Quantum Information Processing (2018) 17:344
https://doi.org/10.1007/s11128-018-2118-0

Advantages of the coherent state compared with squeezed state in unidimensional continuous variable quantum key distribution

Xuyang Wang[1,2] · Yanxia Cao[1] · Pu Wang[1] · Yongmin Li[1,2]

Received: 28 July 2018 / Accepted: 8 November 2018 / Published online: 14 November 2018

Abstract
In this work, a comparison study between unidimensional (UD) coherent-state and UD squeezed-state protocols is performed in the continuous variable quantum key distribution domain. First, a UD squeezed-state protocol is proposed, and the equivalence between the prepare-and-measure and entanglement-based schemes of UD squeezed-state protocol is proved. Then, the security of the UD squeezed-state protocol under collective attack in realistic conditions is analyzed. Finally, the performance of the two UD protocols is compared. Based on the uniform expressions established in our study, the squeezed- and coherent-state protocols can be analyzed simply by varying the squeezing parameter.

Keywords Unidimensional squeezed-state protocol · Unidimensional coherent-state protocol · Continuous variable quantum key distribution

1 Introduction

The unconditional security of quantum key distribution (QKD) prevents information from being eavesdropped; it is expected that this technology will be used for a wide variety of applications in the future with the advent of quantum information technology. In general, QKD technology can be categorized into discrete-variable and continuous-variable (CV) QKD protocols [1, 2]. CV-QKD protocols encode information into continuous quadrature components of quantum states and utilize homodyne detectors

✉ Xuyang Wang
wangxuyang@sxu.edu.cn

✉ Yongmin Li
yongmin@sxu.edu.cn

1 State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China

2 Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China

instead of single-photon detectors. The CV-QKD protocols typically provide a high secret key rate at a relatively short distance; in addition, they have good compatibility with the classical communication networks [3–25].

Based on the utilized quantum states, the CV-QKD protocols can be classified as coherent-state protocols, squeezed-state protocols, and entanglement-state protocols. In general, it is believed that the squeezed-state and entanglement-state protocols perform better than the coherent-state protocols; however, because coherent-state sources are easy to prepare, coherent-state protocols have also been widely researched. To date, many protocols to improve or simplify a QKD system have been proposed, including a unidimensional (UD) coherent-state protocol [26], three-coherent-state protocol [27], and method for passive state preparation [28]. The advantages of the UD coherent-state protocol include easy modulation, low costs, and less random numbers [29, 30]. In the case of a small amount of excess noise, the UD coherent-state protocol performs almost as well as the two-dimensional (TD) coherent-state protocol (GG02). Therefore, the UD coherent-state protocol has the potential to be used for applications in various scenarios, such as in QKD local area networks, where the transmission distance between users is typically short and cost is a key concern.

Thus far, the UD modulation method has only focused on the coherent-state protocol. In this study, a UD squeezed-state protocol was proposed and the equivalence between the prepare-and-measure (PM) scheme and entanglement-based (EB) scheme of the protocol was proved. Using the uniform expression introduced in our study for the squeezed and coherent states, we can analyze and compare the two protocols conveniently.

The remainder of this paper is organized as follows. In Sect. 2, the proposed UD squeezed-state protocol is presented; in addition, the equivalence of PM and EB schemes is discussed. Section 3 presents the security analysis of the UD squeezed-state protocol under collective attack in realistic conditions using the EB scheme. Further, Sect. 4 presents a comparison of the performance between the UD squeezed-state and UD coherent-state protocols. Finally, our conclusions are provided in Sect. 5.

2 UD squeezed and coherent-state protocols

2.1 PM scheme for UD squeezed or coherent-state protocols

It is well known that one of the quadrature variances of squeezed states is lower than the vacuum fluctuation, whereas the other quadrature variance is higher than the vacuum fluctuation. When the amplitude quadrature, which is denoted by x, is squeezed, the covariance matrix is given by

$$\gamma_x = \begin{pmatrix} e^{-2s} & 0 \\ 0 & e^{2s} \end{pmatrix}, \tag{1}$$

where $s > 0$ is the squeezing parameter. When the phase quadrature, which is denoted by y, is squeezed, the covariance matrix is given by

$$\gamma_y = \begin{pmatrix} e^{2s} & 0 \\ 0 & e^{-2s} \end{pmatrix}. \tag{2}$$

The covariance matrix of the coherent state is

$$\gamma_c = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{3}$$

In order to describe the three types of states uniformly in our study, the covariance matrix is described as follows:

$$\gamma = \begin{pmatrix} 1/r & 0 \\ 0 & r \end{pmatrix}, \tag{4}$$

where r represents the variance of the phase quadrature. For $0 < r < 1$, the matrix represents the covariance matrix of the phase quadrature squeezed state or y-squeezed state, whereas when $r > 1$, the matrix represents the covariance matrix of the amplitude quadrature squeezed state or x-squeezed state. Further, when $r = 1$, the matrix is the covariance matrix of the coherent state. It should be noted that all the variances in our study are normalized to the shot noise. Based on this uniform expression, we can analyze these protocols conveniently.

