SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

July 2019, Vol. 62 072501:1–072501:14
https://doi.org/10.1007/s11432-018-9705-x

Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state

Yu WANG[1*], Caixing TIAN[2,3], Qi SU[1], Meihong WANG[2,3] & Xiaolong SU[2,3*]

[1] *State Key Laboratory of Cryptology, Beijing 100878, China;*
[2] *State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China;*
[3] *Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China*

Received 3 September 2018/Revised 5 November 2018/Accepted 21 November 2018/Published online 7 May 2019

Abstract Cluster state is the basic resource for one-way quantum computation and a valuable resource for establishing quantum network, because it has a flexible and varied composition form. We present measurement-device-independent quantum secret sharing (QSS) and quantum conference (QC) schemes based on continuous variable (CV) four-mode cluster state with different structures. The users of the protocol prepare their own Einstein-Podolsky-Rosen (EPR) states, respectively. One mode of these EPR states is sent to an untrusted relay where a generalized Bell measurement creates different types of CV cluster states among four users, while the other mode is kept at their own station. We show that a shared secret key for QSS and QC schemes is distilled based on the shared quantum correlation among four users. QC and four users QSS are implemented based on the star shape CV cluster state. QSS with three users are implemented based on the linear or square shape CV cluster states. The results show that the secure transmission distance for an asymmetric network, where the transmission distances between the users and relay are different, is longer than that of a symmetric network, where the transmission distances between the users and relay are the same. The presented schemes provide concrete references for establishing quantum network with the CV cluster state.

Keywords measurement-device-independent, cluster state, quantum network, continuous variable, quantum secret sharing

Citation Wang Y, Tian C X, Su Q, et al. Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state. Sci China Inf Sci, 2019, 62(7): 072501, https://doi.org/10.1007/s11432-018-9705-x

1 Introduction

Quantum key distribution (QKD) is one of the quantum technologies that are closest to practical applications, and it has been applied in several areas [1–6]. In the practical application, the imperfection of the QKD system will cause security issues [7]. Device-independent QKD protocol provides a solution to side-channel attacks [8–10], but the security of it relies on the violation of a Bell inequality [11]. A more practical solution is measurement-device-independent (MDI) QKD protocol [12–14], which can not only resist all attacks against the measuring terminal, but also reduce the detector requirements to the current level of technical conditions which can be achieved [15–18]. As for the implementation of QKD, besides QKD system based on discrete variable, continuous variable (CV) QKD system, which uses light

[*] Corresponding author (email: wangy@sklc.org, suxl@sxu.edu.cn)

modes and homodyne detections instead of single-photon quantum states and single-photon detection to complete the key distribution process, may achieve high rates [19]. CV-MDI QKD protocol using coherent states [20] and squeezed states [21] was proposed theoretically [22], and implemented experimentally between two parties [23].

With the gradual maturation of QKD devices and technologies in recent years, the QKD network has attracted more attention. Increasing number of quantum communication network users make it necessary to study multiuser quantum communication protocol, such as quantum secret sharing (QSS) [24–27] and quantum conference (QC) [28] protocols. In the QSS protocol, a dealer can distribute an arbitrary secret key among n participants so that only authorized subset of participants can reconstruct the secret. In order to implement the QC protocol, all legitimate participants need to share a set of identical keys that are used to implement encrypted communication between group members. Members outside the group cannot decrypt the communication content of the members within the group.

CV multipartite entangled states, which are mainly composed of Greenberger-Horne-Zeilinger (GHZ) state [29] and cluster state [30] according to the different entangled manners among submodes, are basic resources in quantum information. Cluster state is a basic quantum resource for one-way quantum computation [31]. CV cluster states [30, 32–34], which can be generated deterministically, have been successfully produced for eight-qumode [35], 60-qumode [36] and even up to 10000-qumode [37]. Based on a prepared large scale cluster state, one-way quantum computation can be implemented by measurement and feedforward of the measurement results [38–46]. Besides the application in one-way quantum computation, cluster state can also be used to establish quantum network [47, 48], which has complex structure.

CV MDI multipartite QC and QSS protocols have been designed by using tripartite GHZ state [49]. Recently, a CV MDI star network for QC is also proposed [50] based on GHZ state. Compared to the GHZ state, a cluster state has a variety of structures, and it is more suitable to be used in the network with complex structures. After selecting the appropriate cluster state, the QSS protocol can be implemented in any group with more than three users of all legitimate participants.

In this paper, we propose MDI QSS and QC networks based on four-mode CV cluster states with different structures. Four trusted users send one mode of their Einstein-Podolsky-Rosen (EPR) states, which are prepared by their own respectively, to a middle untrusted relay by quantum channels. After receiving all quantum states from each user, a generalized multipartite Bell detection is performed in the untrusted relay which can even be controlled by Eve. Comparing with the schemes that use pairwise entanglement, what we proposed in this paper is an MDI scheme in which the attacks on measurement devices are moved from the legitimate members' sides to the untrusted party's side. These suitable measurements that project onto a displaced version of the remaining quantum states at the user's station create CV cluster states at last. With different feedforward of measurement results one can create different types of CV cluster states.

QSS with four users and three users can be implemented based on the star shape four-mode CV cluster state and the linear cluster-like quantum correlations, respectively. QC with four users is implemented based on the star shape four-mode CV cluster state. Secret key rates of a symmetric and an asymmetric quantum network structures are compared. The results show that the transmission distance for an asymmetric quantum network is longer than that of a symmetric one. The presented scheme can be easily extended to more complex network structures by using the large scale CV cluster state.

The paper is organized as follows. We present the basic principle of protocols of four-partite CV MDI quantum communication in Section 2. The security analysis and simulation results are discussed in Sections 3 and 4. Finally, the discussion and conclusion are presented in Section 5.

2 MDI quantum network with four-mode Gaussian cluster state

Cluster state is a type of multipartite quantum entangled graph states corresponding to some mathematical graphs [30, 32, 40, 41]. The CV cluster quadrature correlations (so-called nullifiers) can be expressed

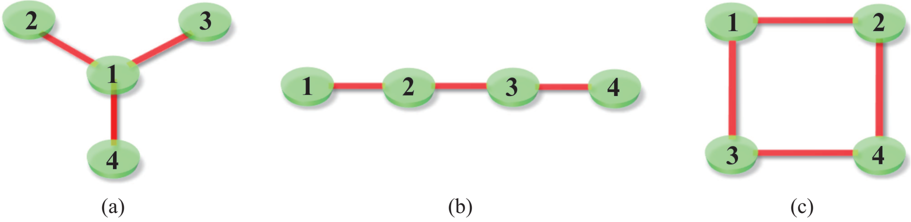

Figure 1 (Color online) The four-partite cluster states. Each cluster node, corresponding to an optical mode, is represented by a circle. Neighboring nodes are connected by lines. (a), (b) and (c) represent star, linear and square shape cluster state, respectively.

by [32, 41].

$$\left(\hat{p}_a - \sum_{b\in N_a} c_{ab}\hat{x}_b\right) \to 0, \qquad \forall a \in G, \tag{1}$$

where $\hat{x}_a = (\hat{a} + \hat{a}^\dagger)/2$ and $\hat{p}_a = (\hat{a} - \hat{a}^\dagger)/2i$ represent the quadrature-amplitude and quadrature-phase operators of an optical mode $\hat{a}$, respectively. The subscript $a(b)$ expresses the designated mode $\hat{a}$ $(\hat{b})$. The modes of $a \in G$ denote the vertices of the graph G, while the modes of $b \in N_a$ are the nearest neighbors of mode $\hat{a}$. The factor c_{ab} corresponds to the strength that the modes $\hat{a}$ and $\hat{b}$ have interacted [51]. For an ideal cluster state, the left-hand side of (1) tends to zero, which represents a simultaneous zero eigenstate of the quadrature combination [41]. The CV cluster quantum entanglements generated by experiments are deterministic, but imperfect, the entanglement features of which have to be verified and quantified by the sufficient conditions for the fully inseparability of multipartite CV entanglement [52, 53].

