Bound on Noise of Coherent Source for Secure Continuous-Variable Quantum Key Distribution

Peng Huang, Guang-Qiang He & Gui-Hua Zeng

International Journal of Theoretical Physics

ISSN 0020-7748
Volume 52
Number 5

Int J Theor Phys (2013) 52:1572-1582
DOI 10.1007/s10773-012-1475-1

Springer

Int J Theor Phys (2013) 52:1572–1582
DOI 10.1007/s10773-012-1475-1

Bound on Noise of Coherent Source for Secure Continuous-Variable Quantum Key Distribution

Peng Huang · Guang-Qiang He · Gui-Hua Zeng

Received: 12 October 2012 / Accepted: 28 December 2012 / Published online: 10 January 2013

Abstract Coherent source of continuous-variable quantum key distribution (CV QKD) system may become noisy in practical applications. The security of CV-QKD scheme with the noisy coherent source is investigated under realistic conditions of quantum channel and detector. In particular, two models are proposed to characterize the noisy coherent source through introducing a party (Fred) who induces the noise with an optical amplifier. When supposing the party Fred is untrusted, two lower security bounds to the noise of the coherent source are derived for reverse reconciliation and realistic homodyne and heterodyne detections. While supposing Fred is a neutral party, we derive two tight security bounds without knowing Fred's exact state for ideal detections. Moreover, the simulation results show that the security of the reverse reconciliation CV-QKD protocols is very sensitive to the noise of coherent source for both the homodyne and heterodyne detections.

Keywords Security bound · Noisy coherent source · Continuous-variable quantum key distribution

1 Introduction

Quantum key distribution (QKD) [1–8] provides a novel way to allow two distant authorized parties, the sender Alice and the receiver Bob, to establish a secret key through quantum and classical channels. Different from the discrete-variable quantum key distribution (DV-QKD) protocols [1–4], in continuous-variable quantum key distribution (CV QKD) [4–8], Alice encodes information in the quadratures of optical field and Bob can decode the secret information with high-efficiency and high-speed homodyne [5, 6], or heterodyne detection [7, 8].

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61170228, 60970109, and 61102053).

P. Huang (✉) · G.-Q. He · G.-H. Zeng
State Key Laboratory of Advanced Optical Communication Systems and Networks,
Key Lab on Navigation and Location-based Service, Department of Electronic Engineering,
Shanghai Jiaotong University, Shanghai 200240, China
e-mail: huang_peng@sjtu.edu.cn

So CV-QKD schemes do not need single photon technology, and have prospect of high rate secure key distribution. Recently, several experimental CV-QKD schemes based on coherent states have been proposed [6, 8–10], and the unconditional security of CV-QKD with ideal optical source have been also studied theoretically [11–18]. The CV-QKD protocols based on coherent state with Gaussian modulation have been proved secure under collective and coherent attacks. Exactly, the security bounds for these two attacks are clarified to be coincident asymptotically by the quantum De Finetti theorem [4, 19].

For a practical CV-QKD system, the ignorance of its practical imperfections may limit Eve's attack strategy. Strictly speaking, the security bound should be reconsidered under more powerful attacks introduced by Eve, since the leakage of information from the loopholes of the imperfect practical QKD system is open to Eve. Recently, the security of the practical CV-QKD system has been analyzed [9, 20–27]. It has been found that adding noise in error correction may be benefit to increase the secret key rate [21], but the noise in coherent state preparation will deteriorate the security [22–26]. In particular, a three-mode entangle-state model [23] and a beam-splitter model [24] are proposed to characterize the noisy modulation of coherent states, where the beam-splitter model is similar to the realistic detector model [9] and the three-mode entangle-state model is under the assumption that the modulation noise is untrusted. From a practical viewpoint, it is more reasonable to consider that the modulation noise should be not controlled by the potential eavesdropper Eve. Thus, a neutral party model is proposed [25] to characterize the whole Gaussian source noise, where a neutral party Fred is introduced and a tighter security bound is derived. Moreover, Weedbrook *et al*. has shown that the security of direct reconciliation CV-QKD protocol is incredibly robust against significant amounts of excess preparation noise [26], and the optical parameter amplifier placed at the receiver's site can improve the secure key rate [27].

