g_2^2-1\right)(\varepsilon-2)T-2\right]}{\left[\left(g_1^2-1\right)\varepsilon T-2\right]\cdot\left[\left(g_2^2-1\right)\varepsilon T-2\right]}} \\ \eta_1 = \frac{4Tg_1^2}{T\left(g_1^2-1\right)\cdot\left[\left(g_1^2-1\right)(\varepsilon-2)\varepsilon T-4(\varepsilon-1)\right]+4} \\ \varepsilon_1^g = \varepsilon - \frac{1}{2}\left(g_1^2-1\right)(\varepsilon-2)\varepsilon T \\ \eta_2 = \frac{4Tg_2^2}{T\left(g_2^2-1\right)\cdot\left[\left(g_2^2-1\right)(\varepsilon-2)\varepsilon T-4(\varepsilon-1)\right]+4} \\ \varepsilon_1^g = \varepsilon - \frac{1}{2}\left(g_2^2-1\right)(\varepsilon-2)\varepsilon T \end{cases} . \tag{12}$$

These could be treated as physical parameters of an equivalent system if they satisfy the following physical constraints:

$$\begin{cases} 0 \leq \varsigma < 1 \\ 0 \leq \eta_1 \leq 1, \varepsilon_1^g \geq 0 \\ 0 \leq \eta_2 \leq 1, \varepsilon_2^g \geq 0 \end{cases} \tag{13}$$

As shown in Equation (12), λ only affects parameter ς, and η_1, ε_1^g, η_2 and ε_2^g do not depend on λ. Thus, the first condition is always satisfied if λ is below a limiting value, given by:

$$0 \leq \lambda < \sqrt{\frac{\left(g_1^2-1\right)\varepsilon T-2}{\left(g_1^2-1\right)(\varepsilon-2)T-2}} \cdot \sqrt{\frac{\left(g_2^2-1\right)\varepsilon T-2}{\left(g_2^2-1\right)(\varepsilon-2)T-2}}. \tag{14}$$

The last two conditions are satisfied if the excess noise ε is smaller than two and if the gain of the two NLAs is smaller than a maximum value, which depends on the channel parameters T and ε:

$$g_1^{\max} = g_2^{\max} = \sqrt{\frac{\varepsilon\left[T(\varepsilon-2)+2\right]-2\sqrt{\varepsilon\left[T(\varepsilon-2)+2\right]}}{T\varepsilon(\varepsilon-2)}}. \tag{15}$$

Using the previous results, we consider the performance of the CV-QKD protocols with EPR in the middle by placing two NLAs, one at each output of the quantum channels. We calculate the secret key rate K_{DR} as a function of distance d under four situations: without NLAs ($g_1 = 1$, $g_2 = 1$), with only an NLA at Alice's side ($g_2 = 1$), with only an NLA at Bob's side ($g_1 = 1$) and with two NLAs at both sides. The various parameters are chosen from typical experimental values [6]: we choose $V = 1.7$, $\beta = 0.948$ and $\varepsilon = 0.002$ (where the shot noise variance is normalized to one). The transmittance $T = 10^{-ad/10}$, where $a = 0.2$ dB/km is the loss coefficient of the optical fibres and d is the length of the quantum channel. The total success probability of using two NLAs for the CV-QKD protocols with EPR in the middle is $P_{\text{total}} = 1/\left(g_1^{2N_A} g_2^{2N_{B|A}}\right)$, where $N_A = T\left(V - 1 + \varepsilon\right) + 1$, $N_{B|A} = T\left(V' - 1 + \varepsilon\right) + 1$. Here, V' is the variance of the equivalent EPR when Alice's amplification succeeds, which is given by $V' = (1 + \varsigma^2)/(1 - \varsigma^2)$ provided $g_2 = 1$.

In our analysis, there are eight protocols that depend on Alice's and Bob's measurements (four possibilities) and reconciliation methods (two possibilities, DR or RR). These eight CV-QKD protocols can be divided into four groups whose secret key rate and maximal transmission distance are the same [37]. When we move the entanglement source into Alice's side, these eight protocols correspond to the entanglement-based version of the eight primary prepare-and-measure CV-QKD protocols, *i.e.*, the protocols where Alice and Bob use homodyne detection corresponding to the protocol of [53]; the protocols where Alice uses heterodyne detection and Bob uses homodyne detection correspond to the protocol of [7,8]; the protocols where Alice uses homodyne detection and Bob uses heterodyne detection correspond to the protocol of [54,55]; the protocols where Alice and Bob use heterodyne detection correspond to the protocol of. [9].