According to the generation method proposed in [32], CV cluster state can be prepared by coupling squeezed states on a beam-splitter network. There are three kinds of four-mode CV cluster states, including star, linear, and square shape cluster states, respectively, as shown in Figure 1. Among these three kinds of cluster states, the linear cluster state can be obtained from the square cluster state via appropriate local Fourier transforms [53], so the square cluster state can also be used to implement the QSS with three users as the linear cluster state. Furthermore, four-mode star shape cluster state can be obtained from those of the four-mode GHZ state with a local phase shift on the mode 1, so the two states are equivalent. In this paper, two types of QSS and QC schemes are proposed using the four-mode CV cluster states with different structures.

A quantum network includes four honest legitimate users (Alice, Bob, Charlie and David) and an untrusted relay, which may be even controlled by Eve, is shown in Figure 2. If the legal users in the network need to implement the MDI QSS or QC, they should follow the steps below. Step 1, four EPR states are prepared independently by the legal users, respectively. One mode $\hat{a}_i, i \in \{1-4\})$ of the EPR states is transmitted to the untrusted relay. Step 2, Bell measurement is performed in the relay after four optical beams are interfered on a beam-splitter network with the prescribed rules in Figure 2 and the homodyning measurement results $(\gamma = \{x_{c_1}, p_{c_2}, x_{c_3}, x_{c_4}\})$ are published. Step 3, according to the measurement results, Alice, Bob, Charlie and David will perform suitable displacement on the remained EPR beams $\hat{b}_i$ $(i \in \{1-4\})$ in their station, respectively. In this way, a four-mode cluster state $(\hat{b}_1' - \hat{b}_4')$ is shared among four users in the network. Based on the quantum correlations of the shared cluster state, secret key of MDI QSS and QC schemes can be achieved. The same secret can be achieved among the four users by QC and the secret key can be shared among four legitimate users or any three users by QSS.

2.1 QC and QSS with the star shape cluster state

It has been shown that the quantum correlations among amplitude or phase quadratures of optical modes can be used to implement QKD [54, 55], tripartite QC and QSS [49]. Based on this method, we design MDI QC and QSS schemes with the shared quantum correlations among amplitude or phase quadratures of optical modes. At the station of untrusted relay in Figure 2, after optical beams $\hat{a}_i, i \in \{1-4\}$

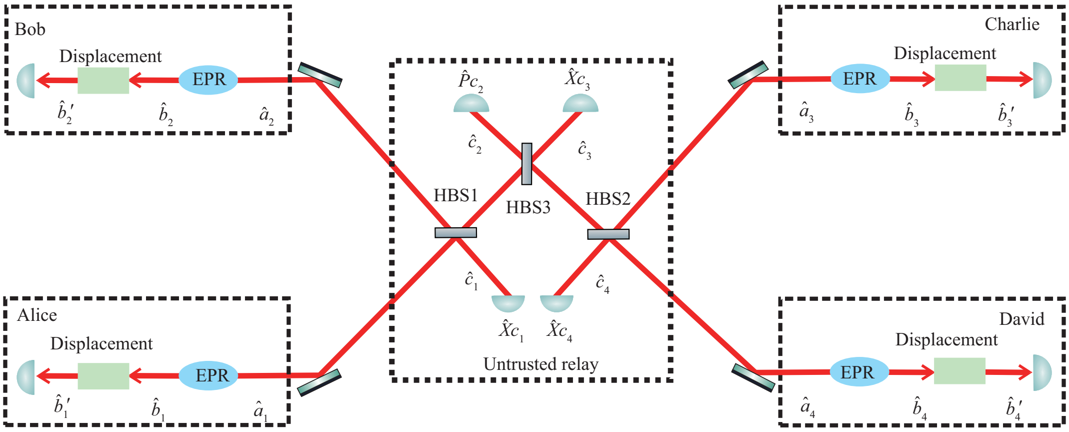

Figure 2 (Color online) Basic protocol for MDI quantum network with a four-mode cluster state. Alice, Bob, Charlie and David prepare an EPR state, respectively. They hold one mode ($\hat{b}_i, i \in \{1-4\}$) of the EPR state in their own station and send the other mode ($\hat{a}_i, i \in \{1-4\}$) to an untrusted relay. After receiving the modes from Alice, Bob, Charlie and David, the Bell measurement is performed in the relay. Displacement operations are performed on the modes ($\hat{b}_i, i \in \{1-4\}$) after the users obtain the measurements results from the relay. HBS, half beam splitter.

passing through a beam-splitter network consists of three half beam splitters (HBS), the output modes $\hat{c}_i, i \in \{1-4\}$ can be expressed as

$$\begin{aligned}
\hat{c}_1 &= \frac{1}{\sqrt{2}}\hat{a}_1 + \frac{1}{\sqrt{2}}\hat{a}_2,\\
\hat{c}_2 &= -\frac{1}{2}\hat{a}_1 + \frac{1}{2}\hat{a}_2 + \frac{1}{2}\hat{a}_3 + \frac{1}{2}\hat{a}_4,\\
\hat{c}_3 &= \frac{1}{2}\hat{a}_1 - \frac{1}{2}\hat{a}_2 + \frac{1}{2}\hat{a}_3 + \frac{1}{2}\hat{a}_4,\\
\hat{c}_4 &= -\frac{1}{\sqrt{2}}\hat{a}_3 + \frac{1}{\sqrt{2}}\hat{a}_4.
\end{aligned} \tag{2}$$

The amplitude quadratures of $\hat{c}_1$, $\hat{c}_3$ and $\hat{c}_4$ and the phase quadrature of $\hat{c}_2$, are measured by homodyne detection system, respectively. Afterwards these measurement results γ are published in classical channel. Based on these published measurement results, four users in the quantum network perform displacement operations on their own optical beams $\hat{b}_i, i \in \{1-4\}$, respectively.

For achieving QC, Bob, Charlie and David displace the amplitude quadratures $\hat{x}_{b_i}$ with $\Delta\hat{x}_{b_i}$, $i \in \{2,3,4\}$, respectively, while Alice keeps the $\hat{x}_{b_1}$ unchanged, so we have

$$\begin{aligned}
\hat{x}_{b_1'} &= \hat{x}_{a_1},\\
\hat{x}_{b_2'} &= \hat{x}_{b_2} + \Delta\hat{x}_{b_2},\\
\hat{x}_{b_3'} &= \hat{x}_{b_3} + \Delta\hat{x}_{b_3},\\
\hat{x}_{b_4'} &= \hat{x}_{b_4} + \Delta\hat{x}_{b_4},
\end{aligned} \tag{3}$$

where

$$\begin{aligned}
\Delta\hat{x}_{b_2} &= -\sqrt{2}\hat{x}_{c_1},\\
\Delta\hat{x}_{b_3} &= -\frac{1}{\sqrt{2}}\hat{x}_{c_1} - \hat{x}_{c_3} + \frac{1}{\sqrt{2}}\hat{x}_{c_4},\\
\Delta\hat{x}_{b_4} &= -\frac{1}{\sqrt{2}}\hat{x}_{c_1} - \hat{x}_{c_3} - \frac{1}{\sqrt{2}}\hat{x}_{c_4}.
\end{aligned} \tag{4}$$

By substituting (2) into (3), and basing on the quantum correlations of the EPR states among the legal users (Alice, Bob, Charlie and David) $\hat{x}_{a_i} - \hat{x}_{b_i} \to 0$, $\hat{p}_{a_i} + \hat{p}_{b_i} \to 0$, where $i \in \{1-4\}$, we obtain the expression of output modes $\hat{b}_1' - \hat{b}_4'$ after the displacement operations, which are

$$\hat{x}_{b_1'} = \hat{x}_{a_1},$$

$$\begin{aligned}\hat{x}_{b'_2} &= -\hat{x}_{a_1},\\ \hat{x}_{b'_3} &= -\hat{x}_{a_1},\\ \hat{x}_{b'_4} &= -\hat{x}_{a_1},\end{aligned} \tag{5}$$

in the ideal case with infinite squeezing.