The previous considerations of imperfection of practical QKD system mainly focus on the modulation, and the noise originated from coherent state generator is neglected or has not been studied separately. In this paper, we explore the security of CV-QKD scheme with imperfect coherent source under realistic conditions of lossy and noisy quantum channel and detector. Specifically, we characterize the imperfect coherent source through introducing a party (Fred) who induces the noise with a practical phase-insensitive amplifier. According to the role of Fred, i.e., Fred being untrusted or neutral, two models are proposed to calculate the secret key rates of the reverse reconciliation CV-QKD protocol under the collective attack. When Fred is untrusted, lower bounds to the degree of the noise of coherent source is derived under realistic homodyne and heterodyne detection. While Fred is a neutral party, two tight bounds are obtained for ideal homodyne and heterodyne detection without knowing Fred's exact state. We find that the noise of coherent source will deteriorate the security of the reverse reconciliation CV-QKD protocol significantly for both the homodyne and heterodyne detections. It should be mentioned that, under the same conditions of modulation variance and quantum channel, the tight bound coincides with the main result in [26].

This paper is organized as follows. In Sect. 2, we introduce the models of prepare-and-measurement(P&M) and the equivalent entanglement-based (E-B) schemes. We calculate the secret key rates of the reverse reconciliation scheme, and derive the corresponding bounds to the noise of imperfect coherent source for homodyne and heterodyne detections, based on two models when supposing Fred is untrusted or neutral, in Sect. 3. Finally, conclusions are drawn in Sect. 4.

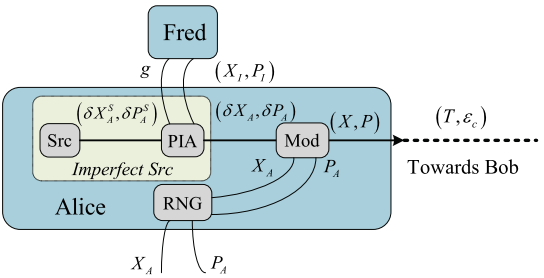

Fig. 1 The P&M scheme of a Gaussian coherent-state CV QKD protocol with imperfect coherent source. A random number generator (RNG) gives two values X_A and P_A. The signal state is generated by the imperfect source (Src) with shot noise $(\delta X_A, \delta P_A)$, which is then displaced in the phase space by using a Gaussian modulator (Mod) with (X_A, P_A). The gain g and idle input (X_I, P_I) is assumed to be individually induced by a third party, Fred

2 Model Description

In this section, we introduce the physical models of CV-QKD scheme with imperfect coherent source under study, i.e., prepare-and-measurement(P& M) and the equivalent entanglement-based (E-B) schemes. As known, for a standard P&M scheme, Alice encodes the key information, i.e., the generated two Gaussian random numbers X_A and P_A, with mean values of 0 and variances V_A, into the state $|X_A + iP_A\rangle$ by modulating an initial coherent state. Then, Alice sends the prepared states to Bob through a quantum channel with transmittance T and excess noise ε_c. At the receiver's site, Bob randomly chooses one quadrature to measure with homodyne detection [6], or measures both quadratures simultaneously with heterodyne detection [7]. Thus, Alice and Bob may share two correlated continuous variable strings. In the final step, Alice and Bob apply reconciliation procedure and privacy amplification to extract a private binary key string from the shared information. However, in a practical CV-QKD system, the coherent source before modulation may become imperfect and inevitably induce extra excess noise. We model this imperfect coherent source as a combination of a phase-insensitive amplifier (PIA) with gain g and idle input(X_I, P_I), and an ideal coherent source denoted by the quadratures $(\delta X_A^s, \delta P_A^s)$, which satisfy $\langle(\delta X_A^s)^2\rangle = \langle(\delta P_A^s)^2\rangle = 1$. The P&M model is depicted in Fig. 1.

The quadratures $(\delta X_A, \delta P_A)$ of imperfect coherent state can be described as

$$\begin{aligned} \delta X_A &= \sqrt{g}\delta X_A^s + \sqrt{g-1}\delta X_I, \\ \delta P_A &= \sqrt{g}\delta P_A^s + \sqrt{g-1}\delta P_I, \end{aligned} \tag{1}$$

where $g \geq 1$ is the gain of amplification, and (X_I, P_I) are the quadratures of the idler mode that is ideally in a vacuum state, or in a realistic state featuring a noise variance V_I. Therefore, the state sent to Bob can be denoted by quadratures (X, P) as

$$\begin{aligned} X &= X_A + \delta X_A, \\ P &= P_A + \delta P_A. \end{aligned} \tag{2}$$

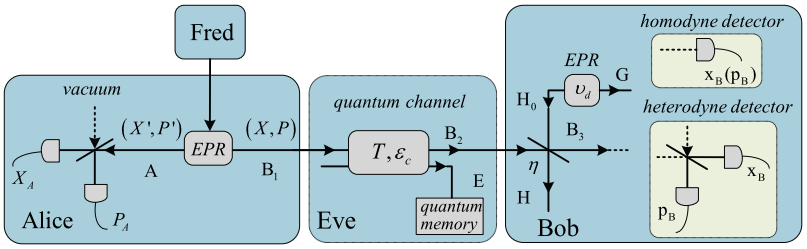

Fig. 2 The equivalent E-B scheme of the Gaussian coherent-state CV-QKD protocol with homodyne or heterodyne detections. Fred prepares state ρ_{AB} for Alice. The transmission efficiency T and excess noise ε_c are controlled by Eve

