Chin. Sci. Bull. (2014) 59(11):1083–1090
DOI 10.1007/s11434-014-0193-x

csb.scichina.com
www.springer.com/scp

Invited Article

Quantum Information

Applying Gaussian quantum discord to quantum key distribution

Xiaolong Su

Received: 31 October 2013 / Accepted: 17 November 2013 / Published online: 25 February 2014

Abstract In this paper, we theoretically prove that the Gaussian quantum discord state of optical field can be used to complete continuous variable (CV) quantum key distribution (QKD). The calculation shows that secret key can be distilled with a Gaussian quantum discord state against entangling cloner attack. Secret key rate is increased with the increasing of quantum discord for CV QKD with the Gaussian quantum discord state. Although the calculated results point out that secret key rate using the Gaussian quantum discord state is lower than that using squeezed state and coherent state at the same energy level, we demonstrate that the Gaussian quantum discord, which only involving quantum correlation without the existence of entanglement, may provide a new resource for realizing CV QKD.

Keywords Quantum information · Quantum key distribution · Quantum discord · Continuous variable

1 Introduction

Quantum correlation, which is measured by quantum discord [1–3], is a fundamental resource for quantum information processing tasks. It has been shown that some quantum computational tasks based on a single qubit can be carried out by separable (that is, non-entangled) states that nonetheless carries non-classical correlations [4–6]. Recently, quantum discord is extended to two-mode Gaussian states [7, 8]. A two-mode Gaussian state is entangled with Gaussian quantum discord $D > 1$, when $0 \leq D \leq 1$ we have either separable or entangled states. Gaussian quantum discord has been experimentally demonstrated too [9–11].

Quantum key distribution (QKD) allows two legitimate parties, Alice and Bob who are linked by a quantum channel and an authenticated classical channel, to establish the secret key only known by themselves. Continuous variable (CV) QKD using Gaussian quantum resource state, such as entangled state, squeezed state, and coherent state, as the resource state, along with reconciliation and privacy amplification procedure to distill the secret key [12]. There are two types of QKD schemes, one is called prepare-and-measure scheme, the other is entanglement-based scheme. The equivalence between these two type CV QKD schemes has been proved. QKD with coherent state (squeezed state) has been proved to be equivalent to heterodyning (homodyning) one of the two entangled modes of an Einstein–Podolsky–Rosen (EPR) entangled state [13]. Generally, the entanglement-based QKD model is used to investigate the security of CV QKD. The security of CV QKD scheme has been analyzed [14–16], and it has been proved to be unconditionally secure, that is, secure against arbitrary attacks over long distance [17, 18]. Recently, a CV QKD scheme with thermal states is also proposed and proved to be secure against collective Gaussian attacks [19].

Very recently, it has been shown that quantum discord can be used as a resource for QKD in general [20]. What we concerned is the role of Gaussian quantum discord in CV QKD. In this paper, we apply a two-mode Gaussian discord state, where only quantum correlation exists and without entanglement, to implement CV QKD. The calculation shows that the secret key can be distilled with the

X. Su (✉)
State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China
e-mail: suxl@sxu.edu.cn

two-mode Gaussian discord state against entangling cloner attack, which is the most important and practical example of collective Gaussian attack. The secret key rate of the QKD scheme with Gaussian discord state is increased with the increasing of the quantum discord. The secret key rates of the CV QKD schemes with the Gaussian discord state, squeezed state and coherent state (no-switching QKD) are compared. Although squeezed state and coherent state offer higher secret key rate than the Gaussian discord state, we demonstrate the Gaussian discord can be used to establish secret key.

2 The Gaussian discord state and QKD scheme

The QKD scheme with a two-mode Gaussian quantum discord state and entangled state is shown in Fig. 1. Figure 1a shows a two-mode Gaussian discord state, as shown in [9], which is prepared by correlated (anti-correlated) displacement of two coherent states in the amplitude (phase) quadrature with a discording noise V. Figure 1b shows an EPR entangled state with a variance $V_{\mathrm{E}} = \cosh 2r$, where $r \in [0, \infty)$ is the squeezing parameter. The amplitude and phase quadratures of an optical mode $\hat{a}$ are defined as $\hat{X}_a = \hat{a} + \hat{a}^{\dagger}$ and $\hat{Y}_a = (\hat{a} - \hat{a}^{\dagger})/i$, respectively. The variances of amplitude and phase quadratures for a vacuum (coherent) state are $V(\hat{X}_v) = V(\hat{Y}_v) = 1$. The covariance matrix of the two-mode Gaussian quantum resource state in Fig. 1a, b is given by

$$\sigma = \begin{pmatrix} \alpha \boldsymbol{I} & \gamma \boldsymbol{Z} \\ \gamma \boldsymbol{Z} & \beta \boldsymbol{I} \end{pmatrix}, \tag{1}$$