The QSS with four users can also be achieved in Figure 2. After receiving the measurement results γ, Alice displaces the phase quadrature $\hat{p}_{b_1}$ of her optical mode with $\Delta\hat{p}_{b_1} = -2\hat{p}_{c_2}$, while Bob, Charlie and David keep their phase quadratures $\hat{p}_{b_i}$ $(i \in \{2,3,4\})$ unchanged, respectively. Using the quantum correlations for the EPR states $\hat{p}_{a_i} + \hat{p}_{b_i} \to 0$, the phase quadratures of Alice, Bob, Charlie and David's modes after the displacement operation can be expressed as

$$\begin{aligned}\hat{p}_{b'_1} &= \hat{p}_{b_1} + \Delta\hat{p}_{b_1} = -\hat{p}_{a_2} - \hat{p}_{a_3} - \hat{p}_{a_4},\\ \hat{p}_{b'_2} &= -\hat{p}_{a_2},\\ \hat{p}_{b'_3} &= -\hat{p}_{a_3},\\ \hat{p}_{b'_4} &= -\hat{p}_{a_4}.\end{aligned} \tag{6}$$

When the phase quadratures of modes $\hat{b}'_i$ are homodyned by the users, respectively, the resulting data satisfy $-\hat{p}_{b'_1} + \hat{p}_{b'_2} + \hat{p}_{b'_3} + \hat{p}_{b'_4} = 0$ in the ideal case.

By applying an inverse Fourier transform (which corresponds to $-90°$ rotation in phase space) on optical modes $\hat{b}'_2$, $\hat{b}'_3$ and $\hat{b}'_4$, respectively, the modes owned by Alice, Bob, Charlie and David meet the distributed CV four partite star shape cluster state, where the corresponding quantum correlations are given by $\hat{p}_{b'_1} - \hat{x}_{b'_2} - \hat{x}_{b'_3} - \hat{x}_{b'_4} = 0$, $\hat{p}_{b'_i} - \hat{x}_{b'_1} = 0$, where $i \in \{2,3,4\}$.

Based on the quantum correlation between amplitude quadratures of the four-mode star shape cluster state (Eq. (5)), QC protocol can be implemented among four users. In QC, four users measure amplitude quadrature of their remained output modes $(\hat{b}'_i)$, respectively, and use the measurement outcomes to do the reconciliation and post selection. Since $\hat{x}_{b_i} = \hat{x}_{b_1}$, $i \in \{2,3,4\}$, the users can obtain coincident quantum keys.

The QSS with four users can also be achieved based on quantum correlations among phase quadratures of the four-mode star shape cluster state (Eq. (6)). In this case, any three users of Alice, Bob, Charlie and David must share their measurement outcomes and perform parameter estimation, information reconciliation, and privacy amplification through a public channel with the fourth user because of the relationship among the measurement results of phase qusdratures of $\hat{b}'_i$, so the QSS with four users is achieved. For example, Bob, Charlie and David must cooperate at the same time to extract the secret of Alice, any one or two users cannot extract the secret without the help of the rest users. Any smaller groups of the four users cannot reconstruct the secret since the shared key depends on the total quantum correlation in phase quadrature of optical beams among four users.

2.2 QSS with the linear cluster-like quantum correlation

In most cases, let n be a set of identities parties, the distributed secret from dealer should be reconstructed by any t-out-of-n parties, and any collusion of less than t parties should have "almost" no information about the underlying secret, which is called the (t,n) secret sharing scheme [56–58]. The previous discussion of QSS scheme is the case of $t = n$.

For achieving QSS among a small group with authorized users, the scheme proposed in [50] must trace out the useless modes. However, any t-out-of-n QSS protocol can be completed by using designed and suitable cluster state. Here, we propose a 2-out-of-3 QSS scheme based on linear cluster-like quantum correlation or box cluster-like quantum correlation, which cannot be achieved by using the star shape cluster state.

Supposing that the dealer Alice wants to distribute secret to Bob, Charlie and David, respectively. Any two users of Bob, Charlie and David can reconstruct the secret, and any one cannot get any information without the help of the other users.

At first we present the QSS among Alice, Bob and Charlie who own optical mode 1, 2 and 3, respectively, as shown in Figure 1. This MDI-QSS protocol can also be achieved by the scheme in Figure 2. Four users prepare their EPR states, respectively, which are same with the preparing step in QC. After receiving the results γ from the untrusted relay, Alice displaces her amplitude quadrature $\hat{x}_{b_1}$ with $\Delta\hat{x}_{b_1} = -2\hat{x}_{c_3} + \sqrt{2}\hat{x}_{c_4}$, while Bob and Charlie keep their amplitude quadratures $\hat{x}_{b_i}$, where $i \in \{2, 3\}$ unchanged, respectively. Using the conditions of EPR entangled states, the amplitude quadratures of Alice, Bob and Charlie's modes can be expressed as

$$\begin{aligned} \hat{x}_{b_1'} &= \hat{x}_{b_1} + \Delta\hat{x}_{b_1} = \hat{x}_{a_2} - 2\hat{x}_{a_3}, \\ \hat{x}_{b_2'} &= \hat{x}_{a_2}, \\ \hat{x}_{b_3'} &= \hat{x}_{a_3}, \end{aligned} \tag{7}$$

in the ideal case. When homodyning the amplitude quadratures of modes $\hat{b}_i'$, we have the quantum correlation expressed by $\hat{x}_{b_1'} - \hat{x}_{b_2'} + 2\hat{x}_{b_3'} = 0$ in the ideal case with infinite squeezing. Based on this quantum correlation, Bob and Charlie can obtain the secret key distributed by Alice.

For the QSS among any three users in the network, the displacements implemented by users are different. For the QSS among Alice, Bob, and David, Alice displaces her amplitude quadrature $\hat{x}_{b_1}$ with $\Delta\hat{x}_{b_1} = -2\hat{x}_{c_3} - \sqrt{2}\hat{x}_{c_4}$, while Bob and David keep their amplitude quadratures $\hat{x}_{b_i}$, $i \in \{2, 4\}$ unchanged, respectively. The resulting states satisfy $\hat{x}_{b_1'} - \hat{x}_{b_2'} + 2\hat{x}_{b_4'} = 0$. For the QSS among Alice, Charlie, and David, Alice displaces her amplitude quadrature $\hat{x}_{b_1}$ with $\Delta\hat{x}_{b_1} = -\frac{1}{\sqrt{2}}\hat{x}_{c_1} - \hat{x}_{c_3}$, while Charlie and David keep their amplitude quadratures $\hat{x}_{b_i}$, where $i \in \{3, 4\}$ unchanged, respectively. The resulting states satisfy $2\hat{x}_{b_1'} + \hat{x}_{b_3'} + \hat{x}_{b_4'} = 0$. So far, Alice has been able to distribute secrets to any two users among Bob, Charlie and David, and the 2-out-of-3 QSS protocol can be implemented.

