Improvement of two-way continuous-variable quantum key distribution using optical amplifiers

Yi-Chen Zhang\textsuperscript{1,5}, Zhengyu Li\textsuperscript{2}, Christian Weedbrook\textsuperscript{3,4}, Song Yu\textsuperscript{1}, Wanyi Gu\textsuperscript{1}, Maozhu Sun\textsuperscript{2}, Xiang Peng\textsuperscript{2} and Hong Guo\textsuperscript{2}

\textsuperscript{1} State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, People’s Republic of China
\textsuperscript{2} State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics Engineering and Computer Science and Center for Quantum Information Technology, Peking University, Beijing 100871, People’s Republic of China
\textsuperscript{3} Department of Physics, University of Toronto, Toronto, MSS 3G4, Canada
\textsuperscript{4} QKD Corp., 112 College St., Toronto, M5G 1L6, Canada

E-mail: yusong@bupt.edu.cn and hongguo@pku.edu.cn

Received 12 August 2013, revised 28 November 2013
Accepted for publication 10 December 2013
Published 21 January 2014

Abstract

The imperfections of a receiver’s detector affect the performance of two-way continuous-variable (CV) quantum key distribution (QKD) protocols and are difficult to adjust in practical situations. We propose a method to improve the performance of two-way CV-QKD by adding a parameter-adjustable optical amplifier at the receiver. A security analysis is derived against a two-mode collective entangling cloner attack. Our simulations show that the proposed method can improve the performance of protocols as long as the inherent noise of the amplifier is lower than a critical value, defined as the tolerable amplifier noise. Furthermore, the optimal performance can approach the scenario where a perfect detector is used.

Keywords: quantum key distribution, continuous variable, two-way quantum key distribution

1. Introduction

Quantum key distribution (QKD) \cite{1, 2} is one of the most practical applications in the field of quantum information. Its goal is to establish a secure key between two legitimate partners, usually called Alice and Bob. Continuous-variable QKD (CV-QKD) \cite{3} has attracted much attention in the past few years \cite{2–4} mainly because it only uses standard telecom components. A CV-QKD protocol based on coherent states \cite{5, 6} with Gaussian modulation has been experimentally demonstrated \cite{4, 7–9} and has been shown to be secure against arbitrary collective attacks \cite{10, 11}. Such an attack is the most optimal in the asymptotical limit \cite{12} and is also used in the finite-size regime \cite{13, 14}.

To enhance the tolerable excess noise of CV-QKD, compared to the typical one-way schemes, the two-way CV-QKD was proposed \cite{15}. Recently, a more feasible two-way CV-QKD protocol was proposed by replacing Alice’s displacement operation with a beam splitter and inserting thermal noise into it. This leads to a protocol that is easier to analyse when considering channel estimation \cite{16}.

In practice, the detector’s imperfections, mainly characterized by the detection efficiency and electronic noise, will affect the performance of two-way CV-QKD protocols and are hard to adjust in an experiment \cite{4, 9}. In this paper, we insert an optical amplifier before Bob’s detection by which the receiver’s efficiency and noise can be optimized to improve the performance of two-way CV-QKD protocols using reverse reconciliation. Previously, a similar method had only been analysed for the case of one-way \cite{17} and
one-way four-state [18] reverse reconciliation schemes. Using numerical simulations, we propose a specific two-mode collective entangling cloner attack as Eve’s action.

The paper is organized as follows. In section 2, we review the two-way CV-QKD protocols with imperfect detectors and describe the extended model of the detector. In section 3, we first analyse the different optical amplifier models and their suitable scopes of application. Then we derive security bounds of the protocols with different optical amplifiers. Finally, the simulation results under collective entangling cloner attack of the protocols with and without the amplifiers. Our conclusions are drawn in section 4.

2. Security analysis of two-way CV-QKD protocols with imperfect detector

In the following, we first review the basic notions of the entanglement-based model related to the Gaussian-modulated two-way CV-QKD protocols with imperfect detection [16, 19]. The entanglement-based model with imperfect detectors is illustrated in figure 1 and can be described as follows.

Step 1: Bob initially prepares an EPR pair (EPR1 with variance \( V_B \)). He keeps one mode \( B_1 \) and sends the other mode \( B_2 \) to Alice through the channel where Eve may perform her attack.