where $\boldsymbol{I}$ and $\boldsymbol{Z}$ are the Pauli matrices

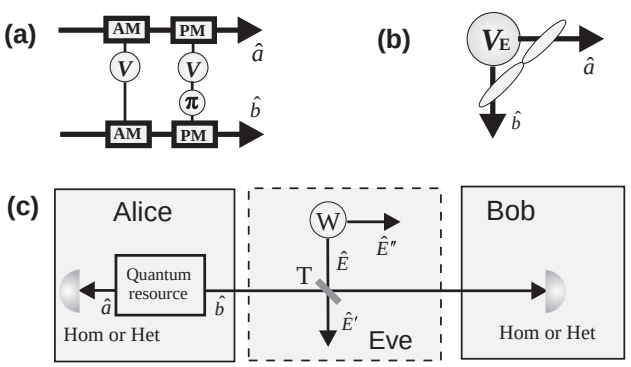

Fig. 1 Schematic of the CV QKD scheme with a two-mode Gaussian state. **a** The two-mode Gaussian discord state, *AM* amplitude modulator, *PM* phase modulator, π π phase shift; **b** EPR entangled state; **c** the CV QKD scheme. The transmission efficiency of quantum channel is modeled by a beam splitter with transmission T. Eve performs entangling cloner attack, where the variance of the ancillary EPR state is W. *Hom* homodyne detection, *Het* heterodyne detection

$$\boldsymbol{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \boldsymbol{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2}$$

$\alpha = \beta = V_{\mathrm{D}} = V + 1$, $\gamma = V$ for the two-mode Gaussian discord state and $\alpha = \beta = V_{\mathrm{E}}, \gamma = \sqrt{V_{\mathrm{E}}^2 - 1}$ for the EPR entangled state, respectively.

Quantum discord is defined as the difference between two quantum analogs of classically equivalent expression of the mutual information. The Gaussian quantum discord of a two-mode Gaussian state is given by [8]

$$D_{AB} = f(\sqrt{I_2}) - f(v_-) - f(v_+) + f(\sqrt{E^{\min}}), \tag{3}$$

where $f(x) = (\frac{x+1}{2}) \log \frac{x+1}{2} - (\frac{x-1}{2}) \log \frac{x-1}{2}$,

$$v_{\pm} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4 \det \sigma}}{2}}, \tag{4}$$

are the symplectic eigenvalues of a two-mode covariance matrix $\sigma = \begin{pmatrix} \boldsymbol{A} & \boldsymbol{C} \\ \boldsymbol{C} & \boldsymbol{B} \end{pmatrix}$ with $\det \sigma$ as the determinant of covariance matrix and $\Delta = \det \boldsymbol{A} + \det \boldsymbol{B} + 2 \det \boldsymbol{C}$, and

$$E^{\min} = \begin{cases} \frac{2I_3^2 + (I_2 - 1)(I_4 - I_1) + 2|I_3| \sqrt{I_3^2 + (I_2 - 1)(I_4 - I_1)}}{(I_2 - 1)^2} \\ \frac{I_1 I_2 - I_3^2 + I_4 - \sqrt{I_3^4 + (I_4 - I_1 I_2)^2 - 2I_3^2 (I_4 + I_1 I_2)}}{2I_2} \end{cases} \tag{5}$$

where the first equation applies if $(I_4 - I_1 I_2)^2 \leq I_3^2 (I_2 + 1)(I_1 + I_4)$ and the second equation applies otherwise. $I_1 = \det \boldsymbol{A}$, $I_2 = \det \boldsymbol{B}$, $I_3 = \det \boldsymbol{C}$, $I_4 = \det \sigma$ are the symplectic invariants.

PPT criterion is a necessary and sufficient criterion for entanglement of Gaussian state [21, 22]. A Gaussian state is entangled if $\tilde{v}_- < 1$, where $\tilde{v}_-$ is the smallest symplectic eigenvalue of partial transposed covariance matrix for two-mode Gaussian state, which is given by [23, 24]

$$\tilde{v}_- = \sqrt{\frac{\tilde{\Delta} - \sqrt{\tilde{\Delta}^2 - 4 \det \sigma}}{2}}, \tag{6}$$

where $\tilde{\Delta} = \det \boldsymbol{A} + \det \boldsymbol{B} - 2 \det \boldsymbol{C}$.

Based on the covariance matrix in Eq. (1) for the Gaussian discord state, we calculated the quantum discord and smallest symplectic eigenvalue of PPT criterion, which are shown in Fig. 2. As shown in Fig. 2a, the quantum discord is increased dramatically with the increasing of input variance V_{D} in the region of $V_{\mathrm{D}} \in [1, 100]$. When $V_{\mathrm{D}} > 100$, the quantum discord increased slowly with the increasing of V_{D}. The smallest quantum discord is 0.12 at $V_{\mathrm{D}} = 1$. The quantum discord is always smaller than 1. In Fig. 2b, the smallest symplectic eigenvalue of partial transposed covariance matrix is always 1, which means that there is no entanglement in the Gaussian discord state.

Figure 1c shows the CV QKD scheme with a two-mode Gaussian state as quantum resource state, which can be the

