entropy

MDPI

Article

Security Analysis of Unidimensional Continuous-Variable Quantum Key Distribution Using Uncertainty Relations

Pu Wang [1], Xuyang Wang [1,2,*] and Yongmin Li [1,2,*]

[1] State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China; 201622607026@email.sxu.edu.cn
[2] Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China
* Correspondence: wangxuyang@sxu.edu.cn (X.W.); yongmin@sxu.edu.cn (Y.L.)

Received: 30 January 2018; Accepted: 27 February 2018; Published: 1 March 2018

Abstract: We study the equivalence between the entanglement-based scheme and prepare-and-measure scheme of unidimensional (UD) continuous-variable quantum key distribution protocol. Based on this equivalence, the physicality and security of the UD coherent-state protocols in the ideal detection and realistic detection conditions are investigated using the Heisenberg uncertainty relation, respectively. We also present a method to increase both the secret key rates and maximal transmission distances of the UD coherent-state protocol by adding an optimal noise to the reconciliation side. It is expected that our analysis will aid in the practical applications of the UD protocol.

Keywords: continuous-variable quantum key distribution; unidimensional modulation; Heisenberg uncertainty relations

1. Introduction

Quantum key distribution (QKD), which is a prominent application of the quantum information, enables two remote parties, conventionally called Alice and Bob, to share a common secret key through an insecure quantum channel and an authenticated classical channel [1,2]. This unconditional security is guaranteed by the basic principles of quantum mechanics. Continuous-variable quantum key distribution (CV-QKD) has attracted considerable attention over the past years because of its good performances in the secret key rates and compatibility with the current optical networks [3–16]. A particular class of CV-QKD protocols that is based on the Gaussian modulation of coherent states has experienced a rapid development [17–27]. In a coherent-state protocol, Alice encodes her information in the amplitude and phase quadratures of the coherent light field by using amplitude and phase modulators, and Bob performs homodyne or heterodyne detection.

Recently, a further simplified unidimensional (UD) CV-QKD protocol has been proposed [28]. In such protocol, Alice, still using coherent states, encodes her information by using one modulator (e.g., amplitude modulator) instead of two, whereas Bob performs a homodyne detection, hence simplifying both the modulation scheme and the key extraction task. The security against collective attacks has been proved in asymptotic regime. However, this early work only considered the UD model under an idea homodyne detector. It does not refer to the realistic condition, such as the efficiency and electronic noise of the homodyne detector. Then, a model of the UD protocol under realistic condition was designed and realized in an experiment [29]. Furthermore, the finite size effect was analyzed in paper [30], and an optimum ratio in parameters estimation was proposed.

In the UD protocol, due to the fact that the phase quadrature is not modulated in Alice's side, we cannot estimate the correlation in the phase quadrature between Alice and Bob. However, this unknown parameter is bounded by the requirement of the physicality of the state. A Gaussian state can typically be characterized by a covariance matrix. However, not all covariance matrices correspond to physical states, as the covariance matrix must respect the Heisenberg uncertainty relation [31,32]. By using this uncertainty relation, we can calculate the physical region boundary of a covariance matrix, which is crucial for the security of the protocol. We can see that the UD CV-QKD protocol is very different from the previous symmetrical (SY) coherent-state protocol [18,21]. Due to the equivalence between the prepare-and-measure (PM) and entanglement-based (EB) scheme of UD protocol, the differences of the Heisenberg uncertainty relations under the idea and realistic condition, and the effect of noise from Bob's setup on secret key rate under realistic condition are not described or investigated in depth [28–30], a further study about above questions is required.

In this paper, we first consider the equivalence between the PM scheme and the EB scheme of the UD CV-QKD protocol. Then, we analyze the boundary of the physical region of the symmetrical coherent-state protocol based on the Heisenberg uncertainty relation. We also study the variances of the physical region of the UD coherent-state protocol under the conditions of different detection efficiency and electronic noise. Secure and unsecure regions of both the protocols are further analyzed under ideal and realistic detection conditions. It is found that adding an optimal noise to Bob's side can truly help the improvement of the secret key rate and increase the transmission distance of the UD coherent-state protocol under the assumption of reverse reconciliation.

The paper is organized as follows. In Section 2, we introduce the equivalence between the EB scheme and the PM scheme of the UD CV-QKD protocol. In Section 3, a comparison between the physical and secure regions of the UD protocol under ideal and realistic detection conditions is shown, and a method to improve the performance of the UD coherent-state protocol by adding an optimal noise to Bob's side is proposed. In Section 4, we give our conclusions and discussions.

2. Unidimensional Quantum Key Distribution

2.1. Equivalence between the EB Scheme and the PM Scheme

Generally, most of the experimental systems in CV-QKD are focused on PM schemes currently, given their ease of implementation in practice. However, it's hard to analyze the security in theory. On the contrary, the theoretical analysis based on EB scheme is maturity. The involved entangled states make the calculations feasible and simpler [33]. Especially in UD CV-QKD protocol, the security analysis based on EB scheme has more advantages. The covariance matrices achieved from the EB schemes contain the constraints of phase amplitude quadrature. However these constraints is difficult to achieve from the PM scheme. More details about the security analysis will be shown later. Now, it is necessary to study the equivalence of EB and PM schemes, firstly. This equivalence is based on the indistinguishability between these two protocols for Bob and Eve. The consequent advantage of this equivalence is that it is sufficient to implement the PM scheme and study the EB scheme.

In the PM scheme, as depicted in Figure 1a, the sender, Alice, prepares coherent states using a laser source. Then, she encodes the information in the amplitude or phase quadratures of coherent states by using either amplitude or phase modulators. Here, without losing generality, we assume that Alice uses an amplitude modulator with a modulation variance V_M, which is assumed to be expressed in shot-noise units, and that the coherent states follow the uncertainty principle of variance 1. Thus, the mixture of Gaussian-modulated coherent states gives rise to a unidimensional chain structure with a thickness of 1 and a length of $\sqrt{1+V_M}$ in the phase space. These quantum states are then sent to Bob through an untrusted quantum channel with transmittance T_x, T_y and excess noise ε_x, ε_y.

