Efficient and secure quantum secret sharing for eight users

Yue Qin,[1,*] Jialin Cheng,[1,*] Jingxu Ma,[1] Di Zhao,[1] Zhihui Yan,[1,2,†] Xiaojun Jia,[1,2,‡] Changde Xie,[1,2] and Kunchi Peng[1,2]

[1]*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan, 030006, People's Republic of China*

[2]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, People's Republic of China*

(Received 28 August 2023; accepted 25 June 2024; published 8 July 2024)

Quantum secret sharing (QSS) has emerged as a promising avenue for storing secret with quantum-enhanced security. However, practical applications are hindered by the challenge for simultaneously implementing high-efficiency, high-security, and high-flexibility QSS with multiple users. Here we present an efficient, secure, and flexible QSS involving eight users with a continuous-variable eight-partite bound entanglement (BE) state, where only two nondegenerated optical parameter amplifiers are required. Such abilities are attributed to the generation of the eight-partite BE state with precise phase controlling systems and a large entanglement network, and fiber distribution with polarization-division multiplexing. In the QSS, a higher key rate can be demonstrated, when a secret is extracted through flexible combinations of more collaborative users. Our system may pave the way for the spatially separated multiuser quantum communications, while minimizing quantum hardware.

DOI: 10.1103/PhysRevResearch.6.033036

I. INTRODUCTION

Quantum communication is rapidly developing because of its high security and rate beyond classical approach. Initially, quantum communication is limited to just point-to-point connection between two users [1–3]. As the scale increases, communication performance can be significantly enhanced. The amount of stored information increases exponentially when the accessible network scale enlarges. The creation of increasingly large multipartite entangled states is not only a fundamental scientific endeavor, but also the enabling technology for quantum communication. Quantum communication has been developed from two users to multiple users, due to the tailor-made multipartite entangled state [4–9]. To achieve this, there are endeavors to interconnect the multiple users, and it is highly demanded to realize a quantum communication network with more users [10–14].

Secret sharing is a cryptographic primitive with multiple users, where the secret information is distributed to several users by the dealer, and only an authorized set of users can reconstruct the original secret information. Quantum secret sharing (QSS) has the capability to protect secret information from eavesdropping and dishonest users based on quantum entanglement source, emerging as a promising avenue for storing secret with quantum-enhanced security [15]. So far, great efforts have been made to extend the advantages to more users by using the multipartite entanglement [16–19]. However, the complex configuration, precise control, fragile distribution, and large cost of quantum resource in current conditions have made the more-user adoption of the QSS an experimental challenge. It remains a longstanding goal to simultaneously implement efficient, secure, and flexible QSS with more users.

In this paper we demonstrate an efficient and practical QSS with high security and flexibility based on the techniques of larger entanglement generation network, precise active feedforward control, and low-noise polarization-division multiplexing fiber distribution with continuous-variable (CV) eight-partite bound entangled (BE) state. CV BE states have emerged as a promising platform to circumvent the above restrictions for exploring the secure and flexible multiuser QSS [20–23]. In realistic implementations, quantum entangled states are more or less mixed, which is caused by environment decoherence processes [24,25]. BE states emerge in certain mixed quantum states and are different from both free entangled (distillable) and separable states [26,27]. They carries elusive and fragile quantum correlations, where no entanglement can be distilled using local operation and classical communication. Thus, BE states are suitable in quantum-enhanced cryptography [28,29], besides superactivation [30,31] and remote information concentration [32]. In this QSS based on CV BE state, the secret can be effectively extracted only when more than half of users collaborate in forming the access structure, whereas the remaining users cannot obtain any secret even if they work together. Differing from the previous scheme employing the four-user BE state [21], we achieve not only a higher secret key rate with eight distant users but also a versatile communication structure with flexible network topology and connectivity, in which the dealer can modify the permitted user number of the access

*These authors contributed equally to this work.
†Contact author: zhyan@sxu.edu.cn
‡Contact author: jiaxj@sxu.edu.cn

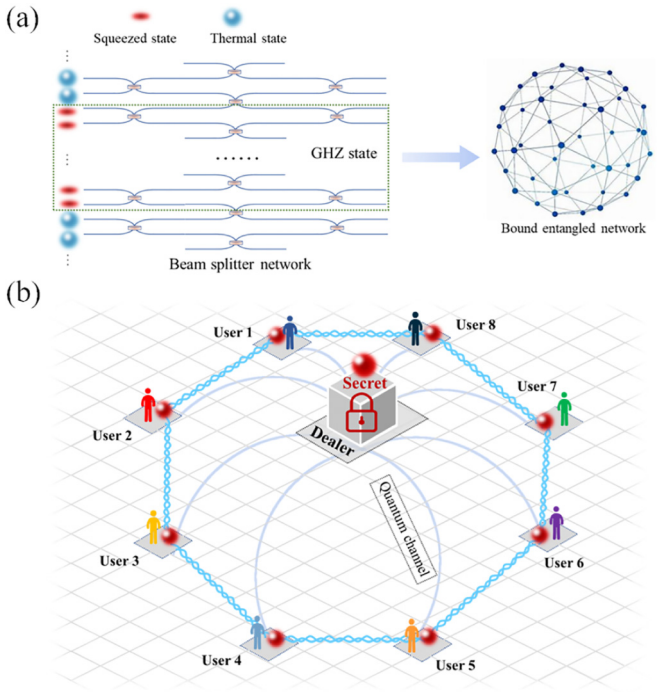

FIG. 1. (a) Schematic diagram of generating a multipartite CV BE state. (b) The eight-user QSS using the BE state generated and distributed by the dealer.

structure by controlling the squeezing factor. Besides, to show the feasibility, this BE state is distributed to eight distant users through fibers. Furthermore, the results demonstrate the possibility to realize QSS with more users and versatile communication structure by combining the integrated technology.

The schematic diagram of generating the multipartite BE state is depicted in Fig. 1(a). We prepare the quadrature squeezed states, and then couple them to obtain an $N/2$-partite Greenberger-Horne-Zeilinger (GHZ) state. Each submode of the resultant GHZ state is coupled with an independent Gaussian noisy thermal state, which forms a N-partite BE state. The eight-partite BE state can be effectively generated by coupling four independent thermal states with the submodes of quadripartite GHZ state, where two nondegenerate optical parametric amplifiers (NOPAs) are employed. In the case of $N = 8$, the eight-user QSS based on eight-partite BE state is illustrated in Fig. 1(b). The dealer modulates the secret on the eight-partite BE state and then distributes it to all eight users through quantum channels. The secret can be extracted by the access structure due to the quantum correlation among these submodes. We start with the generation of eight-partite BE state. The squeezed modes $\hat{a}_i (i = 1, 2, 3, 4)$ with the squeezing factor r are generated. The four modes are coupled in a beam splitter (BS) network to form the quadripartite GHZ state. After coupling the four Gaussian noisy thermal states and four submodes of the GHZ state in another BS network, the multipartite BE state consisting of eight quantum modes $(\hat{c}_1, \hat{c}_2, \hat{c}_3, \hat{c}_4, \hat{c}_5, \hat{c}_6, \hat{c}_7, \hat{c}_8)$ is obtained. The quadrature amplitude and phase of modes $(\hat{c}_j)_{j=1,2,\ldots,8}$ as $\hat{x}_j = \hat{c}_j + \hat{c}_j^\dagger$ and phase $\hat{p}_j = (\hat{c}_j - \hat{c}_j^\dagger)/i$ are defined. Through the verification of the combined quadrature noises of the eight submodes, we have obtained a BE state for QSS, as described in Appendixes A and B. In the QSS scheme based on CV BE state, when ideal squeezing is applied, the quantum correlations of the BE state can protect the secret from the adversary structure and enable it to be extracted perfectly by the access structure. For practical applications of finite squeezing, it is sufficient to consider the adversary structure attack to ensure the security of our QSS protocol. The amplitude and phase components are used to share the secret in our scheme. The secret key rate is usually used to evaluate the performance of CV QSS systems, which is the difference between the classical mutual information obtained by the access structure, and the Holevo bound quantified by the adversary structure's information [33,34]. The secret key rate in different user collaborations is observed, and the larger positive key rate of QSS certifies the better secure performance. The corresponding secret key rate is given by

$$K = I(D{:}A) - I(D{:}E), \tag{1}$$

where $I(D{:}A)$ is the mutual information obtained by the access structure, and $I(D{:}E)$ is the Holevo bound, which represents the maximum possible knowledge obtained by the adversary structure [34].

For sharing secrets with distant users, the submodes of BE state can be distributed through free space or optical fibers. Commercially available free space and fiber-optic systems operate within the near-infrared spectral windows. For instance, the attenuation at 1080 nm through single-mode fiber is approximately 1.50 dB/km [35,36]. The polarization-division multiplexing can simultaneously distribute a slightly weak local oscillator (LO) and signal mode with a perpendicular polarization direction via a short fiber cable. In this way, only the optical loss of the fiber needs to be considered. Moreover, the challenge of relative phase locking can be significantly solved [37].