The traditional TD squeezed-state protocol in the PM scheme proposed in [5] is described as follows: Alice randomly prepares x-squeezed states displaced along x- or y-squeezed states displaced along y with a Gaussian distribution. The covariance matrix of the mixed Gaussian state with the null mean value is given by

$$\gamma_{\text{sym}} = \begin{pmatrix} V_M + e^{-2s} & 0 \\ 0 & e^{2s} \end{pmatrix} = \begin{pmatrix} e^{2s} & 0 \\ 0 & V_M + e^{-2s} \end{pmatrix} = \begin{pmatrix} V & 0 \\ 0 & V \end{pmatrix}, \tag{5}$$

where V_M is the modulation variance, and we define $e^{-2s} + V_M = e^{2s} = V$. It is evident that the mixed Gaussian state has a same covariance matrix as the thermal state with variance V, which cannot be discriminated whether it is derived from the mixture of x-squeezed states or mixture of y-squeezed states. In this case, the information can be safely encoded in two conjugate quadratures.

Similar to the UD coherent-state protocol, for the UD squeezed-state protocol in the PM scheme, Alice displaces the squeezed state along one quadrature with a Gaussian distribution. The squeezed state can be either the y-squeezed state as shown in Fig. 1a or x-squeezed state as shown in Fig. 1b. Figure 2c presents the scheme of the UD coherent-state protocol. The modulation variance along the amplitude quadrature is V_M. At Bob's station, he measures the amplitude or phase quadratures by switching the detection bases randomly with true random numbers.

After Bob has measured a series of signal pulses, the two partners perform the sifting and post-processing steps, which are described as follows:

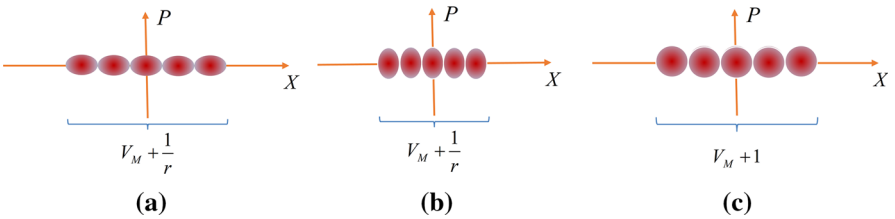

Fig. 1 UD distributed squeezed states in the phase space. **a** Phase quadrature squeezed state. **b** Amplitude quadrature squeezed state. **c** Coherent state

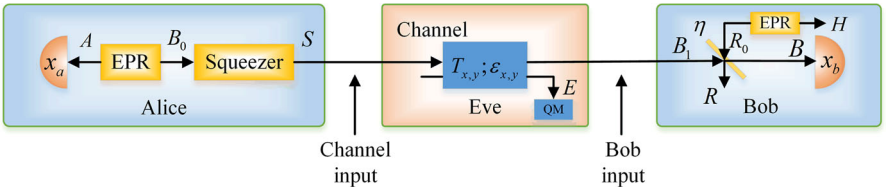

Fig. 2 Schematic of the EB scheme of the UD protocol under realistic conditions

1. Bob discloses the random measurement base of each pulse, and Alice records the data corresponding to the cases wherein Bob measures the amplitude quadrature.
2. Bob declares publicly part of his data to estimate the channel parameters of the amplitude quadrature, i.e., the transmission efficiency and excess noise.
3. Using the channel parameters of the amplitude quadrature and the variance of the phase quadrature, the secret key rate is estimated.
4. Alice and Bob perform data reconciliation and privacy amplification to extract secret keys from raw keys.

2.2 Equivalence of the PM and EB schemes in UD protocols

Most of the current experimental systems for CV-QKD protocols are based on PM schemes because they are easy to implement in practice. However, in theory, it is difficult to analyze the security of such protocols based on the PM schemes. On the contrary, theoretical analysis based on the EB scheme can be performed appropriately; the involved entangled states lead to simple and feasible calculations [2]. In particular, in the case of the UD protocol, security analysis based on the EB scheme has more advantages than that based on the PM scheme. The covariance matrices obtained using the EB schemes contain the constraints of phase quadrature; however, these constraints are difficult to obtain using the PM scheme.

In the EB scheme shown in Fig. 2, Alice prepares an Einstein–Podolsky–Rosen (EPR) state ρ_{AB_0} with covariance matrix γ_{AB_0} as follows:

$$\gamma_{AB_0} = \begin{pmatrix} V \cdot I_2 & \sqrt{V^2-1} \cdot \sigma_z \\ \sqrt{V^2-1} \cdot \sigma_z & V \cdot I_2 \end{pmatrix}, \tag{6}$$

where $I_2 = \mathrm{diag}(1, 1)$ and $\sigma_z = \mathrm{diag}(1, -1)$. Then, Alice squeezes one of its modes B_0 with the squeezing parameter $S = \ln\sqrt{V/r}$. The resulting covariance matrix γ_{AS} is

$$\begin{aligned}\gamma_{AS} &= (I_2 \oplus SQ)\gamma_{AB_0}(I_2 \oplus SQ)^T \\ &= \begin{bmatrix} V & 0 & \sqrt{V(V^2-1)/r} & 0 \\ 0 & V & 0 & -\sqrt{r(V^2-1)/V} \\ \sqrt{V(V^2-1)/r} & 0 & V^2/r & 0 \\ 0 & -\sqrt{r(V^2-1)/V} & 0 & r \end{bmatrix} \\ &= \begin{bmatrix} \gamma_A & \sigma_{AS} \\ \sigma_{AS}^T & \gamma_S \end{bmatrix}, \end{aligned} \tag{7}$$

where SQ is the squeezing operator, which is given by

$$SQ = \begin{bmatrix} \sqrt{V/r} & 0 \\ 0 & 1/\sqrt{V/r} \end{bmatrix}. \tag{8}$$

Here, γ_A and γ_S are the covariance matrices of the modes A and S, respectively, and σ_{AS} is the correlation matrix of the two modes.