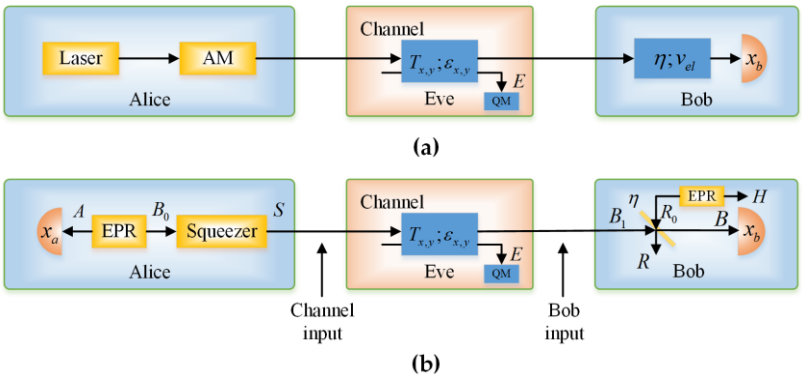

Figure 1. Unidimensional (UD) protocol schemes under realistic conditions. (**a**) Prepare-and-measure (PM) scheme of the UD protocol; (**b**) Entanglement-based (EB) scheme of the UD protocol.

In the EB scheme, as shown in Figure 1b, Alice starts with a two-mode squeezed vacuum state ρ_{AB_0} with variance V. Then, she performs homodyne detection on the first half of the state and squeezes the second half by $r = \ln\sqrt{V}$. The result is the covariance matrix

$$\gamma_{AS} = \begin{bmatrix} V & 0 & \sqrt{V\left(V^2-1\right)} & 0 \\ 0 & V & 0 & -\sqrt{\left(V^2-1\right)/V} \\ \sqrt{V\left(V^2-1\right)} & 0 & V^2 & 0 \\ 0 & -\sqrt{\left(V^2-1\right)/V} & 0 & 1 \end{bmatrix} \tag{1}$$

The covariance matrix of mode S, conditioned on Alice's measurement result (x_a), can be written as

$$\gamma_S^{x_a} = \gamma_S - \sigma_{AS}^T \left(X\gamma_A X\right)^{MP} \sigma_{AS}, \tag{2}$$

and the displacement vector can be expressed as

$$d_S^{x_a} = \sigma_{AS}^T \left(X\gamma_A X\right)^{MP} d_A, \tag{3}$$

where d_A is the result of the homodyne measurement, γ_A and γ_S are the covariance matrices of the modes A and S, respectively, σ_{AS} is the correlation matrix of the two modes, $X = diag(1,0)$, and MP denotes the Moore–Penrose inverse of the matrix [34].

Then, we obtain

$$\gamma_S^{x_a} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } d_S^{x_a} = \sqrt{\frac{V^2-1}{V}}\left(x_a, 0\right), \tag{4}$$

which is a coherent state centered on $d_S^{x_a}$. Furthermore, the variance of $d_S^{x_a}$ is

$$\left\langle \Delta^2 d_S^{x_a} \right\rangle = \frac{V^2-1}{V}\left\langle x_a^2 \right\rangle = \frac{V^2-1}{V}\cdot V = V^2-1, \tag{5}$$

where V^2-1 is exactly the variance of the Alice's V_M. Then, we can establish a one-to-one correspondence between the EB scheme and the PM scheme by multiplying the outcome of Alice's measurements by the factor $\alpha = \sqrt{\frac{V^2-1}{V}}$.

2.2. Calculation of Secret Key Rate with Reverse Reconciliation

Thus far, we have established the equivalence between the EB scheme and the PM scheme of the UD CV-QKD protocol. In this subsection, we present a brief overview of the calculation of the secret key rates. In the EB protocol, the realistic Bob's detector can be modeled by an ideal balanced homodyne detector and a beam splitter, with transmission efficiency η and input noise $V_N = 1 + v_{el}/(1-\eta)$, as the one shown in Figure 1b. The secret key rate against collective attacks for reverse reconciliation in the asymptotic regime can be calculated as [29,30]

$$K_{RR}^{\infty} = \beta \cdot I_{AB} - \chi_{BE}, \tag{6}$$

where β is the reverse reconciliation efficiency and I_{AB} is the mutual information between Alice and Bob. I_{AB} can expressed as

$$I_{AB} = \frac{1}{2}\log_2\left(1 + \frac{V_M}{1+\chi_{\text{totx}}}\right), \tag{7}$$

where

$$\begin{aligned} \chi_{\text{hom}} &= (1+v_{el})/\eta - 1 \\ \chi_{\text{linex}} &= (1-T_x)/T_x + \varepsilon_x \\ \chi_{\text{totx}} &= \chi_{\text{linex}} + \chi_{\text{hom}}/T_x \end{aligned}. \tag{8}$$

Still from Equation (6), χ_{BE} is the Holevo bound, which represents an upper bound on the information acquired for reverse reconciliation by the potential eavesdropper Eve. The procedures to calculate χ_{BE} can be written as:

$$\begin{aligned} \chi_{BE} &= S(\rho_E) - \mathrm{S}\left(\rho_E^{x_b}\right) \\ &= S(\rho_{AB_1}) - S(\rho_{ARH}^{x_b}) \\ &= \sum_{i=1}^{2} g\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} g\left(\frac{\lambda_i - 1}{2}\right) \end{aligned}, \tag{9}$$

where $S(\rho)$ is the von Neumann entropy of the quantum state ρ, $g(x) = (x+1)\log_2(x+1) - x\log_2 x$ and λ_i are the symplectic eigenvalues of the covariance matrix γ, with

$$\begin{aligned} \lambda_{1,2}^2 &= \frac{1}{2}\left(a \pm \sqrt{a^2 - 4b}\right) \\ \lambda_{3,4}^2 &= \frac{1}{2}\left(c \pm \sqrt{c^2 - 4d}\right), \\ \lambda_5 &= 1 \end{aligned} \tag{10}$$

$$\begin{aligned} a &= 1 + V_M + V_y^{B_1}\left(1 + V_M + \chi_{\text{linex}}\right)T_x + 2C_y^{B_1}\left(1+V_M\right)^{1/4}\sqrt{V_M T_x} \\ b &= \left(V_y^{B_1}(1+V_M) - \left(C_y^{B_1}\right)^2\sqrt{1+V_M}\right)\left(1+\varepsilon_x T_x\right) \\ c &= \left(a(\chi_{\text{hom}}+1) + \left((1+\varepsilon_x T_x)(V_M+2) + V_M T_x - a\right)\right)/e \\ d &= \left(b\chi_{\text{hom}} + (1+V_M)(1+\varepsilon_x T_x)\right)/e \\ e &= T_x(1 + V_M + \chi_{\text{totx}}) \end{aligned}, \tag{11}$$

where $V_y^{B_1}$ is the variance of the mode B_1 in phase quadrature with $V_y^{B_1} = 1 + T_y\varepsilon_y$ and $C_y^{B_1}$ is the correlation between A and B_1 in phase quadrature with $C_y^{B_1} = -\sqrt{T_y V_M}\left(1+V_M\right)^{-1/4}$.

