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

Xiao-Dong Wu(吴晓东)[1], Qin Liao(廖骏)[1], Duan Huang(黄端)[1,2,†], Xiang-Hua Wu(吴湘华)[1], and Ying Guo(郭迎)[1,3,‡]

[1] *School of Information Science and Engineering, Central South University, Changsha* 410083, *China*
[2] *State Key Laboratory of Advanced Optical Communication Systems and Networks, Center of Quantum Information Sensing and Processing, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai* 200240, *China*
[3] *School of Engineering and Information Technology, University of New South Wales, Canberra, ACT* 2610, *Australia*

(Received 23 February 2017; revised manuscript received 9 August 2017; published online 29 September 2017)

We show that the secret key generation rate can be balanced with the maximum secure distance of four-state continuous-variable quantum key distribution (CV-QKD) by using the linear optics cloning machine (LOCM). Benefiting from the LOCM operation, the LOCM-tuned noise can be employed by the reference partner of reconciliation to achieve higher secret key generation rates over a long distance. Simulation results show that the LOCM operation can flexibly regulate the secret key generation rate and the maximum secure distance and improve the performance of four-state CV-QKD protocol by dynamically tuning parameters in an appropriate range.

Keywords: four states, linear optics cloning machine, quantum key distribution

PACS: 03.67.–a, 03.67.Bg, 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/26/11/110304

1. Introduction

Quantum key distribution (QKD) allows two remote parties, Alice and Bob, to distill a secret key over insecure quantum and classical channels.[1–4] There are two main versions of QKD, i.e., discrete-variable (DV) QKD[5–7] and continuous-variable (CV) QKD.[8–10] DV-QKD protocols encode information on properties of single photons, and use single-photon counters to measure the photon number. While CV-QKD protocols encode information on the quadrature variables of the optical field, and use a homodyne or heterodyne detector to measure the field quadratures.

A CV-QKD protocol based on Gaussian-modulated coherent states has been proved to be a practical scheme.[11,12] However, the level of signal-to-noise ratio (SNR) has an important effect on the reconciliation efficiency of this protocol, namely, we can obtain high reconciliation efficiency when the protocol operated at high SNR and achieve low reconciliation efficiency when the protocol operated at low SNR values.[13] Fortunately, discrete modulation CV-QKD protocol has no such limitation, and even at low SNR values, this kind of protocol can still have a high reconciliation efficiency. In this paper, we mainly study the four-state CV-QKD protocol, which has been proved to be secure against collective attacks[14–17] and has been experimentally demonstrated.[18]

In order to improve the performance and balance the secret key generation rate and the maximum secure distance of four-state CV-QKD protocol, we insert a linear optics cloning machine (LOCM)[19,20] inside Bob's apparatus. The LOCM, in fact, is the cloning machine which can be practically implemented using just linear optics, homodyne measurement and controlled displacements.[21] 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.[22] The LOCM operation provides a method to control the useful noise by tuning its parameters in appropriate ranges.[19] Therefore, a good performance of four-state CV-QKD protocol can be achieved by using the LOCM operation.

The paper is organized as follows. In Section 2, we give our theoretical analysis of the four-state protocol. In Section 3, a schematic configuration of the four-state CV-QKD protocol based on LOCM operation is described in detail. In Section 4, we derive the secret key generation rate of the four-state CV-QKD protocol based on LOCM operation under collective attacks. We compare the performance of the four-state CV-QKD protocol based on LOCM operation with the standard four-state CV-QKD protocol in Section 5. The conclusions are drawn in Section 6.

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61379153 and 61572529).
†Corresponding author. E-mail: duan.huang@foxmail.com
‡Corresponding author. E-mail: guoyingcsu@sina.com
© 2017 Chinese Physical Society and IOP Publishing Ltd

2. Description of the four-state CV-QKD protocol

We introduce the four-state protocol based on two versions. One is the prepare-and-measure (PM) version, and the other is the entanglement-based (EB) version. Subsequently, we give the region in which the eavesdropper's (Eve) mutual information with reference party (Bob) is similar in the four-state CV-QKD protocol and the Gaussian CV-QKD protocol.

2.1. PM and EB version of the four-state CV-QKD protocol

In the PM version of the four-state CV-QKD, Alice prepares four coherent states $\{|\alpha_k\rangle = |\alpha e^{i\pi((2k+1)/4)}\rangle,\ k = 0,1,2,3\}$ and then sends one of them randomly to Bob through the quantum channel. When Bob receives the transmitted coherent states, he performs either homodyne or heterodyne detection and uses his measurement results to decode the information.

