Quantum-cryptography network via continuous-variable graph states

Yujing Qian, Zhean Shen, Guangqiang He,* and Guihua Zeng
State Key Laboratory of Advanced Optical Communication Systems and Networks, Key Laboratory on Navigation and Location-based Service, Shanghai Jiaotong University, Shanghai 200240, China
(Received 20 September 2012; published 29 November 2012)

We propose a quantum-cryptography network based on a continuous-variable graph state along with its corresponding quantum key distribution (QKD) protocol. It allows two arbitrary parties in the graph state to share a secret Gaussian key (any-to-any QKD). A mathematical model is established to determine an arbitrary graph state's properties, including the possibility of QKD and the relevant criteria. The general entangling cloner attack strategy is analyzed in detail employing Shannon information theory. Results show that the proposed network is secure against such attack if the graph state meets certain criteria.

DOI: 10.1103/PhysRevA.86.052333 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD), as a promising application of quantum information science, enables two partners—Alice, the sender, and Bob, the receiver—to share a secret key with full security. After almost three decades of development, the point-to-point (P2P) QKD scheme is quite mature and has been experimentally realized in telecommunication fibers [1,2]. Moreover, since Townsend *et al.* first discussed and realized the QKD network in a series of works [3–5], many QKD network topologies which aimed to implement one-to-any or any-to-any QKD have been proposed using an optical method [6–9]. In these QKD networks, optical switches, beam splitters, or wavelength division multiplexers [9] were usually employed as quantum routers (QR) to make Alice and Bob directly linked by a quantum channel.

In some previous research [10–12], quantum networks based on multipartite entanglement and graph states have been discussed. These networks are aimed to perform quantum teleportation, and some related experiments were performed in [13]. In these cases, one can "distill" the entanglement and teleport one quantum state to a target mode without the help of a direct quantum channel. In our paper, the cryptography network is proposed utilizing a graph state, which we consider a promising way to implement QKD without direct quantum channels. By using simple measurements and operations, we extract direct entanglement through indirect entanglement, thus acquiring the necessary factor to implement QKD.

In this paper, we introduce a continuous-variable (CV) QKD network based on an arbitrary graph state along with its corresponding QKD protocol. The relation between this protocol and the previous proposals for QKD is analogous to the relation between measurement-based quantum computation [14] and the circuital quantum computation [15]. Using a multipartite entangled state can avoid the direct transmission of quantum information. The network proposed in this paper is an any-to-any QKD network; in other words, QKD can be realized between two arbitrary modes, whether or not they are directly linked. By using Shannon information theory, detailed proof can be given to illustrate the security of this protocol against the general entangling cloner eavesdropping strategy.

This paper is organized as follows. In Sec. II, we propose a universal QKD protocol which can be used on an arbitrary graph state. In Sec. III, we give a detailed analysis of the protocol. Depending on the graph structure, some nodes may need to be disconnected in order to obtain a "core graph" that allows one to proceed with the protocol. We present criteria to identify core graphs and the procedure to extract core graphs from noncore ones. In Sec. IV, the security analysis is presented by analyzing the general individual attack strategy using an entangling cloner and calculating the mutual information rate ΔI_{AB} between Alice and Bob in the presence of eavesdropper Eve. The conclusion is drawn in Sec. V.

II. PROTOCOL OF CV QKD VIA GRAPH STATES

A. Prerequisite notations about CV graph states

A graph state is generated by coupling a set of zero-momentum eigenstates ($\hat{p} = 0$) by quantum nondemolition (QND) interaction [14] characterized by the Hamiltonian $H_{ij} = \hbar\chi_{ij}\hat{x}_i\hat{x}_j$. QND coupling between mode i and mode j transfer the quadrature amplitude x (position) and quadrature phase p (momentum) into the Heisenberg picture according to the following expressions [11]:

$$\hat{x}_i^g = \hat{x}_i, \quad \hat{p}_i^g = \hat{p}_i + g_{ij}\hat{x}_j, \quad \hat{x}_j^g = \hat{x}_j, \quad \hat{p}_j^g = \hat{p}_j + g_{ji}\hat{x}_i, \tag{1}$$

where $g_{ij} = -\chi_{ij}t_{ij}$ is the gain of the interaction, and χ_{ij} and t_{ij} are the coupling coefficient and the interaction time, respectively. This Hamiltonian makes momentum $\hat{p}_i^g$ and $\hat{p}_j^g$ pick up the information of the position $\hat{x}_j$ and $\hat{x}_i$ while the position remains unchanged. The QND coupling of light can be performed by linear optics [16] and was widely investigated in experiments [11].

For an arbitrary N-modes graph state, any modes can be described in the Heisenberg picture by

$$\hat{x}_i^g = \hat{x}_i, \quad \hat{p}_i^g = \hat{p}_i + \sum_{j=1}^{N} g_{ij}\hat{x}_j, \quad i = 1,2,\ldots N, \tag{2}$$

where $g_{ij} \neq 0$ only when modes i and j are neighbors.

Initially, all modes are prepared in the quadrature-phase squeezed state $\hat{x}_i = e^{r_i}\hat{x}_i^{(0)}$ and $\hat{p}_i = e^{-r_i}\hat{p}_i^{(0)}$, where r_i is the squeezing parameter and the superscript (0) denotes the initial

*Corresponding author: gqhe@sjtu.edu.cn

vacuum modes. In the ideal case, $r_i \to \infty$ represent the case in which all states are infinitely squeezed.

In the following, we first clarify three major types of operation that we used to realize QKD on graph states, and then present the QKD protocol.

(1) The first one is called disconnection operation [12]. This type of operation is based on the concept of undoing the coupling. By measuring the x (position) quadrature of the target mode and then displacing the momentum of all its neighbors by the product of the result (x) and the corresponding gain (g_{ij}), the target mode is disconnected from the graph. This operation is the exact inverse transformation of the QND interaction described in Eq. (1). Such an operation simply discards the target mode and eliminates its influence from the graph state.

