applied sciences

MDPI

Article

Multipartite Continuous Variable Quantum Conferencing Network with Entanglement in the Middle

Zhaoyuan Zhang [1], Ronghua Shi [1] and Ying Guo [1,2,*]

[1] School of Information Science and Engineering, Central South University, Changsha 410083, China; zhangzhaoyuan@csu.edu.cn (Z.Z.); shirh@csu.edu.cn (R.S.)
[2] School of IOT Engineering, Taihu University, Wuxi 214064, China
* Correspondence: yingguo@mail.csu.edu.cn

Received: 28 June 2018; Accepted: 4 August 2018; Published: 7 August 2018

Featured Application: This work may be used to establish a cryptographic conference for more than 100 users.

Abstract: We suggest a continuous variable quantum conferencing network scheme with an entangled source in the middle. Here, the source generates a multipartite entangled state and distributes the modes of the state to an arbitrary number of legitimate network users. The entangled modes that were received and measured by the users share mutual information, which is utilized to generate secure conferencing key between users. The scheme is proven secure against collective attacks on both the untrusted source in the middle and all the quantum links. Simulation results show that the presented scheme can achieve high rate secure conferencing for 100 users within a 400 m-radius community or factory area.

Keywords: quantum conferencing; continuous variable; entanglement in the middle

PACS: 03.67.Dd; 42.50.-p; 89.70.Cf

1. Introduction

Quantum key distribution (QKD) [1–3], which is one of the most widely implemented areas of quantum information, enables secure communication for legal participants over public channels. The security of QKD has been guaranteed on the theory of quantum physics against adversaries with unlimited computing power [4,5]. Continuous variable (CV) QKD [6–8] provides secret key rates as high as half of the Pirandola–Laurenza–Ottaviani–Banchi bound with off-the-shelf devices. So far, theoretical studies and experimental implementations of CVQKD have been put forward, respectively.

As a crucial landmark, a quantum network was proposed to extend QKD from point-to-point configuration to a multi-user and large-scale scenario. A series of quantum networks based on point-to-point QKD devices are designed and developed [9–13], including two principle types: quantum channel switching networks [14] and trusted-repeater-based quantum networks [15]. However, in these quantum network schemes, quantum memories are required for restoring quantum states. Moreover, there is an urgent need to address the security problems caused by the repeater nodes in the quantum networks, which may not be trusted in practical situations.

Recent developments in the field of entanglement based multipartite QKD [16–18] have led to a renewed interest in the construction of QKD. Unlike the conventional point-to-point QKD, the CV QKD with entanglement in the middle [16] utilizes an untrusted third party to generalize Einstein-Podolsky-Rosen states, which are used for establishing the secure communication between

two legitimate parties against both collective attacks and coherent attacks [18]. On this basis, the tripartite CV QKD with entanglement source in the middle is proposed for providing secure key generation of three legitimate parties against coherent attacks on both the quantum links and the untrusted source. Although some research has been carried out on the CV QKD with entanglement in the middle, the mechanism by which utilizes an untrusted entanglement source to build a quantum network with arbitrary number of users has not been established.

Recently, an measurement-device-independent (MDI) star network based on CV systems has been proposed [19], which provides high-rate quantum conference and quantum secret sharing services of a building-sized transmission distance. However, the commercial implementation of this MDI star network is limited by the transmission distance. This paper proposes a new methodology for constructing a quantum conferencing network with an entanglement source in the middle, based on multipartite CV Greenberger-Horne-Zeilinger (GHZ) states generation and homodyne detection. Entangled modes of CV GHZ states are generated in the untrusted source in the middle, and distributed to an arbitrary number of legitimate network users. After the homodyne detections of the received modes and the postprocessing procedures, each pair of the parties share mutual information for generating multipartite quantum cryptographic conferencing key. Security analysis proves that the entanglement-based quantum conferencing scheme is able to provide secure communication against collective attacks. Moreover, by applying a Gaussian de Finetti reduction [20], the security against coherent attacks is also guaranteed [19]. Simulation results show that our scheme can establish high rate secure conferencing communication for about 100 users in a quantum network with a radius of hundreds of meters.

This paper is organized as follows. In Section 2, we propose the multipartite quantum conferencing scheme with entanglement in the middle. In Section 3, we analyze the security of the scheme against collective attacks and provide a derivation progress for the key rate. The simulation results are shown in Section 4. Finally, we draw our conclusions in Section 5.

2. A Quantum Conferencing Scheme with Entanglement in the Middle

The proposed entanglement-based CV quantum conferencing network is consists of an arbitrary number (N) of legitimate users, an entanglement source in the middle and links from the source to the users, which include classical networks and quantum channels. The entanglement source prepares an x-quadrature-squeezed state $\hat{a}_1$ and $N-1$ p-quadrature-squeezed state $\hat{a}_{2,\cdots,N}$, which are illustrated in Figure 1. As shown in Figure 1, the source combines the above N states by a sequence of beam splitters with decreasing transmissivities $T_k = 1 - 1/(N-k+1)$ for $k = 1, \cdots, N-1$. The output modes $\hat{a}'_{1,\cdots,N}$ after the combinations by the beam splitters are entangled in a multipartite GHZ state which satisfies the relations of x-quadratures $\sum_{k=1}^{N} \hat{a}'^{x}_{k} \to 0$ and p-quadratures $\hat{a}'^{p}_{k} - \hat{a}'^{p}_{k'} \to 0$ for any $k, k' = 1, \cdots, N$. This multipartite GHZ state is utilized for generating secret key in our quantum conferencing scheme.

