Article

Unidimensional Two-Way Continuous-Variable Quantum Key Distribution Using Coherent States

Yiming Bian , Luyu Huang and Yichen Zhang *

State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China; bianyiming@bupt.edu.cn (Y.B.); hly@bupt.edu.cn (L.H.)

* Correspondence: zhangyc@bupt.edu.cn

Abstract: We propose a unidimensional two-way continuous-variable quantum key distribution protocol with coherent states, where the sender modulates a single quadrature of the coherent states rather than both quadratures to simplify the structure of a two-way system. Security analysis is performed with a general attack strategy, known as two-mode attack, which helps to reduce limitations in the analysis. The performance of the protocol under all accessible two-mode attacks at fixed distance is illustrated. Further, two typical two-mode attack strategies are obtained from it, which are one-mode attack strategy and optimal two-mode attack strategy. Between them, the one-mode attack is the simplest form of the two-mode attack, while the optimal two-mode attack is the most complicated one. Simulations show that though the system is simplified, the performance of the two-way protocol with unidimensional modulation is still comparable to that of the counterpart with Gaussian modulation even against the optimal two-mode attack when Eve's ability is maximized. Thus, the proposed protocol simplifies the two-way system while guaranteeing its performance to a certain extent. Especially in a practical system with short transmission distance and high excess noise, the protocol has a good application prospect.

Keywords: continuous-variable quantum key distribution; two-way scheme; unidimensional modulation; general two-mode attacks; optimal attack strategy

Citation: Bian, Y.; Huang, L.; Zhang, Y. Unidimensional Two-Way Continuous-Variable Quantum Key Distribution Using Coherent States. *Entropy* **2021**, *23*, 294. <https://doi.org/10.3390/e23030294>

Received: 16 January 2021
Accepted: 23 February 2021
Published: 27 February 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Quantum key distribution (QKD) [1] is an effective way to ensure communication security and resist the impact of quantum computing on an encryption system [2,3]. Based on the principles of quantum mechanics, a QKD protocol enables two trusted parties, usually called Alice and Bob, to distill secret keys with unconditional security in theory. Over the last three decades, QKD has developed rapidly and spawned two branches, discrete-variable QKD and continuous-variable QKD (CV-QKD) [4,5]. Compared with the discrete-variable QKD, CV-QKD has higher compatibility of standard telecom components [6], which reduces the cost, improves the integration and facilitates the large-scale application of QKD [7–12]. In recent years, CV-QKD has gathered momentum: the transmission distance of CV-QKD has been further extended in commercial fibers [10], low loss optical fibers in laboratory [12], and the theory of CV-QKD has also been widely improved [13–18].

To enhance the tolerable excess noise of the CV-QKD system, the two-way CV-QKD protocol was proposed [19]. In this protocol, Bob sends states to Alice through the forward channel. After which, Alice couples her own states with the received states and then sends them back to Bob through the backward channel. In this way, the information of the secret key is loaded onto the coupled quantum state, and transferred from Alice to Bob. In order to obtain the key information, an eavesdropper, Eve, must eavesdrop on both channels at the same time, which directly increases the eavesdropping difficulty. The structure is more beneficial to Alice and Bob when the channel is too noisy compared to the one-way protocol. Afterwards, an improved two-way CV-QKD protocol has also been proposed to

make the two-way system easier to implement by replacing Alice's displacement operation with a beam splitter [20], which promotes the practical application of two-way protocol, and thus, has been widely studied [21–27]. Although the performance of the two-way protocol is better than that of the one-way protocol, the complexity of the protocol is fairly high: It takes up two quantum channels and requires Gaussian modulation in both x and p quadratures at both Alice's and Bob's side. Therefore, it is necessary to build a simpler and more feasible two-way scheme.

Reducing the number of the modulators by waiving the symmetry of modulation is one of the strategies to simplify the protocol, namely, the unidimensional (UD) modulation [28]. It simplifies the system by abandoning one quadrature of the modulations, and shows a comparable performance to the conventional Gaussian modulated ones under low noise conditions [28]. Until now, the feasibility of using UD modulation has been demonstrated in the squeezed state protocol [29,30] and the measurement-device-independent protocol [31,32]. Simultaneously, the analysis of UD CV-QKD protocol in practical situations has been improved [33], and the methods to enhance the performance of UD protocol have also been proposed [34,35]. In addition, with single amplitude modulator, the UD protocol has been tested experimentally [36]. Considering that, on the one hand, the using of UD modulation is conducive to the simplification of two-way system. On the other hand, the high anti-noise performance of the two-way system contributes to the compensation of the sensitivity to noise caused by UD modulation. A simplified two-way CV-QKD with UD modulation is expected to have good performance.

In this paper, a UD two-way CV-QKD protocol is proposed. UD modulation is used at Alice's side instead of the conventional Gaussian modulation, which enables the two-way system to work with a single quadrature modulation. In this way, the complexity of the protocol and the number of quantum random numbers required are reduced. In this protocol, Bob still uses conventional Gaussian modulation to reduce the complexity of security analysis, and to avoid dramatic degradation of the protocol performance caused by multiple use of unidimensional modulation. For security analysis of a two-way protocol, a general two-mode attack strategy is used: Eve is assumed to have the ability to exploit the correlation between the modes used to attack the forward channel and backward channel. To illustrate the system performance against the general two-mode attack, we derive the expressions of the secret key rate of the protocol against general two-mode attacks and perform simulations of the protocol against all accessible two-mode attacks at fixed distance. Furthermore, two typical two-mode attack strategies, namely, the one-mode attack strategy and the optimal two-mode attack strategy, are obtained from the general two-mode attack, which are the simplest and the most complex cases of the general two-mode attack strategy, respectively. For the one-mode attack, there is no correlation between the two attack modes, while for the optimal two-mode attack, Eve is able to find the optimal attack correlations and minimize the performance of the protocol. Under these two attack strategies, performances of the protocol within secure transmission distances are simulated and compared with that of symmetrical modulated counterparts.

