

Practical security analysis of continuous-variable quantum key distribution with an unbalanced heterodyne detector

Lingzhi Kong(孔令志), Weiqi Liu(刘维琪)†, Fan Jing(荆凡), and Chen He(贺晨)‡
Citation: Chin. Phys. B, 2022, 31 (**7**): 070303. DOI: 10.1088/1674-1056/ac4102
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Short-wave infrared continuous-variable quantum key distribution over satellite-to-submarine channels

Qingquan Peng(彭清泉), Qin Liao(廖骎), Hai Zhong(钟海), Junkai Hu(胡峻凯), and Ying Guo(郭迎)
Chin. Phys. B, 2022, 31 (**6**): 060306. DOI: 10.1088/1674-1056/ac490a

Parameter estimation of continuous variable quantum key distribution system via artificial neural networks

Hao Luo(罗浩), Yi-Jun Wang(王一军), Wei Ye(叶炜), Hai Zhong(钟海), Yi-Yu Mao(毛宜钰), and Ying Guo(郭迎)
Chin. Phys. B, 2022, 31 (**2**): 020306. DOI: 10.1088/1674-1056/ac2807

Continuous-variable quantum key distribution based on photon addition operation

Xiao-Ting Chen(陈小婷), Lu-Ping Zhang(张露萍), Shou-Kang Chang(常守康), Huan Zhang(张欢), and Li-Yun Hu(胡利云)
Chin. Phys. B, 2021, 30 (**6**): 060304. DOI: 10.1088/1674-1056/abd931

Hybrid linear amplifier-involved detection for continuous variable quantum key distribution with thermal states

Yu-Qian He(贺宇千), Yun Mao(毛云), Hai Zhong(钟海), Duang Huang(黄端), Ying Guo(郭迎)
Chin. Phys. B, 2020, 29 (**5**): 050309. DOI: 10.1088/1674-1056/ab8216

Reconciliation for CV-QKD using globally-coupled LDPC codes

Jin-Jing Shi(石金晶), Bo-Peng Li(李伯鹏), Duan Huang(黄端)
Chin. Phys. B, 2020, 29 (**4**): 040301. DOI: 10.1088/1674-1056/ab6d4f

---

Practical security analysis of continuous-variable quantum key distribution with an unbalanced heterodyne detector

Lingzhi Kong(孔令志), Weiqi Liu(刘维琪)[†], Fan Jing(荆凡), and Chen He(贺晨)[‡]

College of Information Science and Technology, Northwest University, Xi'an 710127, *China*

(Received 6 September 2021; revised manuscript received 15 November 2021; accepted manuscript online 8 December 2021)

When developing a practical continuous-variable quantum key distribution (CVQKD), the detector is necessary at the receiver's side. We investigate the practical security of the CVQKD system with an unbalanced heterodyne detector. The results show that unbalanced heterodyne detector introduces extra excess noise into the system and decreases the lower bound of the secret key rate without awareness of the legitimate communicators, which leaves loopholes for Eve to attack the system. In addition, we find that the secret key rate decreases more severely with the increase in the degree of imbalance and the excess noise induced by the imbalance is proportional to the intensity of the local oscillator (LO) under the same degree of imbalance. Finally, a countermeasure is proposed to resist these kinds of effects.

Keywords: continuous-variable, quantum key distribution, heterodyne detector

PACS: 03.67.Hk, 03.67.Dd, 03.67.–a **DOI:** 10.1088/1674-1056/ac4102

1. Introduction

Quantum key distribution (QKD) enables two distant authorized parties (Alice and Bob) to exchange a secret key basesd on the laws of Heisenberg's uncertainty principle and no-clone theory, which can be divided into the discrete variable quantum key distribution (DVQKD) and CVQKD.[1–6] Focusing on the most favorable CVQKD protocol, the Gaussian-modulated coherent state (GMCS) protocol,[7–13] which encodes the key information on the quadratures (X and P) of coherent states, the modulated states will be sent to Bob along with the LO. Then Bob randomly measures one of the two quadratures using a homodyne detector, or both quadratures simultaneously with a heterodyne detector. So far, the GMCS scheme has been experimentally carried out in both laboratory[14–16] and field tests.[17,18] Furthermore, the composable security of this scheme against collective attack has been established.[19,20]

However, the imperfections of devices and applications used in the practical system may threaten the security of the system. The imperfections include the laser source,[21–23] the local oscillator,[24,25] the beam splitter (BS),[26–28] the basis choice,[29,30] and the detector.[31–37] In the implementation of GMCS protocols, Bob may not need to randomly switch his measurement basis using the heterodyne detector. Theoretically, the scheme gives a higher key rate and allows simpler and higher bandwidth quantum cryptographic experiments. However, the BS used in the heterodyne detector may be imperfect and the four photodiodes may be mismatched. Such imperfections will lead to an imbalance of the heterodyne detector, and further influence the parameter estimation and the lower bound of the secret key rate of CVQKD system and, finally, may bring security loopholes for Eve to attack the system.

In this paper, we investigate the practical security of a GMCS CVQKD system with an unbalanced heterodyne detector. We find that the imbalance will bring in extra excess noise to the system and the lower bound of the secret key rate will be decreased due to the imperfect BS and the mismatch of four photodiodes. Moreover, the secret key rate decreases more severely with the increase in the degree of imbalance and the extra excess noise is proportional to the intensity of the LO under the same degree of imbalance. To resist this imperfection, a countermeasure is proposed.

This paper consists of six sections. In Section 2, we describe the perfect heterodyne detector in detail. Then the practical unbalanced heterodyne detector in CVQKD is investigated in Section 3 and the secret key rate against collective attack in the above case is investigated by theoretical calculation and simulation in Section 4. In Section 5, a possible countermeasure is proposed to resist the imperfection induced by the unbalanced heterodyne detector. In Section 6, we give the conclusion.

2. The balanced heterodyne detector

The balanced heterodyne detector mainly consists of four beam splitters with ideal beam splitting ratio, two pairs of matched photodiodes with the same quantum efficiency, two subtractors and two amplifiers with transimpedance g. The structure of heterodyne detector is shown in Fig. 1. The quantum and LO signal are divided into two beams via two 50:50

[†]Corresponding author. E-mail: vickylwq1991@nwu.edu.cn
[‡]Corresponding author. E-mail: chenhe@nwu.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

beam splitters. Then, the quadratures X and P of the quantum signal are measured simultaneously by two homodyne detectors on the upper and lower arms. It is worth noting that the LO on the lower arm is phase-shifted by 90° to measure quadrature P.

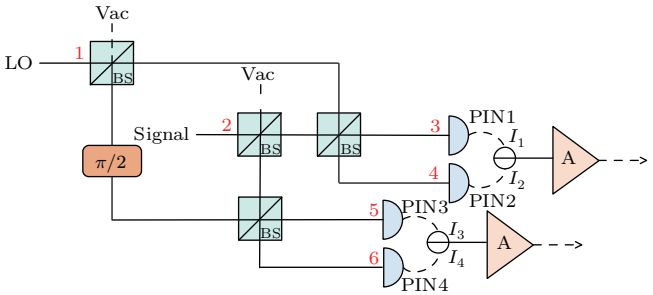


Fig. 1. The structure of the heterodyne detector. BS: beam splitter; $\text{PIN}_{1,2,3,4}$: photodiode with quantum efficiency $\eta_{1,2,3,4}$; A: transimpedance amplifer.