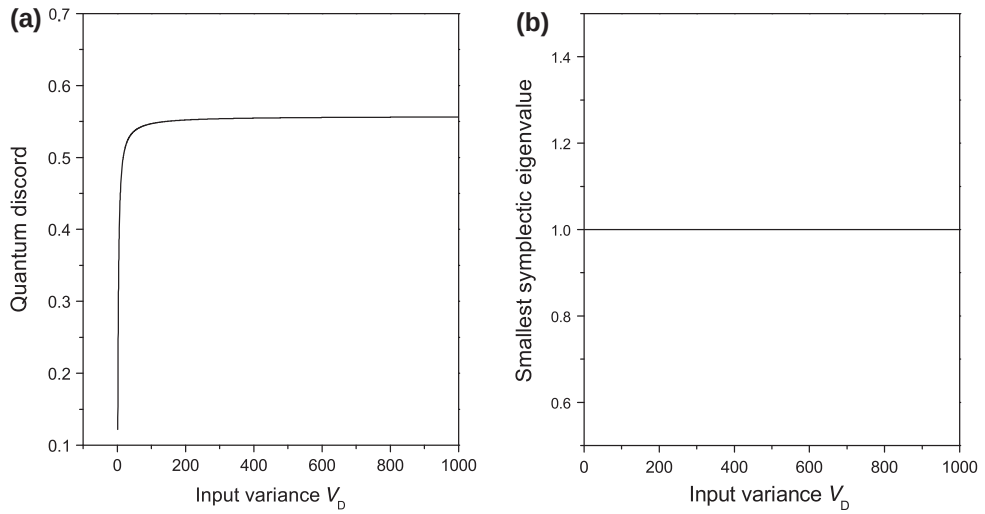

Fig. 2 Quantum discord (**a**) and smallest symplectic eigenvalue of PPT criterion (**b**) for the Gaussian discord state

two-mode Gaussian discord state or the EPR entangled state. Alice hold mode $\hat{a}$, and transmitted mode $\hat{b}$ to Bob over the quantum channel. Here, we consider that Alice and Bob perform homodyne (Hom) or heterodyne (Het) detection on their own beam, which corresponds to the CV QKD scheme with homodyne or heterodyne detection. We assume that Eve perform entangling cloner attack [13], which is the most important and practical example of a collective Gaussian attack [17, 25–27], to steal the information. She prepares an ancillary EPR entangled states with variance W, which corresponds to the excess noise $\delta = W - 1$ in [28] and $\epsilon = (W-1)(1-T)/T$ in [13]. $W = 1$ means there is no excess noise ($\delta = 0$) in the channel, when $W > 1$, there is excess noise ($\delta = W - 1$) in the channel. She keeps one mode $\hat{E}''$ and mixed the other mode $\hat{E}$ with the transmitted mode $\hat{b}$ in the quantum channel by a beam splitter, leading to the output mode $\hat{E}'$. Eve's output modes are stored in a quantum memory and detected collectively at the end of the protocol. Eve's final measurement is optimized based on Alice and Bob's classical communication. After communication is completed, Alice and Bob perform reconciliation, error correction [29, 30] and privacy amplification [31] to distill final secret key.

3 Security of the CV QKD scheme

3.1 Homodyne detection

In the CV QKD scheme with homodyne detection, Alice and Bob perform homodyne detection on their own beams to measure the amplitude or phase quadrature, respectively. For CV QKD with EPR entangled state, homodyning one of the entangled beam is equivalent to the CV QKD with squeezed state. So we will compare the Gaussian discord state QKD with squeezed state QKD in this section. In the following, we use the variable X to represent amplitude or phase quadrature of an optical mode to analyze the secret key without losing the generality.

3.1.1 Direct reconciliation

In direct reconciliation, Bob attempts to guess what Alice sent. The secret key rate is given by

$$K_{DR} = I(X_A{:}X_B) - I(X_A{:}E), \tag{7}$$

where

$$I(X_A{:}X_B) = H(X_B) - H(X_B|X_A), \tag{8}$$

is the mutual information between Alice and Bob, with $H(X_B) = (1/2)\log_2 V(X_B)$ and $H(X_B|X_A) = (1/2)\log_2 V(X_B|X_A)$ being the total and conditional Shannon entropies. Eve's information is

$$I(X_A{:}E) = S(E) - S(E|X_A), \tag{9}$$

where $S(\cdot)$ is the von Neumann entropy. The von Neumann entropy of a Gaussian state ρ can be expressed in terms of its symplectic eigenvalues [32]

$$S(\rho) = \sum_{k=1}^{n} g(v_k), \tag{10}$$

with $g(v) = \frac{1}{2}(v+1)\log_2[\frac{1}{2}(v+1)] - \frac{1}{2}(v-1)\log_2[\frac{1}{2}(v-1)]$, where $v = \{v_1, ...v_n\}$ are the symplectic eigenvalues of Gaussian state ρ. The symplectic spectrum $v = \{v_1, ...v_n\}$ of an arbitrary correlation matrix σ can be calculated by

finding the (standard) eigenvalues of the matrix $|i\Omega\sigma|$, where Ω defines the symplectic form and is given by [12]

$$\Omega = \bigoplus_{k=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{11}$$

Here $\bigoplus$ is the direct sum indicating adding matrices on the block diagonal.

In Fig. 1c, the covariance matrix of the two-mode Gaussian state distributed between Alice and Bob in the CV QKD is given by

$$\sigma_{AB} = \begin{pmatrix} V_A \boldsymbol{I} & \gamma' \boldsymbol{Z} \\ \gamma' \boldsymbol{Z} & V_B \boldsymbol{I} \end{pmatrix}, \tag{12}$$

where $V_A = V_{\mathrm{E}}$, $V_B = TV_{\mathrm{E}} + (1-T)W$, $\gamma' = \sqrt{T(V_{\mathrm{E}}^2 - 1)}$ for the EPR entangled state and $V_A = V_{\mathrm{D}}$, $V_B = TV_{\mathrm{D}} + (1-T)W$, $\gamma' = \sqrt{T}V$ for the Gaussian discord state, respectively.