In what follows, we formulate the EB version of the four-state CV-QKD protocol. Alice starts with a pure two-mode entangled state

$$|\Phi_{AB}(\alpha)\rangle = \frac{1}{2}\sum_{k=0}^{3}|\psi_k\rangle_A|\alpha e^{i\pi\frac{2k+1}{4}}\rangle_B, \tag{1}$$

where the state

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

is a non-Gaussian orthogonal state. Here, the state $|\phi_m\rangle$ is expressed as

$$|\phi_k\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\mu_k}}\sum_{n=0}^{\infty}(-1)^n\frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}}|4n+k\rangle, \tag{3}$$

with the parameters

$$\begin{aligned}\mu_{0,2} &= \frac{1}{2}e^{-\alpha^2}[\cosh(\alpha^2)\pm\cos(\alpha^2)],\\ \mu_{1,3} &= \frac{1}{2}e^{-\alpha^2}[\sinh(\alpha^2)\pm\sin(\alpha^2)].\end{aligned} \tag{4}$$

Alice performs a projective measurement $\{|\psi_k\rangle\langle\psi_k|\}(k = 0,1,2,3)$ on one of the trusted modes (mode A), then the other mode (mode B) can be projected onto one of the four coherent states $|\alpha_k\rangle$ $(k = 0,1,2,3)$ randomly and sent to Bob through a quantum channel. After receiving the transmitted states, Bob measures them by performing either homodyne or heterodyne detection. Once the communication has ended, the raw key is encoded by the signal value which has been modulated and measured. Therefore, Alice and Bob can share correlated strings of bits and achieve a final key by reverse reconciliation and privacy amplification.

Different from the PM version, the EB version does not correspond to the real implementation. However, it is remarkable that this version is fully equivalent to the PM version.[15,17] Moreover, the EB version provides a more powerful description for the establishment of security proofs against collective attacks.[23,24]

2.2. Covariance matrix of the four-state protocol

The initial covariance matrix $\gamma_{A_0B_0}$ of the state $|\Phi_{AB}(\alpha)\rangle$ is given by[13]

$$\gamma_{A_0B_0} = \begin{pmatrix} VI & Z_4\sigma_z \\ Z_4\sigma_z & VI \end{pmatrix}, \tag{5}$$

where I and σ_z are, respectively, the identity matrix and the usual Pauli matrix; V is the variance of the trusted modes (A and B) in the quadratures which can be written as $V = 2\alpha^2+1 = V_A+1$. The parameter

$$\begin{aligned}Z_4 &= 2\alpha^2(\mu_0^{3/2}\mu_1^{-1/2}+\mu_1^{3/2}\mu_2^{-1/2}\\ &\quad+\mu_2^{3/2}\mu_3^{-1/2}+\mu_3^{3/2}\mu_0^{-1/2}),\end{aligned} \tag{6}$$

refers to the correlation between the trusted modes. After mode B passes through a quantum channel, the state $|\Phi_{AB}(\alpha)\rangle$

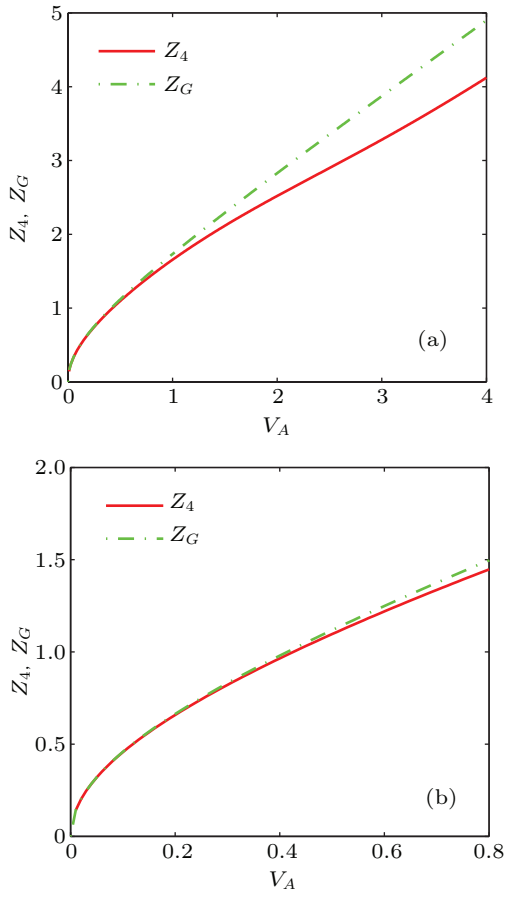


Fig. 1. (color online) Comparison of the correlation for two different modulation protocols. Full lines correspond to the four-state protocol (correlation marked as Z_4) and dashed lines correspond to the Gaussian modulation protocol (correlation marked as Z_G). Both Z_4 and Z_G are functions of the modulation variance $V_A = 2\alpha^2$. (a) V_A in a large range, and (b) V_A in a small range.