3. Security Analysis Using Uncertainty Relations

In this section, we provide a security analysis of continuous variable quantum key distribution with coherent states based on the Heisenberg uncertainty relation. Before describing the UD coherent-state protocol case, it is useful to first consider the SY coherent-state protocol case.

3.1. Uncertainty Relations for Symmetrical Coherent-State Protocol

Let us consider a n-mode quantum mechanical system that is described by the canonical conjugate operators $\hat{x}_j$ and $\hat{p}_j$, with $j=1,2,\cdots,n$. In terms of the annihilation and creation operators ($\hat{a}_j$ and $\hat{a}_j^\dagger$, respectively), one has

$$\hat{x}_j = \frac{1}{\sqrt{2}}\left(\hat{a}_j + \hat{a}_j^\dagger\right) \quad \text{and} \quad \hat{p}_j = -\frac{i}{\sqrt{2}}\left(\hat{a}_j - \hat{a}_j^\dagger\right), \tag{12}$$

which are the dimensionless position and momentum operators. Such operators also satisfy the bosonic canonical commutation relations (CCR)

$$[\hat{x}_i, \hat{p}_j] = i\delta_{i,j}, \quad [\hat{x}_i, \hat{x}_j] = [\hat{p}_i, \hat{p}_j] = 0, \tag{13}$$

Furthermore, if we group together the canonical conjugate operators in a vector $\hat{\gamma}$ as

$$\hat{\gamma} = \left(\hat{r}_1, \hat{r}_2, \cdots \hat{r}_{2n}\right)^T = \left(\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, \cdots, \hat{x}_n, \hat{p}_n\right)^T, \tag{14}$$

we can express the CCR in a compact form:

$$[\hat{\gamma}_j, \hat{\gamma}_k] = i\Omega_{jk}, \tag{15}$$

where Ω is defined as

$$\Omega = \bigoplus_{i=1}^{n} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{16}$$

By combining this CCR relation and the positive semi-definiteness of the density operator ρ, we obtain the following uncertainty relation [35]

$$\gamma + i \cdot \Omega \geq 0, \tag{17}$$

which is a more precise and complete version of the Heisenberg uncertainty relation. This well-known inequality is the only constraint that γ has to respect to be a covariance matrix satisfying a physical state.

Let us consider the physicality of the SY coherent-state protocol by using the uncertainty relation in Equation (17). In the EB protocol, as shown in Figure 2, we have:

$$\gamma_{AB_1}^{sym} = \begin{bmatrix} V & 0 & \sqrt{T\left(V^2-1\right)} & 0 \\ 0 & V & 0 & -\sqrt{T\left(V^2-1\right)} \\ \sqrt{T\left(V^2-1\right)} & 0 & T\left(V+\chi_{\text{line}}\right) & 0 \\ 0 & -\sqrt{T\left(V^2-1\right)} & 0 & T\left(V+\chi_{\text{line}}\right) \end{bmatrix}, \tag{18}$$

$$\gamma_{AB}^{sym} = \begin{bmatrix} V & 0 & \sqrt{\eta T\left(V^2-1\right)} & 0 \\ 0 & V & 0 & -\sqrt{\eta T\left(V^2-1\right)} \\ \sqrt{\eta T\left(V^2-1\right)} & 0 & \eta T\left(V+\chi_{\text{tot}}\right) & 0 \\ 0 & -\sqrt{\eta T\left(V^2-1\right)} & 0 & \eta T\left(V+\chi_{\text{tot}}\right) \end{bmatrix}, \tag{19}$$

where $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{hom}}/T$, $\chi_{\text{line}} = (1-T)/T + \varepsilon$, $\chi_{\text{hom}} = (1-\eta)/\eta + v_{el}/\eta$, and $V = V_A + 1$, V_A is the modulation variance of the Alice's side. According to the Heisenberg uncertainty relation, we have:

$$\begin{cases} \gamma_{AB_1}^{sym} + i \cdot \Omega \geq 0 \\ \gamma_{AB}^{sym} + i \cdot \Omega \geq 0 \end{cases}. \tag{20}$$

Then, we obtain

$$\begin{cases} \varepsilon T\left(2+(\varepsilon-2)T\right)\left(V^2-1\right) \geq 0 \\ \left(\varepsilon T\eta\left(2+(\varepsilon-2)T\eta\right)+2v_{el}\left(1+(\varepsilon-1)T\eta\right)+v_{el}^2\right)\left(V^2-1\right) \geq 0 \end{cases}. \tag{21}$$

The two inequalities in Equation (21) are simultaneously satisfied if $\varepsilon, v_{el} \geq 0$ and $T, \eta \in [0,1]$. Here, we further consider the secure and unsecure regions of the protocol for both ideal and realistic Bob's detectors, which are shown in Figure 3a. In the secure region, the secret key rate is greater than zero; in the unsecure region, the secret key rate is less than zero. We observe that the realistic protocol can provide a bigger secure region. The secret key rate as a function of the excess noise, in correspondence of three values of channel losses, under ideal and realistic detection conditions, is shown in Figure 3b. We can see that the realistic Bob detection improves the resistance of the protocol to the excess noise, although the total noise is increased, which will lead to the appearance of a phenomenon called "fighting noise with noise" [36], and will be discussed in detail in the following. Here, we set the values of the actual parameters: the reconciliation efficiency is $\beta = 0.99$ [37] and the modulation variance is $V_A = 10$.

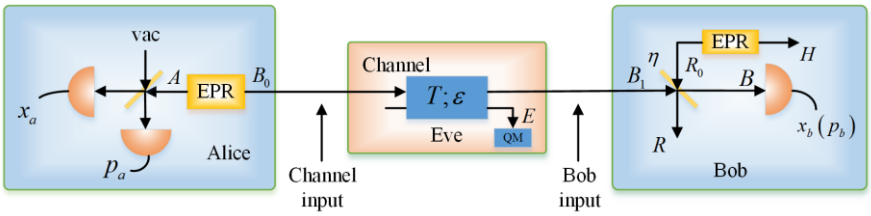

Figure 2. EB scheme of the SY protocol under realistic conditions.