2. The Schemes of Unidimensional Two-Way CV-QKD Protocol

In this part, we first introduce the difference between UD modulation and symmetrical Gaussian modulation with the prepare-and-measure (PM) scheme of the UD two-way CV-QKD protocol. Then the entanglement-based (EB) scheme is illustrated, and the reason of using this modulation strategy is explained.

In terms of the structure of the protocol, as shown in Figure 1, the UD modulation is used at Alice's side and the symmetrical modulation is used at Bob's side. The most different part between the UD protocol and the symmetrical Gaussian modulated protocol is the number of the modulators. The symmetrical Gaussian modulation modulates x quadrature and p quadrature simultaneously, while the UD modulation modulates only one single quadrature (amplitude quadrature x or phase quadrature p). In this way, CV-

QKD can be performed with only one modulator and the complexity of the protocol is reduced. Without loss of generality, the x quadrature is used in the discussion below.

Figure 1. (Color online) (a) The prepare-and-measure (PM) scheme of the unidimensional (UD) two-way protocol. Here, the two quantum channels are fully controlled by Eve while she has no access to the apparatuses in Alice's and Bob's stations. (b) Symmetrical Gaussian modulated coherent state on a phase space. (c) UD modulated coherent state on a phase space, assuming only x quadrature was modulated, which means, the coherent state can only be shifted along x on the phase space. Here, x_A and p_A are two independent identically distributed Gaussian random variables, and the coordinates describe the centers of the shifted coherent states. (BS: beam splitter, AM: amplitude modulator, PM: phase modulator).

The EB scheme of the UD two-way protocol is shown in Figure 2, and can be described as follows:

Step 1. Alice prepares an EPR state with variance V_A . She measures one mode A_1 with homodyne detection and sends the other mode A_2 to a squeezer, which is equivalent to the unidimensional modulation in the PM scheme [35]. At the same time, Bob prepares another EPR state with variance V_B . He keeps one mode B_1 and sends the other mode B_2 to Alice through $Channel_1$ where Eve may perform an attack.

Step 2. Alice couples the received mode A_{in} with her own mode A_3 through a beam splitter, she then sends the coupling mode A_{out} back to Bob through $Channel_2$ while measuring mode A_4 with homodyne detection for parameter estimation.

Step 3. Bob measures the retained mode B_1 with heterodyne detection to get $x_{B_{1x}}$ and $p_{B_{1p}}$, and the received mode B_3 is measured with homodyne detection by him to get x_{B_3} .

Step 4. Bob uses $x_{B_x} = x_{B_3} - k x_{B_{1x}}$ to construct the estimator to Alice's corresponding variable x_A . Here k is the parameter used to optimize Bob's estimator of Alice's corresponding value. Then the postprocessing including reconciliation and privacy amplification is performed.

It is essential to note that although the p quadrature is not modulated, it still needs to be measured sometimes to gather the properties of the channel in the p quadrature in order to ensure the security, and the impact of these measurements on secret key rate is considered negligible [28].

The cost of the simplification by using UD modulation is that the p quadrature is not modulated, which results in the impossibility of estimating the correlation and the channel transmittance in p . Thus, after passing the quantum channel, an unknown parameter Cor_p is introduced into the security analysis to represent the unknown correlation in p quadrature [28], which has a negative impact on the performance of the protocol. In addition to the scheme shown in Figure 1, UD modulation can also be used solely at Bob's side (while Alice still uses symmetrical Gaussian modulation) or both at Alice's and Bob's sides. However, by calculation, these two schemes introduce one or two more unknown parameters into the covariance matrix compared with the scheme shown in Figure 1, mainly because the two-way scheme amplifies the loss of correlation caused by UD modulation in these cases. Considering that more unknown parameters result in more loopholes open to eavesdropper and make numerical simulation in security analysis difficult, in the following security analysis, we focus on the scheme with UD modulation solely used at Alice's side.

Figure 2. (Color online) The entanglement-based (EB) scheme of the UD two-way protocol against two-mode collective attacks, where Eve has full control of the quantum channels while she has no access to the apparatuses in Alice's and Bob's stations. At Alice's side, one mode of the EPR pair is measured by homodyne detection while the other mode is sent to a squeezer, this part is equivalent to the PM scheme of UD modulation with coherent state. The blue beam splitter with a transmittance of T_A is used to couple Alice's state with Bob's state. (QM: quantum memory, B_0 vacuum state).