In heterodyne detection, Bob generally converts the photons into photocurrent. Here we introduce quantum efficiency η to characterize the ability of converting incident light into photocurrent, which is the ratio of the average number of photoelectrons generated per unit time at a certain wavelength to the number of incident light photons. It is supposed that the average electron number of photocurrent output by the photodiode is $N_{\rm e}$, and the average photon number of the incident light on the photodiode is $N_{\rm i}$. Therefore, the average optical power $P_{\rm a}$ can be defined as:

$$P_{\rm a} = \frac{h\nu}{\tau} \times N_{\rm i}, \tag{1}$$

where h is the Planck constant, ν is the optical wavelength and τ is the duration of light incident on the photodiode. For convenience of analysis, we can define $\tau = 1$ and the average photon number of the incident light can be expressed as

$$N_{\rm i} = \frac{P_{\rm a}}{h\nu}. \tag{2}$$

According to the definition of quantum efficiency, η can be written as

$$\eta = \frac{N_{\rm e}}{N_{\rm i}} = \frac{I_{\rm e}/e}{P_{\rm a}/h\nu} = \frac{I_{\rm e}}{P_{\rm a}} \times \frac{h\nu}{e}, \tag{3}$$

where $I_{\rm e}$ is the average output photocurrent of the photodiode and e is a constant denoting the amount of negative charge carried by a single electron. It is noteworthy that $I_{\rm e}/P_{\rm a}$ describing the responsivity of photodiode can be labeled as $R_{\rm pin}$. Consequently, equation (3) can be modified as

$$\eta = R_{\rm pin} \times \frac{h\nu}{e}. \tag{4}$$

When implementing heterodyne detection, the vacuum state is introduced via the 50:50 BS as shown in Fig. 1. Therefore, the final measured quardratures X and P will be coupled into a vacuum fluctuation. The corresponding output of the four photodiodes can be expressed as follows:

$$\hat{a}_{\rm out1,2} = \frac{1}{2}\left[\left(\hat{a}_{\rm s} + \hat{N}_{\rm s}\right) \pm \left(\hat{a}_{\rm LO} + \hat{N}_{\rm LO}\right)\right], \tag{5}$$

$$\hat{a}_{\rm out3,4} = \frac{1}{2}\left[\left(\hat{a}_{\rm s} + \hat{N}_{\rm s}\right) \pm \exp\left(\mathrm{i}\frac{\pi}{2}\right)\left(\hat{a}_{\rm LO} + \hat{N}_{\rm LO}\right)\right], \tag{6}$$

where $\hat{a}_{\rm s}$ denotes the mode of quantum signal optical field, $\hat{a}_{\rm LO}$ denotes the mode of the LO signal optical field, $\hat{N}_{\rm s}$ and $\hat{N}_{\rm LO}$ depict the vacuum noise introduced into the quantum signal and LO signal respectively due to the implementation of the heterodyne detection.Then the photon number of the four output modes can be shown as follows:

$$\begin{aligned}\hat{n}_{1,2} &= \hat{a}^{\dagger}_{\rm out1,2}\hat{a}_{\rm out1,2} \\ &= \frac{1}{4}\left[\left(\hat{a}^{\dagger}_{\rm s} + \hat{N}^{\dagger}_{\rm s}\right) \pm \left(\hat{a}^{\dagger}_{\rm LO} + \hat{N}^{\dagger}_{\rm LO}\right)\right] \\ &\quad \times \left[\left(\hat{a}_{\rm s} + \hat{N}_{\rm s}\right) \pm \left(\hat{a}_{\rm LO} + \hat{N}_{\rm LO}\right)\right],\end{aligned} \tag{7}$$

$$\begin{aligned}\hat{n}_{3,4} &= \hat{a}^{\dagger}_{\rm out3,4}\hat{a}_{\rm out3,4} \\ &= \frac{1}{4}\left[\left(\hat{a}^{\dagger}_{\rm s} + \hat{N}^{\dagger}_{\rm s}\right) \pm \exp\left(-\mathrm{i}\frac{\pi}{2}\right)\left(\hat{a}^{\dagger}_{\rm LO} + \hat{N}^{\dagger}_{\rm LO}\right)\right] \\ &\quad \times \left[\left(\hat{a}_{\rm s} + \hat{N}_{\rm s}\right) \pm \exp\left(\mathrm{i}\frac{\pi}{2}\right)\left(\hat{a}_{\rm LO} + \hat{N}_{\rm LO}\right)\right].\end{aligned} \tag{8}$$

According to the definition of quantum efficiency, the photocurrent output of these four photodiodes can be calculated as follows:

$$\begin{aligned}I_{1,2} &= \frac{h\nu}{\tau} \times R_{\rm pin} \times \hat{n}_{1,2} \\ &= \frac{h\nu}{4\tau} R_{\rm pin}\left[\left(\hat{a}^{\dagger}_{\rm s} + \hat{N}^{\dagger}_{\rm s}\right) \pm \left(\hat{a}^{\dagger}_{\rm LO} + \hat{N}^{\dagger}_{\rm LO}\right)\right] \\ &\quad \times \left[\left(\hat{a}_{\rm s} + \hat{N}_{\rm s}\right) \pm \left(\hat{a}_{\rm LO} + \hat{N}_{\rm LO}\right)\right],\end{aligned} \tag{9}$$

$$\begin{aligned}I_{3,4} &= \frac{h\nu}{\tau} \times R_{\rm pin} \times \hat{n}_{3,4} \\ &= \frac{h\nu}{4\tau} R_{\rm pin}\left[\left(\hat{a}^{\dagger}_{\rm s} + \hat{N}^{\dagger}_{\rm s}\right) \pm \exp\left(-\mathrm{i}\frac{\pi}{2}\right)\left(\hat{a}^{\dagger}_{\rm LO} + \hat{N}^{\dagger}_{\rm LO}\right)\right] \\ &\quad \times \left[\left(\hat{a}_{\rm s} + \hat{N}_{\rm s}\right) \pm \exp\left(\mathrm{i}\frac{\pi}{2}\right)\left(\hat{a}_{\rm LO} + \hat{N}_{\rm LO}\right)\right].\end{aligned} \tag{10}$$

Then, the differential current output on the upper and lower arms can be given by

$$\begin{aligned}\Delta I_1 = I_1 - I_2 = \frac{h\nu}{2\tau} R_{\rm pin}\Big(&\hat{a}^{\dagger}_{\rm s}\hat{a}_{\rm LO} + \hat{a}^{\dagger}_{\rm s}\hat{N}_{\rm LO} + \hat{N}^{\dagger}_{\rm s}\hat{a}_{\rm LO} + \hat{N}^{\dagger}_{\rm s}\hat{N}_{\rm LO} \\ &+ \hat{a}^{\dagger}_{\rm LO}\hat{a}_{\rm s} + \hat{a}^{\dagger}_{\rm LO}\hat{N}_{\rm s} + \hat{N}^{\dagger}_{\rm LO}\hat{a}_{\rm s} + \hat{N}^{\dagger}_{\rm LO}\hat{N}_{\rm s}\Big),\end{aligned} \tag{11}$$

$$\begin{aligned}\Delta I_2 = I_3 - I_4 = \frac{h\nu}{2\tau} R_{\rm pin}\mathrm{i}\Big(&\hat{a}^{\dagger}_{\rm s}\hat{a}_{\rm LO} + \hat{a}^{\dagger}_{\rm s}\hat{N}_{\rm LO} + \hat{N}^{\dagger}_{\rm s}\hat{a}_{\rm LO} + \hat{N}^{\dagger}_{\rm s}\hat{N}_{\rm LO} \\ &- \hat{a}^{\dagger}_{\rm LO}\hat{a}_{\rm s} - \hat{a}^{\dagger}_{\rm LO}\hat{N}_{\rm s} - \hat{N}^{\dagger}_{\rm LO}\hat{a}_{\rm s} - \hat{N}^{\dagger}_{\rm LO}\hat{N}_{\rm s}\Big).\end{aligned} \tag{12}$$

