

Finite-size analysis of eight-state continuous-variable quantum key distribution with the linear optics cloning machine

Hang Zhang(张航), Yu Mao(毛宇), Duan Huang(黄端), Ying Guo(郭迎), Xiaodong Wu(吴晓东), Ling Zhang(张玲)

Citation: Chin. Phys. B . 2018, 27(9): 090307. **doi:** 10.1088/1674-1056/27/9/090307

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Continuous-variable quantum key distribution based on continuous random basis choice

Weiqi Liu(刘维琪), Jinye Peng(彭进业), Peng Huang(黄鹏), Shiyu Wang(汪诗寓), Tao Wang(王涛), Guihua Zeng(曾贵华)

Chin. Phys. B . 2018, 27(7): 070305. **doi:** 10.1088/1674-1056/27/7/070305

Practical security of continuous-variable quantum key distribution under finite-dimensional effect of multi-dimensional reconciliation

Yingming Zhou(周颖明), Xue-Qin Jiang(蒋学芹), Weiqi Liu(刘维琪), Tao Wang(王涛), Peng Huang(黄鹏), Guihua Zeng(曾贵华)

Chin. Phys. B . 2018, 27(5): 050301. **doi:** 10.1088/1674-1056/27/5/050301

Entangled-photons generation with quantum dots

Yuan Li(李远), Fei Ding(丁飞), Oliver G Schmidt

Chin. Phys. B . 2018, 27(2): 020307. **doi:** 10.1088/1674-1056/27/2/020307

Balancing four-state continuous-variable quantum key distribution with linear optics cloning machine

Xiao-Dong Wu(吴晓东), Qin Liao(廖骎), Duan Huang(黄端), Xiang-Hua Wu(吴湘华), Ying Guo(郭迎)

Chin. Phys. B . 2017, 26(11): 110304. **doi:** 10.1088/1674-1056/26/11/110304

Spherical reconciliation for a continuous-variable quantum key distribution

Zhao Lu(卢钊), Jian-Hong Shi(史建红), Feng-Guang Li(李风光)

Chin. Phys. B . 2017, 26(4): 040304. **doi:** 10.1088/1674-1056/26/4/040304

Finite-size analysis of eight-state continuous-variable quantum key distribution with the linear optics cloning machine*

Hang Zhang(张航), Yu Mao(毛宇), Duan Huang(黄端), Ying Guo(郭迎), Xiaodong Wu(吴晓东), and Ling Zhang(张玲)†

School of Information Science and Engineering, Central South University, Changsha 410083, *China*

(Received 27 January 2018; revised manuscript received 17 May 2018; published online 10 August 2018)

We propose a method to improve the secret key rate of an eight-state continuous-variable quantum key distribution (CVQKD) by using a linear optics cloning machine (LOCM). In the proposed scheme, an LOCM is exploited to compensate for the imperfections of Bob's apparatus, so that the generated secret key rate of the eight-state protocol could be well enhanced. We investigate the security of our proposed protocol in a finite-size scenario so as to further approach the practical value of a secret key rate. Numeric simulation shows that the LOCM with reasonable tuning gain λ and transmittance τ can effectively improve the secret key rate of eight-state CVQKD in both an asymptotic limit and a finite-size regime. Furthermore, we obtain the tightest bound of the secure distance by taking the finite-size effect into account, which is more practical than that obtained in the asymptotic limit.

Keywords: continuous-variable quantum key distribution, linear optics cloning machine, finite-size

PACS: 03.67.Hk, 03.67.–a, 03.67.Dd **DOI:** 10.1088/1674-1056/27/9/090307

1. Introduction

Quantum key distribution (QKD) has been a significant practical application in quantum-information science,[1,2] which allows two distant parties to share a secret key over an untrusted quantum channel that is controlled by an eavesdropper. For decades, continuous-variable (CV) QKD has become a hotspot of QKD research due to its high detection efficiency and high key rate.[3–5] It has been certified to be secure against arbitrary collective attacks,[6] which are optimal in the asymptotic limit.

In general, there are two main modulation approaches in CVQKD, called Gaussian modulated CVQKD and discretely modulated CVQKD. A CVQKD protocol based on coherent states with Gaussian modulation has been experimentally demonstrated[7] and has been shown to be secure against arbitrary collective attacks.[8] However, the level of signal-to-noise ratio (SNR) has an important effect on the reconciliation efficiency β of this protocol, which could only achieve a short transmission distance. Recently, an irregular low-density-parity-check (LDPC) technique, i.e., MET-LDPC code[9] and multi-edge quasi-cyclic LDPC codes[10] with a GPU-based decoder have been proposed to reach a high reconciliation efficiency over 95%. However, it would have a high cost of equipment on the practical operation to obtain a high reconciliation efficiency. Fortunately, there is another approach to solve the problem, that is, using discrete modulation such as the four-state CVQKD protocol, proposed by Leverrier *et al.*,[8,11] which generates four nonorthogonal coherent states and exploits the sign of the measured quadrature of each state to encode information rather than using the quadrature $\hat{x}$ or $\hat{p}$ itself. This is the reason why the sign of the measured quadrature is already the discrete value to which the most excellent error-correcting codes are suitable even at very low SNR.[12] In the experimental field, a fiber-based four-state discrete modulation CVQKD system has been demonstrated and various factors that lead to excess noises have also been discussed with the emphasis on the influence of the relative phase fluctuations and local field scattering process.[13,14] Although the security analysis of four-state has not been perfectly proven, we could also find some merits of the discrete modulation scheme such as the concise modulation process and less consumption of the random number.[14]

Recently, a better discretely-modulated scheme with higher secret key rate and longer transmission distance, called the eight-state protocol, was proposed,[15] which potentially provides a better performance by offering a higher secret key rate, better excess noise tolerance, and longer secure transmission distance.[16] Since the discretely modulated eight-state protocol exhibits excellent performance at low SNR, we further enhance its capability by applying a linear optics cloning machine (LOCM) at Bob's apparatus. The LOCM, in fact, is the cloning machine which can be practically implemented using just linear optics, heterodyne measurement, and controlled displacements.[17] It is remarkable that the LOCM used here does not violate the non cloning theorem since we make approximate copies instead of perfect copies of quantum states in our protocol.[18] The proposed scheme (eight-state protocol with an LOCM operation) can improve the generated secret

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61379153 and 61572529).