Next, we experimentally demonstrate the QSS for eight users based on the BE state. The schematic diagram of experimental setup is shown in Fig. 2. The system is built on a dual-wavelength laser of 1080 nm and 540 nm. In the efficient generation scheme of eight-partite BE state, two NOPAs involving the wedged type II nonlinear crystals are employed. Through a parametric down-conversion process, the quadrature squeezed states $(\hat{a}_i (i = 1, 2, 3, 4))$ are produced by a pair of NOPAs. For each NOPA, a 2 mW signal field is injected into the NOPA in the deamplification state to produce an approximately 40 uW two-mode squeezed state when the pump power is about 130 mW. Through the coupling of modes $\hat{a}_i$ on a 50/50 BS network, we generate four output modes that collectively constitute the GHZ state $(\hat{b}_i (i = 1, 2, 3, 4))$. Subsequently, by coupling the four submodes of the GHZ state $\hat{b}_i$ with four independent thermal states of light $[\hat{v}_i^T \ (i = 1, 2, 3, 4)]$ using four 50/50 BSs, the eight-partite BE state is produced. The thermal state is obtained experimentally by modulating Gaussian noise signals to the coherent state using amplitude and phase modulators; see the Appendixes for more details. For realizing the QSS among eight users, the classical secret message $[a_s = (x_s + ip_s)/2]$ and its phase conjugate $[a_s^* = (x_s - ip_s)/2]$ are modulated on the submodes of the GHZ state by using amplitude and phase modulators. The quadrature component x_s and p_s coded secrets are mutually

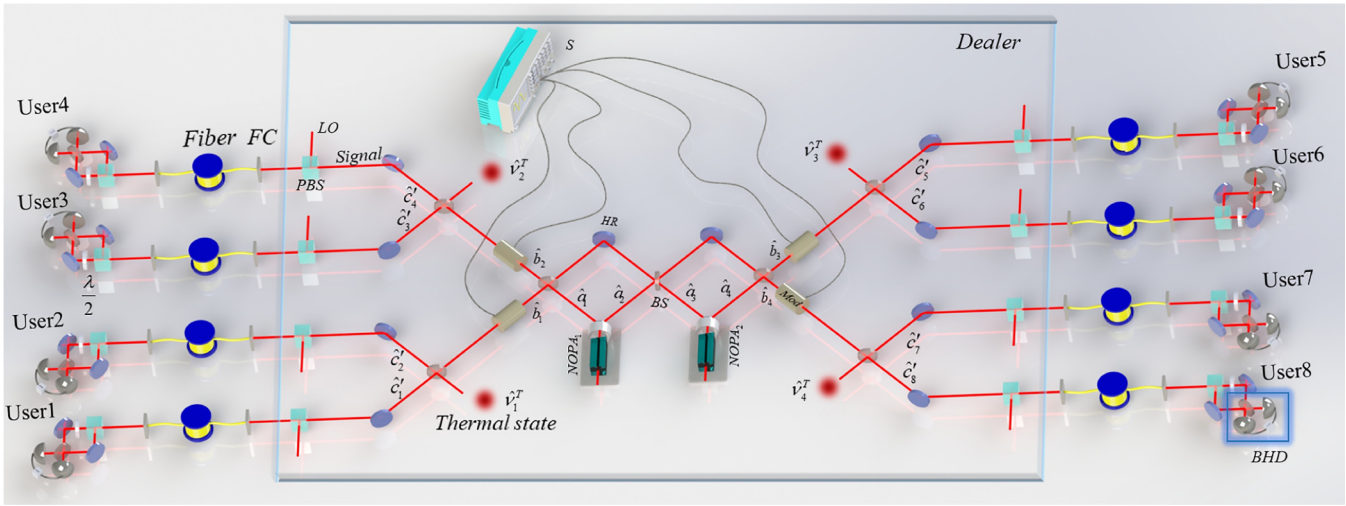

FIG. 2. The experimental setup for QSS using an eight-partite BE state. NOPA, nondegenerate optical parametric amplifier; BS, 50/50 beam splitter; HR, mirror with high reflection; Mod, amplitude and phase modulator; PBS, polarizing beam splitter; BHD, balanced homodyne detector; LO, local oscillator; FC, fiber coupler.

independent, and the strengths of modulated signals ($V_{xs} = \langle \delta^2 x_s \rangle$ and $V_{ps} = \langle \delta^2 p_s \rangle$) can be controlled by the dealer. In our experiment, two sets of modulated signals have identical amplitudes, i.e., $V_{xs} = V_{ps}$. The dealer distributes the submodes ($\hat{c}'_j (j = 1, 2, \ldots, 8)$) of the BE state to eight users. For measuring the correlation variances of amplitude quadrature (or phase quadrature), eight output modes $\hat{c}'_j$ are measured by eight sets of balanced homodyne detectors. For sharing secrets with distant users, the eight submodes loading secrets are distributed separately through indoor 1 km coiled fibers, in which the polarization-division multiplexing is exploited [37]. Quantum states are sensitive to experimental conditions, and imperfect conditions such as phase instability and transmission loss can degrade the quality of the BE state. First, we develop a compact and controllable field programmable gate array (FPGA) system with real-time phase locking; see Appendix C for details. Most components are housed inside the shielded box, so that it provides good long-term stability. Furthermore, it offers good controllability, maintaining a phase lock fluctuation of only 0.06 rad for all phases, even with multiple users. Second, the high-gain detectors are developed to measure weak signals transmitted from high reflection mirrors, which realize both the low-loss transmission and high signal-to-noise ratio phase-locking signals [38].

The correlation variances of the pairs of submodes $(\hat{c}_1, \hat{c}_3)$, $(\hat{c}_1, \hat{c}_4)$ are identified by the inseparability criteria of the BE states, as described in Appendixes A and B. Table I shows the measured correlation variances of BE state, before and after fiber distribution. These results of the BE state before fiber distribution correspond to $\Delta_5 = 2.51 \pm 0.04 < 8$, $\Delta_6 = 2.44 \pm 0.04 < 8$, $\Delta_7 = 2.45 \pm 0.04 < 8$, and $\Delta_8 = 2.46 \pm 0.05 < 8$, indicating that eight-mode correlations are still retained. The definitions of correlation variances Δ_j $(j = 1, 2, \ldots, 8)$ can be found in Table I. The correlation variances $\Delta_1 + \Delta_5 = 8.71 \pm 0.04 > 8$, $\Delta_2 + \Delta_6 = 8.72 \pm 0.04 > 8$, $\Delta_3 + \Delta_7 = 18.13 \pm 0.07 > 8$, and $\Delta_4 + \Delta_8 = 18.18 \pm 0.06 > 8$, which means that no entanglement can be distilled between any two parties with local operation and classical communication, according to the multipartite nonseparability criterion [39]. Thus the eight-partite BE state is experimentally obtained. Although the quantum correlations shown in Table I get worse after fiber distribution, the QSS can be realized with positive secret key rates in this scheme.

The (m, n) access structures are shown in Fig. 3(a), where n is the total number of users, m represents the number of collaborating users forming the access structure, and $m \leqslant n$. In our scheme, the effective access structure includes three scenarios: involving six, seven, and eight collaborative users, respectively. Access structures of types I and II are constituted by eight and seven collaborative users, respectively. For six collaborative users, there exist two distinct access structures, primarily dependent on whether the two submodes possessed by dishonest users originate from the same submode of the GHZ state, which corresponds to type III and type IV, respectively. The dependencies of secret key rates on the squeezing factor of BE state without and with fiber distribution are demonstrated in Figs. 3(b) and 3(c), respectively. These curves are derived from Eq. (1) and the different combinations of collaborative users are analyzed, in which the measured correlation variances listed in Table I have been used. The calculation details and results are given in Appendixes A and B. Before the fiber distribution of BE state, if eight users collaborate, they form the access structure type I, and the secret key rate K_8 equals the mutual information obtained by the access structure. It is evident that the secret key rate K_8 for eight collaborative users with an eight-partite BE state is higher than K'_4 for four collaborative users with a quadripartite BE state. Based on the correlation characteristics of the BE state, the secret key rates for all eight users K_8 and any seven users K_7 (type II) are positive. For different combinations of six users K_{61} (type III) and K_{62} (type IV) may be positive by controlling the value of squeezing factor, and thus the threshold of QSS can be realized by controlling different r. The access structure with five collaborative users is the same as that of six collaborative users and can be

TABLE I. The measured correlation variances of BE state before and after fiber distribution. The eight correlation variances are defined as $\Delta_1 \equiv \langle \delta^2(\hat{p}_{c_1} - \hat{p}_{c_3})\rangle$, $\Delta_2 \equiv \langle \delta^2(\hat{p}_{c_1} - \hat{p}_{c_4})\rangle$, $\Delta_3 \equiv \langle \delta^2(\hat{x}_{c_1} - \hat{x}_{c_3})\rangle$, $\Delta_4 \equiv \langle \delta^2(\hat{x}_{c_1} - \hat{x}_{c_4})\rangle$, $\Delta_5 \equiv \langle \delta^2(\hat{x}_{c_1} + \hat{x}_{c_3} + g_{x2}\hat{x}_{c_2} + g_{x4}\hat{x}_{c_4} + g_{x5}\hat{x}_{c_5} + g_{x6}\hat{x}_{c_6} + g_{x7}\hat{x}_{c_7} + g_{x8}\hat{x}_{c_8})\rangle$, $\Delta_6 \equiv \langle \delta^2(\hat{x}_{c_1} + \hat{x}_{c_4} + g_{x2}\hat{x}_{c_2} + g_{x3}\hat{x}_{c_3} + g_{x5}\hat{x}_{c_5} + g_{x6}\hat{x}_{c_6} + g_{x7}\hat{x}_{c_7} + g_{x8}\hat{x}_{c_8})\rangle$, $\Delta_7 \equiv \langle \delta^2(\hat{p}_{c_1} + \hat{p}_{c_3} + g_{p2}\hat{p}_{c_2} + g_{p4}\hat{p}_{c_4} - g_{p5}\hat{p}_{c_5} - g_{p6}\hat{p}_{c_6} - g_{p7}\hat{p}_{c_7} - g_{p8}\hat{p}_{c_8})\rangle$, and $\Delta_8 \equiv \langle \delta^2(\hat{p}_{c_1} + \hat{p}_{c_4} + g_{p2}\hat{p}_{c_2} + g_{p3}\hat{p}_{c_3} - g_{p5}\hat{p}_{c_5} - g_{p6}\hat{p}_{c_6} - g_{p7}\hat{p}_{c_7} - g_{p8}\hat{p}_{c_8})\rangle$, where g_{xj}, g_{pj} are the gain factor for amplitude and phase quadratures $\hat{x}_j$, $\hat{p}_j$ with the subscript $j = 1, 2, \ldots, 8$.