3. The practical unbalanced heterodyne detector

As aforementioned, the practical heterodyne detector may be unbalanced and imperfect due to the limitations of the BS

and the photodiode. For example, the splitting ratio of the BS may not be ideal and the four photodiodes maybe mismatched. So as to distinguish the characteristics between a balanced heterodyne detector and unbalanced heterodyne detector, we introduce an additional parameter L_{ij} $(i=1,2;\ j=3,4,5,6)$ to demonstrate the effect of the loss from input port i to output port j, as shown in Fig. 1. And considering the mismatch of these four photodiodes, the quantum efficiency of the photodiodes can be defined as η_1, η_2, η_3, and η_4, respectively. Considering the imperfections of the heterodyne detector, the corresponding output of the four photodiodes can be modified as

$$\hat{a}_{\rm out1} = \frac{1}{2}\left[\sqrt{L_{13}}\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right)+\sqrt{L_{23}}\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\right], \quad (13)$$

$$\hat{a}_{\rm out2} = \frac{1}{2}\left[\sqrt{L_{14}}\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right)-\sqrt{L_{24}}\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\right], \quad (14)$$

$$\hat{a}_{\rm out3} = \frac{1}{2}\Big[\sqrt{L_{15}}\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right) + \exp\left(\mathrm{i}\frac{\pi}{2}\right)\sqrt{L_{25}}\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\Big], \quad (15)$$

$$\hat{a}_{\rm out4} = \frac{1}{2}\Big[\sqrt{L_{16}}\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right) - \exp\left(\mathrm{i}\frac{\pi}{2}\right)\sqrt{L_{26}}\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\Big], \quad (16)$$

and the photon number of the four output photodiodes can be rewritten as follows:

$$\hat{n}_1 = \frac{1}{4}\left[\sqrt{L_{13}}\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)+\sqrt{L_{23}}\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\right] \times\left[\sqrt{L_{13}}\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right)+\sqrt{L_{23}}\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\right], \quad (17)$$

$$\hat{n}_2 = \frac{1}{4}\left[\sqrt{L_{14}}\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)-\sqrt{L_{24}}\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\right] \times\left[\sqrt{L_{14}}\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right)-\sqrt{L_{24}}\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\right], \quad (18)$$

$$\hat{n}_3 = \frac{1}{4}\left[\sqrt{L_{15}}\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)+\exp\left(-\mathrm{i}\frac{\pi}{2}\right)\sqrt{L_{25}}\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\right] \times\left[\sqrt{L_{15}}\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right)+\exp\left(\mathrm{i}\frac{\pi}{2}\right)\sqrt{L_{25}}\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\right], \quad (19)$$

$$\hat{n}_4 = \frac{1}{4}\left[\sqrt{L_{16}}\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)-\exp\left(-\mathrm{i}\frac{\pi}{2}\right)\sqrt{L_{26}}\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\right] \times\left[\sqrt{L_{16}}\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right)-\exp\left(\mathrm{i}\frac{\pi}{2}\right)\sqrt{L_{26}}\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\right]. \quad (20)$$

Referring to Eq. (4), the practical responsivity of the four photodiodes of the unbalanced heterodyne detector can be expressed as follows:

$$R_{\rm pin1,2,3,4} = \frac{\eta_{1,2,3,4}\times e}{h\nu}. \quad (21)$$

Consequently, the photocurrent output of the four photodiodes can be calculated as follows:

$$\begin{aligned} I_1 &= \frac{h\nu}{\tau}\times R_{\rm pin1}\times\hat{n}_1 \\ &= \frac{e}{4\tau}\Big[\eta_1 L_{13}\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right) \\ &\quad +\eta_1\sqrt{L_{13}L_{23}}\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right) \\ &\quad +\eta_1\sqrt{L_{23}L_{13}}\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right) \\ &\quad +\eta_1 L_{23}\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\Big], \end{aligned} \quad (22)$$

$$\begin{aligned} I_2 &= \frac{h\nu}{\tau}\times R_{\rm pin2}\times\hat{n}_2 \\ &= \frac{e}{4\tau}\Big[\eta_2 L_{14}\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right) \\ &\quad -\eta_2\sqrt{L_{14}L_{24}}\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right) \\ &\quad -\eta_2\sqrt{L_{24}L_{14}}\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right) \\ &\quad +\eta_2 L_{24}\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\Big], \end{aligned} \quad (23)$$

$$\begin{aligned} I_3 &= \frac{h\nu}{\tau}\times R_{\rm pin3}\times\hat{n}_3 \\ &= \frac{e}{4\tau}\Big[\eta_3 L_{15}\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right) \\ &\quad +\eta_3\sqrt{L_{15}L_{25}}\exp\left(\mathrm{i}\frac{\pi}{2}\right)\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right) \\ &\quad +\eta_3\sqrt{L_{25}L_{15}}\exp\left(-\mathrm{i}\frac{\pi}{2}\right)\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right) \\ &\quad +\eta_3 L_{25}\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\Big], \end{aligned} \quad (24)$$

$$\begin{aligned} I_4 &= \frac{h\nu}{\tau}\times R_{\rm pin4}\times\hat{n}_4 \\ &= \frac{e}{4\tau}\Big[\eta_4 L_{16}\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right) \\ &\quad -\eta_4\sqrt{L_{16}L_{26}}\exp\left(\mathrm{i}\frac{\pi}{2}\right)\left(\hat{a}_{\rm s}^{\dagger}+\hat{N}_{\rm s}^{\dagger}\right)\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right) \\ &\quad -\eta_4\sqrt{L_{26}L_{16}}\exp\left(-\mathrm{i}\frac{\pi}{2}\right)\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\left(\hat{a}_{\rm s}+\hat{N}_{\rm s}\right) \\ &\quad +\eta_4 L_{26}\left(\hat{a}_{\rm LO}^{\dagger}+\hat{N}_{\rm LO}^{\dagger}\right)\left(\hat{a}_{\rm LO}+\hat{N}_{\rm LO}\right)\Big]. \end{aligned} \quad (25)$$

