entropy

MDPI

Article

Unidimensional Continuous-Variable Quantum Key Distribution with Untrusted Detection under Realistic Conditions

Luyu Huang [1], Yichen Zhang [1,*], Ziyang Chen [2] and Song Yu [1]

[1] State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China; hly@bupt.edu.cn (L.H.); yusong@bupt.edu.cn (S.Y.)

[2] State Key Laboratory of Advanced Optical Communication, Systems and Networks, Department of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China; chenziyang@pku.edu.cn

* Correspondence: zhangyc@bupt.edu.cn

Received: 19 October 2019; Accepted: 7 November 2019; Published: 11 November 2019

Abstract: A unidimensional continuous-variable quantum key distribution protocol with untrusted detection is proposed, where the two legitimate partners send unidimensional modulated or Gaussian-modulated coherent states to an untrusted third party, i.e., Charlie, to realize the measurement. Compared with the Gaussian-modulated coherent-state protocols, the unidimensional modulated protocols take the advantage of easy modulation, low cost, and only a small number of random numbers required. Security analysis shows that the proposed protocol cannot just defend all detectors side channels, but also achieve great performance under certain conditions. Specifically, three cases are discussed in detail, including using unidimensional modulated coherent states in Alice's side, in Bob's side, and in both sides under realistic conditions, respectively. Under the three conditions, we derive the expressions of the secret key rate and give the optimal gain parameters. It is found that the optimal performance of the protocol is achieved by using unidimensional modulated coherent states in both Alice's and Bob's side. The resulting protocol shows the potential for long-distance secure communication using the unidimensional quantum key distribution protocol with simple modulation method and untrusted detection under realistic conditions.

Keywords: unidimensional modulated coherent states; continuous-variable quantum key distribution; untrusted detection

1. Introduction

Quantum key distribution (QKD) [1–4], as one of the most prominent applications of quantum information science, allows two legitimate partners, i.e., Alice and Bob, to achieve the secure key distribution phase of an encrypted communication. The QKD protocols can be divided into three main categories, which are called discrete-variable (DV) QKD [5,6], continuous-variable (CV) QKD [7,8], and differential-phase-shift (DPR) QKD [9–11], respectively. Both DV and CV systems can be integrated on chip [12–16] and operate at room temperature, but CV systems have significant advantages to achieve higher rate in a short distance link [17]. Thus, the CV-QKD protocols have attracted much attention in the past few years [18–24]. To meet a variety of application needs, much theoretical and experimental research of CV-QKD was done [25–38]. In the research of fully trusted-device protocols, it is always assumed that the devices at two legitimate partners are honest, and Eve can only control the quantum channels rather than the devices at the two parties.

However, the mismatch between practical devices and their idealized models may open security loopholes, resulting in harmful damages to the security of a protocol and the practical systems [39]. To

eliminate all the loopholes of devices, fully device-independent (DI) protocols are proposed [40], which allow Eve to control all experimental devices without any assumptions. Nevertheless, DI protocols need a loophole-free Bell test [41] which is an experimental challenge. To compromise between practical protocols and full DI protocols, semi-device-independent (semi-DI) protocols are proposed, e.g., measurement-device-independent (MDI) [42–44], source-device-independent [45,46], and one-sided device-independent (1sDI) [47,48] QKD protocols, to consider both the security of some devices and the performance of a protocol. In semi-DI protocols, some devices can be assumed to be fully controlled by the adversary while the others should be well characterized. The investigations on the security analysis of semi-DI protocols develop very fast in recent years, such as CV-MDI [49–51], source-device-independent [46] and CV-1sDI protocols [47,52,53], which extend the application of such protocols.

Compared with one-way CV-QKD protocols, the secret key of CV-MDI QKD protocols is established by the measurement results of an untrusted third party, which reduces the performance of the protocols [42]. A lot of efforts were aimed at improving the performance of the protocols, such as using squeezed states [43], and virtual photon subtraction [54,55]. Recently, the unidimensional CV-QKD protocols were proposed in one-way CV-QKD protocols [56,57]. Compared with the Gaussian-modulated protocols, the features of the unidimensional CV-QKD protocols include easy modulation, low cost, and only a small number of random numbers required [56,58]. Moreover, the performance of the unidimensional coherent-state CV-QKD protocol is comparable to the Gaussian-modulated coherent-state protocol under the condition of low excess noise [56,58,59]. Even if the detectors are not ideal, the performance of the protocols can be improved by adding an optical amplifier [60]. Therefore, the unidimensional CV-QKD protocol using coherent states has a certain potential to be applied to various scenarios.

In this paper, we introduce the unidimensional CV-QKD protocol with untrusted detection under realistic conditions in order to eliminate the loopholes described above. We first present the equivalent entanglement-based (EB) scheme and the prepare-and-measure (PM) scheme of the unidimenaional CV-QKD protocol with untrusted detection under realistic conditions, including three different schemes based on using unidimensional modulated coherent states at each side (Alice's side or Bob's side), and both sides (both Alice's and Bob's side). The expressions of the secret key rate of the protocols are derived and the optimal gain parameters of the displacement are calculated, respectively. It is found that the optimal performance, in terms of both key rates and maximal transmission distance, of the protocol is achieved using unidimensional modulated coherent states at both Alice's and Bob's side. In addition, we also consider the asymmetric case that the distance between Bob and Charlie decreases to make the transmission distance further. Thus we investigate the relationship between the distance from Alice or Bob to Charlie by numeral simulation. Furthermore, an extreme situation is taken into account that Charlie is put on Bob's side, and the simulation result indicates that the total transmission distance increases when the distance from Bob to Charlie decreases.

The paper is organized as follows. In Section 2, we give detailed descriptions of the PM and EB schemes of the proposed protocol in three situations. Then we derive the expressions of secret key rate in detail and show the numerical simulation results of the secret key rate. Our conclusions are drawn in Section 3.

Note added. Recently, an independent work [61] was posted on arXiv. This work studied the performance of the measurement-device-independent CV-QKD protocol using unidimensional modulated coherent states in both Alice's and Bob's sides.

2. Results

2.1. Unidimensional CV-QKD Protocol with Untrusted Detection

Firstly, we propose the PM scheme for unidimensional CV-QKD protocol with untrusted detection, as illustrated in Figure 1. In particular, the modulator in the model can be Gaussian modulator as

well as unidimensional modulator. Thus, there are four probable situations in our discussion, among which the situation that Gaussian modulator in both sides was described in detail in references [50,51]. Therefore, the other three probable schemes are taken into consideration in the proposed protocol with unidimensional modulator, which are the unidimensional modulation only in Alice's side, the unidimensional modulation only in Bob's side and the unidimensional modulation both in Alice's and Bob's side, respectively. The PM schemes of the three cases are described separately as follows:

Case 1: unidimensional modulation only in Alice's side

Step 1. Alice produces coherent states and randomly selects the $x-$ or $p-$quadrature along which the prepared states are displaced according to a random Gaussian variable with displacement variance $V_A^M = V_A^2 - 1$. At the same time, Bob randomly prepares coherent states $|x_B + ip_B\rangle$, where x_B and p_B are Gaussian distributed with modulation variance $V_B^M = V_B - 1$. Subsequently, the states are sent to the untrusted party Charlie through two different channels whose length are L_{AC} and L_{BC}, respectively.