The source sends the N modes of the GHZ state to N legitimate parties named as $\mathrm{Bob}_{1,\cdots,N}$, respectively. The entangled modes travel through N noisy quantum channels toward the users, respectively. For simplicity, we consider a symmetric configuration of the quantum conferencing scheme that all quantum channels from the source to the users have the same length. In a practical scenario, the transmissivity and thermal noise of the longest quantum channel are selected as the reference to the network configuration. The legitimate parties receive the N entangled modes $\hat{a}''_{1,\cdots,N}$ transmitted through the quantum channels and perform homodyne detection on them, respectively. With the measurement results, the users share mutual information which can generate a secret key for network communication after post-processing procedures. For a quantum conferencing scheme, the result of the ith user is used for reference to the reconciliation procedures, which let other users generate secret keys that can establish secure communication with the ith user, respectively. The CV quantum conferencing protocol with an entanglement source in the middle goes as follows.

1. The source in the middle prepares a CV GHZ state ρ_1 of N entangled modes $\hat{a}'_{1,\cdots,N}$, and sends them to N legitimate parties $\mathrm{Bob}_{1,\cdots,N}$ through quantum channels with the same transmissivity η, respectively.
2. After travelling through the noisy channels, N entangled modes $\hat{a}''_{1,\cdots,N}$ of the multipartite GHZ state ρ_2 are received by $\mathrm{Bob}_{1,\cdots,N}$, respectively.
3. The users perform homodyne detections on the p-quadratures of the received modes, respectively. Then, they perform quadrature measurement.
4. With the results of the measurement, the users use a public channel to complete following procedures as parameter estimation, information reconciliation and privacy amplification.

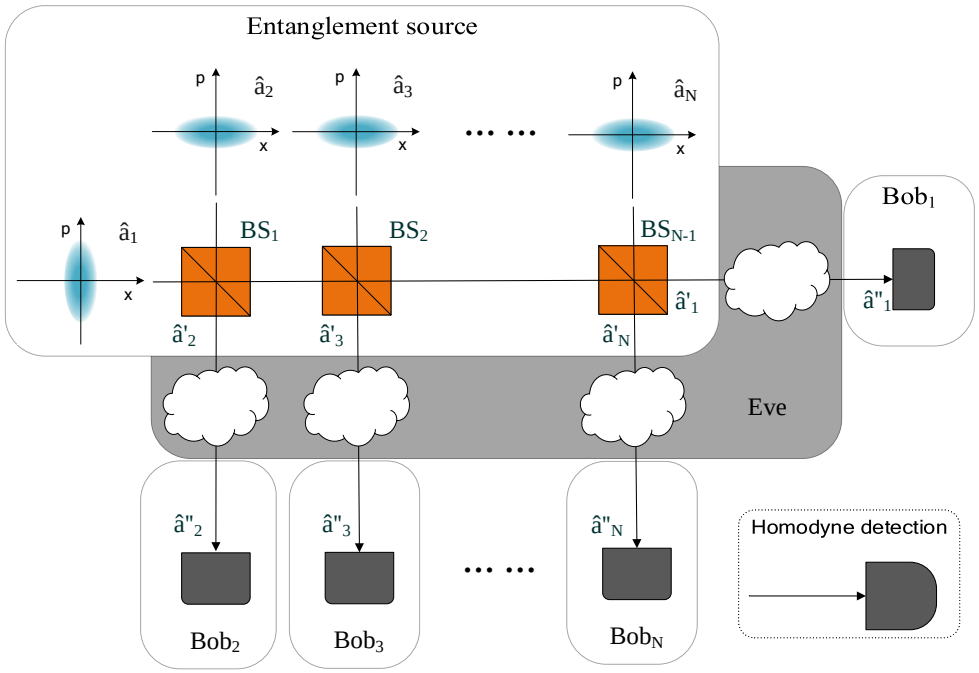

Figure 1. Schematic of the multipartite CV quantum conferencing scheme with entanglement in the middle. The source prepares CV squeezed states $\hat{a}_{1,\cdots,N}$, and combines them by beam splitters $BS_{1,\cdots,N}$. The output entangled modes $\hat{a}'_{1,\cdots,N}$ are distributed to legitimate users $Bob_{1,\cdots,N}$ through noisy quantum links, which are controlled by the eavesdropper Eve. The users receive the modes $\hat{a}'_{1,\cdots,N}$ and perform homodyne detection on them to distill mutual information.

Collective Attacks on Quantum Conferencing Scheme with Entanglement in the Middle

The best attack strategy of the eavesdropper Eve on the quantum star network is to perform attacks on all the quantum links and the entangled source in the middle. Since the Gaussian state can maximize the information of both the users and Eve, we consider the worst case that Eve fakes the source and prepares the multipartite Gaussian GHZ state herself [16]. Moreover, the Gaussian attacks of the links and the entangled source can be reduced to an attack of the links only [21].