The conditional variance is defined as [33] $V_{X|Y} = V(X) - |\langle XY\rangle|^2 / V(Y)$. So Bob's conditional variance in homodyne detection is given by

$$V_{B|A} = V_B - \frac{\gamma'^2}{V_A}. \tag{13}$$

The mutual information between Alice and Bob is $I^{\mathrm{Hom}}(X_A{:}X_B) = \frac{1}{2}\log_2[V_B/V_{B|A}]$, which is same for the direct and reverse reconciliation.

Eve's covariance matrix is made up from the modes $\hat{E}'$ and $\hat{E}''$, which is

$$\sigma_E = \begin{pmatrix} e_v \boldsymbol{I} & \varphi \boldsymbol{Z} \\ \varphi \boldsymbol{Z} & W \boldsymbol{I} \end{pmatrix}, \tag{14}$$

where $e_v = (1-T)V_A + TW$, $\varphi = \sqrt{T(W^2-1)}$.

In order to obtain $S(E|X_A)$ we need to calculate the symplectic spectrum of the conditional covariance matrix $\sigma_{E|X_A}$, which represents the covariance matrix of Eve's system where mode $\hat{a}$ has been measured by Alice using homodyne detection and is given by [12, 34, 35]

$$\sigma_{E|X_A} = \sigma_E - (V_A)^{-1} \boldsymbol{D} \Pi \boldsymbol{D}^{\mathrm{T}}, \tag{15}$$

where

$$\Pi = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{16}$$

and $\boldsymbol{D}$ is the matrix describing the quantum correlations between Eve' modes and Alice's mode, which is given by

$$\boldsymbol{D} = \begin{pmatrix} \langle X_E X_A\rangle \boldsymbol{I} \\ \langle X_{E''} X_A\rangle \boldsymbol{Z} \end{pmatrix} = \begin{pmatrix} \zeta \boldsymbol{I} \\ \eta \boldsymbol{Z} \end{pmatrix}, \tag{17}$$

where $\zeta = \sqrt{1-T}V_A$, $\eta = 0$.

3.1.2 Reverse reconciliation

The 3 dB loss limit on the transmission line in the CV QKD [36] can be beaten with the reverse reconciliation [37, 38] or the post-selection [39]. In reverse reconciliation, Alice attempts to guess what was received by Bob rather than Bob guessing what was sent by Alice [37]. Such a reverse reconciliation protocol gives Alice an advantage over a potential eavesdropper Eve. In reverse reconciliation, the secret key rate is

$$K_{\mathrm{RR}} = I(X_A{:}X_B) - I(X_B{:}E), \tag{18}$$

where the mutual information between Alice and Bob $I(X_A{:}X_B)$ is same with what obtained above.

Eve's information is given by

$$I(X_B{:}E) = S(E) - S(E|X_B). \tag{19}$$

The conditional covariance matrix $\sigma_{E|X_B}$, which represents the covariance matrix of a system where one of the modes has been measured by homodyne detection (in this case Bob), is given by [12, 34, 35]

$$\sigma_{E|X_B} = \sigma_E - (V_B)^{-1} \boldsymbol{D} \Pi \boldsymbol{D}^{\mathrm{T}}. \tag{20}$$

Here $\boldsymbol{D}$ is the matrix describing the quantum correlations between Eve' modes and Bob's mode, which is given by

$$\boldsymbol{D} = \begin{pmatrix} \langle X_{E'} X_B\rangle \boldsymbol{I} \\ \langle X_{E''} X_B\rangle \boldsymbol{Z} \end{pmatrix} = \begin{pmatrix} \zeta' \boldsymbol{I} \\ \eta' \boldsymbol{Z} \end{pmatrix}, \tag{21}$$

where

$\zeta' = \sqrt{T(1-T)}(W - V_A)$, $\eta' = \sqrt{(1-T)(W^2-1)}$.

Figure 3 shows the secret key rate of the CV QKD scheme with homodyne detection, (a) and (b) are corresponding to the direct and reverse reconciliation, respectively. Solid and dashed lines are the secret key rates for the Gaussian discord state with variance V_{D}=40 (typical experimental realistic modulation level [37]) and 1000, respectively. Dotted line is the secret key rate for the squeezed state with variance V_{E}=40. All curves are plotted with excess noise $W = 1$. Comparing the solid and dotted lines in Fig. 3, it is obvious that secret key rate for squeezed state is greater than that for Gaussian discord state at the same energy level in both direct and reverse reconciliation. Comparing solid and dashed lines, we find that the secret key rate is increased with the increasing of the discording noise for the CV QKD with the Gaussian discord state with homodyne detection in both direct and reverse reconciliation.