The state ρ_s that Alice sending to Bob depends on the measurement of mode A. When the modulation is performed on the amplitude quadrature of the state in the PM scheme, Alice will conduct homodyne detection on the amplitude quadrature of the EPR state in the equivalent EB scheme. The covariance matrix of mode S conditioned on Alice's measurement result x_A can be derived using

$$\gamma_S^{x_A} = \gamma_S - \sigma_{AS}(X \cdot \gamma_A \cdot X)^{MP}\sigma_{AS}^T, \tag{9}$$

where $X = \mathrm{diag}(1, 0)$, and MP denotes the Moore–Penrose inverse of a matrix. After a straightforward calculation, we can obtain the result

$$\gamma_S^{x_A} = \begin{pmatrix} 1/r & 0 \\ 0 & r \end{pmatrix}. \tag{10}$$

Before Alice's measurement, the two modes of state ρ_{AS} are centered on $d_A^{\mathrm{in}} = (0, 0)$ and $d_S^{\mathrm{in}} = (0, 0)$. The homodyne detection on mode A, denoted by $m = (x_A, 0)$, projects the mode S to the squeezed or coherent state centered on

$$d_S^{\mathrm{out}} = \sigma_{AS}(X \cdot \gamma_A \cdot X)^{MP}\left(m - d_A^{\mathrm{in}}\right) + d_S^{\mathrm{in}}, \tag{11}$$

which can be simplified to

$$d_S^{\mathrm{out}} = \sqrt{\left(V^2 - 1\right)/rV} \cdot (x_A, 0). \tag{12}$$

From the covariance matrix γ_A of mode A, we can observe that the variance of x_A is V. Therefore, the variance of the center value of mode S is

$$\mathrm{Var}\left(d_S^{\mathrm{out}}\right) = \frac{V^2-1}{rV} \cdot \mathrm{Var}(x_A) = \frac{V^2}{r} - \frac{1}{r}. \tag{13}$$

The variance of the amplitude quadrature for mode S conditioned on Alice's measurement result x_A, $1/r$, plus the variance of the center value will give rise to the total variance V^2/r. These correspond to the variance of the initial state $1/r$, and the modulation variance $V_M = \left(V^2-1\right)/r$ in the PM scheme, respectively. Therefore, the two schemes are indistinguishable for Bob and Eve, i.e., they are equivalent.

3 Security analysis of the UD coherent- and squeezed-state protocols under realistic conditions

In this section, we present the security analysis of the UD coherent and squeezed-state protocols with direct reconciliation (DR) and reverse reconciliation (RR).

3.1 Security analysis of the UD protocols in the RR condition

The asymptotic secret key rate against collective attacks in the RR condition can be calculated as follows:

$$\Delta I = \beta \cdot I_{AB} - \chi_{BE}, \tag{14}$$

where β is the reconciliation efficiency; thus far, the highest value achieved is 99.96% [31]. I_{AB} is the Shannon mutual information between Alice and Bob. χ_{BE} is the Holevo bound, which represents the maximum information eavesdropped by Eve under collective attacks.

I_{AB} can be calculated using Shannon's equation as follows:

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|B}}, \tag{15}$$

where V_A is the variance of the amplitude quadrature of Alice's state, which can be found at the first diagonal element of covariance matrix γ_{AB_1}

$$\gamma_{AB_1} = \begin{bmatrix} \sqrt{1+rV_M} & 0 & \sqrt{T_x V_M}(1+rV_M)^{1/4} & 0 \\ 0 & \sqrt{1+rV_M} & 0 & C_y^{B_1} \\ \sqrt{T_x V_M}(1+rV_M)^{1/4} & 0 & T_x\left(V_M + 1/r + \chi_{\mathrm{linex}}\right) & 0 \\ 0 & C_y^{B_1} & 0 & V_y^{B_1} \end{bmatrix}. \tag{16}$$

Here, $\chi_{\mathrm{linex}} = (1-T_x)/T_x + \varepsilon_x$ is the channel noise in amplitude quadrature added relative to the channel input, $(1-T_x)/T_x$ is the noise due to channel losses, and ε_x is the excess noise in the amplitude quadrature. $C_y^{B_1}$ is the unknown correlation of phase

quadratures, and $V_y^{B_1}$, which could be measured experimentally, is the variance of the phase quadrature. The conditional variance $V_{A|B}$ is the first diagonal element of the conditional matrix $\gamma_{A|B}$, which can be derived as follows:

$$\gamma_{A|B} = \gamma_A - \sigma_{AB}(X\gamma_B X)^{MP}\sigma_{AB}^T, \tag{17}$$

where $X = \mathrm{diag}(1, 0)$. γ_A, γ_B, and σ_{AB} are submatrices of the covariance matrix γ_{AB}

$$\gamma_{AB} = \begin{bmatrix} \sqrt{1+rV_M} & 0 & \sqrt{\eta T_x V_M}(1+rV_M)^{1/4} & 0 \\ 0 & \sqrt{1+rV_M} & 0 & C_y^{B_1}\sqrt{\eta} \\ \sqrt{\eta T_x V_M}(1+rV_M)^{1/4} & 0 & \eta T_x\left(V_M + 1/r + \chi_{\mathrm{tot}x}\right) & 0 \\ 0 & C_y^{B_1}\sqrt{\eta} & 0 & \eta\left(V_y^{B_1} + \chi_{\mathrm{hom}}\right) \end{bmatrix} = \begin{bmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB}^T & \gamma_B \end{bmatrix}. \tag{18}$$