Step 2. After receiving the mode A' from Alice and the mode B' from Bob, Charlie combines them with a 50:50 beamsplitter. The output are mode C and D. Subsequently, Charlie performs measurement on the $x-$quadrature of the mode C and the $p-$quadrature of the mode D with two homodyne detectors, and then announces the results X_C and P_D publicly through the classical channels.

Step 3. According to the information Charlie announces, Bob modifies his data as $x'_B = x_B + kX_C$, $p'_B = p_B + kP_D$, where k is the amplification coefficient. Here Alice keeps her data unchanged.

Step 4. Alice and Bob perform post-processing, including information reconciliation, privacy amplification , and so on.

Case 2: unidimensional modulation only in Bob's side

Step 1. Alice randomly prepares coherent states $|x_A + ip_A\rangle$, where x_A and p_A are Gaussian distributed with modulation variance $V_A^M = V_A - 1$. Meanwhile, Bob produces coherent states and randomly selects the $x-$ or $p-quadrature$ along which the prepared states are displaced according to a random Gaussian variable with displacement variance $V_B^M = V_B^2 - 1$. Subsequently, the states are sent to the untrusted party Charlie through two different channels whose length are L_{AC} and L_{BC}, respectively.

The next steps are the same as those in Case 1.

Case 3: unidimensional modulation in both sides

Step 1. Both Alice and Bob produce coherent states and simultaneously select the $x-$ or $p-$quadrature along which the prepared states are displaced according to two random Gaussian variables with displacement variance $V_A^M = V_A^2 - 1$ and $V_B^M = V_B^2 - 1$, respectively. Subsequently, the states are sent to the untrusted party Charlie through two different channels whose length are L_{AC} and L_{BC}, respectively.

The next steps are the same as those in Case 1.

Furthermore, the equivalent EB schemes are described as followed, among which the Case 3 is revealed in Figure 2a:

Case 1: unidimensional modulation only in Alice's side

Step 1. Alice generates Einstein-Podolsky-Rosen (EPR) states with variance V_A. Then she keeps mode A_1 and squeezes the other mode A_2 on a squeezer. The output is mode A_3, which is sent to the untrusted party Charlie through a channel with length L_{AC}. Meanwhile, Bob generates another Einstein-Podolsky-Rosen (EPR) state with variance V_B. Then he keeps mode B_1 and sends the other mode B_2 through a channel with length L_{BC}.

Step 2. Modes A' and B' received by Charlie interfere at a 50:50 beamsplitter with two output modes C and D. Subsequently, Charlie performs measurement on the $x-$quadrature of the mode C and the $p-$quadrature of the mode D with two homodyne detectors, and then announces the results X_C and P_D publicly through the classical channels.

Step 3. According to the information Charlie announces, Bob displaces mode B_1 by operation $\hat{D}(\beta)$, where $\beta = g(X_C + iP_D)$, and g represents the gain of displacement. The relationship between k and g is well studied in reference [42]. Then Bob measures mode B_1' to get the final data X_B,P_B using heterodyne detection. Alice uses mode A_1 to get the final data $X_A(P_A)$ using homodyne detection.

Step 4. Alice and Bob perform post-processing, including information reconciliation, privacy amplification , and so on.

Case 2: unidimensional modulation only in Bob's side

Step 1. Alice generates Einstein-Podolsky-Rosen (EPR) states with variance V_A. Then she keeps mode A_1 and sends the other mode A_2 through a channel with length L_{AC}. Meanwhile, Bob generates another Einstein-Podolsky-Rosen (EPR) state with variance V_B. Then he keeps mode B_1 and squeezes the other mode B_2 on a squeezer. The output is mode B_3, which is sent to the untrusted party Charlie through a channel with length L_{BC}.

Step 2 and *Step 4* are the same as those in Case 1.

Step 3. According to the information Charlie announces, Bob displaces mode B_1 by operation $\hat{D}(\beta)$, where $\beta = g(X_C + iP_D)$. Then Bob measures mode B_1' to get the final data $X_B(P_B)$ using homodyne detection. Alice uses mode A_1 to get the final data X_A, P_A using heterodyne detection.

Case 3: unidimensional modulation in both sides

Step 1. Both Alice and Bob generate Einstein-Podolsky-Rosen (EPR) states with variance V_A and V_B respectively. Alice and Bob keep mode A_1 and mode B_1 of their own EPR state separately. The other two modes, A_2 and B_2, are squeezed on two squeezers, and the output are modes A_3 and B_3. Then the modes A_3 and B_3 are sent to the untrusted party Charlie through two different channels with length L_{AC} and L_{BC}.

Step 2 and *Step 4* are the same as those in Case 1.

Step 3. According to the information Charlie announces, Bob displaces mode B_1 by operation $\hat{D}(\beta)$, where $\beta = g(X_C + iP_D)$. Then Alice measures mode A_1, Bob measures mode B_1' to get the final data $X_A(P_A)$, $X_B(P_B)$ using homodyne detection, respectively.

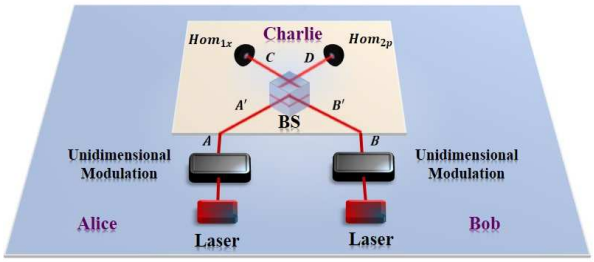

Figure 1. (Color online) The PM scheme of the unidimensional CV-QKD protocol with untrusted detection with the unidimensional modulator in both sides, where both Alice and Bob perform unidimensional modulation. Replacing the unidimensional modulation in Bob's side with the standard Gaussian modulation corresponds to the case of unidimensional modulation only in Alice's side, while replacing the unidimensional modulation in Alice's side with the standard Gaussian modulation corresponds to the case of unidimensional modulation only in Bob's side. In particular, the quantum channels and Charlie are fully controlled by Eve.

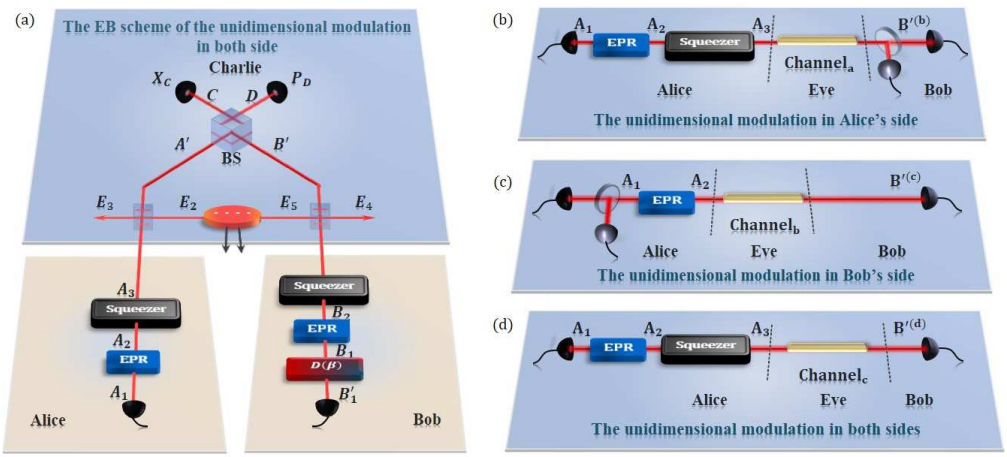

Figure 2. (Color online) The EB scheme and the equivalent one-way model of the unidimensional CV-QKD protocol, where the EPR states are two-mode vacuum states, with untrusted detection and coherent states (**a**) The EB scheme of the unidimentional modulation both in Alice's and Bob's side where the detectors are all homodyne detector. (**b**) The equivalent one-way model of the case that are the unidimentional modulation only in Alice's side. (**c**) The equivalent one-way model of the case that are the unidimentional modulation only in Bob's side. (**d**) The equivalent one-way model of the case that are the unidimentional modulation both in Alice's and Bob's side. In particular, two quantum channels and Charlie are fully controlled by Eve, but Eve has no access to the apparatuses in Alice's and Bob's stations.