Then, the practical differential current output on the upper and lower arms can be expressed as

$$\begin{aligned} \Delta I_{\rm prac1} &= I_1 - I_2 \\ &= \frac{e}{4\tau}\Big[\left(\eta_1 L_{13}-\eta_2 L_{14}\right)\left(\hat{a}_{\rm s}^{\dagger}\hat{a}_{\rm s}+\hat{N}_{\rm s}^{\dagger}\hat{a}_{\rm s}+\hat{a}_{\rm s}^{\dagger}\hat{N}_{\rm s}+\hat{N}_{\rm s}^{\dagger}\hat{N}_{\rm s}\right) \\ &\quad +\left(\eta_1 L_{23}-\eta_2 L_{24}\right) \\ &\quad \times\left(\hat{a}_{\rm LO}^{\dagger}\hat{a}_{\rm LO}+\hat{N}_{\rm LO}^{\dagger}\hat{a}_{\rm LO}+\hat{a}_{\rm LO}^{\dagger}\hat{N}_{\rm LO}+\hat{N}_{\rm LO}^{\dagger}\hat{N}_{\rm LO}\right) \\ &\quad +\left(\eta_1\sqrt{L_{13}L_{23}}+\eta_2\sqrt{L_{14}L_{24}}\right) \\ &\quad \times\left(\hat{a}_{\rm s}^{\dagger}\hat{a}_{\rm LO}+\hat{N}_{\rm s}^{\dagger}\hat{a}_{\rm LO}+\hat{a}_{\rm s}^{\dagger}\hat{N}_{\rm LO}+\hat{N}_{\rm s}^{\dagger}\hat{N}_{\rm LO}\right. \\ &\quad \left.+\hat{a}_{\rm LO}^{\dagger}\hat{a}_{\rm s}+\hat{N}_{\rm LO}^{\dagger}\hat{a}_{\rm s}+\hat{a}_{\rm LO}^{\dagger}\hat{N}_{\rm s}+\hat{N}_{\rm LO}^{\dagger}\hat{N}_{\rm s}\right)\Big], \end{aligned} \quad (26)$$

$$\begin{aligned} \Delta I_{\rm prac2} &= I_3 - I_4 \\ &= \frac{e}{4\tau}\Big[\left(\eta_3 L_{15}-\eta_4 L_{16}\right)\left(\hat{a}_{\rm s}^{\dagger}\hat{a}_{\rm s}+\hat{N}_{\rm s}^{\dagger}\hat{a}_{\rm s}+\hat{a}_{\rm s}^{\dagger}\hat{N}_{\rm s}+\hat{N}_{\rm s}^{\dagger}\hat{N}_{\rm s}\right) \\ &\quad +\left(\eta_3 L_{25}-\eta_4 L_{26}\right) \\ &\quad \times\left(\hat{a}_{\rm LO}^{\dagger}\hat{a}_{\rm LO}+\hat{N}_{\rm LO}^{\dagger}\hat{a}_{\rm LO}+\hat{a}_{\rm LO}^{\dagger}\hat{N}_{\rm LO}+\hat{N}_{\rm LO}^{\dagger}\hat{N}_{\rm LO}\right) \end{aligned}$$

$$+\mathrm{i}\left(\eta_3\sqrt{L_{15}L_{25}}+\eta_4\sqrt{L_{16}L_{26}}\right)$$
$$\times\left(\hat{a}_{\mathrm{s}}^{\dagger}\hat{a}_{\mathrm{LO}}+\hat{N}_{\mathrm{s}}^{\dagger}\hat{a}_{\mathrm{LO}}+\hat{a}_{\mathrm{s}}^{\dagger}\hat{N}_{\mathrm{LO}}+\hat{N}_{\mathrm{s}}^{\dagger}\hat{N}_{\mathrm{LO}}\right.$$
$$\left.-\hat{a}_{\mathrm{LO}}^{\dagger}\hat{a}_{\mathrm{s}}-\hat{N}_{\mathrm{LO}}^{\dagger}\hat{a}_{\mathrm{s}}-\hat{a}_{\mathrm{LO}}^{\dagger}\hat{N}_{\mathrm{s}}-\hat{N}_{\mathrm{LO}}^{\dagger}\hat{N}_{\mathrm{s}}\right)\Big]. \tag{27}$$

Correspondingly, the output voltage of the upper and lower arms of the practical heterodyne can be expressed as follows,

$$\begin{aligned}U_{\mathrm{hom1}} &= g\Delta I_{\mathrm{prac1}}\\ &\approx \frac{eg}{4\tau}\Big[\left(\eta_1L_{13}-\eta_2L_{14}\right)\langle\hat{n}_{\mathrm{s}}\rangle+\left(\eta_1L_{23}-\eta_2L_{24}\right)\langle n_{\mathrm{LO}}\rangle\\ &\quad+\left(\eta_1\sqrt{L_{13}L_{23}}+\eta_2\sqrt{L_{14}L_{24}}\right)\sqrt{\langle n_{\mathrm{LO}}\rangle}\\ &\quad\times\left(\hat{x}\cos\theta_{\mathrm{LO}}+\hat{p}\sin\theta_{\mathrm{LO}}\right)\Big],\end{aligned} \tag{28}$$

$$\begin{aligned}U_{\mathrm{hom2}} &= g\Delta I_{\mathrm{prac2}}\\ &\approx \frac{eg}{4\tau}\Big[\left(\eta_3L_{15}-\eta_4L_{16}\right)\langle\hat{n}_{\mathrm{s}}\rangle+\left(\eta_3L_{25}-\eta_4L_{26}\right)\langle n_{\mathrm{LO}}\rangle\\ &\quad+\left(\eta_3\sqrt{L_{15}L_{25}}+\eta_4\sqrt{L_{16}L_{26}}\right)\sqrt{\langle n_{\mathrm{LO}}\rangle}\\ &\quad\times\left(\hat{p}\cos\theta_{\mathrm{LO}}-\hat{x}\sin\theta_{\mathrm{LO}}\right)\Big],\end{aligned} \tag{29}$$

where g is the transimpedance of the amplifier, $\langle\hat{n}_{\mathrm{s}}\rangle=\hat{a}_{\mathrm{s}}^{\dagger}\hat{a}_{\mathrm{s}}$ and $\langle\hat{n}_{\mathrm{LO}}\rangle=\hat{a}_{\mathrm{LO}}^{\dagger}\hat{a}_{\mathrm{LO}}$ depict the photon numbers of quantum signal and LO respectively. Here we assume that the vacuum noise $\hat{N}_{\mathrm{s}}$, and $\hat{N}_{\mathrm{LO}}$ can reach the order of shot noise, *i.e.* $\hat{N}_{\mathrm{s}}=\hat{N}_{\mathrm{LO}}=\hat{N}_0$, when considering the Heisenberg uncertainty relation and the feature of coherent state. And for simplicity's sake, the $\hat{N}_{\mathrm{s}}$ and $\hat{N}_{\mathrm{LO}}$ can be deemed to be zero because the shot noise $\hat{N}_0$ is a fairly small order of magnitude.

In Eqs. (28) and (29), $\sqrt{\langle n_{\mathrm{LO}}\rangle}(\hat{x}\cos\theta_{\mathrm{LO}}+\hat{p}\sin\theta_{\mathrm{LO}})$ and $\sqrt{\langle n_{\mathrm{LO}}\rangle}(\hat{p}\cos\theta_{\mathrm{LO}}-\hat{x}\sin\theta_{\mathrm{LO}})$ are physical parameters that need to be measured. In order to measure quadratures X and P simultaneously, θ_{LO} is usually set to be 0°, which denotes the reference phase of the local oscillator signal to the quantum signal. As mentioned before, a heterodyne detector can be viewed as being composed of two homodyne detectors. Consequently, the equivalent quantum efficiency of the upper and lower arms can be described as $\eta_1\sqrt{L_{13}L_{23}}+\eta_2\sqrt{L_{14}L_{24}}$ and $\eta_3\sqrt{L_{15}L_{25}}+\eta_4\sqrt{L_{16}L_{26}}$, respectively. In addition, $(\eta_1L_{13}-\eta_2L_{14})\langle\hat{n}_{\mathrm{s}}\rangle$ and $(\eta_1L_{23}-\eta_2L_{24})\langle n_{\mathrm{LO}}\rangle$ denote the direct components, which induce extra excess noise. The analysis of direct components in the lower homodyne detector is similar to that of the upper one. Hence the output voltage of the direct components U_{dc1} and U_{dc2} can be calculated as