Step 2: Alice prepares another EPR pair (EPR2 with variance \( V_A \)). She keeps mode \( A_1 \) and measures it using heterodyne detection to obtain the variables \( x_{A_1} \) and \( \eta_{A_1} \). The modes \( A_0 \) and \( B_0 \) represent the vacuum state. She then couples mode \( A_2 \) and the received mode \( A_{in} \) from Bob with a beam splitter (transmittance: \( T_A \)). Alice then sends mode \( A_{out} \) back to Bob and measures another mode \( A_3 \) with homodyne detection for parameter estimation [16].

Step 3: Bob measures his original mode \( B_1 \) using heterodyne detection to obtain the variables \( x_{B_1} \) and \( \eta_{B_1} \). He also measures the received mode \( B_2 \) with homodyne detection to obtain \( x_{B_2} \) or with heterodyne detection to obtain \( x_{B_5} \) and \( \eta_{B_5} \). The detector’s inefficiency is modelled by a beam splitter with transmittance \( \eta \), while its electronic noise \( \nu_{el} \) is modelled by a thermal state \( \rho_{B_5} \) with variance \( \nu \) [4].

Step 4: when Bob uses homodyne detection, he uses \( x_{B_2} = x_{B_5} - k\eta_{B_5} \) (\( \rho_{B_5} = \rho_{B_5} - k\eta_{B_5}/(1-\eta) \)) to construct the estimator to Alice’s corresponding variable \( x_{A_3} \) (\( \rho_{A_3} \)), where \( k \) is the parameter used to optimize Bob’s estimator of Alice’s corresponding value. When Bob uses heterodyne detection, he uses a similar way to construct the estimators (\( x_{B_5} = x_{B_5} - k\eta_{B_5} \), \( \rho_{B_5} = \rho_{B_5} - k\eta_{B_5}/(1-\eta) \)) to \( (x_{A_3}, \rho_{A_3}) \) at the same time. Then Alice and Bob proceed with classical data postprocessing namely reconciliation and privacy amplification. In this paper, we use reverse reconciliation [7].

In order for Alice and Bob to perform their measurement, Bob initially sends a local oscillator with the signal beam to Alice, then Alice couples it with the local oscillator from her and sends back to Bob with the signal beam. The variance \( \nu \) of the thermal state \( \rho_{B_5} \) is chosen to obtain the appropriate expression for each detection in the following way: for homodyne detection, \( \nu = 1 + \nu_{el}/(1-\eta) \) and for heterodyne detection, \( \nu = 1 + 2\nu_{el}/(1-\eta) \) [9]. Adjusting the efficiency \( \eta \) and the variance \( \nu \), we can optimize the performance of the protocols. For instance, the performance of two-way CV-QKD can be improved by adding noise in homodyne detection [19]. Unfortunately, for a practical detector, the detection efficiency \( \eta \) and electronic noise \( \nu \) are fixed between \( B_3 \) and \( B_5 \) (see figure 1) and generally speaking, they are not the optimal choice. To improve the performance of the protocols, we can insert an adjustable operation with ancilla \( \rho_{B_3} \) before detection, noted as the pre-process (see figure 2). Therefore the pre-process phase and the imperfections of the detector constitute a new receiver, whose efficiency and noise can be optimized to improve the performances of the two-way schemes.

---

**Figure 1.** Entanglement-based scheme of Gaussian-modulated two-way CV-QKD protocols with imperfect homodyne or heterodyne detection where the quantum channel is fully controlled by Eve. However, Eve has no access to the apparatuses in Alice’s and Bob’s stations.

**Figure 2.** The receiver model which consists of a pre-process phase and the imperfections of detector with the ancillas \( \rho_{B_3} \) and \( \rho_{B_5} \), respectively.
3. Improvement of two-way CV-QKD protocols with optical amplifiers

In this section, we present two kinds of optical amplifier models [17, 18, 20]: a perfect phase-sensitive amplifier (PSA) and a practical phase-insensitive amplifier (PIA) as the pre-process to improve the performances of homodyne and heterodyne detection two-way CV-QKD protocols, respectively. Simulation results against a two-mode collective entangling cloner attack are provided to compare the performances of the protocols with and without the amplifiers.

3.1. Homodyne detection with PSA

A PSA is a degenerate optical parametric amplifier, which permits noiseless amplification of a chosen quadrature (̂x or ̂p) [20]. Its mathematical model can be described by the transformation matrix \( Y_{PSA} \)

\[
\begin{pmatrix}
\hat{x}
\end{pmatrix}_{out} = \begin{pmatrix}
\sqrt{g} & 0
\end{pmatrix} \cdot \begin{pmatrix}
\hat{x}
\end{pmatrix}_{in} = Y_{PSA} \cdot \begin{pmatrix}
\hat{x}
\end{pmatrix}_{in},
\]

(1)

where \( g > 1 \) is the gain of the optical amplifier, \( g = 1 \) means the optical amplifier does nothing.