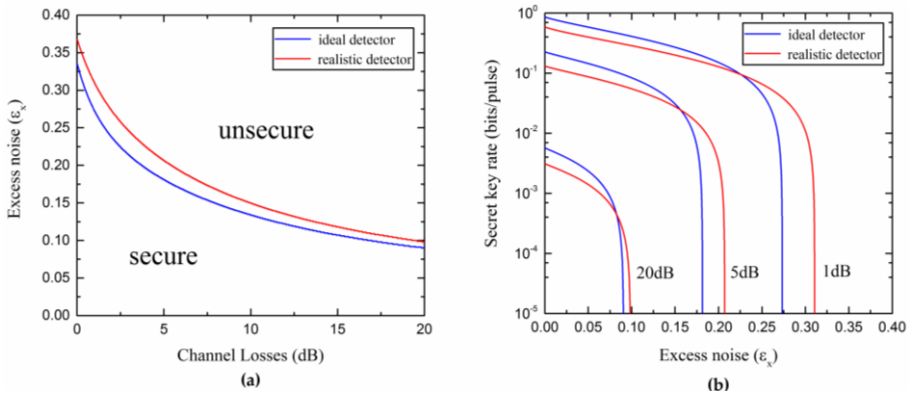

Figure 3. (**a**) Secure and unsecure regions of the SY protocol using ideal homodyne detector ($\eta = 1, v_{el} = 0$) and realistic homodyne detector ($\eta = 0.6, v_{el} = 0.1$); (**b**) Secret key rate versus the excess noise for different channel losses.

3.2. Uncertainty Relations for Unidimensional Coherent-State Protocol

In the above, we have discussed the physicality of the SY coherent-state protocol by using the Heisenberg uncertainty relation. The securities under ideal and realistic homodyne detectors have also been analyzed. Next, let us consider the UD coherent-state protocol. As shown in Figure 1b, in the EB scheme, we have

$$\gamma_{AB_1}^{uni} = \begin{bmatrix} \sqrt{1+V_M} & 0 & \sqrt{T_x V_M}\left(1+V_M\right)^{1/4} & 0 \\ 0 & \sqrt{1+V_M} & 0 & C_y^{B_1} \\ \sqrt{T_x V_M}\left(1+V_M\right)^{1/4} & 0 & T_x\left(V_M+1+\chi_{\text{linex}}\right) & 0 \\ 0 & C_y^{B_1} & 0 & V_y^{B_1} \end{bmatrix} \text{ and} \tag{22}$$

$$\gamma_{AB}^{uni} = \begin{bmatrix} \sqrt{1+V_M} & 0 & \sqrt{\eta T_x V_M}\left(1+V_M\right)^{1/4} & 0 \\ 0 & \sqrt{1+V_M} & 0 & C_y^{B_1}\sqrt{\eta} \\ \sqrt{\eta T_x V_M}\left(1+V_M\right)^{1/4} & 0 & \eta T_x\left(V_M+1+\chi_{\text{totx}}\right) & 0 \\ 0 & C_y^{B_1}\sqrt{\eta} & 0 & \eta\left(V_y^{B_1}+\chi_{\text{hom}}\right) \end{bmatrix}. \tag{23}$$

In the UD protocol, in order to estimate the information of the Eve eavesdropping, χ_{BE}, we have to know the parameters $C_y^{B_1}$ and $V_y^{B_1}$. Here, $V_y^{B_1}$ can be estimated by randomly measuring the phase quadrature in Bob's side, while $C_y^{B_1}$ is unknown due to the fact that the phase quadrature is not modulated in Alice's side. However, such an unknown parameter is constrained by the requirement of the physicality of the state. Differently from Ref. [30], under realistic condition, when the mode B_1 is transformed into mode B after the beam splitter, there will have to be a new constraint on the covariance matrix γ_{AB}^{uni} in order to make it correspondent to a physical state. According to the Heisenberg uncertainty relation, we have

$$\begin{cases} \gamma_{AB_1}^{uni} + i\cdot\Omega \geq 0 \\ \gamma_{AB}^{uni} + i\cdot\Omega \geq 0 \end{cases}. \tag{24}$$

Then, we obtain the following two parabolic equations:

$$\begin{cases} (C_y^{B_1} - C_0)^2 \leq \dfrac{V_M}{\sqrt{(1+V_M)}}\dfrac{\chi_{\text{linex}}}{1+\chi_{\text{linex}}}(V_y^{B_1} - V_0) \\ (C_y^{B_1} - C_0')^2 \leq \dfrac{V_M}{\sqrt{(1+V_M)}}\dfrac{\chi_{\text{totx}}}{1+\chi_{\text{totx}}}(V_y^{B_1} - V_0') \end{cases}, \tag{25}$$

where $C_0 = -\dfrac{V_0\sqrt{T_x V_M}}{(1+V_M)^{1/4}}$, $V_0 = \dfrac{1}{T_x\left(1+\chi_{\text{linex}}\right)}$, $C_0' = -\dfrac{\sqrt{T_x V_M}}{(1+V_M)^{1/4}\eta T_x\left(1+\chi_{\text{totx}}\right)}$ and $V_0' = \dfrac{1}{\eta^2 T_x\left(1+\chi_{\text{totx}}\right)} - \chi_{\text{hom}}$.

The parabolic curves between $C_y^{B_1}$ and $V_y^{B_1}$, under ideal and realistic detection conditions, are shown in Figure 4. The whole plane is divided into two regions: the unphysical and physical regions. In the unphysical region, the values of the parameters $C_y^{B_1}$ and $V_y^{B_1}$ cannot be satisfied simultaneously, otherwise, the Heisenberg uncertainty principle will be violated. In the physical region, the whole region is divided into two parts, R1 and R2. The R1 represents the real physical region, which is delimited by the ideal parabolic curve and ensures the attacks of Eve to the quantum channel complying with the physical principles. The red dashed line further divides the region R1 into unsecure and secure regions. The R2 represents the pseudo physical region, which is the overlapped part between the physical region contained by the realistic parabolic curve and the unphysical region, as defined by the ideal parabolic curve. The appearance of the pseudo physical region is due to the fact that, even if some attacks of Eve are unphysical, after the transform of the realistic homodyne detection of Bob, the final covariance matrix can satisfy a physical state. Hence, the physical region should be delimited at the input side of Bob, or equivalently, Bob performs an ideal detection. Furthermore, in Figure 5, we see how the physical region delimited by the realistic parabolic curve changes according to different conditions of detection efficiency and electronic noise. We also compare such regions with the one delimited by the ideal parabolic curve (black solid line in Figure 5). We find that the physical region defined by the realistic parabolic curve gradually decreases

as the detection efficiency increases and the electronic noise decreases. Therefore, also in this case, in order to ensure the physicality of the UD protocol, we select the smaller region R1.