$$\begin{aligned}U_{\mathrm{dc1}} &= \frac{eg}{4\tau}\big[(\eta_1L_{13}-\eta_2L_{14})\langle\hat{n}_{\mathrm{s}}\rangle\\ &\quad+(\eta_1L_{23}-\eta_2L_{24})\langle n_{\mathrm{LO}}\rangle\big],\end{aligned} \tag{30}$$

$$\begin{aligned}U_{\mathrm{dc2}} &= \frac{eg}{4\tau}\big[(\eta_3L_{15}-\eta_4L_{16})\langle\hat{n}_{\mathrm{s}}\rangle\\ &\quad+(\eta_3L_{25}-\eta_4L_{26})\langle n_{\mathrm{LO}}\rangle\big],\end{aligned} \tag{31}$$

then the variance of U_{dc1} and U_{dc2} can be obtained as follows:

$$\begin{aligned}\mathrm{Var}(U_{\mathrm{dc1}}) &= \left(\frac{eg}{4\tau}\right)^2\big[(\eta_1L_{13}-\eta_2L_{14})^2\mathrm{Var}(\langle\hat{n}_{\mathrm{s}}\rangle)\\ &\quad+(\eta_1L_{23}-\eta_2L_{24})^2\mathrm{Var}(\langle n_{\mathrm{LO}}\rangle)\big],\end{aligned} \tag{32}$$

$$\begin{aligned}\mathrm{Var}(U_{\mathrm{dc2}}) &= \left(\frac{eg}{4\tau}\right)^2\big[(\eta_3L_{15}-\eta_4L_{16})^2\mathrm{Var}(\langle\hat{n}_{\mathrm{s}}\rangle)\\ &\quad+(\eta_3L_{25}-\eta_4L_{26})^2\mathrm{Var}(\langle n_{\mathrm{LO}}\rangle)\big],\end{aligned} \tag{33}$$

where $\mathrm{Var}(\langle\hat{n}_{\mathrm{s}}\rangle)=(V_{\mathrm{A}}^2/4)\mathrm{RIN_sB}$ and $\mathrm{Var}(\langle n_{\mathrm{LO}}\rangle)=(\tau/h\nu)^2\langle P_{\mathrm{LO}}\rangle^2\mathrm{RIN_{LO}B}$, where $\mathrm{RIB_s}$ and $\mathrm{RIN_{LO}}$ represent the corresponding relative intensity noise of the quantum signal and the local oscillator, $\langle P_{\mathrm{s}}\rangle$ and $\langle P_{\mathrm{LO}}\rangle$ depict the average intensity of quantum signal and local oscillator. Then the excess noise induced by the direct components will be given by

$$\begin{aligned}\xi_{\mathrm{dc1}} &= \frac{4\tau}{g^2R_{\mathrm{pin_{eq1}}}^2h\nu\langle P_{\mathrm{LO}}\rangle}\mathrm{Var}(U_{\mathrm{dc1}})\\ &= \frac{e^2}{4R_{\mathrm{pin_{eq1}}}^2}\Big[(\eta_1L_{13}-\eta_2L_{14})^2\frac{V_{\mathrm{A}}^2}{4h\nu\langle P_{\mathrm{LO}}\rangle}\mathrm{RIN_sB}\\ &\quad+(\eta_1L_{23}-\eta_2L_{24})^2\frac{\tau}{h^3\nu^3}\langle P_{\mathrm{LO}}\rangle\mathrm{RIN_{LO}B}\Big],\end{aligned} \tag{34}$$

$$\begin{aligned}\xi_{\mathrm{dc2}} &= \frac{4\tau}{g^2R_{\mathrm{pin_{eq2}}}^2h\nu\langle P_{\mathrm{LO}}\rangle}\mathrm{Var}(U_{\mathrm{dc2}})\\ &= \frac{e^2}{4R_{\mathrm{pin_{eq2}}}^2}\Big[(\eta_3L_{15}-\eta_4L_{16})^2\frac{V_{\mathrm{A}}^2}{4h\nu\langle P_{\mathrm{LO}}\rangle}\mathrm{RIN_sB}\\ &\quad+(\eta_3L_{25}-\eta_4L_{26})^2\frac{\tau}{h^3\nu^3}\langle P_{\mathrm{LO}}\rangle\mathrm{RIN_{LO}B}\Big],\end{aligned} \tag{35}$$

where $R_{\mathrm{pin_{eq1}}}$ and $R_{\mathrm{pin_{eq2}}}$ represent the corresponding equivalent responsivity of the upper and the lower homodyne detector. They are proportional to the equivalent quantum efficiency η_{eq1} and η_{eq2}, where $\eta_{\mathrm{eq_1}}=\eta_1\sqrt{L_{13}L_{23}}+\eta_2\sqrt{L_{14}L_{24}}$ and $\eta_{\mathrm{eq_2}}=\eta_3\sqrt{L_{15}L_{25}}+\eta_4\sqrt{L_{16}L_{26}}$.

4. Performance analysis of the CVQKD system with an unbalanced heterodyne detector

As mentioned before, the splitting ratio of the BS may not be ideal and the four photodiodes maybe mismatched, which will cause an imbalance in heterodyne detector. As a result, extra excess noise is induced by these imperfections. For the convenience of analysis, the imperfections of the BS can be viewed as a part of the mismatch of the four photodiodes. To demonstrate the influence of an unbalanced heterodyne detector on the CVQKD system, here we consider the following four cases: (i) $\eta_1=\eta_2=\eta_3=\eta_4$; (ii) $\eta_1=\eta_2=\eta_3\neq\eta_4$; (iii) $\eta_1=\eta_2\neq\eta_3\neq\eta_4$; (iv) $\eta_1\neq\eta_2\neq\eta_3\neq\eta_4$.

According to Eqs. (1), (34) and (35), we firstly investigate the relationship between the excess noise and the intensity of the local oscillator under the four cases mentioned above, as

shown in Fig. 2. The number of photons of the local oscillator light ranges from 10^8 to 10^9. From top to bottom, the four lines indicate the relationship between the excess noise and the intensity of the LO when the four photodiodes are completely mismatched to fully matched. From Fig. 2, we find that the excess noise is proportional to the intensity of LO under the same degree of mismatched quantum efficiency and the extra excess noise will increase with the increase in the degree of imbalance. In other words, the greater the degree of mismatch of the four photodiodes, the greater the excess noise induced by the unbalanced heterodyne detector.

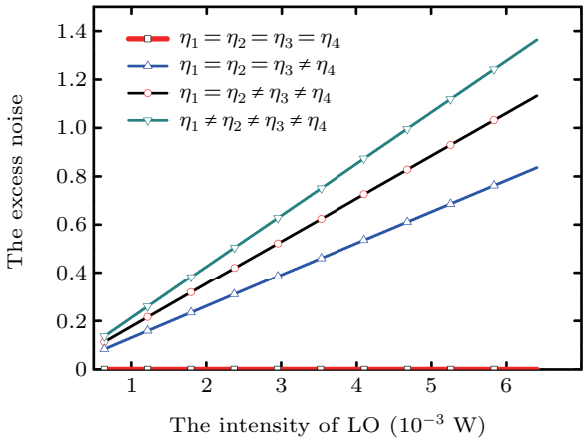


Fig. 2. The relationship between the excess noise and the intensity of the local oscillator under different degrees of imbalance. The simulation parameters are set as follows: elementary charge $e = 1.602176 \times 10^{-9}$, plank constant $h = 6.62607015 \times 10^{-34}$, duration $\tau = 20$ ns, optical wavelength $\nu = 193.4$ THz, photon number $n_{\mathrm{LO}} \in [10^8, 10^9]$, equivalent bandwidth $B = 15$ MHz, $\mathrm{RIN_s} = -210$, $\mathrm{RIN_{LO}} = -135$, and $V_{\mathrm{A}} = 5$.