†Corresponding author. E-mail: lingzhang2017@foxmail.com

© 2018 Chinese Physical Society and IOP Publishing Ltd

key rate of the eight-state protocol by tuning its parameters in appropriate ranges to compensate for the imperfection of the detector at Bob's side with only a slight cost of transmission distance.

In addition, the asymptotic limit is a universal method when performing a security analysis of the CVQKD protocol.[19–21] However, the length of secret key is impossibly unlimited in practice.[22,23] Moreover, one can make the assumption in the asymptotic case that the quantum channel is perfectly known before the transmission is performed, while in a finite-size scenario, one actually does not know the characteristics of the quantum channel in advance, because a part of exchanged signals has to be used for parameter estimation rather than the generation of a secret key.[24] Thus in this paper, the finite-size effect will be taken into consideration. We draw a comparison between the finite-size scenario and the asymptotic case, and discuss the value of the secret key rate with a different number of exchanged signals N.

This paper is organized as follows. In Section 2, we describe the schematic configuration of the eight-state CVQKD protocol based on LOCM operation in detail. In Section 3, we characterize the theoretical analysis of the proposed protocol, and calculate the secret key rate in the finite-size scenario. In Section 4, numeric simulation and performance analysis are discussed. Our conclusions are drawn in Section 5.

2. Eight-state CVQKD with LOCM inserted

In this section, we mainly elaborate the discretely-modulated eight-state CVQKD protocol with an LOCM. To make the derivation self-contained, we firstly briefly introduce the original eight-state CVQKD protocol.

2.1. Description of the eight-state CVQKD protocol

We first take a brief review of the discretely modulated CVQKD protocols. Until now, some types of discretely modulated CVQKD protocols have been proposed, such as the two-[8] and four-state protocols.[25] The discretely modulated protocols can be generalized to the one with N coherent states $|\alpha_k\rangle = |\alpha e^{2ik\pi/N}\rangle$, where α is a positive number related to the modulation variance as $V_A = 2\alpha^2$. Without loss of generality, we focus on the discretely modulated protocol with $N = 8$, which corresponds to the eight-state protocol.

In the prepare-and-measure (PM) scheme of the eight-state CVQKD protocol,[15] Alice firstly prepares one of the eight coherent states,

$$\beta_k = \alpha e^{ik\pi/4}, \quad k = 0,1,2,\ldots,7. \tag{1}$$

Alice then randomly sends one of these eight coherent states to Bob with equal probability through an insecure quantum channel controlled by an eavesdropper called Eve,[26] see Fig. 1(a). For a certain channel, that is, given the transmittance T and excess noise ε, we can set the value of the α to maximize the secret key rate.[27] After receiving the coherent state, Bob measures randomly one of the quadratures in homodyne detection and decodes the information by the sign of his measurement result.

Afterwards, Bob sends the absolute value results to Alice through a classical channel, in which approach Alice and Bob share correlated strings of bits. Then through the operations of error reconciliation and privacy amplification, the secret key can be obtained.

The PM version is relatively easy to implement, but its security is hard to be proved directly.[28] Hence, the security we describe is established by considering the equivalent entanglement-based version of the protocol. In the EB version, Alice initially uses a purification $|\Phi\rangle$ of two-mode entangled state[29]

$$|\Phi_{AB}(\alpha)\rangle = \frac{1}{4}\sum_{k=0}^{7}|\psi_k\rangle|\beta_k\rangle, \tag{2}$$

where the states

$$|\psi_k\rangle = \frac{1}{2}\sum_{m=0}^{7} e^{-i(1+4k)m\pi/4}|\phi_m\rangle, \quad k = 0,1,2,\ldots,7 \tag{3}$$

are a non-Gaussian orthogonal state, and

$$|\phi_k\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}}\sum_{n=0}^{\infty}(-1)^n\frac{\alpha^{8n+k}}{\sqrt{(8n+k)!}}|8n+k\rangle, \quad k = 0,1,2,\ldots,7 \tag{4}$$

where

$$\begin{cases}
\lambda_{0(4)} = \frac{1}{4}e^{-\alpha^2}\left[\cosh(\alpha^2)+\cos(\alpha^2)\pm 2\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\right],\\
\lambda_{1(5)} = \frac{1}{4}e^{-\alpha^2}\left[\sinh(\alpha^2)+\sin(\alpha^2)\pm 2\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right)\pm\sqrt{2}\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\right],\\
\lambda_{2(6)} = \frac{1}{4}e^{-\alpha^2}\left[\cosh(\alpha^2)-\cos(\alpha^2)\pm 2\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right)\right],\\
\lambda_{3(7)} = \frac{1}{4}e^{-\alpha^2}\left[\sinh(\alpha^2)-\sin(\alpha^2)\mp 2\cos\left(\frac{\alpha^2}{\sqrt{2}}\right)\sinh\left(\frac{\alpha^2}{\sqrt{2}}\right)\pm\sqrt{2}\sin\left(\frac{\alpha^2}{\sqrt{2}}\right)\cosh\left(\frac{\alpha^2}{\sqrt{2}}\right)\right].
\end{cases} \tag{5}$$