is transformed into ρ_{AB_1} with covariance matrix

$$\gamma_{AB_1} = \begin{pmatrix} VI & \sqrt{T}Z_4\sigma_z \\ \sqrt{T}Z_4\sigma_z & T(V+\chi_{\text{line}})I \end{pmatrix}, \tag{7}$$

where $\chi_{\text{line}} = (1-T)/T + \varepsilon$ is the channel-added noise referred to the channel input, T is the channel transmittance and ε is the excess noise. Note that in the Gaussian modulation protocol, this covariance matrix can be reconstructed by replacing Z_4 with Z_G, where $Z_G = \sqrt{V_A^2 + 2V_A}$. Fortunately, Z_4 is very close to Z_G when V_A is small enough, as shown in Fig. 1. In other words, for $V_A \in (0, 0.5)$, Z_4 and Z_G are almost equal, meaning that in this region, Eve's mutual information with Bob is very similar in four-state protocol and Gaussian modulation protocol.[24]

3. The four-state CV-QKD protocol based on LOCM operation

In this section, a four-state CV-QKD protocol based on LOCM operation is proposed, as shown in Fig. 2. It is worth noting that we use the LOCM to make the approximate copies instead of perfect copies of quantum states. As we all know, the non cloning theorem forbids making perfect cloning, consequently, the LOCM used here does not violate the non cloning theorem.[22] In this protocol, Alice applies the heterodyne detection, and obtains two measurements $\hat{x}_A$ and $\hat{p}_A$. After receiving the coherent states centered at (x_{B_1}, p_{B_1}), Bob prepares for two vacuum states $\hat{x}_1^{(0)}$ and $\hat{x}_2^{(0)}$, then the LOCM operation is implemented, and the quadratures are measured by Bob via performing either homodyne or heterodyne detection. In the LOCM operation, due to the symmetry of all transformations on pairs of quadratures $(\hat{x}, \hat{p})$, without loss of generality, only one quadrature $\hat{x}_{B_1}$ is considered here. On one hand, at Bob's side, a beam splitter (BS) with transmissions τ reflects a fraction of the input mode $\hat{x}_{B_1}$, as displayed on Fig. 2(a), then we obtain

$$\hat{x}_1 = \sqrt{\tau}\hat{x}_{B_1} + \sqrt{1-\tau}\hat{x}_1^{(0)}, \tag{8}$$

and subsequently

$$\begin{aligned} \hat{x}_{\text{m}} &= \frac{1}{\sqrt{2}}(\hat{x}_1 + \hat{x}_2^{(0)}) \\ &= \sqrt{\frac{\tau}{2}}\hat{x}_{B_1} + \sqrt{\frac{1-\tau}{2}}\hat{x}_1^{(0)} + \frac{1}{\sqrt{2}}\hat{x}_2^{(0)}. \end{aligned} \tag{9}$$

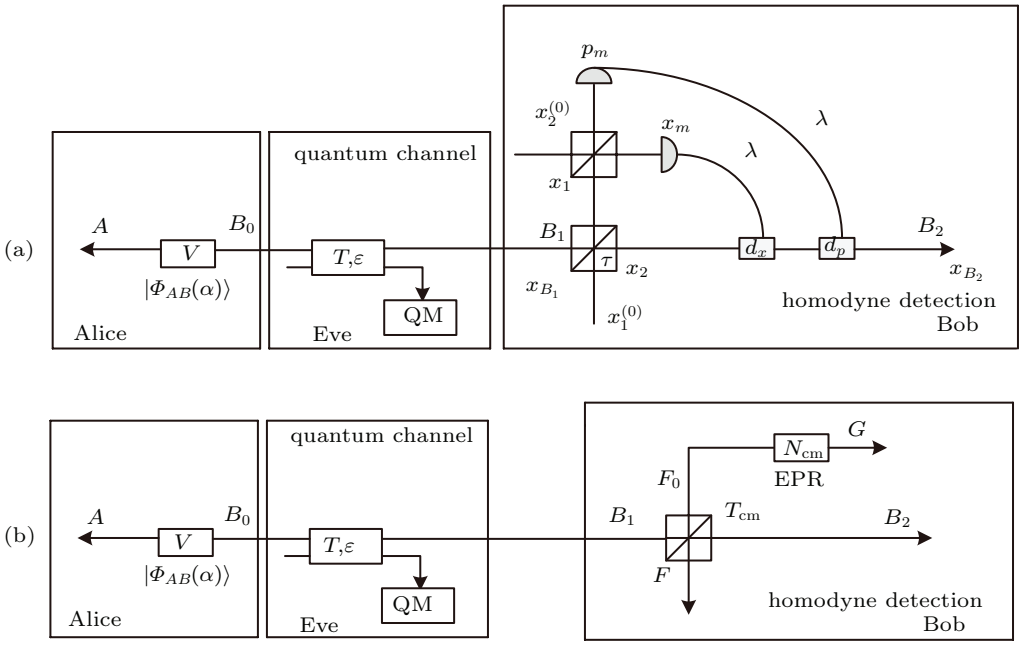


Fig. 2. The EB scheme for the four-state CV-QKD protocol based on LOCM operation. (a) The four-state CV-QKD with LOCM in terms of two parameters λ and τ. (b) The equivalent four-state CV-QKD protocol with a thermal state of variance N_{cm} characterized by the tunable noise χ_{cm} and transmittance T_{cm}.