(2) This one is simply the inverse Fourier transform, denoted by $F^\dagger$, with this operator acting as $\hat{x} \to \hat{p}$ and $\hat{p} \to -\hat{x}$.

(3) This is the displacement operation $\hat{D}(s)$. This operator can be placed on either the position or momentum quadrature. When performing $\hat{D}(s)$ on the position quadrature of mode (a), we have $x_a \to x_a + s$. In our case, s always represents the result of a homodyne detection result.

In some previous research, operations (2) and (3) are combined together as a "distill" operation [12,14]. But to implement QKD, using them separately has better flexibility.

B. Universal protocol of graph-state QKD

Here we assume that a graph-state entanglement network among several modes, including the sender and the receiver, has been prepared. QKD can be realized by performing the following four steps:

(i) Utilize the criteria (detail will be given in the next section) to judge whether the graph state is suitable for QKD. If it is, we call it a "core graph." If not, disconnect a subgraph from the original graph state to obtain a core graph. The subgraph must contain the sender and the receiver. As we will show in the section, if the criteria is already met, this step can be skipped.

(ii) As soon as the criteria is met, perform a series of measurements on the momentum quadrature $\hat{p}_i^g$ of the necessary modes according to the graph-related coefficients α and β. The detailed analysis will be given in the next section.

(iii) Apply a series of displacement operations on the sender's mode (Alice's mode), then perform an inverse Fourier transform on it (if needed). This step makes Alice and Bob directly entangled. Their position and momentum quadrature satisfy the following expression:

$$k_1 \hat{X}_A = \hat{X}_B, \quad k_2 \hat{P}_A = \hat{P}_B, \tag{3}$$

where k_1 and k_2 are nonzero graph-related coefficients known by both sides.

(iv) The three steps above make it possible for Alice and Bob to share pairs of entangled states without direct transmission. In previous research, many protocols were carried out after coherent states are sent to Bob or shared by both sides [17–20]. In our work, the following steps are quite similar to a traditional P2P QKD protocol. Since Alice and Bob share entangled states, the measurement of quadrature of one state gives Alice information on the same quadrature of Bob's state. In this protocol, they randomly choose to measure either x or p. And then, they do a reverse reconciliation (RR) to acquire information [as in the Bennett-Brassard 1984 (BB84) protocol, half of the key is unused] in case there is a eavesdropper, i.e., Eve.

(v) After step (iv), Alice and Bob now share two correlated Gaussian variables. Then they shall use a standard protocol for privacy amplification [21] in order to distill the private key.

III. GENERAL CRITERIA OF A QKD-SUPPORTING GRAPH STATE

In this section, we introduce a general approach to determine whether a graph state can be used as a core graph to implement QKD. Some properties and examples are also given in this section.

A. Criteria detailed analysis

To simplify the discussion, let us assume the graph state as an N-mode multipartite entanglement network with the sender's mode indexed 1 and the receiver's mode indexed N. Also, during the following detailed analysis, we assume all $\hat{p}_i$ are infinitely squeezed. We will consider the finite-squeezing case at the end of the section.

For a given graph state, let G denote the adjacency matrix with $G_{ij} = g_{ij}$. Using the $2N$-dimensional row vector $\hat{R} = (\hat{x}_1 \cdots \hat{x}_N | \hat{p}_1 \cdots \hat{p}_N)$ to represent the quadrature vector after squeezing, Eqs. (2) can be replaced by

$$\hat{X}^g = \hat{R}\begin{pmatrix} I \\ 0 \end{pmatrix}, \quad \hat{P}^g = \hat{R}\begin{pmatrix} G \\ I \end{pmatrix}, \tag{4}$$

where G and I are the $N \times N$ matrix.

Also, due to the assumption that all $\hat{p}_i$ are infinitely squeezed, Eqs. (4) can be rewritten as

$$\hat{x}_i^g = \hat{R}\begin{pmatrix} I_i \\ \forall \end{pmatrix}, \quad \hat{p}_i^g = \hat{R}\begin{pmatrix} G_i \\ \forall \end{pmatrix}, \tag{5}$$

where G_i and I_i represent the ith column of matrix G and unit matrix I, respectively. $\forall$ means arbitrary value since all $\hat{p}_i$ are infinitely squeezed, so that all $p_i \sim 0$, and they can be multiplied by an arbitrary value.

To implement QKD, the final two states between Alice and Bob should satisfy one of the following two equations:

$$\begin{aligned} &\text{(I)} \quad k_1 \hat{X}_A = \hat{X}_B, \quad k_2 \hat{X}_A = \hat{X}_B. \\ &\text{(II)} \quad k_1 \hat{X}_A = \hat{X}_B, \quad k_2 \hat{X}_A = -\hat{X}_B. \end{aligned} \tag{6}$$

Here, k_1, k_2 are nonzero constant coefficients related to the graph. As soon as Alice and Bob know the exact value of k_1 and k_2, QKD can be implemented by multiplying either k_1 or k_2 (depending on the quadrature that Alice measured) with Alice's detection result. The second equation in Eq. (6) is "cross related," and it can be transferred to be "direct related" by simply applying the $F^\dagger$ operator.

We now investigate under which conditions Eq. (6) can be achieved by steps (ii) and (iii) in our protocol, i.e., by only measuring momentum quadratures $\hat{p}_2^g \cdots \hat{p}_{N-1}^g$ (ii) and then performing a displacement $\hat{D}(s)$ on Alice's state (iii).

