Continuous-variable measurement-device-independent multipartite quantum communication

Yadong Wu,[1] Jian Zhou,[2] Xinbao Gong,[1] Ying Guo,[2] Zhi-Ming Zhang,[3] and Guangqiang He[1,3,4,*]

[1]*State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, People's Republic of China*

[2]*School of Information Science and Engineering, Central South University, Changsha 410083, People's Republic of China*

[3]*Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, South China Normal University, Guangzhou 510006, People's Republic of China*

[4]*State Key Laboratory of Precision Spectroscopy, East China Normal University, Shanghai 200062, People's Republic of China*

(Received 16 June 2015; published 22 February 2016)

A continuous-variable measurement-device-independent multiparty quantum communication protocol is investigated in this paper. Utilizing the distributed continuous-variable Greenberger-Horne-Zeilinger state, this protocol can implement both quantum cryptographic conference and quantum secret sharing. We analyze the security of the protocol against both the entangling cloner attack and the coherent attack. The entangling cloner attack is a practical individual attack, and the coherent attack is the optimal attack Eve can implement. Simulation results show that the coherent attack can greatly reduce the secret key rate. Different kinds of entangled attacks are compared and we finally discuss the optimal coherent attacks.

DOI: 10.1103/PhysRevA.93.022325

I. INTRODUCTION

In quantum cryptography, to maximize secure transmission distance and remove detector side attacks, physicists use the measurement-device-independent (MDI) method [1], which has been experimentally realized [2]. In MDI quantum key distribution (QKD), anyone participating in the quantum communication connects to an untrusted party, who is not a legitimate member in the quantum communication. The secure communication relies on the untrusted party's measurement. So attacks on measurement devices are moved from legitimate members' sides to the untrusted party's side. Since any attack on measurement devices can be transformed into some attack in the channel followed by a correctly operated measurement [3], we can just consider attacks in the channels. One important realistic attack is the entangling cloner attack, which utilizes the EPR state to maximize the information Eve can steal in an individual attack [4]. The optimal attack Eve can implement, however, is not an individual attack, but a coherent attack, where Eve uses the ancillary system to globally interact with the signals and finally makes an optimal joint measurement.

MDI multipartite quantum communication with long distance is investigated in Ref. [5]. This research is based on discrete variable systems, while Gaussian modulation and homodyne measurement [6] provide us another way to realize MDI multipartite quantum communication in continuous-variable (CV) quantum systems. In this paper, we use CV to investigate multiparty quantum cryptography. CV MDI two-party quantum cryptography has been investigated in Ref. [3]. Instead of using coherent state and heterodyne measurement as Ref. [3], our protocol utilizes squeezed state of light and homodyne measurement to maximize the secret key rate. Hence the main difficulty for the practical realization of our protocol is to generate squeezed state of light. Although it is much more difficult than generating a coherent state of light, some experiments on CV squeezed states have been done [7,8], indicating that CV quantum communication based on the squeezed state can be realized in the future.

We design and investigate two kinds of CV MDI multipartite quantum communication protocols in this paper. One is quantum cryptographic conference (QCC) [9] and the other is quantum secret sharing (QSS) [10]. QCC enables each individual within a specific group to decrypt the encrypted messages published by any group member, whereas nobody outside the group can successfully decrypt the secret messages. QSS enables an authorized group of people to decrypt the secret messages by collaboration, but any unauthorized group of people fails to decrypt the messages.

This paper is organized as follows. Section II introduces the MDI multipartite quantum communication protocols in detail. Section III analyzes the security of this protocol against the entangling cloner attack and the coherent attack, respectively, for both QCC and QSS. Section IV shows the numerical simulation of this protocol against two kinds of attacks. Section V gives the conclusion of this paper.

II. PROTOCOLS OF MULTIPARTITE QUANTUM COMMUNICATION

We are going to explain the details of the protocols for both QCC and QSS in this section. Both of them rely on the postprocessed GHZ state, while the main difference is within the postprocessing of classical data.

Before going into the detail of the protocol, we want to first introduce the CV Greenberger-Horne-Zeilinger (GHZ) state [11]. To implement these two kinds of multiparty quantum communication protocols, we utilize CV GHZ state, which is theoretically investigated [12] and experimentally realized by linear optics [13,14]. It is a multipartite entangled state whose uncertainties of relative position and total momentum are squeezed. For the tripartite CV GHZ state, their positions and momenta satisfy the relations: $\hat{X}_1 - \hat{X}_2 \to 0, \hat{X}_2 - \hat{X}_3 \to 0$, and $\hat{P}_1 + \hat{P}_2 + \hat{P}_3 \to 0$. The CV GHZ state can be generated by a series of beam splitters with particular transmittances and squeezed vacuum states [15]. But in our protocol, the CV GHZ

*gqhe@sjtu.edu.cn

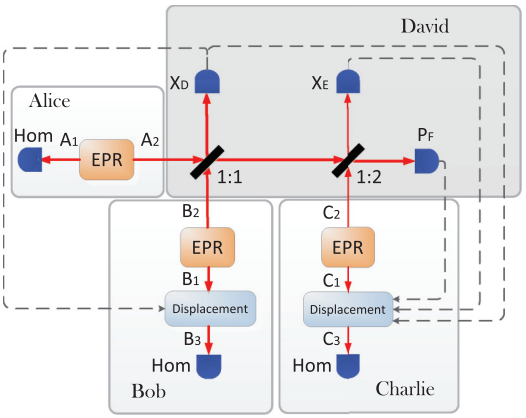

FIG. 1. EB scheme.

state is not prepared and distributed, whereas it is obtained by postprocessing using the idea of entanglement swapping [16,17].

Two schemes of the protocol are shown in the following. One is the entanglement-based (EB) scheme shown in Fig. 1 and the other is the prepare-and-measurement (PM) scheme shown in Fig. 2. In both EB and PM schemes, Alice, Bob, and Charlie are connected with a fourth, untrusted person David and the secure communication relies on David's measurements. It implies that both schemes are MDI multipartite quantum communication protocols, which remove any detector side attack in Alice's, Bob's, and Charlie's sides. We introduce the EB scheme first, then the PM scheme.

Alice, Bob, and Charlie prepare an EPR pair, respectively, which, in the CV case, is a two-mode squeezed state (TMSS) [18]. They hold one mode of the EPR pair in their own possession and send the other mode to the fourth, untrusted person David. Receiving three modes from Alice, Bob, and Charlie, David does the following operation. The two modes from Alice and Bob go through a beam splitter with transmittance $\frac{1}{\sqrt{2}}$. Then the position quadrature $\hat{X}_D$ of the output mode D is detected by a homodyne measurement. The other output mode is mixed with the mode from Charlie by another beam splitter with transmittance $\sqrt{\frac{2}{3}}$ and the output modes are denoted by E and F. The position quadrature $\hat{X}_E$ and the momentum quadrature $\hat{P}_F$ are detected by two homodyne measurements. David publishes the measurement outcomes X_D, X_E, and P_F. To construct a GHZ state, Bob and Charlie use these data

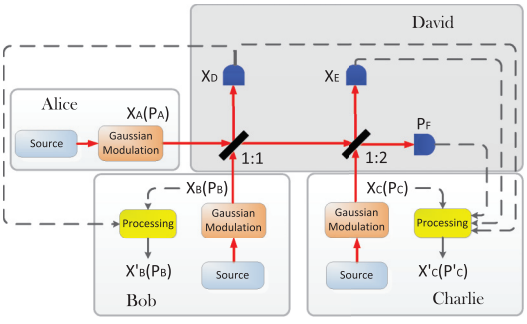

FIG. 2. PM scheme.