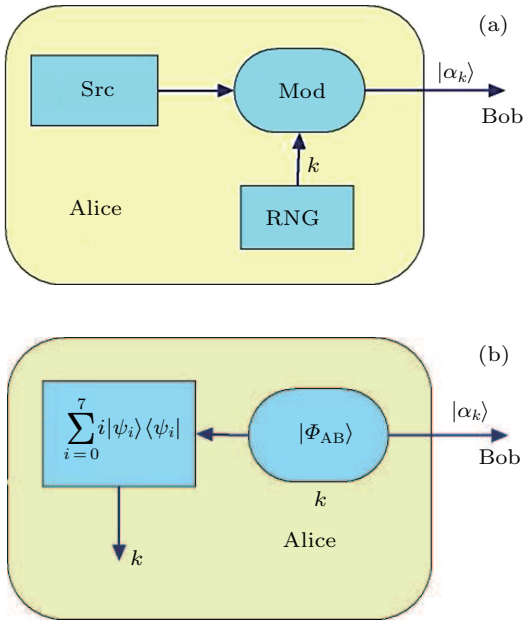


Fig. 1. (color online) (a) PM scheme of the eight-state CV-QKD protocol: Alice obtained the random number k from a random number generator (RNG), and then modulated the original state sent from the source by the modulator. (b) The equivalent EB version of the protocol: Alice prepared a two-mode entangled state, one mode was measured to get the result k. The other state of the mode was sent to Bob.

We can describe the eight-state CVQKD protocol performed in the entanglement-based (EB) version, see Fig. 1(b). Alice prepares the entangled state $|\Phi_{AB}\rangle$ and performs the projective measurement $\{|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|, \ldots, |\psi_7\rangle\langle\psi_7|\}$ on her half. When her measurement gives the result k, the coherent state $|\alpha_k\rangle$ is sent through the quantum channel to Bob who measures both of the quadratures with a heterodyne detection.[30] The EB version provides a valid security proof against collective attacks through the covariance matrix γ_{AB} of the state before their respective measurements.[31]

The covariance matrix $\gamma_{A_0B_0}$ of the original eight-state $|\Phi_{AB}(\alpha)\rangle$ is

$$\gamma_{A_0B_0} = \begin{bmatrix} V\boldsymbol{I}_2 & Z_8\sigma_z \\ Z_8\sigma_z & V\boldsymbol{I}_2 \end{bmatrix}, \tag{6}$$

where $\boldsymbol{I}_2$ is the 2×2 identity matrix, and $\sigma_z = \mathrm{diag}(1,-1)$, $V = 2\alpha^2+1 = V_A+1$ is the variance of quadratures for modes A and B, and

$$Z = V_A \sum_{k=0}^{7} \frac{\lambda_{k-1}^{3/2}}{\lambda_k^{1/2}} \tag{7}$$

reflects the relationship between mode A and mode B.

2.2. The improved eight-state scheme with LOCM

Due to the imperfection in Bob's apparatus, the detection process cannot be ideal, which will mean the final secret key rate is lower than expectation.[32] Fortunately, the effect of imperfect apparatus can be compensated by applying a linear optics cloning machine.[33] In what follows, we elaborate the proposed eight-state CVQKD with an LOCM placed at Bob's side. It is remarkable that the LOCM used here does not violate the non-cloning theorem since we make approximate copies instead of perfect copies of quantum states in our protocol.[18] Figure 2 shows the EB version of the proposed scheme against Eve's collective attacks.

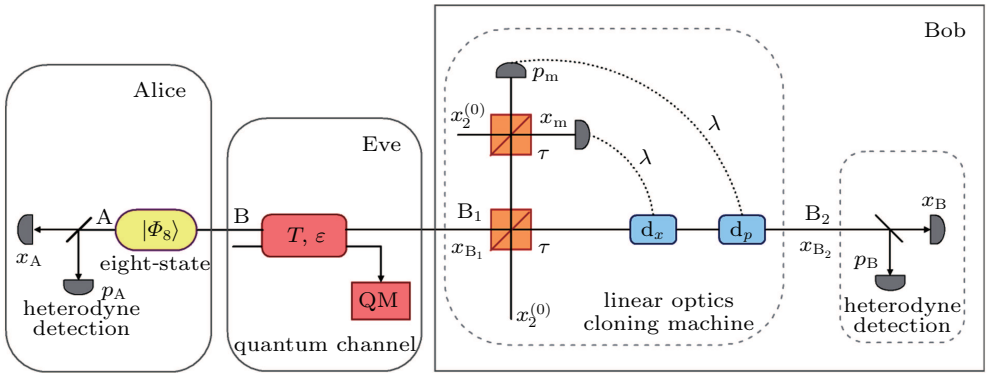


Fig. 2. (color online) The EB scheme for the eight-state CVQKD protocol with LOCM operation. λ and τ are two critical parameters of LOCM. Alice randomly prepares one of the eight-state discrete-modulated states and sends it to Bob through the unsecure quantum channel controlled by an eavesdropper, Eve. Additionally, an LOCM is placed in the input of Bob's apparatus. Bob detects the received mode to derive a sequence of bits shared with Alice by using the heterodyne detector.

Firstly, Alice prepares an entangled state $|\Phi_8\rangle$, one mode of the modulated state with variance $V = V_A + 1$ is sent to Bob through an insecure quantum channel. At Alice's side, she applies the heterodyne detection and obtains two measurements $\hat{x}_A$ and $\hat{p}_A$.[34] After the quantum channel, the mode goes through the LOCM which is placed in the input of Bob's side and then is detected by Bob's apparatus with heterodyne detection. The LOCM consists of two beam splitters (BS) with the transmission efficiency τ and two phase operations with tuning gain λ. Bob prepares two vacuum states $\hat{x}_1^{(0)}$ and $\hat{x}_2^{(0)}$, then the LOCM operation is implemented, and Bob measures both quadratures simultaneously via performing heterodyne detection. As displayed in Fig. 2, we can obtain[35]

$$\hat{x}_m = \frac{1}{\sqrt{2}}(\hat{x}_1 + \hat{x}_2^{(0)}) = \sqrt{\frac{\tau}{2}}\hat{x}_{\mathrm{B}_1} + \sqrt{\frac{1-\tau}{2}}\hat{x}_1^{(0)} + \frac{1}{\sqrt{2}}\hat{x}_2^{(0)}. \quad (8)$$