Therefore, assume we only apply the $\hat{D}(s)$ and $F^\dagger$ operation on Alice's state, i.e., $\hat{X}_A$ and $\hat{P}_A$ are related to $\hat{x}_1$ and $\hat{p}_1$ by a simple displacement. Then, Eq. (6) can be expressed as follows:

$$\begin{aligned} &\text{(I)}\ \ k_1\hat{x}_1^g - u = \hat{x}_N^g, \quad k_2\hat{p}_1^g - v = \hat{p}_N^g, \\ &\text{(II)}\ \ k_1\hat{x}_1^g - u = \hat{p}_N^g, \quad k_2\hat{p}_1^g - v = -\hat{x}_N^g, \end{aligned} \tag{7}$$

where u and v are displacement caused by the $\hat{D}(s)$ operator. More specifically, u and v can be expressed as the linear combination of detection results of momentum quadratures $\hat{p}_2^g \cdots \hat{p}_N^g$:

$$\begin{aligned} u &= \left(p_2^g \cdots p_{N-1}^g\right)\alpha = \hat{R}\begin{pmatrix} G_{2:N-1} \\ I_{2:N-1} \end{pmatrix}\alpha, \\ v &= \left(p_2^g \cdots p_{N-1}^g\right)\beta = \hat{R}\begin{pmatrix} G_{2:N-1} \\ I_{2:N-1} \end{pmatrix}\beta. \end{aligned} \tag{8}$$

Here, $G_{2:N-1}$, $I_{2:N-1}$ represent a $N \times (N-2)$ matrix consisting of the second to $(N-1)$th columns of G and unit matrix I, respectively. α and β are $(N-2)$-dimensional columns vectors.

For a certain graph G, by substituting Eqs. (4), (5), and (8) into Eq. (7) with $\hat{R}$ canceled, we obtain equations with k_1, k_2, α, and β as unknown variables:

$$\begin{aligned} &\text{(I)}\ \ k_1\begin{pmatrix} I_1 \\ \forall \end{pmatrix} = \begin{pmatrix} G_{2:N-1} \\ I_{2:N-1} \end{pmatrix}\alpha + \begin{pmatrix} I_N \\ 0 \end{pmatrix}, \\ &\qquad k_2\begin{pmatrix} G_1 \\ \forall \end{pmatrix} = \begin{pmatrix} G_{2:N-1} \\ I_{2:N-1} \end{pmatrix}\beta + \begin{pmatrix} G_N \\ I_N \end{pmatrix}. \\ &\text{(II)}\ \ k_1\begin{pmatrix} I_1 \\ \forall \end{pmatrix} = \begin{pmatrix} G_{2:N-1} \\ I_{2:N-1} \end{pmatrix}\alpha + \begin{pmatrix} G_N \\ I_N \end{pmatrix}, \\ &\qquad k_2\begin{pmatrix} G_1 \\ \forall \end{pmatrix} = \begin{pmatrix} G_{2:N-1} \\ I_{2:N-1} \end{pmatrix}\beta - \begin{pmatrix} I_N \\ 0 \end{pmatrix}. \end{aligned} \tag{9}$$

If the equations have solutions, then we call the graph a core graph. With a core graph, we can achieve correlated variables [Eq. (6)] by steps (ii) and (iii) in our protocol, and thus we can implement QKD according to the scheme devised in Sec. II. Then, mathematically, the graph can be used as a core graph to implement QKD. After simple calculation, Eq. (9) can be simplified as

$$\begin{aligned} &\text{(I)}\ \ k_1 I_1 - I_N = G_{2:N-1}\alpha, \quad k_2 G_1 - G_N = G_{2:N-1}\beta. \\ &\text{(II)}\ \ k_1 I_1 - G_N = G_{2:N-1}\alpha, \quad k_2 G_1 + I_N = G_{2:N-1}\beta. \end{aligned} \tag{10}$$

Putting unknown variables together into the same vector, Eq. (10) can be further simplified to the following expression:

$$\begin{aligned} &\text{(I)}\ \ (G_{2:N-1}| - I_1)\left(\frac{\alpha}{k_1}\right) = -I_N, \\ &\qquad (G_{2:N-1}| - G_1)\left(\frac{\beta}{k_2}\right) = -G_N. \\ &\text{(II)}\ \ (G_{2:N-1}| - I_1)\left(\frac{\alpha}{k_1}\right) = -G_N, \\ &\qquad (G_{2:N-1}| - G_1)\left(\frac{\beta}{k_2}\right) = I_N. \end{aligned} \tag{11}$$

If the equation above has a solution, then we must get

$$\begin{aligned} &\text{(I)}\ \ \operatorname{rank}(G_{2:N-1}| - I_1) = \operatorname{rank}(G_{2:N-1}| - I_1| - I_N), \\ &\qquad \operatorname{rank}(G_{2:N-1}| - G_1) = \operatorname{rank}(G_{2:N-1}| - G_1| - G_N). \\ &\text{(II)}\ \ \operatorname{rank}(G_{2:N-1}| - I_1) = \operatorname{rank}(G_{2:N-1}| - I_1| - G_N), \\ &\qquad \operatorname{rank}(G_{2:N-1}| - G_1) = \operatorname{rank}(G_{2:N-1}| - G_1|I_N). \end{aligned} \tag{12}$$

If either of two pairs of equations is satisfied and $k_1 k_2 \neq 0$, then graph G can be used as a core graph to implement QKD. Moreover, by solving the equations, one can get the final expressions of u and v and thus know the detail of the displacement operation. Solving Eq. (11) is merely a linear algebra problem, which we can solve by employing the Moore-Penrose pseudoinverse method.

In cases where more than one solution exists, every valid solution is a theoretically possible scheme to implement QKD. Different schemes may have different k_1 and k_2 [described in Eq. (3)]. Once the scheme is determined, the final state can be obtained from Eqs. (7) and (8).

In our protocol, after u and v have been displaced on Alice, the entanglement relationship is given in Eq. (3). Since we use $\hat{x}_N^g$ and $\hat{p}_N^g$ to represent Bob's state, we can get

$$\hat{X}_A = \frac{1}{k_1}\hat{x}_N^g, \quad \hat{P}_A = \frac{1}{k_2}\hat{p}_N^g, \quad \hat{X}_B = \hat{x}_N^g, \quad \hat{P}_B = \hat{p}_N^g, \tag{13}$$

where $(\hat{X}_A, \hat{P}_A)$, $(\hat{X}_B, \hat{P}_B)$ means Alice's and Bob's state, respectively.