At the beginning of eavesdropping, Eve replaces each of the original lossy channels with a noiseless channel and a beam splitter, of which the transmissivity is equal to the channel loss of the original channel η, and the thermal noise is $\bar{n}$. Eve prepares entangled ancillary modes $\hat{E}_{1,\cdots,N}$ and injects them onto the entangled modes $\hat{a}'_{1,\cdots,N}$ by her beam splitters of the channels, respectively. The output ancillary modes $\hat{E}'_{1,\cdots,N}$ are stored in Eve's quantum memory, and the injected modes $\hat{a}''_{1,\cdots,N}$ are sent to the users, respectively. For each ancillary mode of the beam splitters, Eve performs a collective Gaussian attack [22,23]. Although the entangled cloner collective attacks are simpler for analysing the security, coherent attacks are the most general and powerful attacks for the eavesdropper

Eve [22]. Since the performance of coherent attacks can be calculated as in Ref. [20] by applying a Gaussian de Finetti reduction [24], in our work, we focus on the security analysis of the quantum conferencing scheme against collective Gaussian attacks.

3. Security Analysis

The entangled source generates the initial state ρ_0 of an x-quadrature squeezed mode $\hat{a}_1$ and $N-1$ p-quadrature squeezed modes $\hat{a}_{2,\cdots,N}$. The covariance matrices of the initial modes are defined as

$$\mathbf{a}_1 = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}, \tag{1}$$

and

$$\mathbf{a}_{2,\cdots,N} = \begin{pmatrix} e^{2r} & 0 \\ 0 & e^{-2r} \end{pmatrix}. \tag{2}$$

The quadrature vector ξ_0 of ρ_0 is denoted as

$$\xi_0 = \left(\hat{a}_1, \hat{a}_2, \cdots, \hat{a}_N\right)^T. \tag{3}$$

To represent the $2N$ quadratures of the N modes, ξ_0 is restructured into the following form,

$$\xi_1 = \left(\hat{a}_1^x, \hat{a}_2^x, \cdots, \hat{a}_N^x, \hat{a}_1^p, \hat{a}_2^p, \cdots, \hat{a}_N^p,\right)^T. \tag{4}$$

After generating the initial modes, the source firstly combines $\hat{a}_1$ and $\hat{a}_2$ by a beam splitter of transmissivity T_1. In the next $N-2$ steps, one of the output mode from the kth combination and an initial mode $\hat{a}_{k+1}$ are combined by a beam splitter of transmissivity T_k, for $k = 2, \cdots, N-1$. This series of combinations produces N output modes $\hat{a}'_{1,\cdots,N}$, which are entangled in a GHZ state.

The transmissivities of the $N-1$ beam splitters of the entangled source is denoted by $T_k = \frac{N-k}{N-k+1}$, for $k = 1, 2, \cdots, N-1$. The output modes is described by the linear transformations on x-quadratures

$$\hat{a}_1'^x \to \frac{\hat{a}_1^x}{\sqrt{N}} + \sum_{j=2}^{N} \frac{\hat{a}_j^x}{(N+2-j)(N+1-j)}, \tag{5}$$

$$\hat{a}_k'^x \to \frac{\hat{a}_1^x}{\sqrt{N}} + \sum_{j=2}^{k} \frac{\hat{a}_j^x}{(N+2-j)(N+1-j)} \quad \text{for } k = 2, \cdots, N, \tag{6}$$

and the analogous linear transformations on p-quadratures. Moreover, the covariance matrices of the beam splitters are denoted by

$$\mathbf{T}_k = \begin{pmatrix} \sqrt{\frac{N-k}{N+1-k}} & -\frac{1}{\sqrt{N+1-k}} \\ \frac{1}{\sqrt{N+1-k}} & \sqrt{\frac{N-k}{N+1-k}} \end{pmatrix} \quad \text{for } k = 1, \cdots, N-1. \tag{7}$$

We use symplectic matrix $\mathbf{R}$ to describe the combinations of the beam splitters $T_{1,\cdots,N-1}$. The elements of $\mathbf{R}$ are given by

$$\mathbf{R}_{11} = \frac{1}{\sqrt{N}}, \tag{8}$$

$$\mathbf{R}_{1j} = \frac{1}{\sqrt{(N+2-j)(N+1-j)}} \quad \text{for } j = 2, \cdots, N, \tag{9}$$

$$\mathbf{R}_{jk} = -\mathbf{R}_{1k} \quad \text{for } j = 2, \cdots, N \text{ and } k = 1, \cdots, j-1, \tag{10}$$

$$\mathbf{R}_{kk} = \sqrt{\frac{N+1-k}{N+2-k}} \quad \text{for } k = 2, \cdots, N. \tag{11}$$

The covariance matrix (CM) of the initial state ρ_0 is denoted by

$$\mathbf{V}_0 = \begin{pmatrix} \mathbf{V}_x & \mathbf{0} \\ \mathbf{0} & \mathbf{V}_p \end{pmatrix}, \tag{12}$$

in which $\mathbf{V}_x$ and $\mathbf{V}_p$ are the CM of the x-quadratures and the p-quadratures of ρ_0 in terms of the quadrature vector ξ_1, respectively. The CM $\mathbf{V}_x$ and $\mathbf{V}_p$ are denoted by the following forms

$$\mathbf{V}_x = \begin{pmatrix} e^{-2r} & \mathbf{0} \\ \mathbf{0} & e^{2r}\mathbf{I}_{N-1} \end{pmatrix}, \quad \mathbf{V}_p = \begin{pmatrix} e^{2r} & \mathbf{0} \\ \mathbf{0} & e^{-2r}\mathbf{I}_{N-1} \end{pmatrix}, \tag{13}$$