Here, $\chi_{\mathrm{hom}} = (1+v_{\mathrm{el}})/\eta - 1$ is the noise introduced by the realistic homodyne detector relative to Bob's input in the amplitude quadrature, and $\chi_{\mathrm{tot}x} = \chi_{\mathrm{linex}} + \chi_{\mathrm{hom}}/T_x$ is the total noise added between Alice and Bob relative to the channel input in the amplitude quadrature. v_{el} is the electronic noise of the homodyne detector. Finally, the Shannon mutual information can be derived as follows:

$$I_{AB} = \frac{1}{2}\log_2\left(\frac{1/r + V_M + \chi_{\mathrm{tot}}}{1/r + \chi_{\mathrm{tot}}}\right). \tag{19}$$

To obtain the covariance matrix γ_{AB_1}, it is convenient to assume that Eve holds a purification of state ρ_{AB_1}. Considering the freedom-in-purification theorem, any purification of ρ_{AB_1} that Eve may possess will result in the same entropy and hence the same Holevo information χ_{BE} [32]. Here, we suppose that Eve generates an EPR state $\rho_{EE'}$ with covariance matrix $\gamma_{EE'}$ and replaces the channel with a lossless channel in which she inserts a beam splitter with phase-sensitive transmission T_x and T_y (as shown in Fig. 3). The beam splitter mixes the modes S and $E^{'}$. Then, Eve retains one of the output modes F for herself and passes the other mode B_1 to Bob. This process can be expressed as follows:

$$\gamma_{AB_1FE} = (I_2 \oplus BS_{SE'} \oplus I_2)\cdot\left(\gamma_{AS} \oplus \gamma_{E'E}\right)\cdot(I_2 \oplus BS_{SE'} \oplus I_2)^T. \tag{20}$$

The covariance matrix γ_{ABRH} can be obtained using a similar procedure as shown below:

$$\gamma_{ABRH} = \left(I_2 \oplus BS_{B_1R_0} \oplus I_2\right)\cdot\left(\gamma_{AB_1} \oplus \gamma_{R_0H}\right)\cdot\left(I_2 \oplus BS_{B_1R_0} \oplus I_2\right)^T. \tag{21}$$

In order to analyze the security of the protocol easily, the realistic homodyne detector is generally modeled by a beam splitter $BS_{B_1R_0}$ with a transmission efficiency η and ideal homodyne detector (as shown in Fig. 2). The electronic noise v_{el} of the homodyne detector can be modeled by model R_0 of the ERP state ρ_{R_0H} with variance

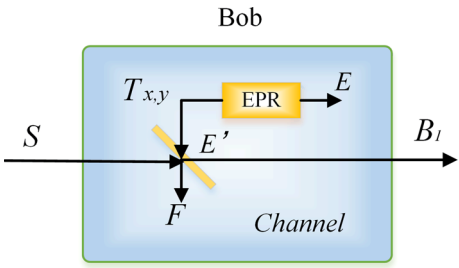

Fig. 3 Beam splitter mode of the channel

$V_N = 1 + v_{\text{el}}/(1-\eta)$ entering the other input port of the beam splitter. Because the detector cannot be accessed by the eavesdropper, it is considered that the detector has phase-insensitive efficiency.

The Holevo bound that represents the maximum information eavesdropped by Eve in the RR condition is defined as

$$\chi_{BE} = S(\rho_{FE}) - S\left(\rho_{FE}^{x_b}\right). \tag{22}$$

Because the quantum states ρ_{AB_1FE} and $\rho_{ARHFE}^{x_b}$ are all pure states, we have $S(\rho_{AB_1}) = S(\rho_{FE})$ and $S(\rho_{EF}^{x_b}) = S(\rho_{ARH}^{x_b})$. χ_{BE} can be rewritten as

$$\chi_{BE} = S(\rho_{AB_1}) - S\left(\rho_{ARH}^{x_b}\right), \tag{23}$$

where $S(\rho)$ is the von Neumann entropy of the quantum state ρ. For an n-mode Gaussian state ρ, this entropy can be calculated using the symplectic eigenvalues of the covariance matrix γ characterizing ρ as follows:

$$S(\rho) = \sum_i G\left(\frac{\lambda_i - 1}{2}\right), \tag{24}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. In general, the symplectic eigenvalues of covariance matrix γ with n mode can be obtained by finding the absolute eigenvalues of the matrix $i\Omega\gamma$, where the matrix Ω is given by

$$\Omega = \bigoplus_{k=1}^{n} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{25}$$

