Improving continuous-variable quantum key distribution under local oscillator intensity attack using entanglement in the middle*

Fang-Li Yang(杨芳丽)[1], Ying Guo(郭迎)[2,†], Jin-Jing Shi(石金晶)[2], Huan-Li Wang(王焕礼)[3], and Jin-Jin Pan(潘矜矜)[1]

[1] College of Electronic Information and Automation, Guilin University of Aerospace Technology, Guilin 541000, China
[2] School of Information Science and Engineering, Central South University, Changsha 410083, China
[3] Guilin Public Works Section of High Speed Railway, Nanning Railway Bureau, Guilin 541000, China

(Received 27 March 2017; revised manuscript received 14 June 2017; published online 10 September 2017)

A modified continuous-variable quantum key distribution (CVQKD) protocol is proposed by originating the entangled source from a malicious third party Eve in the middle instead of generating it from the trustworthy Alice or Bob. This method is able to enhance the efficiency of the CVQKD scheme attacked by local oscillator (LO) intensity attack in terms of the generated secret key rate in quantum communication. The other indication of the improvement is that the maximum transmission distance and the maximum loss tolerance can be increased significantly, especially for CVQKD schemes based on homodyne detection.

Keywords: continuous-variable, quantum key distribution, local oscillator intensity attack, entanglement in the middle

PACS: 03.67.Dd, 03.65.Ud, 03.67.Hk **DOI:** 10.1088/1674-1056/26/10/100303

1. Introduction

Quantum key distribution (QKD) firstly transmits quantum signals in the insecure quantum channel and then shares the secret keys through a classical authenticated channel.[1,2] Since the first demonstration of continuous-variable quantum field was presented in 1998,[3] the continuous-variable quantum key distribution (CVQKD)[4–12] has achieved a great development. Compared with the original discrete-variable protocols, the CVQKD schemes exhibit several advantages, including easier generation of the used Gaussian states[13] and a far quicker repetition rate. As is well known, the traditional Gaussian CVQKD protocols can be classified by three parts, that is the sender's state,[14,15] the receiver's detection,[16] and the reconciliation algorithm.[17,18] Over the years, the CVQKD has become a well-established technology in theory and experiment. Its security has been improved greatly in comparison with the optimal collective attacks.[19–21] Moreover, the CVQKD protocols based on the entanglement properties of two-mode squeezed states[22,23] can distribute the deterministic key.[22] Nowadays, a measurement-device-independent quantum key distribution (MDI-QKD)[24–27] has been demonstrated to be technically practical, which can guarantee the information security, and has received considerable attention.

However, in an ideal CVQKD protocol,[28–31] only the signal is considered and the local oscillator (LO) is ignored. Practically, the LO signal and the Alice's signal, which have the same initial polarization and phase with each other, are derived from Alice in a quantum channel simultaneously[12,32] to control the LO phase drift[33] as small as possible. In this case, not only could the Alice's signal be intercepted but also the LO signal could be eavesdropped and manipulated by Eve. Eve can attack the channel via reducing the LO intensity without being discovering, and this is referred to as LO intensity attack (LOIA) which leads to some security concerns[34,35] in the CVQKD protocol. Consequently, monitoring the LO intensity is a necessary operation to guarantee security. However, the true secret key rate or equivalently monitored key rate was demonstrated to be compromised severely which was described in Ref. [34]. Therefore, what we need to do urgently is to find an approach to enhance the effected performance of the CVQKD protocol under LOIA, we call it as the LOIA–CVQKD protocol.

During the past decade, in regard to both security proofs[36–38] and practical demonstrations,[39,40] the entangled source generated from Eve in the middle has become a focus of discrete-variable QKD. Analogously, in the CVQKD field, Christian proposed protocols[30] where the entanglements were derived from the distrusted Eve, rather than from the legitimate Alice or Bob. The result in Ref. [30] showed that this method can effectively compensate the effect of loss and hence improve secret key rates between Alice and Bob. Based on this background, we conquer the above-mentioned problems in LOIA–CVQKD by changing the structure of the trusted participator originating entanglement to that of Eve

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61379153, 61401519, and 61572529), the Natural Science Foundation of Hunan Province, China (Grant No. 2017JJ3415), the Science and Technology Project of Guangxi Zhuang Autonomous Region, China (Grant Nos. AC16380094 and 1598008-29), and the Natural Science Fund of Guangxi Zhuang Autonomous Region, China (Grant No. 2015GXNSFAA139298).

†Corresponding author. E-mail: yingguo@csu.edu.cn

© 2017 Chinese Physical Society and IOP Publishing Ltd

preparing the source in the middle. We define the modified LOIA–CVQKD as the middle-based LOIA–CVQKD and analyze protocols on the secret key rates, working distances, and channel losses.