	Δ_1	Δ_2	Δ_3	Δ_4	Δ_5	Δ_6	Δ_7	Δ_8
Correlation before distribution (dB)	4.90 ± 0.10	4.97 ± 0.08	8.94 ± 0.08	8.95 ± 0.07	-4.44 ± 0.07	-4.57 ± 0.07	-4.55 ± 0.07	-4.54 ± 0.08
Correlation after distribution (dB)	3.43 ± 0.09	3.36 ± 0.08	6.13 ± 0.08	6.15 ± 0.09	-1.61 ± 0.07	-1.61 ± 0.08	-1.59 ± 0.08	-1.47 ± 0.07

divided into two types based on whether the dishonest users constituting the eavesdropping structure come from the independent submodes of the GHZ state. For five collaborative users, the key rates K_{51} and K_{52} are negative, and no secret can be obtained. In particular, when the collaborative user number is larger, the key rate is higher. Furthermore, it can be seen that the key rates for both quadrature amplitude and phase are equal, and thus the secret key rates extracted from both quadrature components are balanced. The experimental results for the key rates of eight, seven, and six collaborative users are all positive with different squeezing factors of 0.35, 0.40 and 0.55. Thus, the QSSs within (8, 8), (7, 8), and (6, 8) thresholds have been achieved. After the fiber distribution of the BE state, the secret key rates decrease. However, the eight distant collaborative users can still extract the secret with a positive key rate, which demonstrates this protocol is feasible for more users. As shown in Fig. 3(c), the experimental results of the key rates for more than six distant collaborative users are all positive with squeezing factors of 0.55, indicating that the secret can still be extracted. These results further support the feasibility of this protocol for eight distant users. Our results demonstrate that the key rate is higher when more collaborative users participate in the decryption. Thus, the efficient, secure, and flexible QSS for eight users has been realized with the distributed BE state.

In summary, we design and demonstrate an efficient and secure QSS with eight users based on a CV BE state, while minimizing quantum hardware and simplifying the complexity. The eight-partite BE state is deterministically generated by combining independent thermal states and quadripartite GHZ state, where only two NOPAs and precise phase-controlling systems are required. By distributing the resultant BE state through fiber channels, the QSS with eight separated users can be efficiently realized to prove the security against dishonest users. This gives us a clear multiuser advantage with high efficiency, high security, and high flexibility. In the future, security with all collaborative users can be further increased with improved squeezing, and the scheme can be directly extended to more users by combining the integrated technology. Moreover, the QSS can be extended to more users through commercial optical fiber [40–43]. QSS enables sharing secrets with distant parties with in-line and local LO distribution [44–46], and the automatic feedback system can overcome the long-distance channel

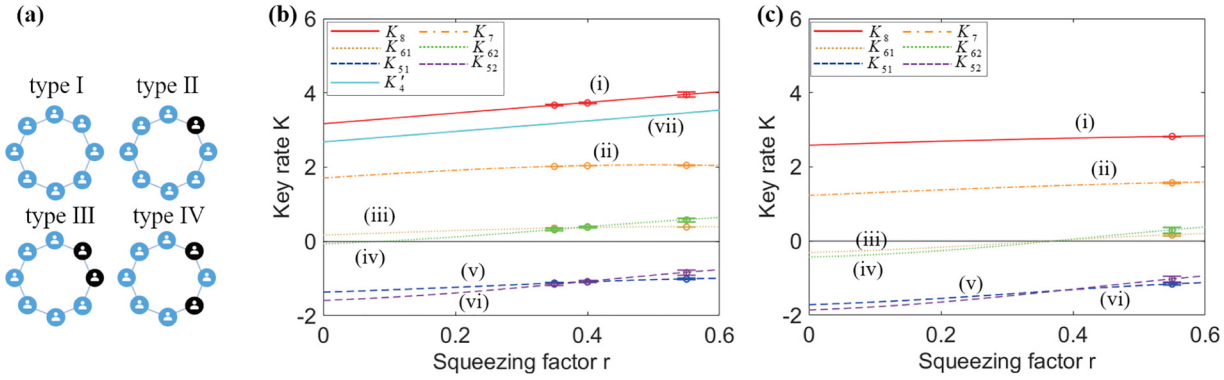

FIG. 3. The dependence of the secret key rate K on the squeezing factor r of two-mode squeezed state with different combination of collaborative users. (a) The access structures of eight-user QSS. The blue and black circles represent the collaborative and possible eavesdropping users, respectively. Panels (b) and (c) stand for secret key rates before and after fiber distribution, respectively. The red solid trace i shows the secret key rate K_8 for eight collaborative users with eight-partite BE state. The orange dot-dashed trace ii shows the secret key rate K_7 for any seven collaborative users. The yellow and green dotted traces iii and iv show the secret key rates K_{61} and K_{62} for different combinations of six collaborative users, respectively. The blue and purple dashed traces v and vi show the secret key rates K_{51} and K_{52} for different combinations of five users, respectively. The cyan solid trace vii shows the secret key rate K_4' for four collaborative users with a quadripartite BE state. The corresponding experimental results are marked with circles. The experimental results are demonstrated with circles.

perturbations to synchronize clocks and frames [47,48], as well as calibrate phase and polarization [49,50]. Overcoming the efficiency, security and flexibility limitations encountered by large user number, our results may offer a way towards practical applications for QSS and may be helpful for building versatile quantum communication systems involving more users.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 61925503, No. 62122044, and No. 62135008), the Key Project of the National Key R&D program of China (Grant No. 2022YFA1404500), the Program for the Innovative Talents of the Higher Education Institutions of Shanxi, the Program for the Outstanding Innovative Teams of the Higher Learning Institutions of Shanxi, and the Fund for Shanxi "1331 Project" Key Subjects Construction.

APPENDIX A: EIGHT-PARTITE BE STATE

We start with the generation of an eight-partite BE state. The quadrature amplitude and phase squeezed modes $\hat{a}_i$ $(i = 1, 2, 3, 4)$ are generated from two NOPAs in identical configuration as $\hat{x}_{a_{1(4)}} = e^r \hat{x}^{(0)}_{1(4)}$, $\hat{p}_{a_{1(4)}} = e^{-r}\hat{p}^{(0)}_{1(4)}$, $\hat{x}_{a_{2(3)}} = e^{-r}\hat{x}^{(0)}_{2(3)}$, $\hat{p}_{a_{2(3)}} = e^{r}\hat{p}^{(0)}_{2(3)}$, where r is the squeezing factor, $\hat{x}^{(0)}_{1(2,3,4)}$ and $\hat{p}^{(0)}_{1(2,3,4)}$ denote the quadrature amplitudes and phases of the injected signal modes. The amplitude and phase of mode $\hat{a}$ can be expressed as $\hat{x} = \hat{a} + \hat{a}^\dagger$ and $\hat{p} = (\hat{a} - \hat{a}^\dagger)/i$ quadratures with the canonical commutation relation $[\hat{x}, \hat{p}] = 2i$, respectively. The four modes are coupled in a BS network to form the quadripartite GHZ state, i.e., $\hat{b}_1 = -\frac{1}{\sqrt{2}}\hat{a}_1 + \frac{1}{2}\hat{a}_3 + \frac{1}{2}i\hat{a}_2$, $\hat{b}_2 = \frac{1}{\sqrt{2}}\hat{a}_1 + \frac{1}{2}\hat{a}_3 + \frac{1}{2}i\hat{a}_2$, $\hat{b}_3 = \frac{1}{\sqrt{2}}\hat{a}_4 + \frac{1}{2}\hat{a}_3 - \frac{1}{2}i\hat{a}_2$, and $\hat{b}_4 = -\frac{1}{\sqrt{2}}\hat{a}_4 + \frac{1}{2}\hat{a}_3 - \frac{1}{2}i\hat{a}_2$ [51]. After coupling the four Gaussian noisy thermal states and four submodes of the GHZ state in another BS network, the multipartite BE state consisting of eight quantum modes $(\hat{c}_1, \hat{c}_2, \hat{c}_3, \hat{c}_4, \hat{c}_5, \hat{c}_6, \hat{c}_7, \hat{c}_8)$ is obtained. The thermal states are generated by modulating randomly amplitude and phase quadratures of a weak coherent state with noisy signals of Gaussian function distribution from arbitrary function generator. According to the inseparability criteria, the minimum noise in quadrature amplitude (phase) of the thermal state satisfies the nondistillability requirement of the BE state. The BE submodes are $\hat{c}_1 = \frac{1}{\sqrt{2}}(\hat{b}_1 + \hat{v}_1^T)$, $\hat{c}_2 = \frac{1}{\sqrt{2}}(\hat{b}_1 - \hat{v}_1^T)$, $\hat{c}_3 = \frac{1}{\sqrt{2}}(\hat{b}_2 + \hat{v}_2^T)$, $\hat{c}_4 = \frac{1}{\sqrt{2}}(\hat{b}_2 - \hat{v}_2^T)$, $\hat{c}_5 = \frac{1}{\sqrt{2}}(\hat{b}_3 + \hat{v}_3^T)$, $\hat{c}_6 = \frac{1}{\sqrt{2}}(\hat{b}_3 - \hat{v}_3^T)$, $\hat{c}_7 = \frac{1}{\sqrt{2}}(\hat{b}_4 + \hat{v}_4^T)$, $\hat{c}_8 = \frac{1}{\sqrt{2}}(\hat{b}_4 - \hat{v}_4^T)$, where $\hat{v}_1^T$, $\hat{v}_2^T$, $\hat{v}_3^T$ and $\hat{v}_4^T$ represent the thermal states and quadrature variances satisfy $\langle \delta^2 \hat{x}_{\hat{v}^T} \rangle = \langle \delta^2 \hat{p}_{\hat{v}^T} \rangle = \langle \delta^2 \hat{x}_{\hat{v}^T_{1,2,3,4}} \rangle = \langle \delta^2 \hat{p}_{\hat{v}^T_{1,2,3,4}} \rangle \gg 1$. The combination noises of quadrature amplitudes $[\delta^2(\hat{x}_{c_1} + \hat{x}_{c_2} + \hat{x}_{c_3} + \hat{x}_{c_4} + \hat{x}_{c_5} + \hat{x}_{c_6} + \hat{x}_{c_7} + \hat{x}_{c_8}) = 8e^{-2r}]$ and phases $[\delta^2(\hat{p}_{c_1} + \hat{p}_{c_2} + \hat{p}_{c_3} + \hat{p}_{c_4} - \hat{p}_{c_5} - \hat{p}_{c_6} - \hat{p}_{c_7} - \hat{p}_{c_8}) = 8e^{-2r}]$ among submodes of the BE state are employed for QSS.