Our simulation results are shown in Figures 4 and 5. We find that the performance of the CV-QKD protocols is improved by placing one NLA at each side and choosing the two gain efficiencies as $g_1 = g_2 = 1.4$. The NLAs enhance the maximal transmission of the protocol, in which Alice is using heterodyne detection and Bob is using homodyne detection with DR, from 17.0 km to 31.6 km. Furthermore, we also find that if we only put an NLA at either Alice's or Bob's side, the performance of the protocols can also be improved. For instance, placing an NLA at the non-reconciliation side (Alice's side for RR protocols and Bob's side for DR protocols) has a greater improvement than placing it at the other side. This is because when adding an NLA only at one side (suppose it is on Alice's side), according to Equation (12), the covariance matrix after the application of the NLA has the feature that Alice's equivalent variance is greater than Bob's variance. If considering Alice's part as the reconciliation part, it is similar to the one-way CV-QKD protocol with DR; while, if considering Bob's part as the reconciliation part, it is similar to the one-way CV-QKD protocol with RR. In one-way protocols, the RR protocol usually has a longer transmission distance than the DR protocol. Therefore, in our protocols, placing an NLA at the non-reconciliation side is better than placing it at the reconciliation side. Obviously, the optimal performance of the protocols is achieved by placing two NLAs at each side. However, if we want to reduce the cost and expense and only have one NLA in the deployment, we need to place it at the correct side to have the greatest improvement.

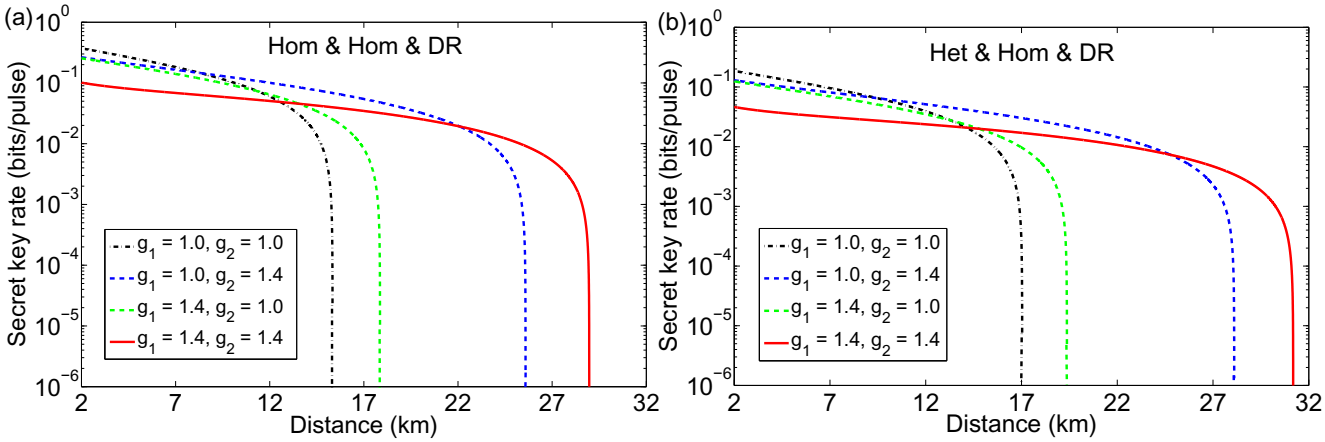

Figure 4. Improvement of the CV-QKD protocols with entanglement-in-the-middle. A comparison among the secret key rates for the protocols where (left panel) Alice uses homodyne detection and Bob uses homodyne detection and DR(equivalent to Alice using homodyne detection and Bob using homodyne detection and RR); and (right panel) Alice uses heterodyne detection and Bob uses homodyne detection and DR (equivalent to Alice using homodyne detection and Bob using heterodyne detection and RR), under the following situations: no NLAs ($g_1 = 1$, $g_2 = 1$), using an NLA at Alice's side ($g_2 = 1$), using an NLA at Bob's side ($g_1 = 1$) and using two NLAs at both sides. Here, we use the realistic parameters: $V = 1.7$, $\beta = 0.948$, $\varepsilon = 0.002$ and $P_{\text{total}} = 1/\left(g_1^{2N_A} g_2^{2N_{B|A}}\right)$.