The rest of this paper is organized as follows. We will review the original LOIA–CVQKD protocol in Section 2. In order to improve the performance of the LOIA–CVQKD protocol, in Section 3, we describe the proposed CVQKD scheme in detail. In Section 4, we discuss the efficiency of the middle-based LOIA–CVQKD protocols and perform some simulations. Section 5 gives a brief conclusion.

2. The original LOIA–CVQKD protocol

We introduce a practical coherent state LOIA–CVQKD protocol with homodyne measurement as shown in Fig. 1. For simplicity, we do not consider other three protocols in this section. In the EB system, Alice first generates an EPR state and the LO signal is divided at a beam splitter (BS) as a classical LO and a low intensity signal. In Alice side, heterodyne detection on mode A_0 (one half mode of the EPR modes) is implemented by mixing A_0 with the auxiliary vacuum C_0 into the BS_1 and homodyning the outputs A and C to obtain P_A and X_A respectively. Then Alice projects the other half of the EPR mode B_0 on a quantum state. In a practical protocol, the quantum signal and the local oscillator travel through the same insecure channel monitored by Eve. As for the P_A and X_A, although the satisfactory Gaussian distributions are different from each other, they have the same variance $V = V_A + 1$ and V_A is the modulation variance of the source. A realistic homodyne detection with efficiency $\eta_{\rm BHD}$ can be described by placing a beamsplitter of transmittance $\eta_{\rm BHD}$ before an ideal homodyne detector with input $\hat{X}_{\rm h} = \sqrt{\eta_{\rm BHD}}\hat{X}_B + \sqrt{1-\eta_{\rm BHD}}\hat{X}_{\rm th}$. We assume this measurement is perfect, so the efficiency $\eta_{\rm BHD} = 1$ and then $\hat{X}_{\rm h} = \hat{X}_B$. Before Bob performing homodyne detection, he achieves the mode $\hat{X}_B \in \{\hat{Q}_B, \hat{P}_B\}$ given by

$$\hat{X}_B = \sqrt{\partial}\hat{X}_{B_0} + \sqrt{1-\partial}\hat{X}_{\rm E}, \tag{1}$$

where the channel transmission is ∂ and $\hat{X}_{\rm E}$ denotes Eve's mode introduced with the quadrature variance M. If the original intensity of LO is not monitored and the fluctuation is not quantified, Bob will perform the measurement

$$X_{\rm B}^n = \sqrt{\kappa}X_{\rm B}, \tag{2}$$

with the proportional LO intensity coefficient κ limited in the range of $0 < \kappa < 1$, where $X_{\rm B}$ is $Q_{\mathbf{B}} \in \mathbb{R}$ (or identically $P_{\mathbf{B}} \in \mathbb{R}$). In the following, we assume that the parameter κ of each pulse is equivalent for simplicity. In practical implementation, the fluctuation of the LO intensity opens a loophole which can be catched by Eve. She attacks not only the signal with conventional Gaussian collective attack, but also the LO with a peculiar intensity attenuation. There appears a serious problem, that is, the so-called LOIA can be partially hidden, since Eve uses the non-changing phase attenuator $\boldsymbol{A}$ to reduce the intensity of LO.

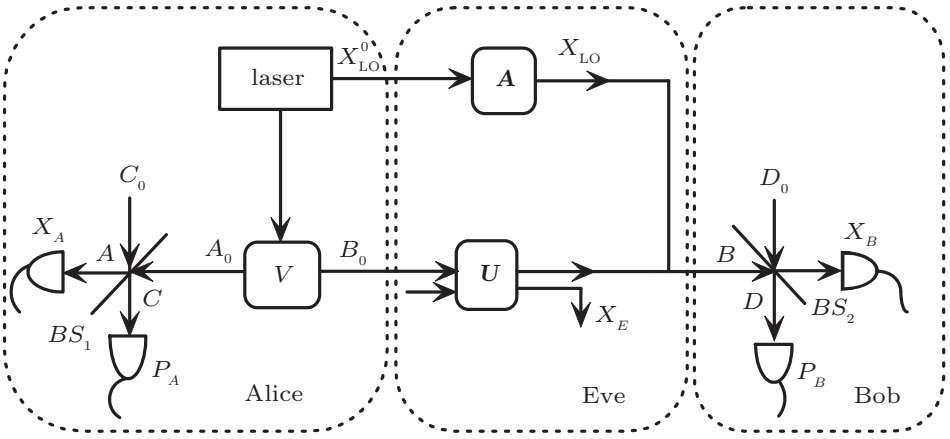


Fig. 1. The original structure of LOIA–CVQKD protocol based on Alice, generating EPR state and LO signal by laser. Eve performs LO intensity attenuation attack, which consists of attacking the signal beam with a traditional Gaussian collective attack with unitary operation $\boldsymbol{U}$ and attacking LO with intensity attenuation by a non-changing phase attenuator $\boldsymbol{A}$.