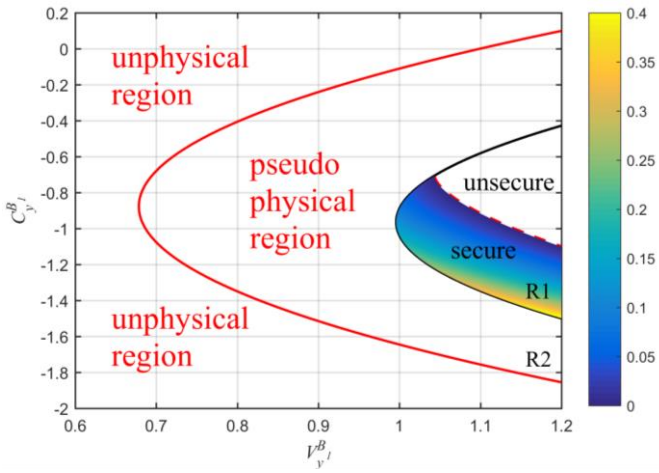

Figure 4. Comparison among physical regions of the UD protocol under both ideal and realistic detection conditions. The red solid line represents the realistic parabolic curve (equivalent to Bob using a realistic homodyne detector with $\eta = 0.6, v_{el} = 0.1$) and black solid line is the ideal parabolic curve (equivalent to Bob using an ideal homodyne detector with $\eta = 1, v_{el} = 0$). The red dashed line represents the part where the key rate is zero under realistic detection condition. Here, we set: $\beta = 0.99$, $T_x = 0.4$ (corresponding to a distance of 20 km fiber), $\varepsilon_x = 0.01$ and $V_M = 6.35$.

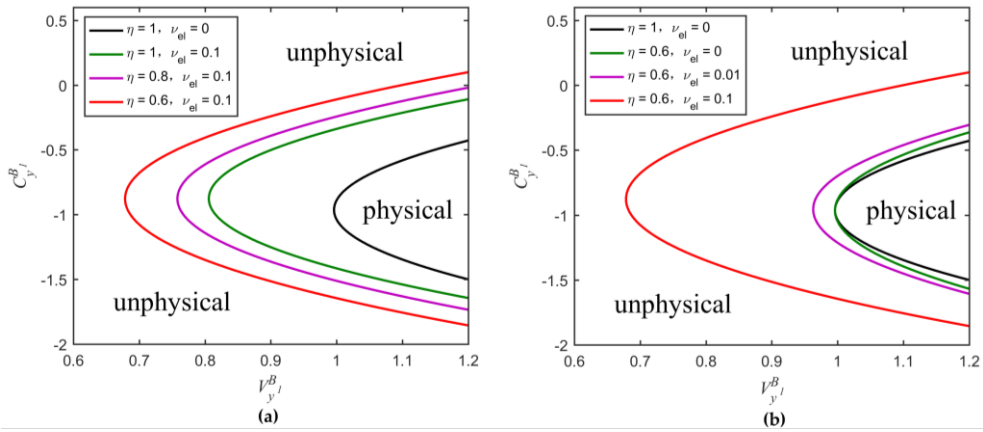

Figure 5. Comparison among physical regions delimited by the parabolic curves of the UD protocol. The black solid curve corresponds to the ideal parabolic curve, whereas the others to the realistic parabolic curves obtained for different parameter conditions. (**a**) Changes of the physical region extension according to different values of η (v_{el} remains constant); (**b**) Changes of the physical region extension according to different values of v_{el} (η remains constant). The values of the parameters T_x, ε_x, and V_M are the same as in Figure 4.

In Figure 6, we consider the dependence of the ideal parabolic curve (R1) on related parameters, including V_M, T_x, ε_x, and β. From Figure 6a, we can find that the parabolic curve moves down and gradually becomes broader as the modulation variance increases. In Figure 6b, the parabolic curve moves towards bottom-left corner and gradually becomes narrower as the transmission efficiency increases. In Figure 6c, as the excess noise increases, the parabolic curve moves towards left and gradually becomes larger. The reconciliation efficiency β does not change the shape of the parabola, but rather expands the secure region. In Figure 6d, the red solid line represents the minimum secret key rate, which was obtained by scanning the parameter $C_y^{B_1}$. The black solid line represents the ideal parabolic curve. It is interesting that a larger $C_y^{B_1}$ does not always give a higher

secret key rate, more details about the red solid line can be seen in paper [30]. Later, we can see that the minimum secret key rate can also be achieved by scanning T_y and ε_y simultaneously.

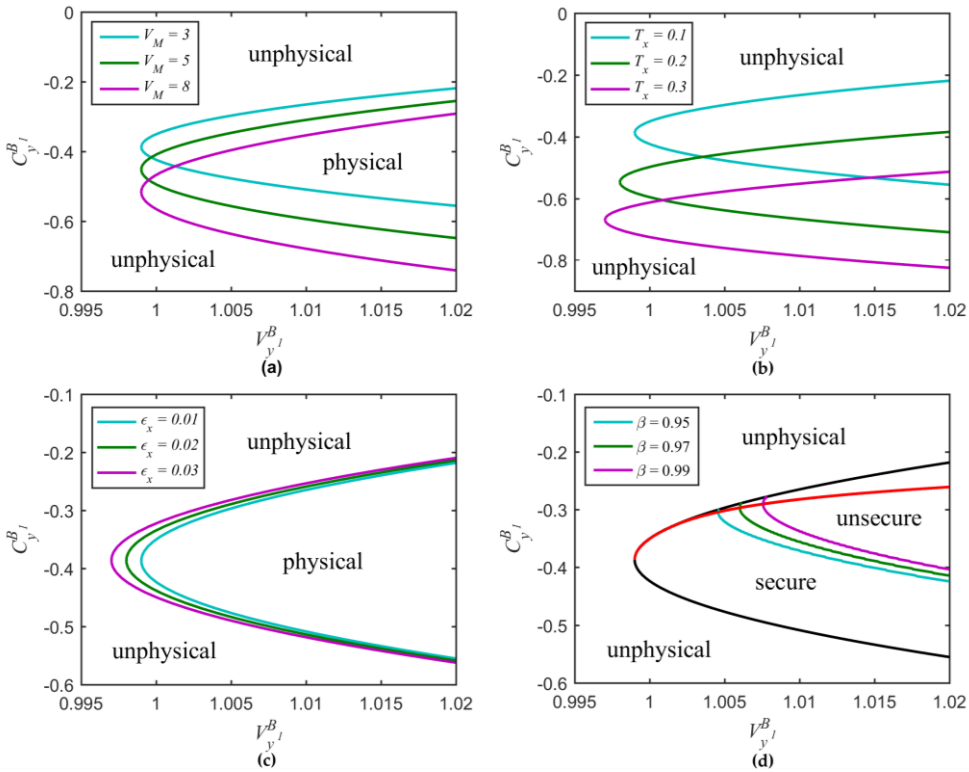

Figure 6. Ideal parabolic curve versus related parameters. (**a**) Different modulation variance values with $T_x = 0.1$ and $\varepsilon_x = 0.01$; (**b**) Different transmission efficiency values with $\varepsilon_x = 0.01$ and $V_M = 3$; (**c**) Different excess noise values with $T_x = 0.1$ and $V_M = 3$; (**d**) Different reconciliation efficiency values with $T_x = 0.1$, $\varepsilon_x = 0.01$, and $V_M = 3$.

