Research Article Vol. 11, No. 4 / April 2023 / Photonics Research 533

PHOTONICS Research

Continuous variable quantum conference network with a Greenberger–Horne–Zeilinger entangled state

Yue Qin,[1] Jingxu Ma,[1] Di Zhao,[1] Jialin Cheng,[1] Zhihui Yan,[1,2] and Xiaojun Jia[1,2,*]

[1]State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China
[2]Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China
*Corresponding author: jiaxj@sxu.edu.cn

Received 17 November 2022; revised 25 January 2023; accepted 31 January 2023; posted 1 February 2023 (Doc. ID 481168); published 9 March 2023

Quantum conference (QC) is a cryptographic task in secure communications that involves more than two users wishing to establish identical secret keys among N users. The Greenberger–Horne–Zeilinger (GHZ) entangled state is the basic resource for quantum cryptographic communication due to the existence of multipartite quantum correlations. An unconditional and efficient quantum network can be established with a continuous variable (CV) GHZ entangled state because of its deterministic entanglement. Here, we report an implementation of QC scheme using a CV multipartite GHZ entangled state. The submodes of a quadripartite GHZ entangled state are distributed to four spatially separated users. The proposed QC scheme is proved to be secure even when the entanglement is distributed through lossy quantum channels and the collective Gaussian attacks are in the all lossy channels. The presented QC scheme has the capability to be directly extended to a larger scale quantum network by using entangled states with more submodes.

https://doi.org/10.1364/PRJ.481168

1. INTRODUCTION

In order to meet the requirements of multiple users for secure communication services at the same time, quantum communication is gradually moving toward the direction of a network. A large-scale quantum communication network is used for distributing entangled qubits in a multipartite communication scheme for further quantum communication and quantum information processing tasks. The development of a quantum conference (QC) network tends to use heterogeneous networks capable of simultaneous data transmission between nodes connected via different types of channels, such as free space and fibers. The free-space channel loss consists of atmospheric absorption, Rayleigh scattering, and geometric loss [1]. The noise in fibers includes guided acoustic wave Brillouin scattering, Rayleigh scattering, and Raman scattering [2,3]. The existing quantum communication scheme uses a single optical medium and needs a trusted node to achieve a corresponding task in which messages at the source node can be transmitted to the user node with the help of a quantum link. The point-to-point quantum communication is established by using several bipartite quantum key distribution (QKD) links. Most implementations and protocols of QKD are limited to two communicating parties; thus the practical applicability is curtailed. The difficulty of scaling the standard two-user QKD protocols to multiple users has limited the large-scale adoption of quantum communication [4]. In contrast, the QC network is characterized for distributing multiple qubits or entangled states to N target users connected via quantum channels directly [5]. Entanglement represents a unique resource in the QC scheme, which provides certifiable security for information transmission and allows the users to broadcast secure messages in a network. The QC enables multipartite users to simultaneously entangle multiple nodes in an arbitrary network [6], which opens up new avenues for reliable and high-performance multipartite communications. The ultimate goal of QC protocols is to enable widespread connectivity; thus a quantum network must be scalable [4]. The feasibility and construction of a QC can be fully researched theoretically [7]. In a practical scheme, the basis of QC is to introduce multipartite entanglement sources rather than establishing high-quality pairwise entanglements among the users, which would necessarily complicate the overall network setup. A QC with a genuine multipartite entangled state may offer advantages over the bipartite case, which allows secure interactions between arbitrary participating users [8], saves the quantum resources [9], and performs fewer rounds of error correction as well as privacy amplification steps [10,11]. By performing QC with multipartite entangled states, the higher key rate and longer transmission distance can be obtained for which the QC protocol can fully

utilize and benefit from the quantum network, while the bipartite protocol cannot [11–14]. It is more adaptable to high-loss scenarios and possesses higher security against attacks than the bipartite protocol [15]. In addition, the scale of the QC scheme can be arbitrarily expanded by using multipartite entangled state resources, which paves the way toward a large-scale quantum network.

Almost all general quantum information tasks can be performed easily based on a near-future quantum network [16–21]. The main built-in feature of quantum information processing's applications is to provide additional security and privacy for communication [16]. Numerous applications of quantum communication have been performed since the emergence of quantum communication, such as QKD [3,22–26], quantum secure direct communication [27–30], quantum teleportation [2,31–36], quantum secret sharing [37–40], quantum random number generators [41,42], and QC [43,44]. It has been proved that the exploitation of CV entangled states of light is beneficial for various kinds of quantum information processing and communication. Cryptographic applications based on multipartite entanglement provide common information for multiusers [45]. There are many different types of CV entanglement systems that have been studied over the past years [46–48]. The CV multipartite entanglement can be generated with the relatively simple experimental schemes [49]. With the diversification of CV entangled states, more complicated quantum communication networks arise. The QC network is the task of extending QKD to the multipartite scenario [43,44]. Recently, two experimental schemes of QC were performed [50]. (1) All users prepare a bipartite entangled state, respectively. They hold one mode and send the other mode to a communal detection part. (2) All users share a genuine multipartite entangled state at once. It was proved that the multipartite case offers advantages over the bipartite case [8,11,51–53].

In a QC network, generating secret keys is of tremendous importance for users that want to keep their shared key secret. We present a general QC protocol under realistic multiple-user scenarios. As the existence of genuine multipartite quantum correlations can bring some advantages to multipartite tasks [7], using CV multipartite entanglement can implement the QC protocols with better performance. The protocol is based on the shared multipartite entangled state, which is a more efficient resource compared to the bipartite entangled resource. It is in fact feasible to establish the necessary entanglement between multiple legal participants, using an entangled state shared by users through the quantum network. Our QC protocol can establish a secret key among the multiple participants. There are N participants named as Bob_j $(j = 1, 2, \ldots, N)$, and the N participants constitute the entire communication network, which are notified through the QC protocol where the multipartite entangled state is shared between the N parties, as shown in Fig. 1. On this basis, the multipartite CV QC with entanglement source is proposed for providing secure key generation of legitimate users against collective Gaussian attacks on the quantum links. We analyze the most realistic security of QC against the collective Gaussian attacks. The attack involving the lossy channels is the most general eavesdropping strategy [54,55] for such a quantum network. In quantum channels, the four submodes from the source interact with an ensemble of ancillary thermal states. The optimal collective attack reduces to a Gaussian attack that is completely characterized by the covariance matrix (CM) of the quadratures observed by the users [56].