where r refers to the squeeze factor of the initial squeezed states. The source combines the modes of ρ_0 by the beam splitters, producing the entangled modes of a GHZ state ρ_1, which is described by the following CM

$$\mathbf{V}_1 = \begin{pmatrix} \mathbf{V}'_x & \mathbf{0} \\ \mathbf{0} & \mathbf{V}'_p \end{pmatrix} = \mathbf{R} \cdot \mathbf{V}_0 \cdot \mathbf{R}^T, \tag{14}$$

where

$$(\mathbf{V}'_x)_{ij} = \begin{cases} -\frac{1}{N}e^{-2r} + \frac{1}{N}e^{2r} & \text{for } i \neq j, \\ \frac{1}{N}e^{-2r} + \frac{N-1}{N}e^{2r} & \text{for } i = j, \end{cases} \tag{15}$$

and

$$\left(\mathbf{V}'_p\right)_{ij} = \begin{cases} \frac{1}{N}e^{-2r} - \frac{1}{N}e^{2r} & \text{for } i \neq j, \\ \frac{N-1}{N}e^{-2r} + \frac{1}{N}e^{2r} & \text{for } i = j. \end{cases} \tag{16}$$

The eavesdropper Eve prepares an ancillary state ρ_E to perform entangled cloner attacks. Each entangled mode of ρ_E is injected onto a travelling mode $\hat{a}'_k$ of ρ_1, respectively. The CM of ρ_E that corresponds to ρ_1 is given by

$$\mathbf{V}_E = \begin{pmatrix} \omega\mathbf{I}_N & \mathbf{0} \\ \mathbf{0} & \omega\mathbf{I}_N \end{pmatrix}, \tag{17}$$

where $\omega = 1 + 2\bar{n}$ denotes the variance of Eve's ancillary modes. The CM of the whole system before the transmission through the quantum channels is defined by

$$\mathbf{V}_2 = \mathbf{V}_1 \bigoplus \mathbf{V}_E. \tag{18}$$

In order to implement eavesdropping, Eve replaces the noisy channels from the source to all the legitimate parties with noisy-free quantum links and beam splitters, respectively. The transmittance η of each beam splitter of Eve is the same as the original noisy channel it has replaced. The symplectic matrices of Eve's beam splitters are denoted by

$$\mathbf{S}_k = \begin{pmatrix} \sqrt{\eta}\mathbf{I} & -\sqrt{1-\eta}\mathbf{I} \\ \sqrt{1-\eta}\mathbf{I} & \sqrt{\eta}\mathbf{I} \end{pmatrix}, \quad k = 1, \cdots, N. \tag{19}$$

We use the symplectic matrix $\mathbf{S}_E$ to describe the transmission action of the entire system of both the entangled modes from the source and Eve's ancillary modes by Eve's beam splitters

$$\mathbf{S}_E = \begin{pmatrix} \sqrt{\eta}\mathbf{I}_{2N} & -\sqrt{1-\eta}\mathbf{I}_{2N} \\ \sqrt{1-\eta}\mathbf{I}_{2N} & \sqrt{\eta}\mathbf{I}_{2N} \end{pmatrix}. \tag{20}$$

After the transmission of the legitimate users' modes through Eve's thermal-loss channels and beam splitters, the CM of the whole system is described by

$$\mathbf{V}_3 = \mathbf{S}_E \cdot \mathbf{V}_2 \cdot \mathbf{S}_E^T. \tag{21}$$

We distill the partial matrix $\mathbf{V}_4$ from $\mathbf{V}_3$, which describes the entangled modes of the users' received state ρ_2. The form of $\mathbf{V}_4$ is described by

$$\mathbf{V}_4 = \begin{pmatrix} \mathbf{\Lambda} & \mathbf{\Gamma} & \cdots & \mathbf{\Gamma} \\ \mathbf{\Gamma} & \mathbf{\Lambda} & \ddots & \mathbf{\Gamma} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{\Gamma} & \mathbf{\Gamma} & \cdots & \mathbf{\Lambda} \end{pmatrix}, \tag{22}$$

with

$$\mathbf{\Lambda} = \begin{pmatrix} \eta\left(\frac{N-1}{N}e^{2r} + \frac{1}{N}e^{-2r}\right) + (1-\eta)\omega & 0 \\ 0 & \eta\left(\frac{1}{N}e^{2r} + \frac{N-1}{N}e^{-2r}\right) + (1-\eta)\omega \end{pmatrix}, \tag{23}$$

and

$$\mathbf{\Gamma} = \begin{pmatrix} \eta\left(\frac{1}{N}e^{2r} - \frac{1}{N}e^{2r}\right) & 0 \\ 0 & \eta\left(-\frac{1}{N}e^{2r} + \frac{1}{N}e^{2r}\right) \end{pmatrix}. \tag{24}$$

As a result, the CM of any ith and jth Bobs' modes is described by

$$\mathbf{V}_5 = \begin{pmatrix} \mathbf{\Lambda} & \mathbf{\Gamma} \\ \mathbf{\Gamma} & \mathbf{\Lambda} \end{pmatrix}. \tag{25}$$

3.1. Mutual Information

In the presented CV quantum conferencing scheme, all the Bobs receive their entangled modes and then perform homodyne detection on the p-quadratures of them, respectively. The legitimate users pick the measurement results of an arbitrary ith Bob's mode as the reference of the reconciliation procedure. Each of the other users (noted as the jth Bob) can generate a secret key with the ith Bob to establish secure communication between them.