The transmitted mode $\hat{x}_2$ can be expressed as

$$\hat{x}_2 = \sqrt{1-\tau}\hat{x}_{\mathrm{B}_1} - \sqrt{\tau}\hat{x}_1^{(0)}. \quad (9)$$

Based on the measuring result $\hat{x}_{\mathrm{m}}$ and the tuning gain λ, we can derive the relationship of the transmitted mode that could be written as

$$\hat{x}_{\mathrm{B}_2} = \hat{x}_2 + \lambda\hat{x}_{\mathrm{m}}. \quad (10)$$

On the basis of the calculations above, we can obtain the variance $V_{\mathrm{B}_2} := \langle \hat{x}_{\mathrm{B}_2}^2 \rangle$ of mode $\hat{x}_{\mathrm{B}_2}$ as follows:

$$V_{\mathrm{B}_2} = \left(\sqrt{1-\tau} + \lambda\sqrt{\frac{\tau}{2}}\right)^2 V_{\mathrm{B}_1} + \frac{\lambda^2}{2} + \left(\lambda\sqrt{\frac{1-\tau}{2}} - \sqrt{\tau}\right)^2. \quad (11)$$

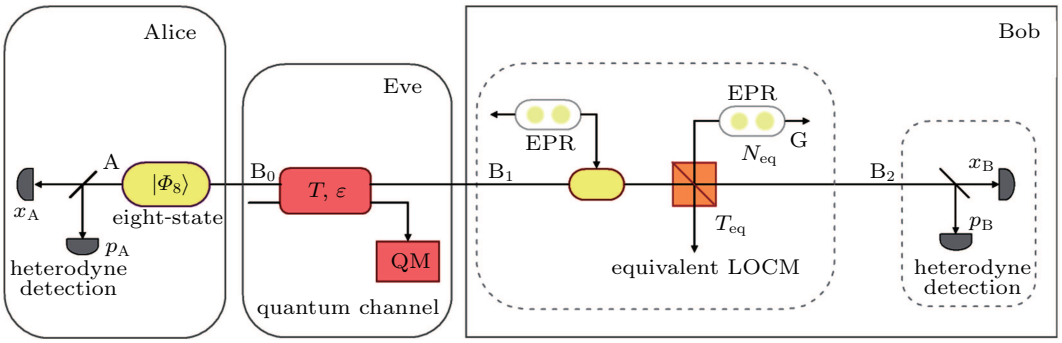


Fig. 3. (color online) Equivalent eight-state CVQKD protocol with a thermal state of variance N_{eq} characterized by the tunable noise χ_{eq} and transmittance T_{eq}.

In order to expediently discuss the security of the protocol, we establish an equivalent system by considering the entanglement-based version of the protocol, as shown in Fig. 3. Accordingly, the expression of equivalent transmittance T_{eq} is given by

$$T_{\mathrm{eq}} = \left(\sqrt{1-\tau} + \lambda\sqrt{\frac{\tau}{2}}\right)^2. \quad (12)$$

It should be noted that the equivalent transmittance T_{eq} limits of a numerical range in $[0,1]$. Thus, we can derive the LOCM-tuned noise χ_{eq} with two parameters λ and τ referred to Bob's input, the expression can be written as

$$\chi_{\mathrm{eq}} = \frac{\frac{\lambda^2}{2} + \left(\lambda\sqrt{\frac{1-\tau}{2}} - \sqrt{\tau}\right)^2}{\left(\sqrt{1-\tau} + \lambda\sqrt{\frac{\tau}{2}}\right)^2}. \quad (13)$$

In the equivalent scheme, Bob's detection efficiency is modeled by a beam splitter with transmission efficiency T_{eq}. An EPR state with variance N_{eq} is used to model the thermal noise υ_{el} that is introduced by the process of Bob's detector,[36] where $N_{\mathrm{eq}} = (T_{\mathrm{eq}}\chi_{\mathrm{eq}} - 1)/(1 - T_{\mathrm{eq}})$ is for heterodyne detection. After that, Bob implements reverse reconciliation and privacy amplification to generate the final bit string of the secret key shared with Alice.

In this section, we introduce the EB version of the proposed eight-state scheme using LOCM, and establish an equivalent scheme. By utilizing an LOCM, the performance of eight-state CVQKD can be enhanced especially in terms of the secret key rate.

3. Security analysis in finite-size regime

In order to simplify the theoretical QKD security proofs, researchers usually expand their theories based on some assumptions, which can be more or less explicit. One assumption might be considered that the security of a protocol in the asymptotic regime of infinitely numerous signals could be exchanged by Alice and Bob.[37] However, the number of exchanged signals cannot be infinite, Alice and Bob need some signals for parameter estimation so that they can ensure the accuracy of QKD.[38] We here consider the secret key rate K_{f} that is derived from heterodyne detection in the finite-size scenario where the number of exchanged signals is confined to a finite value. The finite-size scenario includes the loss of parameter estimation, so the analysis can be closer to the realistic value than the asymptotic scenario.

In the following, we mainly focus the analysis on heterodyne detection in the case of reverse reconciliation.[39] N denotes the total number of signals exchanged by Alice and Bob during the protocol. n is the segmental number of N signals that is used for establishment of the secret key, and $m = N - n$ signals will be used in parameter estimation. Hence, in the case of a CVQKD protocol, the finite-size secret key rate can be written as

$$K_{\mathrm{f}} = \frac{n}{N}[\beta I(x:y) - S_{\varepsilon_{\mathrm{PE}}}(y:E) - \Delta(n)], \quad (14)$$

where β is the efficiency of reconciliation, which ranges from 0 when no information was extracted to 1 for a perfect reconciliation scheme. $I(x:y)$ represents mutual information be-

tween Alice and Bob. $S_{\varepsilon_{\rm PE}}(y:E)$ is defined as the maximum conditional entropy compatible with the statistics given by the parameter estimation except with probability $\varepsilon_{\rm PE}$, and $\Delta(n)$ is related to the security of the privacy amplification.