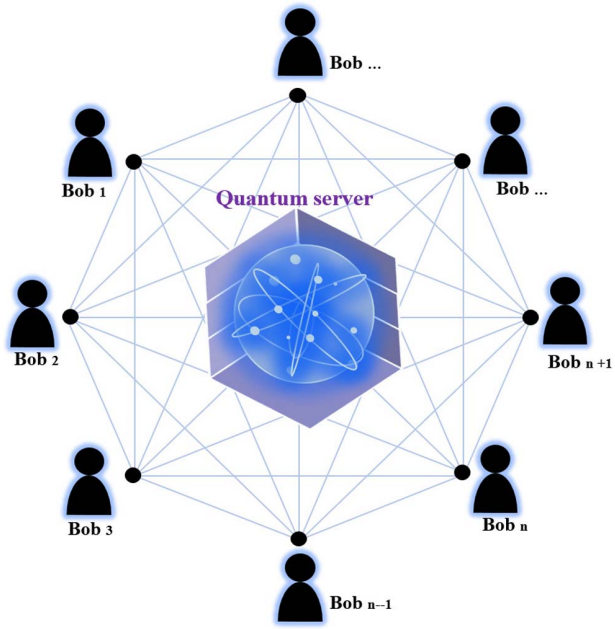

Fig. 1. Visualization of QC protocol. A quantum server distributes the entangled state to all legitimate participants. They establish a common key based on multipartite quantum correlations. The N participants are notified through the QC protocol, where N participants are named as Bob_j $(j = 1, 2, \ldots, N)$.

2. PRINCIPLE AND EXPERIMENTAL SETUP

The basic quantum resource used in the experiment is the Greenberger–Horne–Zeilinger (GHZ) entangled state of light. The CV quadripartite GHZ state is generated by using two identical nondegenerate optical parametric amplifiers (NOPAs). The entangled modes transmitted through the lossy channels are received and measured by the legitimate users Bob_{1-4}. With the homodyne detections of the Bobs' received modes and the postprocessing procedures, the participants share secret keys among themselves based on the quantum correlations. Experiment results show that our scheme can establish a secure conference.

In the experiment, we present the QC protocol among four legitimate users $\mathrm{Bob}_{1,2,3,4}$, who own optical mode $\hat{b}_{1,2,3,4}$, respectively. The quantum server prepares a quadripartite GHZ entangled state; then the entangled modes travel through lossy channels toward the legitimate users $\mathrm{Bob}_{1,2,3,4}$, respectively. These users perform homodyne detections on the quadrature amplitude $(\hat{x})$ and quadrature phase $(\hat{p})$ measurement of the received modes, respectively. The quadrature amplitudes $\hat{x}_{a_i}$ and phase $\hat{p}_{a_i}$ of the four squeezed modes $\hat{a}_i$ $(i = 1, 2, 3, 4)$ are expressed by $\hat{x}_{a_{1(4)}} = e^{r}\hat{x}^{(0)}_{1(4)}$, $\hat{p}_{a_{1(4)}} = e^{-r}\hat{p}^{(0)}_{1(4)}$, $\hat{x}_{a_{2(3)}} = e^{-r}\hat{x}^{(0)}_{2(3)}$, and $\hat{p}_{a_{2(3)}} = e^{r}\hat{p}^{(0)}_{2(3)}$. Here, r is the squeezing parameter, and $\hat{x}^{(0)}_i$

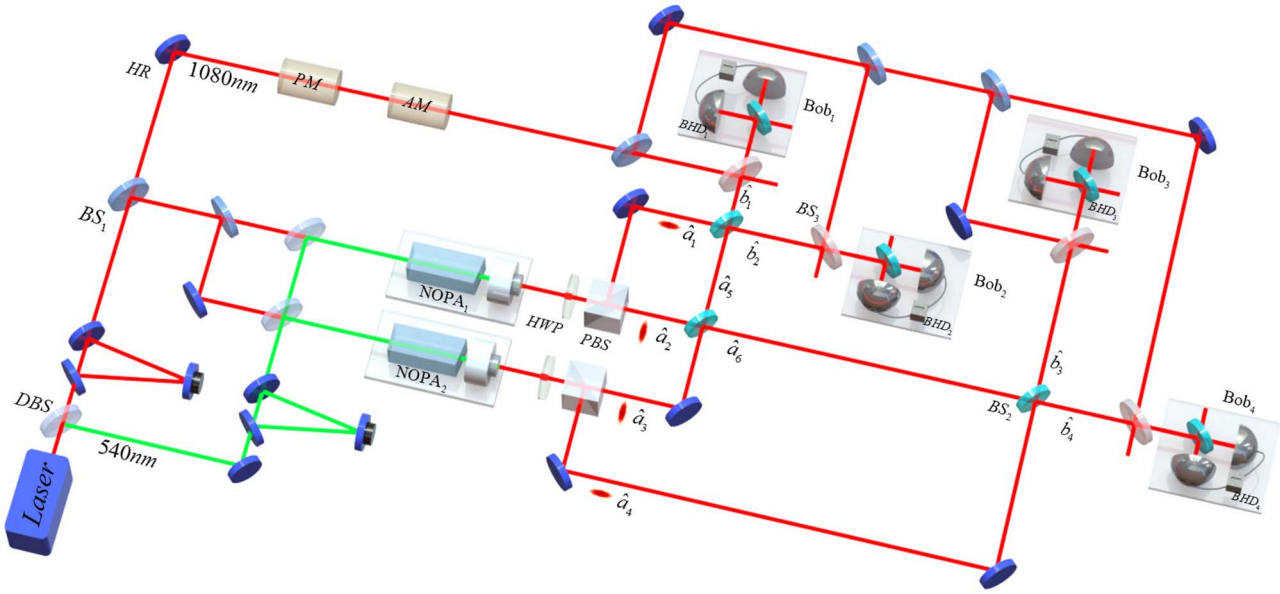

Fig. 2. Schematic of the experimental setup. $NOPA_{1,2}$, nondegenerate optical parametric amplifier; PM, phase modulator; AM, amplitude modulator; $HWP_{1,2}$, half-wave plate; $PBS_{1,2}$, polarizing optical beam splitter; DBS, dichroic beam splitter; BS_1, 90/10 optical beam splitter; BS_2, 50/50 optical beam splitter; BS_3, 80/20 (90/10) optical beam splitter; HR, mirror with high reflection; BHD_{1-4}, balanced homodyne detector. $(\hat{a}_1, \hat{a}_4)$ and $(\hat{a}_2, \hat{a}_3)$ are phase-quadrature and amplitude-quadrature squeezed states, respectively. $\hat{b}_1, \hat{b}_2, \hat{b}_3$, and $\hat{b}_4$ combine a quadripartite GHZ state.