2.2. Security Analysis

In this section, the three schemes involved above, which are designed to reduce the cost and simplify the implementation of CV-QKD with untrusted detectors, are discussed separately. In each case, we derive the secure bound of the protocol using the EB scheme owing to ease of calculation in detail. In particular, under the assumptions that Eve controls the channels, Charlie and Bob's EPR state, and the displacement in Figure 2a, their equivalent EB models of one-way CV-QKD model are illustrated in Figure 2b–d.

2.2.1. Using Unidimensional Modulated Coherent States Only in Alice's Side

The EB description of this case is similar to that shown in Figure 1, and the only difference is that there is no squeezer in Bob's side. Thus, the EB scheme discussed here is equivalent to the one-way CV-QKD with unidimentional modulated coherent states and heterodyne detection shown in Figure 2b. The secret key rate K against collective attacks for reverse reconciliation is given by [62]

$$K^{(b)} = \beta I^{(b)}(A:B) - \chi^{(b)}(B:E), \tag{1}$$

where β is the reconciliation efficiency, $I(A:B) = \frac{1}{2} log_2 \left(\frac{V_B^{(b)}+1}{V_{B|A}^{(b)}+1} \right)$ is the classical mutual information between Alice and Bob, $\chi(B:E)$ is the Holevo quantity [63]:

$$\chi^{(b)}(B:E) = S\left(\rho_E^{(b)}\right) - \sum_{x_B} p^{(b)}(x_B)\, S\left(\rho_{E|x_B}^{(b)}\right), \tag{2}$$

where $S(\rho)$ is the von Neumann entropy of the state ρ, x_B is Bob's measurement result obtained with the probability $p^{(b)}(x_B)$, $\rho_{E|x_B}^{(b)}$ is the corresponding state of Eve's ancillary, and $\rho_E^{(b)} = \sum_{x_B} p^{(b)}(x_B)\, \rho_{E|x_B}^{(b)}$ are Eve's partial states.

Since Eve is able to purify the whole system $\rho_{A_1B_1'}^{(b)}$ to maximize the information she can get, we have $S\left(\rho_E^{(b)}\right) = S\left(\rho_{A_1B_1'}^{(b)}\right)$. Furthermore, after Bob's projective measurement resulting in x_B, the system $\rho_{A_1E}^{(b)}$ is pure, so that $S\left(\rho_{E|x_B}^{(b)}\right) = S\left(\rho_{A_1|x_B}^{(b)}\right)$. According to the Gaussian optimality theorem, we assume the final state $\rho_{A_1B_1'}^{(b)}$ shared by Alice and Bob is Gaussian so that the information available to the eavesdropper is maximum [64,65]. Thus, the entropy $S(\rho_{A_1B_1'}^{(b)})$ and $\sum_{x_B} p^{(b)}(x_B)\, S\left(\rho_{A_1|x_B}^{(b)}\right)$ can be calculated directly from the covariance matrices $\gamma_{A_1B_1'}^{(b)}$ and $\gamma_{A_1|x_B}^{(b)}$. In addition, now the expression for $\chi_{BE}^{(b)}$ can be simplified as followed:

$$\chi(B:E) = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right), \tag{3}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, $\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix $\gamma_{A_1B_1'}^{(b)}$ and λ_3 is the symplectic eigenvalue of the covariance matrix $\gamma_{A_1|x_B}^{(b)}$, which can be obtained in terms of the corresponding EB scheme. As is described in the corresponding EB scheme, mode A_3 in Alice's side and B_2 in Bob's side turn into mode A' and B' after the channel, which satisfy the following relationships:

$$\hat{A}_{x,p}^{\prime(b)} = \sqrt{\eta_A}\hat{A}_{3x,p} + \sqrt{1-\eta_A}\hat{E}_{2x,p}, \tag{4}$$

$$\hat{B}_{x,p}^{\prime(b)} = \sqrt{\eta_B}\hat{B}_{2x,p} + \sqrt{1-\eta_B}\hat{E}_{5x,p}, \tag{5}$$

where $\eta_A = 10^{-\alpha L_{AC}/10}$, $\eta_B = 10^{-\alpha L_{BC}/10}$ is the channel parameter transmittance on Alice's and Bob's side, with the loss of channel $\alpha = 0.2$ dB/km, the transmission distance between Alice and Charlie L_{AC}, and the transmission distance between Bob and Charlie L_{BC}.

Then passing through a beamsplitter, mode A' becomes mode C and mode B' becomes mode D, and

$$\hat{C}_{x,p}^{(b)} = \frac{1}{\sqrt{2}}(\hat{A}_{x,p}^{\prime(b)} - \hat{B}_{x,p}^{\prime(b)}), \hat{D}_{x,p}^{(b)} = \frac{1}{\sqrt{2}}(\hat{A}_{x,p}^{\prime(b)} + \hat{B}_{x,p}^{\prime(b)}). \tag{6}$$

After measurement and displacement operation, mode B_1 becomes mode B_1', which is entangled with A_1. In addition, the relationship between mode B_1 and mode B_1' can be written as

$$\hat{B}_{1x}^{\prime(b)} = \hat{B}_{1x} + g\hat{C}_x^{(b)}, \hat{B}_{1p}^{\prime(b)} = \hat{B}_{1p} + g\hat{D}_p^{(b)}, \tag{7}$$

where g represents the gain of the displacement. Thus, the covariances of mode A_1 and mode B_1' in $x-$quadrature and $p-$quadrature can be calculated as

$$\left\langle \hat{A}_{1x}, \hat{B}_{1x}^{\prime(b)} \right\rangle = \sqrt{T^{(b)} V_A \left(V_A^2 - 1\right)}, \tag{8}$$

$$\left\langle \hat{A}_{1p}, \hat{B}_{1p}^{\prime(b)} \right\rangle = -\sqrt{T^{(b)} \left(V_A^2 - 1\right) / V_A}, \tag{9}$$

where $T^{(b)} = \frac{g^{2(b)}}{2}\eta_A$. Furthermore, the variances of mode $B_1^{\prime(b)}$ are calculated by

$$\begin{aligned} V_{B_{1x}^{\prime(b)}} &= V_B + \frac{g^{2(b)}}{2}\eta_A \left(V_A^2 + \chi_A\right) + \frac{g^{2(b)}}{2}\eta_B \left(V_B + \chi_B\right) - g\sqrt{2\eta_B}\sqrt{\left(V_B^2 - 1\right)}, \\ V_{B_{1p}^{\prime(b)}} &= V_B + \frac{g^{2(b)}}{2}\eta_A \left(1 + \chi_A\right) + \frac{g^{2(b)}}{2}\eta_B \left(V_B + \chi_B\right) - g\sqrt{2\eta_B}\sqrt{\left(V_B^2 - 1\right)}. \end{aligned} \tag{10}$$