We now derive the security bound of the two-way CV-QKD protocol with homodyne detection adding a PSA before detection at the receiver (see figure 3(a)). When Alice and Bob use reverse reconciliation, the secret key rate is given by

\[
K = \beta I(a : b) - S(b : E),
\]

(2)

where \( \beta \in [0, 1] \) is the reconciliation efficiency, \( I(a : b) \) is the classical mutual information between Alice and Bob and \( S(b : E) \) is the quantum mutual information between Bob and Eve. The classical mutual information between Alice and Bob can be written as

\[
I(a : b) = \frac{1}{2} \log V_{A_x} - \frac{1}{2} \log V_{A_i | b_i},
\]

(3)

where \( V_{A_x} = \frac{1}{2} (V_{A} + 1), V_{A_i | b_i} \) is the variance of mode \( A_i \) conditioned on Bob’s data, and Bob using \( x_{B_x} = x_{B_i} - k x_{B_i} \), as his final data. The state Bob obtains after total channels is

\[
\hat{B}_B = \sqrt{\eta g T_A T_2} \hat{B}_A + \sqrt{1 - T_2} \eta g \hat{A}_2 + \sqrt{1 - \eta} \hat{F}_1 + \hat{E},
\]

(4)

where \( \hat{E} \) represents the total excess noise introduced by Eve. Bob uses \( x_{B_x} \) and \( x_{B_i} \) to construct his estimator of Alice’s variable \( x_{A_x} \), \( x_{B_x} = x_{B_i} - k x_{B_i} \), where \( x_{B_x}, x_{B_i}, \) and \( x_{A_x} \) are the measurement results of the modes \( \hat{B}_B, \hat{B}_i, \) and \( \hat{A}_1 \). To make Bob’s estimator as precise as possible, he chooses a value of \( k \) to reduce the interference from \( \hat{B}_2 \), specifically minimizing the variance of \( x_{B_x} \)

\[
k = \sqrt{2 \eta g T_A T_2 \left( \frac{V_B}{V_B + 1} \right)}.
\]

(5)

The maximum information available to Eve on Bob’s raw key is bounded by the Holevo bound [23]

\[
S(b : E) = S(\rho_E) - \int p(x_B) S(\rho_E^{x_B}) \, dx_B,
\]

(6)

where \( p(x_B) \) is the probability density function of the measurement output, \( \rho_E^{x_B} \) is the eavesdropper’s state conditioned on Bob’s measurement result \( x_B \) and \( S(\rho) \) is the von Neumann entropy of the quantum state \( \rho \).

To calculate \( \chi_{BE} \), we first have \( S(\rho_A, A_i | B_i) = S(\rho_E) \) since Eve can purify Alice and Bob’s system \( A_i A_j B_i B_j \). Second, after Bob’s projective measurement resulting in \( x_B \), the system \( A_i A_j B_i B_j E F \) is pure, so that \( S(\rho_E^{x_B}) = S(\rho_{E}^{x_B}) \), where \( S(\rho_{x_B}^{E}) \) is independent of \( x_B \) for protocols applying Gaussian modulation of Gaussian states. Thus, \( \chi_{BE} \) becomes

\[
\chi_{BE} = S(\rho_{x_B}^{E})
\]

(7)

The entropies \( S(\rho_{x_B}^{E}) \) and \( S(\rho_{x_B}^{E}) \) can be calculated using the covariance matrices \( \Gamma_{A_i A_j B_i B_j} \), characterizing the state \( \rho_{x_B}^{E} \), and \( \Gamma_{A_i A_j B_i B_j} \), characterizing the state \( \rho_{x_B}^{E} \). So the expression for \( \chi_{BE} \) can be further simplified as follows:

\[
\chi_{BE} = \sum_{i=1}^{4} G \left( \lambda_i - \frac{1}{2} \right) - \sum_{i=5}^{10} G \left( \lambda_i - \frac{1}{2} \right),
\]

(8)

where \( G(x) = (x + 1) \log_2 (x + 1) - x \log_2 x, \lambda_{1-4} \) are the symplectic eigenvalues of the covariance matrix \( \Gamma_{A_i A_j B_i B_j} \) and \( \lambda_{5-10} \) are the symplectic eigenvalues of the covariance matrix \( \Gamma_{A_i A_j B_i B_j} \). After Alice and Bob measure the mode \( A_i \) with imperfect homodyne detection, CNOT gate can be seen as one symplectic transformation between \( \rho_{A_i A_j B_i B_j}^{E} \) and \( \rho_{A_i A_j B_i B_j}^{E} \), thus \( S(\rho_{A_i A_j B_i B_j}^{E}) = S(\rho_{A_i A_j B_i B_j}^{E}) = S(\rho_{A_i A_j B_i B_j}^{E}) = S(\rho_{A_i A_j B_i B_j}^{E}) \).