The covariance matrixes[34] between Alice's mode A and Bob's mode B read,

$$\begin{aligned}\gamma_{AB} &= \begin{pmatrix} \gamma_A & \sigma_{AB}^{\rm T} \\ \sigma_{AB} & \gamma_B \end{pmatrix} = \begin{pmatrix} a\boldsymbol{I} & c\sigma_z \\ c\sigma_z & b\boldsymbol{I} \end{pmatrix} \\ &= \begin{pmatrix} V\boldsymbol{I} & \sqrt{\partial(V^2-1)}\sigma_z \\ \sqrt{\partial(V^2-1)}\sigma_z & [\partial(V+\chi)]\boldsymbol{I} \end{pmatrix}, \end{aligned} \tag{3}$$

where σ_z represents the Pauli matrix and $\boldsymbol{I}$ is an identity matrix. From Eq. (3), we obtain $a = V$, $b = \partial V + (1-\partial)M$, and $c = \sqrt{\partial(V^2-1)}$. In addition, the total added noise is defined as $\chi = (1-\partial)/\partial + \varepsilon$ with excess noise $\varepsilon = (1-\partial)(M-1)/\partial$. Another covariance matrix between the two modes reads,

$$\gamma_{AB}^n = \begin{pmatrix} V\boldsymbol{I} & \sqrt{\kappa\partial(V^2-1)}\sigma_z \\ \sqrt{\kappa\partial(V^2-1)}\sigma_z & [\kappa\partial(V+\chi^n)]\boldsymbol{I} \end{pmatrix}. \tag{4}$$

Note that the superscript n indicates the intensity of the LO. In

this case, the total added noise is $\chi^n = (1-\kappa\partial)/\kappa\partial + \varepsilon^n$ with $\varepsilon^n = (\kappa\partial - 1 + \kappa M(1-\partial))/\kappa\partial$.[30] As a consequence, when Bob monitors the channel at destination, the channel transmission is ∂ and the excess noise is $\varepsilon = (1-\partial)(M-1)/\partial$. Without monitoring, the two variances become $\kappa\partial$ and $\varepsilon^n = [\kappa\partial - 1 + \kappa M(1-\partial)]/\kappa\partial$, respectively. If Eve wants to steal the largest amount of information while cannot be discovered, she must reduce ε^n to zero and introduce a noise M

$$M = \frac{1-\kappa\partial}{\kappa(1-\partial)}. \tag{5}$$

3. The middle-based LOIA–CVQKD protocol

Inspired by the method in Ref. [30], the middle-based LOIA–CVQKD protocol is proposed. The goal of our exploration is to improve the performance of the CVQKD under Eve's LOIA; see Fig. 2. In other words, the structure of the LOIA–CVQKD is modified by generating the entanglements from a distrusted eavesdropper Eve in the middle instead of preparing from the legal party Alice or Bob.

In our new scheme, the entangled source, a Gaussian state of variance V, is derived from the middle of the transmission based on a laser beam that generates the EPR state while producing two local oscillators LO_A^0 and LO_B^0. The modes A_0 and B_0 are emitted by the entangled source as the two-mode squeezed vacuum state. Alice and Bob independently implement measurement for one of two quadratures between the measured mode and the corresponding LO (LO_A and LO_B). The rotated quadratures are $\hat{x}_\alpha^A = \cos\alpha\hat{x}^A + \sin\alpha\hat{p}^A$ and $\hat{x}_\psi^B = \cos\psi\hat{x}^B + \sin\psi\hat{p}^B$, where α is referred to as the relative phase of the signal A and LO_A. Similarly, ψ is the relative phase between the signal B and LO_B. Figure 2 shows that Eve's attack consists of two LOIAs on each side of the source. The loss of the quantum channel of the protocol is described by the channel transmittances ∂_1 and ∂_2 with $\partial_n \in [0,1]$. It can be seen that Alice is the sender to create the initial entangled state where $\partial_1 = 1$. In the middle-based protocol, the channels are symmetric, i.e., $\partial_1 = \partial_2$. The Gaussian variances of the two entangled modes A_0 and B_0 are symmetric too, i.e., $V := V(A_0) = V(B_0)$.