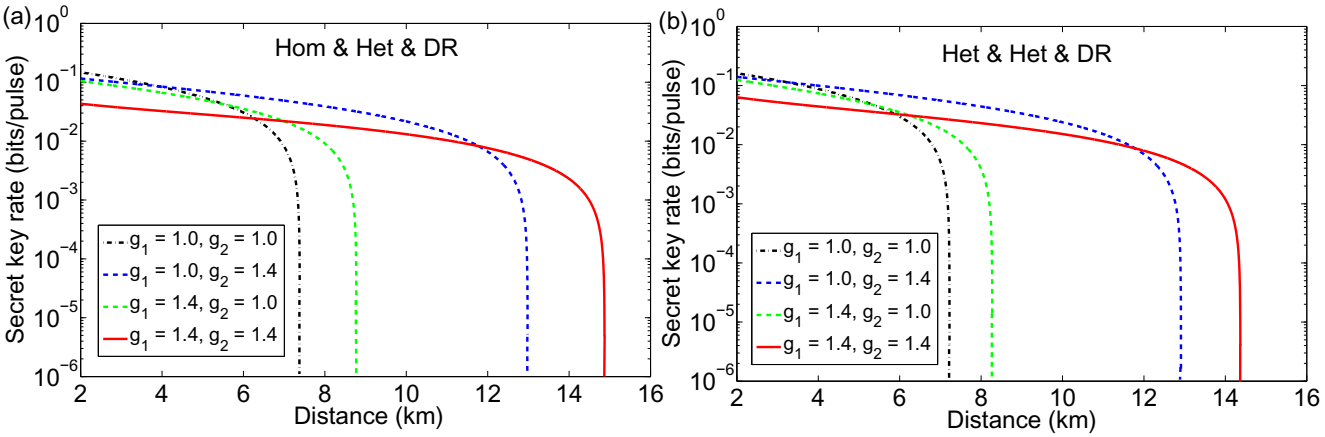

Figure 5. Improvement of the CV-QKD protocols with entanglement-in-the-middle. A comparison among the secret key rates for the protocols where (left panel) Alice uses homodyne detection and Bob uses heterodyne detection and DR (equivalent to Alice using heterodyne detection and Bob using homodyne detection and RR); and (right panel) Alice uses heterodyne detection and Bob uses heterodyne detection and DR (equivalent to Alice using heterodyne detection and Bob using heterodyne detection and RR), under the following situations: no NLAs ($g_1 = 1$, $g_2 = 1$), using an NLA at Alice's side ($g_2 = 1$), using an NLA at Bob's side ($g_1 = 1$) and using two NLAs at both sides. Here, we use the realistic parameters: $V = 1.7$, $\beta = 0.948$, $\varepsilon = 0.002$ and $P_{\text{total}} = 1/\left(g_1^{2N_A} g_2^{2N_{B|A}}\right)$.

Furthermore, as proven in [39,40], the physical implementation of the NLA could be replaced by a suitable data post-processing (Gaussian post-selection) after the measurement, although provided that certain conditions are met [52]. Thus, in such cases, we would not need to implement the physical implementation of the NLA, which requires single-photon addition and subtraction, or an auxiliary source of single photons and multiphoton interference [39,40].