However, it is impossible to acquire infinite squeezing in practice. Thus, when the squeezing is finite and we still use the method above to generate direct entanglement, some extra noise will exist. According to Eq. (1), each $\hat{p}_i^g$ contains a $\hat{p}_i$ and $\hat{p}_i \neq 0$ when the squeezing is finite. So, after multiplying either k_1 or k_2 (which depends on the quadrature that Alice measured) to Alice's detection result and performing the inverse Fourier transform (if needed), we can obtain the expression of extra noise (with vacuum variance normalized to unity):

$$\begin{aligned} &\text{(I)}\ \ \hat{N}_{X_A} = \sum_{i=2}^{N-1} \alpha_i\ \hat{p}_i^{(0)} e^{-r_i}, \quad \hat{N}_{X_B} = 0. \\ &\qquad \hat{N}_{P_A} = k_2 \hat{p}_1^0 e^{-r_1} + \sum_{i=2}^{N-1} \beta_i \hat{p}_i^{(0)} e^{-r_i}, \quad \hat{N}_{P_B} = \hat{p}_N^{(0)} e^{-r_N}. \\ &\text{(II)}\ \ \hat{N}_{X_A} = k_1 \hat{p}_1^0 e^{-r_1} + \sum_{i=2}^{N-1} \alpha_i\ \hat{p}_i^{(0)} e^{-r_i}, \quad \hat{N}_{X_B} = 0. \\ &\qquad \hat{N}_{P_A} = \sum_{i=2}^{N-1} \beta_i\ \hat{p}_i^{(0)} e^{-r_i}, \quad \hat{N}_{P_B} = \hat{p}_N^{(0)} e^{-r_N}. \end{aligned} \tag{14}$$

The final expression of Alice and Bob's states can be given as

$$\begin{aligned} \hat{X}_A &= \frac{1}{k_1}\hat{x}_N^g + \hat{N}_{X_A}, \quad \hat{P}_A = \frac{1}{k_2}\hat{p}_N^g + \hat{N}_{P_A}, \\ \hat{X}_B &= \hat{x}_N^g, \quad \hat{P}_B = \hat{p}_N^g + \hat{N}_{P_B}. \end{aligned} \tag{15}$$

B. Further discussion about step (i)

The first step in our protocol is disconnection, which is used to extract a core graph from an arbitrary graph in case the graph cannot be used to implement QKD. For a QKD-supporting graph, its quality can be evaluated by Eq. (13). The less the extra noise, the better the communication quality (this will be shown in the next section). When the graph states cannot implement QKD directly, different ways of disconnection may lead to different qualities. Here, we present a basic way to generate the optimal core graph which leads to the smallest noise:

(a) Polish. The first stage of disconnection is a series of operations we call "polish." This operation is based on the fact that for any vertex (except Alice and Bob) with only one neighbor, its neighbor should not be measured unless we disconnect the vertex from the graph. This can be easily proven: Assume a vertex like this has a index of i. Then its neighbor contains the information of $\hat{x}_i$, which cannot be eliminated through linear combination since this vertex only has one neighbor. The detailed operation of polish can be described as follows:

(1) Find a vertex (except Alice and Bob) with only a neighbor and disconnect it.

(2) Once such vertex is disconnected, we simply trace back to its only neighbor and do the disconnection operation again if it also needs to be "polished off."

The polish operation will not stop unless a vertex has more than one neighbor. This operation can reduce the dimension of adjacent matrix G and thus to some extent reduce the time complexity O of the subsequent traverse step (ii). Figure 1 shows a simple example of polish.

(b) Traverse. This part is more of an algorithmic problem. "Traverse" mean that Eqs. (11) are checked for all possible subgraphs. Here we simply traverse the whole graph and find all possible ways to extract a core graph according to Eq. (12). Among all of these graphs, we select the one with the smallest extra noise.

Note that when the adjacent matrix has a huge dimension, traversing the entire graph can be extremely time consuming. We can reduce the time complexity O at the cost of noise. In such cases, we may have to find a good way rather than the best way to extract a core graph, e.g., finding the shortest path by using the Dijkstra algorithm [22]. This is because a graph with no branches can be proven to be always QKD supporting. This is easy to prove considering the unique form of single-pass

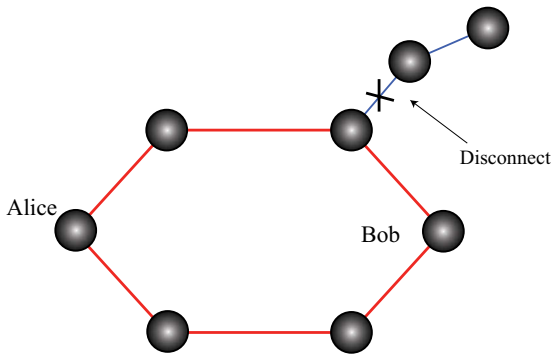

FIG. 1. (Color online) An example of "polish."

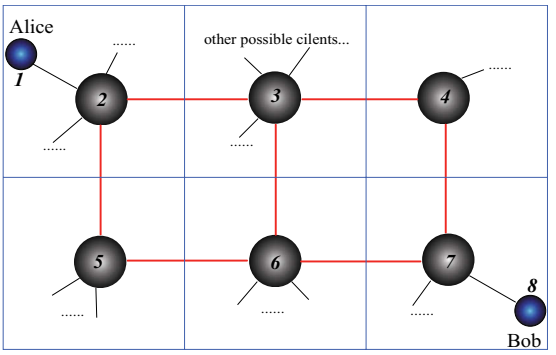

FIG. 2. (Color online) Cellular cryptography network.

graphs' adjacent matrices:

$$\begin{pmatrix} 0 & g_{12} & & & \\ g_{12} & \ddots & \ddots & & \\ & \ddots & \ddots & g_{(N-1)N} & \\ & & g_{(N-1)N} & 0 & \end{pmatrix}.$$

If there are an odd number of modes (N is a odd number) on this single-pass graph, then condition (I) in Eq. (12) will always be satisfied; if N is a even number, then condition (II) in Eq. (12) will always be satisfied.