3. Security Analysis of the Protocol Against Two-Mode Attack

In the security analysis of two-way protocols, one-mode attack strategy is usually used, which assumes that there are no correlations between the two modes of Eve used for attack. However, it has some limitations: It is a special attack structure which can not describe the other attack strategies, and it may not be optimal for the UD two-way protocol. Thus, it is essential to use the general two-mode attack strategies to make a comprehensive analysis. In this section, we first introduce the two-mode attack strategy used by Eve. Then, the process of calculating the secret key rate of the protocol is deduced. To obtain the worst secret key rate and analyze the protocol in the strictest case, we use a double pessimistic worst-case assumption, which is composed of two parts: The first part is used to obtain the optimal attack strategy from the two-mode attack, and the second part is used to get the worst unknown correlation parameters in p quadrature.

3.1. Two-Mode Attack Strategy

The entanglement-based (EB) scheme of two-mode attack strategy is shown in Figure 2. For a two-way system, Eve needs to attack both quantum channels, which makes it more difficult for her to carry out eavesdropping but also enables her to maximize the information eavesdropped by optimizing the correlation of E_1 and E_2 [26,37]. If we simply use a one-mode attack for analysis, the correlation of the two attacking modes cannot be reflected, therefore, a general two-mode attack is used for the following analysis to evaluate the protocol performance comprehensively and to get the optimal attack strategy.

As shown in Figure 2, Eve mixes the modes B_2 and A_{out} with E_1 and E_2 in Channel₁ and Channel₂, through beam splitters with transmissivity T_1 and T_2 . The other modes e , together with E_1 and E_2 , form a whole, and can be globally described by a pure Gaussian state. Afterwards, E'_1 , E'_2 and e are stored in a quantum memory and measured at the end of the protocol. The covariance matrix of E_1 and E_2 has the normal form

$$\gamma_{E_1 E_2} = \begin{pmatrix} V_{E_1} \cdot I_2 & C_{E_1 E_2} \\ C_{E_1 E_2} & V_{E_2} \cdot I_2 \end{pmatrix} \quad (1)$$

where $C_{E_1 E_2} = \begin{pmatrix} C_x & 0 \\ 0 & C_p \end{pmatrix}$ is the correlation parameter matrix between E_1 and E_2 , $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $V_{E_1} = 1 + \frac{T_1 \epsilon}{1 - T_1}$, $V_{E_2} = 1 + \frac{T_2 \epsilon}{1 - T_2}$ are the variances of the thermal noise. Here T_1 and T_2 are given by $T_1 = T_2 = 10^{-\alpha L/10}$, and $\alpha = 0.2 \text{ dB/km}$ is the loss coefficient of the optical fibers. ϵ is the excess noise, for simplicity, we assume that the excess noise of the

two channels are the same. Thus, when ϵ and L are fixed, V_{E_1} and V_{E_2} are also determined accordingly. At this point, Eve's attack strength is totally determined by C_x and C_p .

To explore the performance of the protocol in the worst case, the ability of Eve is maximized: We assume that Eve is able to determine C_x and C_p arbitrarily within the limits of physical existence condition [26,37,38], and she can further find the optimal attack parameters $C_{E_1E_2}^{worst}$ to minimize the performance of the protocol. This is the first part of our double pessimistic worst-case assumption.

The bound of C_x and C_p can be written as

$$\gamma_{E_1E_2} > 0, \quad v_- \geq 1, \quad (2)$$

where v_- is the least symplectic eigenvalue of $\gamma_{E_1E_2}$, written as

$$v_- = \sqrt{0.5(\Delta - \sqrt{\Delta^2 - 4\det(\gamma_{E_1E_2})})}, \quad (3)$$

with

$$\Delta = V_{E_1}^2 + V_{E_2}^2 + 2C_xC_p. \quad (4)$$

From $\gamma_{E_1E_2} > 0$, the following restriction is derived,

$$|C_x| < \sqrt{V_{E_1}V_{E_2}}, \quad |C_p| < \sqrt{V_{E_1}V_{E_2}}. \quad (5)$$

3.2. The Secret Key Rate of the Protocol

In reverse reconciliation, the secret key rate K of the protocol against two-mode Gaussian attacks is given by [39]

$$K = \beta I(A : B) - \chi(B : E), \quad (6)$$

where β is the reconciliation efficiency, $I(A : B)$ is the classical mutual information between Alice and Bob, and $\chi(B : E)$ is the upper bound of the von Neumann entropy between Eve and Bob, called the Holevo bound [40]. $I(A : B)$ and $\chi(B : E)$ can be derived from the covariance matrix $\gamma_{A_1A_4B_1B_3}$ and $\gamma_{A_1A_4B_6B_{1p}}^{B_x}$, which describes the system after the modes go through the channels, and the system after the measurements, respectively. Here, I_{AB} is given by

$$I(A : B) = 0.5 \log_2(V_{A_1}/V_{A_1}^{x_{B_x}}), \quad (7)$$

where $V_{A_1} = \gamma_{A_1A_4B_6B_{1p}}^{B_x}(2, 2)$ and $V_{A_1}^{x_{B_x}} = \gamma_{A_1A_4B_6B_{1p}}^{B_x}(1, 1)$. Assuming that Eve can purify Alice and Bob's system, $\chi(B : E)$ is given by

$$\chi(B : E) = S(\rho_{A_1A_4B_1B_3}) - S(\rho_{A_1A_4B_6B_{1p}}^{x_{B_x}}) = \sum_{i=1}^4 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{j=5}^8 G\left(\frac{\lambda_j - 1}{2}\right), \quad (8)$$

where $\lambda_{1\sim 4}$ and $\lambda_{5\sim 8}$ are the symplectic eigenvalues of the covariance matrix $\gamma_{A_1A_4B_1B_3}$, and $\gamma_{A_1A_4B_6B_{1p}}^{x_{B_x}}$.