to finish the displacement operations on their own modes. Specifically, Bob shifts the position quadrature $\hat{X}_{B_1}$ with $\sqrt{2}X_D$ and Charlie shifts the position $\hat{X}_{C_1}$ and the momentum $\hat{P}_{C_1}$ with $(\sqrt{\frac{1}{2}}X_D - \sqrt{\frac{3}{2}}X_E)$ and $\sqrt{3}P_F$, respectively. After that, Alice, Bob, and Charlie own the modes A_1, B_3, and C_3, respectively, and these three modes form a distributed CV GHZ state. As for the QCC scheme, they apply homodyne measurements over the positions, respectively, and use the measurement outcomes X_{A_1}, X_{B_3}, and X_{C_3} to do reconciliation and postselection. Since $\hat{X}_{A_1} - \hat{X}_{B_3} \to 0$ and $\hat{X}_{B_3} - \hat{X}_{C_3} \to 0$, they can obtain coincident keys. As for the QSS scheme, they homodyne the momentum quadratures, respectively. At least two of the three must share their measurement outcomes and do reconciliation and postselection with the third person. Because of the relation $\hat{P}_{A_1} + \hat{P}_{B_3} + \hat{P}_{C_3} \to 0$, they can obtain the third person's secret key. In both the QCC and QSS schemes, with the random secret keys, they can use the one-time pad [19] to implement unconditional secure multipartite quantum communication.

Now we introduce the equivalent PM scheme. Alice, Bob, and Charlie first generate Gaussian-distributed random numbers, respectively, and keep these data private. In QCC, Alice, Bob, and Charlie do Gaussian modulation on position-squeezed vacuum states so that the mean positions of the modulated squeezed states become Gaussian-distributed random numbers X_A, X_B, and X_C. In QSS, they do Gaussian modulation on momentum-squeezed vacuum states so that the mean momenta of the modulated squeezed states become Gaussian-distributed random numbers P_A, P_B, and P_C. This preparation of a Gaussian modulated squeezed state is equivalent to making a single-mode homodyne measurement over a TMSS. This is because as for a TMSS, single-mode homodyne detection projects the other mode into a squeezed state with a specific mean value related to the measurement outcome. Then the Gaussian modulated squeezed states are sent to the fourth, untrusted person David. David mixes these three modes by two specific beam splitters, makes homodyne measurements on the three outputs, and publishes the measurement outcomes, same as the EB scheme. Bob and Charlie use the public data to postprocess their own data. In QCC, Alice remains her data constant, Bob modifies X_B as $X'_B = X_B + \sqrt{2}X_D$ and Charlie modifies X_C as $X'_C = X_C + (\sqrt{\frac{1}{2}}X_D - \sqrt{\frac{3}{2}}X_E)$, so that their data satisfy the relation $X_A - X'_B \to 0$ and $X'_B - X'_C \to 0$. By doing reconciliation and postprocessing, they can obtain the coincident keys for QCC. In QSS, Alice and Bob remain their data unchanged and Charlie replaces P_C with $P'_C = P_C + \sqrt{3}P_F$, making their data satisfy $P_A + P_B + P'_C \to 0$. Finally, two of them share their private data with each other. By reconciliation and postprocessing, they can obtain the secret key of the third person.

III. SECURITY ANALYSIS

Now let's investigate the security of this protocol for both QCC and QSS schemes. The security of EB and PM schemes are equivalent. Since in the EB scheme, we can use the method of purification to calculate the secret key rate, we choose to analyze the EB scheme. Our security analysis involves two

kinds of attacks: one is the entangling cloner attack and the other is the coherent attack.

In general, there can be any attack at the detector side, i.e., at David's side in Fig. 1. But any attack at the detector side is equivalent to adding a specific attack in the channel followed by a correctly operated measurement device [3]. Thus we can assume that Eve's attack only exists in the channel and that David's operation and measurement data can be trusted.

A. Independent entangling cloner attack

In this subsection, we focus on the independent entangling cloner attack in each channel. As shown in Fig. 3, at the beginning, Eve owns three independent EPR pairs, i.e., three TMSS's. He injects one mode of each pair into the channel, through a beam splitter with transmittance $\eta_A(\eta_B,\eta_C)$, and stores the output mode of each beam splitter, $\hat{E}_{A1(B1,C1)}$, and the other mode of each EPR pair, $\hat{E}_{A2(B2,C2)}$, in the quantum memory.

In QCC, we consider the case when Alice wants to send her secret message to Bob and Charlie. To achieve this, Alice needs to share secret keys with Bob and Charlie, respectively, by implementing QKD. The secret key rate can be defined as

$$K_{\mathrm{QCC}} = \min\{K_{\mathrm{AB}}, K_{\mathrm{AC}}\}, \tag{1}$$

where K_{AB} is the secret key rate between Alice and Bob, and K_{AC} is the secret key rate between Alice and Charlie.

Two kinds of reconciliation methods lead to different secret key rates. With reverse reconciliation,

$$\begin{aligned} K_{\mathrm{AB}}^{\mathrm{RR}} &= \beta I\left(X_{A_1} : X_{B_3}\right) - I\left(X_{A_1} : X_{E_{A1}}, X_{E_{A2}}\right), \\ K_{\mathrm{AC}}^{\mathrm{RR}} &= \beta I\left(X_{A_1} : X_{C_3}\right) - I\left(X_{A_1} : X_{E_{A1}}, X_{E_{A2}}\right). \end{aligned} \tag{2}$$

With direct reconciliation,

$$\begin{aligned} K_{\mathrm{AB}}^{\mathrm{DR}} &= \beta I\left(X_{A_1} : X_{B_3}\right) - I\left(X_{B_3} : X_{E_{B1}}, X_{E_{B2}}\right), \\ K_{\mathrm{AC}}^{\mathrm{DR}} &= \beta I\left(X_{A_1} : X_{C_3}\right) - I\left(X_{C_3} : X_{E_{C1}}, X_{E_{C2}}\right). \end{aligned} \tag{3}$$

At the right-hand sides of Eq. (2) and Eq. (3), the first term represents the mutual information between the measurement data of X_{A_1} and the measurement data of $X_{B_3(C_3)}$ [20], and the second term denotes the mutual information between the measurement data of $X_{A_1(B_3,C_3)}$ and the measurement data of $X_{E_{A1(B1,C1)}}$ and $X_{E_{A2(B2,C2)}}$. β is the reconciliation efficiency.

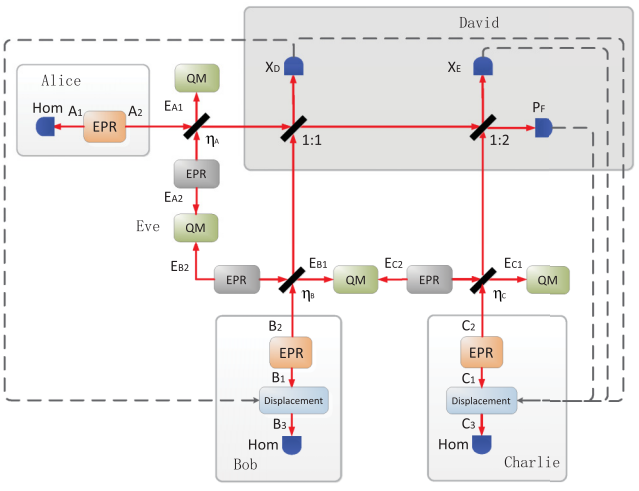

FIG. 3. EB scheme against independent entangling cloner attacks.