C. Application example: A QKD network

In this example, we use our QKD protocol and corresponding criteria to present a "cellular cryptography network." This scheme enables two arbitrary clients to share quantum keys. Unlike the traditional cellular mobile network, we choose quadrilateral rather than hexagonal as the shape of the cells. That is because a network with quadrilateral cells requires less disconnection operations compare with hexagonal cells.

In Fig. 2, there are 3×2 cells and every cell has a "base station" which connects to its neighbor cell. If a client (Alice) in the picture wants to communicate with another client (Bob), then the u and v can be given as (with all nonzero g_{ij} set to unity)

$$u = \hat{p}_2^g - \hat{p}_6^g, \quad v = \hat{p}_7^g - \hat{p}_3^g.$$

Also, by using the criteria, we can get $k_1 = 1$, $k_2 = -1$, and an inverse Fourier transform is needed. In this case, $\hat{p}_4^g$ and $\hat{p}_5^g$ are not used in constructing a direct entanglement between Alice and Bob, which is because of the assumption that all nonzero g_{ij} is set to unity. In practice, it is hard to make every nonzero g_{ij} equal to 1. Thus, in most cases, every vertex in the network needs to be measured.

IV. SECURITY ANALYSIS

A. Principle of general individual attack strategy

In our protocol, there is no direct transmission between Alice and Bob (except for the case in which they are neighbors). Thus, it would be impossible for Eve to eavesdrop after the graph state is prepared. To acquire information, the only way for Eve to eavesdrop is during the generation of the graph state, or, more specifically, during the time when

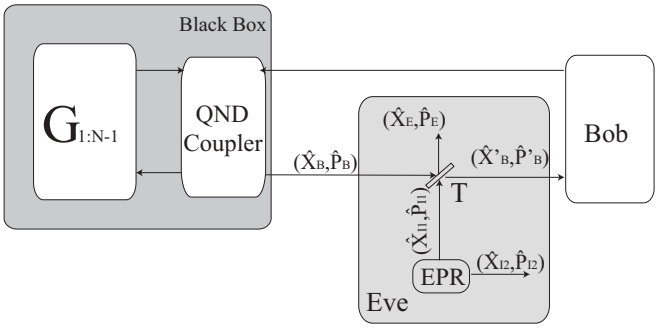

FIG. 3. Equivalent system diagram in the presence of Eve.

the QND coupled state is transmitted back to Bob. We now explain this strategy in detail.

The entangling cloner is a system that allows Eve to guess the results of Bob's measurement [23]. This kind of system can be described as a cloner creating two entangled outputs, with Eve keeping one of them and sending the other one to Bob. In the following analysis, we assume this system consists of a beam splitter and an Einstein-Podolsky-Rosen (EPR) source (see Fig. 4).

Here we consider security against individual attacks only. The whole discussion, including notations, parallels the one done in Ref. [23]. Suppose that Eve employs the entangling cloner to eavesdrop on the channel and that she can perfectly eavesdrop all of the classical information, including Alice's and Bob's position in graph state, G, u, and v. In this case, if Eve is to acquire information rather than obstruct the communication, the best occasion for her to eavesdrop shall be the transmission of Bob's final state during the generation of the graph state.

Let us suppose that the other modes in the graph, except Bob, and the measuring apparatus of all of these modes are hidden in a black box. The only output of this box is beam $(\hat{X}_B, \hat{P}_B)$, which is the QND coupled beam heading to Bob. The whole system is equivalent to Fig. 3.

By using the entangling cloner, Eve takes in the output of the black box as an input and produces two entangled outputs: $(\hat{X}_E, \hat{P}_E)$ and $(\hat{X}_B^{'}, \hat{P}_B^{'})$. The former is kept by Eve, and the latter is sent to Bob through a perfect line.

B. Mutual information of reverse reconciliation (RR)

After the displacement operation and inverse Fourier transform (if needed), Alice and Bob are entangled. The measurement of a quadrature of her own state gives Alice information on the same quadrature of Bob's.

According to the Csiszar-Korner formula [24,25], the final key rate should be expressed as

$$\Delta I = \gamma I_{AB} - I_{BE}, \tag{16}$$

where γ represents the efficiency of the reconciliation.

Considering Eq. (15), since $\hat{x}_N^g$ and $\hat{p}_N^g$ are Gaussian variables, we have

$$\left\langle \hat{x}_N^{g2} \right\rangle = V_x N_0, \quad \left\langle \hat{p}_N^{g2} \right\rangle = V_p N_0, \tag{17}$$

where $V_x = e^{2r_i}$, $V_p = \sum_{i=1}^{N} g_{iN}^2 e^{2r_i}$. N_0 is the vacuum variance. Also, the extra noise is the linear combination of $p_i = p_i^{(0)} e^{-2r_i}$, $i = 1 \cdots N$ [shown in Eq. (14)]. With vacuum variance set to unity, we get

$$\begin{aligned}
&\text{(I)} \ \left\langle \hat{N}_{X_A}^2 \right\rangle = \sum_{i=2}^{N-1} \alpha_i^2 e^{-2r_i}, \quad \left\langle \hat{N}_{X_B}^2 \right\rangle = 0, \\
&\qquad \left\langle \hat{N}_{P_A}^2 \right\rangle = \frac{1}{k_2^2} e^{-2r_1} + \sum_{i=2}^{N-1} \beta_i^2 e^{-2r_i}, \quad \left\langle \hat{N}_{P_B} \right\rangle = e^{-2r_N}. \\
&\text{(II)} \ \left\langle \hat{N}_{X_A}^2 \right\rangle = \frac{1}{k_1^2} e^{-2r_1} N_0 + \sum_{i=2}^{N-1} \alpha_i^2 e^{-2r_i}, \quad \left\langle \hat{N}_{X_B}^2 \right\rangle = 0, \\
&\qquad \left\langle \hat{N}_{P_A}^2 \right\rangle = \sum_{i=2}^{N-1} \beta_i^2 \, e^{-2r_i}, \quad \left\langle \hat{N}_{P_B}^2 \right\rangle = e^{-2r_N}.
\end{aligned} \tag{18}$$