The term $\Delta(n)$ related to security of privacy amplification can be written as

$$\Delta(n) \equiv (2\dim \mathcal{H}_x + 3)\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}} + \frac{2}{n}\log_2(1/\varepsilon_{\rm PA}), \quad (15)$$

where $\mathcal{H}_x$ is the Hilbert space corresponding to the variable x used in the raw key, $\bar{\varepsilon}$ is the smoothing parameter, $\varepsilon_{\rm PA}$ is the failure probability of the privacy amplification procedure. Generally, we have $\mathcal{H}_x = 2$ since for all continuous-variable protocols. Moreover, the second term can be neglected because the convergence speed of $2/n$ is faster than $\log_2(1/\varepsilon_{\rm PA})$ largely. So, we have $\Delta(n)$ as a function of n,

$$\Delta(n) \simeq 7\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}}. \quad (16)$$

The efficiency of reconciliation is set to 0.95,[14] and the mutual information $I(x:y)$ for heterodyne detection can be expressed as

$$I(x:y) = \log_2 \frac{V_{\rm B}}{V_{\rm B|A}} = \log_2 \frac{V+\chi_{\rm tot}}{1+\chi_{\rm tot}}, \quad (17)$$

where $V = V_{\rm A}+1$, $\chi_{\rm tot} = \chi_{\rm line} + \chi_{\rm LOCM}/T$ represent the total noise referred to the channel input, $\chi_{\rm line} = 1/T + \varepsilon - 1$, and $\chi_{\rm LOCM}$ can be calculated as

$$\chi_{\rm LOCM} = \frac{(1-T_{\rm eq})N_{\rm eq}}{T_{\rm eq}} = \frac{\lambda^2 - 2 + (\lambda\sqrt{1-\tau} - \sqrt{2\tau})^2}{(\sqrt{2(1-\tau)} + \lambda\sqrt{\tau})^2}. \quad (18)$$

In order to calculate $S_{\varepsilon_{\rm PE}}(y:E)$, first we have a matrix representing the shared state $\rho_{\rm AB_1}$,

$$\gamma_{\rho_{\rm AB_1}} = \begin{bmatrix} (V_{\rm A}+1)\boldsymbol{I}_2 & \sqrt{T}Z_8\boldsymbol{\sigma}_z \\ \sqrt{T}Z_8\boldsymbol{\sigma}_z & (TV_{\rm A}+1+T\varepsilon)\boldsymbol{I}_2 \end{bmatrix}, \quad (19)$$

where $\boldsymbol{I}_2$ is the 2×2 identity matrix, and $\boldsymbol{\sigma}_z = {\rm diag}(1,-1)$.

We need to evaluate the covariance matrix $\gamma_{\rho_{\rm AB_1}}$ compatible with the exchanged data except with failure probability of parameter estimation $\varepsilon_{\rm PE}$. Parameters estimation of covariance matrix $\gamma_{\varepsilon_{\rm PE}}$ can be implemented by sampling of m couples of correlated variables $(x_i, y_i)_{i=1,2,\ldots,m}$. Thus, we can find a covariance matrix $\gamma_{\varepsilon_{\rm PE}}$ which successfully minimizes the secret key rate $K_{\rm f}$ as follows:

$$\gamma_{{\rm AB_1}\varepsilon_{\rm PE}} = \begin{bmatrix} (V_{\rm A}+1)\boldsymbol{I}_2 & t_{\min}Z_8\boldsymbol{\xi}_z \\ t_{\min}Z_8\boldsymbol{\xi}_z & (t_{\min}V_{\rm A} + \xi^2_{\max})\boldsymbol{I}_2 \end{bmatrix}, \quad (20)$$

where $t_{\min}$ represents the minimum of $\sqrt{T}$, and $\xi^2_{\max}$ indicates the maximum of ξ^2 compatible with sample couples.

The parameters $t_{\min}$ and $\xi^2_{\max}$ can be calculated respectively as

$$\begin{cases} t_{\min} = \sqrt{T} - Z_{\varepsilon_{\rm PE}/2}\sqrt{\dfrac{1+T\varepsilon}{mV_{\rm A}}}, \\ \xi^2_{\max} = 1 + T\varepsilon + Z_{\varepsilon_{\rm PE}/2}\dfrac{\sqrt{2}(1+T\varepsilon)}{\sqrt{m}}. \end{cases} \quad (21)$$

Then, we can obtain symplectic eigenvalues $\lambda_{1,2,3,4,5}$ as follows:

$$\begin{aligned} \lambda_{1,2} &= \sqrt{\frac{1}{2}(A \pm \sqrt{A^2-4B})}, \\ \lambda_{3,4} &= \sqrt{\frac{1}{2}(C \pm \sqrt{C^2-4D})}, \\ \lambda_5 &= 1. \end{aligned} \quad (22)$$

with

$$\begin{aligned} A &= \det\gamma_{A_{\varepsilon_{\rm PE}}} + \det\gamma_{B_{1\varepsilon_{\rm PE}}} + 2\det\sigma_{AB_{1\varepsilon_{\rm PE}}}, \\ B &= \det\gamma_{AB_{1\varepsilon_{\rm PE}}}, \\ C &= \frac{A\chi^2_{\rm LOCM} + B + 1 + 2\chi_{\rm LOCM}[V\sqrt{B} + T(V+\chi_{\rm line}) + 2TZ_8]}{T^2(V+\chi_{\rm tot})^2}, \\ D &= \left(\frac{V+\sqrt{B}\chi_{\rm LOCM}}{T(V+\chi_{\rm tot})}\right)^2. \end{aligned} \quad (23)$$

The $S_{\varepsilon_{\rm PE}}(y:E)$ can be derived by

$$S_{\varepsilon_{\rm PE}}(y:E) = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \quad (24)$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$.