3.2 Heterodyne detection

In the CV QKD scheme with heterodyne detection, Alice and Bob perform heterodyne detection to measure the

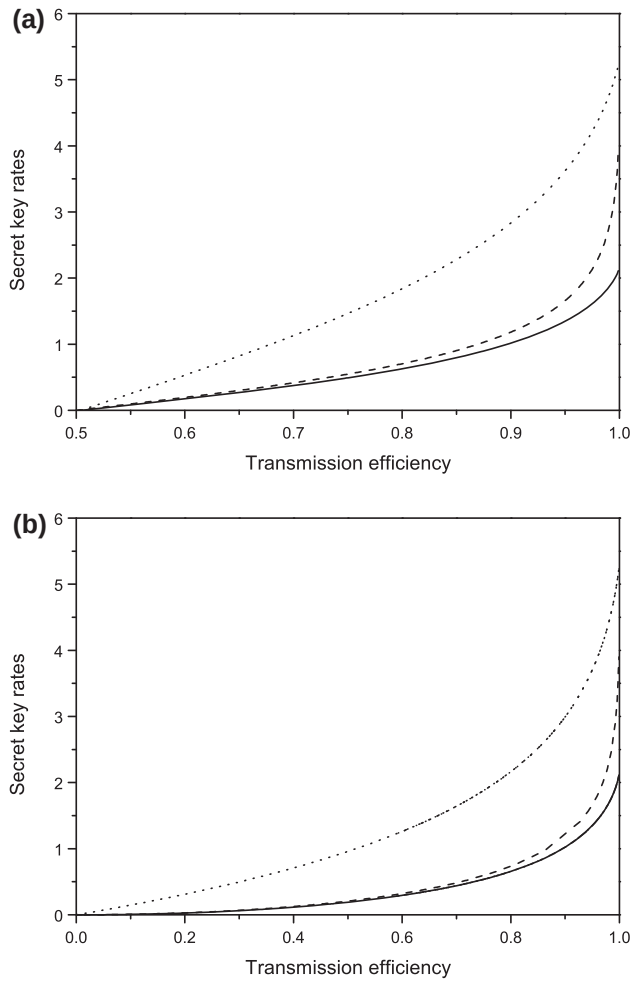

Fig. 3 Secret key rates for the CV QKD schemes with homodyne detection. **a** The direct reconciliation; **b** the reverse reconciliation. *Solid and dashed lines* are the secret key rates for the Gaussian discord state with variance $V_{\mathrm{D}} = 40$ and 1000, respectively. *Dotted line* is the secret key rate for the entangled state with $V_{\mathrm{E}} = 40$. All curves are plotted with excess noise $W = 1$

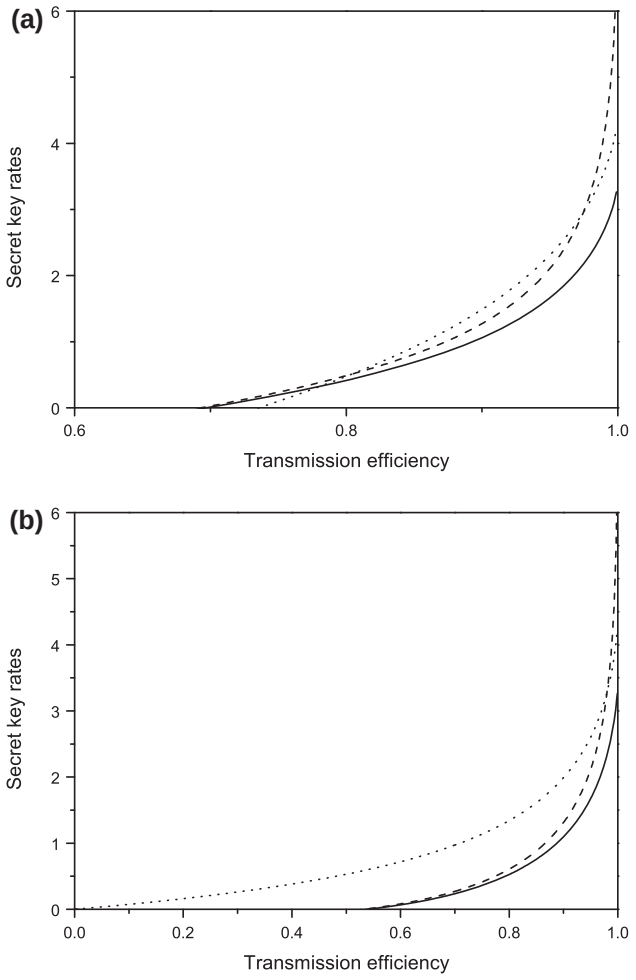

Fig. 4 Secret key rates for the CV QKD schemes with heterodyne detection. **a** The direct reconciliation; **b** the reverse reconciliation. *Solid and dashed lines* are the secret key rates for the Gaussian discord state with $V_{\mathrm{D}} = 40$ and 1000, respectively. *Dotted line* is the secret key rate for the entangled state with $V_{\mathrm{E}} = 40$. All curves are plotted with excess noise $W = 1$

amplitude and phase quadratures of their own beams simultaneously. Since heterodyning one of EPR entangled state is equivalent to QKD with coherent state. In this section, we will compare the Gaussian discord state QKD with no-switching coherent state QKD [40].

In heterodyne detection system, a vacuum mode $\hat{v}$ is mixed with the optical mode $\hat{a}$ ($\hat{b}$) on a balanced beam splitter and the output modes are measured by two homodyne detectors respectively. The amplitude quadrature measured by Alice and Bob are $\hat{X}_A^M = (\hat{X}_a + \hat{X}_v)/\sqrt{2}$ and $\hat{X}_B^M = (\hat{X}_B + \hat{X}_v)/\sqrt{2}$, respectively. The corresponding noise variance measured by Alice and Bob are $V_A^M = (V_A + 1)/2$ and $V_B^M = (V_B + 1)/2$, respectively.