In QSS, we assume Charlie holds the secret key, and Alice and Bob have to collaborate with each other to obtain the secret key. The secret key rate can be defined as

$$K_{\mathrm{QSS}}^{\mathrm{RR}} = \beta I\left(P_{A_1}, P_{B_3} : P_{C_3}\right) - I\left(P_{C_3} : P_{E_{C1}}, P_{E_{C2}}\right), \tag{4}$$

with reverse reconciliation, and

$$\begin{aligned} K_{\mathrm{QSS}}^{\mathrm{DR}} = \beta I\left(P_{A_1}, P_{B_3} : P_{C_3}\right) - I\left(P_{A_1} : P_{E_{A1}}, P_{E_{A2}}\right) \\ - I\left(P_{B_3} : P_{E_{B1}}, P_{E_{B2}}\right), \end{aligned} \tag{5}$$

with direct reconciliation. At the right-hand sides of Eq. (4) and Eq. (5), the first term represents the mutual information between the measurement data of P_{A_1} and the measurement data of P_{B_3} and P_{C_3}, and the second term denotes the mutual information between the measurement data of $P_{A_1(B_3,C_3)}$ and the measurement data of $P_{E_{A1(B1,C1)}}$ and $P_{E_{A2(B2,C2)}}$.

To calculate the mutual information in Eqs. (2)–(5), we need to obtain the covariance matrix of the whole state held by Alice, Bob, Charlie, and Eve in the following way.

At the beginning of this protocol, the initial whole state ρ_{A,E_A,B,E_B,C,E_C} is the tensor product of six independent TMSS's. Its covariance matrix is

$$\mathbf{V}_{A,E_A,B,E_B,C,E_C} = \bigoplus_{k=1}^{3} \mathbf{V}, \tag{6}$$

where

$$\mathbf{V} = \begin{pmatrix} V\mathbf{I} & \sqrt{V^2-1}\mathbf{Z} & \mathbf{0} & \mathbf{0} \\ \sqrt{V^2-1}\mathbf{Z} & V\mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & V_E\mathbf{I} & \sqrt{V_E^2-1}\mathbf{Z} \\ \mathbf{0} & \mathbf{0} & \sqrt{V_E^2-1}\mathbf{Z} & V_E\mathbf{I} \end{pmatrix}. \tag{7}$$

V ($V \geqslant 1$) is the variance of Alice's (Bob's, Charlie's) TMSS's, V_E ($V_E \geqslant 1$) is the variance of Eve's TMSS's, $\mathbf{I}$ is identity matrix, $\mathbf{0}$ is zero matrix, and $\mathbf{Z}$ is the Pauli Z matrix.

In each channel, Alice's (Bob's, Charlie's) mode goes through a beam splitter with transmittance $\eta_A(\eta_B,\eta_C)$. The overall operation of these three beam splitters can be written as

$$\mathbf{U_{Eve}} = \mathbf{BS_A} \bigoplus \mathbf{BS_B} \bigoplus \mathbf{BS_C}, \tag{8}$$

where

$$\mathbf{BS_{A(B,C)}} = \begin{pmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \sqrt{\eta_{A(B,C)}}\mathbf{I} & \sqrt{1-\eta_{A(B,C)}}\mathbf{I} & \mathbf{0} \\ \mathbf{0} & -\sqrt{1-\eta_{A(B,C)}}\mathbf{I} & \sqrt{\eta_{A(B,C)}}\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I} \end{pmatrix}. \tag{9}$$

At David's side, the overall operation of the two beam splitters is

$$\mathbf{U_{David}} = \mathbf{BS_2 BS_1}, \tag{10}$$

where

$$\mathbf{BS_1}=\begin{pmatrix}\mathbf{W_1}&\mathbf{W_2}&\mathbf{0}\\-\mathbf{W_2}&\mathbf{W_1}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{I}\end{pmatrix},\ \mathbf{BS_2}=\begin{pmatrix}\mathbf{W_3}&\mathbf{0}&\mathbf{W_4}\\\mathbf{0}&\mathbf{I}&\mathbf{0}\\-\mathbf{W_4}&\mathbf{0}&\mathbf{W_3}\end{pmatrix},$$

$$\mathbf{W_1}=\begin{pmatrix}\mathbf{I}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\frac{\mathbf{1}}{\sqrt{2}}\mathbf{I}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{I}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{I}\end{pmatrix},\ \mathbf{W_2}=\begin{pmatrix}\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\frac{\mathbf{1}}{\sqrt{2}}\mathbf{I}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}\end{pmatrix},$$

$$\mathbf{W_3}=\begin{pmatrix}\mathbf{I}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\sqrt{\frac{\mathbf{2}}{\mathbf{3}}}\mathbf{I}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{I}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{I}\end{pmatrix},\ \mathbf{W_4}=\begin{pmatrix}\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\frac{\mathbf{1}}{\sqrt{3}}\mathbf{I}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}\\\mathbf{0}&\mathbf{0}&\mathbf{0}&\mathbf{0}\end{pmatrix}. \tag{11}$$

Before any homodyne measurement, the whole state becomes $\rho_{A_1,F,E_{A1},E_{A2},B_1,D,E_{B1},E_{B2},C_1,E,E_{C1},E_{C2}}$ with the covariance matrix,

$$\mathbf{V}_{A_1,F,E_{A1},E_{A2},B_1,D,E_{B1},E_{B2},C_1,E,E_{C1},E_{C2}} = \mathbf{U}_{\text{David}}\mathbf{U}_{\text{Eve}}\mathbf{V}_{A,E_A,B,E_B,C,E_C}\mathbf{U}_{\text{Eve}}^T\mathbf{U}_{\text{David}}^T. \tag{12}$$

By permutating the modes in the covariance matrix in Eq. (12) in the order of A_1,B_1,C_1,Eve,D,E,F, we can rewrite it in the form of

$$\mathbf{V}_{A_1,B_1,C_1,\text{Eve},D,E,F}=\begin{pmatrix}\mathbf{V}_{A_1,B_1,C_1,\text{Eve},D,E}&\mathbf{C}\\\mathbf{C}^T&\mathbf{V}_F\end{pmatrix}, \tag{13}$$

where the subscript Eve denotes all the six modes $E_{A1},E_{A2},E_{B1},E_{B2},E_{C1}$, and E_{C2}, and $\mathbf{C}$ represents the covariance submatrix.

Homodyning $\hat{P}_F$ turns the reduced covariance matrix $\mathbf{V}_{A_1,B_1,C_1,\text{Eve,D,E}}$ into [21]

$$\mathbf{V}_{A_1,B_1,C_1,\text{Eve},D,E|P_F} = \mathbf{V}_{A_1,B_1,C_1,\text{Eve},D,E}-\mathbf{C}\begin{pmatrix}0&0\\0&\frac{1}{V(\hat{P}_F)}\end{pmatrix}\mathbf{C}^T, \tag{14}$$

where $V(\hat{P}_F)$ is the variance of $\hat{P}_F$, given in the matrix $\mathbf{V}_F$. As shown in Eq. (14), the covariance matrix following partial homodyne measurement has nothing to do with the measurement outcome. Thus, although the measurement result may be different each time, the covariance matrix following the partial measurement remains the same.