4. Performance analysis

In this section, we mainly research the effect of the LOCM operation on the performance of the eight-state CV-QKD protocol for reverse reconciliation with the heterodyne detection. We consider the secret key rate $K_{\rm f}$ under the circumstance that the estimation of $\bar{t}$ and $\bar{\xi}^2$ are equivalent to their expected values, see Eq. (21). Based on the security analysis above, the performance of LOCM in our scheme mainly depends on two parameters τ and λ. In our simulation, the fluctuation of the value of excess noise ε[40,41] exerts a small influence on the final value of secret key rate $K_{\rm f}$, thus we set ε to be a conservative value $\varepsilon = 0.005$. More details of parameter settings are shown in Table 1. Furthermore, the relationship between transmission distance d and transmissivity T is $T = 10^{-ad/10}$, where d represents the length of the quantum channel and $a = 0.2$ dB/km means the loss coefficient of optical fibers.

The analysis of the equivalent state allows us to compare the secret key rate obtained with and without an LOCM operation in the finite-size scenario. As is shown in Eq. (12),

the equivalent transmittance T_{eq} has a relationship with two parameters of LOCM, λ and τ. We need to notice that the constraint $T_{eq} \in [0,1]$. Thus, it is necessary for us to solve the parameter λ in an available range $[0, \sqrt{2}(1-\sqrt{1-\tau})/\sqrt{\tau}]$ for the given parameter $\tau \in [0,1]$. Afterwards, the function of T_{eq} has been plotted, as can be seen in Fig. 4, which is of value for us to find the applicable parameter T_{eq} according to the values of λ and τ. Thus, we can regulate T_{eq} in a valid range by properly tuning these two parameters.

Table 1. Parameter settings in the simulation.

Symbol	Parameters description	Values
T	transmission efficiency	independent variable
ε	excess noise	0.005
τ	transmittance of LOCM	changed
λ	tuning gain of LOCM	changed
η	detection efficiency	0.6
β	reconciliation efficiency	0.95
V_A	Alice's modulated variance	0.25
υ_{el}	thermal noise	0.05

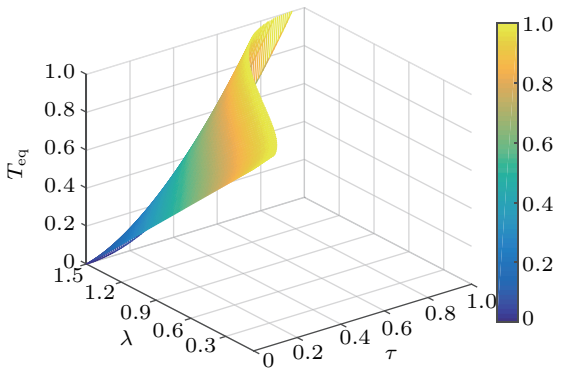


Fig. 4. (color online) The LOCM-tuned transmittance T_{eq} as a function of two parameters λ and τ. By choosing appropriate parameter values, the transmittance T_{eq} can be regulated in [0,1].

Based on the analysis above, we take $\tau = \{0.25, 0.45, 0.65\}$ as examples, the corresponding T_{eq} can be calculated from Eq. (12) by $\{0.945, 0.781, 0.582\}$, where the tuning gain λ is 0.3. The secret key rate K_f in the finite-size regime can be derived in Fig. 5(a). It is clear that the secret key rate of eight-state CVQKD using LOCM operation has a better performance than the original eight-state protocol. Furthermore, by tuning the value of parameter τ to be smaller in a suitable range, we can obtain the higher secret key rate and longer maximum transmission distance.

Accordingly, we can use the similar analytical approach to take the fixed efficiency $\tau = 0.45$ for example to illustrate the effect of the tuning gain λ on the eight-state protocol with LOCM. Here, we choose $\lambda = \{0.1, 0.3, 0.5\}$, and the values of the corresponding T_{eq} are $\{0.623, 0.781, 0.958\}$, the numeral relation can be displayed in Fig. 5(b). It is remarkable that by using LOCM operation the secret key rate under the analysis of finite-size scenario is increased obviously for the eight-state protocol in comparison to the original protocol, which means that the modified protocol has better security on a collective Gaussian attack. Besides we can achieve the higher secret key rate and longer maximum transmission distance by tuning the value of parameter λ to be larger in a compatible range.

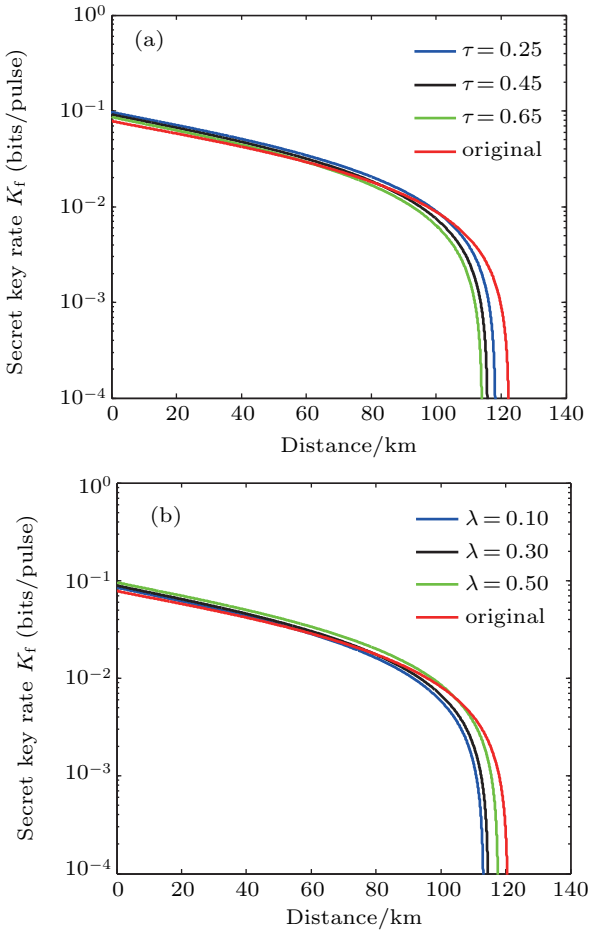


Fig. 5. (color online) Relationship between maximum transmission distance and secret key rate with the parameters' analysis of LOCM in the finite-size scenario, where the exchanged number signals $N = 10^{12}$. (a) Comparison of the performance between the eight-state protocol based on LOCM operation and the original eight-state protocol with parameters $\lambda = 0.3$ and $\tau = \{0.25, 0.45, 0.65\}$. (b) Comparison of the performance between the eight-state protocol based on LOCM operation and the original eight-state protocol with parameters $\tau = 0.45$ and $\lambda = \{0.1, 0.3, 0.5\}$.