We obtain $\langle X^2\rangle = \langle P^2\rangle = V + \varepsilon_s$, where $V = V_A + 1$ and $\varepsilon_s = g - 1 + (g-1)V_I$. The conditional variances $V_{X|X_A} = V_{P|P_A}$ are given by

$$V_{X|X_A} = V_{P|P_A} = \langle X^2\rangle - \frac{\langle XX_A\rangle^2}{\langle X_A^2\rangle} = \varepsilon_s + 1. \tag{3}$$

For the convenience of security analysis, an equivalent E-B scheme is proposed in Fig. 2. Fred prepares a pair of Gaussian EPR beams ρ_{AB} and takes it purification. Thus, the global pure state shared by Alice, Bob and Fred can be denoted by $|\Psi_{ABF}\rangle$. Quadratures (X', P') and (X, P) denote the state kept by Alice and the one sent Bob, which satisfy

$$\langle X'^2\rangle = \langle P'^2\rangle = V, \qquad \langle X^2\rangle = \langle P^2\rangle = V + \varepsilon_s. \tag{4}$$

According to the uncertainty relationship [28], we get

$$|\langle XX'\rangle^2| \le V(V+\varepsilon_s) - \frac{V}{V+\varepsilon_s}. \tag{5}$$

Since the three-party system ABF may not be maximally entangled, the correlation between modes A and B_1 may not saturate the limit in Eq. (5). So it can be reasonably assumed that

$$\begin{aligned} \langle XX'\rangle &= \sqrt{V^2-1}, \\ \langle PP'\rangle &= -\sqrt{V^2-1}. \end{aligned} \tag{6}$$

In the E-B scheme, when Alice takes a heterodyne detection on X' and P' simultaneously, the measurement values of X' and P' can be expressed as

$$X'_A = X' - \delta X'_A, \qquad P'_A = P' - \delta P'_A, \tag{7}$$

where $\langle(\delta X'_A)^2\rangle = \langle(\delta P'_A)^2\rangle = 1$. Thus, Alice's estimate of (X, P), denoted by (X_A, P_A), satisfy

$$X_A = \sqrt{\frac{V-1}{V+1}}X'_A, \qquad P_A = -\sqrt{\frac{V-1}{V+1}}P'_A. \tag{8}$$

It can be easily calculated $\langle X_A^2\rangle = \langle P_A^2\rangle = V_A$, and $V_{X|X_A} = V_{P|P_A} = \varepsilon_s + 1$, which is the same as the P&M scheme. Therefore, when supposing the EPR source and Alice's detection

are hidden in the black box, Eve can not distinguish which scheme is applied, since the only outputs of the black box are the values of ε_s, X_A and P_A, and the state (X, P). The total channel-added noise referred to the channel input is expressed in shot noise units as $\chi_{line} = 1/T - 1 + \varepsilon_c + \varepsilon_s$.

When Bob receives the modulated quantum states, he takes homodyne or heterodyne detection. As shown in Fig. 2, a practical detector can be modeled by assuming that the quantum signal is attenuated by factor η and mixed with an added thermal noise ν_{el} due to the detector electronics, which can be modeled by an EPR state ρ_{H_0G} with variance ν_d. Also, we can define a detection-added noise for homodyne and heterodyne detection referred to Bob's input, which can be expressed in shot-noise units as $\chi_{hom} = (1 - \eta + \nu_{el})/\eta$ and $\chi_{het} = (2 - \eta + 2\nu_{el})/\eta$. The variance ν_d for homodyne and heterodyne detections are then correspondingly valued as $\nu_d^{hom} = \eta\chi_{hom}/(1-\eta)$ and $\nu_d^{het} = (\eta\chi_{het} - 1)/(1-\eta)$. Thus, the total noise referred to the channel input can then be expressed as $\chi_{thom} = \chi_{line} + \chi_{hom}/T$ and $\chi_{thet} = \chi_{line} + \chi_{het}/T$ for homodyne and heterodyne detection, respectively.