and $\hat{p}_i^{(0)}$ denote the quadrature amplitudes and phases of the initial injected signal fields into NOPA. It has been theoretically demonstrated in Ref. [49] that the four submodes $\hat{b}_i$ are in the GHZ state if the interfering modes $\hat{a}_2$ and $\hat{a}_3$ with the phase difference of $\pi/2$, and the phase differences of $\hat{a}_1$ and $\hat{a}_5$, $\hat{a}_4$ and $\hat{a}_6$ are both controlled at 0, as shown in Fig. 2. Using the GHZ entangled state, the four submodes are expressed by $\hat{b}_1 = -\frac{1}{\sqrt{2}}\hat{a}_1 + \frac{1}{2}\hat{a}_3 + \frac{1}{2}i\hat{a}_2$, $\hat{b}_2 = \frac{1}{\sqrt{2}}\hat{a}_1 + \frac{1}{2}\hat{a}_3 + \frac{1}{2}i\hat{a}_2$, $\hat{b}_3 = \frac{1}{\sqrt{2}}\hat{a}_4 + \frac{1}{2}\hat{a}_3 - \frac{1}{2}i\hat{a}_2$, and $\hat{b}_4 = -\frac{1}{\sqrt{2}}\hat{a}_4 + \frac{1}{2}\hat{a}_3 - \frac{1}{2}i\hat{a}_2$. Here, the quantum state submodes $\hat{b}_j\,(j = 1, 2, 3, 4)$ can be expressed in terms of the electromagnetic field annihilation operator $\hat{a} = (\hat{x} + i\hat{p})/2$, where quadrature amplitude $(\hat{x})$ and quadrature phase $(\hat{p})$ with the canonical commutation relation $[\hat{x}, \hat{p}] = 2i$. Owing to the quadripartite CV GHZ entangled state, the conference secret can be shared among all users. Eve controls the lossy channels from the source to all legitimate users with a beam splitter (BS_3). The lossy channel is characterized by the transmission efficiency η. In order to perform the collective Gaussian attacks, Eve prepares and injects thermal states ρ_E into the channel, which are interfered by four BSs with the submodes of the GHZ entangled state; the output modes of all BS_3 are, respectively, received by $Bob_{1,2,3,4}$. Users perform homodyne detections on the $\hat{x}(\hat{p})$-quadratures and the cross correlations of the received modes. The elements of the output modes' CM can be calculated by the variances of the quadratures and cross correlations,

$$\mathrm{COV}(\hat{O}_1, \hat{O}_2) = \frac{1}{2}[\Delta^2(\hat{O}_1 + \hat{O}_2) - \Delta^2\hat{O}_1 - \Delta^2\hat{O}_2]. \quad (1)$$

The generated GHZ entangled state ρ_B is sent to the Bobs via the unsafe channels. Eve combines submodes of GHZ entanglement ρ_B and the ancillary state ρ_E in the lossy channels. The variance of Eve's ancillary modes of state ρ_E is ω. The transmittance η of the lossy channels is the same. In the lossy channel, the entangled submodes and thermal states are coupled via BS_3. In this case, the output modes are $\hat{b}_j' = \sqrt{\eta}\hat{b}_j - \sqrt{1-\eta}\hat{\nu}_j$, where $\hat{\nu}_j$ represents the thermal noise in the quantum channel. Combining Eq. (1), the CM of the Bobs' received modes $\rho_{B|E}$ can be calculated as follows:

$$V_B = \begin{pmatrix} \Lambda & \Gamma & \Gamma & \Gamma \\ \Gamma & \Lambda & \Gamma & \Gamma \\ \Gamma & \Gamma & \Lambda & \Gamma \\ \Gamma & \Gamma & \Gamma & \Lambda \end{pmatrix}. \quad (2)$$

The resulting state $\rho_{B|E}$ is symmetric under permutation of the Bobs' modes, and the correlations between any pair of modes should be the same. It is easy to write the CM of ith and jth Bobs' modes as

$$V_{B_iB_j} = \begin{pmatrix} \Lambda & \Gamma \\ \Gamma & \Lambda \end{pmatrix},$$

$$\Lambda = \begin{pmatrix} \frac{1}{4}(e^{-2r} + 3e^{2r+2r'})\eta + (1-\eta)\omega & 0 \\ 0 & \frac{1}{4}(3e^{-2r} + e^{2r+2r'})\eta + (1-\eta)\omega \end{pmatrix},$$

$$\Gamma = \begin{pmatrix} \frac{1}{4}(e^{-2r} - e^{2r+2r'})\eta & 0 \\ 0 & \frac{1}{4}(-e^{-2r} + e^{2r+2r'})\eta \end{pmatrix}. \quad (3)$$

Figure 2 shows the schematic of the experimental setup. A dual-wavelength laser at 540 and 1080 nm is used for the pump fields and the injected signals of the two NOPAs, respectively. The two NOPAs are constructed in an identical configuration, which consists of a half-monolithic optical cavity and an α-cut nonlinear $KTiOPO_4$ (KTP) crystal. The 540 nm laser is employed to pump the nonlinear resonator. Both NOPAs operate below threshold to generate four quadrature squeezed states through the intracavity frequency downconversion process [57]. To generate a CV quadripartite GHZ state, we first prepare two amplitude-quadrature squeezed states and two phase-quadrature squeezed states. Then, by locking the relative phases of these optical submodes under certain phase relations, the resultant modes form the quadripartite GHZ state [49]. The output optical fields are distributed to legitimate users $Bob_{1,2,3,4}$ through lossy channels. For measuring the fluctuation variances of the amplitude or phase quadratures of the corresponding mode $\hat{b}_j'$, the user's modes are detected by the four sets of the balanced homodyne detectors (BHDs) in which all needed local oscillators (LOs) at 1080 nm are deriving from the laser. When the relative phase between the signal beam and the corresponding LO in the BHD is locking at 0 or $\pi/2$, the measured photocurrent variances of the respective modes are combined by positive (+) or negative (−) power combiners, according to the different correlation variances, which are measured and recorded by a spectrum analyzer (SA).