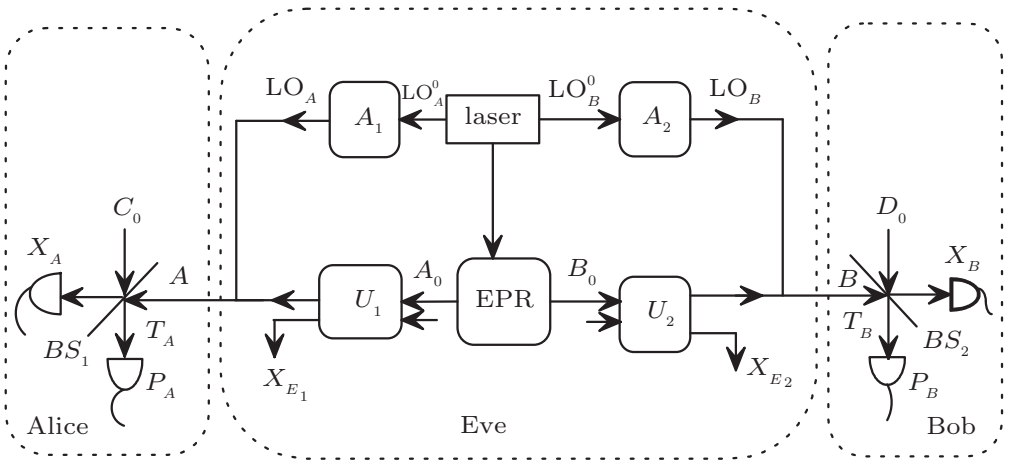


Fig. 2. The proposed structure of middle-based LOIA–CVQKD protocol where the EPR source and the LO signal are placed in the middle between Alice and Bob. Eve's attack consists of two LOIAs on either side of the entangled source. Alice and Bob can implement either homodyne or heterodyne detection with direct or reverse reconciliation.

When the system is monitored, the middle-based covariance matrix of Alice's mode A and Bob's mode B is shown as

$$\gamma_{AB}^m = \begin{pmatrix} \partial_1(V+\chi_1)\boldsymbol{I} & \sqrt{\partial_1\partial_2(V^2-1)}\sigma_z \\ \sqrt{\partial_1\partial_2(V^2-1)}\sigma_z & \partial_2(V+\chi_2)\boldsymbol{I} \end{pmatrix}, \tag{6}$$

where $a = \partial_1(V+\chi_1)$, $b = \partial_2(V+\chi_2)$, $c = \sqrt{\partial_1\partial_2(V^2-1)}$, $\chi_1 = (1-\partial_1)M_1/\partial_1$, and $\chi_2 = (1-\partial_2)M_2/\partial_2$. The superscript m represents the entanglement placed in the middle. When the channel is free of monitoring, the channel excess noise between Alice and Eve is

$$\varepsilon_n^m = \frac{\kappa\partial_1 - 1 + \kappa M_1(1-\partial_1)}{\kappa\partial_1}. \tag{7}$$

Considering the LOIA in the improved scheme, we obtain the equation for noise M_1

$$M_1 = \frac{1-\kappa\partial_1}{\kappa(1-\partial_1)}. \tag{8}$$

Similarly, we can calculate the noise

$$M_2 = (1-\kappa\partial_2)/(\kappa-\kappa\partial_2) \tag{9}$$

related to the transmission ∂_2, which is symmetric to ∂_1. Obviously, the result $M_1 = M_2 = (1-\kappa\partial)/(\kappa-\kappa\partial)$ is concluded by $\partial_1 = \partial_2 = \partial$.

When the entangled source is originated in the middle, the usual eight protocols[31] in entanglement-based CVQKD schemes can be summarized as four, which lies on the type of measurement used by Alice and Bob. As shown in Fig. 2, Alice applies a beam splitter (BS_1) of transmittance T_A over mode

A, if we fix $T_A = 1$ ($T_A = 1/2$) the homodyne (heterodyne) detection is done by Alice, resulting in preparing squeezed (coherent) states. Similarly, Bob can realize homodyne (heterodyne) detection by selecting the transmittance $T_B = 1$ ($T_B = 1/2$) of the beam splitter (BS_2) used by him. If Alice and Bob employ a same type of measurement, which means $T_A = T_B$, there is no difference between direct and reverse reconciliation protocols.[31] Therefore, the explicit equivalences between the middle-based protocols can be summarized as follows: (i) For squeezed states with $T_A = 1$ (coherent states with $T_A = 1/2$) and homodyne detection with $T_B = 1$ (heterodyne detection with $T_B = 1/2$), direct and reverse reconciliation protocols can be seen to be the same. (ii) Direct (reverse) reconciliation protocols based on coherent states and homodyne detection are equivalent for reverse (direct) reconciliation schemes on basis of squeezed states and heterodyne detection.