The derivation of the above two matrices is as follows. First, the covariance matrix which describes the states A_1 , A_2 , B_1 and B_2 is given by

$$\gamma_{A_1 A_2 B_1 B_2} = \begin{pmatrix} V_A \cdot I_2 & \sqrt{V_A^2 - 1} \cdot \sigma_z & 0 \cdot I_2 & 0 \cdot I_2 \\ \sqrt{V_A^2 - 1} \cdot \sigma_z & V_A \cdot I_2 & 0 \cdot I_2 & 0 \cdot I_2 \\ 0 \cdot I_2 & 0 \cdot I_2 & V_B \cdot I_2 & \sqrt{V_B^2 - 1} \cdot \sigma_z \\ 0 \cdot I_2 & 0 \cdot I_2 & \sqrt{V_B^2 - 1} \cdot \sigma_z & V_B \cdot I_2 \end{pmatrix}, \quad (9)$$

where $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, V_A and V_B are the variances of Alice's EPR state and Bob's EPR state. Then, after A_2 goes through the squeezer, which is equivalent to the UD modulation in PM scheme, the covariance matrix which describes the state A_1, A_3 is given by

$$\gamma_{A_1 A_3} = \begin{pmatrix} V_A & 0 & \sqrt{V_A(V_A^2 - 1)} & 0 \\ 0 & V_A & 0 & -\sqrt{\frac{(V_A^2 - 1)}{V_A}} \\ \sqrt{V_A(V_A^2 - 1)} & 0 & V_A^2 & 0 \\ 0 & -\sqrt{\frac{(V_A^2 - 1)}{V_A}} & 0 & 1 \end{pmatrix}. \quad (10)$$

After transmission through quantum channels, following the channel transmission relationships as below

$$\begin{cases} A_{in} = \sqrt{T_1} B_2 + \sqrt{1 - T_1} E_1, \\ A_4 = \sqrt{T_A} A_3 - \sqrt{1 - T_A} A_{in}, \\ A_{out} = \sqrt{T_A} A_{in} + \sqrt{1 - T_A} A_3, \\ B_3 = \sqrt{T_2} A_{out} + \sqrt{1 - T_2} E_2. \end{cases} \quad (11)$$

The covariance matrix which describes the states A_1, A_4, B_1 and B_3 is given by

$$\gamma_{A_1 A_4 B_1 B_3} = \begin{pmatrix} V_A \cdot I_2 & C_{A_1 A_4} & 0 \cdot I_2 & C_{A_1 B_3} \\ C_{A_1 A_4} & \gamma_{A_4} & C_{A_4 B_1} & C_{A_4 B_3} \\ 0 \cdot I_2 & C_{A_4 B_1} & V_B \cdot I_2 & C_{B_1 B_3} \\ C_{A_1 B_3} & C_{A_4 B_3} & C_{B_1 B_3} & \gamma_{B_3} \end{pmatrix}, \quad (12)$$

where

$$\gamma_{A_4} = \begin{pmatrix} T_A V_A^2 + [V_E (T_1 - 1) - T_1 V_B] (T_A - 1) & 0 \\ 0 & T_A + [V_E (T_1 - 1) - T_1 V_B] (T_A - 1) \end{pmatrix}, \quad (13)$$

and

$$\gamma_{B_3} = \begin{pmatrix} V_{B_{3x}} & 0 \\ 0 & V_{B_{3p}} \end{pmatrix}. \quad (14)$$

Here, $V_{B_{3x}}$ and $V_{B_{3p}}$ are the variances of the x quadrature and p quadrature of B_3 , and have the following form:

$$\begin{aligned} V_{B_{3x}} = & 2 C_x \sqrt{T_2 T_A (T_1 - 1) (T_2 - 1) - V_E (T_2 - 1)} \\ & - T_2 V_A^2 (T_A - 1) - T_2 T_A V_E (T_1 - 1) + T_1 T_2 T_A V_B, \end{aligned} \quad (15)$$

and

$$V_{B_3p} = 2C_p \sqrt{T_2 T_A (T_1 - 1) (T_2 - 1)} - V_E (T_2 - 1) - T_2 (T_A - 1) - T_2 T_A V_E (T_1 - 1) + T_1 T_2 T_A V_B. \quad (16)$$

The correlation between modes A_1 and A_4 is represented by

$$C_{A_1 A_4} = \sqrt{T_A (V_A^2 - 1)} \begin{pmatrix} \sqrt{V_A} & 0 \\ 0 & -\sqrt{1/V_A} \end{pmatrix}, \quad (17)$$

and the correlation between modes A_1 and B_3 is represented by

$$C_{A_1 B_3} = \begin{pmatrix} \sqrt{V_A (V_A^2 - 1) T_2 (1 - T_A)} & 0 \\ 0 & Cor_p \end{pmatrix}. \quad (18)$$

Here, as discussed in Section 2, Cor_p is used to represent the unknown correlation in p quadrature and assumed to be bounded by the physical existence condition, which is given by the Heisenberg uncertainty principle. In the strictest case, to get the worst protocol performance degradation caused by the loss of correlation parameters, the worst correlation parameter Cor_p^{worst} which minimize the secret key rate is used for security analysis [28–36]. In this way, we get the worst key rate under UD modulation, and this is the second part of our double pessimistic worst-case assumption in terms of unknown correlation parameters.