The QC relies on the quantum correlations of the CV multipartite GHZ entangled state. In order to simplify the experimental preparation of the GHZ state, the four quadrature squeezed states need same squeezing parameter r and anti-squeezing parameter $r + r'$, where r' is the extra noise factor. The parameters r and $r + r'$ depend on the strength of the parametric deamplification and the intracavity losses in NOPA, respectively [49,57], so two NOPAs need to be constructed in identical configuration. The experimentally measured squeezing degrees and anti-squeezing degrees of the output fields from NOPA1 and NOPA2 equal 4.2 dB below the shot noise limit (SNL) and 9.2 dB above the SNL (the corresponding squeezing parameter r and the extra noise factor r' equal 0.46 and 0.58, respectively).

3. RESULTS

We consider the Gaussian attacks on the QC with the quadripartite GHZ state and give the simulation results of our security analysis. The ith Bob performs homodyne detection on the $\hat{x}$ (or $\hat{p}$)-quadrature of his mode $\hat{b}_i'$. Thus, the mode $\hat{b}_j'$ of the jth Bob is mapped into a Gaussian state with CM $V_{B_iB_j}$ that can be calculated [58–61]. Then the mutual information $I(B_i{:}B_j)$ between the two Bobs can be estimated. Similarly, we can calculate the Holevo bound $H(E{:}B_i)$ between eavesdropper Eve and the ith Bob when Eve performs a collective Gaussian attack [56,62,63] in lossy channels. Different conditions of transmission efficiency of the quantum channel and thermal noises are taken into account. For a given value of thermal noise variance ω, Eve's CM is determined by the parameters η, r, and r'. In order to simplify the analysis and design, we consider a symmetric configuration of the QC scheme in which all lossy channels have the same transmission efficiency η. In the following

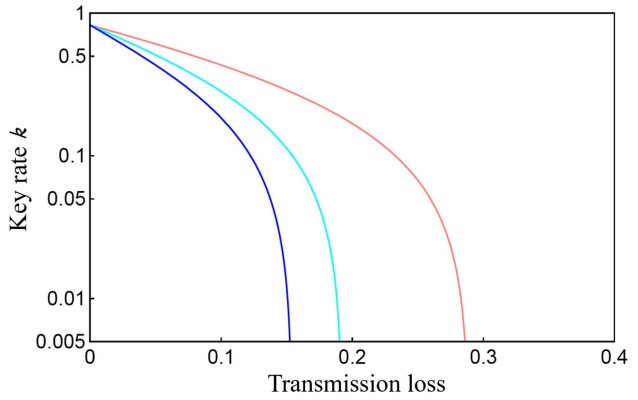

Fig. 3. Calculated key rate k of the CV QC system versus the transmission loss when the thermal noise variances are taken as $\omega = 1.5$ (red line), $\omega = 3.5$ (cyan line), and $\omega = 5.5$ (blue line), respectively.

simulation, we show the relationship between the secret key rate k in the QC and the transmission loss $1 - \eta$ when $r = 0.46, r' = 0.58$ in Fig. 3, where the variances of thermal states are taken as 1.5, 3.5, and 5.5, respectively. Three cases of different thermal noises are analyzed. Regarding the key rate k of the QC, it was shown that, even though the QC protocol can tolerate higher noise, the QC protocol shows better performance for the low-noise case.

Figure 4 presents the theoretical results of the QC key rate k as functions of the transmission loss of the lossy channels for different squeezing factor r and the extra noise factor r', where r' equals r. We choose three kinds of status to analyze the relationship between the k and r; the red, green, and blue traces correspond to squeezing factors $r = 0.46, 0.92,$ and 1.38 in Fig. 4. The key rate can be improved and QC presents the stronger resistance to the loss of the lossy channels with the increasing squeezing parameter r. To attain a high secret key rate, the high-quality CV GHZ entanglement is necessary.

In the experiment, the achievable QC key rate is limited by the squeezing factor r and extra noise factor r' of the GHZ entangled state. In order to demonstrate the QC key rate as a function of the transmission loss of lossy channels, two

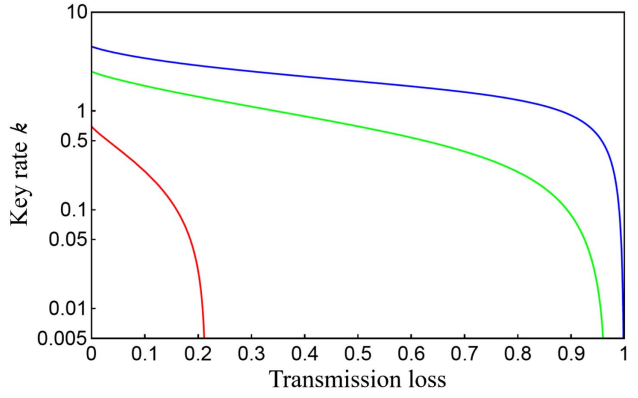

Fig. 4. Calculated dependences of the key rate k on the transmission loss for different squeezing factors r and the extra noise factor r'. The red, green, and blue traces correspond to squeezing factors r of 0.46, 0.92, and 1.38 when r' equals r, respectively.

different transmission efficiencies η are investigated, $\eta = 0.9$ and $\eta = 0.8$. The experimentally measured squeezing and antisqueezing degrees of the squeezed states equal 4.2 dB below the SNL and 9.2 dB above the SNL. The CM V_B of the output modes are obtained from local measurements. All the variances of the amplitude and phase quadratures and the cross correlation are measured. Figure 5 shows that some of the measured variances of the amplitude and phase quadratures and the cross correlation variances of the Bobs' received modes $\hat{b}_j'$ when $1-\eta = 0.1$ and $1-\eta = 0.2$ at the analysis frequency of 3 MHz, respectively. The measured variances of $\Delta^2\hat{x}_{B_1}$, $\Delta^2\hat{x}_{B_2}$, $\Delta^2\hat{p}_{B_1}$, $\Delta^2\hat{p}_{B_2}$, $\Delta^2(\hat{x}_{B_1}+\hat{x}_{B_2})$, and $\Delta^2(\hat{p}_{B_1}+\hat{p}_{B_2})$ are 6.50 ± 0.12 dB, 6.40 ± 0.11 dB, 2.57 ± 0.12 dB, 2.55 ± 0.10 dB, 5.14 ± 0.11 dB, and 5.14 ± 0.12 dB above the SNL when $1-\eta = 0.1$, respectively. The measured variances of $\Delta^2\hat{x}_{B_1}$, $\Delta^2\hat{x}_{B_2}$, $\Delta^2\hat{p}_{B_1}$, $\Delta^2\hat{p}_{B_2}$, $\Delta^2(\hat{x}_{B_1}+\hat{x}_{B_2})$, and $\Delta^2(\hat{p}_{B_1}+\hat{p}_{B_2})$ are 6.25 ± 0.10 dB, 6.20 ± 0.10 dB, 2.45 ± 0.11 dB, 2.42 ± 0.10 dB, 4.66 ± 0.10 dB, and 4.75 ± 0.10 dB above the SNL when $1-\eta = 0.2$, respectively. The resolution bandwidth (RBW) and the video bandwidth (VBW) of the SA are set at 30 kHz and 30 Hz, respectively. From the measured results shown in Fig. 5, we can calculate the CM $V_{B_1B_2}$. According to all the measurements, we can calculate the key rates as $0.55\pm0.11, 0.15\pm0.03$ when $1-\eta = 0.9, 1-\eta = 0.8$, respectively. The simulation results of our security analysis and the experiment result are plotted in Fig. 6.