4. Secret key rates

To demonstrate the effectiveness of the middle-based method on performances, the secret key rates of coherent states protocols are analyzed and for simplicity the squeezed states protocols are not be considered, as they are analogous to the coherent states protocols. A detailed investigation of the secret key rate of a monitored CVQKD based on direct reconciliation is described as

$$R = I_{AB} - \chi_{AE}, \tag{10}$$

where I_{AB} is cited as the Shannon mutual information of Alice and Bob, while χ_{AE} is the Holevo bound of Alice and Eve. The modulation variance V_A and Bob's measurements on Alice's encodings V_B can be given, separately, by

$$V_A = T_1 V + (1 - T_1) M_1, \tag{11}$$

$$V_B = T_2 V + (1 - T_2) M_2. \tag{12}$$

The conditional variance reads

$$V_{X|Y} = V(X) - \frac{|\langle XY\rangle|^2}{V(Y)}. \tag{13}$$

Accordingly, the conditional variances in the middle-based system are obtained as

$$V_{A|B} = a - c^2/b, \tag{14}$$

and

$$V_{B|A} = b - c^2/a. \tag{15}$$

A monitoring is used to guarantee the instantaneous changed LO intensity in the practical protocol. The practical or unconditional secure secret key rate R_R and the monitoring secret key rate R are equal when the CVQKD system is attacked by LOIA, which is proved in Ref. [34].

Alice and Bob's mutual information of coherent states CVQKD with homodyne or heterodyne detection are calculated, respectively, by

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}}, \tag{16}$$

$$I_{AB} = \log_2 \frac{V_B + 1}{V_{B|A^M} + 1}, \tag{17}$$

where $V_{B|A^M} = b - c^2/(a+1)$. Eve and Alice's mutual information was mentioned by many publications[30,31] and can be displayed as

$$\chi_{AE} = S(E) - S(E|A). \tag{18}$$

To derive χ_{AE}, we should figure out the computing methods of $S(E)$ and $S(E|A)$. Fortunately, $S(E) = S(AB)$ can be obtained by using the fact that system E can apply a purification of the system AB. What is more, $S(AB)$ is relevant to the eigenvalues λ_1 and λ_2 of γ_{AB}, so the equation is

$$S(E) = S(AB) = G\Big(\frac{\lambda_1 - 1}{2}\Big) + G\Big(\frac{\lambda_2 - 1}{2}\Big), \tag{19}$$

where

$$\lambda^2_{1,2} = \frac{\Delta \pm \sqrt{\Delta^2 - 4D^2}}{2}, \tag{20}$$

with $\Delta = a^2 + b^2 - 2c^2$, $D = ab - c^2$, and $G(x) = (x+1)\log(x+1) - x\log(x)$. Two separate calculations $S(E|A)$ performed as Alice's measurement are different according to homodyne or heterodyne detection applied by Bob in the coherent states CVQKD. Firstly, the homodyne detection is introduced. The system BCE is pure with the purification arguments, so $S(E|A) = S(BC|A)$. The modes A and C can be mixed in a beam splitter (BS), then the covariance matrix γ^A_{BC} is gained by an operation of homodyne over mode A, as $S(BC|A)$ is correlated with the symplectic eigenvalues of γ^A_{BC}. This process is described as

$$\gamma_{ACB} = [S^{BS}_{AC} \otimes I_B]^T \gamma_{A_0C_0B} [S^{BS}_{AC} \otimes I_B]. \tag{21}$$

System BS acts on mode A and mode C then we can gain the symplectic transformation S^{BS}_{AC}. After Alice uses homodyne measurement, the correlation matrix γ^A_{BC} reads,

$$\begin{pmatrix} b - c^2/(a+1) & 0 & \sqrt{2}c/(a+1) & 0 \\ 0 & b & 0 & -c/\sqrt{2} \\ \sqrt{2}c/(a+1) & 0 & 2a/(a+1) & 0 \\ 0 & -c/\sqrt{2} & 0 & (a+1)/2 \end{pmatrix}. \tag{22}$$

Thus the conditional Von Neumann entropy based on homodyne detection is

$$S(E|A) = G\Big(\frac{\lambda_3}{2}\Big) + G\Big(\frac{\lambda_4}{2}\Big), \tag{23}$$

where $\lambda^2_{3,4} = (A \pm \sqrt{A^2 - 4B})/2$ with $A = (a + bD + \Delta)/(a + 1)$ and $B = D(b + D)/(a + 1)$.

Then, the conditional von Neumann entropy $S(E|A)$ is calculated when Bob heterodynes the incoming mode B. That is

$$S(E|A) = S(B|A) = G[(\lambda_3 - 1)/2], \tag{24}$$

with $\lambda_3 = b - c^2/(a + 1)$.

The efficiencies of the middle-based LOIA–CVQKD protocol in terms of the secret key rates and the maximal channel losses will be illustrated in this section. There are several parameters affected the performances of the respective systems, such as the variance of entangled source V, the transmission κ of LO, and channel losses.