On the other hand, the transmitted mode $\hat{x}_2$ can be written as

$$\hat{x}_2 = \sqrt{1-\tau}\hat{x}_{B_1} - \sqrt{\tau}\hat{x}_1^{(0)}, \tag{10}$$

then based on the measurement result $\hat{x}_{\text{m}}$ with the tuning gain λ, the transmitted mode can be displaced as

$$\begin{aligned} \hat{x}_{B_2} &= \hat{x}_2 + \lambda\hat{x}_{\text{m}} \\ &= \left(\sqrt{1-\tau} + \lambda\sqrt{\frac{\tau}{2}}\right)\hat{x}_{B_1} \\ &\quad + \frac{\lambda}{\sqrt{2}}\hat{x}_2^{(0)} + \left(\lambda\sqrt{\frac{1-\tau}{2}} - \sqrt{\tau}\right)\hat{x}_1^{(0)}. \end{aligned} \tag{11}$$

Based on the right side of Eq. (11), the variance $V_{B_2} := \langle \hat{x}_{B_2}^2 \rangle$ of the mode $\hat{x}_{B_2}$ can be calculated as

$$V_{B_2} = \left(\sqrt{1-\tau}+\lambda\sqrt{\frac{\tau}{2}}\right)^2 V_{B_1} + \frac{\lambda^2}{2} + \left(\lambda\sqrt{\frac{1-\tau}{2}}-\sqrt{\tau}\right)^2. \quad (12)$$

According to Eq. (12), the expression of transmittance $T_{\rm cm}$ is given by

$$T_{\rm cm} = \left(\sqrt{1-\tau}+\lambda\sqrt{\frac{\tau}{2}}\right)^2. \quad (13)$$

With the constraint $T_{\rm cm} \leqslant 1$ in mind, it is necessary for us to solve the parameter λ in a range $[0, \sqrt{2}(1-\sqrt{1-\tau})/\sqrt{\tau}]$ for the given parameter $\tau \in (0,1)$. Thus, we can derive the LOCM-tuned noise $\chi_{\rm cm}$ with two parameters λ and τ referred to Bob's input, the expression can be written as

$$\chi_{\rm cm} = \frac{\frac{\lambda^2}{2} + \left(\lambda\sqrt{\frac{1-\tau}{2}}-\sqrt{\tau}\right)^2}{\left(\sqrt{1-\tau}+\lambda\sqrt{\frac{\tau}{2}}\right)^2}. \quad (14)$$

The equivalent system can be established by combining a thermal state of variance $N_{\rm cm} = T_{\rm cm}\chi_{\rm cm}/(1-T_{\rm cm})$ on a beamsplitter of transmittance $T_{\rm cm}$, as shown in Fig. 2(b).

It is clear that $T_{\rm cm}$ is a function of two parameters λ, τ, as shown in Fig. 3. We can regulate the $T_{\rm cm}$ in a range [0,1] by properly tuning these two parameters.

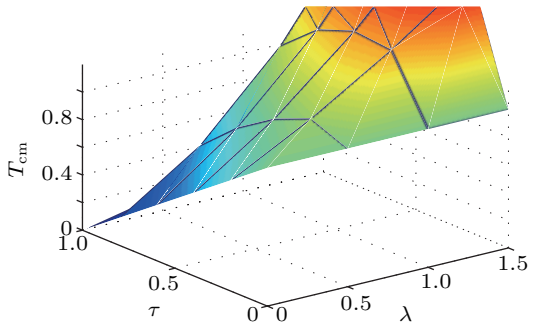


Fig. 3. (color online) Relation between the LOCM-tuned transmittance $T_{\rm cm}$ and two parameters λ and τ. It is clear that the transmittance $T_{\rm cm}$ can be regulated in [0,1] by choosing some appropriate parameters λ and τ.

Note that when we consider an additional constraint on parameters λ and τ of LOCM operation,[25] equation (11) can be rewritten as

$$\hat{x}'_{B_2} = \frac{1}{\sqrt{1-\tau}}\hat{x}_{B_1} + \sqrt{\frac{\tau}{1-\tau}}\hat{x}_2^{(0)}. \quad (15)$$