Iteratively calculating the covariance matrix of the state after partial Gaussian measurements [6,22], we can obtain the covariance matrix of the partial state $\rho_{A_1,B_1,C_1,\text{Eve}}$ after $\hat{X}_D,\hat{X}_E$, and $\hat{P}_F$ are homodyned.

Since displacement operations $e^{i\xi\hat{X}}$ and $e^{i\xi'\hat{P}}$ remain the variances and covariances of $\hat{X}$ and $\hat{P}$ the same, while only changes their mean values, the partial state ρ_{A_1,B_3,C_3} owns the same covariance matrix as $\rho_{A_1,B_1,C_1|X_D,X_E,P_F}$. Thus, by now, we have obtained the covariance matrix of the state $\rho_{A_1,B_3,C_3,\text{Eve}}$, denoted by $\mathbf{V}_{A_1,B_3,C_3,\text{Eve}}$.

Now we can calculate Eqs. (2)–(5) by using $\mathbf{V}_{A_1,B_3,C_3,\text{Eve}}$. In this calculation, we may need to obtain the covariance matrix of a reduced state of $\rho_{A_1,B_3,C_3,\text{Eve}}$ by using the formula similar to Eq. (14), when a partial homodyne measurement is applied.

The first terms at the right-hand sides of Eqs. (2) and (3) are given by

$$I\left(X_{A_1}:X_{B_3(C_3)}\right)=\frac{1}{2}\log_2\frac{V(\hat{X}_{B_3(C_3)})}{V(\hat{X}_{B_3(C_3)}|X_{A_1})}, \tag{15}$$

where $V(\hat{X}_{B_3(C_3)}|X_{A_1})$ is the conditional variance of $\hat{X}_{B_3(C_3)}$ after $\hat{X}_{A_1}$ is homodyned and can be obtained from the covariance matrix $\mathbf{V}_{B_3C_3|X_{A_1}}$.

The second terms in Eqs. (2) and (3) are

$$I\left(X_{A_1(B_3,C_3)}:X_{E_{A1(B1,C1)}},X_{E_{A2(B2,C2)}}\right) = \frac{1}{2}\log_2\frac{V(\hat{X}_{A1(B1,C1)})}{V(\hat{X}_{A1(B1,C1)}|X_{E_{A1(B1,C1)}},X_{E_{A2(B2,C2)}})}, \tag{16}$$

where $V(\hat{X}_{A1(B1,C1)}|X_{E_{A1(B1,C1)}},X_{E_{A2(B2,C2)}})$ is the variance of $\hat{X}_{A1(B1,C1)}$ after $\hat{X}_{E_{A1(B1,C1)}}$ and $\hat{X}_{E_{A2(B2,C2)}}$ are homodyned, and can be obtained from the reduced covariance matrix $\mathbf{V}_{A_1(B_3,C_3)|X_{E_{A1(B1,C1)}},X_{E_{A2(B2,C2)}}}$. It is the maximal mutual information between Eve's measurement data and Alice's (Bob's, Charlie's) measurement data. Because Eve can decrease $V(\hat{X}_{A1})$ most by homodyning on $\hat{X}_{E_{A1}}$ and $\hat{X}_{E_{A2}}$ for reverse reconciliation, and reduce $V(\hat{X}_{B_3(C_3)})$ most by homodyning on $\hat{X}_{E_{B1(C1)}}$ and $\hat{X}_{E_{B2(C2)}}$ for direct reconciliation.

The first terms at the right-hand sides of Eq. (4) and Eq. (5) are

$$I\left(P_{A_1},P_{B_3}:P_{C_3}\right)=\frac{1}{2}\log_2\frac{V\left(\hat{P}_{C_3}\right)}{V\left(\hat{P}_{C_3}|P_{A_1},P_{B_3}\right)}. \tag{17}$$

The second term in Eq. (4) is

$$I\left(P_{C_3}:P_{E_{C1}},P_{E_{C2}}\right)=\frac{1}{2}\log_2\frac{V\left(\hat{P}_{C_3}\right)}{V\left(\hat{P}_{C_3}|P_{E_{C1}},P_{E_{C2}}\right)}, \tag{18}$$

which is the maximal mutual information between Eve's measurement data and Charlie's measurement data with reverse reconciliation. The second term in Eq. (5) is

$$I\left(P_{A_1}:P_{E_{A1}},P_{E_{A2}}\right)+I\left(P_{B_3}:P_{E_{B1}},P_{E_{B2}}\right) = \frac{1}{2}\log_2\frac{V\left(\hat{P}_{A_1}\right)}{V\left(\hat{P}_{A_1}|P_{E_{A1}},P_{E_{A2}}\right)}+\frac{1}{2}\log_2\frac{V\left(\hat{P}_{B_3}\right)}{V\left(\hat{P}_{B_3}|P_{E_{B1}},P_{E_{B2}}\right)}, \tag{19}$$

which gives the maximal mutual information between Eve's measurement data and Alice's and Bob's measurement data with direct reconciliation.

B. Coherent attack

In the previous subsection, we analyze the security of our protocol under individual entangling cloner attacks. But this is not sufficient to show its unconditional security. In this subsection, we investigate the security of our protocol against a more general attack, which is a coherent attack within each time when Alice, Bob, and Charlie, respectively, send one qumode to David. Note that a general coherent attack can be simplified to the coherent attack in Fig. 4 under the assumption

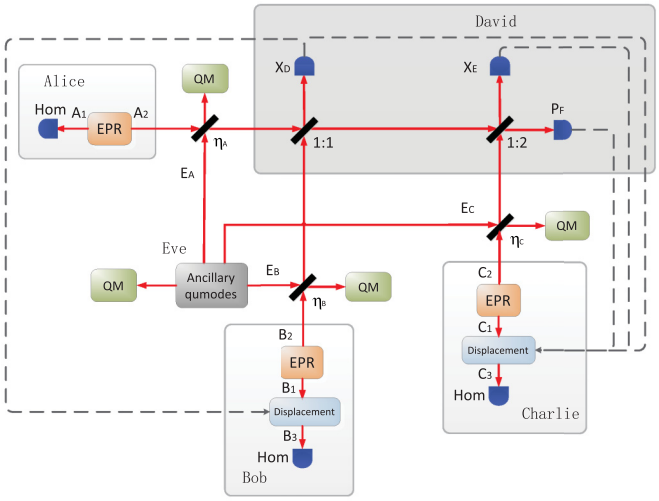

FIG. 4. EB scheme against a coherent attack.

that Alice, Bob, and Charlie's input states are, respectively, permutationally symmetric [23].

Figure 4 shows a coherent attack against our protocol. Eve takes three qumodes out of his ancillary qumodes, which is globally a pure Gaussian state, and injects them into three channels through beam splitters, respectively. The output states coming out of the beam splitters and the remaining ancillary qumodes are all stored in Eve's quantum memory. After monitoring all the data in public channels, Eve implements an optimal measurement on these qumodes in the quantum memory to obtain maximal information.