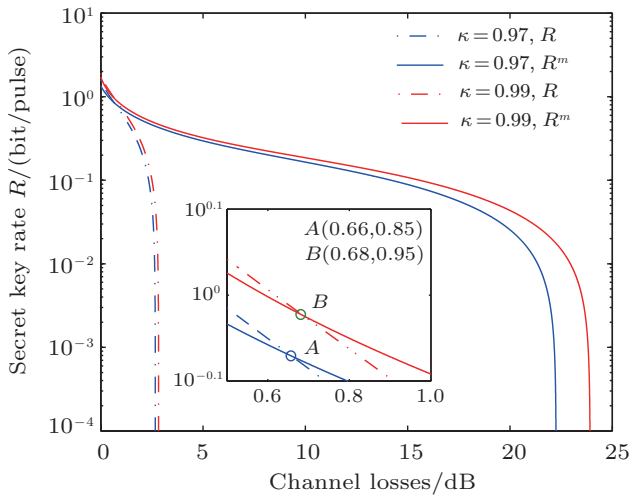


Fig. 3. (color online) The balances between the secret key rates and the maximal channel losses of the middle-based and the original LOIA–CVQKD protocols with coherent states and homodyne detection for the given parameters $V = 20$, $\kappa \in \{0.97, 0.99\}$.

So far we have assumed the parameter $V = 20$ to study the effects of κ on the coherent states protocols with the homodyne detection as shown in Fig. 3 and the heterodyne detection as shown in Fig. 4. The practical secret key rates of the middle-based LOIA–CVQKD are denoted by solid lines, and the practical secret key rates of the initial LOIA–CVQKD without the entangled source in the middle are represented by the dashed lines. The secret rates and maximum channel losses can be increased with the increase of κ, both for the middle-based and the original LOIA–CVQKD protocols. Noting that the dashed and solid lines meet at point $A(0.66, 0.85)$ corresponding to $\kappa = 0.97$ and $B(0.68, 0.95)$ corresponding to $\kappa = 0.99$ as shown in Fig. 3. The point $A(0.66, 0.85)$ is taken as an example from which we can see that if the channel loss is greater than 0.66 dB, the key rate of the middle-based protocol is far higher than that of the original one under the LOIA. While if the value is lower than 0.66 dB, the secret key rate of the former is slightly lower than the latter. In view of the above characteristic, the abscissa value of intersection is defined as the threshold value. Therefore, as the heterodyne case shown in Fig. 4, the threshold value is 1.03 dB and 0.91 dB when $\kappa = 0.97$ and $\kappa = 0.99$. By comparison, we find the homodyne threshold value is smaller than the heterodyne one when the κ value of the two types of protocols is the same. Thus the middle-based method with the homodyne detection may play a positive role in performance earlier than that in performing heterodyne detection. In Fig. 3, when $\kappa = 0.99$ (red lines), the maximum gap of the channel losses between the solid lines and dashed ones in the same color appears, and a similar result can be seen in Fig. 4. What the phenomenon indicates that the performance of the middle-based LOIA–CVQKD is improved as the value of κ increases. By studying the data of Figs. 3 and 4, the maximum gap of the homodyne case is 21.04 dB. Obviously, it is much bigger than that of the heterodyne detection protocol, which is about 0.09 dB.

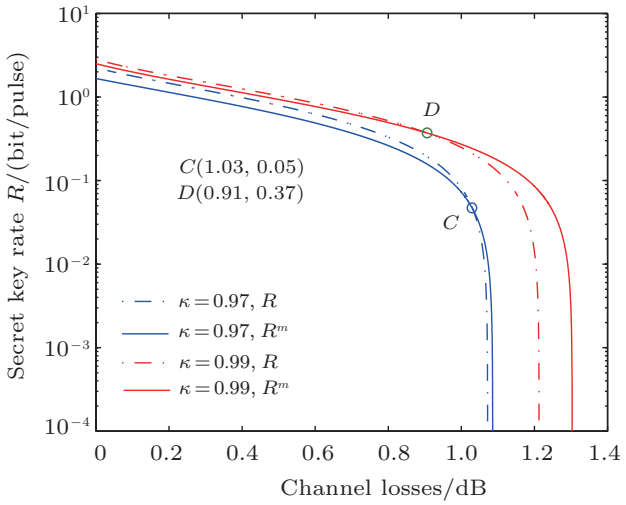


Fig. 4. (color online) The balances between the secret key rates and the maximal channel losses of the middle-based and the original LOIA–CVQKD protocols with coherent states and heterodyne detection for the given parameters $V = 20$, $\kappa \in \{0.97, 0.99\}$.