Not only that, QSS among Bob, Charlie, and David can also be implemented. Charlie can shift her amplitude quadrature $\hat{x}_{b_3}$ with $\Delta\hat{x}_{b_3} = \sqrt{2}\hat{x}_{c_1} - 2\hat{x}_{c_3}$, while Bob and David keep their amplitude quadratures $\hat{x}_{b_i}$, where $i \in \{2, 4\}$ unchanged, respectively. The resulting states satisfy $2\hat{x}_{b_2'} + \hat{x}_{b_3'} + \hat{x}_{b_4'} = 0$.

In the presented 2-out-of-3 QSS protocols, the inactive fourth user cannot obtain any information of the secret sharing among the legitimate three users, since his optical mode has no quantum correlation with the optical modes hold by the legitimate three users. For example, in QSS among Alice, Bob and Charlie, the inactive user David cannot obtain the share key.

3 Security analysis

In this section, we analyze the most realistic security of QSS and QC against the coherent attack (shown in Figure 3). A joint attack involving both the untrusted relay and the four links is the most general eavesdropping strategy for such a quantum network which is shown in Figure 3. In Eve's station, the four modes ($\hat{a}_i$ where $i \in \{1, 4\}$) sent by users are intercepted and interacted with an ensemble of ancillary vacuum modes via a general unitary. The output modes from Eve's station are sent to the untrusted relay, where they are homodyned and the results are published following the protocols. Eve stores the remaining modes in a quantum memory, which will be measured at the end of the protocol. The joint statistical variables must be retrieved by four users to deal with the joint attack. Four users should compare a small part of their data via the public channel and reconstruct the error probability.

In order to calculate the secret key rate, the covariance matrix should be written firstly. Four independent EPR states are prepared by Alice, Bob, Charlie and David at beginning, respectively. The covariance matrix is

$$V_{\mathrm{A,B,C,D}} = \bigoplus_{i=1}^{4} \boldsymbol{V}_i, \tag{8}$$

where

$$\boldsymbol{V}_i = \begin{pmatrix} V_i I & \sqrt{V_i^2 - 1}\sigma_{\mathrm{Z}} \\ \sqrt{V_i^2 - 1}\sigma_Z & V_i I \end{pmatrix},$$

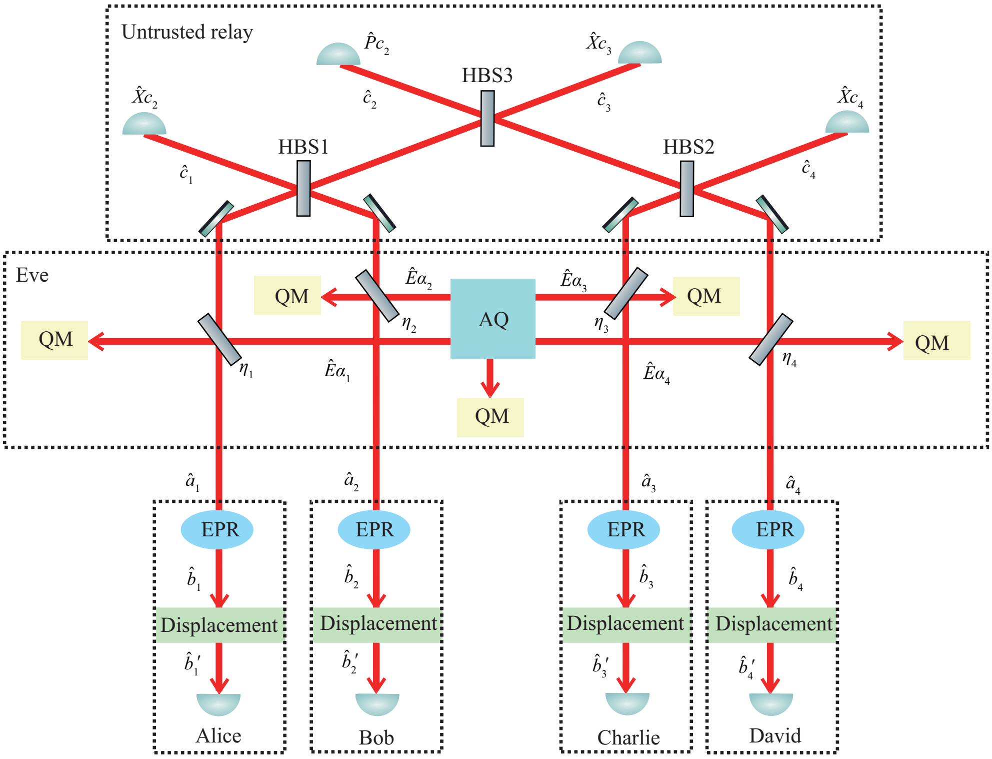

Figure 3 (Color online) Scheme against a coherent attack. Eve chooses four pure Gaussian states ($\hat{E}_{a_i}, i = 1-4$) from his ancillary qumodes (AQ), and injects them into the channel between Alice (Bob, Charlie, David) and the relay by beam splitter whose transmission efficiency is η_i $(i = 1-4)$. One of the output modes is sent to the relay as a fake mode, while the other modes and the remaining AQ are stored in Eve's quantum memory (QM).

where $V_i = \cosh(2r)$ $(i \in \{\mathrm{A,B,C,D}\})$ is the variance of Alice's, Bob's, Charlie's and David's EPR state and r is the squeezing parameter. We choose $V_\mathrm{A} = V_\mathrm{B} = V_\mathrm{C} = V_\mathrm{D} = V$ for simplify. $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is the identity matrix, and the $\sigma_\mathrm{Z} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is the Pauli Z matrix.

Eve produces the state $\rho_{E_\mathrm{A},E_\mathrm{B},E_\mathrm{C},E_\mathrm{D}}$, whose covariance matrix can be expressed as

$$V_{E_\mathrm{A},E_\mathrm{B},E_\mathrm{C},E_\mathrm{D}} = \begin{pmatrix} V_{E_{\mathrm{A}1}}I & g_1 I & g_4 I & g_6 I \\ g_1 I & V_{E_{\mathrm{A}2}}I & g_2 I & g_5 I \\ g_4 I & g_2 I & V_{E_{\mathrm{A}3}}I & g_3 I \\ g_6 I & g_5 I & g_3 I & V_{E_{\mathrm{A}4}}I \end{pmatrix}, \tag{9}$$

where the $V_{E_{\mathrm{A}1}}, V_{E_{\mathrm{A}2}}, V_{E_{\mathrm{A}3}}$ and $V_{E_{\mathrm{A}4}}$ are the variances of the thermal states which are injected into the Alice's, Bob's, Charlie's and David's channels, respectively. $g_1 - g_6$ represents the correlations between different modes, where the amplitude and phase quadratures correlations are supposed to be the same. Then the variance matrix in the initial system can be written as

$$V_{\mathrm{A,B,C,D,Eve}} = V_{\mathrm{A,B,C,D}} \oplus V_{E_\mathrm{A},E_\mathrm{B},E_\mathrm{C},E_\mathrm{D}}. \tag{10}$$

Eve interferes the submode $\hat{E}_{a_i}$ with mode $\hat{a}_i$ $(i = 1-4)$ on the beam splitter (BS) with transmittance η_i $(i = 1-4)$, respectively. The performance of BS can be written as

$$\mathrm{BS}_{\mathrm{Eve}_i} = \begin{pmatrix} \sqrt{\eta_i}I & \sqrt{1-\eta_i}I \\ -\sqrt{1-\eta_i}I & \sqrt{\eta_i}I \end{pmatrix}, \quad i = 1-4. \tag{11}$$

Eve's overall operation of these four beam splitters is given by

$$U_{\mathrm{Eve}} = \bigoplus_{i=1}^{4} \mathrm{BS}_{\mathrm{Eve}_i}. \tag{12}$$

When the submodes are transmitted to the relay, they are interfered on three HBSs, which are shown in Figure 3. The overall operations at the relay are

$$U_{\mathrm{R}} = \mathrm{HBS}_3\mathrm{HBS}_2\mathrm{HBS}_1, \tag{13}$$

where the expression of HBS_i $(i = 1 - 3)$ is given by (11) with $\eta = 1/2$.