The inseparability criteria are usually used to check the quantum entanglement among the multipartite states [39]. To check the eight submodes of the BE state $(\hat{c}_1, \hat{c}_2, \hat{c}_3, \hat{c}_4, \hat{c}_5, \hat{c}_6, \hat{c}_7, \hat{c}_8)$, we have to prove whether any entangled state can be distilled out from the eight space separated submodes only by local operation and classical communication (LOCC). For all the pairs $(\hat{c}_i, \hat{c}_j)_{i,j=1,2,\ldots,8}(i \neq j)$ of submodes $(\hat{c}_j)_{j=1,2,\ldots,8}$, the entanglement between $(\hat{c}_1, \hat{c}_2)$, $(\hat{c}_3, \hat{c}_4)$, $(\hat{c}_5, \hat{c}_6)$, and $(\hat{c}_7, \hat{c}_8)$ cannot be obtained by LOCC. Each pair is generated by mixing a submode of the GHZ state and a single-mode thermal state on a 50/50 BS, thus there is no any quantum correlation between them [31]. However, the eight-mode quantum correlations are still retained. For generating genuine multipartite BE state using GHZ state, the whole multipartite states of the quadrature amplitudes combinations are $[\delta^2(\hat{x}_{c_1} + \hat{x}_{c_2} + \hat{x}_{c_3} + \hat{x}_{c_4} + \hat{x}_{c_5} + \hat{x}_{c_6} + \hat{x}_{c_7} + \hat{x}_{c_8}) = 8e^{-2r}]$ and quadrature phases combinations are $[\delta^2(\hat{p}_{c_1} + \hat{p}_{c_2} - \hat{p}_{c_3} - \hat{p}_{c_4} + \hat{p}_{c_5} + \hat{p}_{c_6} - \hat{p}_{c_7} - \hat{p}_{c_8}) = 8e^{-2r}]$, $[\delta^2(-\hat{p}_{c_1} - \hat{p}_{c_2} + \hat{p}_{c_3} + \hat{p}_{c_4} + \hat{p}_{c_5} + \hat{p}_{c_6} - \hat{p}_{c_7} - \hat{p}_{c_8}) = 8e^{-2r}]$, $[\delta^2(\hat{p}_{c_1} + \hat{p}_{c_2} - \hat{p}_{c_3} - \hat{p}_{c_4} - \hat{p}_{c_5} - \hat{p}_{c_6} + \hat{p}_{c_7} + \hat{p}_{c_8}) = 8e^{-2r}]$, $[\delta^2(-\hat{p}_{c_1} - \hat{p}_{c_2} + \hat{p}_{c_3} + \hat{p}_{c_4} + \hat{p}_{c_5} + \hat{p}_{c_6} - \hat{p}_{c_7} - \hat{p}_{c_8}) = 8e^{-2r}]$, $[\delta^2(\hat{p}_{c_1} + \hat{p}_{c_2} + \hat{p}_{c_3} + \hat{p}_{c_4} - \hat{p}_{c_5} - \hat{p}_{c_6} - \hat{p}_{c_7} - \hat{p}_{c_8}) = 8e^{-2r}]$, $[\delta^2(-\hat{p}_{c_1} - \hat{p}_{c_2} - \hat{p}_{c_3} - \hat{p}_{c_4} + \hat{p}_{c_5} + \hat{p}_{c_6} + \hat{p}_{c_7} + \hat{p}_{c_8}) = 8e^{-2r}]$, respectively. The correlation among submodes will be much lower than the corresponding quantum noise limit (QNL); however, it satisfies the inseparability criteria inequalities

$$\langle \delta^2(\hat{p}_i - \hat{p}_j) \rangle + \langle \delta^2(\hat{x}_i + \hat{x}_j + g_{xk}\hat{x}_k + g_{xl}\hat{x}_l + g_{xm}\hat{x}_m + g_{xn}\hat{x}_n + g_{xr}\hat{x}_r + g_{xs}\hat{x}_s) \rangle > 8, \tag{A1}$$

$$\langle \delta^2(\hat{x}_i - \hat{x}_j) \rangle + \langle \delta^2(\hat{p}_i + \hat{p}_j + g_{pk}\hat{p}_k + g_{pl}\hat{p}_l - g_{pm}\hat{p}_m - g_{pn}\hat{p}_n - g_{pr}\hat{p}_r - g_{ps}\hat{p}_s) \rangle > 8, \tag{A2}$$

where g_{xa}, g_{pa} are the gain factor (arbitrary real parameter) for amplitude and phase quadratures $\hat{x}_a$, $\hat{p}_a$, and the subscript $a = i, j, k, l, m, n, r, s$ represents the different submodes $(\hat{c}_j)_{j=1,2,\ldots,8}$. For simplification, the same gain factors are chosen $g_x = g_{xa}$ and $g_p = g_{pa}(a = i, j, k, l, m, n, r, s)$. It is sufficient to verify the full separability inequalities of the eight-mode BE state. For example, the total variances of $(\hat{c}_1, \hat{c}_3)$ are obtained by

$$\begin{aligned}
A &= \langle \delta^2(\hat{p}_{c1} - \hat{p}_{c3}) \rangle + \langle \delta^2(\hat{x}_{c1} + \hat{x}_{c3} + g_x\hat{x}_{c2} + g_x\hat{x}_{c4} + g_x\hat{x}_{c5} + g_x\hat{x}_{c6} + g_x\hat{x}_{c7} + g_x\hat{x}_{c8}) \rangle \\
&= \tfrac{1}{2}e^{-2r}[3 + e^{4r+2r'} + 2e^{2r}(\langle \delta^2 \hat{p}_{v^T} \rangle + \langle \delta^2 \hat{x}_{v^T} \rangle) - 2g_x(-3 + e^{4r+2r'} + 2e^{2r}\langle \delta^2 \hat{x}_{v^T} \rangle) \\
&\quad + (g_x)^2(9 + e^{4r+2r'} + 2e^{2r}\langle \delta^2 \hat{x}_{v^T} \rangle)], \\
B &= \langle \delta^2(\hat{x}_{c1} - \hat{x}_{c3}) \rangle + \langle \delta^2(\hat{p}_{c1} + \hat{p}_{c3} + g_p\hat{p}_{c2} + g_p\hat{p}_{c4} - g_p\hat{p}_{c5} - g_p\hat{p}_{c6} - g_p\hat{p}_{c7} - g_p\hat{p}_{c8}) \rangle \\
&= e^{2(r+r')} + \tfrac{1}{2}e^{2(r+r')}(-1 + g_p)^2 + \tfrac{1}{2}e^{-2r}(1 + 3g_p)^2 + (-1 + g_p)^2\langle \delta^2 \hat{p}_{v^T} \rangle + \langle \delta^2 \hat{x}_{v^T} \rangle,
\end{aligned} \tag{A3}$$

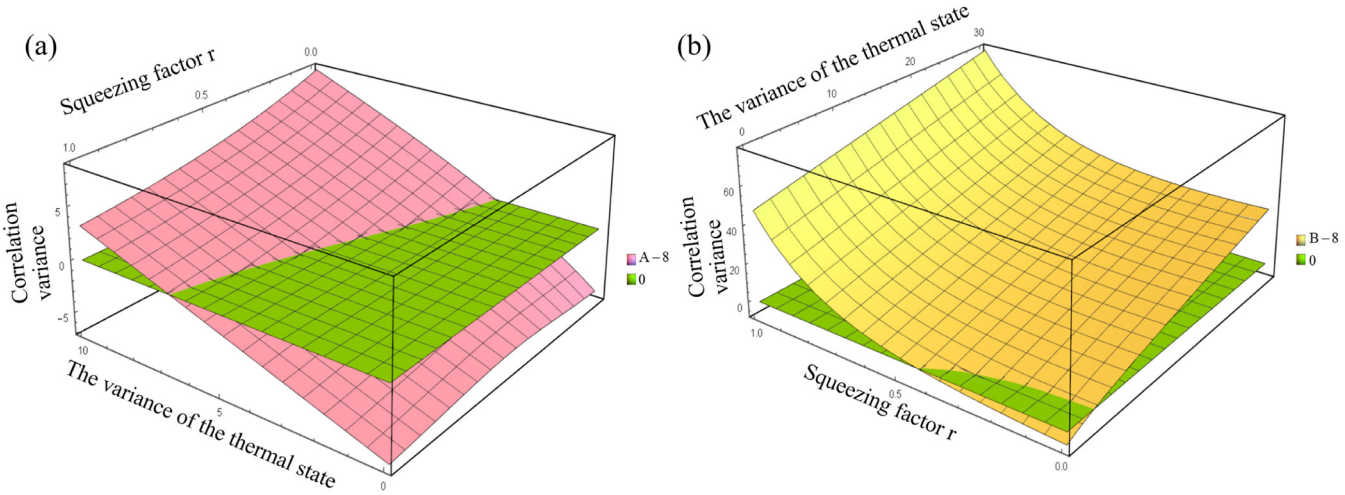

FIG. 4. The dependence of combinations of quantum correlation variance of amplitude (phase) quadrature among BE entangled states generated by GHZ state on the squeezing factor r and the noise of the thermal states, where the gains g_{xi}, $g_{pi}(i = 1, 2, \ldots, 8)$ are taken as the optimal gain g_{xopt}, g_{popt}. The green plane represents the critical surface for which the nonseparability criterion is satisfied. The pink and yellow curved surfaces represent the quantum correlation variance $(A - 8)$ (a) and $(B - 8)$ (b), respectively, where the expressions of A and B can be found in Eq. (A3).