Bob's conditional variance is given by $V_{B^M|A^M} = (V_{B|A^M} + 1)/2$, where

$$V_{B|A^M} = V_B - \frac{\gamma'^2/2}{V_A^M}. \tag{22}$$

The mutual information between Alice and Bob are $I^{\mathrm{Het}}(X_A{:}X_B) = \log_2[V_{B^M}/V_{B^M|A^M}]$, which is same for the direct and reverse reconciliation.

3.2.1 Direct reconciliation

In order to obtain $S(E|X_B)$ we need to calculate the symplectic spectrum of the conditional covariance matrix $\sigma_{E|\hat{X}_A,\hat{Y}_A}$, which represents the covariance matrix of a system where two modes has been measured by heterodyne detection (in this case Alice), is given by [12, 34, 35]

$$\sigma_{E|\hat{X}_A,\hat{Y}_A} = \sigma_E - (\Lambda)^{-1}\boldsymbol{D}(\Omega\sigma_A\Omega^{\mathrm{T}} + \boldsymbol{I})\boldsymbol{D}^{\mathrm{T}}, \tag{23}$$

where $\Lambda = \det\sigma_A + \mathrm{Tr}\sigma_A + 1, \Omega\sigma_A\Omega^{\mathrm{T}} + \boldsymbol{I} = \sigma_A + \boldsymbol{I}$, and $\boldsymbol{D}$ is given by Eq. (18).

3.2.2 Reverse reconciliation

The correlation matrix $\sigma_{E|\hat{X}_B,\hat{Y}_B}$, which represents the covariance matrix of a system where two modes has been measured by heterodyne detection (in this case Bob), is given by [12, 34, 35]

$$\sigma_{E|\hat{X}_B,\hat{Y}_B} = \sigma_E - (\Lambda')^{-1}\boldsymbol{D}(\Omega\sigma_B\Omega^{\mathrm{T}} + \boldsymbol{I})\boldsymbol{D}^{\mathrm{T}}, \quad (24)$$

where $\Lambda' = \det\sigma_B + \mathrm{Tr}\sigma_B + 1, \Omega\sigma_B\Omega^{\mathrm{T}} + \boldsymbol{I} = \sigma_B + \boldsymbol{I}$, and the matrix $\boldsymbol{D}$ is same with Eq. (22), which describing the quantum correlations between Eve's modes and Bob's mode.

Figure 4 shows the secret key rates for the CV QKD schemes with heterodyne detection, (a) and (b) are for the direct and reverse reconciliation, respectively. Solid and dashed lines are the secret key rates for the Gaussian discord state with $V_{\mathrm{D}} = 40$ and 1000, respectively. Dotted line is the secret key rate for the entangled state with $V_{\mathrm{E}} = 40$. All curves are plotted with excess noise $W = 1$. In Fig. 4a, comparing solid and dotted lines, we find that secret key can be distilled for the Gaussian discord state at lower transmission efficiency than that for coherent state with heterodyne detection. When $T > 0.78$, secret key rate for coherent state is still higher than that for the Gaussian discord state with heterodyne detection. In Fig. 4b, comparing solid and dotted lines, it is obvious that no-switching coherent state QKD offers higher secret key rate and longer transmission distance than that the Gaussian discord state QKD. We also noticed that no secret key can be distilled for the Gaussian discord state at lower transmission efficiency ($T < 0.55$) with reverse reconciliation, which is different from coherent state QKD. Comparing solid and