3 Security of the CV-QKD Scheme with Noisy Coherent Source

Since the P&M scheme and E-B scheme are equivalent for Alice, Bob, and the eavesdropper Eve, the secure key rate can be calculate in the E-B scheme. In the case of collective attack, she interacts individually with each pulse sent by Alice in the same way. So, the three-party global pure state becomes four-party state $|\Psi_{ABEF}\rangle$. In this section, we consider the homodyne and heterodyne detection cases in parallel for reverse reconciliation. So the raw key rate can be calculated as

$$K_R = I_{AB} - \chi_{BE}, \tag{9}$$

where I_{AB} is the Shannon mutual information between Alice and Bob, and χ_{BE} is the Holevo bound [29], which defines the maximum information available to Eve on Bob's key, with the form

$$\chi_{BE} = S(\rho_E) - \int dm_B\, p(m_B) S(\rho_E^{m_B}), \tag{10}$$

where m_B represents the measurements of Bob, and it takes the form $m_B = x_B$ or $m_B = x_B, p_B$ for homodyne or heterodyne detector, respectively. Also, $p(m_B)$ is the probability density of the measurement results, $\rho_E^{m_B}$ is the state of Eve's state conditional on Bob's measurement outcome, and $S(\rho)$ is the von Neumann entropy of the quantum state ρ. When using homodyne detection, the mutual information I_{AB}^{hom} can be derived from Bob's measured variance $V_B = \eta T(V + \chi_{thom})$ and the conditional variance $V_{B|A} = \eta T(1 + \chi_{thom})$ as

$$I_{AB}^{hom} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} = \frac{1}{2}\log_2 \frac{V + \chi_{thom}}{1 + \chi_{thom}}. \tag{11}$$

While for the heterodyne detection, two quadratures are measured, we get

$$I_{AB}^{het} = \log_2 \frac{V_B}{V_{B|A}} = \log_2 \frac{V + \chi_{thet}}{1 + \chi_{thet}}. \tag{12}$$

To calculate Eve's information χ_{BE}, we can use the fact that Eve's system purifies the system FAB_2, and Bob's measurement purifies the system FAEHG. Since $S(\rho_{FAHG}^{m_B})$ is

independent of m_B for Gaussian protocols, we get

$$\chi_{BE} = S(\rho_{FAB_2}) - S(\rho_{FAHG}^{m_B}). \tag{13}$$

In what follows, we calculate the key rate based on two models according to the role of Fred.

3.1 Untrusted Party Model

In this subsection, we suppose that Fred is an untrusted party, and his state can be controlled by Eve. This corresponds to the situation that Eve controls the noise of the coherent source. Thus, a lower bound of the secret key rate can be derived as

$$\tilde{K}_R = I_{AB} - \chi_{BEF}, \tag{14}$$

where I_{AB} represents the mutual information between Alice and Bob, and χ_{BEF} takes the form

$$\begin{aligned}\chi_{BEF} &= S(\rho_{AB_2}) - S(\rho_{AHG}^{m_B}) \\ &= \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right),\end{aligned} \tag{15}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, $\lambda_{1,2}$ are the symplectic eigenvalues of covariance matrix γ_{AB_2} characterizing state ρ_{AB_2}, and $\lambda_{3,4,5}$ are the symplectic eigenvalues of the covariance matrix $\gamma_{AHG}^{m_B}$ characterizing the state $\rho_{AHG}^{m_B}$ after Bob's measurement. The covariance matrix γ_{AB_2} does not depend on the type of detection. Easily, we obtain

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}], \tag{16}$$

where

$$\begin{aligned}A &= V^2 + 2T(1 - V^2) + T^2(V + \chi_{line})^2, \\ B &= T^2(1 + V\chi_{line})^2.\end{aligned} \tag{17}$$

The covariance matrix $\gamma_{AHG}^{m_B}$ can be calculated as

$$\gamma_{AHG}^{m_B} = \gamma_{AHG} - \sigma_{AHGB_3}^T H \sigma_{AHGB_3}, \tag{18}$$

where H is the symplectic matrix that represents the homodyne or heterodyne measurement on mode B_3. For homodyne case, $H_{hom} = (X\gamma_{B_3}X)^{MP}$ with $X = \left(\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right)$ and MP the Moore-Penrose pseudo-inverse of a matrix. While for heterodyne case, $H_{het} = (\gamma_{B_3} + \mathbb{I}_2)^{-1}$. We find that the symplectic eigenvalues $\lambda_{3,4}$ are given by

$$\lambda_{3,4}^2 = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}], \tag{19}$$

where for the homodyne detection,

$$\begin{aligned}C_{hom} &= \frac{A\chi_{hom} + V\sqrt{B} + T(V + \chi_{line})}{T(V + \chi_{thom})}, \\ D_{hom} &= \frac{\sqrt{B}V + B\chi_{hom}}{T(V + \chi_{thom})},\end{aligned} \tag{20}$$