To simplify the discussion, let us assume all squeezing parameters r_i are the same. According to [23,26,27], the conditional variance $V_{X_B|X_A}$ of $\hat{X}_B$ knowing X_A (the measurement result of $\hat{X}_A$) represents the remaining uncertainty on $\hat{X}_B$ after measurement of $\hat{X}_A$ giving the estimate $k_1 X_A$ of $\hat{X}_B$ and equal to

$$V_{X_B|X_A} = \left\langle \hat{X}_B^2 \right\rangle - \frac{|\langle k_1 X_A \hat{X}_B \rangle|}{k_1^2 X_A^2}. \tag{19}$$

When there is no extra noise [shown in Eq. (13)], we have the uncertainty principle

$$V_{X_B|X_A} \left\langle \hat{P}_B^2 \right\rangle \geqslant N_0^2 = 1. \tag{20}$$

Considering the increase of uncertainty caused by the extra noise [shown in Eq. (15)] and the fact that the squeezed state minimizes inequality, we obtain

$$V_{X_B|X_A} = \frac{1}{V_p} + \left\langle \hat{N}_{X_A}^2 \right\rangle. \tag{21}$$

By measuring her state $(\hat{X}_A)$ and multiplying the result (X_A) with k_1, Alice deduces $k_1 X_A$. Bob's state $(\hat{x}_N^g, \hat{p}_N^g + \hat{N}_{P_B})$ is then projected onto a position-squeezed state of squeezing parameter $s_x = \frac{V_{X_B|X_A}}{N_0} = V_{X_B|X_A}$ centered on $(k_1 X_A, 0)$.

Similarly, if Alice measures the quadrature $\hat{P}_A$, then Bob's state is projected onto a momentum-squeezed state of squeezing parameter $s_p = V_{P_B|P_A} = \frac{1}{V_x} + \langle \hat{N}_{P_A}^2 \rangle + \langle \hat{N}_{P_B}^2 \rangle$ centered on $(k_2 P_A, 0)$.

To eavesdrop a reverse reconciliation scheme, Eve needs to guess Bob's measurement result. As we presented in the previous discussion, $(\hat{X}_B, \hat{P}_B)$ is the input of the cloner, and $(\hat{X}_B^{'}, \hat{P}_B^{'})$, $(\hat{X}_E, \hat{P}_E)$ are its two outputs. Here, we assume the conditional variances $V_{X_B|X_E}$ and $V_{P_B|P_E}$ can be minimized by the best cloner.

Since Eve uses the best cloner, the channel can be described by

$$\hat{X}_B^{'} = \sqrt{T_X}(\hat{X}_B + \delta \hat{X}_B), \quad \hat{P}_B^{'} = \sqrt{T_P}(\hat{P}_B + \delta \hat{P}_B), \tag{22}$$

where

$$\left\langle \delta \hat{X}_B^2 \right\rangle = \chi_X N_0 = \chi_X, \quad \left\langle \delta \hat{P}_B^2 \right\rangle = \chi_P N_0 = \chi_P. \tag{23}$$

Here, T_X and T_P represent the transmission rates for each quadrature (T_X for X and T_P for P) of the beam splitter that Eve uses to split apart the light. $\chi_X = \frac{1}{T_X} - 1 + \epsilon$ and $\chi_P = \frac{1}{T_P} - 1 + \epsilon$ means the additive noise of each quadrature,

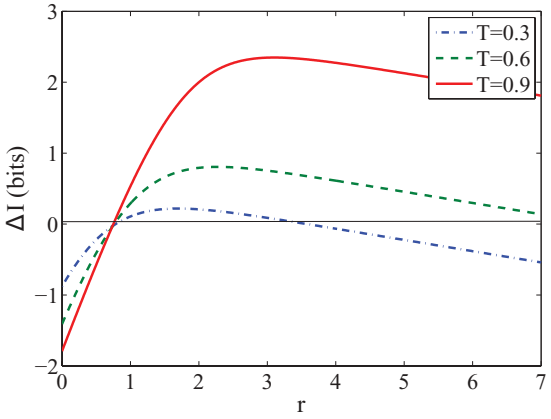

FIG. 4. (Color online) The lines show the relationship between ΔI and squeezing parameter r. Here we assume $T_X = T_Y = T$, $\gamma = 0.89$, $\epsilon = 0.02$, and that all nonzero g_{ij} are set to unity.

respectively. Usually, $T_X = T_P = T$ and $\chi_X = \chi_P = \chi$. The ϵ in the expression means the excess noise during the transmission.