Finally, the whole system's covariance matrix before homodyne measurement can be calculated as

$$V_{b_1b_2b_3b_4c_1c_2c_3c_3\mathrm{Eve}} = U_{\mathrm{R}}U_{\mathrm{Eve}}V_{\mathrm{A,B,C,D,Eve}}U_{\mathrm{Eve}}^{\mathrm{T}}U_{\mathrm{R}}^{\mathrm{T}}. \tag{14}$$

The amplitude quadratures of $\hat{c}_1$, $\hat{c}_3$, $\hat{c}_4$ and phase quadrature of $\hat{c}_2$ are measured by homodyne detection system in the relay. We rewrite the matrix in the new form:

$$V_{b_1b_2b_3b_4c_1c_2c_3c_3\mathrm{Eve}} = \begin{pmatrix} V_{b_1b_2b_3b_4\mathrm{Eve}} & C \\ C^{\mathrm{T}} & V_{c_1c_2c_3c_3} \end{pmatrix}. \tag{15}$$

After homodyning $\hat{x}_{c_1}$, $\hat{p}_{c_2}$, $\hat{x}_{c_3}$ and $\hat{x}_{c_4}$, the conditional covariance matrix is

$$V_{b_1b_2b_3b_4\mathrm{Eve}|c_1c_2c_3c_3} = V_{b_1b_2b_3b_4\mathrm{Eve}} - CH_{\mathrm{Hom}}C^{\mathrm{T}}, \tag{16}$$

where $H_{\mathrm{Hom}} = (WV_{c_1c_2c_3c_3}W)^{\mathrm{MP}}$ means one quadrature of mode $\hat{c}_i$ is homodyned. $W = x \bigoplus p \bigoplus x \bigoplus x$, in which $x = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ means the amplitude quadrature is homodyned, $p = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ stands for homodyning the phase quadrature. MP denotes the Moore Penrose inverse of the matrix.

Since the variances and covariances of quadratures remain the same by displacement operations, only mean values are changed, the partial state $\rho_{b_1'b_2'b_3'b_4'}$ owns the same covariance matrix as $\rho_{b_1b_2b_3b_4|c_1c_2c_3c_3}$.

3.1 Secret key rate of QC

When the four users receive the measurement result γ from the untrusted relay, the local mode $\hat{b}_i$ is homodyned by its owner with random outcome β_i. The local mode $\hat{b}_j$ of its owner is mapped into a Gaussian state $\rho_{b_j|b_i\gamma}$ after the measurement. Then the mutual information $I(\beta_i : \beta_j)$ by two users can be calculated. The amount of information Eve can obtain is quantified by the Holevo bound $H(\beta_i : \rho_{\mathrm{Eve}})$.

In this paper, we suppose that Alice shares her secret key with the other users in QC. Thus the secret key rate ($K_{\mathrm{AB}}^{\mathrm{QC}_{\mathrm{RR}}}$, $K_{\mathrm{AC}}^{\mathrm{QC}_{\mathrm{RR}}}$ and $K_{\mathrm{AD}}^{\mathrm{QC}_{\mathrm{RR}}}$) with reverse reconciliation can be defined as

$$\begin{aligned} K_{\mathrm{AB}}^{\mathrm{QC}_{\mathrm{RR}}} &= \beta I(b_1' : b_2') - H(b_1' : \rho_{\mathrm{Eve}}), \\ K_{\mathrm{AC}}^{\mathrm{QC}_{\mathrm{RR}}} &= \beta I(b_1' : b_3') - H(b_1' : \rho_{\mathrm{Eve}}), \\ K_{\mathrm{AD}}^{\mathrm{QC}_{\mathrm{RR}}} &= \beta I(b_1' : b_4') - H(b_1' : \rho_{\mathrm{Eve}}), \end{aligned} \tag{17}$$

respectively, where $I(b_1' : b_i') = \frac{1}{2}\log_2 \frac{V(b_i')}{V(b_i'|b_1')}$ $(i = 2, 3, 4)$ denotes the mutual information between Alice and Bob (Charlie or David). $V(b_i' \mid b_1')$ denotes the conditional variance of b_i' after b_1' is homodyned. $H(b_1' : \rho_{\mathrm{Eve}}) = S(\rho_{\mathrm{Eve}}) - S(\rho_{\mathrm{Eve}} \mid b_1')$ denotes the Holevo bound between b_1' and Eve, which represents the amount of information Eve can obtain. $S(M) = \sum_i h\left(m_i\right)$ is the von Neumann entropy, where $h\left(x\right) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}$ and m_i are the symplectic eigenvalues of covariance matrix M, which can be calculated by the eigenvalue spectrum of the matrix $|i\Omega M|$, where $\Omega = \bigoplus_i \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Since Eve can purify the whole state $\rho_{b_1',b_2',b_3',b_4',\mathrm{Eve}}$, the Holevo information can be written as

$$H\left(b_1' : \rho_{\mathrm{Eve}}\right) = S\left(\rho_{b_1',b_2',b_3',b_4'}\right) - S\left(\rho_{b_2',b_3',b_4'} \mid b_1'\right). \tag{18}$$

3.2 Secret key rate of QSS

In QSS with four users, we assume Alice is the dealer who holds the secret key, Bob, Charlie and David collaborate with each other to share the secret key. Alice can make suitable local Gaussian operation to share secret key with Bob, Charlie and David. The secret key rate $K_{\rm ABCD}^{\rm QSS_{RR}}$ with reverse reconciliation can be expressed as

$$K_{\rm ABCD}^{\rm QSS_{RR}} = \beta I\left(b_2', b_3', b_4' : b_1'\right) - H\left(b_1' : \rho_{\rm Eve}\right), \tag{19}$$

where $I\left(b_2', b_3', b_4' : b_1'\right) = \frac{1}{2}\log_2 \frac{V(b_1')}{V(b_1'|b_2', b_3', b_4')}$ denotes the mutual information among phase quadratures of Bob, Charlie, David and Alice. $H(b_1' : \rho_{\rm Eve}) = S(\rho_{\rm Eve}) - S(\rho_{\rm Eve} \mid b_1')$ denotes the Holevo bound between b_1' and Eve, which represents the amount of information Eve can obtain.

In QSS with three users, the secret key rate with reverse reconciliation can be written as

$$\begin{aligned} K_{\rm ABC}^{\rm QSS_{RR}} &= \beta I\left(b_2', b_3' : b_1'\right) - H\left(b_1' : \rho_{\rm Eve}\right), \\ K_{\rm ABD}^{\rm QSS_{RR}} &= \beta I\left(b_2', b_4' : b_1'\right) - H\left(b_1' : \rho_{\rm Eve}\right), \\ K_{\rm ACD}^{\rm QSS_{RR}} &= \beta I\left(b_3', b_4' : b_1'\right) - H\left(b_1' : \rho_{\rm Eve}\right), \\ K_{\rm BCD}^{\rm QSS_{RR}} &= \beta I\left(b_2', b_4' : b_3'\right) - H\left(b_3' : \rho_{\rm Eve}\right), \end{aligned} \tag{20}$$

respectively. The secret key rate is calculated in the same way as (17).