6 The models we build for PSA, imperfections of homodyne detector and CNOT gate can be seen as one symplectic transformation between \( \rho_{A_i A_j B_i B_j}^{E} \) and \( \rho_{A_i A_j B_i B_j}^{E} \), thus \( S(\rho_{A_i A_j B_i B_j}^{E}) = S(\rho_{A_i A_j B_i B_j}^{E}) = S(\rho_{A_i A_j B_i B_j}^{E}) = S(\rho_{A_i A_j B_i B_j}^{E}) \).
heterodyne detection and measure the modes $A_3$, $B_3$, $B_4$, and $B_6$ with homodyne detection in figures 1 and 3(a), we can obtain the covariance matrices $\gamma_{A_3A_1B_1}$ and $\gamma_{A_3B_3B_4}^{xx}$ in the experiment. However, in numerical simulation, we could not have the measurement results and we need the specific description of Eve’s attack [16, 19] to help us to obtain the final data to calculate the covariance matrices $\gamma_{A_3A_1B_1}$ and $\gamma_{A_3B_3B_4}^{xx}$, which we will describe in the later section 3.3 in detail.

3.2. Heterodyne detection with PIA

A PIA is a nondegenerate optical parametric amplifier, which amplifies both quadratures [20]. However, the amplification process is associated with a fundamental excess noise. As described by a noiseless amplifier whose transformation is entering the amplifier’s second input port

$$[\hat{B}_4] = \begin{bmatrix} \sqrt{g} \cdot I_2 & \sqrt{g - 1} \cdot \sigma_c \\ \sqrt{g - 1} \cdot \sigma_c & \sqrt{g} \cdot I_2 \end{bmatrix} \begin{bmatrix} \hat{B}_3 \\ \hat{l}_0 \end{bmatrix} = Y_{\text{PLA}} \begin{bmatrix} \hat{B}_3 \\ \hat{l}_0 \end{bmatrix}.$$ (9)

The EPR state of variance $N$ is used to represent the inherent noise of the amplifier and its covariance matrix is given by

$$\gamma_{ij} = \begin{bmatrix} N \cdot I_2 & \sqrt{N^2 - 1} \cdot \sigma_c \\ \sqrt{N^2 - 1} \cdot \sigma_c & N \cdot I_2 \end{bmatrix}.$$ (10)

We can now derive the security bound of the two-way CV-QKD protocol with heterodyne detection when adding a PIA at the receiver’s device. For the heterodyne detection, Bob uses $x_{B_4} = x_{B_6} - k x_{B_6}$ and $p_{B_4} = p_{B_6} - k p_{B_6}$ to construct the optimal estimator to Alice’s corresponding variables $x_A$ and $p_{A_3}$, where $k = (\eta g T_A T_T E_2 (V_B - 1) / (V_B + 1))$ for heterodyne detection to reduce the interference from $\hat{B}_2$, specifically minimizing the variance of $x_{B_6}$. We can use the same method to calculate the classical mutual information between Alice and Bob. The information Eve has is again given by equation (8) and the first part of it remains unchanged. But for the second part of it, we need to add modes $I_0$ and $J$ to represent the inherent noise of the amplifier in this case. Then, $\chi_{B}$ is calculated from the following equations:

$$\chi_{BE} = S(\rho_{A_3A_1B_1}) - S(\rho_{A_3A_1JFGB_1})$$

$$= \sum_{i=1}^{4} G(\frac{\gamma_i - 1}{2}) - \sum_{i=5}^{12} G(\frac{\gamma_i - 1}{2}).$$ (11)

Therefore, it is necessary to derive the covariance matrix $\gamma_{A_3A_1JFGB_1}$, which we can obtain after measuring the mode $A_1$ with heterodyne detection and measuring the modes $A_3$, $B_6$, $B_4$, $B_1$, and $B_6$ with homodyne detection as figures 1 and 3(b) show.