Furthermore, if we assume $C_y^{B_1} = -\sqrt{T_y V_M}\left(1+V_M\right)^{-1/4}$ and $V_y^{B_1} = 1+T_y\varepsilon_y$, the parabolic equations (Equation (25)), as determined by the Heisenberg uncertainty relation under ideal and realistic detection conditions transform into

$$\begin{cases} \left(k\sqrt{T_x}-\sqrt{T_y}\right)^2 \le \left(1-kT_x\right)\left(1+T_y\varepsilon_y-k\right) \\ \left(k'\sqrt{T_x}-\sqrt{T_y}\right)^2 \le \left(1-k'T_x\eta\right)\left(1+T_y\varepsilon_y-k'/\eta+\chi_{\text{hom}}\right) \end{cases}, \tag{26}$$

where $k = \dfrac{1}{T_x\left(1+\chi_{\text{linex}}\right)}$ and $k' = \dfrac{1}{\eta T_x\left(1+\chi_{\text{totx}}\right)}$. By this way, more details about eavesdropping method taken by Eve can be found. Moreover, one can easily see that the transformed equations do not depend on V_M. We redraw the physical regions delimited by the new curves for different values of detection efficiency and electronic noise as shown in Figure 7. We obtain the same rule as in Figure 5 that the physical region gradually decreases as the detection efficiency increases and the electronic noise decreases. Secure and unsecure regions under the realistic detection condition are shown in Figure 8. The cyan curve with the secret key rate of zero represents the boundary of two regions. Although the parameters T_y and ε_y are unknown, they are confined to the curve $V_y^{B_1} = 1+T_y\varepsilon_y$, which can be estimated by randomly measuring the phase quadrature in Bob's side, meaning that T_y and ε_y cannot be set simultaneously in other physical places outside this curve. We can see that Eve essentially changes the value of the parameter $C_y^{B_1}$ by controlling the value of T_y. For a constant value of $V_y^{B_1}$, we can calculate the minimum secret key rate by scanning T_y or ε_y in the physical

region. As shown in Figure 8, the curve corresponding to the minimum secret key rate is divided into three parts. The red curve part overlaps with the left boundary of the black solid curve which corresponds to the black solid curve in Figure 6d. As the value of $V_y^{B_1}$ increases, the worst-case T_y and ε_y (green curve part) gradually separate from the black solid curve, meaning that the secret key rate of the protocol is not always monotonically decreasing as ε_y increases or T_y decreases, but still lie in the secure region. The blue curve represents the part where the minimum secret key rate is less than zero. We also find that this minimum secret key rate is equal to the minimum secret key rate that was obtained by scanning $C_y^{B_1}$ (corresponding to the red solid line of Figure 6d) when other parameter values are set to be consistent.

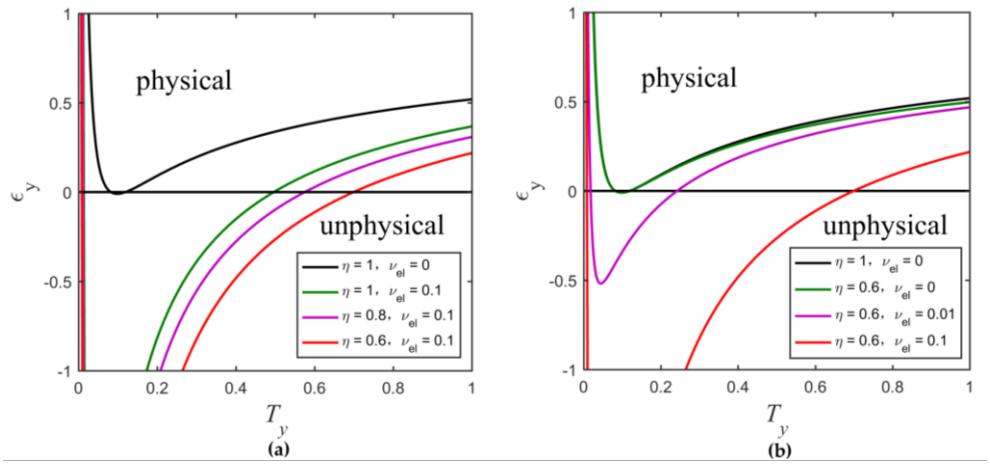

Figure 7. Comparison among physical regions delimited by the new curves of the UD protocol. (**a**) Changes of the physical region according to different values of η (v_{el} remains constant); (**b**) Changes of the physical region according to different values of v_{el} (η remains constant). The other parameters are $\beta = 0.99$, $T_x = 0.1$, $\varepsilon_x = 0.01$, and $V_M = 3$.

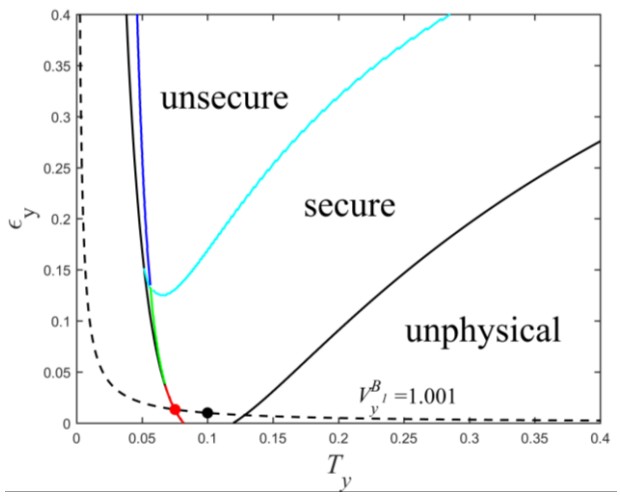

Figure 8. Secure and unsecure regions of the UD protocol under realistic detection condition. The parameters are set to $\beta = 0.99$, $V_M = 3$, $T_x = 0.1$, $\varepsilon_x = 0.01$, $\eta = 0.6$, and $v_{el} = 0.1$.