3.3. Entanglement-Based Protocol with an Untrusted Relay

The improvement seen in the previous section can also be employed in the modified CV-QKD protocol with an untrusted relay. The modified CV-QKD protocol with an untrusted relay is shown in Figure 6 where we place an NLA at both Alice's and Bob's sides. As illustrated in Figure 7a, the modified entanglement-based protocol can increase the maximal transmission distance when we choose $V = V_A = V_B = 1.7$, $\beta = 0.948$, $\varepsilon = \varepsilon_1 = \varepsilon_2 = 0.002$, $g_A = \sqrt{(V^2-1)/[2T_1(V+\varepsilon)+2(1-T_1)]}$, $g_B = \sqrt{(V^2-1)/[2T_2(V+\varepsilon)+2(1-T_2)]}$. Under these simulation parameters, the modified entanglement-based protocol in the symmetric case (the distance from Alice to Charlie L_{AC} is equal to the distance from Bob to Charlie L_{BC}) can successfully distribute secret keys under such conditions. Then, using the same method as above, we place an NLA at each side to improve its performance; we find an improvement when we set the two gain efficiencies as $g_1 = g_2 = 1.8$. The NLAs enhance the maximal transmission distance of the protocol from 1.6 km to 5.3 km in the symmetric case.

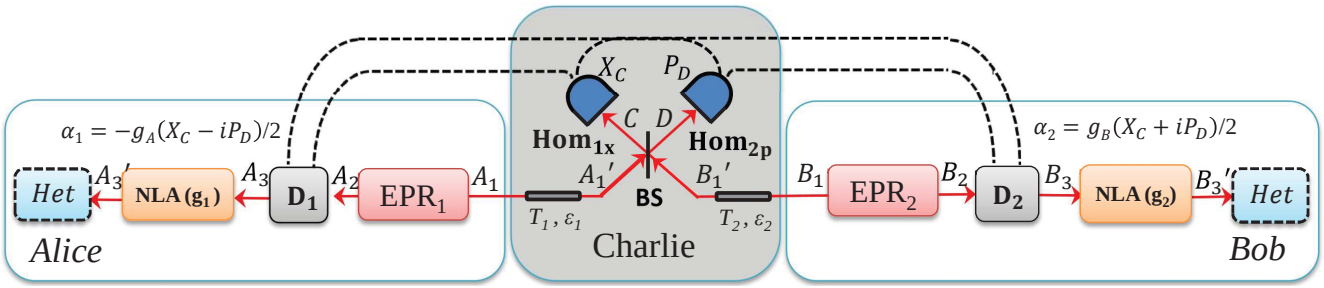

Figure 6. Entanglement-based scheme of the modified CV-QKD protocol with an untrusted relay, where a displacement operator D is placed at both Alice's and Bob's sides and the two NLAs are placed before the measurement devices.

Furthermore, for DR, we also find that when Charlie's position is close to Alice, the total maximal transmission distance L_{AB} will increase to a relatively longer distance. Thus, we study the performance of the asymmetric case where $L_{AC} \neq L_{BC}$. As illustrated in Figure 7b, the total maximal transmission distance increases when L_{AC} decreases. In the asymmetric case, the performance of the modified CV-QKD protocol is also improved by placing two NLAs, one at each side. The maximal total transmission distance of the modified protocol using two NLAs, with gain efficiencies $g_1 = g_2 = 1.8$, is enhanced from 17.5 km to 25.2 km in the most asymmetric case (*i.e.*, $L_{AC} \approx 0\ km$). Here '0 km' indicates that the transmission distance from Alice to Charlie is very short but not exactly zero. In fact, even when Charlie is at Alice's side, there still exists a distance between Alice's laser and the beamsplitter. Therefore, in the numerical simulation although we assume the channel transmittance is $T_1 = 1$, the excess noise ε_1 still exists, and is $\varepsilon_1 = 0.002$.

Note that the sources for Alice and Bob are EPR states. Thus, the protocols can remove side-channel attacks, as discussed in [31], which makes the CV-QKD protocol with untrusted relay more secure. Finally, we also find that if we only put an NLA at Alice's or Bob's side, the performance of the protocols can also be improved. This is the same conclusion as before: placing an NLA at the non-reconciliation side (Alice's side for RR protocols and Bob's side for DR protocols) has a greater improvement than placing it at the other side.