Then the covariance matrix $\gamma_{A_1B_1'}^{(b)}$ can be written naturally as

$$\gamma_{A_1B_1'}^{(b)} = \begin{bmatrix} V_A & 0 & \sqrt{T^{(b)} V_A \left(V_A^2 - 1\right)} & 0 \\ 0 & V_A & 0 & C_p^{(b)} \\ \sqrt{T^{(b)} V_A \left(V_A^2 - 1\right)} & 0 & T^{(b)}\left(V_A^2 - 1 + \varepsilon'^{(b)}\right) + 1 & 0 \\ 0 & C_p^{(b)} & 0 & 1 + T^{(b)}\varepsilon'^{(b)} \end{bmatrix} = \begin{bmatrix} \gamma_{A_1} & \sigma_{A_1B_1'}^{T(b)} \\ \sigma_{A_1B_1'}^{(b)} & \gamma_{B_1'}^{(b)} \end{bmatrix}, \tag{11}$$

where

$$\varepsilon'^{(b)} = \varepsilon_A + \frac{1}{\eta_A}\left[\eta_B \left(V_B + \varepsilon_B - 1\right) + 2\right] + \frac{V_B - 1 - g\sqrt{2\eta_B}\sqrt{V_B^2 - 1}}{\frac{g^{2(b)}}{2}\eta_A}. \tag{12}$$

The value of $\varepsilon'^{(b)}$ reaches the minimum when $g^{(b)} = \sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B - 1}{V_B + 1}}$, and the minimum $\varepsilon'^{(b)} = \varepsilon_A + \frac{1}{\eta_A}\left[\eta_B \left(\varepsilon_B - 2\right) + 2\right]$. Furthermore, since the $p-$quadrature is not modulated, the correlation $C_p^{(b)}$ is unknown. Yet the matrix is restricted by the constraint following from Heisenberg uncertainly principle:

$$\gamma_{A_1B_1'}^{(b)} + i\Omega \geq 0, \tag{13}$$

where $\Omega = \bigoplus_{k=1}^{N} \omega$ *and* $\omega = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Thus the possible values of $C_p^{(b)}$ is limited, and its value corresponding to the minimum secret key distribution should be concerned so that we can get the lower secure bound.

Next, the symplectic eigenvalues λ_3 is given by the matrix $\gamma_{A_1|x_B}^{(b)}$, which can be calculated by :

$$\gamma_{A_1|x_B}^{(b)} = \gamma_{A_1} - \sigma_{A_1B_1'}^{T(b)}\left(\gamma_{B_1'}^{(b)} + I\right)^{-1}\sigma_{A_1B_1'}^{(b)}, \tag{14}$$

where I is an identity matrix.

2.2.2. Using Unidimensional Modulated Coherent States ONLY in Bob's Side

Similarly, the EB description in this case is similar to that shown in Figure 2a, and the only difference is that there is no squeezer in Alice's side. In addition, the EB scheme discussed here is equivalent to the one-way CV-QKD model with homodyne detection, which is illustrated in Figure 2c. The secret key rate K against collective attacks for reverse reconciliation is also given by (1), where the first part in right side is now $I^{(c)}(A:B) = \frac{1}{2} log_2 \left(\frac{V_A+1}{V_{A|B}^{(c)}+1} \right)$. The second part $\chi^{(c)}(B:E)$ is given by (3), where $\lambda_{1,2}^{(c)}$ are the symplectic eigenvalues of the covariance matrix $\gamma_{A_1B_1'}^{(c)}$ and $\lambda_3^{(c)}$ is the symplectic eigenvalue of the covariance matrix $\gamma_{A_1|x_B}^{(c)}$. The calculations to obtain $\gamma_{A_1B_1'}^{(c)}$ and $\gamma_{A_1|x_B}^{(c)}$ resemble those in Section 2.2.1. Finally, the matrix $\gamma_{A_1B_1'}^{(c)}$ has the following form:

$$\gamma_{A_1B_1'}^{(c)} = \begin{bmatrix} V_A & 0 & \sqrt{T_x^{(c)}(V_A^2-1)} & 0 \\ 0 & V_A & 0 & C_p^{(c)} \\ \sqrt{T_x^{(c)}(V_A^2-1)} & 0 & T_x^{(c)}\left(V_A+\chi_{line_x}^{(c)}\right) & 0 \\ 0 & C_p^{(c)} & 0 & T_p^{(c)}\left(V_A+\chi_{line_p}^{(c)}\right) \end{bmatrix} = \begin{bmatrix} \gamma_{A_1}^{(c)} & \sigma_{A_1B_1'}^{T(c)} \\ \sigma_{A_1B_1'}^{(c)} & \gamma_{B_1'}^{(c)} \end{bmatrix}, \quad (15)$$

where $T_x^{(c)} = g_x^{2(c)}\eta_A/2$ and $T_p^{(c)} = g_p^{2(c)}\eta_A/2$. The factors $\chi_{line_x}^{(c)}$ and $\chi_{line_p}^{(c)}$ can be calculated by:

$$\chi_{line_x}^{(c)} = \frac{1-T_x^{(c)}}{T_x^{(c)}} + \varepsilon_x'^{(c)}, \chi_{line_p}^{(c)} = \frac{1-T_p^{(c)}}{T_p^{(c)}} + \varepsilon_p'^{(c)}, \quad (16)$$

with

$$\begin{aligned} \varepsilon_x'^{(c)} &= \varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(V_B^2+\varepsilon_B-1\right)+2\right] + \frac{V_B-1-g_x^{(c)}\sqrt{2\eta_B}\sqrt{V_B(V_B^2-1)}}{\frac{g_x^{2(c)}}{2}\eta_A}, \\ \varepsilon_p'^{(c)} &= \varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(V_B^2+\varepsilon_B-1\right)+2\right] + \frac{V_B-1-g_p^{(c)}\sqrt{2\eta_B}\sqrt{(V_B^2-1)/V_B}}{\frac{g_p^{2(c)}}{2}\eta_A}. \end{aligned} \quad (17)$$

The value of $\varepsilon_x'^{(c)}$ reaches the minimum when $g_x^{(c)} = \sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B-1}{V_B(V_B+1)}}$, and the minimum $\varepsilon_x'^{(c)} = \varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(\varepsilon_B - V_B - 1\right) + 2\right]$. The value of $\varepsilon_p'^{(b)}$ reaches the minimum when $g_p^{(c)} = \sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B(V_B-1)}{V_B+1}}$, and the minimum $\varepsilon_p'^{(c)} = \varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(\varepsilon_B - \frac{1}{V_B} - 1\right) + 2\right]$.