4 Results

For any given values of thermal noise $V_{E_{{\rm A}_i}} \geqslant 1$ $(i = 1-4)$, Eve's covariance matrix (Eq. (9)) is fully determined by the parameters g_i $(i = (1-6))$. To analyze the protocols in different situations, the bona fide condition [59] $\mu^2 \geqslant 1$ is needed, where μ is the smallest symplectic eigenvalue of the matrix $V_{E_{\rm A}E_{\rm B}E_{\rm C}E_{\rm D}}$. According to the current experimental technology, in the following simulation we set the reconciliation efficiency $\beta = 0.95$, the variance of Eve's EPR entangled state $V_{A_i} = 1.5$ $(i \in \{1-4\})$. In order to facilitate the analysis and design, we replace the transmission efficiency with the realistic transmission distance by $(\eta_i = 10^{-\alpha\frac{L_i}{10}})$, where $\alpha = 0.2$ dB/km is the loss of the optical fibers, L_i $(i = 1-4)$ denotes the transmission distance between Alice (Bob, Charlie, David) and the untrusted relay.

In our designed QC, Bob, Charlie and David share the secret keys with Alice, respectively. There are many entangled categories among the submodes in Eve's state. If Eve wants to obtain secret keys from Bob's, Charlie's and David's channel simultaneously, the symmetric attack manner can be implemented to Bob's, Charlie's and David's channel at the same time, i.e., $g_1 = g_4 = g_6$ in (9), and we take $g_2 = g_3 = g_5$ for simplification. The bona-fide conditions must be satisfied, and a numerical example is provided in Figure 4. Referring to the discussion in [23, 49], the colored regions are divided into three parts accoding to the positive partial transpose (PPT) criterion [60, 61]. The inner area and four peripheral areas correspond to the separable attack with separable ancillas and entangled attacks with entangled ancillas, respectively.

The relationship between the final secret key rates ($K_{\rm AB}^{\rm QC_{RR}}$) in QC and the transmission distance is shown in Figure 5, where g_1 and g_2 are taken as the status (1) ($g_1 = -0.65$ and $g_2 = 0$), status (2) ($g_1 = g_2 = 0$) and status (3) ($g_1 = 0.65$ and $g_2 = 0$), respectively. The variance of Alice's (Bob's, Charlie's, David's) thermal node $(a_i, i \in \{1-4\})$ is quantified as $V_i = 10$, $i \in \{{\rm A, B, C, D}\}$ (corresponding to 13 dB squeezing).

Two cases of symmetry and asymmetry network are analyzed in Figure 5. Symmetry network means that the distances between Alice, Bob, Charlie, David and the relay are equal, where $L_1 = L_2 = L_3 = L_4 = L$ (solid lines). In the asymmetric network, Alice is very close to the relay, while the distance between Bob, Charlie, David and the untrusted relay are equal, where we assume $L_1 = 0.01$ km and $L_2 = L_3 = L_4 = L$ (dash lines). In both symmetric and asymmetric network, if the attacker Eve chooses the entangled state in status (3), the transmission distance in QC is the shortest. On the other hand, the highest secret key rate and longest transmission distance are obtained when Eve chooses entangled state in status (1). Comparing the transmission distance in the symmetric and asymmetric network, it is obvious that the transmission distance between legitimate users and the relay is increased in the asymmetric network.

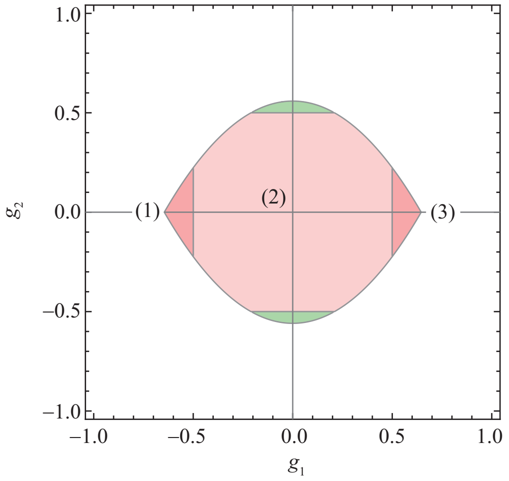

Figure 4 (Color online) The accessible region satisfying the bona fide condition for QC protocol. The position of three status are marked by (1), (2) and (3), respectively.

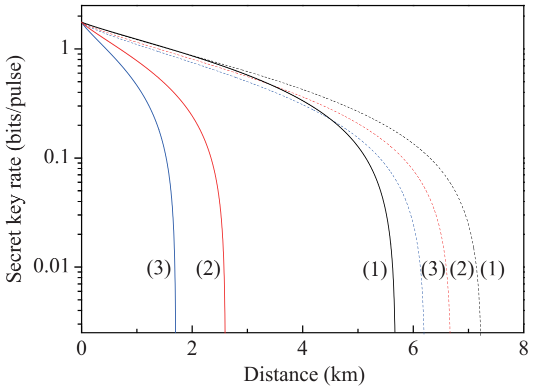

Figure 5 (Color online) The secret key rate versus transmission distance for QC protocol. The straight lines are for the symmetry case and the dash lines are for the asymmetry case.

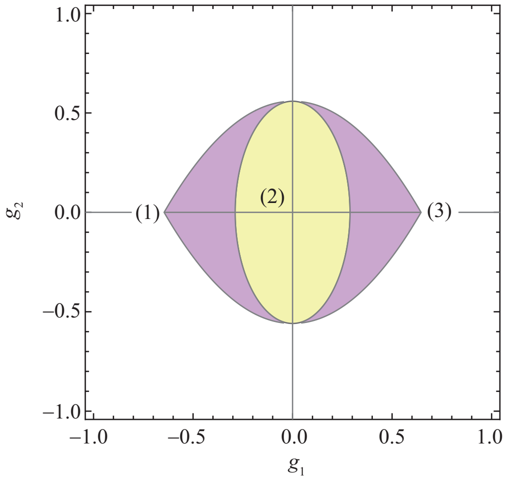

Figure 6 (Color online) The accessible region satisfying the bona fide condition for four participants QSS protocol. The position of three status are marked by (1), (2) and (3), respectively.

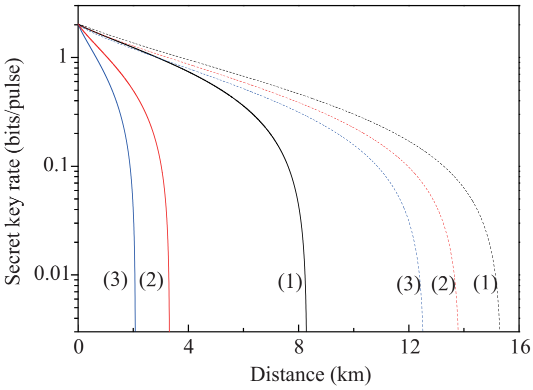

Figure 7 (Color online) The secret key rate versus transmission distance for four participants QSS protocol. The straight lines are for the symmetry case and the dash lines are for the asymmetry case.

For QSS with four users, we suppose the attacks in Bob's, Charlie's and David's channels are the same, that is $g_1 = g_4 = g_6$ and $g_2 = g_3 = g_5$. By using the PPT criterion, the bona field (shown in Figure 6) can be divided into two parts. The purple part stand for the case ρ_{E_A} is entangled with $\rho_{E_\mathrm{B},E_\mathrm{C},E_\mathrm{D}}$, while the yellow part means they are separated.

We also choose three kinds of status to analyze the relationship between the secret key rate and the transmission efficiency. Status (1) ($g_1 = g_4 = g_6 = -0.65$ and $g_2 = g_3 = g_5 = 0$), status (2) ($g_1 = g_4 = g_6 = 0$ and $g_2 = g_3 = g_5 = 0$) and status (3) ($g_1 = g_4 = g_6 = 0.65$ and $g_2 = g_3 = g_5 = 0$) are compared, respectively. The similar results as that of the QC are obtained in the symmetric and asymmetric network for the different quantum states used by Eve in QSS with four users which are shown in Figure 7.