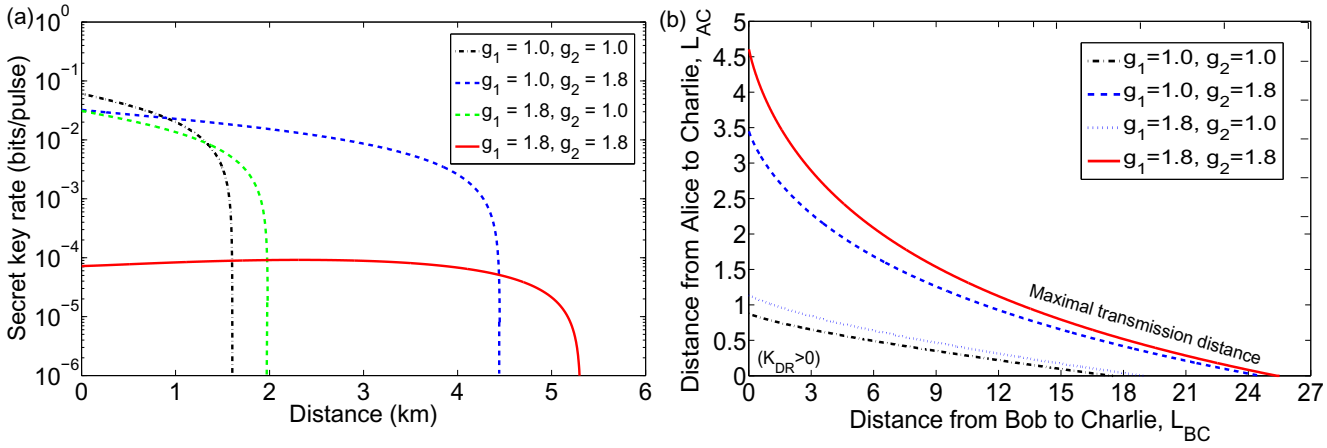

Figure 7. Improvement of the modified CV-QKD protocol with an untrusted relay in (**a**) the symmetric case (*i.e.*, $L_{AC} = L_{BC}$) and (**b**) the asymmetric case (*i.e.*, $L_{AC} \neq L_{BC}$). A comparison among the secret key rates in DR under the following situations: no NLAs ($g_1 = 1$, $g_2 = 1$), using an NLA at Alice's side ($g_2 = 1$), using an NLA at Bob's side ($g_1 = 1$) and using two NLAs one at each side. Here, we use the realistic parameters: $V_A = V_B = 1.7$, $\beta = 0.948$, $\varepsilon = 0.002$ and $P_{\text{total}} = 1/\left(g_1^{2N_A} g_2^{2N_{B|A}}\right)$.

4. Conclusion

In this paper, we have discussed how to improve the performance of two entanglement-based continuous-variable QKD protocols using noiseless linear amplifiers. The first scheme was an entanglement distribution protocol: continuous-variable QKD protocols with an untrusted source, where the entangled source is generated by a third party, but may have actually been created or controlled by the eavesdropper. The second scheme was an entanglement swapping protocol: entanglement-based continuous-variable QKD protocol with an untrusted relay.

By inserting two noiseless linear amplifiers, one at each of Alice's and Bob's side, simulation results show that the proposed method can increase the maximal transmission distances of both protocols in the experimentally-feasible regime of small entanglement, corresponding to small modulation. In fact, in certain situations, we see a doubling of the allowed secure transmission distances. Furthermore, it is also found that placing only one NLA at the non-reconciliation side (Alice's side for reverse reconciliation protocols and Bob's side for direct reconciliation protocols) has a greater improvement than placing it at the other corresponding side.

Future investigations will involve the analysis of the protocols against more general two-mode Gaussian attacks, which are coherent between the two channels connecting the remote parties with the

middle source or relay. In fact, as pointed out in [34], the unconditional secret-key rate of the relay-based protocol must be derived in the presence of such attacks, which may outperform the collective one-mode Gaussian attacks (based on the use of independent entangling cloners).

Acknowledgements

We thank T. C. Ralph, N. Walk, A. Leverrier and M. Gu for valuable discussions. This work was supported in part by the National Basic Research Program of China (973 Program) under Grants 2012CB315605, in part by the National Science Fund for Distinguished Young Scholars of China (Grant No. 61225003), and in part by the Fund of State Key Laboratory of Information Photonics and Optical Communications. Stefano Pirandola would like to thank Engineering and Physical Sciences Research Council (EPSRC) and the Leverhulme Trust for support.