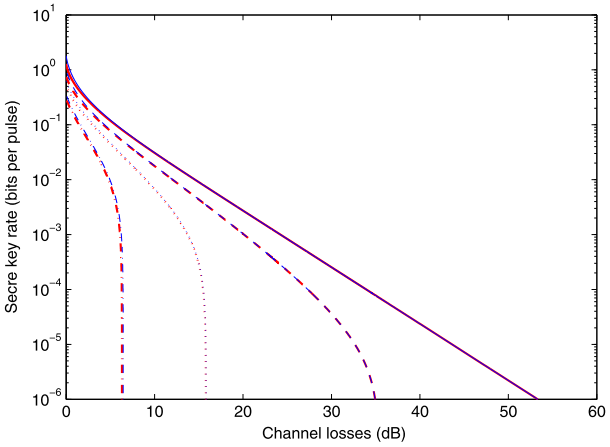

Fig. 3 $\tilde{K}_R^{hom}$ and $\tilde{K}_R^{het}$ as a function of the channel losses for reverse reconciliation and imperfect homodyne (*red thick lines*) and heterodyne (*blue thin lines*) detections. The *solid, dashed, dotted*, and *dot-dashed lines* represent the key rate for $g = 1$, 1.03, 1.06, and 1.1, respectively (Color figure online)

and for the heterodyne detection,

$$C_{het} = \frac{1}{[T(V+\chi_{thet})]}[A\chi_{het}^2 + B + 1 + 2\chi_{het}(V\sqrt{B} + T(V+\chi_{line})) + 2T(V^2-1)],$$
$$D_{het} = \left(\frac{V+\sqrt{B}\chi_{het}}{T(V+\chi_{thet})}\right)^2, \tag{21}$$

where A, B are given in Eq. (18). The last symplectic eigenvalue is $\lambda_5 = 1$ for both detections. Based on Eqs. (15–17) and Eqs. (19–21), we can calculate the Holevo information bound χ_{BEF}, and thus derive the secret key rate as $\tilde{K}_R^{hom}$ and $\tilde{K}_R^{het}$ from Eq. (14) for homodyne and heterodyne detections, respectively.

The secret key rates $\tilde{K}_R^{hom}$ and $\tilde{K}_R^{het}$ are plotted in Fig. 3. The parameters V_A, ε_c, η and v_{el} are fixed in the simulations to the values $V_A = 18.9$, $\varepsilon_c = 0.02$ (in shot-noise units), $\eta = 0.526$ and $v_{el} = 0.04361$ (in shot-noise units), which are practical in our CV-QKD experiment. The noise of the PIA V_I is set to 1. It can be seen that the homodyne and heterodyne detections take similar performance, and the security key rates for both detections are very sensitive to the noise of coherent source. The security bound to the noise of imperfect coherent source is weighted by the parameter g. The relationship between the secret key rates $\tilde{K}_R^{hom}$, $\tilde{K}_R^{het}$ and g are shown in Fig. 4 when transmission efficiency is $T = 0.268$, which corresponds to 27.2 km long optical fiber with loss coefficient of 0.21 dB/km . Also, we can obtain the lower bounds for homodyne and heterodyne detections as $g_{hom}^{u\dagger} = 1.104$ and $g_{het}^{u\dagger} = 1.105$, respectively. It should be mentioned that when assuming the homodyne and heterodyne detectors are perfect, the lower bounds are renewed as $g_{hom}^{u*} = 1.088$ and $g_{het}^{u*} = 1.090$, which are even lower than bounds $g_{hom}^{u\dagger}$ and $g_{het}^{u\dagger}$. It is because that the noise introduced by imperfect detector enhance the tolerable excess noise for RR schemes. This is quite coincident with result in [21] that adding some noise which is not controlled by Eve on the reference partner of the reconciliation could make the schemes more robust against noise. It can be easily understood that the additional noise affects the mutual information between Alice and Bob, and decreases more information eavesdropped by Eve on the final key.

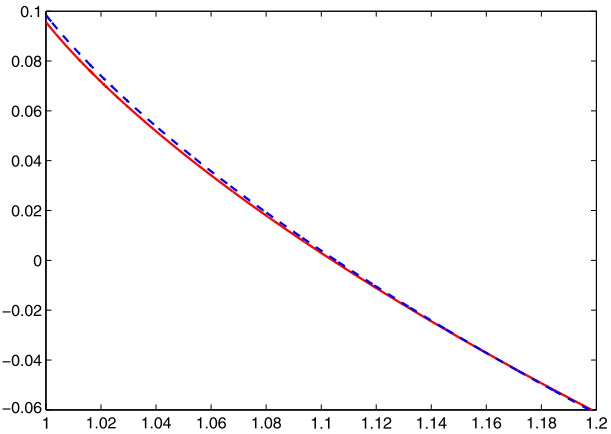

Fig. 4 $\tilde{K}_R^{hom}$ and $\tilde{K}_R^{het}$ as a function of the gain g for homodyne (*red solid line*) and heterodyne (*blue dashed line*) detections (Color figure online)