Also, the matrix $\gamma_{A_1B_1}^{(c)}$, is restricted by constraint following from Heisenberg uncertainly principle:

$$\gamma_{A_1B_1'}^{(c)} + i\Omega \geq 0. \quad (18)$$

Furthermore, the symplectic eigenvalues $\lambda_3^{(c)}$ is given by the matrix $\gamma_{A_1|x_B}^{(c)}$, which can be calculated by :

$$\gamma_{A_1|x_B}^{(c)} = \gamma_{A_1}^{(c)} - \sigma_{A_1B_1'}^{T(c)}\left(X\gamma_{B_1'}^{(c)}X\right)^{-1}\sigma_{A_1B_1'}^{(c)}. \quad (19)$$

2.2.3. Using Unidimensional Modulated Coherent States Both in Alice's and Bob's Side

The EB description in this case is illustrated in Figure 2a, which is equivalent to the one-way CV-QKD model with homodyne detection shown in Figure 2d. Then the secret key rate K against

collective attacks for reverse reconciliation is obtained by (1), with the $I^{(d)}(A:B) = \frac{1}{2}log_2\left(\frac{V_A}{V_{A|B}^{(d)}}\right)$. Furthermore, $\chi^{(d)}(B:E)$ is given identically by (3), and all the parameters in the expression can be obtained from the final matrix $\gamma_{A_1B_1'}^{(d)}$, whose form is as followed:

$$\gamma_{A_1B_1'}^{(d)} = \begin{bmatrix} V_A & 0 & \sqrt{T_x^{(d)}V_A\left(V_A^2-1\right)} & 0 \\ 0 & V_A & 0 & C_p^{(d)} \\ \sqrt{T_x^{(d)}V_A\left(V_A^2-1\right)} & 0 & T_x^{(d)}\left(V_A^2-1+\varepsilon_x'^{(d)}\right)+1 & 0 \\ 0 & C_p^{(d)} & 0 & 1+T_p^{(d)}\varepsilon_p'^{(d)} \end{bmatrix} = \begin{bmatrix} \gamma_{A_1}^{(d)} & \sigma_{A_1B_1'}^{T(d)} \\ \sigma_{A_1B_1'}^{(d)} & \gamma_{B_1'}^{(d)} \end{bmatrix}, \quad (20)$$

where $T_x^{(d)} = g_x^{2(d)}\eta_A/2$, $T_p^{(d)} = g_p^{2(d)}\eta_A/2$, and

$$\begin{aligned} \varepsilon_x'^{(d)} &= \varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(V_B^2+\varepsilon_B-1\right)+2\right] + \frac{V_B-1-g_x^{(d)}\sqrt{2\eta_B}\sqrt{V_B(V_B^2-1)}}{\frac{g_x^{2(d)}}{2}\eta_A}, \\ \varepsilon_p'^{(d)} &= \varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(V_B^2+\varepsilon_B-1\right)+2\right] + \frac{V_B-1-g_p^{(d)}\sqrt{2\eta_B}\sqrt{(V_B^2-1)/V_B}}{\frac{g_p^{2(d)}}{2}\eta_A}. \end{aligned} \quad (21)$$

The values of $\varepsilon_x'^{(d)}$ and $\varepsilon_p'^{(d)}$ reaches the minimum similarly when

$$g_x^{(d)} = \sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B-1}{V_B(V_B+1)}}, g_p^{(d)} = \sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B(V_B-1)}{V_B+1}}, \quad (22)$$

at this time are the minimum

$$\begin{aligned} \varepsilon_x'^{(d)} &= \varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(\varepsilon_B-V_B-1\right)+2\right], \\ \varepsilon_p'^{(d)} &= \varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(\varepsilon_B-\frac{1}{V_B}-1\right)+2\right]. \end{aligned} \quad (23)$$

Furthermore, the matrix $\gamma_{A_1B_1'}^{(d)}$ is restricted by the constraint following from Heisenberg uncertainly principle:

$$\gamma_{A_1B_1'}^{(d)} + i\Omega \geq 0. \quad (24)$$

Finally, the symplectic eigenvalues $\lambda_3^{(d)}$ is given by the matrix $\gamma_{A_1|x_B}^{(d)}$, which can be calculated by :

$$\gamma_{A_1|x_B}^{(d)} = \gamma_{A_1}^{(d)} - \sigma_{A_1B_1'}^{T(d)}\left(X\gamma_{B_1'}^{(d)}X\right)^{-1}\sigma_{A_1B_1'}^{(d)}. \quad (25)$$

2.3. Numeral Simulation

In this section, the performance of the proposed three schemes of the unidimensional CV-QKD protocol with untrusted detection are illustrated and compared. In particular, we first summarize the optimal parameters of the proposed three schemes into a table illustrated in Table 1. Here, the performance of the three cases discussed above is considered to make a contrast.

Table 1. Optimal parameters of the unidimensional CV-QKD protocol with untrusted detection.

	Using Unidimensional Modulated Coherent States Only in Alice's Side	**Using Unidimensional Modulated Coherent States Only in Bob's Side**	**Using Unidimensional Modulated Coherent States Only in Both Sides**
ε'_x	$\varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(\varepsilon_B - 2\right) + 2\right]$	$\varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(\varepsilon_B - V_B - 1\right) + 2\right]$	$\varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(\varepsilon_B - V_B - 1\right) + 2\right]$
ε'_p	$\varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(\varepsilon_B - 2\right) + 2\right]$	$\varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(\varepsilon_B - \frac{1}{V_B} - 1\right) + 2\right]$	$\varepsilon_A + \frac{1}{\eta_A}\left[\eta_B\left(\varepsilon_B - \frac{1}{V_B} - 1\right) + 2\right]$
g_x	$\sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B-1}{V_B+1}}$	$\sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B-1}{V_B(V_B+1)}}$	$\sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B-1}{V_B(V_B+1)}}$
g_p	$\sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B-1}{V_B+1}}$	$\sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B(V_B-1)}{V_B+1}}$	$\sqrt{\frac{2}{\eta_B}}\sqrt{\frac{V_B(V_B-1)}{V_B+1}}$

The parameters that will affect the secret key rate are the reconciliation efficiency β, the variance of Alice and Bob V_A, V_B, the transmission efficiency η_A, η_B, excess noise ε_A, ε_B of two quantum channels. It can be seen in Table 1 that the excess noises ε'_x, ε'_p are related to the variance V_B. When the values of ε'_x, ε'_p are less than zero, the excess noises are physically absent. Therefore, the values of variance V_B, which make the excess noises ε'_x, ε'_p less than zero, are unreasonable. Conversely, when the values of V_B make ε'_x, ε'_p greater than or equal to zero at the same time, they are reasonable. Thus, we make the variance V_B take the values 1.001, 1.1, and 2, and simulate the performances of the excess noise ε'_x, ε'_p. As is shown in Figure 3, when the variance $V_B = 1.001$, the excess noises in $x-$ and $p-$quadrature are both greater than zero, so we choose this value for numerical simulation. In particular, we choose a large variance of $V_A = 10^5$ to see the performance of the ideal modulation, and use practical variance of $V_A = 4$ to observe the realistic performance. Excess noise is set to $\varepsilon_A = \varepsilon_B = \varepsilon = 0.001$ and transmittance are $\eta_A = 10^{-\alpha L_{AC}/10}$, $\eta_B = 10^{-\alpha L_{BC}/10}$ ($\alpha = 0.2$ dB/km) for simulation, which are standard parameters in one-way CV-QKD experiment. Furthermore, the other parameter reconciliation efficiencies in the three cases are set as $\beta = 0.98$ for practical case, and $\beta = 1$ for ideal case.