Author Contributions

Yichen Zhang: conception and design of the study, accomplishing formula derivation and numerical simulations, drafting the article. Zhengyu Li: conception and design of the study, accomplishing formula derivation, checking numerical simulations. Christian Weedbrook: conception of the study, review of relevant literature, critical revision of the manuscript. Kevin Marshall: checking formula derivation, critical revision of the manuscript. Stefano Pirandola: review of relevant literature, critical revision of the manuscript. Song Yu: review of relevant literature, critical revision of the manuscript. Hong Guo: review of relevant literature, 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. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195.
2. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350.
3. Braunstein, S.L.; van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513–577.
4. Wang, X.B.; Hiroshima, T.; Tomita, A.; Hayashi, M. Quantum Information with Gaussian States. *Phys. Rep.* **2007**, *448*, 1–111.
5. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621–669.
6. Jouguet, P.; Kunz-Jacques,S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photon.* **2013**, *7*, 378–381.

7. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902.
8. Grosshans, F.; van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238-241.
9. 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.
10. Lance, A.M.; Symul, T.; Sharma, V.; Weedbrook, C.; Ralph, T.C.; Lam, P.K. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.* **2005**, *95*, 180503.
11. Lodewyck, J.; Bloch, M.; García-Patrón, R.; Fossier, S.; Karpov, E.; Diamanti, E.; Debuisschert, T.; Cerf, N.J.; Tualle-Brouri, R.; McLaughlin, S.W.; Grangier, P. Quantum key distribution over $25\ \mathrm{km}$ with an all-fiber continuous-variable system. *Phys. Rev. A* **2007**, *76*, 042305.
12. Khan, I.; Wittmann, C.; Jain, N.; Killoran, N.; Lütkenhaus, N.; Marquardt, C.; Leuchs, G. Optimal working points for continuous-variable quantum channels. *Phys. Rev. A* **2013**, *88*, 010302.
13. Renner, R.; Cirac, J.I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **2009**, *102*, 110504.
14. Leverrier, A.; García-Patrón, R.; Renner, R.; Cerf, N.J. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.* **2013**, *110*, 030502.
15. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **2008** *4*, 726–730.
16. Sun, M.; Peng, X.; Shen, Y.; Guo, H. Security of a new two-way continuous-variable quantum key distribution protocol. *Int. J. Quantum Inf.* **2012**, *10*, 1250059.
17. Zhang, Y.-C.; Li, Z.; Weedbrook, C.; Yu, S.; Gu, W.; Sun, M.; Peng, X.; Guo, H. Improvement of two-way continuous-variable quantum key distribution using optical amplifiers. *J. Phys. B* **2014**, *47*, 035501.
18. Weedbrook, C.; Ottaviani, C.; Pirandola, S. Two-way quantum cryptography at different frequencies. *Phys. Rev. A* **2014**, *89*, 012309.
19. Weedbrook, C.; Pirandola, S.; Lloyd, S.; Ralph, T.C. Quantum Cryptography Approaching the Classical Limit. *Phys. Rev. Lett.* **2010**, *105*, 110501.
20. Usenko, V.C.; Filip, R. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **2010**, *81*, 022318.
21. Weedbrook, C.; Pirandola, S.; Ralph, T.C. Continuous-Variable Quantum Key Distribution using Thermal States. *Phys. Rev. A* **2012**, *86*, 022318.
22. 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.
23. Huang, J.-Z.; Weedbrook, C.; Yin, Z.-Q.; Wang, S.; Li, H.-W.; Chen, W.; Guo, G.-C.; Han, Z.-F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329.