Furthermore, we draw a comparison between the finite-size scenario and the asymptotic case (see Fig. 6). From Fig. 6, we notice that the maximum transmission distance in the asymptotic scenario is longer than the transmission distance in the finite-size scenario. Yet the values of the secret key rates are basically equal to 10^{-1}, which means that the different analysis approaches of finite-size region and asymptotic case produce little impact on the secret key rate. Moreover, with the growth of the exchanged number signals N, the performance in the finite-size regime will converge to the asymptotic case. This is because more signals parameter estimation can be used and therefore the parameter estimation is approaching perfection. Actually, it is impossible for the

number of exchanged signals to reach infinity in practice. The value of the block length of exchanged signals $N = 10^8$ is an enormous number for a practical CVQKD system. Nevertheless, the eight-state protocol with LOCM always has better improvement of the secret key rate K_f than the original eight-state protocol in the finite-size scenario.

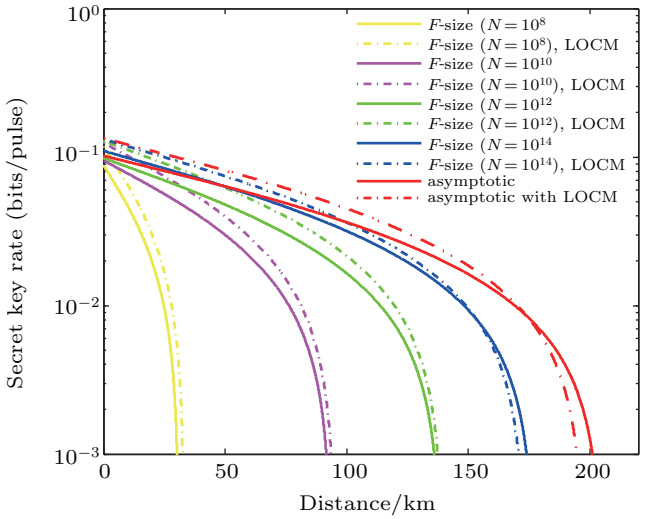


Fig. 6. (color online) Discretely-modulated eight-state protocol with LOCM in finite-size scenario in the case of heterodyne detection, where $V_A = 0.25$, $\eta = 0.6$, $\upsilon_{el} = 0.05$, and $\beta = 0.95$. Solid curves indicate the original eight-state protocol while the dashed curves represent the scenario with an LOCM (where the two parameters are set to $\lambda = 0.3$ and $\tau = 0.45$). From left to right, the first eight curves correspond to the finite-size scenario of block length $N = 10^8$, 10^{10}, 10^{12}, 10^{14} respectively, and the last two curves represent the asymptotic scenario.

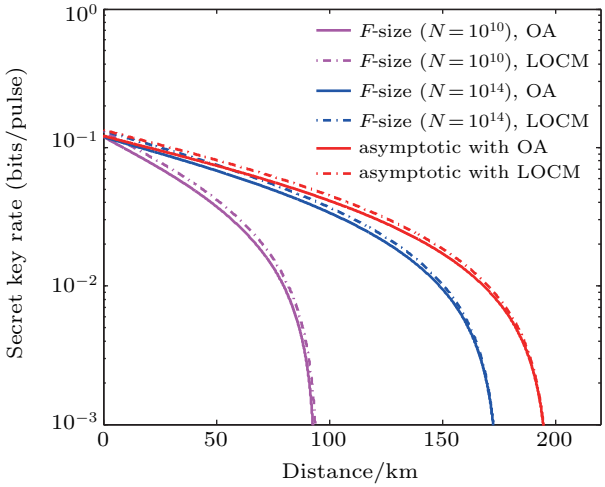


Fig. 7. (color online) Numerical analysis of secret key rates based on the comparison between the LOCM-CVQKD protocol and the OA protocol, where $V_A = 0.25$, $\eta = 0.6$, $\upsilon_{el} = 0.05$, $\beta = 0.95$, the two parameters of LOCM are $\lambda = 0.3$ and $\tau = 0.45$, and the parameter $g = 20$. Solid curves mean the OA eight-state protocol, and the dashed curves represent the scenario with an LOCM.

We are interested to compare our previous work on eight-state CVQKD using an optical amplifier (OA),[42] with our proposed scheme, which both belong to a phase-insensitive amplifier. The secret key rates are compared in Fig. 7, which shows that the two schemes both have the ability to enhance the secret key rate about 20%–30%. Our proposed LOCM-CVQKD protocol obtains a little better performance for the secrete key rate than the OA-based CVQKD, while the maximum transmission distance is nearly the same.

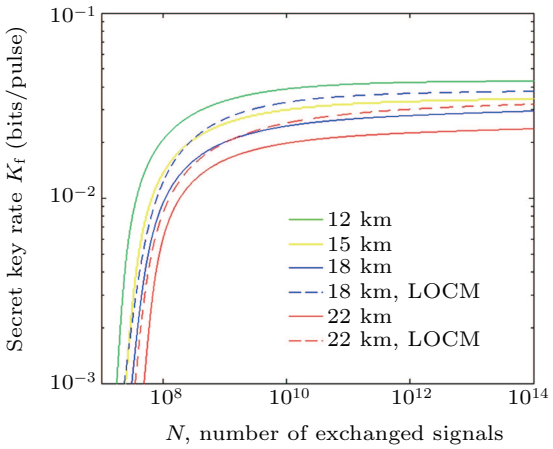


Fig. 8. (color online) Number of exchanged signals and secret key rate in the case of heterodyne detection, where $V_A = 0.25$, $\eta = 0.6$, $\upsilon_{el} = 0.05$, $\beta = 0.95$, and the two parameters of LOCM are $\lambda = 0.3$ and $\tau = 0.45$. Solid curves mean the original eight-state protocol, and the dashed curves represent the scenario with an LOCM.