Then we calculate the conditional variance in the presence of Eve: Inside the entangling cloner, sketched in Fig. 4, Eve injects into the beam splitter a beam $(\hat{X}_{I1}, \hat{P}_{I1})$ and uses the other half pair of EPR-correlated beams $(\hat{X}_{I2}, \hat{P}_{I2})$ to achieve maximal knowledge of $(\hat{X}_{I1}, \hat{P}_{I1})$. The inequality on conditional variances for a reverse reconciliation can be expressed as follows according to [23]:

$$V_{X'_B|X_A} V_{P'_B|P_E} \geqslant N_0^2, \quad V_{P'_B|P_A} V_{X'_B|X_E} \geqslant N_0^2. \tag{24}$$

The conditional variance depends on the amount of squeezing that Alice and the graph generate in the black box. The minimized conditional variances on $\hat{X}'_B$ can be deducted in a similar way to Eq. (19):

$$V_{X'_B|X_A,\min} = T_X(\chi_X + s_x)N_0, \quad V_{P'_B|P_A,\min} = T_P(\chi_P + s_p)N_0. \tag{25}$$

We then have

$$V_{X'_B|X_E,\min} = \frac{N_0}{T_P(\chi_P + s_p)}, \quad V_{P'_B|P_E,\min} = \frac{N_0}{T_X(\chi_X + s_x)}. \tag{26}$$

The mutual information can be given according to Shannon's theory [28]:

$$\begin{aligned} I^X_{BA} &= \frac{1}{2}\log_2 \frac{\langle \hat{X}'^2_B \rangle}{V_{X'_B|X_A}}, \quad I^X_{BE} = \frac{1}{2}\log_2 \frac{\langle \hat{X}'^2_B \rangle}{V_{X'_B|X_E}}, \\ I^P_{BA} &= \frac{1}{2}\log_2 \frac{\langle \hat{P}'^2_B \rangle}{V_{P'_B|P_A}}, \quad I^P_{BE} = \frac{1}{2}\log_2 \frac{\langle \hat{P}'^2_B \rangle}{V_{P'_B|P_E}}. \end{aligned} \tag{27}$$

Due to the fact that X and P have an equal possibility to be chosen to measure, Eq. (16) can be rewritten according to Eq. (27) as

$$\Delta I = \tfrac{1}{2}\left(\gamma I^X_{BA} + \gamma I^P_{BA} - I^X_{BE} - I^P_{BE}\right). \tag{28}$$

We can further simplify the equation as

$$\begin{aligned} \Delta I = {} & \frac{1}{4}\log_2 \left(\frac{1}{T_X T_P (\chi_X + s_x)^{\beta} (\chi_P + s_p)(V_x + \chi_X)^{1-\beta}} \right) \\ & + \frac{1}{4}\log_2 \left(\frac{1}{T_P T_X (\chi_P + s_p)^{\beta} (\chi_X + s_x)(V_P + \chi_P)^{1-\beta}} \right). \end{aligned} \tag{29}$$

The (sufficient) conditions for the security of an arbitrary QKD-supporting graph state based on the reverse reconciliation protocol can then be expressed as

$$\begin{aligned} & T_X^2 T_P^2 [(\chi_X + s_x)(\chi_P + s_p)]^{1+\gamma} \\ & \quad \times [(\chi_X + V_x)(\chi_P + V_P)]^{1-\gamma} < 1. \end{aligned} \tag{30}$$

This condition can be rewritten by using the definition of $\chi_X = \frac{1}{T_X} - 1 + \epsilon$ and $\chi_P = \frac{1}{T_P} - 1 + \epsilon$, where ϵ means the excess noise:

$$\begin{aligned} & [T_X T_X (\chi_X + V_x)(\chi_P + V_P)]^{1-\gamma} \\ & \times [(1 - T_X + T_X\epsilon + T_X s_x)(1 - T_P + T_P\epsilon + T_P s_p)]^{1+\gamma} < 1. \end{aligned} \tag{31}$$

When r is large enough to make s_x and s_p smaller than 1, this condition is always fulfilled for $\epsilon = 0$ when the reconciliation efficiency $\gamma = 1$. This result is similar and in conformity with those obtained by previously proposed QKD protocols [19]. When $\gamma < 1$, the left-hand side of Eq. (31) increases as r goes up, since $V_x = e^{2r}$, $V_p = \sum_{i=1}^N g_{iN}^2 e^{2r}$ [Eq. (17)]. This may finally lead to the insecurity of the protocol (Fig. 4). Different graphs may also result in different secure ranges since $V_p = \sum_{i=1}^N g_{iN}^2 e^{2r}$: when other parameters are fixed, bigger $\sum_{i=1}^N g_{iN}^2$ means the protocol can be secure only with a smaller r.

Taking Fig. 2 as an example, Fig. 4 shows the relationship between ΔI and squeezing parameter r under different T. The values $\gamma = 0.89$, $\epsilon = 0.02$ are typical values which can be achieved experimentally; in fact, they are chosen quite conservatively (so far, γ can reach 0.95 and ϵ can reduce to 0.01) [29]. When r is small, ΔI increases significantly as r goes up. However, the lines bend down as r keeps going up,

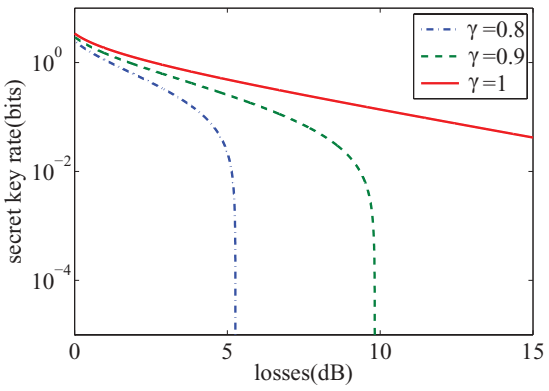

FIG. 5. (Color online) The lines show the relationship between the secret key rate and the losses ($-10\log_{10} T$) under different reconciliation efficiency γ. Here we assume $r = 2$, $\epsilon = 0.02$, and that all nonzero g_{ij} are set to unity.