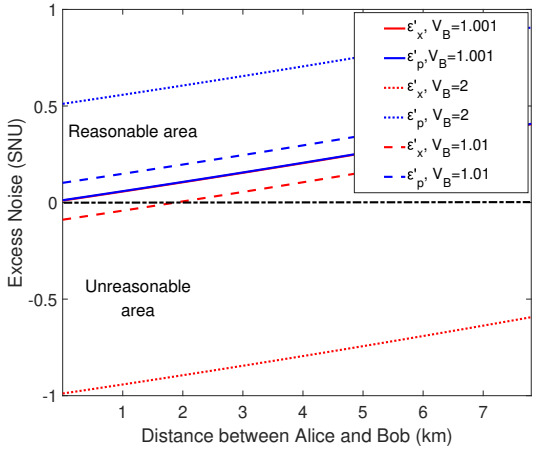

Figure 3. (Color online) Excess noise versus distance with different V_B in the situation that unidimensional modulation is in both sides. The dotted lines are under the condition that $V_B = 2$, the dashed lines represent the condition that $V_B = 1.1$, and the solid lines represent the case that $V_B = 1.001$. ε_A and ε_B is set as $\varepsilon_A = \varepsilon_B = 0.001$. In particular, the region is divided into two parts by a black dotted-dashed line, where upper part is a reasonable region, indicating that the excess noise is greater than zero, and the lower half is an unreasonable area, indicating that the excess noise is less than zero.

Firstly, we consider the performance of the symmetric case where the length of two quantum channels $L_{AC} = L_{BC}$. Then we make a numerical simulation of the secret key rates K in the three cases.

Unfortunately, even the parameters are set to be ideal, the secret key is unable to be distilled in the case that unidimensional modulated coherent states only in Bob's side. The phenomenon may be resulted from the structure of the scheme and the awful effect of the excess noise in the $p-$ quadrature where the states are not modulated. Since MDI-type protocol requires displacement operation in Bob's side, at least 1-unit extra variance will be introduced to the quadrature by Charlie's announced data when displacing a coherent state, we find it rational that no secure key could be extracted in the case that the unidimensional modulation only in Bob's side. Thus, the cases that unidimensional modulated coherent states only in Alice's side as well as in both sides are taken into consideration. The simulation results are shown in Figure 4, from which we make a comparison. We find that the secret key rate of ideal condition is always larger than that of practical condition. Furthermore, it can be directly seen that the case of unidimentional modulation both in two sides corresponds to higher secret key rate and further transmission distance.

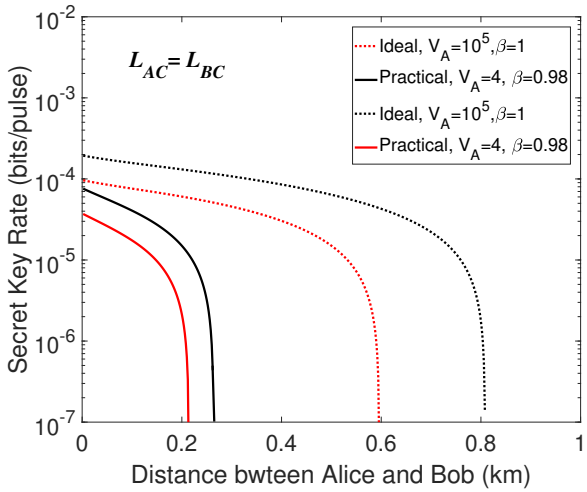

Figure 4. (Color online) Secret key rate in the symmetric case ($L_{AC} = L_{BC}$). the dotted lines are under the ideal condition ($V_A = 10^5$, $\beta = 1$ in the situations of unidimensional modulation only in Alice's side as well as in both sides) and the solid lines represent the practical condition ($V_A = 4$, $\beta = 0.98$ in the situations of unidimensional modulation only in Alice's side as well as in both sides). The red lines represent the case that the unidimentional modulation only exists in Alice's side, the black lines are on behalf of the case that the unidimensional modulation exists in both sides.

Secondly, we can consider the EB schemes of the proposed protocol as a continuous-variable quantum teleportation process, i.e., Alice and Bob prepare EPR states respectively, and then pass the mode from Alice to Bob. Therefore, any loss and noise in the channel from Bob to Charlie with the length L_{BC} will reduce the quality of the EPR source, thus affecting the final performance, as is revealed in Figure 4. In other words, L_{BC} has a much greater impact on the final performance than L_{AC}. In order to eliminate this effect as much as possible and increase the total transmission distance, we try to shorten the distance between Bob and Charlie (L_{BC}). The change of the total transmission distance is displayed by numerical simulation, where the distance between Bob and Charlie L_{BC} is a function of the distance between Alice and Charlie L_{AC}. Specifically, we find the maximum L_{BC}, which makes the secret key rate greater than zero, corresponding to each L_{AC}. The results are displayed in Figure 5, from which we can find that when Charlie's position is close to Bob, the total maximal transmission distance L_{AB} ($L_{AB} = L_{AC} + L_{BC}$) will be relatively longer. Also, L_{AB} improves with large variance $V_A = 10^5$. Furthermore, examining different locations the unidimentional modulation in, we find that the identical result that the transmission distance corresponding to the unidimentional modulation in both sides has a better performance.

Finally, an extreme asymmetric situation is considered when $L_{BC} = 0$. As revealed in Figure 6, the transmission distance between the two legitimate parties L_{AB} increases significantly in a comparison

with the symmetric case. In this case, the secret key rates correlated with the unidimentional modulation in both sides provide a better performance and the performance of the secret key rate in the ideal condition is better than that in the practical condition. Besides, we also plot the curves of standard CV-MDI QKD in Figure 6 for a better understanding of the secret key rate performance of our proposed protocol. As is revealed in Figure 6, the performance of the proposed protocol is comparable to the standard CV-MDI QKD protocol.

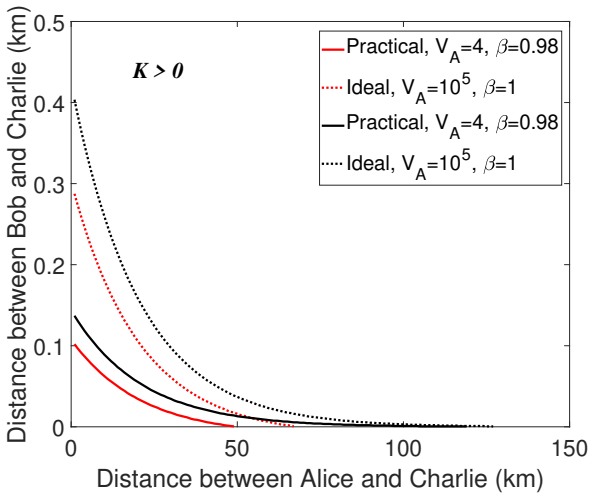

Figure 5. (Color online) Curves of the correlation between L_{AC} and L_{BC}. The transmission distance from Alice and Charlie L_{AC} is considered to be a function of the distance from Bob to Charlie L_{BC}. the dotted lines are under the ideal condition ($V_A = 10^5$, $\beta = 1$ in the situations of unidimensional modulation only in Alice's side as well as in both sides) and the solid lines represent the practical condition ($V_A = 4$, $\beta = 0.98$ in the situations of unidimensional modulation only in Alice's side as well as in both sides). The red lines represent the case that the unidimentional modulation only exists in Alice's side, the black lines are on behalf of the case that the unidimensional modulation exists in both sides of Alice and Bob. The excess noise to be $\varepsilon_A = \varepsilon_B = 0.001$.