The Bobs perform homodyne detections on the p-quadratures of their received modes, respectively. The conditional CM of the ith and the jth Bobs' modes B_i and B_j after homodyne detections is given by

$$\mathbf{V}_{B_i|B_j} = \mathbf{\Lambda} - \mathbf{\Gamma}(\mathbf{\Pi}\mathbf{\Lambda}\mathbf{\Pi})^{-1}\mathbf{\Gamma}^T, \tag{26}$$

where

$$\mathbf{\Pi} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{27}$$

The mutual information between the ith and the jth Bobs' results is generated by

$$I(B_i : B_j) = \frac{1}{2} log_2 \frac{\mathbf{\Lambda}^p}{\mathbf{V}^p_{B_i|B_j}}. \tag{28}$$

We also consider each user performs heterodyne detection on both x-quadrature and p-quadrature of their received mode. The conditional CM of the the ith and the jth Bobs' modes after one of them performs heterodyne detection is given by

$$\mathbf{V}'_{B_i|B_j} = \mathbf{\Lambda} - \theta^{-1}\mathbf{\Gamma}(\Theta\mathbf{\Lambda}\Theta^T)\mathbf{\Gamma}^T, \tag{29}$$

where

$$\theta = det\mathbf{\Lambda} + Tr\mathbf{\Lambda} + 1, \tag{30}$$

and

$$\Theta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{31}$$

The mutual information between the ith and the jth Bobs' heterodyne results is given by

$$I'(B_i : B_j) = \frac{1}{2} log_2 \frac{\mathbf{\Lambda}^x}{\mathbf{V}'^x_{B_i|B_j}} + \frac{1}{2} log_2 \frac{\mathbf{\Lambda}^p}{\mathbf{V}'^p_{B_i|B_j}}. \tag{32}$$

3.2. Holevo Bound of the Stolen Information

Since the results of the ith Bob's mode are utilized as the reference, the eavesdropper Eve's stolen information is defined by the Holevo information $H(E : B_i)$ between Eve and the result of the ith Bob. Since Eve has the ability to purify the entire system, the state $\rho_{E\rho_2}$ that describes the system after transmission through the quantum links is pure, where E denotes the measurement results of Eve's restored modes $\hat{E}'_{1,\cdots,N}$. After the users' homodyne measurement, the conditional state $\rho_{EB'|B_i}$ is still pure, where B' denotes the measurement results of all the users. Hence, the Holevo bound of the stolen information is given by

$$H(E : B_i) = S(\rho_E) - S(\rho_{E|B_i}) = S(\rho_2) - S(\rho_{B'|B_i}), \tag{33}$$

where $S(\rho)$ denotes the Holevo entropy of state ρ. In order to derive the Holevo entropy $S(\rho_2)$, we calculate the symplectic eigenvalues of the CM $\mathbf{V}_4$, which is the eigenvalues of the Williamson normal form $|I\Omega\mathbf{V}_4|$ [25,26], where I is the imaginary unit and Ω is the symplectic form

$$\Omega = \bigoplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{34}$$

We derive the single N-degenerate symplectic eigenvalues of $\mathbf{V}_4$, which is described by

$$\nu = \sqrt{[\eta e^{-r} + (1-\eta)e^{r}\omega][\eta e^{r} + (1-\eta)e^{-r}\omega]}. \tag{35}$$

The von Neumann entropy $S(\rho_2)$ is generated from the N symplectic eigenvalues ν by the following equation

$$S(\rho_2) = Nh(\nu), \tag{36}$$

where

$$h(x) = \frac{x+1}{2} log_2 \frac{x+1}{2} - \frac{x-1}{2} log_2 \frac{x-1}{2}. \tag{37}$$

The conditional CM $\mathbf{V}_{B'|B_i}$ describes the received modes of the Bobs after the ith Bob performs homodyne detection on his mode. We reconstruct the CM $\mathbf{V}_4$ in the following matrix:

$$\mathbf{V}_4' = \begin{pmatrix} \mathbf{A}_1 & \mathbf{C}_1 \\ \mathbf{C}_1 & \mathbf{B}_1 \end{pmatrix}, \tag{38}$$

where $\mathbf{B}_1$ describes the mode of the ith Bob, $\mathbf{A}_1$ describes all the other Bobs' modes and $\mathbf{C}_1$ describes the relations between the above two blocks. After the homodyne detection on the p-quadrature of the ith Bob's mode, the conditional CM $\mathbf{V}_{B'|B_i}$ is given by

$$\mathbf{V}_{B'|B_i} = \mathbf{A}_1 - \mathbf{C}_1 \left(\mathbf{\Pi}\mathbf{B}_1\mathbf{\Pi}\right) \mathbf{C}_1^T. \tag{39}$$