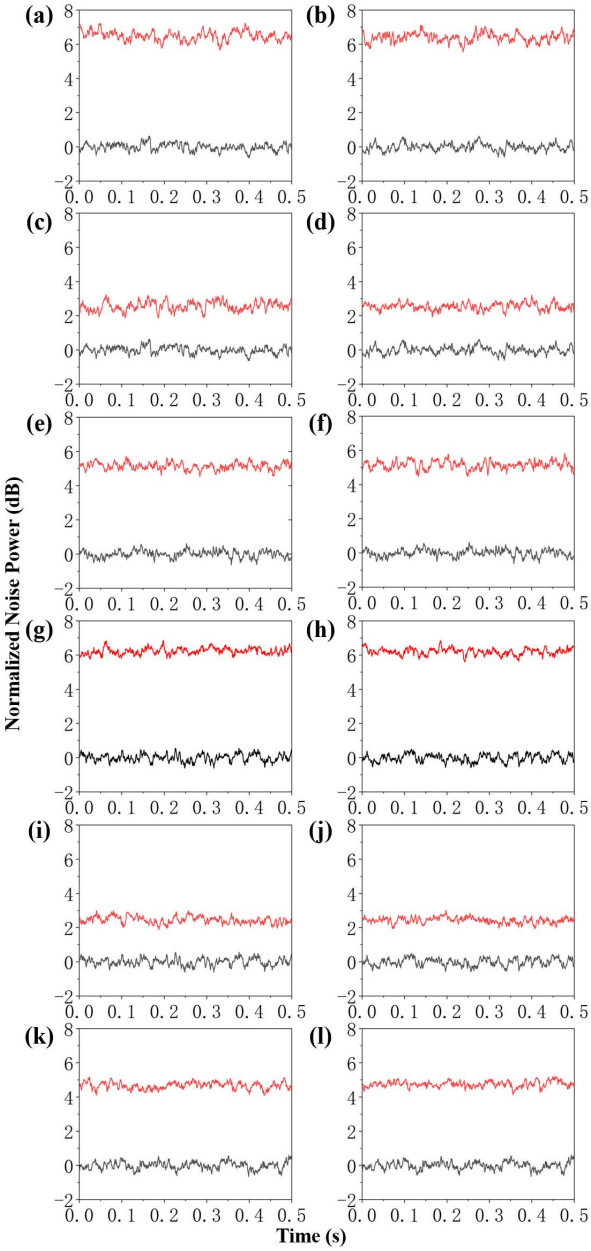

Fig. 5. Measured variances of the amplitude and phase quadratures and the cross correlation variances of the Bobs' received modes $\hat{b}_j'$ when (a)–(f) $1-\eta = 0.1$ and (g)–(l) $1-\eta = 0.2$, respectively. (a), (g) $\Delta^2\hat{x}_{B_1}$; (b), (h) $\Delta^2\hat{x}_{B_2}$; (c), (i) $\Delta^2\hat{p}_{B_1}$; (d), (j) $\Delta^2\hat{p}_{B_2}$; (e), (k) $\Delta^2(\hat{x}_{B_1}+\hat{x}_{B_2})$; (f), (l) $\Delta^2(\hat{p}_{B_1}+\hat{p}_{B_2})$. The black and red lines correspond to the SNL and corresponding noise power, respectively. The analysis frequency is 3 MHz and the measurement parameters of the SA: RBW 30 kHz; VBW 30 Hz.

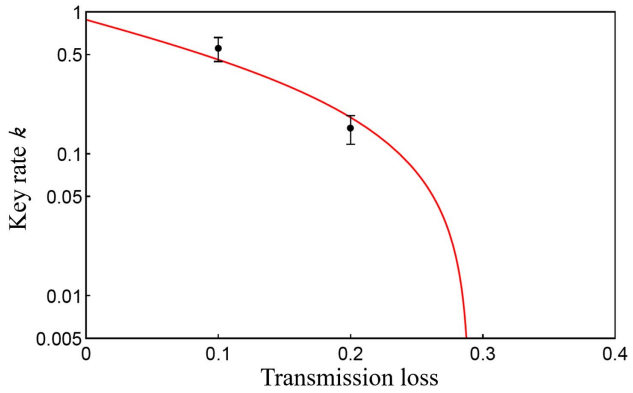

Fig. 6. Calculated key rate k and experiment result versus transmission loss. Two different transmission losses of the lossy channels are investigated, $1-\eta = 0.1$ and $1-\eta = 0.2$. Using the experimentally determined parameters $r = 0.46$ and $r' = 0.58$, the red trace curves the theoretical result of the QC key rate versus transmission loss, while the data points are numerically calculated key rate k from experimentally obtained CM V_B.

4. CONCLUSION

In summary, we have experimentally demonstrated a CV QC system based on a GHZ entangled state. The aim is to establish a secure, high-speed QC network for multiple users within a community. Encouragingly, the performance of the current QC system can be improved further by improving the degree of entanglement of the GHZ source [44]. The security against the collective Gaussian attacks is analyzed; this protocol presents excellent robustness to the terrible condition of the lossy channel. In practical applications, developing long-distance QC protocols resistant to losses and noise is of great importance. Owing to the better efficiency of homodyne detection over single-photon counting, a higher secret key rate is obtained in the short distance with the CV system. However, the classical postprocessing of the data is a task far more complicated than its discrete counterpart [64]. Hybrid quantum information processing takes advantages of both discrete

variable (DV) and CV systems to implement quantum information processing [65]. A hybrid QC network can be proposed in which the CV system is used to establish metropolitan communication networks and the DV system is used to connect metropolitan networks. The hybrid QC network takes advantage of high secret key rates for CV systems and long distance for DV systems. Of course, the hybrid QC network makes it possible to distill secret keys over much longer distances. When a GHZ state with more submodes is available, the presented QC scheme can be directly extended to larger systems with many more users. Further research should be carried out to establish a more complex QC network based on the large-scale CV GHZ state [44,54,66].