3.2 Neutral Party Model

From a practical viewpoint, the noise of the coherent source is originated from the physical imperfection of the apparatus, which is not controlled by the legitimated parties. Also, from the viewpoint of basic assumption in QKD, potential eavesdropper Eve has no access to the laboratories of the legitimate parties. So it is reasonable to consider the noise of the imperfect coherent source is just controlled by a third neutral party, Fred. To simplify the calculation, detector on Bob's side is assumed to be perfect in the followings. Thus, the mutual information between Alice and Bob in Eqs. (11) and (12) are simplified to

$$\begin{aligned} I_{AB}^{hom} &= \frac{1}{2}\log_2 \frac{V+\chi_{line}}{1+\chi_{line}}, \\ I_{AB}^{het} &= \log_2 \frac{T(V+\chi_{line})+1}{T(1+\chi_{line})+1}, \end{aligned} \tag{22}$$

and Eq. (13) can be rewritten as

$$\begin{aligned} \chi_{BE} &= S(\rho_{FAB_2}) - S(\rho_{FA}^{m_B}) \\ &= \sum_{i=1}^{3} G\left(\frac{\lambda_i'-1}{2}\right) - \sum_{i=4}^{5} G\left(\frac{\lambda_i'-1}{2}\right). \end{aligned} \tag{23}$$

The covariance matrix of purification of ρ_{FAB_2} would be expressed as

$$\gamma_{FAB_2} = \begin{pmatrix} F_{11} & F_{12} & F_{13} \\ F_{21} & (V+\varepsilon_s)\mathbb{I} & \sqrt{T[(V+\varepsilon_s)^2-1]}\sigma_z \\ F_{31} & \sqrt{T[(V+\varepsilon_s)^2-1]}\sigma_z & T(V+\chi_{line})\mathbb{I} \end{pmatrix}, \tag{24}$$

where each F_{ij} represents an unknown 2×2 matrix describing either F or its correlations with AB. Obviously, we can not calculate χ_{BE} through Eq. (24). However, there exists another Gaussian state ρ'_{FAB_2} with known covariance matrix γ'_{FAB_2}, which can be used to

obtain an upper bound of χ_{BE}. The covariance matrix γ'_{FAB_2} is in the form

$$\gamma'_{FAB_2} = \begin{pmatrix} \mathbb{I} & 0 & 0 \\ 0 & (V+\varepsilon_s)\mathbb{I} & \sqrt{T[(V+\varepsilon_s)^2-1]}\sigma_z \\ 0 & \sqrt{T[(V+\varepsilon_s)^2-1]}\sigma_z & T(V+\chi_{line})\mathbb{I} \end{pmatrix}. \tag{25}$$

Obviously, the reduced state $\rho'_{B_2} = \mathrm{Tr}_{FA}(\rho'_{FAB_2})$ is identical to the reduced state $\rho_{B_2} = \mathrm{Tr}_{FA}(\rho_{FAB_2})$, then ρ_{FAB_2} can be changed to ρ'_{FAB_2} through a unitary transformation U_{FA} on the system [30]. Thus, we get $S(\rho_{FAB_2}) = S(\rho'_{FAB_2})$. Similarly, we also find $S(\rho_{FA}^{m_B}) = S(\rho_{FA}^{\prime m_B})$. We then derive the symplectic eigenvalues of the covariance matrix γ'_{FAB_2} as

$$\lambda_{1,2}^{\prime 2} = \frac{1}{2}(A' \pm \sqrt{A'^2 - 4B'}), \lambda'_3 = 1, \tag{26}$$

where $A' = (V+\varepsilon_s)^2 - 2T[(V+\varepsilon_s)^2 - 1] + T^2(V+\chi_{line})^2$, and $B' = T^2[1 + (V+\varepsilon_s)(\chi_{line} - \varepsilon_s)]^2$. Also, the symplectic eigenvalues of the covariance matrix $\gamma_{FA}^{\prime m_B}$ for homodyne and heterodyne detections are given by

$$\lambda_4^{\prime hom} = \sqrt{\left[V + \varepsilon_s - \frac{(V+\varepsilon_s)^2 - 1}{V + \chi_{line}}\right](V+\varepsilon_s)}, \qquad \lambda_5^{\prime hom} = 1, \tag{27}$$

and

$$\lambda_4^{\prime het} = V + \varepsilon_s - \frac{T[(V+\varepsilon_s)^2 - 1]}{1 + T(V+\chi_{line})}, \qquad \lambda_5^{\prime het} = 1, \tag{28}$$

respectively. Therefore, the Holevo information χ_{BE} can be calculated from Eqs. (23) and (26–28), and thus we obtain the secret key rate in the neutral party model as K_R^{hom} and K_R^{het} for ideal homodyne and heterodyne detections, respectively.