Similarly, we derive the symplectic eigenvalues of $\mathbf{V}_{B'|B_i}$, which contain $N-1$ identical symplectic eigenvalues given by Equation (36). The conditional von Neumann entropy $S(\rho_B|B_i)$ is given by

$$S(\rho_B|B_i) = (N-1)h(\nu). \tag{40}$$

Then, the Holevo bound of Eve's stolen information is derived from the above equations

$$H(Eve : B_i) = h(\nu). \tag{41}$$

In addition, we consider the Holevo bound when the users perform heterodyne detection on their received modes. The symplectic eigenvalues of $\mathbf{V}_{B'|B_i}$ after the heterodyne detecion include $N-2$ symplectic eigenvalues given by Equation (36), and one given by

$$\nu_N = \sqrt{\frac{\tau_1\tau_2}{\lambda_1\lambda_2}}, \tag{42}$$

where

$$\begin{aligned}
\tau_1 &= N(1-\eta)\omega\left(\eta + \eta e^{4r} + e^{2r}\right) + \eta[e^{4r} + N\eta e^{2r} + (N-1)] + N(1-\eta)^2 e^{2r}\omega^2, \\
\tau_2 &= N(1-\eta)\omega\left(\eta + \eta e^{4r} + e^{2r}\right) + \eta[(N-1)e^{4r} + N\eta e^{2r} + 1] + N(1-\eta)^2 e^{2r}\omega^2, \\
\lambda_1 &= (N-1)\eta + e^{2r}[N(1-\eta)\omega + \eta e^{2r} + N], \\
\lambda_2 &= \eta + e^{2r}[N(1-\eta)\omega + (N-1)\eta e^{2r} + N].
\end{aligned} \tag{43}$$

The conditional von Neumann entropy $S(\rho_B|B_i)$ is given by

$$S(\rho_B|B_i) = (N-2)h(\nu) + h(\nu_N). \tag{44}$$

Then, the Holevo bound of Eve's stolen information is derived from the above equations

$$H(Eve : B_i) = 2h(\nu) - h(\nu_N). \tag{45}$$

With the results in Equations (28) and (41), we finally derive the secret key rate of our quantum conferencing with entanglement in the middle scheme

$$K_{Rate} = I(B_i : B_j) - H(E : B_i). \tag{46}$$

4. Simulation Results

In this section, we consider the CV quantum conferencing with entanglement in the middle against collective attacks and give the simulation results of our security analysis. All of the quantum channels

have the same transmissivity η, which is mapped into a fiber distance l in km, using $\eta := 10^{l/50}$. Different conditions of thermal noise and number of users are taken into account.

In Figure 2, we plot the secret key rate of our quantum conferencing scheme versus the maximum distance of the quantum link in our network. The solid blue lines, small dashed red lines and large dashed black lines refer to $N = 3$, $N = 10$ and $N = 100$ network users of our quantum conferencing scheme, respectively. As shown in Figure 2, the scheme can reach a network radius of 2 km when the number of users is less than 10. When the number of users increases to 100, the scheme can still provide a quantum conferencing network with a longest transmission distance of over 500 m (520 m when thermal noise is set to 0.05, and 575 m when thermal noise is set to 0). Furthermore, the curves show that, with a network radius of 480 m, 100 users can establish secure conferencing communication at about 0.1 bit per pulse. The conferencing key rate can reach 2.5 Mbits per second based on a CV QKD network with a clock of 25 MHz [27].

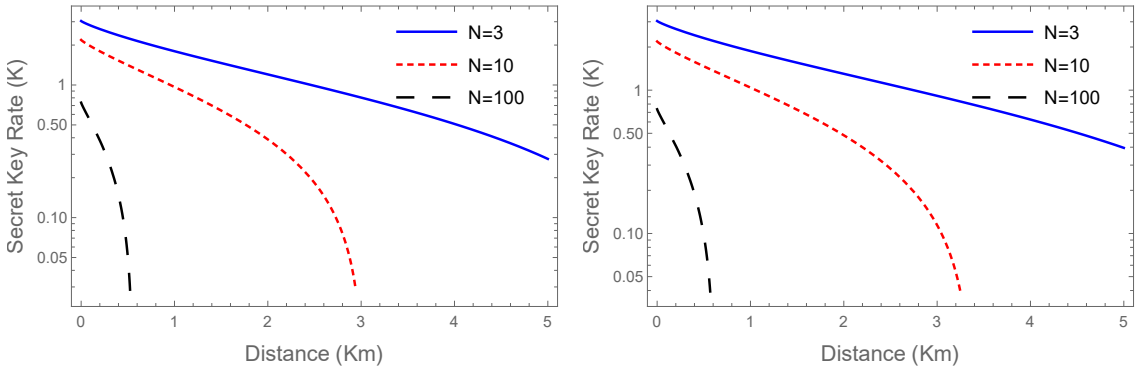

Figure 2. The performance analysis of the entanglement-based multipartite CV quantum conferencing scheme in terms of the derived secret key rate. The curves represent the conferencing key rate as a function of the radius of the network, in conditions of $N = 3$ (solid blue line), $N = 10$ (small dashed red line) and $N = 100$ (large dashed black line) of users, respectively. The thermal noise is set to $\bar{n} = 0.05$ in (**a**) and $\bar{n} = 0$ in (**b**), respectively.

Figure 3 presents the relationship between number of users and the maximum network distance when the secret conferencing key rate is asymptotic to 0, and the thermal noise is set to $\bar{n} = 0.05$ in (a) and $\bar{n} = 0$ in (b), respectively. As can be seen from Figure 3, there is a trade-off between the number of network users and the maximum transmission distance. Moreover, the conferencing scheme can achieve secure communication for 300 users on a building-size scale (about a radius of 150 m), or for dozens of users between multiple buildings (within a radius of 500 m or more). This result shows that the quantum conferencing with entanglement in the middle scheme can be applied to more scenarios than the MDI-based high-rate quantum conferencing scheme [19], which provides secure conference for 50 users within a radius of 40 m.