where $\langle\delta^2\hat{x}_{\upsilon^T}\rangle$, $\langle\delta^2\hat{p}_{\upsilon^T}\rangle$ are quadrature variances of the thermal state and $\langle\delta^2\hat{x}_{\upsilon^T}\rangle = \langle\delta^2\hat{p}_{\upsilon^T}\rangle \gg 1$. By calculating the minimum values of the inequalities' left-hand side for BE state, the optimized gain factors $g_{\mathrm{xopt}}, g_{\mathrm{popt}}$ for BE state are $g_{\mathrm{xopt}} = \frac{-3+\mathrm{e}^{4r+2r'}+2\mathrm{e}^{2r}\langle\delta^2\hat{x}_{\upsilon^T}\rangle}{9+\mathrm{e}^{4r+2r'}+2\mathrm{e}^{2r}\langle\delta^2\hat{x}_{\upsilon^T}\rangle}$ and $g_{\mathrm{popt}} = \frac{-3+\mathrm{e}^{4r+2r'}+2\mathrm{e}^{2r}\langle\delta^2\hat{p}_{\upsilon^T}\rangle}{9+\mathrm{e}^{4r+2r'}+2\mathrm{e}^{2r}\langle\delta^2\hat{p}_{\upsilon^T}\rangle}$. According to the inseparability criteria, the minimum noise in quadrature amplitude (phase) of the thermal state $\delta^2\hat{x}_{\upsilon^T}(\delta^2\hat{p}_{\upsilon^T})$ should satisfy the nondistillability requirement of the BE state, which is given by

$$\langle\delta^2\hat{x}_{\upsilon^T}\rangle = \langle\delta^2\hat{p}_{\upsilon^T}\rangle \geqslant \tfrac{1}{4}\mathrm{e}^{-4r}(-27\mathrm{e}^{2r} + 16\mathrm{e}^{4r} - \mathrm{e}^{6r+2r'} + \mathrm{e}^{2r}\sqrt{657 - 288\mathrm{e}^{2r} + 256\mathrm{e}^{4r} - 18\mathrm{e}^{4r+2r'} + 32\mathrm{e}^{6r+2r'} + \mathrm{e}^{8r+4r'}}), \quad \text{(A4)}$$

where r and r' are the squeezing and antisqueezing factors, respectively.

From Eq. (A3) we can see that the quantum correlation variances and the optimum gains depend not only on the squeezing factor r, but also on the noise of the thermal states. Figure 4 is the function of the quantum correlation variance of amplitude and phase quadrature of BE state as the squeezing factor r and the variance of the thermal states. It shows the normalized quantum correlation variances for different combinations of quadrature components of the BE state generated by the GHZ state, where the optimal gain factors $(g_{\mathrm{xopt}}, g_{\mathrm{popt}})$ are used for minimizing the corresponding correlation variances. With the increasing squeezing factor r, the larger noise of the thermal states is required for generating the BE state.

APPENDIX B: THE SECRET KEY RATE *K* FOR THE QSS

The dealer modulates the secret information $[a_s = (x_s + ip_s)/2]$ on amplitude and phase quadratures of two submodes of GHZ entanglement state $(\hat{b}_1, \hat{b}_2)$ and modulates $[a_s^* = (x_s - ip_s)/2]$ on amplitude and phase quadratures of other submodes of GHZ entanglement state $(\hat{b}_3, \hat{b}_4)$. Then he sends eight submodes of BE state to eight users (users 1–8), respectively. Thus, the submodes received by eight users are expressed by

$$\hat{c}'_{1(3)} = \frac{1}{\sqrt{2}}\big(\hat{b}_{1(2)} + \hat{\upsilon}^T_{1(2)} + \hat{a}_s\big), \quad \hat{c}'_{2(4)} = \frac{1}{\sqrt{2}}\big(\hat{b}_{1(2)} - \hat{\upsilon}^T_{1(2)} + \hat{a}_s\big),$$
$$\hat{c}'_{5(7)} = \frac{1}{\sqrt{2}}\big(\hat{b}_{3(4)} + \hat{\upsilon}^T_{3(4)} + \hat{a}^*_s\big), \quad \hat{c}'_{6(8)} = \frac{1}{\sqrt{2}}\big(\hat{b}_{3(4)} - \hat{\upsilon}^T_{3(4)} + \hat{a}^*_s\big). \quad \text{(B1)}$$

In the QSS protocol, the different combinations of collaborative users are analyzed. For five collaborative users, the combination noises of quadrature amplitude and quadrature phase between any submodes are

$$\big\langle\delta^2\big(g_{51}\hat{x}_{c'_1} + g_{51}\hat{x}_{c'_2} + g_{51}\hat{x}_{c'_3} + g_{51}\hat{x}_{c'_4} + g_{51}\hat{x}_{c'_5}\big)\big\rangle = \frac{1}{8}\mathrm{e}^{-2r}(25 + 11\mathrm{e}^{4r+2r'})g_{51}{}^2 + \frac{25g_{51}{}^2V_{xs}}{2} + \frac{1}{2}g_{51}{}^2\langle\delta^2(\hat{x}_{\hat{\upsilon}^T})\rangle,$$
$$\big\langle\delta^2\big(g_{51}\hat{p}_{c'_1} + g_{51}\hat{p}_{c'_2} + g_{51}\hat{p}_{c'_3} + g_{51}\hat{p}_{c'_4} - \hat{p}_{c'_5}\big)\big\rangle = \frac{1}{8}\mathrm{e}^{-2r}[3 + \mathrm{e}^{4r+2r'}(1 - 4g_{51})^2 + 8g_{51}(1 + 2g_{51})]$$
$$+ \frac{\langle\delta^2(\hat{p}_{\hat{\upsilon}^T})\rangle}{2} + \left(\frac{1}{2} + 4g_{51} + 8g_{51}{}^2\right)V_{ps},$$

$$\left\langle\delta^2\left(g_{52}\hat{x}_{c_1'}+g_{52}\hat{x}_{c_2'}+g_{52}\hat{x}_{c_3'}+g_{52}\hat{x}_{c_5'}+g_{52}\hat{x}_{c_7'}\right)\right\rangle=\frac{1}{8}\mathrm{e}^{-2r}(25+3\mathrm{e}^{4r+2r'})g_{52}{}^2+\frac{25g_{52}{}^2V_{xs}}{2}+\frac{3}{2}g_{52}{}^2\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle,$$
$$\left\langle\delta^2\left(g_{52}\hat{p}_{c_1'}+g_{52}\hat{p}_{c_2'}+g_{52}\hat{p}_{c_3'}-g_{52}\hat{p}_{c_5'}-\hat{p}_{c_7'}\right)\right\rangle=\frac{1}{8}\mathrm{e}^{-2r}[3+\mathrm{e}^{4r+2r'}(1-2g_{52})^2+4g_{52}(1+5g_{52})]$$
$$+\left(\frac{1}{2}+g_{52}{}^2\right)\langle\delta^2(\hat{p}_{\hat{v}^T})\rangle+\left(\frac{1}{2}+4g_{52}+8g_{52}{}^2\right)V_{ps},\tag{B2}$$

where g_{5j} $(j=1,2)$ are the adjustable classical gains for balancing the noises of amplitude quadrature and phase quadrature. Calculating the values of the Eq. (B2), the gain factors g_{5j} $(j=1,2)$ are

$$g_{51}=[-18\mathrm{e}^{4r+2r'}-2\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle+5\sqrt{-7\mathrm{e}^{4r+2r'}+11\mathrm{e}^{8r+4r'}+2\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle-10\mathrm{e}^{6r+2r'}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle+4\mathrm{e}^{4r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle^2}]/$$
$$\times 4[-7\mathrm{e}^{4r+2r'}+2\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle],$$
$$g_{52}=25+31\mathrm{e}^{4r+2r'}+24\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle$$
$$-5\sqrt{-25+14\mathrm{e}^{4r+2r'}+27\mathrm{e}^{8r+4r'}-44\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle+12\mathrm{e}^{6r+2r'}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle+16\mathrm{e}^{4r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle^2}$$
$$/2[25+13\mathrm{e}^{4r+2r'}+2\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle].\tag{B3}$$