The correlations between modes A_4 and B_1 , and between A_4 and B_3 , are represented by $C_{A_4 B_1}$ and $C_{A_4 B_3}$, written as below:

$$C_{A_4 B_1} = \sqrt{(V_B^2 - 1) (1 - T_A) T_1} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (19)$$

$$C_{A_4 B_3} = \begin{pmatrix} C_{A_4 B_{3x}} & 0 \\ 0 & C_{A_4 B_{3p}} \end{pmatrix}, \quad (20)$$

with

$$C_{A_4 B_{3x}} = \sqrt{T_2 T_A (1 - T_A)} \left[V_A^2 - V_B T_1 - V_E (1 - T_1) - C_x \sqrt{(1 - T_2) (1 - T_1) / (T_2 T_A)} \right], \quad (21)$$

and

$$C_{A_4 B_{3p}} = \sqrt{T_2 T_A (1 - T_A)} \left[1 - V_B T_1 - V_E (1 - T_1) - C_p \sqrt{(1 - T_2) (1 - T_1) / (T_2 T_A)} \right]. \quad (22)$$

$C_{B_1 B_3}$ represents the correlation between modes B_1 and B_3 , and can be written as

$$C_{B_1 B_3} = \sqrt{(V_B^2 - 1) T_1 T_2 T_A} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (23)$$

In the formulas above, T_A is the transmission efficiency of the beam splitter at Alice's side. With heterodyne detection of B_1 at Bob's side, we can get $\gamma_{A_1 A_4 B_3 B_{1x} B_{1p}}$, which is given by

$$\gamma_{A_1 A_4 B_3 B_{1x} B_{1p}} = \gamma_{BS} \cdot (\gamma_{A_1 A_4 B_3 B_1} \oplus I_2) \cdot \gamma_{BS}^T, \quad (24)$$

where $\gamma_{BS} = (I_6 \oplus \gamma_{BS}^0)$, I_6 is an identity matrix of 6×6 , and $\gamma_{BS}^0 = \sqrt{\eta} \begin{pmatrix} I_2 & I_2 \\ -I_2 & I_2 \end{pmatrix}$. For heterodyne detection, $\eta = 0.5$. In the same way as the original two-way system for covariance matrix derivation [20], the construction of the estimator mentioned in Section 2 can be simplified with a Control-Not gate, thus $\gamma_{A_1 A_4 B_{1p} B_6 B_x}$ is given by

$$\gamma_{A_1 A_4 B_{1p} B_6 B_x} = \Gamma^T \cdot \gamma_{A_1 A_4 B_{1p} B_{1x} B_3} \cdot \Gamma, \quad (25)$$

where

$$\Gamma = I_6 \oplus \Gamma_x, \quad (26)$$

and

$$\Gamma_x = \begin{pmatrix} 1 & 0 & -k & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & k & 0 & 1 \end{pmatrix} \quad (27)$$

represents a Control-Not gate, $k = \sqrt{2T_A T_1 T_2 \frac{V_B - 1}{V_B + 1}}$ is used to optimize the performance of system.

Finally we get $\gamma_{A_1 A_4 B_6 B_{1p}}^{x_{B_x}}$, which is given by

$$\gamma_{A_1 A_4 B_6 B_{1p}}^{x_{B_x}} = \gamma_{A_1 A_4 B_6 B_{1p}} - \sigma_{A_1 A_4 B_6 B_{1p} B_x}^T \cdot H_{hom} \cdot \sigma_{A_1 A_4 B_6 B_{1p} B_x}, \quad (28)$$

where $H_{hom} = (X \cdot \gamma_{B_x} \cdot X)^{MP}$, $X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and MP means the Moore–Penrose pseudo-inverse of a matrix. The matrices $\gamma_{A_1 A_4 B_6 B_{1p}}$, $\sigma_{A_1 A_4 B_6 B_{1p} B_x}$, γ_{B_x} are derived from $\gamma_{A_1 A_4 B_6 B_{1p} B_x}$ in the following way:

$$\gamma_{A_1 A_4 B_6 B_{1p} B_x} = \begin{pmatrix} \gamma_{A_1 A_4 B_6 B_{1p}} & \sigma_{A_1 A_4 B_6 B_{1p} B_x}^T \\ \sigma_{A_1 A_4 B_6 B_{1p} B_x} & \gamma_{B_x} \end{pmatrix}. \quad (29)$$

So far, we get the two matrices needed to calculate the secret key rate, and here the secret key rate can be written as a function form as below:

$$K = K(\beta, \epsilon, V_A, V_B, Cor_p, C_x, C_p, T_A, L). \quad (30)$$

From Equation (30), the parameters that determines the secret key rate are shown. Compared with the analysis of the symmetrical modulated two-way protocols [20], three more parameters are introduced, which are Cor_p , C_x and C_p , respectively. Here, different values of Cor_p represent different correlations of A_1 and B_3 in p quadrature, and C_x and C_p represent different two-mode attack strategies. Furthermore, the worst-case secret key rate K_p^{worst} can be obtained by using Cor_p^{worst} and $C_{E_1 E_2}^{worst}$ instead of Cor_p and (C_x, C_p) , where Cor_p^{worst} and $C_{E_1 E_2}^{worst}$ can be obtained by simulations. At this point, the theoretical derivation of security analysis is finished.