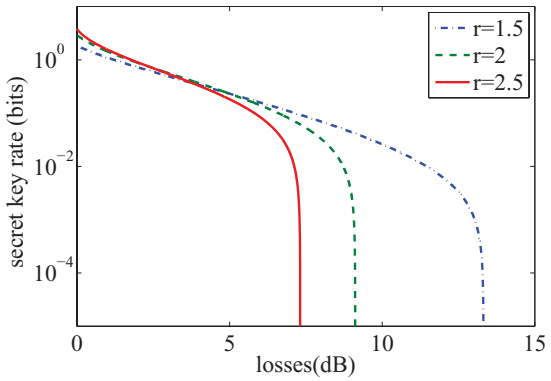

FIG. 6. (Color online) The lines shows the relationship between the secret key rate and the losses ($-10\log_{10}T$). Here we assume $\gamma = 0.89$, $\epsilon = 0.02$, and that all nonzero g_{ij} are set to unity.

since $\gamma < 1$. This result is in conformity with what is discussed above.

Figures 5 and 6 show the relationship between the secret key rate and the losses (dB), which equals to $-10\log_{10}(T)$ under different γ and r, respectively. In Fig. 5, we can see that the scheme with a higher reconciliation efficiency γ can tolerate higher losses. More specifically, when $\gamma = 1$, the protocol will always be secure. For Fig. 6, some unique conclusions can be drawn: in the previously proposed P2P QKD scheme, a larger squeezing parameter r usually means that the system can tolerate higher losses. However, in our protocol, it is just the opposite: we can see from the figure that a graph state with smaller squeezing parameter r can tolerate higher losses than those with larger ones. This is because of the special properties of the graph state, which are described in Eq. (17). In a graph state, V_x and V_p increase as r goes up. According to Eq. (29), when T is small enough, increasing r will accelerate the decrease of ΔI as T keeps going down.

We can draw some general conclusions when we combine Figs. 4–6 together. For a QKD network described in our protocol, whether it is secure or not depends on its adjacency matrix G, squeezing parameter r, reconciliation efficiency γ, and transmission rate T. Although a smaller r leads to a longer transmission distance, it would significantly reduce the secret key rate if it is too small. Also, a higher T or γ always means a higher key rate.

V. CONCLUSION

In this paper, we have proposed a CV QKD network and the corresponding protocol based on graph states and homodyne detection. In this QKD network, any two modes can launch a communication whether or not they are directly linked. Also, a general and efficient way, based on linear algebra, to devise an implementable QKD scheme based on any graph states is proposed. By examining adjacency matrix G with the criteria, there may exist different QKD schemes. Also, by calculating the conditional variance and the mutual information ΔI, the proposed protocol is proven to be secure against the individual attack strategy as long as Eq. (31) is satisfied. For any QKD-supporting graph state (core graph) described in our protocol, whether it is secure or not depends on its adjacency matrix G, squeezing parameter r, reconciliation efficiency γ, and transmission rate T.

So far, experimentalists have already generated four-mode graph states [30] and an eight-mode Greenberger-Horne-Zeilinger (GHZ) state [31]. Since we present a general approach to implement QKD in this paper, the protocol will still be valid when more sophisticated graph states are generated.

ACKNOWLEDGMENTS

We thank Peng Huang and Yadong Wu for helpful discussions. We also acknowledge support from the National Natural Science Foundation of China (Grants No. 61102053, No. 61170228, and No. 60970109), the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry, and SMC Excellent Young Faculty program, SJTU 2011.

[1] A. Tanaka *et al.*, Opt. Express. **16**, 11354 (2008).
[2] X. F. Mo *et al.*, Opt. Lett. **30**, 2632 (2005).
[3] P. D. Townsend *et al.*, Electron. Lett. **30**, 1875 (1994).
[4] P. D. Townsend, Nature (London) **385**, 47 (1997).
[5] P. D. Townsend, Electron. Lett. **33**, 188 (1997).
[6] W. Chen *et al.*, IEEE Photon. Tech. Lett. **21**, 575 (2009).
[7] A. Poppe *et al.*, Int. J. Quantum Inform. **6**, 209 (2008).
[8] T. Y. Chen *et al.*, Opt. Express **17**, 6540 (2009).
[9] G. Brassard *et al.*, AIP Conf. Proc. **734**, 323 (2004).
[10] P. van Loock and S. L. Braunstein, Phys. Rev. Lett. **84**, 3482 (2000).
[11] J. Zhang and S. L. Braunstein, Phys. Rev. A **73**, 032318 (2006).
[12] L. J. Ren, G. Q. He, and G. H. Zeng, Phys. Rev. A **78**, 042302 (2008).
[13] J. Zhang, K. Peng, and S. L. Braunstein, Phys. Rev. A **68**, 035802 (2003).
[14] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, Phys. Rev. Lett. **97**, 110501 (2006).
[15] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[16] P. van Loock, C. Weedbrook, and M. Gu, Phys. Rev. A **76**, 032321 (2007).
[17] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).
[18] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[19] F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).
[20] Y. Shen, X. Peng, J. Yang, and H. Guo, Phys. Rev. A **83**, 052304 (2011).
[21] G. Brassard and L. Salvail, *Advances in Cryptology CEUROCRYPT 93*, Lecture Notes in Computer Science, Vol. 765 (Springer-Verlag, Berlin, Heidelberg, New York, 1994), pp. 410–423.
[22] E. W. Dijkstra, Numer. Math. **1**, 269 (1959).

[23] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and Ph. Grangier, Quantum. Inf. Comput. **3**, 535 (2003).
[24] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[25] I. Csiszar and J. Korner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[26] Ph. Grangier *et al.*, Nature (London) **396**, 537 (1998).
[27] J. Ph. Poizat, J. F. Roch, and P. Grangier, Ann. Phys. (Paris) **19**, 265 (1994).
[28] C. E. Shannon, Bell Syst. Tech. J. **27**, 339 (1948); **27**, 623 (1948).
[29] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
[30] M. Yukawa, R. Ukai, P. van Loock, and A. Furusawa, Phys. Rev. A **78**, 012301 (2008).
[31] Y. Huang *et al.*, Nature Commun. **2**, 546 (2011).