24. Huang, J.-Z.; Kunz-Jacques, S.; Jouguet, P.; Weedbrook, C.; Yin, Z.-Q.; Wang, S.; Chen, W.; Guo, G.-C.; Han, Z.-F. Quantum hacking on quantum key distribution using homodyne detection. *Phys. Rev. A* **2014**, *89*, 032304.
25. 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.
26. 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.
27. Acín, A.; Brunner, N.; Gisin, N.; Massar, S.; Pironio, S.; Scarani, V. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **2007**, *98*, 230501.
28. Brunner, N.; Cavalcanti, D.; Pironio, S.; Scarani, V.; Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **2014**, *86*, 419–478.
29. Walk, N.; Wiseman, H.M.; Ralph, T.C. Continuous variable one-sided device independent quantum key distribution. **2014**, arXiv:1405.6593.
30. Marshall, K.; Weedbrook, C. Device-independent quantum cryptography for continuous variables. *Phys. Rev. A* **2014**, *90*, 042311.
31. Braunstein, S.L.; Pirandola, S. Side-Channel-Free Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502.
32. Li, Z.; Zhang, Y.-C.; Xu, F.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052301.
33. Zhang, Y.-C.; Li, Z.; Yu, S.; Gu, W.; Peng, X.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. *Phys. Rev. A* **2014**, *90*, 052325.
34. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. *Nat. Photon.* **2015**, 397–402.
35. Ottaviani, C.; Spedalieri, G.; Braunstein, S.L.; Pirandola, S. Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric conguration. *Phys. Rev. A* **2015**, *91*, 022320.
36. Xiang, G.Y.; Ralph, T.C.; Lund, A.P.; Walk, N.; Pryde, G.J. Heralded noiseless linear amplification and distilation of entanglement. *Nat. Photon.* **2010**, *4*, 316–319.
37. Weedbrook, C. Continuous-variable quantum key distribution with entanglement in the middle. *Phys. Rev. A* **2013**, *87*, 022308.
38. Blandino, R.; Leverrier, A.; Barbieri, M.; Etesse, J.; Grangier, P.; Tualle-Brouri, R. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A* **2012**, *86*, 012327.
39. Fiurášek, J.; Cerf, N.J. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. *Phys. Rev. A* **2012**, *86*, 060302.
40. Walk, N.; Ralph, T.C.; Symul, T.; Lam, P.K. Security of continuous-variable quantum cryptography with Gaussian postselection. *Phys. Rev. A* **2013**, *87*, 020303.

41. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. London Ser. A* **2005** *461* 207-235.
42. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Communication*; Cambridge University Press: Cambridge, UK, 2000.
43. Navascués, M.; Grosshans, F.; Acín, A. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502.
44. García-Patrón, R.; Cerf, N.J. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503.
45. Xu, B.; Tang, C.; Chen, H.; Zhang, W.; Zhu, F. Improving the maximum transmission distance of four-state continuous-variable quantum key distribution by using a noiseless linear amplifier. *Phys. Rev. A* **2013**, *87*, 062311.
46. Wang, T.; Yu, S.; Zhang, Y.-C.; Gu, W.; Guo, H. 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.
47. Walk, N., Lund, A.P.; Ralph, T.C. Non-deterministic noiseless amplification via non-symplectic phase space transformations. *New J. Phys.* **2013**, *15*, 073014.
48. Bernu, J.; Armstrong, S.; Symul, T.; Ralph, T.C.; Lam, P.K. Theoretical analysis of an ideal noiseless linear amplifier for Einstein-Podolsky-Rosen entanglement distilation. *J. Phys. B* **2014**, *47*, 215503.
49. Eisert, J.; Browne, D.E.; Scheel, S.; Plenio, M.B. Distillation of continuous-variable entanglement with optical means. *Ann. Phys.* **2004**, *311*, 431–458.
50. Pandey, S.; Jiang, Z.; Combes, J.; Caves, C.M. Quantum limits on probabilistic amplifiers. *Phys. Rev. A* **2013**, *88*, 033852.
51. Pirandola, S.; Braunstein, S.L.; Lloyd, S. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **2008**, *101*, 200504.
52. Chrzanowski, H.M.; Walk, N.; Assad, S.M.; Janousek, J.; Hosseini, S.; Ralph, T.C.; Lam, P.K. Measurement-based noiseless linear amplification for quantum communication. *Nat. Photon.* **2014**, *8*, 333–338.
53. Cerf, N.J.; Levy, M.; van Assche, G. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **2001**, *63*, 052311.
54. García-Patrón, R.; Cerf, N.J. Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels. *Phys. Rev. Lett.* **2009**, *102*, 130501.
55. Pirandola, S.; García-Patrón, R.; Braunstein, S.L.; Lloyd, S. Direct and Reverse Secret-Key Capacities of a Quantum Channel. *Phys. Rev. Lett.* **2009**, *102*, 050503.