The attacks of the four types of QSS with three users are similar because our scheme is symmetric. In order to achieve the symmetric attack of the protocol, Eve selects different input states by selecting

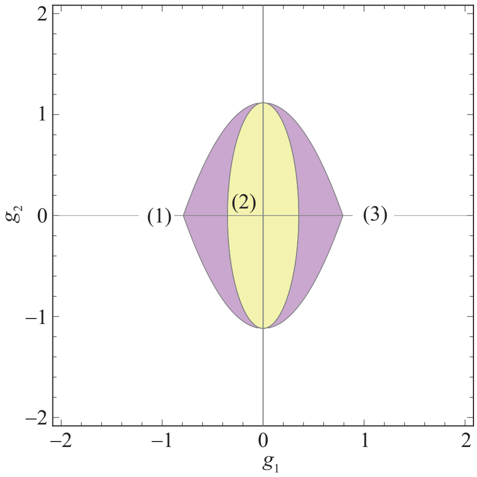

Figure 8 (Color online) The bona fide condition for three participants QSS protocol. The position of three status are marked by (1), (2) and (3), respectively.

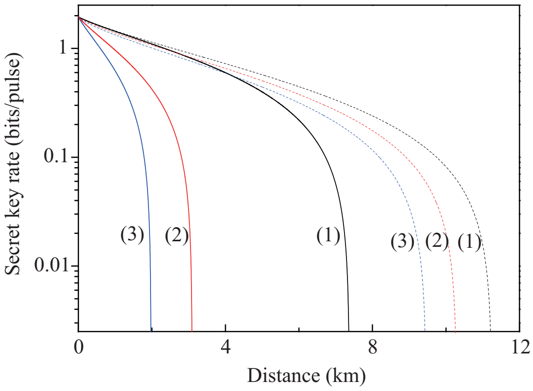

Figure 9 (Color online) The secret key rate versus transmission distance for three participants QSS protocol. The straight lines are for the symmetry case and the dash lines are for the asymmetry case.

different coefficients $g_1 - g_6$. For the QSS scheme among Alice, Bob and Charlie, Eve chooses $g_1 = g_4$; for the QSS scheme among Alice, Bob and David, Eve chooses $g_1 = g_6$; for the QSS scheme among Alice, Charlie and David, Eve chooses $g_4 = g_6$; for the QSS scheme among Bob, Charlie and David, Eve chooses $g_2 = g_3$.

The bona fide condition for Alice, Bob and Charlie's QSS protocol is shown in Figure 8. Similar to QSS with four users, the inner part can also be divided into two parts according to the PPT criterion. The two peripheral parts and the yellow part (inner part) stand for the ancillas states are entangled and separated, respectively.

The relationship between the secret key rate and the transmission efficiency is indicated in Figure 9 for QSS among Alice, Bob and Charlie. Three status (1) with $g_1 = -0.80$ and $g_2 = 0$, (2) with $g_1 = g_2 = 0$, and (3) with $g_1 = 0.80$ and $g_2 = 0$ are compared, respectively. In the symmetry network, we assume that the distances between Alice, Bob, Charlie and the relay are equal, where $L_1 = L_2 = L_3 = L$ (solid lines). In the asymmetric network, we assume that Alice is very close to the relay $L_1 = 0.01$ km, while the distance between Bob, Charlie and the relay are equal $L_2 = L_3 = L$ (dash lines). We also find that the highest secret key and longest transmission distance are obtained when the state in status (1) is chosen by Eve. The asymmetric network provides longer transmission distance than that of the symmetric network for the QSS with three users. Since the transmission loss between Alice and untrusted relay is omitted, the longer transmission distance can be achieved in the asymmetric network than that of the symmetric network in Figures 5, 7 and 9, respectively.

Figure 10 shows the relationship between the secret key rate and the variance of EPR entangled state V (squeezing) when the transmission distance between users and untrusted relay is 1 km. Three protocols in asymmetric networks are compared, which are chosen to be status (1) in Figures 5, 7 and 9, respectively. When the variance $V > 1.59$ (corresponding to 4.52 dB squeezing), the secret key can be obtained in all protocols. The secret key is increased with the increasing of the variance of EPR state.

5 Conclusion

We propose MDI quantum networks for QC and QSS with a star shape four-mode CV cluster state, and QSS with three users based on a linear CV cluster-like quantum correlation, respectively. The cluster state is prepared by performing Bell measurement in an untrusted relay and suitable displacement at the user's station. We show that the secret key rate and transmission distance depend on the state used by

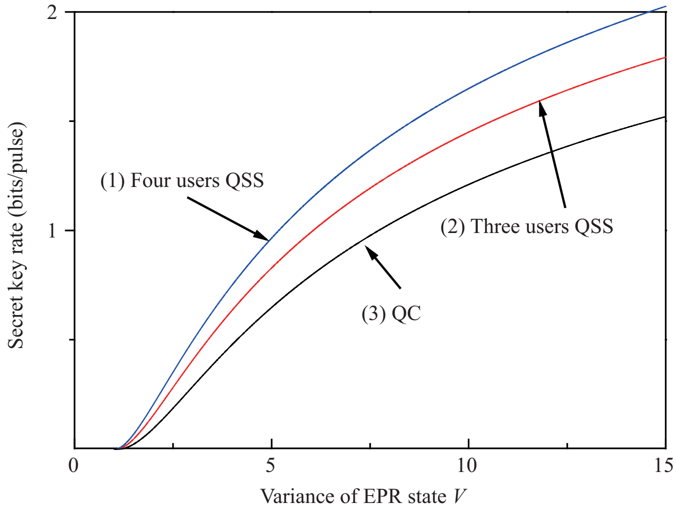

Figure 10 (Color online) The secret key rate versus variance of EPR states for four users QSS, three users QSS and QC protocols. Line (1) four users QSS; line (2) three users QSS; line (3) QC protocol.

Eve in the attack scheme and the structure of the network. The longer transmission distance is obtained in the asymmetric network than that of the symmetric network. The secret key can be obtained only when the squeezing of the CV entangled state is higher than a threshold.

Compared with CV GHZ state, various quantum correlations can be obtained in CV cluster states with different structures. Thus the MDI quantum network based on the CV cluster state can be more flexible and various quantum communication tasks can be implemented in the network. The smaller groups of participants cannot reconstruct the quantum secret in QSS. For example, any user except the secret dealer cannot reconstruct the quantum secret without the help of the other participant users in QSS with three users, and any one or two users cannot reconstruct the quantum secret without the help of the rest of users in QSS with four users. The proposed MDI network can be extended to more complex network based on the large scale CV cluster state.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 11504024, 11834010, 61602045, 11522433, 61502041, 61602046), National Key Research and Development Program of China (Grant No. 2016YFA0302600, 2018YFA0306404, 2016YFA0301402), and Program of Youth Sanjin Scholar.