The effect of V on the performance of the schemes is also taken into account with parameter $\kappa = 0.99$. From the Figs. 5 and 6, we can find that the efficiency of all protocols can be enhanced with the increase of the value of V. As displayed in Fig.5 or Fig. 6, with the different values of the parameter V the threshold values are different. For example, when Bob employs the heterodyne detection, the threshold values of protocols with $V = 10$ and $V = 20$ are 0.77 dB and 0.68 dB, respectively. By comparisons, it is found that in protocols based on the heterodyne detection the bigger value of parameter V, which is controlled in an appropriate range, may cause a faster key rate of the growth. Moreover, by observing the simulation results of Figs. 3, 4, 5, and 6, we conclude that the middle-based schemes based on coherent states and the homodyne

detection can circumvent the 3-dB loss limit while the heterodyne detection cases cannot. Note that when the quantum channel is attacked under the LOIA, the secret key rates can be compromised severely. Fortunately, this problem can be solved via the entanglement in the middle when channel loss reaches the threshold value.

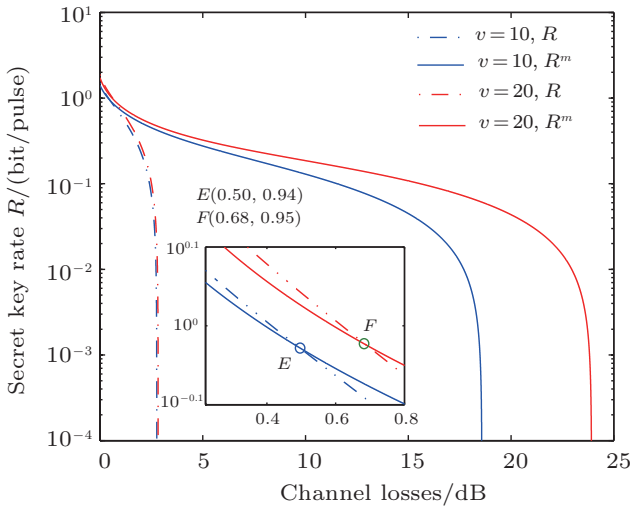


Fig. 5. (color online) The balances between the secret key rates and the maximal channel losses of the middle-based and the original LOIA–CVQKD protocols with coherent states and homodyne detection for the given parameters $\kappa = 0.99$, $V \in \{10, 20\}$.

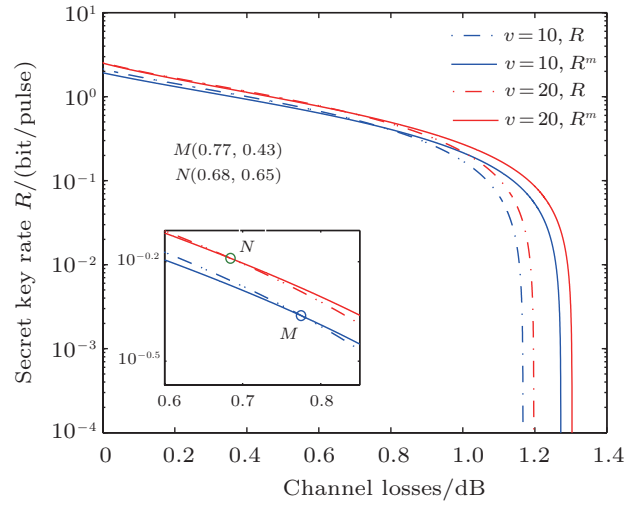


Fig. 6. (color online) The balances between the secret key rates and the maximal channel losses of the middle-based and the original LOIA–CVQKD protocols with coherent states and heterodyne detection for the given parameters $\kappa = 0.99$, $V \in \{10, 20\}$.

As is well known, the channel loss = aL dB is certificated and L represents the transmission distance between Alice and Bob with channel loss coefficient of optical fiber $a =$ 0.2 dB/km, thus we can conclude from our study that the maximum transmission distance can increase almost 105.2 km for the homodyne detection, while that for the heterodyne detection is about 0.45 km when $V = 20$ and $\kappa = 0.99$. Compared with the striking effect of the middle-based LOIA–CVQKD on the homodyne detection, the effect on the heterodyne detection is much less. All the results show that it is much beneficial to originate the entanglement in the middle with appropriate parameters V and κ to balance the high secret key rate and the transmission distance for the LOIA–CVQKD based on cohere states.