In typical communication channels, the value of $V_y^{B_1}$ can be estimated by setting $V_y^{B_1} \approx 1 + T_x \varepsilon_x = 1.001$, which is plotted with the black dashed line of Figure 8. At the black point, the conditions $T_x = T_y$ and $\varepsilon_x = \varepsilon_y$ are satisfied. The red point represents the worst-case T_y and ε_y, which is the intersection of the red line and black dashed line. Because Eve can distinguishes T_y, ε_y from T_x, ε_x by measuring coherent states sent by Alice, she can arbitrarily change the values of

both T_y and ε_y, while keeps $V_y^{B_1}$ unchanged, eventually, obtains more information. If Alice and Bob use T_x and ε_x to estimate T_y and ε_y (black point), then this will underestimate the ability of the eavesdropper Eve and provide security loopholes. Therefore, here we should consider the minimum secret key rate (red point).

In Figure 9, the curves representing the maximal tolerable excess noise versus the channel losses under ideal and realistic detection conditions are shown. We observe that the UD protocol has a lower tolerance to the excess noise than the SY protocol. However, the UD protocol reduces the complexity of the experiment and still provides a reasonable secure region (all of the parameters are set under the actual conditions).

In addition, from Figure 9b, it is not difficult to find out that the realistic Bob's detection can slightly increase the secure region of the UD protocol. This effect can be explained by considering the fact that the noise added on Bob's side not only affects Alice's and Bob's mutual information, but also decreases Eve's information in reverse reconciliation. Due to the detection at Bob's side, which can be controlled and observed by Bob, the noise added on Bob's side could be considered as a believable noise not controlled by the eavesdropper Eve. Moreover, it is found that there is an optimal noise χ_{hom} (characterized by the detection efficiency η and electronic noise v_{el}) that Bob needs to add to maximize the secret key rate for each channel loss. Then, we can effectively improve the secret key rate and increase the transmission distance by adding proper noise to Bob's side, as we show in Figure 10.

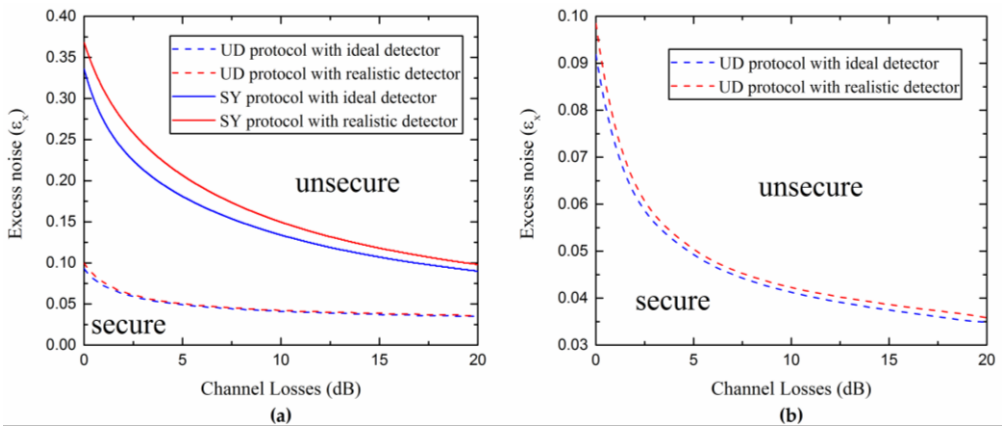

Figure 9. (**a**) Comparison between secure and unsecure regions for the SY coherent-state protocol and UD coherent-state protocol under different detection conditions; (**b**) Secure and unsecure regions of the UD protocol using an ideal homodyne detector ($\eta = 1, v_{el} = 0$) and a realistic one ($\eta = 0.6, v_{el} = 0.1$). Here we consider $V_M = 3$, $\beta = 0.99$, and the estimated value $V_y^{B_1} \approx 1 + T_x \varepsilon_x$.

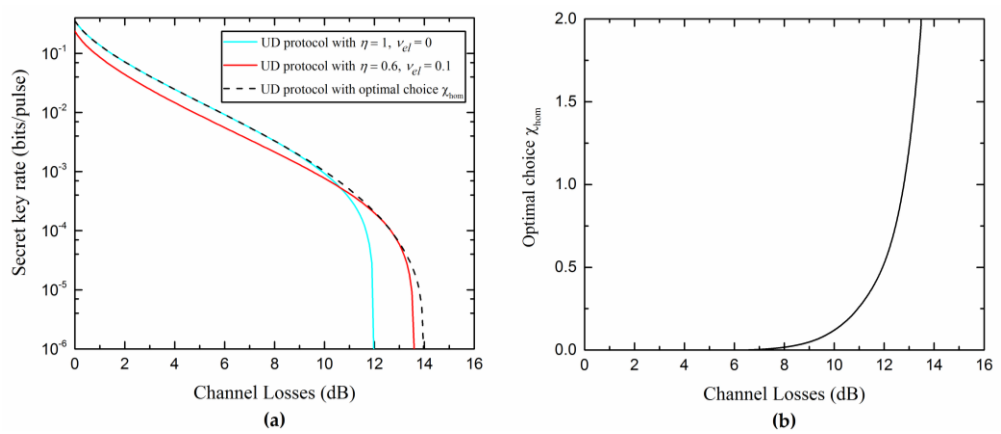

Figure 10. (**a**) Minimum secret key rate as a function of the channel losses; (**b**) Optimal choice of χ_{hom} that maximizes the secret key rate in (**a**). The other parameters are $\beta = 0.99$, $\varepsilon_x = 0.04$, $V_M = 3$, and $V_y^{B_1} \approx 1 + T_x \varepsilon_x$.

4. Conclusions

In this paper, we have proven the equivalence between the EB scheme and the PM scheme of the UD CV-QKD protocol, and investigated the physical and secure regions of the SY coherent-state protocol based on the Heisenberg uncertainty relation. It was shown that the realistic detection condition in UD protocol results in an excess pseudo physical region, which corresponds to the unphysical attack of Eve. In order to ensure the physicality, we should select the physical region delimited by the ideal curve. We also found that a realistic Bob's detection improves the resistance of the protocol to the channel excess noise, therefore, the performance in terms of the secret key rates and transmission distances of the UD coherent-state protocol can be improved by adding an optimal noise to the reconciliation side. Overall, the results confirm the potential of a long-distance secure communication through the usage of the UD CV-QKD protocol.

Acknowledgments: This work was supported by the Key Project of the Ministry of Science and Technology of China (2016YFA0301403), the National Natural Science Foundation of China (NSFC) (Grants No. 11504219, No. 61378010), the Shanxi 1331KSC, and the Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi.