The covariance matrix $\gamma_{ARH}^{x_b}$ of the state $\rho_{ARH}^{x_b}$ can be derived using

$$\gamma_{ARH}^{x_b} = \gamma_{ARH} - \sigma_{ARH;B}(X\gamma_B X)^{MP}\sigma_{ARH;B}^T, \tag{26}$$

where γ_{ARH}, γ_B, and $\sigma_{ARH;B}^T$ are submatrices of the matrix γ_{ARHB} as shown below:

$$\gamma_{ARHB} = \begin{bmatrix} \gamma_{ARH} & \sigma_{ARH;B} \\ \sigma_{ARH;B}^T & \gamma_B \end{bmatrix}. \tag{27}$$

The covariance matrix γ_{ARHB} is obtained by rearranging the lines and columns of the matrix γ_{ABRH}. In the above expression (23), there are two unknown variables $C_y^{B_1}$ and $V_y^{B_1}$. To find the secret key rate, we need to constraint them using the Heisenberg uncertainty principle [33]:

$$\gamma_{AB_1} + i\Omega \geq 0. \tag{28}$$

Then, the following parabolic equation can be derived:

$$\left(C_y^{B_1} - C_0\right)^2 \leq \frac{V^2-1}{V} \frac{\chi_{\text{linex}}}{1/r + \chi_{\text{linex}}} \left(V_y^{B_1} - V_0\right), \tag{29}$$

where

$$C_0 = -\frac{\sqrt{(V^2-1)/r}}{\sqrt{T_x V}\left(1/r + \chi_{\text{linex}}\right)} \quad \text{and} \quad V_0 = \frac{1}{T_x\left(1/r + \chi_{\text{linex}}\right)}. \tag{30}$$

Figure 4 shows a black parabolic curve between $C_y^{B_1}$ and $V_y^{B_1}$. The parameter r is set to 1.1, which indicates that 1-dB x-squeezed states are generated. The other parameters are set as $\beta = 0.99$, $V_M = 3$, $T_x = 0.1$, $\varepsilon_x = 0.01$, $\eta = 0.6$, and $\upsilon_{\text{el}} = 0.1$. The entire plane is divided into physical and unphysical regions by the parabolic curve. In particular, the physical region is contained in the parabolic curve. In the unphysical region, the values of $C_y^{B_1}$ and $V_y^{B_1}$ cannot be satisfied simultaneously. The cyan curve with the secret key rate of zero separates the entire physical region into secure and unsecure regions. The secret key rate in the secure region is larger than zero, whereas it is less than zero in the unsecured region. For a fixed value $V_y^{B_1}$, there is a group of secret key rates with different values of $C_y^{B_1}$. To find the minimum secret key rate $\Delta I_{\min}$, $C_y^{B_1}$ is scanned in the secure region to find the specific correlation of phase quadratures $C_{y\min}^{B_1}$. It is evident that different values of $V_y^{B_1}$ result in different $C_{y\min}^{B_1}$. The red and green lines in Fig. 4 record the trajectory of $C_{y\min}^{B_1}$ in the secure region, where the red line indicates that the points with minimum secret key rate lie on the parabolic curve. When the value of $V_y^{B_1}$ increases, the points with the minimum secret key rate gradually separate from the parabolic curve, which is denoted by the green line. The minimum secret key rate as a function of $V_y^{B_1}$ is shown in Fig. 5.

When the transmission efficiency T_y and the excess noise ε_y in the phase quadrature equal the transmission efficiency T_x and the excess noise ε_x in the amplitude quadrature, the variance of the phase quadrature $V_y^{B_1}$ can be derived as follows:

$$V_y^{B_1}\big|_{T_x=T_y} = T_x(r + \chi_{\text{linex}}). \tag{31}$$

It is depicted as the black virtual line in Figs. 4 and 5. The minimum secret key rate for the phase quadrature variance $V_y^{B_1}\big|_{T_x=T_y}$ is used to estimate the secret key rate for a typical quantum channel using a single-mode fiber.

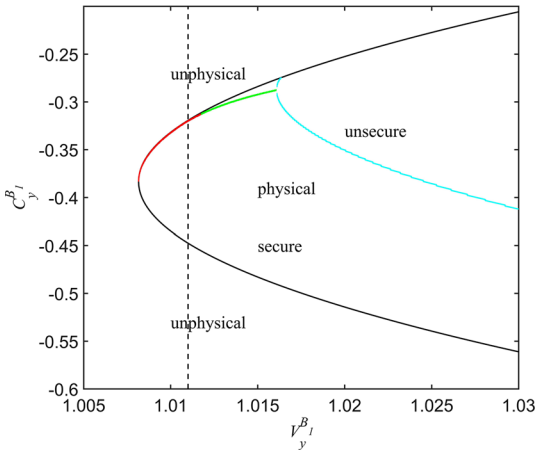

Fig. 4 Regions of the UD 1-dB x-squeezed-state protocol under realistic detection conditions