For six collaborative users, the noises among any submodes are

$$\left\langle\delta^2\left(g_{61}\hat{x}_{c_1'}+g_{61}\hat{x}_{c_2'}+g_{61}\hat{x}_{c_3'}+g_{61}\hat{x}_{c_4'}+g_{61}\hat{x}_{c_5'}+g_{61}\hat{x}_{c_6'}\right)\right\rangle=\frac{3}{2}\mathrm{e}^{-2r}(3+\mathrm{e}^{4r+2r'})g_{61}{}^2+18g_{61}{}^2V_{xs},$$
$$\left\langle\delta^2\left(g_{61}\hat{p}_{c_1'}+g_{61}\hat{p}_{c_2'}+g_{61}\hat{p}_{c_3'}+\hat{p}_{c_4'}-\hat{p}_{c_5'}-\hat{p}_{c_6'}\right)\right\rangle=\frac{1}{8}\mathrm{e}^{-2r}(19+\mathrm{e}^{4r+2r'}(1-3g_{61})^2+g_{61}(14+11g_{61}))$$
$$+\left(\frac{9}{2}+9g_{61}+\frac{9g_{61}{}^2}{2}\right)V_{ps}+\left(\frac{1}{2}-g_{61}+\frac{g_{61}{}^2}{2}\right)\langle\delta^2(\hat{p}_{\hat{v}^T})\rangle,$$
$$\left\langle\delta^2\left(g_{62}\hat{x}_{c_1'}+g_{62}\hat{x}_{c_2'}+g_{62}\hat{x}_{c_3'}+g_{62}\hat{x}_{c_4'}+g_{62}\hat{x}_{c_5'}+g_{62}\hat{x}_{c_7'}\right)\right\rangle=\frac{1}{2}\mathrm{e}^{-2r}(9+\mathrm{e}^{4r+2r'})g_{62}{}^2+18g_{62}{}^2V_{xs}$$
$$+g_{62}{}^2\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle,$$
$$\left\langle\delta^2\left(g_{62}\hat{p}_{c_1'}+g_{62}\hat{p}_{c_2'}+g_{62}\hat{p}_{c_3'}+g_{62}\hat{p}_{c_4'}-\hat{p}_{c_5'}-\hat{p}_{c_7'}\right)\right\rangle=\mathrm{e}^{r'}[(1+4g_{62}{}^2)\cosh(2r+r')-4g_3\sinh(2r+r')]$$
$$+(2+8g_{62}+8g_{62}{}^2)V_{ps}+\langle\delta^2(\hat{p}_{\hat{v}^T})\rangle,\tag{B4}$$

where the gain factors $g_{6j}(j=1,2)$ are

$$g_{61}=\frac{1+3\mathrm{e}^{4r+2r'}+2\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle-2\sqrt{-1-2\mathrm{e}^{4r+2r'}+3\mathrm{e}^{8r+4r'}-2\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle+2\mathrm{e}^{6r+2r'}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle}}{1+3\mathrm{e}^{4r+2r'}+2\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle},$$
$$g_{62}=\frac{\mathrm{e}^{2r+2r'}+2\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle}{4\mathrm{e}^{2r+2r'}-\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle}.\tag{B5}$$

For seven collaborative users, the noises among any submodes and the gain factor are

$$\left\langle\delta^2\left(g_7\hat{x}_{c_1'}+g_7\hat{x}_{c_2'}+g_7\hat{x}_{c_3'}+g_7\hat{x}_{c_4'}+g_7\hat{x}_{c_5'}+g_7\hat{x}_{c_6'}+g_7\hat{x}_{c_7'}\right)\right\rangle=\tfrac{1}{8}\mathrm{e}^{-2r}(49+3\mathrm{e}^{4r+2r'})g_7{}^2+\tfrac{49}{2}g_7{}^2V_{xs}+\tfrac{1}{2}g_7{}^2\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle,$$
$$\left\langle\delta^2\left(g_7\hat{p}_{c_1'}+g_7\hat{p}_{c_2'}+g_7\hat{p}_{c_3'}+g_7\hat{p}_{c_4'}-g_7\hat{p}_{c_5'}-g_7\hat{p}_{c_6'}-\hat{p}_{c_7'}\right)\right\rangle=\tfrac{1}{8}\mathrm{e}^{-2r}[3+\mathrm{e}^{4r+2r'}(1-2g_7{}^2)+4g_7+44g_7{}^2]$$
$$+\left(\tfrac{1}{2}+6g_7+18g_7{}^2\right)V_{ps}+\tfrac{1}{2}\langle\delta^2(\hat{p}_{\hat{v}^T})\rangle,\tag{B6}$$

where

$$g_7=[-49-29\mathrm{e}^{4r+2r'}-6\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle+7\sqrt{6}\sqrt{4\mathrm{e}^{4r+2r'}+2\mathrm{e}^{8r+4r'}-11\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle-\mathrm{e}^{6r+2r'}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle+6\mathrm{e}^{4r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle^2}]$$
$$/2[-49-11\mathrm{e}^{4r+2r'}+18\mathrm{e}^{2r}\langle\delta^2(\hat{x}_{\hat{v}^T})\rangle].\tag{B7}$$

For eight collaborative users, the noises among all the submodes are

$$\begin{aligned}\left\langle \delta^2\left(\hat{x}_{c_1'}+\hat{x}_{c_2'}+\hat{x}_{c_3'}+\hat{x}_{c_4'}+\hat{x}_{c_5'}+\hat{x}_{c_6'}+\hat{x}_{c_7'}+\hat{x}_{c_8'}\right)\right\rangle &= 8\mathrm{e}^{-2r}+32V_{xs},\\ \left\langle \delta^2\left(\hat{p}_{c_1'}+\hat{p}_{c_2'}+\hat{p}_{c_3'}+\hat{p}_{c_4'}-\hat{p}_{c_5'}-\hat{p}_{c_6'}-\hat{p}_{c_7'}-\hat{p}_{c_8'}\right)\right\rangle &= 8\mathrm{e}^{-2r}+32V_{ps}.\end{aligned} \tag{B8}$$

The secret key rate K of the proposed QSS scheme should be the minimum secret sharing rate in each round between the dealer and users [34,52], the secret key rate can be calculated as $K = I(D{:}A) - I(D{:}E)$, where $I(D{:}A)$ is the classical mutual information obtained by the access structure and the amount of possible information eavesdropper can obtain is quantified by the Holevo bound $I(D{:}E)$ [53]. For the Gaussian noise in the BE state and the modulated signals, the optimum mutual information rate can be calculated through the signal-to-noise ratio (SNR,Σ) as [21]

$$I(D:A) = \tfrac{1}{2}\log_2(1+\Sigma). \tag{B9}$$

The classical mutual information among all eight users $I(D{:}A)_8$, any seven users $I(D{:}A)_7$, any six users $I(D{:}A)_6$ and any five users $I(D{:}A)_5$ can be represented as

$$\begin{aligned}I(D:A)_8 &= \frac{1}{2}\log_2\left(1+\frac{4V_s}{e^{-2r}}\right),\\ I(D:A)_7 &= \frac{1}{2}\log_2\left(1+\frac{49g_7^2V_s/2}{e^{-2r}(49+3e^{4r+2r'})g_7^2/8+g_7^2\langle\delta^2\hat{x}_{\hat{v}^T}\rangle/2}\right),\\ I(D:A)_{61} &= \frac{1}{2}\log_2\left(1+\frac{18g_{61}^2V_s}{3e^{-2r}(3+e^{4r+2r'})g_{61}^2/2}\right),\\ I(D:A)_{62} &= \frac{1}{2}\log_2\left(1+\frac{18g_{62}^2V_s}{e^{-2r}(9+e^{4r+2r'})g_{62}^2/2+g_{62}^2\langle\delta^2\hat{x}_{\hat{v}^T}\rangle}\right),\\ I(D:A)_{51} &= \frac{1}{2}\log_2\left(1+\frac{25g_{51}^2V_s/2}{e^{-2r}(25+11e^{4r+2r'})g_{51}^2/8\ +g_{51}^2\langle\delta^2\hat{x}_{\hat{v}^T}\rangle/2}\right),\\ I(D:A)_{52} &= \frac{1}{2}\log_2\left(1+\frac{25g_{53}^2V_s/2}{e^{-2r}(25+3e^{4r+2r'})g_{53}^2/8\ +3g_{53}^2\langle\delta^2\hat{x}_{\hat{v}^T}\rangle/2}\right),\end{aligned} \tag{B10}$$

respectively, where $r' = r$ is used in the theoretical calculation. The Holevo bound $I(D:E)$ between the user's and adversary structure's data is

$$I(D{:}E) = S(\hat{\rho}_E) - \int P_D(s)S_D(\hat{\rho}_{E|D}(s))\,ds, \tag{B11}$$

where $S(\hat{\rho})$ is the von Neumann entropy, $\hat{\rho}_{E|D}$ is the state obtained by the adversary structure when the secret information is prepared by the dealer, and $\hat{\rho}_E$ is the average state obtained by the adversary structure [34]. The secret key rate K_8 is the classical mutual information among all eight users: $K_8 = I(D{:}A)_8$. The secret key rate $K_m(n/2 < m \leqslant n)$ for the $(m, 8)$ QSS protocol, where the m users form the access structure and the adversary structure is the remaining $(8-m)$ users. The secret key rate can be calculated as $K_m = I(D{:}A)_m - I(D{:}E)_{8-m}(m = 7, 6, 5)$. Thus, the secret key rate K_7, $K_{6i}(i = 1, 2)$, $K_{5j}(j = 1, 2)$ for the QSS protocol can be obtained.

We efficiently implement an eight-user QSS, which offers secure and flexible advantages. First, the higher security is demonstrated, and the higher key rate is achieved with eight-partite BE state compared with quadripartite BE state. The secret key rate K_8 and K_4' for all collaborative users with eight-partite BE state with eight- and four-partite BE states can be obtained, respectively:

$$K_8 = \frac{1}{2}\log_2\left(1+\frac{4V_s}{e^{-2r}}\right), \quad K_4' = \frac{1}{2}\log_2\left(1+\frac{2V_s}{e^{-2r}}\right). \tag{B12}$$

Figure 3(b) demonstrates the dependence of the secure key rate on the squeezing factor of BE state, where the red and blue traces show that the secret key rates K_8 and K_4' for the eight and four users, respectively. We can see that the secret key rate with eight-partite BE state K_8 is higher than that with quadripartite BE state K_4'. Our scheme has the clear advantage that the secret key rate is improved compared with the previous scheme.