We use the Holevo bound to quantify the amount of information Eve can obtain. The secret key rate in the QCC protocol becomes

$$\begin{aligned} K_{\mathrm{AB}}^{\mathrm{RR}} &= \beta I\left(X_{A_1} : X_{B_3}\right) - H\left(\rho_{\mathrm{Eve}} : X_{A_1}\right), \text{ and} \\ K_{\mathrm{AC}}^{\mathrm{RR}} &= \beta I\left(X_{A_1} : X_{C_3}\right) - H\left(\rho_{\mathrm{Eve}} : X_{A_1}\right), \end{aligned} \tag{20}$$

where $I(X_{A_1} : X_{B_3(C_3)})$ has been given in Eq. (15), and $H(\rho_{\mathrm{Eve}} : X_{A_1}) = S(\rho_{\mathrm{Eve}}) - S(\rho_{\mathrm{Eve}|\mathrm{X}_{A_1}})$ denotes the Holevo information between Eve's quantum state and Alice's measurement data X_{A_1}. Here we use $S(\rho)$ to denote the von Neumann entropy of the quantum state ρ. Since Eve can purify the whole state $\rho_{A_1,B_3,C_3,\mathrm{Eve}}$, we have

$$H(\rho_{\mathrm{Eve}} : X_{A_1}) = S\left(\rho_{A_1,B_3,C_3}\right) - S\left(\rho_{B_3,C_3|X_{A_1}}\right). \tag{21}$$

For $S(\rho_{A_1,B_3,C_3})$, we can calculate it from a function of the symplectic eigenvalues ν_1, ν_2, and ν_3 of the covariance matrix $\mathbf{V}_{A_1,B_3,C_3}$.

$$S\left(\rho_{A_1,B_3,C_3}\right) = h(\nu_1) + h(\nu_2) + h(\nu_3), \tag{22}$$

where $h(x) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}$. For $S(\rho_{B_3,C_3|X_{A_1}})$, we have

$$S\left(\rho_{B_3,C_3|X_{A_1}}\right) = h(\nu_4) + h(\nu_5), \tag{23}$$

where ν_4 and ν_5 are the symplectic eigenvalues of the covariance matrix $\mathbf{V}_{B_3,C_3|X_{A_1}}$.

The secret key rate for QSS scheme is

$$K_{\mathrm{QSS}}^{\mathrm{RR}} = \beta I\left(P_{A_1}, P_{B_3} : P_{C_3}\right) - H\left(\rho_{\mathrm{Eve}} : P_{C_3}\right), \tag{24}$$

where $I(P_{A_1}, P_{B_3} : P_{C_3})$ has been given in Eq. (17), and

$$\begin{aligned} H\left(\rho_{\mathrm{Eve}} : P_{C_3}\right) &= S(\rho_{\mathrm{Eve}}) - S\left(\rho_{\mathrm{Eve}|\mathrm{P}_{C_3}}\right) \\ &= S\left(\rho_{A_1,B_3,C_3}\right) - S\left(\rho_{A_1,B_3|P_{C_3}}\right). \end{aligned} \tag{25}$$

$S(\rho_{A_1,B_3|P_{C_3}})$ can be calculated from $h(\nu_6) + h(\nu_7)$, where ν_6 and ν_7 are the symplectic eigenvalues of the covariance matrix $\mathbf{V}_{A_1,B_3|P_{C_3}}$.

Both the secret key rates for QCC and QSS are functions of the elements of the covariance matrix $\mathbf{V}_{A_1,B_3,C_3}$ and its reduced covariance matrix under partial homodyne measurement. In the following, we show how to obtain the covariance matrix $\mathbf{V}_{A_1,B_3,C_3}$.

At the beginning, the whole system is the tensor product of Alice's, Bob's, and Charlie's TMSS's and Eve's globally pure Gaussian state. Generally, up to local Gaussian operation, the covariance matrix of Eve's reduced state ρ_{E_A,E_B,E_C} in Fig. 4 can be given by

$$\mathbf{V}_{\mathbf{E_A},\mathbf{E_B},\mathbf{E_C}} = \begin{pmatrix} \mathbf{V_A} & \mathbf{G_1} & \mathbf{G_2} \\ \mathbf{G_1} & \mathbf{V_B} & \mathbf{G_3} \\ \mathbf{G_2} & \mathbf{G_3} & \mathbf{V_C} \end{pmatrix}, \tag{26}$$

where

$$\begin{aligned} &\mathbf{V}_{\mathbf{E_A}} = V_{E_A}\mathbf{I}, \mathbf{V}_{\mathbf{E_B}} = V_{E_B}\mathbf{I}, \mathbf{V}_{\mathbf{E_C}} = V_{E_C}\mathbf{I}, \\ &\mathbf{G_1} = \begin{pmatrix} g_1 & 0 \\ 0 & g_1' \end{pmatrix}, \quad \mathbf{G_2} = \begin{pmatrix} g_2 & 0 \\ 0 & g_2' \end{pmatrix}, \\ &\text{and } \mathbf{G_3} = \begin{pmatrix} g_3 & 0 \\ 0 & g_3' \end{pmatrix}. \end{aligned} \tag{27}$$

V_{E_A}, V_{E_B}, and V_{E_C} are the variances of the thermal noise Eve injects into each channel. g_1, g_2, and g_3 represent the correlations between the noises Eve adds into the three channels. Then the covariance matrix of the whole system can be written as

$$\mathbf{V}_{A,B,C,\mathrm{Eve}} = \bigoplus_{k=1}^{3} \mathbf{V}' \bigoplus \mathbf{V}_{E_A,E_B,E_C}, \tag{28}$$

where

$$\mathbf{V}' = \begin{pmatrix} V\mathbf{I} & \sqrt{V^2-1}\mathbf{Z} \\ \sqrt{V^2-1}\mathbf{Z} & V\mathbf{I} \end{pmatrix}. \tag{29}$$

Permutate the modes in the covariance matrix $\mathbf{V}_{A,B,C,\mathrm{Eve}}$ to make the order of the modes becomes A, E_A, B, E_B, C, E_C. Applying the conjugate unitary operation on the covariance matrix $\mathbf{V}_{A,E_A,B,E_B,C,E_C}$, we obtain the covariance matrix of the whole state including the modes A_1, B_1, C_1 and Eve's modes, that is,

$$\mathbf{U}_{\mathrm{David}}\mathbf{U}_{\mathrm{Eve}}\mathbf{V}_{A,E_A,B,E_B,C,E_C}\mathbf{U}_{\mathrm{Eve}}^{T}\mathbf{U}_{\mathrm{David}}^{T}. \tag{30}$$

Here the matrices $\mathbf{U}_{\mathrm{David}}$ and $\mathbf{U}_{\mathrm{Eve}}$ are different from those given in Eqs. (8)–(11). We must delete the seventh and eighth rows and columns of the matrices $\mathbf{BS}_{A(B,C)}$ in Eq. (9) and $\mathbf{W}_{1(2,3,4)}$ in Eq. (11), to make the dimensions of the matrices $\mathbf{U}_{\mathrm{David}}$ and $\mathbf{U}_{\mathrm{Eve}}$ match $\mathbf{V}_{A,E_A,B,E_B,C,E_C}$. Since we want to obtain the covariance matrix $\mathbf{V}_{A_1,B_3,C_3}$, we delete the rows and the columns corresponding to Eve's modes in the covariance matrix given by Eq. (30). Then we permutate the modes in

the order A_1, B_1, C_1, D, E, F, obtaining the covariance matrix $\mathbf{V}_{A_1,B_1,C_1,D,E,F}$. Using the formula of the reduced covariance matrix following partial homodyne measurement as shown in Eq. (14), we get the covariance matrix $\mathbf{V}_{A_1,B_1,C_1|X_D,X_E,P_F}$. Since displacement operations don't change the covariance matrix, $\mathbf{V}_{A_1,B_1,C_1|X_D,X_E,P_F}$ is the covariance matrix $\mathbf{V}_{A_1,B_3,C_3|X_D,X_E,P_F}$.