APPENDIX A: KEY RATE OF QC

To study the QC network of multipartite entanglement under transmission losses, the lossy channel for all submodes is simulated using BS_3. The output mode is given by $\hat{b}_j' = \sqrt{\eta}\hat{b}_j - \sqrt{1-\eta}\hat{v}_j$, where η and $\hat{v}_j$ represent the transmission efficiency of the quantum channel and the thermal noise in the quantum channel, respectively, as shown in Fig. 2.

In the QC, we consider the case where any Bob_j wants to share his secret message with other Bobs. To achieve this, Bob_1 needs to share secret keys with $\mathrm{Bob}_{2,3,4}$, respectively. The corresponding secret key rate of our QC is given by

$$K_{\mathrm{Rate}} = I(B_i{:}B_j) - H(E{:}B_j). \tag{A1}$$

The information obtained by the legitimate user B_j $(j = 1, 2, 3, 4)$ is quantified by the mutual information $I(B_i{:}B_j)$, between two users B_i and B_j. The mutual information is defined by $I(B_i{:}B_j) = H(B_i) - H(B_i|B_j)$, where $H(B_i)$ and $H(B_i|B_j)$ are the Shannon entropy of measurement of variables B_i and the conditional entropy of B_i conditioned on the knowledge of B_j, respectively [67,68]. $I(B_i{:}B_j)$ represents the Shannon mutual information between the measurement results of the ith and jth Bobs, given by

$$I(B_i{:}B_j) = \frac{1}{2}\log_2\frac{\Lambda^p}{V^p_{B_i|B_j}}, \tag{A2}$$

where Λ^p is the variance of the $\hat{p}$-quadrature measured by the ith Bob, and $V^p_{B_i|B_j}$ denotes the conditional variance of the ith Bob B_i after the jth Bob B_j homodyne detections on the $\hat{p}$-quadrature. The conditional CM of the users B_i and B_j after homodyne detection is given by $V_{B_i|B_j} = \Lambda - \Gamma(\Pi\Lambda\Pi)^{-1}\Gamma^T$, where $\Pi = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

The collective Gaussian attacks are shown to be the optimal attack strategy against our protocol. Eve prepares four Gaussian thermal states as ancillary states, and injects them into the lossy channels through BS_3, respectively. The transmitted entanglement modes coming out of the BS_3 and the partial ancillary states are send to legitimate users. The remaining states are all stored in Eve's quantum memory.

Use the ith Bob's mode as a reference, the eavesdropper Eve can implement an optimal measurement in the quantum memory to obtain maximal information. The information that Eve can obtain is quantified by the Holevo bound $H(E{:}B_i)$. The Holevo bound between Bob's data and Eve's states is given by $H(E{:}B_i) = S(\rho_E) - S(\rho_{E|B_i})$, where $S(\rho)$ denotes the von Neumann entropy of the quantum state ρ, ρ_E denotes the Eve's quantum state, and conditional state $\rho_{E|B_i}$ represents Eve's quantum state after the ith Bob's homodyne detection results. As the CV GHZ state is Gaussian, the state Eve can eavesdrop is also Gaussian. The von Neumann entropy $S(\rho)$ of a Gaussian state ρ can be written as

$$S(\rho) = \sum_{k=1}^{N} g(\nu_k), \tag{A3}$$

where

$$g(x) := \left(\frac{x+1}{2}\right)\log\left(\frac{x+1}{2}\right) - \left(\frac{x-1}{2}\right)\log\left(\frac{x-1}{2}\right). \tag{A4}$$

Here, ν_k represents the symplectic eigenvalues of the CM, which is the eigenvalues of the Williamson normal form $|I\Omega V|$ [69,70], where I is the imaginary unit and Ω is the symplectic form $\Omega = \bigoplus_{i=1}^{N}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Gaussian attacks turn out to be optimal for these protocols, which minimize the bounds on the key rate [62]. The collective Gaussian attacks [56,62,71] provide a powerful tool to estimate the Holevo bound using the CM formalism. The conditional CM $V_{E|B_i}$ denotes the conditional variance of Eve's modes after the ith Bob performs homodyne detection on his mode. To compute the CM $V_{E|B_i}$, we need to construct the CM V_{EB_i} in the following matrix:

$$V_{EB_i} = \begin{pmatrix} V_E & V_{eB_i} \\ V_{eB_i}^T & V_{B_i} \end{pmatrix}. \tag{A5}$$

The quadrature vectors $\hat{x}$ and $\hat{p}$ of ρ_E are denoted as $\hat{O}_E = (\hat{x}_{e_1}, \hat{p}_{e_1}, \hat{x}_{e_2}, \hat{p}_{e_2}, \hat{x}_{e_3}, \hat{p}_{e_3}, \hat{x}_{e_4}, \hat{p}_{e_4})^T$, where $\hat{x}(\hat{p})_{e_i}$ describes the eavesdropper Eve's modes of stolen information from the ith Bob, V_{B_i} describes the mode of the ith Bob, and V_{eB_i} describes the relations between the above two blocks. After the homodyne detection on the $\hat{x}$ $(\hat{p})$-quadrature of the ith Bob's mode, the conditional CM $V_{E|B_i}$ is given by

$$V_{E|B_i} = V_E - V_{eB_i}(\Pi V_{B_i}\Pi)^{-1}V_{eB_i}^T. \tag{A6}$$

We derive the four degenerate symplectic eigenvalues of V_E, which are given by ν_1. The von Neumann entropy $S(\rho_E)$ is generated from the four symplectic eigenvalues ν_1 by the following equation:

$$S(\rho_E) = 4g(\nu_1). \tag{A7}$$

Similarly, we compute the symplectic spectrum of the conditional CM $V_{E|B_i}$, which contains three identical symplectic eigenvalues given by ν_1, and one given by ν_2. The conditional von Neumann entropy $S(\rho_{E|B_i})$ is given by

$$S(\rho_{E|B_i}) = 3g(\nu_1) + g(\nu_2). \tag{A8}$$

Then, the Holevo bound $H(E{:}B_i)$ can be written as the following equation:

$$H(E{:}B_i) = g(\nu_1) - g(\nu_2). \tag{A9}$$

With the results in Eq. (A2) and Eq. (A9), the corresponding secret key rate of our QC can be calculated.