3.3. Simulation and discussion

As discussed above, we need the specific description of Eve’s attack to help us to obtain the final data to calculate the covariance matrices $\gamma_{A_3A_1B_1}$, $\gamma_{A_3A_1B_3B_4}^{xx}$, and $\gamma_{A_3A_1JFGB_1}$, for doing the numerical simulation. In the two-way protocol, the two-mode attack is more general and is used as Eve’s attack (see figure 4). Although the two-mode entangling cloner attack has not been proven to be the optimal attack against the two-way protocol, such an attack is the most practical benchmark to test two-way CV-QKD systems thus far in the literature [16, 19] and we again employ it here. Eve first prepares an EPR pair (EPR3 with variance $V_E$), she keeps mode $E_1$ and splits mode $E_2$ into $E_3$ and $E_5$ with a beam splitter whose transmittance is $T_E$. $E_3$ and $E_5$ are the modes introduced into the channels. $T_1$ and $T_2$ are the channel transmission efficiencies. Here we use $T = T_1 = T_2 = 10^{-a/10}$ for calculations and simulations, where $a = 0.2$ dB km$^{-1}$ is the loss coefficient of the optical fibres and $d$ is the length of the quantum channel.

![Figure 4](image-url)

Figure 4. The entanglement-based scheme of two-way CV-QKD protocols against a specific two-mode attack where Eve prepares an EPR pair (EPR3 with variance $V_E$), she keeps mode $E_1$ and splits mode $E_2$ with a beam splitter whose transmittance is $T_E$. $E_3$ and $E_5$ are the modes introduced into the channels. $T_1$ and $T_2$ are the channel transmission efficiencies. Here we use $T = T_1 = T_2 = 10^{-a/10}$ for calculations and simulations, where $a = 0.2$ dB km$^{-1}$ is the loss coefficient of the optical fibres and $d$ is the length of the quantum channel.

The parameters affecting the value of the secret key rate are the reconciliation efficiency $\beta$, the variance of Alice’s and Bob’s modulation: $(V_A - 1)$ and $(V_B - 1)$, the transmittance of the beam splitter at Alice’s side $T_A$, the transmission efficiency $T$, the efficiency $\eta$ and the electronic noise $\nu_0$ of the detector. The parameters $V_A$, $V_B$, $\beta$, $\eta$, and $\nu_0$ are fixed in all simulations. The variance $V_A = V_B = 40$ which allows for the reconciliation efficiency of $\beta = 0.948$, $\epsilon = 0.02$, $\eta = 0.552$ and $\nu_0 = 0.015$, which are standard in one-way CV-QKD experiments [4]. We choose $T_A = 0.4$ as the value of the beam splitter transmittance at Alice’s side and different levels of channel noise $\epsilon = 0.005, 0.02, 0.2$.

Firstly, we consider the performance of an imperfect homodyne detector with a PSA placed at the output of the quantum channel. We calculate the secret key rate $K$ as a
Figure 5. A comparison among the secret key rates under the following situations: no amplifier ($g = 1$), using a phase sensitive amplifier whose gain is 2 or 15 with an imperfect homodyne detector ($\eta = 0.552, \nu_d = 0.015$), and no amplifier with a perfect homodyne detector ($\eta = 1$) under different levels of channel noise: (a) $\varepsilon = 0.005$, (b) $\varepsilon = 0.02$, (c) $\varepsilon = 0.2$. The reconciliation efficiency $\beta$ is 0.948 [4].

Figure 6. A comparison among the secret key rates under the following situations: no amplifier ($g = 1$), using a phase insensitive amplifier whose gain is 2 or 15 with an inherent noise of 1 or 1.5 with an imperfect heterodyne detector ($\eta = 0.552, \nu_d = 0.015$), and no amplifier with a perfect heterodyne detector ($\eta = 1$) under different levels of channel noise: (a) $\varepsilon = 0.005$, (b) $\varepsilon = 0.02$, (c) $\varepsilon = 0.2$. The reconciliation efficiency $\beta$ is 0.948 [4].

The simulation results are shown in figure 5, where we find that the larger the amplification gain of the PSA, the higher the secret key rate and the longer the secure transmission distance we can achieve. We also calculate the secret key rate under perfect homodyne detection for comparison. Then we find that the new transformation of inserting a PSA at the receiver can enhance the performance of the protocol with imperfect homodyne detection under different levels of channel noise. The optimal improvement of the proposed method can approach the performances of the protocol with a perfect homodyne detector.