We consider different measurement methods that the network perform on their received modes. In the key rate equation Equation (46), we replace the mutual information $I(B_i : B_j)$ that was derived in Equation (28) with the result in Equation (32), and give the simulation results in Figure 4. Obviously, the scheme with homodyne detection has better performance of the secure conferencing key rate than the scheme with heterodyne detection. As we mentioned in Section 2, the p-quadratures of the entangled GHZ state have correlations of $\hat{a}_k^{\prime p} - \hat{a}_{k'}^{\prime p} \to 0$ for any $k, k' = 1, \cdots, N$, which is utilized for the conferencing key generation of our scheme. As a result, we select homodyne detection as the measurement method for the network users.

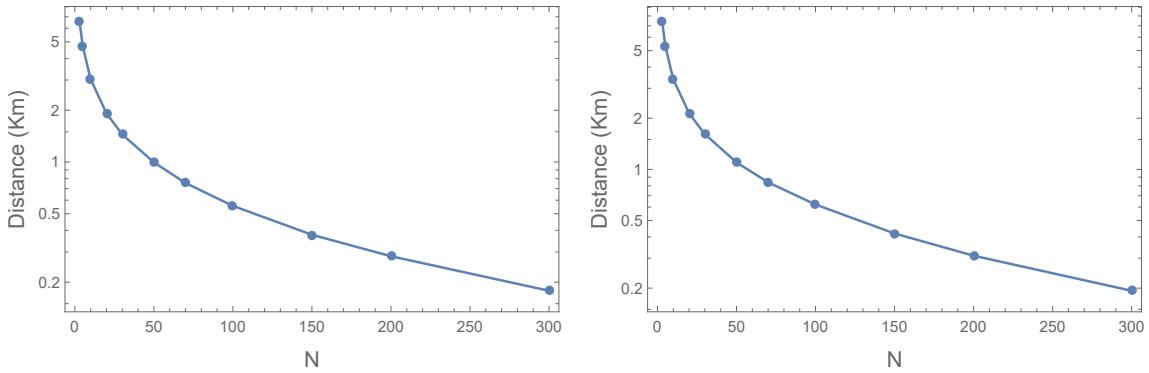

Figure 3. The maximum distance from the source to a user with conferencing key rate $K \to 0$, in terms of different number N of network users. The thermal noise is set to $\bar{n} = 0.05$ in (**a**) and $\bar{n} = 0$ in (**b**), respectively.

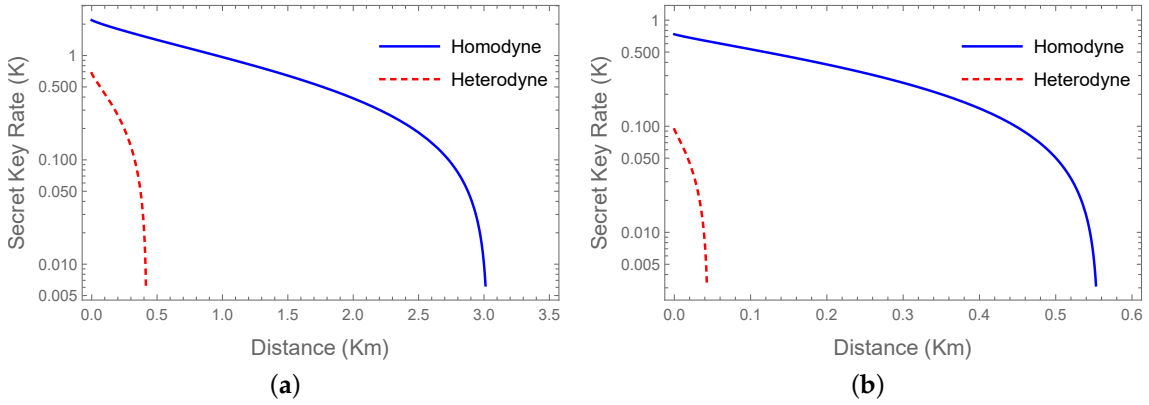

Figure 4. The maximum transmission distance of the network with different detection methods of the users. The number of users is set to 10 in (**a**) and 100 in (**b**), respectively. The blue solid (red dashed) lines show the conferencing key rate when all the users perform homodyne (heterodyne) detection on their received modes.

5. Conclusions

We have proposed a quantum network with entanglement in the middle scheme, which provides secure conferencing communication for an arbitrary number of users. An entanglement source in the middle generates an multipartite GHZ state and distributes each mode of the state to the network users, respectively. The legitimate users receive the entangled modes, and perform homodyne measurement on them to distill mutual information for generating secret conferencing keys for each pair of users. Our security analysis shows that the quantum conferencing scheme can generate secret keys against collective attacks on both the untrusted entangled source and all of the quantum links.

The aim of this paper is to establish a secure conferencing network for dozens of users within a community or a factory area. Simulation results show that our scheme can provide high rate secure conferencing keys for more than 100 users in a quantum network with a radius of hundreds of meters. The security analysis of our scheme is against collective attacks, whereas the analysis against coherent attacks can be achieved by applying a Gaussian de Finetti reduction [20]. Further research should be carried out to establish the finite-size composable security of the quantum conferencing with entanglement in the middle scheme.