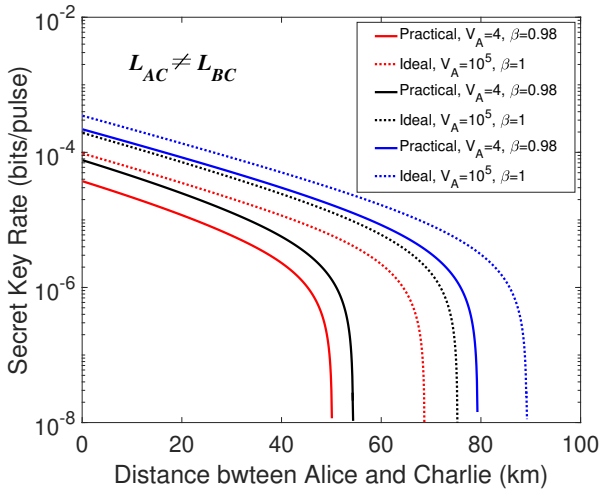

Figure 6. (Color online) Secret key rate versus transmission distance between Alice and Charlie, and the distance L_{BC} is set to $L_{BC} = 0$. Identically, the dotted lines are under the ideal condition, and the solid lines represent the practical condition. The red lines represent the case that the unidimentional modulation only exists in Alice's side, the black lines are on behalf of the case that the unidimensional modulation exists in both sides of Alice and Bob, and the blue lines are the secret key rates of the standard CV-MDI protocols. The parameters are set the same as the symmetric situation.

3. Discussion and Conclusions

In this paper, a unidimensional continuous-variable quantum key distribution protocol with untrusted detection under realistic conditions is proposed. We consider three situations including using unidimensional modulated coherent states at each side or both sides and derive the expressions of the secret key rates against the collective attacks of protocols in each situation, where the third party is untrusted and may be controlled by the eavesdropper. Making use of the expression we make numeral simulations and compare the performances of the cases that the unidimensional modulation exists only in Alice's side as well as in both sides. From the simulation results can we know that the protocol provides a better performance when the unidimensional modulation is used in both sides of the two legitimate partners, and decreasing the distance between Bob and Charlie helps make the total transmission distance further. Indeed, with the appropriate parameters and schemes selected, we could extract the secret key based on the proposed protocol except in the case of unidimensional coherent states only in Bob's side. We provide a possible explanation of the phenomenon, and the reason for more accuracy is still an open question. We would like to model this situation better in the future. Undoubtedly, the proposed protocol provides a simple method to simplify the implementation of the CV-QKD systems, and the security analysis is based on the uncertainty relation. In addition, the scheme has the ability to immune to the collective attacks against standard detectors that are very likely to exist in practical system.

Author Contributions: Conceptualization, L.H. and Z.C.; methodology, Y.Z.; validation, L.H.; formal analysis, L.H.; investigation, L.H., Y.Z., Z.C., and S.Y.; resources, Y.Z. and S.Y.; writing–original draft preparation, L.H.; writing—review and editing, L.H. and Y.Z; visualization, L.H.; funding acquisition, Y.Z. and S.Y.

Funding: This work was supported in part by the Key Program of National Natural Science Foundation of China under Grants 61531003, the National Natural Science Foundation under Grants 61427813, and the Fund of State Key Laboratory of Information Photonics and Optical Communications.

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*. [CrossRef]
2. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
3. Diamanti, E.; Lo, H.-K.; Qi, B.; Yuan, Z. Practical challenges in quantum key distribution. *npj Quantum Inf.* **2016**, *2*, 16025. [CrossRef]
4. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in Quantum Cryptography. *arxiv* **2019**, arxiv:1906.01645.
5. Bennett, C.; Brassard, G. Quantum Cryptography: Public key cryptography and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
6. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
7. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621–669. [CrossRef]
8. Diamanti, E.; Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy* **2015**, *17*, 6072–6092. [CrossRef]
9. Inoue, K.; Waks, E.; Yamamoto, Y. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A* **2003**, *68*, 022317. [CrossRef]
10. Stucki, D.; Brunner, N.; Gisin, N.; Scarani, V.; Zbinden, H.; Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **2005**, *87*, 194108. [CrossRef]
11. Bacco, D.; Christensen, J.B.; Castaneda, M.A.U.; Ding, Y.; Forchhammer, S.; Rottwitt, K.; Oxenløwe, L.K.; Two-dimensional distributed-phase-reference protocol for quantum key distribution. *Sci. Rep.* **2016**, *6*, 36756. [CrossRef] [PubMed]

12. Sibson, P.; Erven, C.; Godfrey, M.; Miki, S.; Yamashita, T.; Fujiwara, M.; Sasaki, M.; Terai, H.; Tanner, M.G.; Natarajan, C.M.; et al. Chip-based quantum key distribution. *Nat. Commun.* **2017**, *8*, 13984. [CrossRef] [PubMed]
13. Ding, Y.; Bacco, D.; Dalgaard, K.; Cai, X.; Zhou, X.; Rottwitt, K.; Oxenløwe, L.K.; High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Inf.* **2017**, *3*, 25. [CrossRef]
14. Agnesi, C.; Da Lio, B.; Cozzolino, D.; Cardi, L.; Ben Bakir, B.; Hassan, K.; Della Frera, A.; Ruggeri, A.; Giudice, A.; Vallone, G.; et al. Hong-Ou-Mandel interference between independent III-V on silicon waveguide integrated lasers. *Opt. Lett.* **2019**, *2*, 271–274. [CrossRef] [PubMed]
15. Bacco, D.; Ding, Y.; Dalgaard, K.; Rottwit, K.; Oxenløwe, L.K.; Space division multiplexing chip-to-chip quantum key distribution. *Sci. Rep.* **2017**, *7*, 12459. [CrossRef] [PubMed]
16. Zhang, G.; Haw, J.Y.; Cai, H.; Xu, F.; Assad, S.M.; Fitzsimons, J.F.; Zhou, X.; Zhang, Y.; Yu, S.; Wu, J.; et al. Integrated chip for continuous-variable quantum key distribution using silicon photonic fabrication. *Nat. Photonics* **2019**, 10.1038/s41566-019-0504-5. [CrossRef]
17. Zhang, Y.; Li, Z.; Chen, Z.; Weedbrook, C.; Zhao, Y.; Wang, X.; Huang, Y.; Xu, C.; Zhang, X.; Wang, Z.; et al. Continuous-variable QKD over 50 km commercial fiber. *Quantum Sci. Technol.* **2019**, *4*, 035006. [CrossRef]
18. 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. [CrossRef]
19. Qi, B.; Lougovski, P.; Pooser, R.; Grice, W.; Bobrek, M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X* **2015**, *5*, 041009. [CrossRef]
20. Soh, D.; Brif, C.; Coles, P.J.; Lütkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar, M. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X* **2015**, *5*, 04101. [CrossRef]
21. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501. [CrossRef] [PubMed]
22. Leverrier, A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Phys. Rev. Lett.* **2017**, *118*, 200501. [CrossRef] [PubMed]
23. Zhang, Y.; Huang, Y.; Chen, Z.; Li, Z.; Yu, S.; Guo, H. One-time shot-noise unit calibration method for continuous-variable quantum key distribution. *arxiv* **2019**, arxiv:1908.06230.
24. Zhou, C.; Wang, X.; Zhang, Y.; Zhang, Z.; Yu, S.; Guo, H. Continuous-variable quantum key distribution with rateless reconciliation protocol. *Phys. Rev. Appl.* **2019**, *12*, 054013. [CrossRef]
25. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef] [PubMed]
26. Grosshans, F.; Wenger, J.; Tualle-Brouri, R.; Grangier, P.; Cerf, N.J. High-rate quantum key distribution using Gaussian-modulated coherent states. *Nature* **2003**, *421*, 8160581 . [CrossRef] [PubMed]
27. Weedbrook, C.; Lance, A.M.; Bowen, W.P.; Symul, T.; Ralph, T.C.; Ping, K.L. Quantum cryptography without switching. *Phys. Rev. Lett.* **2004**, *93*, 170504. [CrossRef] [PubMed]
28. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **2008**, *4*, 726. [CrossRef]
29. García-Patrón, R.; Cerf, N.J.; Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.* **2009**, *102*, 130501.
30. 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. [CrossRef] [PubMed]
31. 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. [CrossRef] [PubMed]
32. Weedbrook, C.; Pirandola, S.; Lloyd, S.; Ralph, T.C.; Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **2010**, *105*, 110501. [CrossRef] [PubMed]
33. 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. [CrossRef]
34. Zhang, Y.; 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 At. Mol. Opt. Phys.* **2014**, *47*, 035501. [CrossRef]