APPENDIX C: EXPERIMENTAL DETAILS OF CV BE-STATE-BASED QSS

The experimental setup of the QSS based on the CV BE state is given in Fig. 2. The NOPA consists of an α-cut KTP and a concave mirror, serving as the nonlinear crystal and output coupler, respectively. The front surface of the KTP is coated to be used as the input coupler [21]. Through a parametric down-conversion process, quadrature squeezed states $[\hat{a}_i\ (i = 1, 2, 3, 4)]$ are produced [31]. The measured noise power of one of these squeezed states is shown in Fig. 5, indicates a squeezing degree of 4.78 $\pm$ 0.05 dB with a transmission loss of 1%, an average interference efficiency of 98.5%, and a quantum efficiency of 94% for these photodiodes. The four modes $\hat{b}_i$, in the quadripartite GHZ state, are generated by combining modes $\hat{a}_i$ on 50/50 BSs [51]. The eight-partite BE state is produced by combining four submodes of the GHZ entangled state $\hat{b}_i$ and four thermal states of light $[\hat{v}_i^T\ (i = 1, 2, 3, 4)]$ on four BSs. To realize QSS among

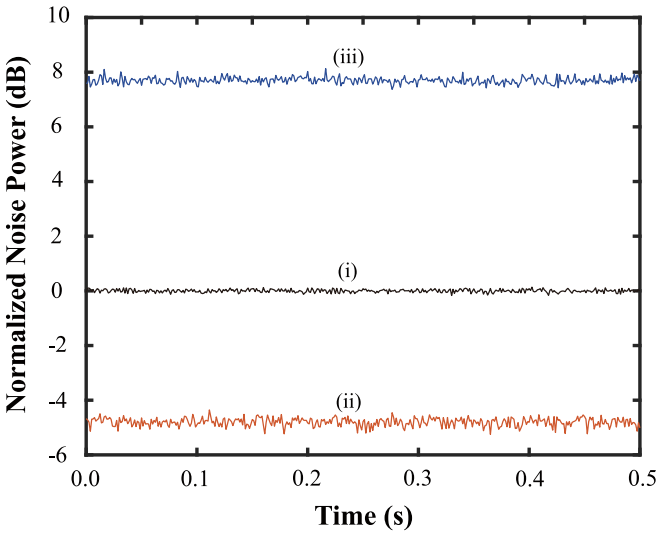

FIG. 5. The measured squeezing noise of the two-mode squeezed state output from the NOPA. (i) The corresponding QNL; (ii) the measured squeezed noise; (iii) the measured antisqueezed noise.

eight users, classical secret information $[a_s = (x_s + ip_s)/2]$ and its phase conjugate $[a_s^* = (x_s - ip_s)/2]$ are modulated onto the submodes of the GHZ entangled state using amplitude and phase modulators. The two components (x_s and p_s) are mutually independent, and the strengths of modulated signals ($V_{xs} = \langle \delta^2 x_s \rangle$ and $V_{ps} = \langle \delta^2 p_s \rangle$) can be controlled by the dealer. In our experiment, the two sets of modulated signals have identical intensity: $V_{xs} = V_{ps}$. The dealer distributes the submodes $[\hat{c}'_j \ (j = 1, 2, , 8)]$ of the BE state to eight users. The output modes $\hat{c}'_j$ are measured by eight sets of balanced homodyne detectors (BHD18) with the help of eight LOs derived from the same laser. According to the correlation variances of different inequalities, the measured photocurrent variances of the respective modes are combined using positive (+) or negative (−) power combiners. The results are then analyzed by a spectrum analyzer to record the desired variety correlation variances. With this experimental setup, the correlation noises of the eight-partite BE state, with an averaged quantum correlation of 4.53 dB below the QNL are measured, as illustrated in Fig. 6, to compile Table I.

The phase stabilization system for the BE state is implemented using active feedforward control. The eight-partite BE state is generated by coupling quadripartite two-mode squeezed state and thermal states on a beam splitter network. For generating the BE state, the NOPA status and the relative phases of beams are locked. The FGPAs provide precise and fast controls of all the PZTs in the cavity and interference mirrors through high-voltage amplifiers. In addition, polarization-division multiplexing is employed to effectively achieve relative phase locking in fiber transmission. While the quadrature correlation of the two-mode squeezed state is 4.78 ± 0.05 dB (trace ii in Fig. 5), the quadrature correlation of the BE state is 4.53 ± 0.07 dB [trace ii in Fig. 6(c)]. The phase fluctuation is inferred from the quadrature correlation of 4.78 ± 0.05 dB and 4.53 ± 0.07 dB before and after the beam splitter network, respectively. Thus, a phase fluctuation of 0.06 rad is obtained.

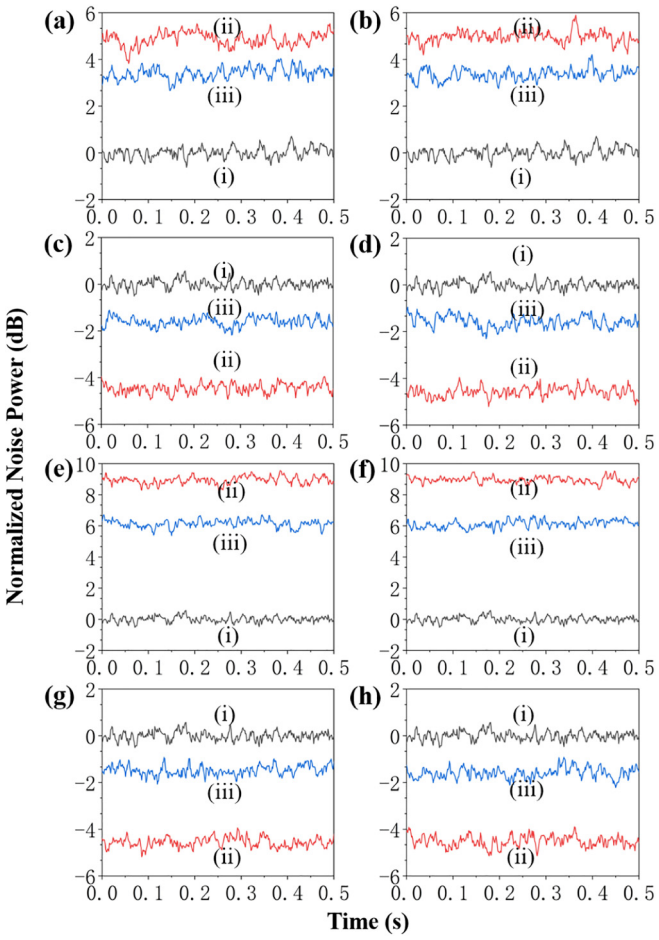

FIG. 6. The measured correlation variances of the BE state at 3 MHz. (a) $\langle \delta^2(\hat{p}_{c_1} - \hat{p}_{c_3}) \rangle$, (b) $\langle \delta^2(\hat{p}_{c_1} - \hat{p}_{c_4}) \rangle$, (c) $\langle \delta^2(\hat{x}_{c_1} + \hat{x}_{c_3} + g_{x2}\hat{x}_{c_2} + g_{x4}\hat{x}_{c_4} + g_{x5}\hat{x}_{c_5} + g_{x6}\hat{x}_{c_6} + g_{x7}\hat{x}_{c_7} + g_{x8}\hat{x}_{c_8}) \rangle$, (d) $\langle \delta^2(\hat{x}_{c_1} + \hat{x}_{c_4} + g_{x2}\hat{x}_{c_2} + g_{x3}\hat{x}_{c_3} + g_{x5}\hat{x}_{c_5} + g_{x6}\hat{x}_{c_6} + g_{x7}\hat{x}_{c_7} + g_{x8}\hat{x}_{c_8}) \rangle$, (e) $\langle \delta^2(\hat{x}_{c_1} - \hat{x}_{c_3}) \rangle$, (f) $\langle \delta^2(\hat{x}_{c_1} - \hat{x}_{c_4}) \rangle$, (g) $\langle \delta^2(\hat{p}_{c_1} + \hat{p}_{c_3} + g_{p2}\hat{p}_{c_2} + g_{p4}\hat{p}_{c_4} - g_{p5}\hat{p}_{c_5} - g_{p6}\hat{p}_{c_6} - g_{p7}\hat{p}_{c_7} - g_{p8}\hat{p}_{c_8}) \rangle$, (h) $\langle \delta^2(\hat{p}_{c_1} + \hat{p}_{c_4} + g_{p2}\hat{p}_{c_2} + g_{p3}\hat{p}_{c_3} - g_{p5}\hat{p}_{c_5} - g_{p6}\hat{p}_{c_6} - g_{p7}\hat{p}_{c_7} - g_{p8}\hat{p}_{c_8}) \rangle$. (i) The corresponding QNL. (ii) The correlation noise power before fiber distribution of BE state. (iii) The correlation noise power after fiber distribution of BE state. The measurement parameters of the spectrum analyzer: RBW 30 kHz; VBW 30 Hz.