If we set $\sqrt{g} = 1/\sqrt{1-\tau}$, obtaining $\hat{x}'_{B_2} = \sqrt{g}\hat{x}_{B_1} + \sqrt{g-1}\hat{x}_2^{(0)}$, which is an exact operation of a linear optics amplifier (LOA) on the input mode of Bob. According to Ref. [13], the LOA is a phase-insensitive amplifier with gain $g = 1/\sqrt{1-\tau}$. The variance of the quadrature $\hat{x}'_{B_2}$ can be calculated as

$$V_{B'_2} = \frac{1}{1-\tau}V_{B_1} + \frac{\tau}{1-\tau}. \quad (16)$$

Using a method similar to the one mentioned above, we can derive a quantum channel which features a transmittance $T_a = 1/(1-\tau)$ in the LOA quantum system. As a result, the LOA-tuned noise can be calculated as $\chi_a = \tau$ and this noise can be regulated in a simple range $(0,1)$ since $\tau \in (0,1)$. Comparing the tunable noise $\chi_{\rm cm}$ with χ_a, it is obvious that we can tune two parameters λ and τ of $\chi_{\rm cm}$ but only one parameter τ of χ_a. Thus, the LOCM-tuned noise $\chi_{\rm cm}$ characterized by two parameters λ and τ can be made much larger than the LOA-tuned noise χ_a, which is dependent on only one parameter τ in a large range.

To describe the relation between the tuned noise $\chi_{\rm cm}$ based on LOCM operation and the tuned noise χ_a based on LOA operation, we particularly define the differential noise $\chi_{\rm l} = \chi_{\rm cm} - \chi_a$, as shown in Fig. 4. This parameter contains the information of both LOCM-tuned and LOA-tuned noise. If we set $\chi_{\rm l} = 0$, meaning that the tuned noise based on LOCM operation is exactly equivalent to the tuned noise based on LOA operation. In other words, the LOCM can be transformed into LOA for $\chi_{\rm l} = 0$.

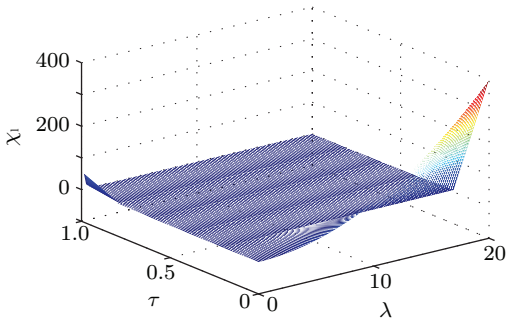


Fig. 4. (color online) Relation between the differential noise $\chi_{\rm l}$ and two parameters λ, τ. We can obtain $\chi_{\rm l} = 0$ easily and then derive $\chi_{\rm cm} = \chi_a$ by selecting appropriate parameters λ and τ.

Note that the homodyne or heterodyne detection at Bob's side may be followed by a noise with variance $\chi_{\rm cm}$ (implementation of LOCM operation) or χ_a (implementation of LOA operation) in the four-state CV-QKD protocol. Under certain conditions ($\chi_{\rm l} = 0$), these two operations are virtually equivalent which has been demonstrated above. Once this implementation procedure is ended, data postprocessing is conducted by Alice and Bob, and then the final secret key is generated. Here we should remark that in direct reconciliation, the data owned by Alice is seen as a reference to complete the key establishment and in reverse reconciliation, the data owned by Bob is the reference.[26] Reverse reconciliation has been demonstrated that it can offer a great advantage in performance improvement of the CV-QKD,[11,13] thus we perform our calculations with this reconciliation.

4. Secret key generation rate of the four-state CV-QKD based on LOCM operation

Based on the above-mentioned analysis, we will limit our calculations to reverse reconciliation. The secret key genera-

tion rate for reverse reconciliation under collective attacks can be given by

$$K = \beta I(A:B) - S_4(B:E), \tag{17}$$

where $I(A:B)$ and β are, respectively, the mutual information of Alice and Bob and reconciliation efficiency; $S_4(B:E)$ is Eve's mutual information with Bob.

In order to predigest the security analysis of the four-state CV-QKD protocol based on LOCM operation, we suppose that Alice applies heterodyne detection with measurements $\{x_A, p_A\}$. Considering the fact that the degraded LOCM operation is essentially a phase-insensitive amplifier, therefore, Bob here performs heterodyne detection via using a detector, which features an efficiency η and an electronics noise $v_{\rm el}$.[13] For simplicity, we assume the heterodyne detector used by Bob is perfect in our protocol, which means $\eta = 1$ and $\upsilon_{\rm el} = 0$.[13,25] It is remarkable that the four-state CV-QKD protocol with LOCM is equivalent to a system by combining a thermal state of variance $N_{\rm cm}$, which are shown in Figs. 2(a) and 2(b). Therefore, the additional noise referred to the input of the detector can be derived as $\chi_{\rm LOCM} = (1 - T_{\rm cm})N_{\rm cm}/T_{\rm cm}$ based on Fig. 2(b).[25]

For the protocol based on LOCM operation, the mutual information of Alice and Bob $I(A:B)$ can be calculated from the measurement variance of Bob $V_{B_2} = \tau_0 T T_{\rm cm}(V + \chi_{\rm tot})$ and conditional variance $V_{B_2|A} = \tau_0 T T_{\rm cm}(1 + \chi_{\rm tot})$ which is given by[12]

$$I(A:B) = \frac{1}{2}\log_2 \frac{V_{B_2}}{V_{B_2|A}} = \frac{1}{2}\log_2 \frac{V + \chi_{\rm tot}}{1 + \chi_{\rm tot}}, \tag{18}$$

where $\chi_{\rm tot} = \chi_{\rm line} + \chi_{\rm LOCM}/T$ represent the total noise referred to the channel input.