Author Contributions: Conceptualization, Z.Z.; Methodology, Z.Z.; Formal Analysis, Z.Z.; Resources, R.S.; Writing—Original Draft Preparation, Z.Z.; Writing—Review and Editing, Y.G.; Visualization, Z.Z.; Supervision, Y.G.; Project Administration, Y.G.; Funding Acquisition, Y.G.

Funding: This research was funded by the National Natural Science Foundation of China (Grant No. 61572529).

Conflicts of Interest: The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum Key Distribution
CV	Continuous Variable
MDI	Measurement-Device-Independent
GHZ	Greenberger–Horne–Zeilinger
CM	Covariance Matrix

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
2. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [CrossRef]
3. Weedbrook, C.; Pirandola, S.; Garcia-Patron, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621. [CrossRef]
4. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
5. Bang, J.Y.; Berger, M.S. Quantum mechanics and the generalized uncertainty principle. *Phys. Rev. D* **2006**, *74*, 125012. [CrossRef]
6. Braunstein, S.L.; Van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513. [CrossRef]
7. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [CrossRef] [PubMed]
8. Weedbrook, C.; Lance, A.M.; Bowen, W.P.; Symul, T.; Ralph, T.C.; Lam, P.K. Quantum cryptography without switching. *Phys. Rev. Lett.* **2004**, *93*, 170504. [CrossRef] [PubMed]
9. Elliott, C. Building the quantum network. *New J. Phys.* **2002**, *4*, 46. [CrossRef]
10. Elliott, C.; Colvin, A.; Pearson, D.; Pikalo, O.; Schlafer, J.; Yeh, H. Current status of the DARPA quantum network. In *Quantum Information and Computation III*; International Society for Optics and Photonics: Bellingham, WA, USA, 2005; Volume 5815, pp. 138–150.
11. Chen, W.; Han, Z.F.; Zhang, T.; Wen, H.; Yin, Z.Q.; Xu, F.X.; Wu, Q.L.; Liu, Y.; Zhang, Y.; Mo, X.F.; et al. Field experiment on a "star type" metropolitan quantum key distribution network. *IEEE Photon. Technol. Lett.* **2009**, *21*, 575–577. [CrossRef]
12. Poppe, A.; Peev, M.; Maurhart, O. Outline of the SECOQC quantum-key-distribution network in Vienna. *Int. J. Q. Inf.* **2008**, *6*, 209–218. [CrossRef]
13. Peev, M.; Pacher, C.; Alléaume, R.; Barreiro, C.; Bouda, J.; Boxleitner, W.; Debuisschert, T.; Diamanti, E.; Dianati, M.; Dynes, J.; et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **2009**, *11*, 075001. [CrossRef]
14. Biham, E.; Huttner, B.; Mor, T. Quantum cryptographic network based on quantum memories. *Phys. Rev. A* **1996**, *54*, 2651. [CrossRef] [PubMed]
15. Salvail, L.; Peev, M.; Diamanti, E.; Alléaume, R.; Lütkenhaus, N.; Länger, T. Security of trusted repeater quantum key distribution networks. *J. Comput. Secur.* **2010**, *18*, 61–87. [CrossRef]
16. Weedbrook, C. Continuous-variable quantum key distribution with entanglement in the middle. *Phys. Rev. A* **2013**, *87*, 022308. [CrossRef]
17. Guo, Y.; Liao, Q.; Wang, Y.; Huang, D.; Huang, P.; Zeng, G. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction. *Phys. Rev. A* **2017**, *95*, 032304. [CrossRef]

18. Zhang, Z.; Shi, R.; Zeng, G.; Guo, Y. Coherent attacking continuous-variable quantum key distribution with entanglement in the middle. *Q. Inf. Process.* **2018**, *17*, 1–18. [CrossRef]
19. Ottaviani, C.; Lupo, C.; Laurenza, R.; Pirandola, S. High-rate quantum conferencing and secret sharing. *arXiv* **2017**, arXiv:1709.06988.
20. Lupo, C.; Ottaviani, C.; Papanastasiou, P.; Pirandola, S. Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks. *Phys. Rev. A* **2018**, *97*, 052327. [CrossRef]
21. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. *Nat. Photon.* **2015**, *9*, 397. [CrossRef]
22. Garcia-Patron, R.; Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503. [CrossRef] [PubMed]
23. Pirandola, S.; Braunstein, S.L.; Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **2008**, *101*, 200504. [CrossRef] [PubMed]
24. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501. [CrossRef] [PubMed]
25. Simon, R.; Chaturvedi, S.; Srinivasan, V. Congruences and canonical forms for a positive matrix: Application to the Schweinler–Wigner extremum principle. *J. Math. Phys.* **1999**, *40*, 3632–3642. [CrossRef]
26. Nicolas, C.; SANCHEZ, R.G.P. Quantum Information with Optical Continuous Variables: From Bell Tests to Key Distribution. Ph.D. Thesis, Université Libre de Bruxelles, Bruxelles, Belgium, 2007.
27. Wang, C.; Huang, D.; Huang, P.; Lin, D.; Peng, J.; Zeng, G. 25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel. *Sci. Rep.* **2015**, *5*, 14607. [CrossRef] [PubMed]