35. Zhang, Y.; Li, Z.; Zhao, Y.; Yu, S.; Guo, H. Numerical simulation of the optimal two-mode attacks for two-way continuous-variable quantum cryptography in reverse reconciliation. *J. Phys. B At. Mol. Opt. Phys.* **2017**, *50*, 035501. [CrossRef]
36. 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. [CrossRef] [PubMed]
37. Weedbrook, C.; Ottaviani, C.; Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **2014**, *89*, 012309. [CrossRef]
38. Chen, Z.; Zhang, Y.; Wang, X.; Yu, S.; Guo, H. Improving parameter estimation of entropic uncertainty relation in continuous-variable quantum key distribution. *Entropy* **2019**, *21*, 652. [CrossRef]
39. Huang, A.; Barz, S.; Andersson, E.; Makarov, V. Implementation vulnerabilities in general quantum cryptography. *New J. Phys.* **2018**, *20*, 103016. [CrossRef]
40. Antonio, A.; Nicolas, B.; Nicolas, G.; Serge, M.; Stefano, P.; Valerio, S. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **2007**, *98*, 230501.
41. Thearle, O.; Janousek, J.; Armstrong, S.; Hosseini, S.; Schünemann (Mraz), M.; Assad, S.; Symul, T.; James, M.R.; Huntington, E.; Ralph, T.C.;et al. Violation of Bell's inequality using continuous variable measurements. *Phys. Rev. Lett.* **2018**, *120*, 040406. [CrossRef] [PubMed]
42. 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. [CrossRef]
43. 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. [CrossRef]
44. 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. Photonics* **2015**, *9*, 397. [CrossRef]
45. Weedbrook, C. Continuous-variable quantum key distribution with entanglement in the middle. *Phys. Rev. A* **2013**, *87*, 022308. [CrossRef]
46. Zhang, Y.; Chen, Z.; Weedbrook, C.; Yu, S.; Guo, H. Continuous-variable source-device-independent quantum key distribution against general attacks. *arxiv* **2018**, arxiv:1811.11973.
47. 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. [CrossRef] [PubMed]
48. Walk, N.; Hosseini, S.; Geng, J.; Thearle, O.; Haw, J.Y.; Armstrong, S.; Assad, S.M.; Janousek, J.; Ralph, T.C.; Symul, T.; et al. Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution. *Optica* **2016**, *3*, 634. [CrossRef]
49. Zhang, X.; Zhang, Y.; Zhao, Y.; Wang, X.; Yu, S.; Guo, H. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A* **2017**, *96*, 042334. [CrossRef]
50. Lupo, C.; Ottaviani, C.; Papanastasiou, P.; Pirandola, S. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. *Phys. Rev. A* **2018**, *97*, 052327. [CrossRef]
51. Chen, Z.; Zhang, Y.; Wang, G.; Li, Z.; Guo, H. Composable security analysis of continuous-variable measurement-device-independent quantum key distribution with squeezed states for coherent attacks. *Phys. Rev. A* **2018**, *98*, 012314. [CrossRef]
52. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.B.; Tomamichel, M.; Werner, R.F. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **2012**, *109*, 100502. [CrossRef] [PubMed]
53. Furrer, F. Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. *Phys. Rev. A* **2014**, *90*, 042325. [CrossRef]
54. Zhao, Y.; Zhang, Y.; Xu, B.; Yu, S.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction. *Phys. Rev. A* **2018**, *97*, 042328. [CrossRef]
55. Ma, H.; Huang, P.; Bai, D.; Wang, S.; Bao, W.; Zeng, G. Continuous-variable measurement-device-independent quantum key distribution with photon subtraction. *Phys. Rev. A* **2018**, *97*, 042329. [CrossRef]
56. Usenko, V.; Grosshans, F. Unidimensional continuous-variable quantum key distribution. *Phys. Rev. A* **2015**, *92*, 062337. [CrossRef]

57. Usenko, V.; Unidimensional continuous-variable quantum key distribution using squeezed states. *Phys. Rev. A* **2018**, *98*, 032321. [CrossRef]
58. Wang, X.; Liu, W.; Wang, P.; Li, Y. Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *95*, 062330. [CrossRef]
59. Wang, P.; Wang, X.; Li, J.; Li, Y. Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions. *Opt. Express* **2017**, *25*, 27995. [CrossRef]
60. Huang, L.; Zhang, Y.; Huang, Y.; Jiang, T.; Yu, S. Improvement of unidimensional continuous-variable quantum key distribution systems by using a phase-sensitive amplifier. *J. Phys. B At. Mol. Opt. Phys.* **2019**, *52*, 225502. [CrossRef]
61. Bai, D.; Huang, P.; Zhu, Y.; Ma, H.; Xiao, T.; Wang, T.; Zeng, G. Unidimensional continuous-variable measurement-device-independent quantum key distribution. *arxiv* **2019**, arxiv:1905.09029.
62. Devetak, I.; Winter, A. Efficient quadrature of highly-oscillatory integrals using derivatives. *Proc. R. Soc. A* **2005**, *461*, 2057.
63. Holevo, A.S. Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel. *Probl. Inf. Transm.* **1973**, *9*, 177.
64. García-Patrón, R.; Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef] [PubMed]
65. Wolf, M.M.; Giedke, G.; Cirac, J.I. Extremality of Gaussian Quantum States. *Phys. Rev. Lett.* **2006**, *96*, 080502. [CrossRef] [PubMed]