We have mentioned in the previous that when $V_A \in (0, 0.5)$, Eve's mutual information with Bob is similar in four-state protocol and Gaussian modulation protocol. Therefore, one has $S_4(B:E) \approx S_G(B:E)$. Based on this result, the expression of $S_4(B:E)$ can be given by

$$S_4(B:E) = S(\rho_E) - S(\rho_{E|B_2}), \tag{19}$$

where $S(\rho)$ is the von Neumann entropy of the state ρ. Considering the fact that Eve can purify the system EAB_1 and Bob's measurement can purify the system $AEFG$ [the mode notations are shown in Fig. 2(b)], we thus get $S(\rho_E) = S(\rho_{AB_1})$ and $S(\rho_{E|B_2}) = S(\rho_{AFG}^{x_{B_2}})$. Then $S_4(B:E)$ can be rewritten as

$$S_4(B:E) = S(\rho_{AB_1}) - S(\rho_{AFG}^{x_{B_2}}). \tag{20}$$

For the first term $S(\rho_{AB_1})$, we can use the symplectic eigenvalues $\upsilon_{1,2}$ of covariance matrix γ_{AB_2} to calculate it. The symplectic eigenvalues $\upsilon_{1,2}$ can be expressed as[13]

$$\upsilon_{1,2}^2 = \frac{A \pm \sqrt{A^2 - 4B^2}}{2}, \tag{21}$$

with

$$\begin{aligned} A &= V^2 + T^2(V + \chi_{\rm line})^2 - 2TZ_4^2, \\ B &= TV^2 + TV\chi_{\rm line} - TZ_4^2. \end{aligned} \tag{22}$$

In order to calculate $S(\rho_{AFG}^{x_{B_2}})$, we need to derive the symplectic eigenvalues $\upsilon_{3,4,5}$ of the covariance matrix $\gamma_{AFG}^{x_{B_2}}$ characterizing the state $\rho_{AFG}^{x_{B_2}}$. The matrix $\gamma_{AFG}^{x_{B_2}}$ can be written as

$$\gamma_{AFG}^{x_{B_2}} = \gamma_{AFG} - \sigma_{AFGB_2}^{\rm T}(X\gamma_{B_2}X)^{MP}\sigma_{AFGB_2}, \tag{23}$$

where $X = {\rm diag}(1, 0)$ and MP is the Moore–Penrose inverse of a matrix. The decomposed covariance matrix γ_{AFGB_2} is given by

$$\gamma_{AFGB_2} = \begin{pmatrix} \gamma_{AFG} & \sigma_{AFGB_2}^{\rm T} \\ \sigma_{AFGB_2} & \gamma_{B_2} \end{pmatrix}. \tag{24}$$

It is clear that we can achieve the sub-matrices γ_{AFG}, σ_{AFGB_2}, and γ_{B_2} from this matrix. Besides, matrix γ_{AFGB_2} can be obtained from the rearrangements of lines and columns of the matrix characterizing the system AB_2FG:

$$\gamma_{AB_2FG} = \Omega^{\rm T}(\gamma_{AB_1} \oplus \gamma_{F_0G})\Omega, \tag{25}$$

where $\Omega = I_A \bigoplus \Omega_{BF_0}^{BS} \bigoplus I_G$ represents the beamsplitter transformation performed on modes B and F_0 with

$$\Omega_{BF_0}^{BS} = \begin{pmatrix} \sqrt{T_{\rm cm}}I & \sqrt{1 - T_{\rm cm}}\sigma_z \\ -\sqrt{1 - T_{\rm cm}}\sigma_z & \sqrt{T_{\rm cm}}I \end{pmatrix}, \tag{26}$$

and the matrix γ_{F_0G} illustrates an effect of the additional LOCM-tuned noise which can be written as

$$\gamma_{F_0G} = \begin{pmatrix} N_{\rm cm}I & \sqrt{N_{\rm cm}^2 - 1}\sigma_z \\ \sqrt{N_{\rm cm}^2 - 1}\sigma_z & N_{\rm cm}I \end{pmatrix}. \tag{27}$$

After that, we can calculate the eigenvalues $\upsilon_{3,4,5}$, which are given by[24]

$$\upsilon_{3,4}^2 = \frac{C \pm \sqrt{C^2 - 4D}}{2}, \quad \upsilon_5 = 1, \tag{28}$$

where for the heterodyne detection case,

$$\begin{aligned} C &= \frac{A\chi_{\rm LOCM}^2 + B + 1 + 2\chi_{\rm LOCM}[V\sqrt{B} + T(V + \chi_{\rm line})] + 2TZ_4^2}{[T(V + \chi_{\rm tot})]^2}, \\ D &= \left(\frac{V + \sqrt{B}\chi_{\rm LOCM}}{T(V + \chi_{\rm tot})}\right)^2. \end{aligned} \tag{29}$$