The secret key rates K_R^{hom} and K_R^{het} as a function of the channel losses (measured in dB) are plotted in Fig. 5. The parameters V_A, V_I, ε_c are fixed the same as in the untrusted party model, and $\eta = 1$, $v_{el} = 0$ corresponding to the ideal detection. Obviously, it is shown in Fig. 5 that the security key rate is also very sensitive to the noise of coherent source in this

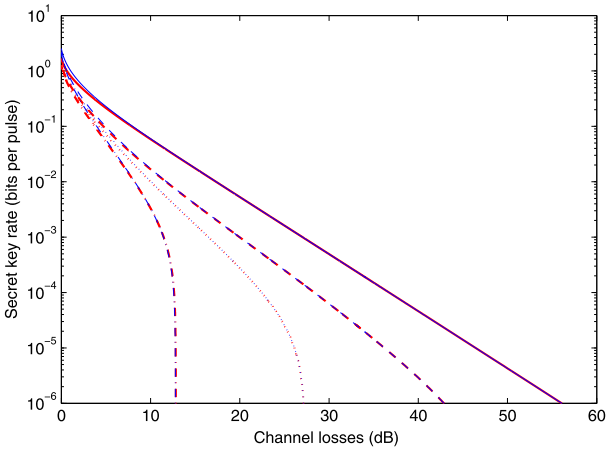

Fig. 5 K_R^{hom} and K_R^{het} as a function of the channel losses for reverse reconciliation and ideal homodyne (*red thick lines*) and heterodyne (*blue thin lines*) detections. The *solid, dashed, dotted*, and *dot-dashed lines* represent the key rate for $g = 1, 1.3, 1.35$, and 1.4, respectively (Color figure online)

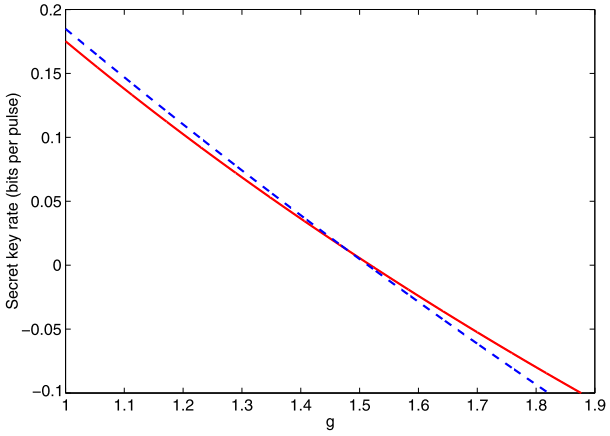

Fig. 6 K_R^{hom} and K_R^{het} as a function of the gain g for homodyne (*red solid line*) and heterodyne (*blue dashed line*) detections (Color figure online)

model. The relationship between K_R^{hom} and K_R^{het} and g are shown in Fig. 6 when transmission efficiency is $T = 0.268$. We then obtain the tight bounds for homodyne and heterodyne detections as $g_{hom}^{n*} = 1.585$ and $g_{het}^{n*} = 1.514$, respectively. It is quite reasonable that the tight bounds g_{hom}^{n*} and g_{het}^{n*} are higher than the corresponding lower bounds g_{hom}^{u*} and g_{het}^{u*}, since Eve captures less information in the neutral party model. It should be mentioned that, when we set the channel excess noise $\varepsilon_c = 0$ in high modulation variance ($V_A = 10^5$), the bound of g would be extremely high (larger than 500), which is quite coincident with the previous research result in [26]. Exactly, the bound in [26] is calculated under the consideration that Eve performing a given collective Gaussian attack, i.e., the entangling cloner attack [28]. So this coincidence demonstrates the efficiency of the entangling cloner attack in collective Gaussian attacks. Also, the bounds to the noise of the imperfect coherent source will be also significant large when the modulation variance is a proper value, such as $V_A = 18.9$, for $\varepsilon_c = 0$. Therefore, it can be concluded that the excess noise ε_c of the quantum channel is the crucial parameter, which affects the toleration of noise of coherent source, for the reverse reconciliation CV QKD schemes.