4. Simulation and Discussion

In this section, we first show the performance of the UD two-way protocol against all accessible two-mode attacks at fixed distance, which is the basis of the analysis. Then, from the general two-mode attacks, two typical two-mode attack strategies are obtained, which are one-mode attack strategy and the optimal two-mode attack strategy. The simulations

of the protocol against these two attack strategies are performed, which is conducive to the accurate analysis of the protocol performance. For all the simulations, Cor_p^{worst} is used, which can be obtained from the comparison of $K(Cor_p)$, when all the parameters except for Cor_p are fixed and Cor_p traverses within the physical existence constraint. This is a reflection of the pessimistic worst-case assumption of the unknown correlation parameters in the simulations. Ideal cases and practical cases are mainly simulated, with reconciliation efficiency of 1 and 0.956 [41,42], and variance of 1000 and 5, respectively.

As shown in Figure 3, on a C_x, C_p plane, each point represents a two-mode attack strategy of Eve, the region that resembles an olive pit represents the physical existing two-mode attack, which means that Eve can choose these pairs of C_x and C_p for two-mode attack at the fixed parameters of the protocol. When L and ϵ are fixed, as shown in Figure 3a,b, the boundaries of the regions are same, but the distribution of the secret key rate varies with modulation variance and reconciliation efficiency. As the distance increases, as shown in Figure 3a,c, the region will gradually shrink, which means the two-mode attack is limited. What is more, the point $(0, 0)$ on the C_x, C_p plane represents the one-mode attack, which is the simplest case of two-mode attacks.

Figure 3. (Color online) Secret key rate of UD two-way CV-quantum key distribution (QKD) protocol under all accessible two-mode attacks under different situations. (a) At 5 km while $V = 5$, $\beta = 0.956$, $\epsilon = 0.04$. (b) At 5 km while $V = 10^3$, $\beta = 1$, $\epsilon = 0.04$. (c) At 10 km while $V = 5$, $\beta = 0.956$, $\epsilon = 0.04$. (For all simulations $T_A = 0.8$).

Despite the different secret key rate distributions, these two-mode attack simulations still have one thing in common, that is, all of them have a minimum secret key rate center, shown in dark blue in the figure. This confirms that Eve can achieve a set of optimal two-mode attack parameters $C_{E_1 E_2}^{worst}$ to get the most information, which minimizes the performance of the protocol and can be obtained from the comparison of $K(C_x, C_p)$, when all the parameters except for (C_x, C_p) are fixed and (C_x, C_p) traverses within the physical existence constraint. Thus, it requires us to perform two-mode attack at each distance and obtain the optimal attack parameters in security analysis to avoid overestimating the performance of the protocol. In this way, the performance of the protocol under the optimal two-mode attack is obtained and the worst performance of the UD two-way CV-QKD protocol is reflected, which is a representation of the pessimistic worst-case assumption of two-mode attack in the simulations.

Against one-mode attack, the secret key rate and tolerable excess noise of UD two-way CV-QKD protocol is simulated and compared with the conventional symmetrical Gaussian modulated two-way CV-QKD protocol ($Het - Hom_M$) [20] in ideal case and practical case, as shown in Figures 4 and 5. Here, $Het - Hom_M$ represents a two-way protocol with coherent state and homodyne detection at Bob's side. Compared with the conventional two-way protocol, the performance of the UD two-way protocol is reduced to some extent because of the missing of information in p quadrature, which is similar to the performance degradation caused by UD modulation in one-way scheme [28]. In terms of the secret key rate, in the ideal case shown in Figure 4a, the key rate attenuation of the UD two-way protocol is acceptable when the excess noise is low. When $\beta = 1$ and $\epsilon = 0.04$, in the range of 50 km to 150 km, the key rate of UD two-way protocol is approximately 1 to

1.5 orders of magnitude lower than the original protocol. In the practical case shown in Figure 4b, the performance gap is smaller, in the range of 0 km to 10 km, the secret key rate of UD two-way protocol is even higher than that of the original two-way protocol. Here, the outperformance of the UD two-way protocol in the practical case at short distances is mainly due to the fact that the modulation variance V is not optimal for the two protocols under the practical simulation parameters. The optimal modulation variance of the UD two-way protocol is about 10, while it is more than 20 for the original ones. This property limits the performance of the original two-way protocol when the modulation variance is low, and thus, causes the outperformance of the UD two-way protocol. In the aspect of the tolerable excess noise, as shown in Figure 5, the performance of the UD two-way protocol is similar to that of the original two-way protocol in practical, and is acceptable in the ideal conditions especially when the transmission distance is long. At 80 km, in the ideal case, the tolerable excess noise of UD two-way protocol is less than 0.1 lower compared with the original two-way protocol, and the performance gap is further reduced with the increase of distance.

Figure 4. (Color online) Comparisons of secret key rates between UD two-way CV-QKD protocol (solid line) and a sub-protocol ($H_{et} - Hom_M$) of the conventional symmetrical Gaussian modulated two-way CV-QKD protocol family [20] (dashed line), under ideal and practical situations. The attack strategies against both protocols are one-mode attack. (a) Ideal situations where $V = 10^3$, $\beta = 1$, $\epsilon = 0.04$ (red line), 0.045 (blue line) and 0.05 (black line). (b) Practical situations where $V = 5$, $\beta = 0.956$, $\epsilon = 0.04$ (red line), 0.045 (blue line), 0.05 (black line). (For both protocols $T_A = 0.8$).