Funding. National Natural Science Foundation of China (61925503, 62122044, 62135008, 12147215, 11834010); Program for the Innovative Talents of Higher Education Institutions of Shanxi; Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi; Fund for Shanxi "1331 Project" Key Subjects Construction.

Disclosures. The authors declare no conflicts of interest.

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
2. M. Huo, J. Qin, J. Cheng, Z. Yan, Z. Qin, X. Su, X. Jia, C. Xie, and K. Peng, "Deterministic quantum teleportation through fiber channels," Sci. Adv. **4**, eaas9401 (2018).
3. N. Wang, S. Du, W. Liu, X. Wang, and K. Peng, "Long-distance continuous-variable quantum key distribution with entangled states," Phys. Rev. Appl. **10**, 064028 (2018).
4. S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, and R. Ursin, "A trusted node–free eight-user metropolitan quantum communication network," Sci. Adv. **6**, eaba0959 (2020).
5. H. V. Nguyen, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, M. A. M. Izhar, S. X. Ng, and L. Hanzo, "Towards the quantum internet: generalised quantum network coding for large-scale quantum communication networks," IEEE Access **5**, 17288–17308 (2017).
6. I. B. Djordjevic, "Surface-codes-based quantum communication networks," Entropy **22**, 1059 (2020).
7. J. Ribeiro, G. Murta, and S. Wehner, "Fully device-independent conference key agreement," Phys. Rev. A **97**, 022307 (2018).
8. G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, "Quantum conference key agreement: a review," Adv. Quantum Technol. **3**, 2000025 (2020).
9. F. Hahn, J. de Jong, and A. Pappa, "Anonymous quantum conference key agreement," PRX Quantum **1**, 020325 (2020).
10. X.-Y. Cao, J. Gu, Y.-S. Lu, H.-L. Yin, and Z.-B. Chen, "Coherent one-way quantum conference key agreement based on twin field," New J. Phys. **23**, 043002 (2021).
11. M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, "Multi-partite entanglement can speed up quantum key distribution in networks," New J. Phys. **19**, 093012 (2017).
12. J.-L. Bai, Y.-M. Xie, Z. Li, H.-L. Yin, and Z.-B. Chen, "Post-matching quantum conference key agreement," Opt. Express **30**, 28865–28881 (2022).
13. X.-Y. Cao, Y.-S. Lu, Z. Li, J. Gu, H.-L. Yin, and Z.-B. Chen, "High key rate quantum conference key agreement with unconditional security," IEEE Access **9**, 128870 (2021).
14. S. Zhao, P. Zeng, W.-F. Cao, X.-Y. Xu, Y.-Z. Zhen, X. Ma, L. Li, N.-L. Liu, and K. Chen, "Phase-matching quantum cryptographic conferencing," Phys. Rev. Appl. **14**, 024010 (2020).
15. F. Grasselli, H. Kampermann, and D. Bruß, "Conference key agreement with single-photon interference," New J. Phys. **21**, 123002 (2019).
16. M. Epping, H. Kampermann, and D. Bruß, "Large-scale quantum networks based on graphs," New J. Phys. **18**, 053036 (2016).
17. F. Hahn, A. Pappa, and J. Eisert, "Quantum network routing and local complementation," npj Quantum Inf. **5**, 76 (2019).
18. A. Pirker, J. Wallnöfer, and W. Dür, "Modular architectures for quantum networks," New J. Phys. **20**, 053054 (2018).
19. V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, and B. P. Lanyon, "Light-matter entanglement over 50 km of optical fibre," npj Quantum Inf. **5**, 72 (2019).
20. A. Tchebotareva, S. Hermans, P. C. Humphreys, D. Voigt, P. J. Harmsma, L. K. Cheng, A. L. Verlaan, N. Dijkhuizen, W. D. Jong, and A. Dreau, "Entanglement between a diamond spin qubit and a photonic time-bin qubit at telecom wavelength," Phys. Rev. Lett. **123**, 063601 (2019).
21. S. K. Liao, W. Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J. G. Ren, and W. Y. Liu, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett. **120**, 030501 (2018).
22. F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," Nature **421**, 238–241 (2003).
23. A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and K. L. Ping, "No-switching quantum key distribution using broadband modulated coherent light," Phys. Rev. Lett. **95**, 180503 (2005).
24. J. Lodewyck, M. Bloch, R. Garciapatron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tuallebrouri, and S. W. Mclaughlin, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," Phys. Rev. A **76**, 042305 (2007).
25. G.-J. Fan-Yuan, F. Lu, S. Wang, Z. Yin, D. He, Z. Zhou, J. Teng, W. Chen, G. Guo, and Z. Han, "Measurement device-independent quantum key distribution for nonstandalone networks," Photon. Res. **9**, 1881–1891 (2021).
26. C. Jiang, X. Hu, Z. Yu, and X. Wang, "Measurement-device-independent quantum key distribution protocol with phase post-selection," Photon. Res. **10**, 1703–1711 (2022).
27. F. G. Deng, G. L. Long, and X. S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," Phys. Rev. A **68**, 113–114 (2003).
28. F. G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," Phys. Rev. A **69**, 052319 (2004).
29. C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," Phys. Rev. A **71**, 044305 (2005).
30. D. Pan, Z. Lin, J. Wu, H. Zhang, Z. Sun, D. Ruan, L. Yin, and G. Long, "Experimental free-space quantum secure direct communication and its security analysis," Photon. Res. **8**, 1522–1531 (2020).
31. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett. **70**, 1895–1899 (1993).
32. S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation," Nat. Photonics **9**, 641–652 (2015).
33. I. Marcikic, H. D. Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, "Long-distance teleportation of qubits at telecommunication wavelengths," Nature **421**, 509–513 (2003).
34. J. Yin, J. Ren, H. Lu, Y. Cao, H. Yong, Y. Wu, C. Liu, S. Liao, F. Zhou, and Y. A. Jiang, "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," Nature **488**, 185–188 (2012).
35. S. Liu, Y. Lou, and J. Jing, "Orbital angular momentum multiplexed deterministic all-optical quantum teleportation," Nat. Commun. **11**, 3875 (2020).
36. Y. Wu, Q. Wang, L. Tian, X. Zhang, J. Wang, S. Shi, Y. Wang, and Y. Zheng, "Multi-channel multiplexing quantum teleportation based on the entangled sideband modes," Photon. Res. **10**, 1909–1914 (2022).
37. Y. Zhou, J. Yu, Z. Yan, X. Jia, J. Zhang, C. Xie, and K. Peng, "Quantum secret sharing among four players using multipartite bound entanglement of an optical field," Phys. Rev. Lett. **121**, 150502 (2018).
38. M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," Phys. Rev. A **59**, 1829–1834 (1999).
39. B. A. Bell, D. Markham, D. Herrera-Martí, A. Marin, and M. S. Tame, "Experimental demonstration of graph-state quantum secret sharing," Nat. Commun. **5**, 5480 (2014).