Based on these consequences, the expression for $S_4(B:E)$ can be written as

$$S_4(B:E)=\sum_{i=1}^{2}G\left(\frac{\upsilon_i-1}{2}\right)-\sum_{i=3}^{5}G\left(\frac{\upsilon_i-1}{2}\right), \tag{30}$$

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

5. Performance analysis and discussion

Considering the fact that the four-state protocol based on LOCM operation depends much on parameters λ and τ, thus we can tune λ and τ of the LOCM operation in appropriate ranges to improve the performance of the four-state protocol. We have mentioned in the above that the LOCM-tuned noise $\chi_{\rm cm}$ characterized by two parameters λ and τ can be made much larger than the LOA-tuned noise χ_a, which is dependent on only one parameter τ in a large range. Therefore, in this section, we mainly study the effect of the LOCM operation on the performance of four-state CV-QKD protocol for reverse reconciliation with the heterodyne detection, as the LOA operation can be analyzed in a similar way.

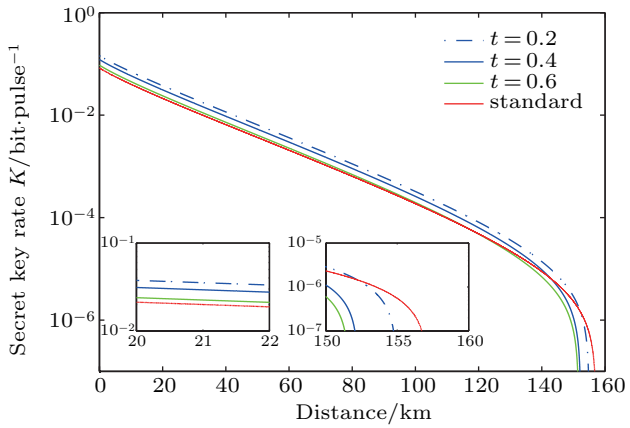


Fig. 5. (color online) Comparison of the performance between the four-state protocol based on LOCM operation and the standard four-state protocol with parameters $\lambda=0.3$ and $\tau=\{0.2,0.4,0.6\}$.

In order to simplify the analysis, as mentioned above, we assume that Bob uses a perfect heterodyne detector in our protocol as well as in the standard four-state protocol, namely, the parameters $\eta=1$ and $\upsilon_{\rm el}=0$. Other parameters such as reconciliation efficiency β and excess noise ε are fixed in all simulations to the values $\varepsilon=0.005$ and $\beta=0.8$,[24] respectively. The channel transmittance is $T=10^{-\varsigma L/10}$, where $\varsigma=0.2$ dB/km is the loss coefficient of optical fibers and L is the channel length. Based on the previous analysis, correlations Z_4 and Z_G are almost equal when $V_A\in(0,0.5)$, thus we can take $V_A=0.25$ and $V=V_A+1=1.25$ in our simulations.

In what follows, we compare the performance of the four-state CV-QKD protocol based on LOCM operation with the standard four-state CV-QKD protocol, as shown in Fig. 5 with gain $\lambda=0.3$. We take $\tau=\{0.2,0.4,0.6\}$ as examples, the corresponding $T_{\rm cm}$ calculated from Eq. (13) are $\{0.9787,0.8258,0.6348\}$, respectively, which are all physical results. In Fig. 5, for the gain value $\lambda=0.3$, the secret key generation rates of our protocol are higher than the standard four-state protocol over long distance, and what is more, we can tune the parameter τ to improve the performance of our protocol. It is clear in Fig. 5 that we can achieve the higher secret key rate and longer maximum secure distance by tuning the value of parameter τ to be smaller in an appropriate range.

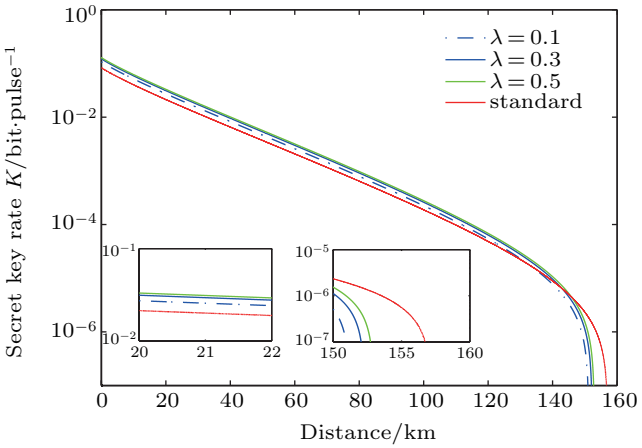


Fig. 6. (color online) Comparison of the performance between the four-state protocol based on LOCM operation and the standard four-state protocol with parameters $\tau=0.4$ and $\lambda=\{0.1,0.3,0.5\}$.