Secondly, we consider the performance of an imperfect heterodyne detector with a PIA placed at the output of the quantum channel. We also calculate the secret key rate under the same three situations. Additionally, we take the inherent noise of the PIA into account. The inherent noise $N$ of the PIA is set to either 1 for minimal noise (vacuum noise) or to a more realistic value 1.5 (referred to the input) [17]. These results are shown in figure 6. We observe that the performance of the two-way CV-QKD protocol with imperfect heterodyne detection is improved by inserting a PIA at the output of the quantum channel under different levels of channel noise. The protocol under large amplification and vacuum noise gives the highest key rate, which can approach the secret key rate of a perfect heterodyne detector. It is shown that the larger the amplification gain and the smaller the noise of PIA, the higher the secret key rate and the longer the secure transmission distance we can achieve. Certainly, for a practical PIA, the noise will not be as low as the vacuum noise. Therefore, in the practical system, it is important to know the tolerable PIA noise which means the most inherent noise of the PIA that the protocol can tolerate. Furthermore, the tolerable PIA noise is also the point that the method does not work.

As illustrated in figure 7(a), we calculate the secret key rate as a function of the inherent noise of the PIA with constant gain ($g = 15$) for a certain fixed distance ($d = 60$ km) and channel noise ($\varepsilon = 0.02$) of the protocol. We observe that the secret key rate decreases as the noise of PIA increases and a reference line is drawn to represent the key rate of imperfect heterodyne detection without PIA. Above the reference line, the performance of the protocol is improved by using a PIA. Therefore, when the transmission distance is 60 km, the critical value of the inherent noise of the PIA is 2.678 which we define as tolerable PIA noise. With the method to calculate the tolerable PIA noise under a fixed gain coefficient and transmission distance, we can draw a picture of the tolerable PIA noise over the gain of the PIA and the transmission distance (see figure 7(b)). The performance of the two-way CV-QKD protocol with imperfect heterodyne detection can be improved by placing a PIA at the output of the quantum channel, whose noise should be less than the tolerable PIA noise. From figure 7(b), the tolerable PIA noise is constant with transmission distance less than the maximal distance the protocol without a PIA can achieve (e.g. 63.13 km for $g = 15$).
This is because the tolerable PIA noise only depends on the detector’s electronic noise $\nu_d$ in this model [17, 18]. After the maximal distance the protocol without a PIA can achieve, the tolerable PIA noise decreases and finally reaches 1 (the minimal noise of PIA), which represents the maximal distance the protocol without a PIA can achieve (e.g. 71.55 km for $g = 15$). To improve the performance of the protocol by inserting a PIA, the inherent noise of the PIA needs to be below the tolerable amplifier noise for a fixed gain coefficient and the transmission distance.

4. Conclusion

The imperfections of a detector can affect the performance of two-way continuous-variable quantum key distribution protocols and are hard to adjust experimentally. In this paper, we propose a method to improve the performance of two-way continuous-variable QKD protocols by adding an adjustable optical amplifier at the output of the quantum channel, which combined with the fixed imperfect detector can be seen as an adjustable receiver. Here, we present two kinds of optical amplifier models, a phase-sensitive amplifier and a phase-insensitive amplifier, to improve the performances of homodyne detection and heterodyne detection two-way continuous-variable QKD protocols, respectively. The simulation results against a two-mode collective entangling cloner attack show that for homodyne detection, the optimal performance of adding a phase-sensitive amplifier at the receiver can approach the case of using a perfect detector. On the other hand, for heterodyne detection, the optimal performance of adding a phase-insensitive amplifier at the receiver can also approach the case of using a perfect detector. We note that the proposed methods can improve the performance of protocols as long as the inherent noise of the amplifier is lower than the critical value which we define as the tolerable amplifier noise.

Acknowledgments

This work is supported by the National Basic Research Program of China (973 Program) under grant 2012CB315605 and 2014CB340102, the National Science Fund for Distinguished Young Scholars of China under grant 61225003, the National Natural Science Foundation under grant 61101081, 61271191 and 61271193, and the Fundamental Research Funds for the Central Universities. CW would like to thank NSERC for support.

Appendix. Detailed calculation of parameter $TE$, covariance matrices and symplectic eigenvalues

Here we give the detailed calculation of parameter $TE$, the covariance matrices $\gamma_{A_1 B_1 B_2}$, $\gamma_{A_2 B_1 B_2 E F G}$ and $\gamma_{A_1 A_2 J F G B_1 B_2}$, and their symplectic eigenvalues $\lambda_1 - 4, \lambda_5 - 10$ and $\lambda_{5 - 12}$.