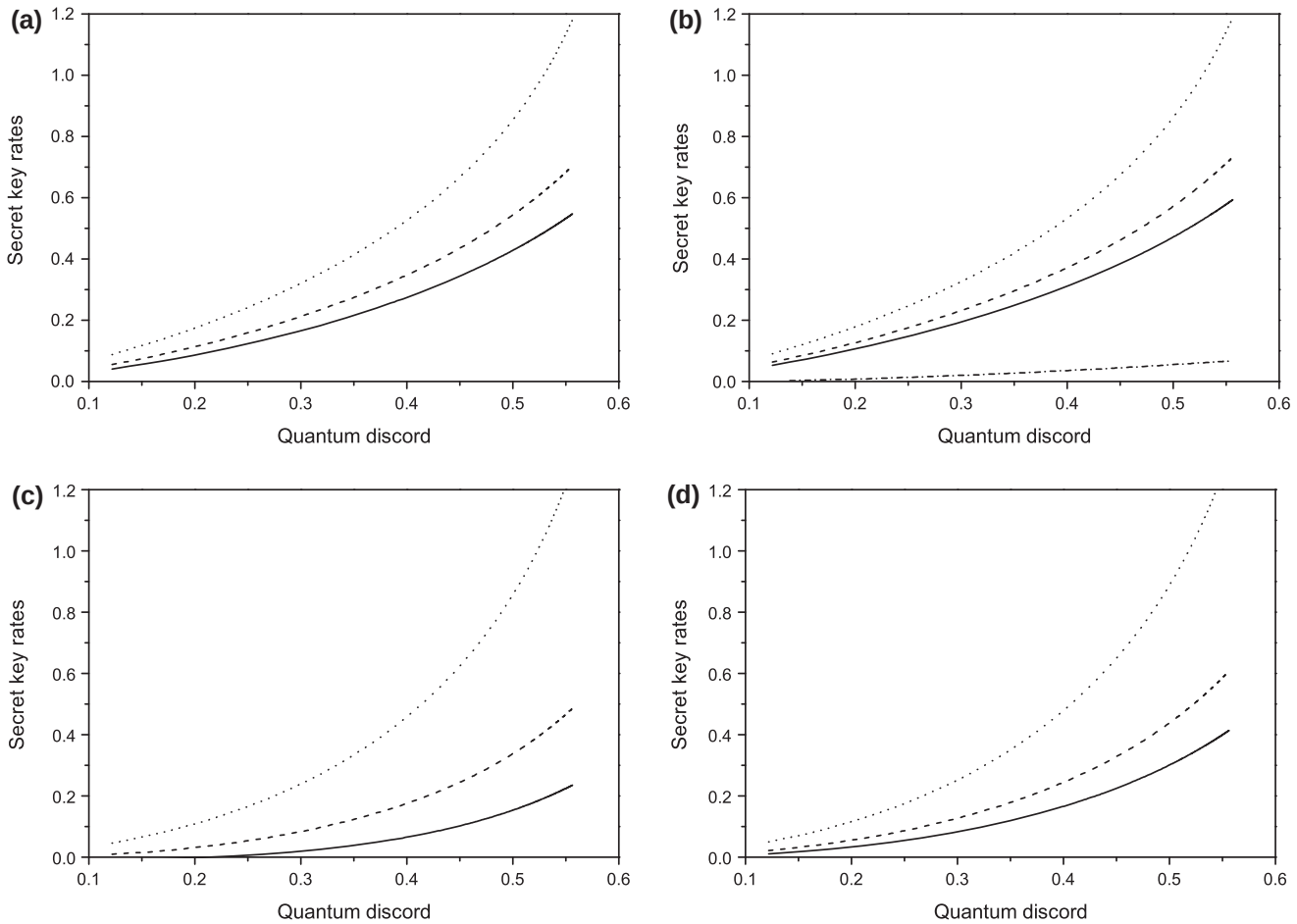

Fig. 5 The dependence of secret key rates on quantum discord for the CV QKD schemes with the Gaussian discord state. **a**, **b** The direct and reverse reconciliation for homodyne detection, respectively; **c**, **d** the direct and reverse reconciliation for heterodyne detection, respectively. *Solid, dashed, and dotted lines* are the secret key rates for the Gaussian discord state with transmission efficiency of 0.75, 0.8, and 0.9, respectively. *Dash-dotted line* in **b** is the secret key rate for the Gaussian discord state with transmission efficiency of 0.3. All curves are plotted with excess noise $W = 1, V_{\mathrm{D}} \in [1, 1000]$

dashed lines in Fig. 4a, b, respectively, we find that secret key rate is increased with increasing of the discording noise for both direct and reverse reconciliation in CV QKD with the Gaussian quantum discord state, which is same with the result of homodyne detection.

4 Dependence of secret key rate on quantum discord

As shown in Fig. 5, the dependence of secret key rate for the Gaussian discord state on quantum discord are investigated at different transmission efficiency with input variance $V_{\mathrm{D}} \in [1, 1000]$. Figure 5a, b is the case of direct and reverse reconciliation for homodyne detection, respectively. Figure 5c, d is the case of direct and reverse reconciliation for heterodyne detection, respectively. It is obvious that secret key rate is monotonically increased with the increasing of quantum discord. Solid, dashed and dotted lines are the secret key rates for the Gaussian discord state with transmission efficiency of 0.75, 0.8 and 0.9, respectively. Dash-dotted line in Fig. 5b is the secret key rate for the Gaussian discord state with transmission efficiency of 0.3, which means that secret key can be distilled when $T < 0.5$ in reverse reconciliation for homodyne detection. Comparing these traces, we find that secret key rate is increased with the increasing of transmission efficiency, which is same with the result in Figs. 3 and 4. Most of the secret key rates start from $D_{AB} = 0.12$, since 0.12 is the smallest quantum discord with $V_{\mathrm{D}} = 1$ as shown in Fig. 2a. When $T = 0.75$ (solid line) in Fig. 5c, secret key can be distilled when $D_{AB} > 0.22$.

5 Conclusion

In this paper, by considering CV QKD with a two-mode Gaussian discord state, which has only quantum correlation and without entanglement, we show that secret key can be distilled against entangling cloner attack. In CV QKD with the Gaussian discord state, the secret key rate is increased with increasing of quantum discord in both homodyne and heterodyne detection schemes with direct and reverse reconciliation. By comparing the secret key rates of CV QKD schemes with the Gaussian discord state, squeezed state and coherent state, we find that squeezed state and coherent state offer higher secret key rate than the Gaussian discord state at the same energy level for both direct and reverse reconciliation. This is a natural result since Gaussian discord of the Gaussian discord state ($0 \leq D \leq 1$) is smaller than that of EPR entangled state ($D > 1$). This work provides a possible application of Gaussian quantum discord.

Acknowledgments The author thanks for helpful discussion with Prof. Changde Xie, Kunchi Peng, Jing Zhang, and Xiaojun Jia. This work was supported by the National Basic Research Program of China (2010CB923103), the National Natural Science Foundation of China (11174188, 61121064), Shanxi Scholarship Council of China (2012-010) and Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi.