Figure 5. (Color online) Comparison of tolerable excess noise between UD two-way CV-QKD protocol (solid lines) and the sub-protocol ($H_{et} - Hom_M$) of the conventional symmetrical Gaussian modulated two-way protocol family (dashed lines), the red lines represent the ideal situations and the blue lines represent the practical situations. (The attack strategies against both protocols are one-mode attack, and for both protocols $T_A = 0.8$).

By using the optimal two-mode attack parameters $C_{E_1 E_2}^{worst}$ and the worst correlation parameters Cor_p^{worst} , we get the secret key rate simulation of the UD two-way CV-QKD protocol against the optimal two-mode attack, which is shown in Figure 6. Against the optimal two-mode attack, the performance of the UD two-way CV-QKD protocol is further reduced, however, compared with the performance of the protocol against one-mode attack, the performance loss is not serious when the excess noise is low. Especially under the practical case where $\epsilon = 0.04$, the loss of transmission distance is less than 5 km. This means, though Eve is able to utilize the two-mode correlation between E_1 and E_2 to optimize the attack strategy, the enhancement of the attack strength is limited. These show that the UD two-way protocol has good resistance to two-mode attacks under low noise condition, and its lower performance limit is acceptable. Thus, the lower bound of the UD two-way CV-QKD protocol is obtained.

Figure 6. (Color online) Comparison of secret key rate between UD two-way CV-QKD protocol against the optimal two-mode attack (red line) and the one-mode attack (black line). Here, the solid line represents the practical situation, the dashed line and the dotted line represent the ideal situation. (For both cases $T_A = 0.8$).

5. Conclusions

In this paper, a two-way CV-QKD protocol with UD modulation is proposed, and we focus on the case where UD modulation and symmetrical modulation are used at the sender's (Alice's) side and receiver's (Bob's) side, respectively. The expressions of the secret key rate of the protocol against general two-mode attacks are derived, and the simulations of the protocol against all accessible two-mode attacks are performed. Here, we use a double pessimistic worst-case assumption to analyze the protocol in the strictest case. Through this assumption, the missing correlation parameters and the two-mode attack strength are limited to the worst case, which minimize the protocol performance. Furthermore, one-mode attack strategy and optimal two-mode attack strategy are obtained from the general two-mode attacks, and the lower bound of the protocol performance is shown.

Through simulations, although the performance of UD two-way protocol is partially reduced, which is the price of the protocol simplification, it is still acceptable compared to that of the symmetrical Gaussian modulated counterpart. In practical cases, the performance of the UD two-way CV-QKD protocol is similar to the symmetrical Gaussian modulated counterpart, and at a short transmission distance, the UD two-way protocol even performs better. Therefore, it is reasonable to use unidimensional modulation in a two-way scheme to simplify the system, which expands the application scenario of the two-way CV-QKD system. The future research on the protocol will focus on the other UD modulation strategy of the two-way scheme, such as using UD modulation singly at Bob's side or at both Alice's and Bob's side. Multiple pessimistic worst-case assumptions can be used for security analysis of those cases, and the study of the analytic solution of the

security bound is also helpful to simplify the security analysis of unidimensional two-way CV-QKD protocols.

Author Contributions: Conceptualization, Y.Z. and L.H.; methodology, Y.Z. and L.H.; software, Y.B. and L.H.; validation, Y.B.; formal analysis, Y.B. and L.H.; investigation, Y.B., L.H. and Y.Z.; resources, Y.Z.; data curation, Y.B.; writing—original draft preparation, Y.B.; writing—review and editing, Y.B., L.H. and Y. Z.; visualization, Y.B.; supervision, Y.Z.; project administration, Y.Z.; funding acquisition, Y.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the Key Program of National Natural Science Foundation of China under Grant 61531003, the National Natural Science Foundation under Grant 62001044, and the Fundamental Research Funds for the Central Universities from China.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

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

References

- Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
- 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. *Adv. Opt. Photon.* **2020**, *12*, 1012–1236. [\[CrossRef\]](#)
- Xu, F.; Ma, X.; Zhang, Q.; Lo, H.-K.; Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Diamanti, E.; Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, Security and Implementations. *Entropy* **2015**, *17*, 6072–6092. [\[CrossRef\]](#)
- Guo, H.; Li, Z.; Yu, S.; Zhang, Y. Toward practical quantum key distribution using telecom components. *Fundam. Res.* **2021**, *1*, 96–98. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Kumar, R.; Qin, H.; Alléaume, R. Coexistence of continuous variable QKD with intense DWDM classical channels. *New J. Phys.* **2015**, *17*, 043027. [\[CrossRef\]](#)
- Zhang, G.; Haw, J.Y.; Cai, H.; Xu, F.; Assad, S.; Fitzsimons, J.F.; Zhou, X.; Zhang, Y.; Yu, S.; Wu, J. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nat. Photonics* **2019**, *13*, 839. [\[CrossRef\]](#)
- Zhang, Y.; Li, Z.; Chen, Z.; Weedbrook, C.; Zhao, Y.; Wang, X.; Huang, Y.; Xu, C.; Zhang, X.; Wang, Z. Continuous-variable QKD over 50 km commercial fiber. *Quantum Sci. Technol.* **2019**, *4*, 035006. [\[CrossRef\]](#)
- Eriksson, T.A.; Hirano, T.; Puttnam, B.J.; Rademacher, G.; Luís, R.S.; Fujiwara, M.; Namiki, R.; Awaji, Y.; Takeoka, M.; Wada, N. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels. *Commun. Phys.* **2019**, *2*, 9. [\[CrossRef\]](#)
- Zhang, Y.; Chen, Z.; Pirandola, S.; Wang, X.; Zhou, C.; Chu, B.; Zhao, Y.; Xu, B.; Yu, S.; Guo, H. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **2020**, *125*, 010502. [\[CrossRef\]](#)
- Navascués, M.; Grosshans, F.; Acín, A. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [\[CrossRef\]](#)
- García-Patrón, R.; Cerf, N.J.; Acín, A. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [\[CrossRef\]](#)
- Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501. [\[CrossRef\]](#) [\[PubMed\]](#)
- Leverrier, A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Phys. Rev. Lett.* **2017**, *118*, 200501. [\[CrossRef\]](#) [\[PubMed\]](#)
- Lupo, C.; Ottaviani, C.; Papanastasiou, P.; Pirandola, S. Parameter estimation with almost no public communication for continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2018**, *120*, 220505. [\[CrossRef\]](#)
- Pirandola, S. Satellite quantum communications: Fundamental bounds and practical security. *arXiv* **2020**, arXiv:2012.01725.
- Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **2008**, *4*, 726. [\[CrossRef\]](#)