The covariance matrix $\gamma_{A_1 A_2 B_1 B_2}$ only depends on the system including Alice and the quantum channel whose relationships are as follows:

$$
\begin{align}
\hat{E}_3 &= \sqrt{T_E} \hat{E}_2 + \sqrt{1 - T_E} \hat{E}_0 \\
\hat{E}_5 &= -\sqrt{1 - T_E} \hat{E}_2 + \sqrt{T_E} \hat{E}_0 \\
\hat{A}_m &= \sqrt{T_E} \hat{B}_2 + \sqrt{1 - T_E} \hat{E}_1 \\
\hat{E}_4 &= -\sqrt{1 - T_E} \hat{B}_2 + \sqrt{T_E} \hat{E}_3 \\
\hat{A}_{out} &= \sqrt{T_E} \hat{A}_{in} + \sqrt{1 - T_E} \hat{A}_2 \\
\hat{A}_3 &= -\sqrt{1 - T_E} \hat{A}_{in} + \sqrt{T_E} \hat{A}_2 \\
\hat{B}_1 &= \sqrt{T_E} \hat{A}_{out} + \sqrt{1 - T_E} \hat{A}_2 \\
\hat{E}_6 &= -\sqrt{1 - T_E} \hat{A}_{out} + \sqrt{T_E} \hat{E}_3
\end{align}
$$

(A.1)

where $B_2, B_1$ and $E_0$ represents the original mode from Bob, the mode back to Bob and the vacuum state. $T_1$ and $T_2$ are the channel transmission efficiency, which we use $T = T_1 = T_2$ for calculation here. $T_A$ and $T_E$ are the transmittances in Alice and Eve. After simplification, the state $B_3$ is

$$
\begin{align}
\hat{B}_3 &= \sqrt{T_E} \hat{B}_2 + \sqrt{1 - T_E} \hat{A}_2 \\
&+ (\sqrt{T_E} \hat{E}_2 (1 - T_E) (1 - T_2) - \sqrt{1 - T_E} (1 - T_2)) \hat{E}_0 \\
&+ (\sqrt{T_E} (1 - T_E) (1 - T_1) T_2 - \sqrt{T_E} (1 - T_2)) \hat{E}_0
\end{align}
$$

(A.2)
Therefore, we can adjust parameter $T_E$ to reduce the interference of mode $B_3$. When $T_E = 1/(1 + T T_A)$, $B_3$ becomes

$$B_3 = \sqrt{T_A T \hat{B}_2 + \sqrt{(1 - T_A) T \hat{A}_2 + (1 - T)(1 + T T_A)}} e_0.$$  

(A.3)

The covariance matrix $\gamma_{a, a, b_1, b_1}$ becomes

$$\begin{pmatrix}
V_a \cdot I_2 & \sqrt{T_A (V_a^2 - 1) \cdot \sigma_2} & 0 \cdot I_2 & \gamma_{a, b_1} \cdot \sigma_2 \\
\sqrt{T_A (V_a^2 - 1) \cdot \sigma_2} & \gamma_{a, b_1} \cdot \sigma_2 & V_b \cdot I_2 & \gamma_{b_1} \cdot \sigma_2 \\
0 \cdot \sigma_2 & \gamma_{a, b_1} \cdot \sigma_2 & V_b \cdot I_2 & \gamma_{b_1} \cdot \sigma_2 \\
\gamma_{a, b_1} \cdot \sigma_2 & \gamma_{a, b_1} \cdot \sigma_2 & V_b \cdot I_2 & \gamma_{b_1} \cdot \sigma_2 \\
\end{pmatrix},$$  

(A.4)

where $I_2$ is the $n \times n$ identity matrix and $\sigma_2 = \text{diag}(1, -1)$, $V_b$, $V_a$ and $V_b$ are the variance of EPR1, EPR2 and EPR3. Here we choose $V_b = 1 + 2 T / (1 - T)$ for keeping the average excess noise of the forward and backward path as $\hat{e}$. We use the average excess noise $\hat{e} = (\hat{e}_1 + \hat{e}_2)/2$ as the average value of forward path excess noise $\hat{e}_1$ and backward path excess noise $\hat{e}_2$. $\gamma_{a, b_1}$, $\gamma_{a, b_1}$, $\gamma_{a, b_1}$, $\gamma_{b_1}$ and $\gamma_{b_1}$ are

$$\gamma_{a, b_1} = \sqrt{\frac{1}{T} - 1} (V_a^2 - 1),$$  

$$\gamma_{a, b_1} = T A V_a + 1 - T (1 - T) V_b$$

$$\gamma_{a, b_1} = \sqrt{T} - \frac{T}{1 + T T_A} V_b$$

$$\gamma_{a, b_1} = \sqrt{T} - \frac{T}{1 + T T_A} V_b + (1 - T) V_B + (1 - T) T A$$

$$\gamma_{a, b_1} = \sqrt{T} - \frac{T}{1 + T T_A} V_b - (1 - T) V_B + (1 - T) T A$$