Then taking the finite-size effect into account,[38] we analyze the secret key rate of the CVQKD system with unbalanced heterodyne detector. The secret key rate of the CVQKD system under collective attack can be given by (see Appendix A for detailed derivation)

$$R = f_{\mathrm{rep}} K_{\mathrm{finite}} = f_{\mathrm{rep}} \frac{n}{N} \left[\beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}} - \Delta(n)\right]. \tag{36}$$

To demonstrate the influence of the imbalance of the heterodyne detector on the secret key rate, we performed a simulation. In the simulation, the repetition frequency of system is fixed to 10 MHz. Curves from top to bottom represent the relationship between the secret key rate and the transmission distance under different degrees of imbalance in Fig. 3. Specifically, the black curve with circle denotes the ideal balanced heterodyne detector with $\eta_1 = \eta_2 = \eta_3 = \eta_4$, which possesses the maximum transmission distance and secret key rate. The brown curve with squares denotes the most mismatched case with $\eta_1 \neq \eta_2 \neq \eta_3 \neq \eta_4$ that has the minimum transmission distance and secret key rate. From the simulation results, we find that the imperfection of the BS and the mismatch of the four photodiodes will lead to a decrease in both secret key rate and the maximum transmission distance of the practical CVQKD system. Moreover, the security bound and the maximum transmission distance decrease more steeply with increase in the degree of imbalance.

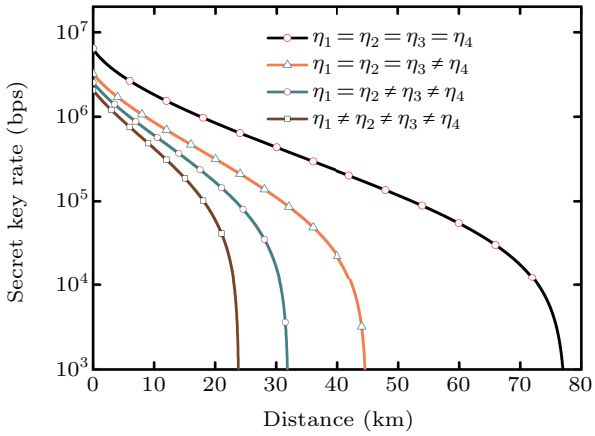


Fig. 3. The relationship between the secret key rate and the transmission distance under different degrees of imbalance. The simulation parameters are set as follows: photon number $n_{\mathrm{LO}} = 10^8$, equivalent bandwidth $B = 15$ MHz, excess noise $\xi = 0.01$, electric noise $v_{\mathrm{el}} = 0.01$ and reconciliation efficiency $\beta = 0.96$.

5. A possible countermeasure against the imbalance of the heterodyne detector

In this section, we propose a possible countermeasure to rebalance the CVQKD system with unbalanced heterodyne detector. Commonly, an unbalanced heterodyne detector will induce a mismatch between the intensity of the quantum and LO signal. As an important optical passive device in optical fiber communication, the variable optical attenuator (VOA) can realize the real-time control of the intensity of the signal by attenuating the transmitted optical power.[39] Hence we propose an improved scheme to rebalance the unbalanced heterodyne detector, in which six VOAs are applied in proper situations. As plotted in Fig. 4, $\mathrm{VOA}_{5,6}$ are set to rebalance arm 5 and arm 6 in red, $\mathrm{VOA}_{1,2}$ are set to rebalance arm 1 and arm 2 in green and $\mathrm{VOA}_{3,4}$ are set to rebalance arm 3 and arm 4 in yellow.

Based on the previous analysis, a practical heterodyne detector can be regarded as two unbalanced homodyne detector.Therefore, the rebalancing of the heterodyne detector can be derived from that of the homodyne detector. Referring to Ref. [34], the expected voltage at the output of the homodyne detector $\langle \hat{v}_{\mathrm{H}}(t) \rangle$ is given by,

$$\langle \hat{v}_{\mathrm{H}}(t) \rangle = q_{\mathrm{e}} g_{\mathrm{TIA}} \gamma |\alpha_{\mathrm{LO}}|^2 \int_{-\infty}^{+\infty} \mathrm{d}\tau |\zeta(\tau)|^2 h(t-\tau) \tag{37}$$

with

$$\gamma = \eta_{\mathrm{VOA5}} \left[\left(\frac{1}{2} - \Delta \right) \eta_{\mathrm{PIN1}} \eta_{\mathrm{VOA1}} - \left(\frac{1}{2} + \Delta \right) \eta_{\mathrm{PIN2}} \eta_{\mathrm{VOA2}} \right], \tag{38}$$

where $h(t)$ denotes the impulse response. For rebalancing the unbalanced homodyne detector, it is indispensable for us to adjust the attenuation efficiency of the VOA_i dynamically by monitoring the output voltage mean value $\langle \hat{v}_{\mathrm{H}}(t) \rangle$ in real

time.When $t=0$, $\langle \hat{v}_{\mathrm{H}}(t)\rangle$ is only equal to zero under the circumstance that $\gamma=0$. And from the Eq. (38), we can deduce that $\gamma=0$ when $(1/2-\Delta)\eta_{\mathrm{PIN1}}\eta_{\mathrm{VOA1}}=(1/2+\Delta)\eta_{\mathrm{PIN2}}\eta_{\mathrm{VOA2}}$, thus a rebalanced homodyne detector is obtained. So similarly, we can deduce that,

$$\frac{\eta_{\mathrm{VOA_1}}}{\eta_{\mathrm{VOA_2}}}=\left(\frac{1/2+\Delta_1}{1/2-\Delta_1}\right)\frac{\eta_{\mathrm{PIN2}}}{\eta_{\mathrm{PIN1}}}, \tag{39}$$

$$\frac{\eta_{\mathrm{VOA_3}}}{\eta_{\mathrm{VOA_4}}}=\left(\frac{1/2+\Delta_2}{1/2-\Delta_2}\right)\frac{\eta_{\mathrm{PIN4}}}{\eta_{\mathrm{PIN3}}}, \tag{40}$$

where η_{VOA_i} is the parameter indicating the transmissivity of the VOA_i and can be adjusted dynamically. Besides, Δ_1 and Δ_2 characterize the imbalance of the upper and the lower homodyne detector respectively, which are the reference values for dynamic adjustment of VOA_i. Details are as follows:

(i) When $\Delta_1<0$ and $\Delta_2<0$, only $\eta_{\mathrm{VOA_1}}$ in arm 1 and $\eta_{\mathrm{VOA_3}}$ in arm 3 need to be adjusted;

(ii) When $\Delta_1<0$ and $\Delta_2>0$, only $\eta_{\mathrm{VOA_1}}$ in arm 1 and $\eta_{\mathrm{VOA_4}}$ in arm 4 need to be adjusted;

(iii) When $\Delta_1>0$ and $\Delta_2<0$, only $\eta_{\mathrm{VOA_2}}$ in arm 2 and $\eta_{\mathrm{VOA_3}}$ in arm 3 need to be adjusted;

(iv) When $\Delta_1>0$ and $\Delta_2>0$, only $\eta_{\mathrm{VOA_2}}$ in arm 2 and $\eta_{\mathrm{VOA_4}}$ in arm 4 need to be adjusted.