IV. SIMULATION RESULTS

In this section, we simulate both QCC and QSS schemes against two kinds of attacks according to the state-of-art technology. The simulation results show that under independent entangling cloner attacks, the maximal transmission distances can be significantly enlarged in the case of unbalanced L_A, L_B, and L_C. But under coherent attacks, the maximal transmission distances are markedly reduced. By comparing different entangled attacks, we finally investigate the optimal coherent attacks in QCC and QSS.

A. Simulation for independent entangling cloner attack

We can replace the transmittance of the beam splitter in Fig. 3, with a realistic transmission distance in experiment by using $\eta_{A(B,C)} = 10^{-\alpha \frac{L_{A(B,C)}}{10}}$, where $L_{A(B,C)}$ is the transmission distance from Alice (Bob, Charlie) to David, and α denotes the coefficient of loss in optical fibers. In the following simulation, we set the coefficient of loss $\alpha = 0.2dB/km$.

Besides the transmission distances, the secret key rate also depends on the variance of Alice's (Bob's, Charlie's) initial TMSS's V, the variance of Eve's TMSS's V_E, and the reconciliation efficiency β. According to the current state-of-art experimental technology, we set $V = 10$ and $\beta = 0.95$ in the following simulation. Since larger V_E indicates higher noise in the channel and lower uncertainty for Eve's estimation, we set $V_E = 1$ for the pure loss case, $V_E = 2$ for the weak entangling cloner attack, and $V_E = 5$ for the strong entangling cloner attack in our simulation.

In QCC, we assume that the transmission distances from Bob and Charlie to David are equal, i.e., $L_B = L_C$, while the transmission distance from Alice to David, L_A, is different from L_B and L_C. With reverse reconciliation, when Alice is close to David, the transmittance $\eta_A = 10^{-0.2\frac{L_A}{10}}$ approaches 1, so that little information can be obtained by Eve from Alice's measurement data. So the secure transmission distance from Bob and Charlie to David can be significantly increased. Figure 5 shows the maximal transmission distances of L_A and $L_{B(C)}$ satisfying $K^{\mathrm{RR}}_{\mathrm{AB(AC)}} > 10^{-3}$. With direct reconciliation, the situation is opposite. To attain a high secret key rate, Bob and Charlie must be close to David, while Alice can be far away from David.

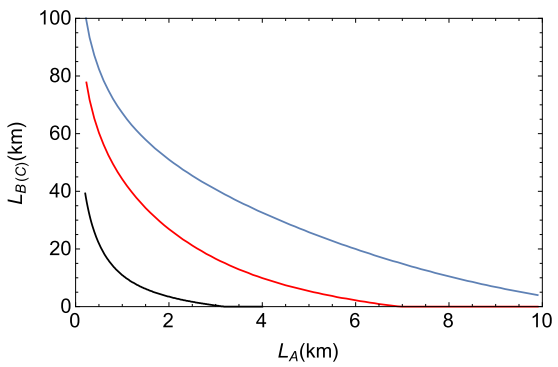

FIG. 5. The maximal transmission distances satisfying the condition $K^{\mathrm{RR}}_{\mathrm{AB(AC)}} > 10^{-3}$. The blue curve is for the case $V_E = 1$; the red curve is for the case $V_E = 2$; the black is for the case $V_E = 5$.

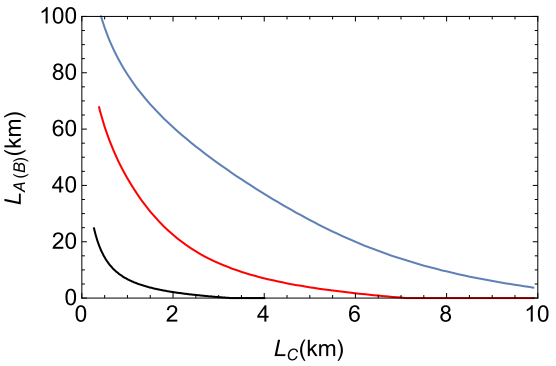

FIG. 6. The maximal transmission distances satisfying the condition $K^{\mathrm{RR}}_{\mathrm{QSS}} > 10^{-3}$. The blue curve is for the case $V_E = 1$; the red curve is for the case $V_E = 2$; the black is for the case $V_E = 5$.

In QSS, we consider the case that $L_A = L_B$, but L_C is different from L_A and L_B. With reverse reconciliation, when L_C approaches zero, the transmittance $\eta_C = 10^{-0.2\frac{L_C}{10}}$ gets close to 1, so that Eve can obtain little amount of information from Charlie's measurement data. Hence, both the secure transmission distances L_A and L_B are greatly enlarged as shown in Fig. 6. With direct reconciliation, to keep the secret key rate high, Alice can be far from David, but both Alice and Bob must be close to David.

The simulation results in both Figs. 5 and 6 show that imbalanced transmission distances of the three channels lead to further total maximal transmission distances when Eve implements the entangling cloner attack.

B. Simulation for coherent attack

To guarantee the matrix $\mathbf{V}_{\mathbf{E_A},\mathbf{E_B},\mathbf{E_C}}$ in Eq. (26) a valid covariance matrix, for any thermal noise $V_{E_A}, V_{E_B}, V_{E_C} \geqslant 1$, g_1, g_2, and g_3 must satisfy the *bona fide* condition [24], that is, $\nu_-^2 \geqslant 1$, where ν_- is the smallest symplectic eigenvalue of the matrix $\mathbf{V}_{\mathbf{E_A},\mathbf{E_B},\mathbf{E_C}}$. The symplectic eigenvalue spectrum of the matrix $\mathbf{V}_{\mathbf{E_A},\mathbf{E_B},\mathbf{E_C}}$ equals to the eigenvalue spectrum of the matrix $|i\Omega\mathbf{V}_{\mathbf{E_A},\mathbf{E_B},\mathbf{E_C}}|$, where

$$\Omega = \bigoplus_{k=1}^{3} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{31}$$

The secret key rates depend on the transmission distances, the variance of Alice (Bob, Charlie)'s TMSS's V, the thermal noise Eve injects in each channel, denoted by V_{E_A}, V_{E_B}, and V_{E_C}, the correlations between the noises in the three channels, represented by g_1, g_2, and g_3, and the reconciliation efficiency β. Here we set $V = 10$ and $\beta = 0.95$, same as above.

To minimize the secret key rate in Eq. (1), Eve only needs to concentrate on attacking the communication either between

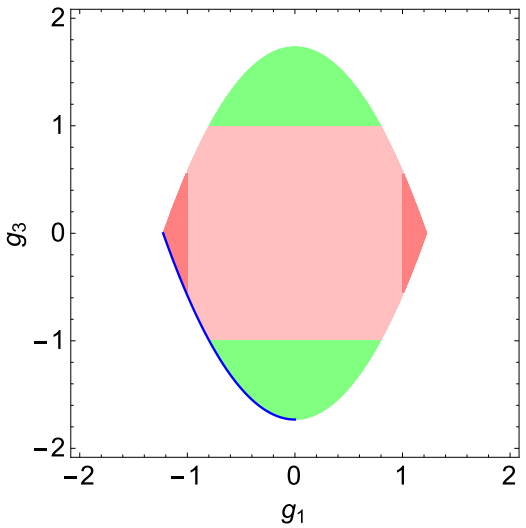

FIG. 7. The accessible values of g_1 and g_3 satisfying the *bona fide* condition when $V_{E_A} = V_{E_B} = V_{E_C} = 2$. The red region shows the values of g_1 and g_3, with which ρ_{E_A} is bipartitely entangled with ρ_{E_B} and ρ_{E_C}, respectively. The green region shows the values of g_1 and g_3, with which ρ_{E_B} and ρ_{E_C} are entangled.