References

1. Ollivier H, Zurek WH (2001) Quantum discord: a measure of the quantumness of correlations. Phys Rev Lett 88:017901
2. Modi K, Brodutch A, Cable H et al (2012) The classical-quantum boundary for correlations: discord and related measures. Rev Mod Phys 84:1655–1707
3. Aaronson B, Franco RL, Compagno G et al (2013) Hierarchy and dynamics of trace distance correlations. New J Phys 18:093022
4. Knill E, Laflamme R (1998) Power of one bit of quantum information. Phys Rev Lett 81:5672–5675
5. Ryan CA, Emerson J, Poulin D et al (2005) Characterization of complex quantum dynamics with a scalable NMR information processor. Phys Rev Lett 95:250502
6. Lanyon BP, Barbieri M, Almeida MP et al (2008) Experimental quantum computing without entanglement. Phys Rev Lett 101:200501
7. Giorda P, Paris MGA (2010) Gaussian quantum discord. Phys Rev Lett 105:020503
8. Adesso G, Datta A (2010) Quantum versus classical correlations in Gaussian states. Phys Rev Lett 105:030501
9. Gu M, Chrzanowski HM, Assad SM et al (2012) Observing the operational significance of discord consumption. Nat Phys 8:671–675
10. Blandino R, Genoni MG, Etesse J et al (2012) Homodyne estimation of Gaussian quantum discord. Phys Rev Lett 109:180402
11. Madsen LS, Berni A, Lassen M et al (2012) Experimental investigation of the evolution of Gaussian quantum discord in an open system. Phys Rev Lett 109:030402
12. Weedbrook C, Pirandola S, García-Patrón R et al (2012) Gaussian quantum information. Rev Mod Phys 84:621–669
13. Grosshans F, Cerf NJ, Wenger J et al (2003) Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quantum Inf Comput 3:535–552
14. Iblisdir S, Van Assche G, Cerf NJ (2004) Security of quantum key distribution with coherent states and homodyne detection. Phys Rev Lett 3:170502
15. Grosshans F (2005) Collective attacks and unconditional security in continuous variable quantum key distribution. Phys Rev Lett 94:020504
16. Navascués M, Acín A (2005) Security bounds for continuous variables quantum key distribution. Phys Rev Lett 94:020505
17. Renner R, Cirac JI (2009) A de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Phys Rev Lett 102:110504
18. Leverrier A, Grangier P (2009) Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys Rev Lett 102:180504
19. Weedbrook C, Pirandola S, Ralph TC (2012) Continuous-variable quantum key distribution using thermal states. Phys Rev A 86:022318
20. Pirandola S. Quantum discord as a resource for quantum cryptography. arxiv:quant-ph/1309.2446
21. Simon R (2000) Peres–Horodecki separability criterion for continuous variable systems. Phys Rev Lett 84:2726–2729

22. Werner RF, Wolf MM (2001) Bound entangled Gaussian states. Phys Rev Lett 86:3658
23. Serafini A, Illuminati F, De Siena S (2004) Symplectic invariants, entropic measures and correlations of Gaussian states. J Phys B 37:L21
24. Adesso G, Serafini A, Illuminati F (2004) Extremal entanglement and mixedness in continuous variable systems. Phys Rev A 70:022318
25. Navascués M, Grosshans F, Acín A (2006) Optimality of Gaussian attacks in continuous-variable quantum cryptography. Phys Rev Lett 97:190502
26. García-Patrón R, Cerf NJ (2006) Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys Rev Lett 97:190503
27. Pirandola S, Braunstein SL, Lloyd S (2008) Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. Phys Rev Lett 101:200504
28. Namiki R, Hirano T (2004) Practical limitation for continuous-variable quantum cryptography using coherent states. Phys Rev Lett 92:117901
29. Brassard G, Salavail L (1993) Secret-key reconciliation by public discussion. In: Helleseth T (ed) Advances in Cryptology—Eurocrypt'93 Lecture Notes in Computer Science. Springer, New York, pp 410–423
30. Bennett CH, Brassard G, Crépeau C et al (1995) Generalized privacy amplification. IEEE Trans Inf Theor 41:1915–1923
31. Cachin C, Maurer UM (1997) Linking information reconciliation and privacy amplification. J Cryptol 10:97–110
32. Holevo AS, Sohma M, Hirota O (1999) Capacity of quantum Gaussian channels. Phys Rev A 59:1820–1828
33. Grangier P, Levenson JA, Poizat JP (1998) Quantum non-Demolition measurements in optics. Nature 396:537–542
34. Eisert J, Scheel S, Plenio MB (2002) Distilling Gaussian states with Gaussian operations is impossible. Phys Rev Lett 89:137903
35. Fiurášek J (2002) Gaussian transformations and distillation of entangled Gaussian states. Phys Rev Lett 89:137904
36. Grosshans F, Grangier P (2002) Continuous variable quantum cryptography using coherent states. Phys Rev Lett 88:057902
37. Grosshans F, Van Assche G, Wenger J et al (2003) Quantum key distribution using gaussian-modulated coherent states. Nature 421:238–241
38. Lu ZX, Yu L, Li K et al (2010) Reverse reconciliation for continuous variable quantum key distribution. Sci China Phys Mech Astron 53:100–105
39. Silberhorn C, Ralph T C, Lütkenhaus N et al (2002) Continuous variable quantum cryptography: beating the 3 dB loss limit. Phys Rev Lett 89:167901
40. Weedbrook C, Lance AM, Bowen WP et al (2004) Quantum cryptography without switching. Phys Rev Lett 93:170504