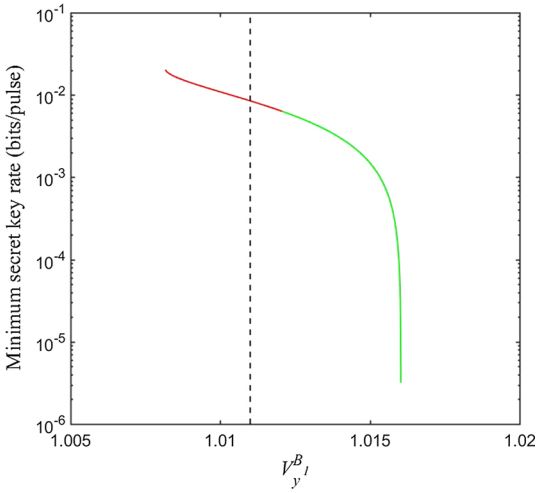

Fig. 5 The minimum secret key rate versus the $V_y^{B_1}$

3.2 Security analysis of the UD protocols in the DR condition

The minimum secret key rate $\Delta I_{\min}$ in the DR condition can be calculated using the following equations:

$$\begin{cases} \Delta I = \beta \cdot I_{AB} - \chi_{AE} \\ \gamma_{AB_1} + i\Omega \geq 0 \end{cases}. \tag{32}$$

Here, the mutual information I_{AB} and the covariance matrix γ_{AB_1} are the same as those in the RR condition. The information eavesdropped by Eve in the DR condition is denoted by Holevo bound χ_{AE}, which can be calculated by

$$\chi_{AE} = S(\rho_{EF}) - S\left(\rho_{EF}^{x_a}\right). \tag{33}$$

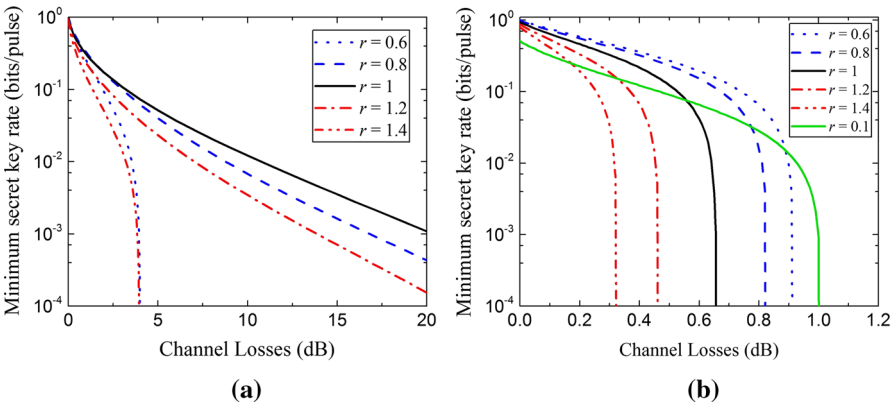

Fig. 6 Minimum secret key rate versus channel losses at different squeezing parameters. **a** RR condition. **b** DR condition. The other parameters are set to $\beta = 0.99$, $\varepsilon_x = 0.01$, $\eta = 0.6$, $v_{\text{el}} = 0.1$, and the modulation variances are optimized

Because the states ρ_{AB_1EF} and $\rho^{x_a}_{BRHFE}$ are pure states, we can rewrite χ_{AE} as

$$\chi_{AE} = S(\rho_{AB_1}) - S(\rho^{x_a}_{BRH}). \tag{34}$$

Notably, state $\rho^{x_a}_{B_1EF}$ is also a pure state; thus, $S\left(\rho^{x_a}_{EF}\right) = S\left(\rho^{x_a}_{B_1}\right)$. Therefore, Eq. (34) can be simplified to

$$\chi_{AE} = S(\rho_{AB_1}) - S(\rho^{x_a}_{B_1}). \tag{35}$$

The remaining calculations and analysis are similar to the procedures in the RR condition. We directly present the comparison results of the UD protocols in the RR and DR conditions in the next section.

4 Performance comparison of the UD coherent- and squeezed-state protocols

The secret key rate $\Delta I_{\min}$ versus distance for different squeezing parameters is plotted in Fig. 6 in which (a) and (b) present the cases in the RR and DR conditions, respectively. The black solid line represents the squeezed parameter $r = 1$ (coherent state). The blue dash and blue dot lines represent the phase quadrature squeezed states with squeezing parameters of $r = 0.8$ and $r = 0.6$, respectively. The squeezed parameters of the red dash-dot and red dash-dot-dot lines are $r = 1.2$ and $r = 1.4$, respectively, both of which represent the amplitude quadrature squeezed state.

In the RR condition, we observe that neither the amplitude quadrature nor the phase quadrature squeezed state performs better than the coherent state when the channel