Alice and Bob, or between Alice and Charlie using the optimal "negative EPR attack," which has been defined in Refs. [3,25].

Another case, which has not been investigated before, is that Eve intends to reduce the secret key rates K_{AB} and K_{AC} simultaneously, such that Alice can securely communicate neither with Bob, nor with Charlie. To do this, one way for Eve is to apply the symmetric attack in Bob's and Charlie's channels, which means that interchanging ρ_{E_B} and ρ_{E_C} leaves Eve's attack invariant, i.e., $V_{E_B} = V_{E_C}$ and $g_1 = g_2$. We keep $V_{E_B} = V_{E_C}$ and $g_1 = g_2$ in the following simulation for QCC.

We find that the *bona fide* condition in this symmetric case becomes

$$4g_1^2 + g_3^2 - V_{E_A}^2 - V_{E_C}^2 + \sqrt{8g_1^2\left[g_3^2 - \left(V_{E_A} - V_{E_C}\right)^2\right] + \left(g_3^2 + V_{E_A}^2 - V_{E_C}^2\right)^2} \leqslant -2. \tag{32}$$

A numerical example of the accessible values of g_1 and g_3 satisfying the *bona fide* condition is shown by the colored region in Fig. 7. We divide this colored region into three subregions by checking the separability of each two modes in their reduced states using the positive partial transpose (PPT) criterion [26]. In the red region, ρ_{E_A} is entangled with ρ_{E_B} and ρ_{E_C}, respectively. In the green region, ρ_{E_B} and ρ_{E_C} are entangled. In the pink region, ρ_{E_A},ρ_{E_B}, and ρ_{E_C} are pairwise separable.

In the left red region, the fluctuations of $\hat{X}_{E_A} - \hat{X}_{E_B}$ and $\hat{X}_{E_A} - \hat{X}_{E_C}$ are amplified. Injecting this kind of noise results in the increase of the fluctuations of $\hat{X}_{A_1} - \hat{X}_{B_3}$ and $\hat{X}_{A_1} - \hat{X}_{C_3}$. In the bottom green region, the fluctuation of $\hat{X}_{E_B} - \hat{X}_{E_C}$ is amplified. Injecting this kind of noise makes the fluctuation of $\hat{X}_{B_3} - \hat{X}_{C_3}$ increase. For both cases, the secret key rate is declined. Referring to the discussion in Ref. [3,25], the entanglement corresponding to the left red region and the bottom green region is "bad" entanglement. Whereas, the

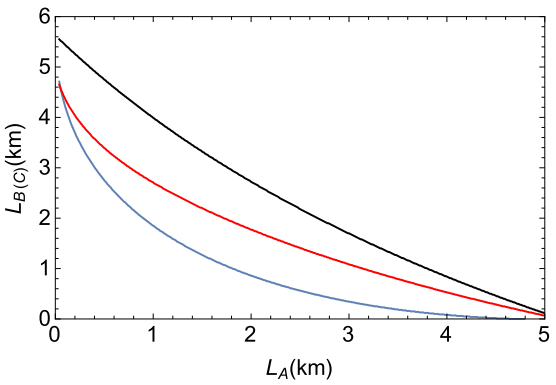

FIG. 8. The maximal transmission distances satisfying $K^{\mathrm{RR}}_{\mathrm{AB(AC)}} > 0$ when $V_{E_A} = V_{E_B} = V_{E_C} = 2$. The blue curve is the attack with minimal g_1 and vanishing g_3. The red curve is the attack with minimal g_3 and vanishing g_1. The black curve is the attack with $g_1 = g_3 = 0$.

entanglement corresponding to the right red region and the top green region helps increasing the key rate, which we call "good" entanglement. To minimize the secret key rate, Eve needs to maximize the "bad" correlation between the noises in each channel. Thus, the optimal attack must lie in the blue contour curve in Fig. 7.

We first compare two maximally entangled attacks with the independent attack. The first entangled attack corresponds to the left-most point in the red region, where $g_1(g_2)$ is minimized and $g_3 = 0$. The second entangled attack corresponds to the down-most point in the green region, where g_3 is minimized and $g_1 = 0$. The independent attack corresponds to the origin given by $g_1 = g_3 = 0$. The simulation results of these three attacks are given in Fig. 8. It indicates that entangled attacks perform better than the independent attack and the attack with minimal g_1 and zero g_3 is stronger than the other two attacks.

But the attack with minimal g_1 and zero g_3 is not a general optimal attack. For instance, in the case shown by Fig. 9, when L_A is short, the attack corresponding to the dashed green curve performs better than the attack with minimal g_1 and vanishing

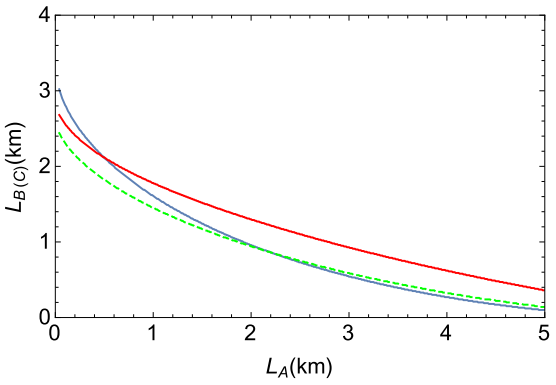

FIG. 9. The maximal transmission distances satisfying $K^{\mathrm{RR}}_{\mathrm{AB(AC)}} > 0$ when $V_{E_A} = 1.5$ and $V_{E_B} = V_{E_C} = 3$. The blue curve is the attack with g_1 minimized and g_3 vanishing; the red curve is the attack with g_1 vanishing and g_3 minimized; the dashed green curve is the attack, where g_1 equals 2/3 times of its minimal value and g_3 saturates the *bona fide* condition in Eq. (32).

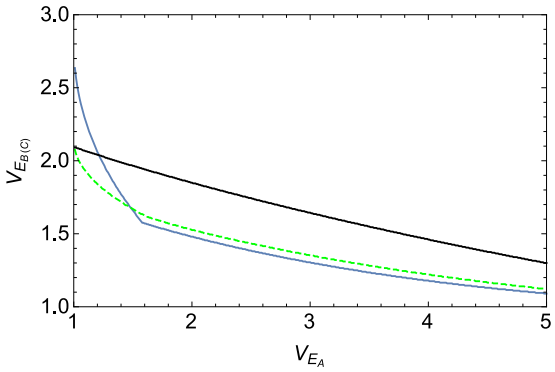

FIG. 10. The maximal tolerable thermal noises satisfying $K^{\mathrm{RR}}_{\mathrm{AB(AC)}} > 0$ when $L_A = 1\,km$ and $L_B = L_C = 3\,km$. The blue curve is the attack with g_1 minimized and g_3 vanishing; the black curve is the attack with g_1 vanishing and g_3 minimized; the dashed green curve is the attack, where g_1 equals half of its minimal value and g_3 saturates the *bona fide* condition in Eq. (32).