Similarly, the adjustment of $\eta_{\mathrm{VOA_{5,6}}}$ is the same as that of $\eta_{\mathrm{VOA_{1,2,3,4}}}$. Through dynamic adjustment and quantitative analysis of the six VOAs, the extra excess noise caused by the unbalanced heterodyne detector can be eliminated and the performance of the practical CVQKD system can be improved.

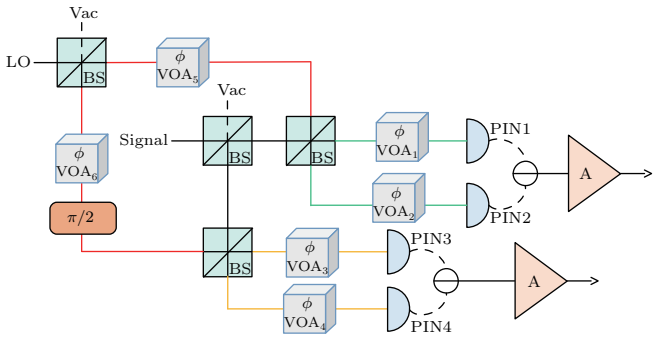


Fig. 4. The scheme of the countermeasure against the imbalance of the heterodyne detector. VOA: variable optical attenuator. The VOAs are set to rebalance the unbalanced heterodyne detector by attenuating the transmitted optical power of the corresponding arm.

6. Conclusion

Focusing on the practical heterodyne detector with imperfect components, for instance, a BS with non-ideal beam splitting ratio and photodiodes with mismatched quantum efficiency, we investigate the performance of the practical CVQKD system with an unbalanced heterodyne detector. The results show that such imperfections will inevitably induce extra excess noise, which decreases both the maximum secret key rate and the secure communication distance. And as the degree of imbalance increases, the secret key rate and the communication distance decrease more severely. We also find that the extra excess noise caused by the unbalanced heterodyne detector is proportional to the intensity of the local oscillator. Finally, we propose a possible countermeasure using six VOAs to counteract the impact of the unbalanced heterodyne detector to improve the performance of the practical CVQKD system.

Acknowledgments

Project supported by the National Natural Science Foundation of China (Grant No. 62001383) and the Natural Science Basic Research Plan in Shaanxi Province of China (Grant No. 2019JM-591).

Appendix A: Derivation for secret key rate with finite-size effect under collective attack

Considering collective attack, the secret key rate shared between Alice and Bob with finite-size effect can be defined as follows:

$$K_{\mathrm{finite}}=\frac{n}{N}\left[\beta I_{\mathrm{AB}}-\chi_{\mathrm{BE}}-\Delta(n)\right], \tag{A1}$$

where N is the length of valid data collected, n is the data length used for the final key rate generation, $m=N-n$ is the data length for parameter estimation, $\Delta(n)$ is a function related to privacy enhancement and β is the efficiency of reverse reconciliation. Moreover, I_{AB} is the amount of mutual information between Alice and Bob, which can be calculated as follows:

$$I_{\mathrm{AB}}^{\mathrm{het}}=\log_2\frac{V_{\mathrm{B}}}{V_{\mathrm{A|B}}}=\frac{V+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}} \tag{A2}$$

with the parameters $V=V_{\mathrm{A}}+1$, $\chi_{\mathrm{tot}}=\chi_{\mathrm{line}}+(\chi_{\mathrm{het}}/T)$, $\chi_{\mathrm{line}}=1/T-1+\xi$, $\chi_{\mathrm{het}}=(2(1+v_{\mathrm{el}})/\eta)-1$; here V_{A} is the modulation variance of Alice, χ_{tot} represents the total noise at the input of the channel, T is the transmittance of the channel, χ_{het} is the additive noise of the heterodyne detector, χ_{line} is the additive noise of the channel, v_{el} is the electric noise of the heterodyne detector and ξ is the excess noise of the system.

Besides, χ_{BE} represents the maximum amount of information that Eve can obtain from Bob, which is restricted by the Holevo bound.[40] χ_{BE} can be expressed as follows:

$$\chi_{\mathrm{BE}}=S(\rho_{\mathrm{E}})-\int \mathrm{d}m_{\mathrm{B}}\,p(m_{\mathrm{B}})S(\rho_{\mathrm{E}})^{m_{\mathrm{B}}}. \tag{A3}$$

For the Gaussian-modulated coherent states,[7] χ_{BE} can be simplified as follows:

$$\chi_{\mathrm{BE}}=\sum_{i=1}^{2}G\left(\frac{\lambda_i-1}{2}\right)-\sum_{i=3}^{5}G\left(\frac{\lambda_i-1}{2}\right), \tag{A4}$$

where $G(x)=(x+1)\log_2(x+1)-x\log_2 x$. λ_1 and λ_2 are the symplectic eigenvalue of the covariance matrix $\gamma_{\mathrm{AB_1}}$ characterizing the quantum state $\rho_{\mathrm{AB_1}}$, which has nothing to do with the

detection mode. λ_3, λ_4, and λ_5 are the symplectic eigenvalue of the covariance matrix $\gamma_{\mathrm{AFG}}^{m_{\mathrm{B}}}$ characterizing the quantum state $\rho_{\mathrm{AFG}}^{m_{\mathrm{B}}}$, where λ_3 and λ_4 are related to the detection mode. Considering the finite-size effect, the covariance matrix γ_{AB_1} of Gaussian modulation protocol can be written as:

$$\gamma_{\mathrm{AB}_1} = \begin{bmatrix} \gamma_{\mathrm{A}} & \sigma_{\mathrm{AB}_1}^T \\ \sigma_{\mathrm{AB}_1} & \gamma_{\mathrm{B}_1} \end{bmatrix} = \begin{bmatrix} (V_{\mathrm{A}}+1)I_2 & \sqrt{T_{\min}(V_{\mathrm{A}}^2+2V_{\mathrm{A}})}\sigma_z \\ \sqrt{T_{\min}(V_{\mathrm{A}}^2+2V_{\mathrm{A}})}\sigma_z & [T_{\min}(V_{\mathrm{A}}+\xi_{\max})+1]I_2 \end{bmatrix}, \tag{A5}$$

where matrices $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $T_{\min}$ and $\xi_{\max}$ represent the minimum value of the transmission effciency and the maximum value of the excess noise respectively. When m reaches a certain order of magnitude, for instance, $m > 10^6$, $T_{\min}$ and $\xi_{\max}$ can be calculated by

$$T_{\min} = (t_{\min})^2, \tag{A6}$$

$$\xi_{\max} = \frac{\sigma_{\max}^2 - 1}{T} \tag{A7}$$

with the following parameters

$$t_{\min} \approx \sqrt{T} - z_{\varepsilon_{\mathrm{PE}}/2}\sqrt{\frac{(1+T\xi)}{mV_{\mathrm{A}}}},$$

$$\sigma_{\max} \approx 1 + T\xi + z_{\varepsilon_{\mathrm{PE}}/2}\frac{(1+T\xi)\sqrt{2}}{\sqrt{m}}, \tag{A8}$$

where $z_{\varepsilon_{\mathrm{PE}}/2}$ can be calculated by

$$1 - \frac{1}{2}\mathrm{erf}(z_{\varepsilon_{\mathrm{PE}}/2}/2) = \frac{1}{2}\varepsilon_{\mathrm{PE}} \tag{A9}$$

with the error function

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x \mathrm{e}^{-t^2}\,\mathrm{d}t. \tag{A10}$$