For simplicity, we take the fixed efficiency $\tau=0.4$ for example to illustrate the effect of the tuned gain $\lambda\in[0,\sqrt{2}(1-\sqrt{1-\tau})/\sqrt{\tau}]$ on the four-state protocol based on the LOCM operation in Fig. 6. Here, we choose $\lambda=\{0.1,0.3,0.5\}$, thus the corresponding $T_{\rm cm}$ calculated from Eq. (13) are $\{0.6713,0.8258,0.9964\}$ respectively, which are all physical results. As shown in Fig. 6, the secret key generation rates of our protocol are higher than the standard four-state protocol over a long distance. Besides, we can tune the parameter λ in this case to improve the performance of our protocol. It is clear in Fig. 6 that we can achieve the higher secret key generation rate and longer maximum secure distance by tuning the value of parameter λ to be larger in a suitable range.

It is necessary to point out that the maximum secure distance of our protocol is slightly shorter than the standard four-state protocol. Fortunately, we can reduce the distance gap between our protocol and the standard four-state protocol by controlling the parameters λ and τ of LOCM operation. For example, in Fig. 5, when we choose $\lambda=0.3$ and $\tau=0.2$ ($T_{\rm cm}=0.9787<1$), the distance gap between our protocol and the standard four-state protocol is about 2 km and in Fig. 6, when we choose $\tau=0.4$ and $\lambda=0.5$ ($T_{\rm cm}=0.9964<1$), the

distance gap between our protocol and the standard four-state protocol is about 4 km. In other words, based on LOCM operation, the secret key generation rate of our protocol improves in a large range of distance with the price of decreasing little of the maximum transmission distance compared with the standard four-state protocol.

6. Conclusion

We have proposed an improved four-state CV-QKD protocol by inserting the tunable LOCM with reverse reconciliation. The LOCM is actually a cloning machine which can be implemented by using linear optics, homodyne measurement and controlled displacement. We have pointed out 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. The secret key generation rate can be commendably harmonized with the maximum secure distance as the parameters λ and τ can be stabilized to an appropriate value. We focus on reverse reconciliation in performance analysis mainly because this reconciliation has been proved to provide a great advantage in CV-QKD protocol. Simulation results show that by tuning the parameters of LOCM operation in a suitable range, we can improve the secret key generation rate of the four-state protocol over long distance and decrease the distance gap between our protocol and the standard four-state protocol.

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[2] Lo H K, Curty M and Tamaki K 2014 *Nat. Photonics* **8** 595
[3] Huang D, Huang P, Lin D K and Zeng G H 2016 *Sci. Rep.* **6** 19201
[4] Huang D, Huang P, Wang T, Li H S, Zhou Y M and Zeng G H 2016 *Phys. Rev. A* **94** 032305
[5] Chen M and Liu X 2011 *Chin. Phys. B* **20** 100305
[6] Erven C, Conteau C, Laamme R and Weihs G 2008 *Opt. Exp.* **16** 1684053
[7] Liang J W, Cheng Z, Shi J J and Guo Y 2016 *Acta Phys. Sin.* **65** 160301 (in Chinese)
[8] 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
[9] Weedbrook C 2013 *Phys. Rev. A* **87** 022308
[10] Ma H X, Bao W S, Li H W and Zhou C 2016 *Chin. Phys. B* **25** 080309
[11] Grosshans F, van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
[12] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
[13] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R and Grangier P 2009 *J. Phys. B-At. Mol. Opt.* **42** 114014
[14] Shen Y and Zou H X 2010 *Acta Phys. Sin.* **59** 1473 (in Chinese)
[15] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[16] Leverrier A and Grangier P 2011 *Phys. Rev. A* **83** 042312
[17] Yang S and Yao Z 2017 *Design. Code. Cryptogr.* **82** 663
[18] Wang X Y, Bai Z L, Wang S F, Li Y M and Peng K C 2013 *Chin. Phys. Lett.* **30** 010305
[19] Guo Y, Lv G and Zeng G H 2015 *Quatum. Inf. Process.* **14** 4323
[20] Guo Y, Qiu D L, Huang P and Zeng G H 2015 *J. Phys. Soc. Jpn.* **84** 094003
[21] Andersen U L, Josse V and Leuchs G 2005 *Phys. Rev. Lett.* **94** 240503
[22] Olivares S, Paris M G A and Andersen U L 2006 *Acta Phys. Hung. Ser. B* **26** 293
[23] Blandino R, Leverrier A, Barbieri M, Etesse J, Grangier P and Tualle-Brouri R 2012 *Phys. Rev. A* **86** 012327
[24] Zhang H, Fang J and He G Q 2012 *Phys. Rev. A* **86** 022338
[25] García-Patrón R 2007 *Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution* (Ph.D. Thesis) (Université Libre de Bruxelles)
[26] Usenko V C and Filip R 2016 *Entropy* **18** 20