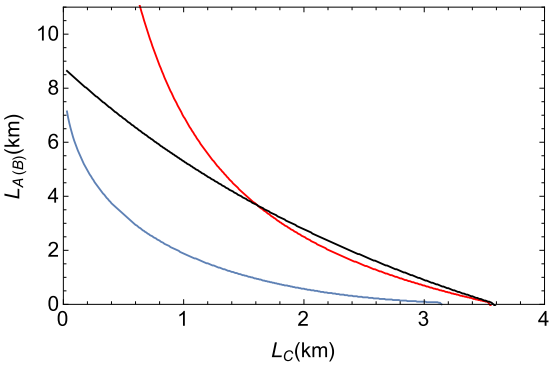

FIG. 12. The maximal transmission distances satisfying $K^{\mathrm{RR}}_{\mathrm{QSS}} > 0$ when $V_{E_A} = V_{E_B} = 2$ and $V_{E_C} = 3$. The blue curve is the attack with minimal $g_2(g_3)$ and vanishing g_1; the red curve is the attack with vanishing $g_2(g_3)$ and minimal g_1; the black curve represents independent attack with $g_1 = g_2 = g_3 = 0$.

g_3, shown by the blue curve. We cannot give a universal optimal attack strategy of g_1 and g_3 for all the cases. The values of g_1 and g_3 to achieve optimal attack depend on the transmission distance of each channel and the thermal noise in each channel.

In Figs. 8 and 9, we fix the thermal noise in each channel to see the maximal transmission distances. Now we fix the transmission distances to look at the maximal tolerable thermal noise in each channel. Figure 10 gives the simulation when $L_A = 1\,km$ and $L_B = L_C = 3\,km$. The simulation result indicates that the maximal tolerable V_{E_A} and $V_{E_{B(C)}}$ is markedly asymmetric.

For QSS, we consider the symmetric case where the transmission distances of Alice's and Bob's channels are equal, $L_A = L_B$, and that the attacks in Alice's and Bob's channels are the same, $V_{E_A} = V_{E_B}$ and $g_2 = g_3$. It implies that after Charlie distributes the secret to Alice and Bob, both of them can obtain the same amount of information about the secret. We keep $V_{E_A} = V_{E_B}$ and $g_2 = g_3$ in the following simulation for QSS.

A numerical example of the accessible values of g_1 and g_3 is shown in Fig. 11. By using the PPT criterion, we divide the colored region further into two subregions. ρ_{E_C} and ρ_{E_A,E_B} are separable in the blue region and entangled in the red region. For the entangled states in the left red region, the fluctuations of $\hat{P}_{E_A} + \hat{P}_{E_C}$ and $\hat{P}_{E_B} + \hat{P}_{E_C}$ are simultaneously amplified, which makes the fluctuation of $\hat{P}_{A_1} + \hat{P}_{B_3} + \hat{P}_{C_3}$ increase. So it is "bad" entanglement, helping Eve to decrease the secret key rate. Whereas the entanglement in the right red region is "good" entanglement, helping to increase the secret key rate. For any V_{E_C} and V_{E_A}, the optimal attack corresponds to the attack with minimal g_3 and vanishing g_1. In the optimal attack, ρ_{E_C} and ρ_{E_A,E_B} are maximally entangled.

We compare the optimal attack with the other two attacks. One is the independent attack given by $g_1 = g_3 = 0$. The other attack is the attack with minimal g_1 and vanishing g_3, in which, ρ_{E_A} and ρ_{E_B} form an EPR pair and ρ_{E_C} is independent. Figure 12 shows the maximal transmission distances of $L_{A(B)}$ and L_C under these three attacks when $V_{E_A} = V_{E_B} = 2$ and $V_{E_C} = 3$. It's easy to see that the attack with minimal g_3 performs better than the other two attacks.

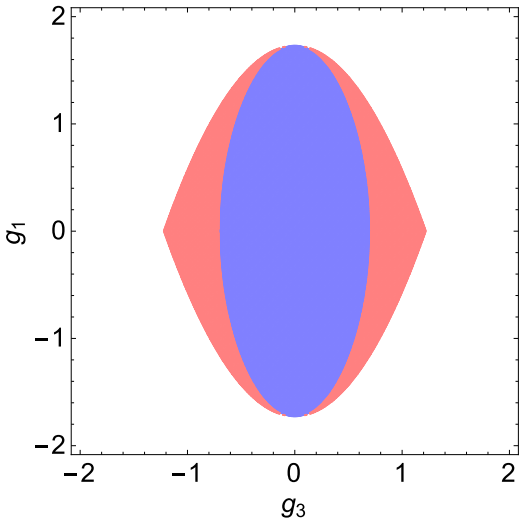

FIG. 11. The accessible values of g_1 and $g_2(g_3)$ satisfying the *bona fide* condition when $V_{E_A} = V_{E_B} = V_{E_C} = 2$. The red region shows the values of g_1 and $g_2(g_3)$, with which ρ_{E_C} is entangled with ρ_{E_A,E_B}. The blue region shows the values of g_1 and $g_2(g_3)$, with which ρ_{E_C} and ρ_{E_A,E_B} are separable.

V. CONCLUSION

This paper investigates CV MDI multipartite quantum communication, where detector side attacks are removed from the side of each party participating in the quantum communication. Our protocol can implement both QCC and QSS. The security against the entangling cloner attack and the coherent attack is analyzed, respectively. Under the entangling cloner attack, the maximal transmission distances can be significantly enlarged in the case of unbalanced distribution. Compared with the entangling cloner attack, the coherent attack reduces the maximally transmission distances markedly. Finally, we study the optimal coherent attacks in QCC and QSS, respectively.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (Grants No. 61475099, No. 61102053, No. 61379153, and No. 61378012), Program of State Key Laboratory of Quantum Optics and Quantum Optics Devices (Grant No. KF201405), and Open Fund of IPOC (BUPT) (Grant No. IPOC2015B004).

[1] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[2] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).
[3] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photonics **9**, 397 (2015).
[4] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[5] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Phys. Rev. Lett. **114**, 090501 (2015).
[6] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[7] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nat. Commun. **3**, 1083 (2012).
[8] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs, Phys. Rev. Lett. **113**, 060502 (2014).
[9] S. Bose, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 822 (1998).
[10] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[11] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Springer, New York, 1989), pp. 69–72.
[12] P. van Loock and A. Furusawa, Phys. Rev. A **67**, 052315 (2003).
[13] J. Jing, J. Zhang, Y. Yan, F. Zhao, C. Xie, and K. Peng, Phys. Rev. Lett. **90**, 167903 (2003).
[14] T. Aoki, N. Takei, H. Yonezawa, K. Wakui, T. Hiraoka, A. Furusawa, and P. van Loock, Phys. Rev. Lett. **91**, 080404 (2003).
[15] J. Zhang and S. L. Braunstein, Phys. Rev. A **73**, 032318 (2006).
[16] P. van Loock and S. L. Braunstein, Phys. Rev. A **61**, 010302 (1999).
[17] R. E. S. Polkinghorne and T. C. Ralph, Phys. Rev. Lett. **83**, 2095 (1999).
[18] A. Heidmann, R. J. Horowicz, S. Reynaud, E. Giacobino, C. Fabre, and G. Camy, Phys. Rev. Lett. **59**, 2555 (1987).
[19] C. E. Shannon, Bell Labs Tech. J. **28**, 656 (1949).
[20] R. García-Patrón, Ph.D thesis, Université Libre de Bruxelles, 2007.
[21] J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002).
[22] G. Spedalieri, C. Ottaviani, and S. Pirandola, Open Syst. Inf. Dyn. **20**, 1350011 (2013).
[23] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[24] G. Adesso and F. Illuminati, J. Phys. A: Math. Theor. **40**, 7821 (2007).
[25] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Phys. Rev. A **91**, 022320 (2015).
[26] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).