20. Sun, M.; Peng, X.; Shen, Y.; Guo, H. Security of a new two-way continuous-variable quantum key distribution. *Int. J. Quantum Inf.* **2012**, *10*, 1250059. [[CrossRef](#)]
21. Sun, M.; Peng, X.; Guo, H. An improved two-way continuous-variable quantum key distribution protocol with added noise in homodyne detection. *J. Phys. B At. Mol. Opt. Phys.* **2013**, *46*, 085501. [[CrossRef](#)]
22. Zhang, Y.-C.; Li, Z.; Weedbrook, C.; Yu, S.; Gu, W.; Sun, M.; Peng, X.; Guo, H. Improvement of two-way continuous-variable quantum key distribution using optical amplifiers. *J. Phys. B At. Mol. Opt. Phys.* **2014**, *47*, 035501. [[CrossRef](#)]
23. Weedbrook, C.; Ottaviani, C.; Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **2014**, *89*, 012309. [[CrossRef](#)]
24. Wang, T.; Yu, S.; Zhang, Y.-C.; Gu, W.; Guo, H. Security of two-way continuous-variable quantum key distribution with source noise. *J. Phys. B At. Mol. Opt. Phys.* **2014**, *47*, 215504. [[CrossRef](#)]
25. Ottaviani, C.; Mancini, S.; Pirandola, S. Two-way Gaussian quantum cryptography against coherent attacks in direct reconciliation. *Phys. Rev. A* **2015**, *92*, 062323. [[CrossRef](#)]
26. 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](#)]
27. Zhao, Y.; Zhang, Y.; Li, Z.; Yu, S.; Guo, H. Improvement of two-way continuous-variable quantum key distribution with virtual photon subtraction. *Quantum Inf. Process.* **2017**, *16*, 184. [[CrossRef](#)]
28. Usenko, V.; Grosshans, F. Unidimensional continuous-variable quantum key distribution. *Phys. Rev. A* **2015**, *92*, 062337. [[CrossRef](#)]
29. Usenko, V. Unidimensional continuous-variable quantum key distribution using squeezed states. *Phys. Rev. A* **2018**, *98*, 032321. [[CrossRef](#)]
30. Wang, X.; Cao, Y.; Wang, P.; Li, Y. Advantages of the coherent state compared with squeezed state in unidimensional continuous variable quantum key distribution. *Quantum Inf. Process* **2018**, *17*, 344. [[CrossRef](#)]
31. Huang, L.; Zhang, Y.; Chen, Z.; Yu, S. Unidimensional continuous-variable quantum key distribution with untrusted detection under realistic conditions. *Entropy* **2019**, *21*, 1100. [[CrossRef](#)]
32. Bai, D.; Huang, P.; Zhu, Y.; Ma, H.; Xiao, T.; Wang, T.; Zeng, G. Unidimensional continuous-variable measurement-device-independent quantum key distribution. *Quantum Inf. Process* **2020**, *19*, 53. [[CrossRef](#)]
33. Wang, P.; Wang, X.; Li, J.; Li, Y. Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions. *Optics Express* **2017**, *25*, 27995–28009. [[CrossRef](#)]
34. 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](#)]
35. Wang, P.; Wang, X.; Li, Y. Security analysis of unidimensional continuous-variable quantum key distribution using uncertainty relations. *Entropy* **2018**, *20*, 157. [[CrossRef](#)] [[PubMed](#)]
36. 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](#)]
37. 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*, 397–402. [[CrossRef](#)]
38. Pirandola, S.; Serafini, A.; Lloyd, S. Correlation matrices of two-mode bosonic systems. *Phys. Rev. A* **2009**, *79*, 052327. [[CrossRef](#)]
39. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. Roy. Soc. A* **2005**, *461*, 207–235. [[CrossRef](#)]
40. Holevo, A.S. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Inf. Transm.* **1973**, *9*, 177.
41. Milicevic, M.; Feng, C.; Zhang, L.M.; Gulak, P.G. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. *NPJ Quantum Inf.* **2018**, *4*, 21. [[CrossRef](#)]
42. 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](#)]