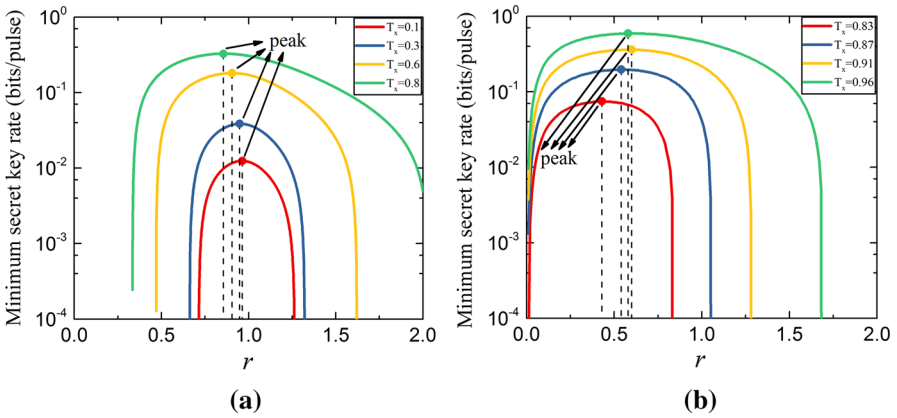

Fig. 7 Minimum secret key rate versus parameter r at different transmission efficiencies in RR and DR conditions. The parameters are set to $\beta = 0.99$, $\varepsilon_x = 0.01$, $\eta = 0.6$, and $v_{\mathrm{el}} = 0.1$. The modulation variances at different transmission efficiencies are optimized. **a** RR condition. The red, blue, yellow, green lines correspond to the transmission efficiencies $T_x = 0.1$ (50 km), 0.6 (10 km), 0.3 (26 km), and 0.8 (5 km), respectively. **b** DR condition. The red, blue, yellow, green lines correspond to the transmission efficiencies $T_x = 0.83$ (4 km), 0.87 (3 km), 0.91 (2 km) and 0.96 (1 km), respectively (Color fiure online)

loss is higher than 2 dB. In general, the larger the degree of squeezing, the lower the performance. This phenomenon is different from the TD protocols in which the squeezed-state protocol performs better than the coherent-state protocol [2, 34]. In the DR condition, it is clear that the amplitude squeezed state still has a lower performance than the coherent state. Different from the RR condition, the phase quadrature squeezed state presents a better performance than the coherent state. However, strong squeezing is not necessarily beneficial to the system, as shown by the green line in Fig. 6b.

In order to investigate the performance of the UD protocol in detail, the minimum secret key rate ΔI_{min} versus parameter r at different transmission efficiencies is plotted in Fig. 7. Four curves correspond to four different transmission efficiencies. The performance in both the RR (a) and DR (b) conditions is analyzed. For all curves, the minimum secret key rate reaches its peak value at the region of $r < 1$ i.e., the phase-squeezed states have the best performance at a special r. In contrast, the amplitude squeezed states always present a lower performance than the coherent states. For each curve, we denote the peak point as "best r" and the range of r, which has a secret key rate larger than that of the coherent state, as "better r."

In the RR condition, when the distance increases, the range of better r decreases and the value of the best r moves closer to 1. Owing to the relatively flat top of the curve, the minimum secret key rate at the point of best r approximately equals the value at point $r = 1$ or the coherent state. In the DR condition, when the distance increases, the range of better r also decreases; however, the value of the best r increases at first, and then moves farther from 1. When $T_x = 0.83$ (corresponding to a transmission distance of 4 km in telecom single-mode fiber), the coherent-state protocol is no longer available in the DR condition. However, the coherent-state protocol in the RR condition at a longer distance ($T_x = 0.8$, green line in Fig. 7a) is available and has a higher secret key

rate than that of the squeezed-state protocol at best r in the DR condition ($T_x = 0.83$, red line in Fig. 7b).

5 Conclusions

In this work, we proposed a UD squeezed-state protocol. A uniform expression is designed to analyze the UD squeezed-state protocol and UD coherent-state protocol conveniently by simply varying a parameter r. The equivalence of the PM and EB scheme of the UD protocols is proved based on this uniform expression. Then, the security of UD protocols under collective attacks is proved in both the RR and DR conditions.

In contrast to the two-dimensional squeezed-state protocol, where higher squeezing usually obtains a better performance, in the UD protocol, the phase-squeezed state can present a better performance than the coherent state for a relatively long distance (RR condition); however, the improvement and the required optimal squeezing level are small. In the DR condition, the improvement due to the phase-squeezed state is more obvious than that in the RR condition. However, the distance is limited, and its performance is inferior to that of the coherent state in the RR condition except that T_x is very close to 1. Considering the coherent state is easy to prepare than the squeezed state and the performance improvement arising from the squeezing effect is not significant, the coherent state is still appealing and has advantages in the UD domain from a practical viewpoint.

For future research and experiments, an integration of CV-QKD in the deployed optical-network-based UD coherent-state protocol is expected [35], particularly, when the cost is a key concern. In theory, the composable security [36, 37] of the UD coherent-state protocol will be considered.

Acknowledgements This research was supported by the Key Project of the Ministry of Science and Technology of China (2016YFA0301403), National Natural Science Foundation of China (NSFC) (11504219, 61378010), Shanxi 1331KSC, and Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi.

References

1. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**(3), 1301 (2009)
2. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H., Lloyd, S.: Gaussian quantum information. Rev. Mod. Phys. **84**(2), 621 (2012)
3. Ralph, T.C.: Continuous variable quantum cryptography. Phys. Rev. A **61**(1), 010303 (1999)
4. Hillery, M.: Quantum cryptography with squeezed states. Phys. Rev. A **61**(2), 022309 (2000)
5. Cerf, N.J., Levy, M., Assche, G.V.: Quantum distribution of Gaussian keys using squeezed states. Phys. Rev. A **63**(5), 052311 (2001)
6. Gottesman, D., Preskill, J.: Secure quantum key distribution using squeezed states. Phys. Rev. A **63**(2), 022309 (2001)
7. Silberhorn, C., Ralph, T.C., Lütkenhaus, N., Leuchs, G.: Continuous variable quantum cryptography: beating the 3 dB loss limit. Phys. Rev. Lett. **89**(16), 167901 (2002)

8. Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. **88**(5), 057902 (2002)
9. Grosshans, F., Assche, G.V., Wenger, J., Brouri, R., Cerf, N.J., Grangier, P.: Quantum key distribution using Gaussian-modulated coherent states. Nature **421**(6920), 238 (2003)
10. Weedbrook, C., Lance, A.M., Bowen, W.P., Symul, T., Ralph, T.C., Lam, P.K.: Quantum cryptography without switching. Phys. Rev. Lett. **93**(17), 170504 (2004)
11. Lance, A.M., Symul, T., Sharma, V., Weedbrook, C., Ralph, T.C., Lam, P.K.: No-switching quantum key distribution using broadband modulated coherent light. Phys. Rev. Lett. **95**(18), 180503 (2005)
12. García-Patrón, R., Cerf, N.J.: Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys. Rev. Lett. **97**(19), 190503 (2006)
13. Navascués, M., Grosshans, F., Acín, A.: Optimality of Gaussian attacks in continuous-variable quantum cryptography. Phys. Rev. Lett. **97**(19), 190502 (2006)
14. Qi, B., Huang, L.L., Qian, L., Lo, H.K.: Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. Phys. Rev. A **76**(5), 052323 (2007)
15. Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N.J., Tualle-Brouri, R., McLaughlin, S.W., Grangier, P.: Quantum key distribution over 25 km with an all-fiber continuous-variable system. Phys. Rev. A **76**(4), 042305 (2007)
16. García-Patrón, R., Cerf, N.J.: de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Phys. Rev. Lett. **102**(13), 130501 (2009)
17. Leverrier, A., Grangier, P.: Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys. Rev. Lett. **102**(18), 180504 (2009)
18. Zhao, Y.B., Heid, M., Rigas, J., Lutkenhaus, N.: Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. Phys. Rev. A **79**(1), 012307 (2009)
19. 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. **109**(10), 100502 (2012)
20. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P., Diamanti, E.: Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat. Photonics **7**, 378 (2013)
21. Pirandola, S., Ottaviani, C., Spedalieri, G., Weedbrook, C., Braunstein, S.L., Lloyd, S.: High-rate measurement-device-independent quantum cryptography. Nat. Photonics **9**, 397 (2015)
22. Wang, X.Y., Liu, J.Q., Li, X.F., Li, Y.M.: Generation of stable and high extinction ratio light pulses for continuous variable quantum key distribution. IEEE J. Quantum Electron. **51**(6), 5200206 (2015)
23. Huang, D., Huang, P., Lin, D., Zeng, G.: Long distance continuous variable quantum key distribution by controlling excess noise. Sci. Rep. **6**, 19201 (2016)
24. Yang, S.S., Bai, Z.L., Wang, X.Y., Li, Y.M.: FPGA-based implementation of size-adaptive privacy amplification in quantum key distribution. Photonics J. **9**(6), 7600308 (2017)
25. Li, Y.M., Wang, X.Y., Bai, Z.L., Liu, W.Y., Yang, S.S., Peng, K.C.: Continuous variable quantum key distribution. Chin. Phys. B **26**(4), 040303 (2017)
26. Usenko, V.C., Grosshans, F.: Unidimensional continuous-variable quantum key distribution. Phys. Rev. A **92**(6), 062337 (2015)
27. Brádler, K., Weedbrook, C.: Security proof of continuous-variable quantum key distribution using three coherent states. Phys. Rew. A **97**(2), 022310 (2018)
28. Qi, B., Evans, P.G., Grice, W.P.: Passive state preparation in the Gaussian-modulated coherent-states quantum key distribution. Phys. Rev. A **97**(1), 012317 (2018)
29. Wang, X.Y., Liu, W.Y., Wang, P., Li, Y.M.: Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution. Phys. Rev. A **95**(6), 062330 (2017)
30. Wang, P., Wang, X.Y., Li, J.Q., Li, Y.M.: Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions. Opt. Express **25**(23), 27995 (2017)
31. Milicevic, M., Feng, C., Zhang, L.M., Gulak, P.G.: Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. NPJ Quantum Inf. **4**, 21 (2018)
32. Laudenbach, F., Pacher, C., Fung, C.F., Poppe, A., Peev, M., Schrenk, B., Hentschel, M., Walther, P., Hübel, H.: Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. Adv. Quantum Technol. **1**, 1800011 (2018)
33. Wang, P., Wang, X.Y., Li, Y.M.: Security analysis of unidimensional continuous-variable quantum key distribution using uncertainty relations. Entropy **20**, 157 (2018)
34. Usenko, V.C., Filip, R.: Squeezed-state quantum key distribution upon imperfect reconciliation. New J. Phys. **13**, 113007 (2011)

35. Karinou, F., Brunner, H.H., Fung, C.F., Comandar, L.C., Bettelli, S., Hillerkuss, D., Kuschnerov, M., Mikroulis, S., Wang, D., Xie, C., Peev, M., Poppe, A.: Toward the integration of CV quantum key distribution in deployed optical networks. IEEE Photonics Technol. Lett. **30**(7), 650 (2018)
36. Leverrier, A.: Composable security proof for continuous-variable quantum key distribution with coherent States. Phys. Rev. Lett. **114**(7), 070501 (2015)
37. Leverrier, A.: Security of continuous variable quantum key distribution via a Gaussian de finetti reduction. Phys. Rev. Lett. **118**(20), 200501 (2017)