(A.5)

Similarly, the covariance matrix $\gamma_{a, a, b_1, b_1}$ can be written as

$$\gamma_{a, a, b_1, b_1} = \gamma_{a, a, b_1, b_1}$$

$$\gamma_{a, b_1} = \gamma_{a, b_1}$$

$$\gamma_{a, b_1} = \gamma_{a, b_1}$$

$$\gamma_{a, b_1} = \gamma_{a, b_1}$$

where $X = \text{diag}(1, 0)$ and the inverse is a pseudo inverse. The matrices $\gamma_{a, a, b_1, b_1}$, $\gamma_{a, b_1}$ and $\gamma_{a, a, b_1, b_1}$ can all be derived from the decomposition of the matrix

$$\gamma_{a, a, b_1, b_1} = \gamma_{a, a, b_1, b_1}$$

$$\gamma_{a, b_1} = \gamma_{a, b_1}$$

$$\gamma_{a, b_1} = \gamma_{a, b_1}$$

The above matrix can be derived with appropriate rearrangement of lines and columns from the matrix describing the system (see figure 3(a))

$$\gamma_{a, b_1} = \gamma_{a, b_1}$$

(A.6)

Finally, we need to calculate the symplectic eigenvalues of the covariance matrices $\gamma_{a, a, b_1, b_1}$, $\gamma_{a, a, b_1, b_1}$ and $\gamma_{a, a, b_1, b_1}$. Given an arbitrary $N$-mode covariance matrix $\gamma$, there exists a symplectic matrix $S$, such that

$$\gamma = S \gamma^S T,$$

where the diagonal matrix $\gamma^S$ is called the Williamson form of $\gamma$ and the $N$ positive quantities $\lambda_k$ are called the symplectic eigenvalues of $\gamma$. Here the symplectic spectrum $[\lambda_k]_{k=1}^N$ can be easily computed as the standard eigenspectrum of the matrix $[i \Omega \gamma]$, where the modulus must be understood in the operational sense. Here, $\Omega$ is the symplectic form

$$\Omega = \frac{N}{\sum_{k=1}^N \left[ 0 \ 1 \ -1 \ 0 \right].$$

(A.15)

References:

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74 145

[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 Rev. Mod. Phys. 81 1301

[3] Weedbrook C, Pirandola S, Garcia-Patron R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 Rev. Mod. Phys. 84 621

[4] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 Nature Photon. 7 375
[5] Grosshans F and Grangier P 2002 Phys. Rev. Lett. 88 057902
[6] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 Phys. Rev. Lett. 93 170504
[7] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 Nature 421 238
[8] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C and Lam P K 2005 Phys. Rev. Lett. 95 180503
[9] Lodewyck J et al 2007 Phys. Rev. A 76 042305
[10] Grosshans F 2005 Phys. Rev. Lett. 94 020504
[11] Navascués M and Acín A 2005 Phys. Rev. Lett. 94 020505
[12] Renner R and Cirac J I 2009 Phys. Rev. Lett. 102 110504
[13] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 Phys. Rev. Lett. 109 100502
[14] Leverrier A, García-Patrón R, Renner R and Cerf N J 2013 Phys. Rev. Lett. 110 030502
[15] Pirandola S, Mancini S, Lloyd S and Braunstein S L 2008 Nature Phys. 4 726
[16] Sun M, Peng X, Shen Y and Guo H 2012 Int. J. Quantum Inform. 10 1250059
[17] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R and Grangier P 2009 J. Phys. B: At. Mol. Opt. Phys. 42 114014
[18] Zhang H, Fang J and He G 2012 Phys. Rev. A 86 022338
[19] Sun M, Peng X and Guo H 2013 J. Phys. B: At. Mol. Opt. Phys. 46 085501
[20] Caves C M 1982 Phys. Rev. D 26 1817
[21] García-Patrón R 2007 PhD Thesis ULB Bruxelles
[22] Yoshikawa J I, Miwa Y, Huck A, Andersen U L, van Loock P and Furusawa A 2008 Phys. Rev. Lett. 101 250501
[23] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Communication (Cambridge: Cambridge University Press)