40. Y. G. Yang, Y. C. Wang, Y. L. Yang, X. B. Chen, D. Li, Y. H. Zhou, and W. M. Shi, "Participant attack on the deterministic measurement-device-independent quantum secret sharing protocol," Sci. China Phys. Mech. Astron. **64**, 260321 (2021).
41. X.-B. An, H.-W. Li, Z.-Q. Yin, M.-J. Hu, W. Huang, B.-J. Xu, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, "Experimental three-party quantum random number generator based on dimension witness violation and weak measurement," Opt. Lett. **43**, 3437–3440 (2018).
42. J. Cheng, J. Qin, S. Liang, J. Li, Z. Yan, X. Jia, and K. Peng, "Mutually testing source-device-independent quantum random number generator," Photon. Res. **10**, 646–652 (2022).
43. Y. Zhao, C. Fung, B. Qi, C. Chen, and H. K. Lo, "Quantum hacking: experimental demonstration of time-shift attack against practical quantum key distribution systems," Phys. Rev. A **78**, 4702–4705 (2007).
44. Y. Wang, C. Tian, Q. Su, M. Wang, and X. Su, "Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state," Sci. China Inf. Sci. **62**, 72501 (2019).
45. K. Chen and H.-K. Lo, "Multi-partite quantum cryptographic protocols with noisy GHz states," arXiv, arXiv quant-ph/0404133 (2004).
46. Z. Qin, M. Gessner, Z. Ren, X. Deng, D. Han, W. Li, X. Su, A. Smerzi, and K. Peng, "Characterizing the multipartite continuous-variable entanglement structure from squeezing coefficients and the Fisher information," npj Quantum Inf. **5**, 3 (2019).
47. S. Li, X. Pan, Y. Ren, H. Liu, S. Yu, and J. Jing, "Deterministic generation of orbital-angular-momentum multiplexed tripartite entanglement," Phys. Rev. Lett. **124**, 083605 (2020).
48. K. Zhang, W. Wang, S. Liu, X. Pan, J. Du, Y. Lou, S. Yu, S. Lv, N. Treps, C. Fabre, and J. Jing, "Reconfigurable hexapartite entanglement by spatially multiplexed four-wave mixing processes," Phys. Rev. Lett. **124**, 090501 (2020).
49. X. Su, A. Tan, X. Jia, J. Zhang, C. Xie, and K. Peng, "Experimental preparation of quadripartite cluster and Greenberger-Horne-Zeilinger entangled states for continuous variables," Phys. Rev. Lett. **98**, 070502 (2007).
50. M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, "Experimental quantum conference key agreement," Sci. Adv. **7**, eabe0395 (2021).
51. P. Singkanipa and P. Kok, "Quantum conference key agreement with photon loss," arXiv, arXiv:2101.01483 (2021).
52. F. Grasselli, H. Kampermann, and D. Bruß, "Finite-key effects in multipartite quantum key distribution protocols," New J. Phys. **20**, 113014 (2018).
53. J. Ribeiro, L. P. Thinh, J. Kaniewski, J. Helsen, and S. Wehner, "Device independence for two-party cryptography and position verification with memoryless devices," Phys. Rev. A **97**, 062307 (2018).
54. Z. Zhang, R. Shi, and Y. Guo, "Multipartite continuous variable quantum conferencing network with entanglement in the middle," Appl. Sci. **8**, 1312 (2018).
55. S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," Nat. Photonics **9**, 397–402 (2015).
56. R. Garcia-Patron and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," Phys. Rev. Lett. **97**, 190503 (2006).
57. Y. Zhou, X. Jia, F. Li, C. Xie, and K. Peng, "Experimental generation of 8.4 dB entangled state with an optical cavity involving a wedged type-II nonlinear crystal," Opt. Express **23**, 4952–4959 (2015).
58. K. Chen and H.-K. Lo, "Conference key agreement and quantum sharing of classical secrets with noisy GHz states," in *Proceedings International Symposium on Information Theory (ISIT)* (IEEE, 2005), pp. 1607–1611.
59. J. Eisert, S. Scheel, and M. B. Plenio, "Distilling Gaussian states with Gaussian operations is impossible," Phys. Rev. Lett. **89**, 137903 (2002).
60. J. Fiurášek, "Gaussian transformations and distillation of entangled Gaussian states," Phys. Rev. Lett. **89**, 137904 (2002).
61. G. Spedalieri, C. Ottaviani, and S. Pirandola, "Covariance matrices under Bell-like detections," Open Syst. Inf. Dyn. **20**, 1350011 (2013).
62. M. Navascués, F. Grosshans, and A. Acin, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," Phys. Rev. Lett. **97**, 190502 (2006).
63. S. Pirandola, S. L. Braunstein, and S. Lloyd, "Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography," Phys. Rev. Lett. **101**, 200504 (2008).
64. A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," Phys. Rev. Lett. **102**, 180504 (2009).
65. U. L. Andersen, J. S. Neergaard-Nielsen, P. Van Loock, and A. Furusawa, "Hybrid discrete-and continuous-variable quantum information," Nat. Phys. **11**, 713–719 (2015).
66. Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, "Continuous-variable measurement-device-independent multipartite quantum communication," Phys. Rev. A **93**, 022325 (2016).
67. C. Weedbrook, S. Pirandola, R. Garca-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621–669 (2012).
68. M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," Phys Today **54**, 60 (2001).
69. R. Simon, S. Chaturvedi, and V. Srinivasan, "Congruences and canonical forms for a positive matrix: application to the Schweinler-Wigner extremum principle," J. Math. Phys. **40**, 3632–3642 (1999).
70. R. Garcia-Patron Sanchez, "Quantum information with optical continuous variables: from Bell tests to key distribution," Ph.D. thesis (Université Libre de Bruxelles, 2007).
71. M. M. Wolf, G. Giedke, and J. I. Cirac, "Extremality of Gaussian quantum states," Phys. Rev. Lett. **96**, 080502 (2006).