4 Summary and Conclusions

We have investigated the security of CV-QKD scheme with imperfect coherent source, lossy and noisy quantum channel, and realistic detector. In particular, we model the imperfect coherent source by an ideal coherent source and an optical amplifier which is controlled by a third party Fred. And then we propose two models, i.e., the untrusted and neutral party model, to calculate the secret key rates when supposing Fred is an untrusted or neutral party, correspondingly. When Fred is untrusted, we derive two lower bounds $g_{hom}^{u\dagger}$ (g_{hom}^{u*}) and $g_{het}^{u\dagger}$ (g_{het}^{u*}) to the noise of the imperfect coherent source under reverse reconciliation and imperfect (perfect) homodyne and heterodyne detections. While Fred is neutral, we derive two tight security bounds g_{hom}^{n*} and g_{het}^{n*} without knowing the exact state of Fred for ideal detections. The simulation results show that the security of the reverse reconciliation CV-QKD protocol is very sensitive to the noise of coherent source for both homodyne and heterodyne detection. Due to the different roles of Fred, the simulations demonstrate that g_{hom}^{n*} and g_{het}^{n*} are reasonably higher than g_{hom}^{u*} and g_{het}^{u*}. Moreover, we show that the security bounds g_{hom}^{n*} is coincident with the previous studies.

References

1. Bennett, C.H., Brassard, G.: In: Proceedings of IEEE International Conference Computers, System and Signal Processing, pp. 175–179. IEEE, New York (1984)
2. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Rev. Mod. Phys. **74**, 145 (2002)
3. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: Rev. Mod. Phys. **81**, 1301 (2009)
4. Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N.J., Ralph, T.C., Shapiro, J.H., Lloyd, S.: arXiv:1110.3234 (2011)
5. Grosshans, F., Grangier, P.: Phys. Rev. Lett. **88**, 057902 (2002)
6. Grosshan, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N.J., Grangier, P.: Nature **421**, 238 (2003)
7. Weedbrook, C., Lance, A.M., Bowen, W.P., Symul, T., Ralph, T.C., Lam, P.K.: Phys. Rev. Lett. **93**, 170504 (2004)
8. Lance, A.M., Symul, T., Sharma, V., Weedbrook, C., Ralph, T.C., Lam, P.K.: Phys. Rev. Lett. **95**, 180503 (2005)
9. Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N.J., Tuallebrouri, R., McLaughlin, S.W., Grangier, P.: Phys. Rev. A **76**, 042305 (2007)
10. Qi, B., Huang, L.L., Qian, L., Lo, H.K.: Phys. Rev. A **76**, 052323 (2007)
11. Grosshans, F.: Phys. Rev. Lett. **94**, 020504 (2005)
12. Navascués, M., Acín, A.: Phys. Rev. Lett. **94**, 020505 (2005)
13. Lodewyck, J., Debuisschert, T., Tualle-Brouri, R., Grangier, P.: Phys. Rev. A **72**, 050303(R) (2005)
14. García-Patrón, R., Cerf, N.J.: Phys. Rev. Lett. **97**, 190503 (2006)
15. Navascués, M., Grosshans, F., Acín, A.: Phys. Rev. Lett. **97**, 190502 (2006)
16. Pirandola, S., Braunstein, S.L., Lloyd, S.: Phys. Rev. Lett. **101**, 200504 (2008)
17. Leverrier, A., Grangier, P.: Phys. Rev. Lett. **102**, 180504 (2009)
18. Leverrier, A., Grangier, P.: Phys. Rev. Lett. **106**, 259902(E) (2011)
19. Renner, R., Cirac, J.I.: Phys. Rev. Lett. **102**, 110504 (2009)
20. Leverrier, A., Grosshans, F., Grangier, P.: Phys. Rev. A **81**, 062343 (2010)
21. García-Patrón, R., Cerf, N.J.: Phys. Rev. Lett. **102**, 130501 (2009)
22. Filip, R.: Phys. Rev. A **77**, 022310 (2008)
23. Shen, Y., Yang, J., Guo, H.: J. Phys. B **42**, 235506 (2009)
24. Usenko, V.C., Filip, R.: Phys. Rev. A **81**, 022318 (2010)
25. Shen, Y., Peng, X., Yang, J., Guo, H.: Phys. Rev. A **83**, 052304 (2011)
26. Weedbrook, C., Pirandola, S., Lloyd, S., Ralph, T.C.: Phys. Rev. Lett. **105**, 110501 (2010)
27. Fossier, S., Diamanti, E., Debuisschert, T., Tualle-Brouri, R., Grangier, P.: J. Phys. B **42**, 114014 (2009)
28. Grosshans, F., Cerf, N.J., Wenger, J., Tualle-Brouri, R., Grangier, P.: Quantum Inf. Comput. **3**, 535 (2003)
29. Holevo, A.S.: Probl. Inf. Transm. **9**, 177 (1973)
30. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum information. Cambridge University Press, Cambridge (2000)