References

1 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145–195

2 Weedbrook C, Pirandola S, García-Patrón R, et al. Gaussian quantum information. Rev Mod Phys, 2012, 84: 621–669

3 Wang S, Chen W, Yin Z Q, et al. Field and long-term demonstration of a wide area quantum key distribution network. Opt Express, 2014, 22: 21739

4 Wang S, Chen W, Guo J F, et al. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber. Opt Lett, 2012, 37: 1008

5 Wang S, Yin Z Q, Chau H F, et al. Proof-of-principle experimental realization of a qubit-like qudit-based quantum key distribution scheme. Quantum Sci Technol, 2018, 3: 025006

6 Yin Z Q, Wang S, Chen W, et al. Improved security bound for the round-robin-differential-phase-shift quantum key distribution. Nat Commun, 2018, 9: 457

7 Diamanti E, Lo H K, Qi B, et al. Practical challenges in quantum key distribution. Npj Quantum Inf, 2016, 2: 16025

8 Braunstein S L, Pirandola S. Side-channel-free quantum key distribution. Phys Rev Lett, 2012, 108: 130502

9 Wang S, Chen W, Yin Z Q, et al. Practical gigahertz quantum key distribution robust against channel disturbance. Opt Lett, 2018, 43: 2030

10 Wang S, Yin Z Q, Chen W, et al. Experimental demonstration of a quantum key distribution without signal disturbance monitoring. Nat Photon, 2015, 9: 832–836

11 Acín A, Brunner N, Gisin N, et al. Device-independent security of quantum cryptography against collective attacks. Phys Rev Lett, 2007, 98: 230501

12 Wang C, Yin Z Q, Wang S, et al. Measurement-device-independent quantum key distribution robust against environmental disturbances. Optica, 2017, 4: 1016

13 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett, 2012, 108: 130503

14 Lai H, Luo M X, Pieprzyk J, et al. High-rate and high-capacity measurement-device-independent quantum key distribution with Fibonacci matrix coding in free space. Sci China Inf Sci, 2018, 61: 062501

15 Rubenok A, Slater J A, Chan P, et al. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. Phys Rev Lett, 2013, 111: 130501

16 Ferreira da Silva T, Vitoreti D, Xavier G B, et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. Phys Rev A, 2013, 88: 052303

17 Tang Z, Liao Z, Xu F, et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. Phys Rev Lett, 2014, 112: 190503

18 Yin H L, Chen T Y, Yu Z W, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys Rev Lett, 2016, 117: 190501

19 Braunstein S L, van Loock P. Quantum information with continuous variables. Rev Mod Phys, 2005, 77: 513–577

20 Li Z, Zhang Y C, Xu F, et al. Continuous-variable measurement-device-independent quantum key distribution. Phys Rev A, 2014, 89: 052301

21 Zhang Y C, Li Z, Yu S, et al. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. Phys Rev A, 2014, 90: 052325

22 Grosshans F, Cerf N J, Wenger J, et al. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quantum Inf Comput, 2003, 3: 535–552

23 Pirandola S, Ottaviani C, Spedalieri G, et al. High-rate measurement-device-independent quantum cryptography. Nat Photon, 2015, 9: 397–402

24 Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys Rev Lett, 1999, 83: 648–651

25 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834

26 Gottesman D. Theory of quantum secret sharing. Phys Rev A, 2000, 61: 042311

27 Dou Z, Xu G, Chen X B, et al. A secure rational quantum state sharing protocol. Sci China Inf Sci, 2018, 61: 022501

28 Zhao Y, Fung C H F, Qi B, et al. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. Phys Rev A, 2008, 78: 042333

29 van Loock P, Braunstein S L. Multipartite entanglement for continuous variables: a quantum teleportation network. Phys Rev Lett, 2000, 84: 3482–3485

30 Zhang J, Braunstein S L. Continuous-variable Gaussian analog of cluster states. Phys Rev A, 2006, 73: 032318

31 Briegel H J, Raussendorf R. Persistent entanglement in arrays of interacting particles. Phys Rev Lett, 2001, 86: 910–913

32 van Loock P, Weedbrook C, Gu M. Building Gaussian cluster states by linear optics. Phys Rev A, 2007, 76: 032321

33 Lv S, Jing J. Generation of quadripartite entanglement from cascaded four-wave-mixing processes. Phys Rev A, 2017, 96: 043873

34 Wang H, Zheng Z, Wang Y, et al. Generation of tripartite entanglement from cascaded four-wave mixing processes. Opt Express, 2016, 24: 23459

35 Su X, Zhao Y, Hao S, et al. Experimental preparation of eight-partite cluster state for photonic qumodes. Opt Lett, 2012, 37: 5178

36 Chen M, Menicucci N C, Pfister O. Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb. Phys Rev Lett, 2014, 112: 120505

37 Yokoyama S, Ukai R, Armstrong S C, et al. Ultra-large-scale continuous-variable cluster states multiplexed in the time domain. Nat Photon, 2013, 7: 982–986

38 Raussendorf R, Briegel H J. A one-way quantum computer. Phys Rev Lett, 2001, 86: 5188–5191

39 Walther P, Resch K J, Rudolph T, et al. Experimental one-way quantum computing. Nature, 2005, 434: 169–176

40 Menicucci N C, van Loock P, Gu M, et al. Universal quantum computation with continuous-variable cluster states. Phys Rev Lett, 2006, 97: 110501

41 Gu M, Weedbrook C, Menicucci N C, et al. Quantum computing with continuous-variable clusters. Phys Rev A, 2009, 79: 062318

42 Loock P. Examples of Gaussian cluster computation. J Opt Soc Am B, 2007, 24: 340–346

43 Wang Y, Su X, Shen H, et al. Toward demonstrating controlled-X operation based on continuous-variable four-partite cluster states and quantum teleporters. Phys Rev A, 2010, 81: 022311

44 Ukai R, Iwata N, Shimokawa Y, et al. Demonstration of unconditional one-way quantum computations for continuous variables. Phys Rev Lett, 2011, 106: 240504

45 Su X, Hao S, Deng X, et al. Gate sequence for continuous variable one-way quantum computation. Nat Commun, 2013, 4: 2828

46 Wang L, Lv S, Jing J. Quantum steering in cascaded four-wave mixing processes. Opt Express, 2017, 25: 17457

47 Lau H K, Weedbrook C. Quantum secret sharing with continuous-variable cluster states. Phys Rev A, 2013, 88: 042313

48 Deng X, Xiang Y, Tian C, et al. Demonstration of monogamy relations for einstein-podolsky-rosen steering in gaussian cluster states. Phys Rev Lett, 2017, 118: 230501

49 Wu Y, Zhou J, Gong X, et al. Continuous-variable measurement-device-independent multipartite quantum communication. Phys Rev A, 2016, 93: 022325

50 Ottaviani C, Lupo C, Laurenza R, et al. High-rate secure quantum conferencing. 2017. ArXiv: 1709.06988

51 Zhang J. Graphical description of local Gaussian operations for continuous-variable weighted graph states. Phys Rev A, 2008, 78: 052307

52 Su X, Tan A, Jia X, et al. Experimental preparation of quadripartite cluster and Greenberger-Horne-Zeilinger entangled

states for continuous variables. Phys Rev Lett, 2007, 98: 070502

53 Yukawa M, Ukai R, van Loock P, et al. Experimental generation of four-mode continuous-variable cluster states. Phys Rev A, 2008, 78: 012301

54 Usenko V C, Grosshans F. Unidimensional continuous-variable quantum key distribution. Phys Rev A, 2015, 92: 062337

55 Wang X, Liu W, Wang P, et al. Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution. Phys Rev A, 2017, 95: 062330

56 Beimel A. Secret-sharing schemes: a survey. In: Proceedings of the 3rd International Conference on Coding and Cryptology (IWCC'11), Heidelberg, 2011. 11–46

57 Goyal V, Kumar A. Non-malleable secret sharing. In: Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, New York, 2018. 685–698

58 Lance A M, Symul T, Bowen W P, et al. Continuous variable (2, 3) threshold quantum secret sharing schemes. New J Phys, 2003, 5: 4

59 Adesso G, Illuminati F. Entanglement in continuous-variable systems: recent advances and current perspectives. J Phys A-Math Theor, 2007, 40: 7821–7880

60 Horodecki M, Horodecki P, Horodecki R. Separability of mixed states: necessary and sufficient conditions. Phys Lett A, 1996, 223: 1–8

61 Simon R. Peres-Horodecki separability criterion for continuous variable systems. Phys Rev Lett, 2000, 84: 2726–2729