As shown in Fig. 8, we can find that various transmission distances with different number of exchanged signals reflect regular curves relative to the secret key rates K_f. It shows that this novel scheme not only enhances the numerical value of the secret key rate K_f, but also numerously decreases the number of exchanged signals. Thus, the whole data size of the CVQKD derivation procedure can be cut down and the system load also decreases correspondingly. Therefore, the proposed scheme could also be a considerable approach to enhance the performance of the CVQKD system in practical applications.

5. Conclusion

In this paper, we propose a scheme to improve the performance of the eight-state CVQKD protocol by using a linear optics cloning machine. In the proposed scheme, we show the secret key rate of the modified CVQKD scheme with LOCM operation in the case of a finite-size scenario, as a function of total exchanged signals N, which can further approach the practical value of the secret key rate. The numerical simulation shows that by setting the two appropriate values of λ and τ, the LOCM is exploited to compensate for the imperfection of Bob's apparatus so that the secret key rate can be well enhanced and commendably harmonized with the maximum transmission distance. Furthermore, we need to notice that the performance of secret key rate K_f that is analysed in the finite-size scenario is more pessimistic than that obtained in the asymptotic case, whereas the finite-size region approach is closer to the practical situation of the CVQKD protocol.

References

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

[2] 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

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

[4] Samuel L B and Peter V L 2005 *Rev. Mod. Phys.* **77** 513

[5] Li Y M, Wang X Y, Bai Z L, Liu W Y, Yang S S and Peng K C 2017 *Chin. Phys. B* **26** 040303

[6] Li H W, Zhao Y B, Yin Z Q, Wang S, Han Z F, Bao W S and Guo G C 2009 *Opt. Commun.* **20** 4162

[7] Qi B, Huang L L, Qian L and Lo H K 2007 *Phys. Rev. A* **76** 052323

[8] Pirandola S, Braunstein S L and Lloyd S 2008 *Phys. Rev. Lett.* **101** 200504

[9] Wang X Y, Zhang Y C, Li Z Y, Xu B J, Yu S and Guo H 2017 *Quantum Inf. Comput.* **17** 1123

[10] Milicevic M, Feng C, Zhang L M and Gulak P G 2018 *Quantum Inf.* **4** 21

[11] Diamanti E and Leverrier A 2015 *Entropy* **17** 6072

[12] Liao Q, Guo Y, Huang D, Huang P and Zeng G H 2018 *New J. Phys.* **20** 023015

[13] Xuan Q D, Zhang Z S and Voss P L 2009 *Opt. Express* **17** 24244

[14] Wang X Y, Bai Z L, Wang S F, Li Y M and Peng K C 2013 *Chin. Phys. Lett.* **30** 010305

[15] Becir A, El-Orany F A A and Wahiddin M R B 2012 *Int. J. Quantum Inform.* **10** 1250004

[16] Qu Z and Djordjevic I B 2017 *IEEE Photon. J.* **9** 7600408

[17] Andersen U L, Josse V and Leuchs G 2005 *Phys. Rev. Lett.* **94** 240503

[18] Guo Y, Lv G L and Zeng G H 2015 *Quantum Inf. Process* **14** 4323

[19] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W and Grangier P 2007 *Phys. Rev. A* **76** 042305

[20] Jouguet P, Kunz-Jacques S, Diamanti E and Leverrier A 2012 *Phys. Rev. A* **86** 6429

[21] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 *Nat. Photonics* **9** 397

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

[23] Zhou C, Bao W S, Li H W, Wang Y, Li Y, Yin Z Q, Chen W and Han Z F 2013 *Phys. Rev. A* **89** 052328

[24] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501

[25] Leverrier A and Grangier P 2011 *Phys. Rev. A* **83** 042312

[26] Hu L Y, Liao Z Y and Zubairy M S 2017 *Phys. Rev. A* **95** 012310

[27] Yang J, Xu B, Peng X and Guo H 2012 *Phys. Rev. A* **85** 052302

[28] Guo Y, Liao Q, Wang Y J, Huang D, Huang P and Zeng G H 2017 *Phys. Rev. A* **95** 032304

[29] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504

[30] Lodewyck J and Grangier P 2007 *Phys. Rev. A* **76** 022332

[31] Thearle O, Assad S M and Symul T 2016 *Phys. Rev. A* **93** 042343

[32] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501

[33] Guo Y, Qiu D L, Huang P and Zeng G H 2015 *J. Phys. Soc. Jpn.* **84** 094003

[34] Huang P, He G Q, Fang J and Zeng G H 2013 *Phys. Rev. A* **87** 012317

[35] Wu X D, Liao Q, Huang D, Wu X H and Guo Y 2017 *Chin. Phys. B* **26** 110304

[36] Ma H X, Bao W S, Li H W and Chou C 2016 *Chin. Phys. B* **25** 080309

[37] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev. A* **87** 52309

[38] Wang P, Wang X, Li J and Li Y 2017 *Opt. Express* **25** 27995

[39] Zhang H, Fang J and He G Q 2012 *Phys. Rev. A* **86** 022338

[40] Usenko V C and Filip R 2016 *Entropy* 18

[41] Yang Y, Xu L P, Yan B, Zhang H Y and Shen Y H 2017 *Chin. Phys. B* **26** 110305

[42] Guo Y, Li R J, Liao Q, Zhou J and Huang D 2018 *Phys. Lett. A* **382** 372