Similarly, λ_3 and λ_4 can be calculated by covariance matrix $\gamma_{\mathrm{AFG}}^{m_{\mathrm{B}}}$ with parameter H_{het}:[41]

$$\gamma_{\mathrm{AFG}}^{m_{\mathrm{B}}} = \gamma_{\mathrm{AFG}} - \sigma_{\mathrm{AFG}B_3}^T H_{\mathrm{het}}\sigma_{\mathrm{AFG}B_3},$$
$$H_{\mathrm{het}} = (\gamma_{B_3} + I_2)^{-1}. \tag{A11}$$

Hence λ_i $(i = 1,2,3,4,5)$ can be calculated as follows by referring to equations from Eqs. (A4)–(A11)

$$\lambda_{1,2}^2 = \frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right),$$
$$\lambda_{3,4}^2 = \frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right),$$
$$\lambda_5 = 1 \tag{A12}$$

with the following parameters:[42]

$$A = (V_A+1)^2 - 2T_{\min}\left(V_A^2+2V_A\right) + \left[T_{\min}\left(V_A+\xi_{\max}\right)+1\right]^2, \quad B = \left[\left(T_{\min}\xi_{\max}+1\right)\left(V_A+1\right) - T_{\min}V_A\right]^2,$$
$$C = \frac{A[2(1+v_{\mathrm{el}})/\eta - 1]^2 + B + 1 + 2T_{\min}(V_A^2+2V_A)}{T_{\min}^2[V_A + 1/T_{\min} + \xi_{\max} + (2-\eta+2v_{\mathrm{el}})/T_{\min}]^2} + \frac{[4(1+v_{\mathrm{el}})/\eta - 2][(V_A+1)\sqrt{B} + T_{\min}(V_A + 1/T_{\min} + \xi_{\max})]}{T_{\min}^2[V_A + 1/T_{\min} + \xi_{\max} + (2-\eta+2v_{\mathrm{el}})/T_{\min}]^2},$$
$$D = \frac{[V_A + 1 + \sqrt{B}(2+2v_{\mathrm{el}} - \eta)/\eta]^2}{T_{\min}^2[V_A + 1/T_{\min} + \xi_{\max} + (2-\eta+2v_{\mathrm{el}})/T_{\min}]^2}. \tag{A13}$$

As mentioned before, $\Delta(n)$ is a linear function related to privacy enhancement, which can be written as follows:

$$\Delta(n) = 7\sqrt{\frac{\log_2(2/\varepsilon_{\mathrm{PE}})}{n}} + \frac{2}{n}\log_2(1/\varepsilon_{\mathrm{PE}}), \tag{A14}$$

here $\varepsilon_{\mathrm{PE}}$ depicts the failure probability of the parameter estimation.

References

[1] Ralph T C 1999 *Phys. Rev. A* **61** 010303
[2] Reid M D 2000 *Phys. Rev. A* **62** 062308
[3] Braunstein S L and Van Loock P 2005 *Rev. Mod. Phys.* **77** 513
[4] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621
[5] Bennett C H and Brassard G 1984 *Proceeding of International Conference on Computers Systems and Signal Processing*, December 10-12, Bangalore, India, p. 175
[6] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[7] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
[8] Chi Y M, Qi B, Zhu W, Qian L, Lo H K, Youn S H, Lvovsky A and Tian L 2011 *New J. Phys.* **13** 013003
[9] Carleton H R and Maloney W T 1968 *Appl. Opt.* **7** 1241
[10] Yuen H P and Chan V W S 1983 *Opt. Lett.* **8** 177
[11] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
[12] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2005 *Phys. Rev. A* **73** 022316
[13] Zeng G H 2010 *Quantum Private Communication* (Beijing: Higher Education Press) pp. 260–309
[14] Qi B, Huang L L, Qian L and Lo H K 2007 *Phys. Rev. A* **76** 052323
[15] Huang D, Lin D K, Wang C, Liu W Q, Fang S H, Peng J Y, Huang P, and Zeng G H 2015 *Opt. Express* **23** 17511
[16] Huang D, Huang P, Lin D K and Zeng G H 2016 *Sci. Rep.* **6** 19201
[17] Huang D, Huang P, Li H, Wang T, Zhou Y M, Zeng G H 2016 *Opt. Lett.* **41** 3511
[18] Jouguet P, Kunz-Jacques S, Debuisschert T, Fossier S, Diamanti E, Alléaume R, Tualle-Brouri R, Grangier P, Leverrier A, Pache P and Painchault P 2012 *Opt. Express* **20** 14030

[19] Navascués M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502

[20] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503

[21] Bugge A N, Sauge S, Ghazali A M M, Skaar J, Lydersen L and V. Makarov 2014 *Phys. Rev. Lett.* **112** 070503

[22] Huang A Q, Navarrete Á, Sun S H, Chaiwongkhot P, Curty M and Makarov V 2019 *Phys. Rev. Appl.* **12** 064043

[23] Huang A Q, Li R, Egorov V, Tchouragoulov S, Kumar K and Makarov V 2020 *Phys. Rev. Appl.* **13** 034017

[24] Jouguet P, Kunz-Jacques S and Diamanti E 2013 *Phys. Rev. A* **87** 062313

[25] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev. A* **88** 022339

[26] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev. A* **87** 052309

[27] Huang J Z, Weedbrook C, Yin Z Q, Wang S, Li H W, Chen W, Guo G C and Han Z F 2013 *Phys. Rev. A* **87** 062329

[28] Kunz-Jacques S and Jouguet P 2015 *Phys. Rev. A* **91** 022307

[29] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[30] Liu W Q, Peng J Y, Qi J, Cao Z W and He C 2020 *Laser Phys. Lett.* **17** 055203

[31] Cives-Esclop A, Luis A and Sánchez-Soto L L 2000 *Opt. Commun.* **175** 153

[32] Kühn B and Vogel W 2016 *Phys. Rev. Lett.* **116** 163603

[33] Huang Y D, Zhang Y C, Xu B J, Huang L Y and Yu S 2020 *J. Phys. B: At. Mol. Opt. Phys* **54** 015503

[34] Almeida M, Pereira D, Facão M, Pinto A N and Silva N A 2020 *Opt. Quant. Electron.* **52** 503

[35] Wallentowitz S and Vogel W 1996 *Phys. Rev. A* **53** 4528

[36] Silva N A, Pereira D, Muga N J and Pinto A N 2020 *Proceedings of the* 2020 22*nd International Conference on Transparent Optical Networks*, July 19–23, Bari, Italy, p. 1

[37] Huang L Y, Zhang Y C and Yu S 2021 *Chin. Phys. Lett.* **38** 040301

[38] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev. A* **81** 062343

[39] Zheng Y, Huang P, Huang A Q, Peng J Y and Zeng G H 2019 *Phys. Rev. A* **100** 012313

[40] Holevo A S 1973 *Problems Inform. Transmission* **9** 177

[41] Garcia-Patron Sanchez R 2007 "Quantum information with optical continuous variables: from Bell tests to key distribution", Ph.D. dissertation (Brussels: Université libre de Bruxelles)

[42] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R and Grangier P 2009 *J. Phys. B-At. Mol. Opt. Phys.* **42** 114014