5. Conclusion

In this paper, we proposed the LOIA–CVQKD protocols with the entanglement in the middle. The most obvious superiority of the modified protocols is that the larger tolerance to loss can be received over the lossy channel in comparison with the original protocols under LOIA. Alternative advantage is found in increasing the secret key rates of the schemes when channel loss reaches the threshold value. In addition, by choosing appropriately the system parameters κ and V, the performance of the protocols can be enhanced to some extent. By studying the threshold values of the simulation data, we find the middle-based method in the homodyne detection can play a positive role in performance earlier than that in the heterodyne detection. Furthermore, especially the simulation results indicate that if Bob homodynes the incoming mode B, the improved protocol can conquer the 3-dB loss limit while the heterodyne protocol cannot realize this goal, even though other conditions are identical. By comparing the above two cases, we conclude that the entanglement in the middle is more suitable for LOIA–CVQKD protocols with the homodyne detection than that with the heterodyne detection.

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Du? sek M, Lutkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[3] Furusawa A, Sørensen J L, Braunstein S L, Fuchs C A, Kimble H J and Polzik E S 1998 *Science* **282** 706
[4] Grosshans F 2005 *Phys. Rev. Lett.* **94** 020504
[5] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[6] Jouguet P, Kunz-Jacques S, Diamanti E and Leverrier A 2012 *Phys. Rev. A* **86** 032309
[7] Guo Y, Liao Q, Wang Y, Huang D, Huang P and Zeng G 2017 *Phys. Rev. A* **95** 032304
[8] Thearle O, Assad S M and Symul T 2016 *Phys. Rev. A* **93** 042343
[9] Li Y, Bao W S, Li H W, Zhou C and Wang Y 2015 *Chin. Phys. B* **24** 110307
[10] Gao G 2015 *Chin. Phys. B* **24** 080305
[11] Ma H X, Bao W S, Li H W and Chou C 2016 *Chin. Phys. B* **25** 080309
[12] Yang F, Shi R, Guo Y, Shi J J and Zeng G 2015 *Quantum Inf. Process.* **14** 3041
[13] Li H R, Li F L and Yang Y 2006 *Chin. Phys.* **15** 2947
[14] He G Q, Zhu S W, Guo H B and Zeng G H 2008 *Chin. Phys. B* **17** 1263
[15] Pirandola S, Braunstein S L and Lloyd S 2008 *Phys. Rev. Lett.* **101** 200504
[16] Lorenz S, Rigas J, Heid M, Andersen U L, Lütkenhaus N and Leuchs G 2002 *Phys. Rev. Lett.* **88** 057902
[17] Ottaviani C, Mancini S and Pirandola S 2015 *Phys. Rev. A* **92** 062323
[18] Lu Z, Shi J H and Li F G 2017 *Chin. Phys. B* **26** 040304
[19] Navascués M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502
[20] Navascués M and Acín A 2005 *Phys. Rev. Lett.* **94** 020505
[21] Leverrier A and Grangier P 2010 *Phys. Rev. A* **81** 062314

[22] Gong L H, Song H C, He C S, Liu Y and Zhou N R 2014 *Phys. Scr.* **89** 035101
[23] Zhou N R, Li J F, Yu Z B, Gong L H and Farouk A 2017 *Quantum Inf. Process.* **16** 4
[24] Liu C Q, Zhu C H, Wang L H, Zhang L X and Pei C X 2016 *Chin. Phys. Lett.* **33** 100301
[25] Liu Q and Tan Y G 2016 *Chin. Phys. Lett.* **33** 90303
[26] Wu C F, Du Y N, Wang J D, Wei Z J, Qin X J, Zhao F and Zhang Z M 2016 *Acta Phys. Sin.* **65** 100302 (in Chinese)
[27] Bao H Z, Bao W S, Wang Y, 2, Chen R K, Ma H X, Zhou C and Li H W 2017 *Chin. Phys. B* **26** 050302
[28] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
[29] Huang P, He G Q, Fang J and Zeng G H 2013 *Phys. Rev. A* **87** 012317
[30] Weedbrook C 2013 *Phys. Rev. A* **87** 022308
[31] García-Patrón R and Cerf N J 2009 *Phys. Rev. Lett.* **102** 130501
[32] Häseler H, Moroder T and L ütkenhaus N 2008 *Phys. Rev. A* **77** 032303
[33] 2017 *Phys. Rev. A* **95** 012316
[34] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev. A* **88** 022339
[35] Jouguet P, Kunz-Jacques S and Diamanti E 2013 *Phys. Rev. A* **87** 062313
[36] Lo H K and Chau H F 1999 *Science* **283** 2050
[37] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[38] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[39] Ma X, Fung C H F and Lo H K 2007 *Phys. Rev. A* **76** 012307
[40] Erven C, Couteau C, Laflamme R and Weihs G 2008 *Opt. Express* **16** 16840
[41] Raymer M G, Cooper J, Carmichael H J, Beck M and Smithey D T 1995 *J. Opt. Soc. Am. B* **12** 1801