Author Contributions: Pu Wang conceived the study, performed theoretical calculations and numerical simulations and drafted the article. Xuyang Wang designed the conception of the study, discussed the results, checked the draft and critically reviewed the manuscript. Yongmin Li proposed and supervised the project, checked the draft and provided a 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. Cerf, N.J.; Levy, M.; Van Assche, G. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A* **2001**, *63*, 052311, doi:10.1103/PhysRevA.63.052311.
4. Silberhorn, C.; Ralph, T.C.; Lütkenhaus, N.; Leuchs, G. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Phys. Rev. Lett.* **2002**, *89*, 167901, doi:10.1103/PhysRevLett.89.167901.
5. 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, doi:10.1103/PhysRevLett.93.170504.
6. Fossier, S.; Diamanti, E.; Debuisschert, T.; Villing, A.; Tualle-Brouri, R.; Grangier, P. Field test of a continuous-variable quantum key distribution prototype. *New J. Phys.* **2009**, *11*, 045023, doi:10.1088/1367-2630/11/4/045023.
7. Leverrier, A.; Grangier, P. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Phys. Rev. A* **2011**, *83*, 042312, doi:10.1103/PhysRevA.83.042312.
8. Madsen, L.S.; Usenko, V.C.; Lassen, M.; Filip, R.; Andersen, U.L. Continuous variable quantum key distribution with modulated entangled states. *Nat. Commun.* **2012**, *3*, 1083, doi:10.1038/ncomms2097.
9. Wang, X.Y.; Bai, Z.L.; Du, P.Y.; Li, Y.M.; Peng, K.C. Ultrastable fiber-based time-domain balanced homodyne detector for quantum communication. *Chin. Phys. Lett.* **2012**, *29*, 124202, doi:1088/0256-307X/29/12/124202.
10. 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.
11. Wang, X.Y.; Bai, Z.L.; Wang, S.F.; Li, Y.M.; Peng, K.C. Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise. *Chin. Phys. Lett.* **2013**, *30*, 010305, doi:10.1088/0256-307X/30/1/010305.
12. Gehring, T.; Handchen, V.; Duhme, J.; Furrer, F.; Franz, T.; Pacher, C.; Werner, R.F.; Schnabel, R. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nat. Commun.* **2015**, *6*, 8795, doi:10.1038/ncomms9795.

13. Zhang, Y.; Li, Z.; Weedbrook, C.; Marshall, K.; Pirandola, S.; Yu, S.; Guo, H. Noiseless linear amplifiers in entanglement-based continuous-variable quantum key distribution. *Entropy* **2015**, *17*, 4547, doi:10.3390/e17074547.
14. Li, H.S.; Wang, C.; Huang, P.; Huang, D.; Wang, T.; Zeng, G.H. Practical continuous-variable quantum key distribution without finite sampling bandwidth effects. *Opt. Express* **2016**, *24*, 20481–20493.
15. Bai, D.Y.; Huang, P.; Ma, H.X.; Wang, T.; Zeng, G.H. Performance improvement of plug-and-play dual-phase-modulated quantum key distribution by using a noiseless amplifier. *Entropy* **2017**, *19*, 546, doi:10.3390/e19100546.
16. Bai, Z.L.; Yang, S.S.; Li, Y.M. High-efficiency reconciliation for continuous variable quantum key distribution. *Jpn. J. Appl. Phys.* **2017**, *56*, 044401, doi:10.7567/JJAP.56.044401.
17. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902, doi:10.1103/PhysRevLett.88.057902.
18. 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.
19. Iblisdir, S.; Van Assche, G.; Cerf, N.J. Security of quantum key distribution with coherent states and homodyne detection. *Phys. Rev. Lett.* **2004**, *93*, 170502, doi:10.1103/PhysRevLett.93.170502.
20. Grosshans, F. Collective attacks and unconditional security in continuous variable quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 020504, doi:10.1103/PhysRevLett.94.020504.
21. 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, doi:10.1103/PhysRevLett.95.180503.
22. Lodewyck, J.; Bloch, M.; Garcia-Patron, 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*, 042503, doi:10.1103/PhysRevA.76.042503.
23. Qi, B.; Huang, L.L.; Qian, L.; Lo, H.K. Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **2007**, *76*, 052323, doi:10.1103/PhysRevA.76.052323.
24. Yang, S.S.; Bai, Z.L.; Wang, X.Y.; Li, Y.M. FPGA-based implementation of size-adaptive privacy amplification in quantum key distribution. *Photonics J.* **2017**, *9*, 7600308, doi:10.1109/JPHOT.2017.2761807.
25. 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*, 378–381.
26. Li, Y.M.; Wang, X.Y.; Bai, Z.L.; Liu, W.Y.; Yang, S.S.; Peng, K.C. Continuous variable quantum key distribution. *Chin. Phys. B* **2017**, *26*, 040303.
27. Liu, W.Y.; Wang, X.Y.; Wang, N.; Du, S.N.; Li, Y.M. Imperfect state preparation in continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *96*, 042312, doi:10.1103/PhysRevA.96.042312.
28. Usenko, V.C.; Grosshans, F. Unidimensional continuous-variable quantum key distribution. *Phys. Rev. A* **2015**, *92*, 062337, doi:10.1103/PhysRevA.92.062337.
29. Wang, X.Y.; Liu, W.Y.; Wang, P.; Li, Y.M. Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *95*, 062330, doi:10.1103/PhysRevA.95.062330.
30. Wang, P.; Wang, X.Y.; Li, J.Q.; Li, Y.M. Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions. *Opt. Express* **2017**, *25*, 27995–28009.
31. Braunstein, S.L.; van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513–577.
32. Serafini, A. Detecting entanglement by symplectic uncertainty relations. *J. Opt. Soc. Am. B* **2007**, *24*, 347–354.
33. Grosshans, F.; Cerf, N.J.; Wenger, J.; Tualle-Brouri, R.; Grangier, P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Inform. Comput.* **2003**, *3*, 535–552.
34. Ben-Israel, A.; Greville, T.N.E. *Generalized Inverses: Theory and Applications*, 2nd ed.; Springer: New York, NY, USA, 2003.
35. Serafini, A.; Paris, M.G.A.; Illuminati, F.; Siena, S.D. Quantifying decoherence in continuous variable systems. *J. Opt. B* **2005**, *7*, R19, doi:10.1088/1464-4266/7/4/R01.

36. Garcia-Patron, R.; Cerf, N.J. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.* **2009**, *102*, 130501, doi:10.1103/PhysRevLett.102.130501.
37. Milicevic, M.; Feng, C.; Zhang, L.M.; Gulak, P.G. Key reconciliation with low-density parity-check codes for long-distance quantum cryptography. *arXiv* **2017**, arXiv:1702.07740.