QSS enables the secure sharing of secrets with distant parties. Long-distance quantum communication can be realized using either in-line or local LO systems [42,43]. In the in-line LO scheme, both the quantum signal and strong LO are generated by the same laser within the sender, and propagated to the receiver simultaneously, so that the phase noises of the quantum signal and LO are suppressed [44]. The transmission efficiency of BE submodes over a long-distance link can be expressed as $\eta = e^{-\frac{L\times\xi}{10}}$, where L is the transmission distance and ξ is the attenuation factor. The eight submodes can be transmitted over fibers, as $\hat{d}'_j = \sqrt{\eta}\hat{c}'_j + \sqrt{1-\eta}\hat{V}(j = 1, 2, \ldots, 8)$, where $\hat{c}'_j$ is the submode before the fiber and $\hat{V}$ represents the introduced vacuum noise. In our experiment, the quantum properties of quantum states are limited by the coupling loss of the fiber coupler, the

transmission loss of the fiber, and the influence of guided acoustic wave Brillouin scattering [54]. Alternatively, the local LO scheme generates quantum signal and LO using different lasers at the sender and receiver, respectively. The phase noise from the different lasers can be removed by using a pilot [45,46].

Clock synchronization responses for the alignment of the sampling points at the sender and the receiver, while the frame synchronization defines the beginning and end of data. Clock synchronization is implemented by splitting a part of the LO pulses, and their detection results are fed to generate the clock synchronization signals [42]. By inserting the specific training sequences, data synchronization is implemented [47]. In addition, the digital signal processor (DSP) can also realize the clock and frame synchronization by using algorithms [48].

It is crucial to overcome polarization perturbations due to changed environmental conditions. While quantum signal is transmitted in quantum channel, the polarization correction can compensate the polarization drift through the quantum channel. Both the hardware-based automatic feedback and algorithm-based DSP systems can correct polarization [49,50]. Therefore, the automatic feedback system can overcome the long-distance channel perturbations to synchronize clock and frame, as well as calibrate phase and polarization. These techniques makes this protocol feasible in metropolitan areas.

[1] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. Van der Molen, J. W. Los, V. Zwiller, M. A. Versteegh, A. Mura *et al.*, Entanglement distribution over a 96-km-long submarine optical fiber, Proc. Natl. Acad. Sci. USA **116**, 6684 (2019).

[2] C. Portmann and R. Renner, Security in quantum cryptography, Rev. Mod. Phys. **94**, 025008 (2022).

[3] Y. Chen, S. Liu, Y. Lou, and J. Jing, Orbital angular momentum multiplexed quantum dense coding, Phys. Rev. Lett. **127**, 093601 (2021).

[4] S. Hermans, M. Pompili, H. Beukers, S. Baier, J. Borregaard, and R. Hanson, Qubit teleportation between non-neighbouring nodes in a quantum network, Nature (London) **605**, 663 (2022).

[5] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Long-distance measurement-device-independent multiparty quantum communication, Phys. Rev. Lett. **114**, 090501 (2015).

[6] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, An entanglement-based wavelength-multiplexed quantum communication network, Nature (London) **564**, 225 (2018).

[7] Y. Li, Y. Huang, T. Xiang, Y. Nie, M. Sang, L. Yuan, and X. Chen, Multiuser time-energy entanglement swapping based on dense wavelength division multiplexed and sum-frequency generation, Phys. Rev. Lett. **123**, 250505 (2019).

[8] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling *et al.*, A trusted node–free eight-user metropolitan quantum communication network, Sci. Adv. **6**, eaba0959 (2020).

[9] G. Murta and F. Baccari, Self-testing with dishonest parties and device-independent entanglement certification in quantum communication networks, Phys. Rev. Lett. **131**, 140201 (2023).

[10] M. Pompili, S. L. N. Hermans, S. Baier, H. K. C. Beukers, P. C. Humphreys, R. N. Schouten, R. F. L. Vermeulen, M. J. Tiggelman, L. dos Santos Martins, B. Dirkse *et al.*, Realization of a multinode quantum network of remote solid-state qubits, Science **372**, 259 (2021).

[11] X. Wang, J. Fu, S. Liu, Y. Wei, and J. Jing, Self-healing of multipartite entanglement in optical quantum networks, Optica **9**, 663 (2022).

[12] Y. Zheng, C. Zhai, D. Liu, J. Mao, X. Chen, T. Dai, J. Huang, J. Bao, Z. Fu, Y. Tong *et al.*, Multichip multidimensional quantum networks with entanglement retrievability, Science **381**, 221 (2023).

[13] S. Armstrong, J.-F. Morizur, J. Janousek, B. Hage, N. Treps, P. K. Lam, and H.-A. Bachor, Programmable multimode quantum networks, Nat. Commun. **3**, 1026 (2012).

[14] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, Science **362**, eaam9288 (2018).

[15] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[16] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Experimental demonstration of four-party quantum secret sharing, Phys. Rev. Lett. **98**, 020503 (2007).

[17] B. Bell, D. Markham, D. Herrera-Martí, A. Marin, W. Wadsworth, J. Rarity, and M. Tame, Experimental demonstration of graph-state quantum secret sharing, Nat. Commun. **5**, 5480 (2014).

[18] H. Lu, Z. Zhang, L.-K. Chen, Z.-D. Li, C. Liu, L. Li, N.-L. Liu, X. Ma, Y.-A. Chen, and J.-W. Pan, Secret sharing of a quantum state, Phys. Rev. Lett. **117**, 030501 (2016).

[19] S. M. Lee, S.-W. Lee, H. Jeong, and H. S. Park, Quantum teleportation of shared quantum secret, Phys. Rev. Lett. **124**, 060501 (2020).

[20] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Tripartite quantum state sharing, Phys. Rev. Lett. **92**, 177903 (2004).

[21] 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).

[22] G. Leuchs and D. Bruss, *Quantum Information: From Foundations to Quantum Technology Applications* (John Wiley & Sons, New York, 2019).

[23] Z. Yan, J. Qin, Z. Qin, X. Su, X. Jia, C. Xie, and K. Peng, Generation of nonclassical states of light and their application in deterministic quantum teleportation, Fund. Res. **1**, 43 (2021).

[24] K. G. H. Vollbrecht and M. M. Wolf, Activating distillation with an infinitesimal amount of bound entanglement, Phys. Rev. Lett. **88**, 247901 (2002).

[25] J. Zhang, Continuous-variable multipartite unlockable bound entangled Gaussian states, Phys. Rev. A **83**, 052327 (2011).

[26] E. Amselem and M. Bourennane, Experimental four-qubit bound entanglement, Nat. Phys. **5**, 748 (2009).

[27] J. Lavoie, R. Kaltenbaek, M. Piani, and K. J. Resch, Experimental bound entanglement in a four-photon state, Phys. Rev. Lett. **105**, 130501 (2010).

[28] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Secure key from bound entanglement, Phys. Rev. Lett. **94**, 160502 (2005).

[29] R. Augusiak and P. Horodecki, Generalized Smolin states and their properties, Phys. Rev. A **73**, 012318 (2006).

[30] P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Superactivation of bound entanglement, Phys. Rev. Lett. **90**, 107901 (2003).

[31] X. Jia, J. Zhang, Y. Wang, Y. Zhao, C. Xie, and K. Peng, Superactivation of multipartite unlockable bound entanglement, Phys. Rev. Lett. **108**, 190501 (2012).

[32] M. Murao and V. Vedral, Remote information concentration using a bound entangled state, Phys. Rev. Lett. **86**, 352 (2001).

[33] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, Quantum secret sharing with qudit graph states, Phys. Rev. A **82**, 062315 (2010).

[34] H.-K. Lau and C. Weedbrook, Quantum secret sharing with continuous-variable cluster states, Phys. Rev. A **88**, 042313 (2013).

[35] H. Willebrand and B. S. Ghuman, *Free Space Optics: Enabling Optical Connectivity in Today's Networks* (SAMS Publishing, Indianapolis, Indiana, 2002).

[36] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber, Optica **9**, 492 (2022).

[37] 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).

[38] X. Wang, L. Wu, S. Liang, J. Cheng, Y. Liu, Y. Zhou, J. Qin, Z. Yan, and X. Jia, Stabilization improvement of the squeezed optical fields using a high signal-to-noise ratio bootstrap photodetector, Opt. Express **30**, 47826 (2022).

[39] P. Van Loock and A. Furusawa, Detecting genuine multipartite continuous-variable entanglement, Phys. Rev. A **67**, 052315 (2003).

[40] H. Takesue, S. D. Dyer, M. J. Stevens, V. Verma, R. P. Mirin, and S. W. Nam, Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors, Optica **2**, 832 (2015).

[41] S. Shen, C. Yuan, Z. Zhang, H. Yu, R. Zhang, C. Yang, H. Li, Z. Wang, Y. Wang, G. Deng *et al.*, Hertz-rate metropolitan quantum teleportation, Light Sci. Appl. **12**, 115 (2023).

[42] Y.-C. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-distance continuous-variable quantum key distribution over 202.81 km of fiber, Phys. Rev. Lett. **125**, 010502 (2020).

[43] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and B. Xu, Sub-Mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber, Opt. Lett. **48**, 1766 (2023).

[44] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, Nature (London) **421**, 238 (2003).

[45] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Generating the local oscillator locally in continuous-variable quantum key distribution based on coherent detection, Phys. Rev. X **5**, 041009 (2015).

[46] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-referenced continuous-variable quantum key distribution protocol, Phys. Rev. X **5**, 041010 (2015).

[47] D. Lin, P. Huang, D. Huang, C. Wang, J. Peng, and G. Zeng, High performance frame synchronization for continuous variable quantum key distribution systems, Opt. Express **23**, 22190 (2015).

[48] H. M. Chin, N. Jain, U. L. Andersen, D. Zibar, and T. Gehring, Digital synchronization for continuous-variable quantum key distribution, Quantum Sci. Technol. **7**, 045006 (2022).

[49] W. Liu, Y. Cao, X. Wang, and Y. Li, Continuous-variable quantum key distribution under strong channel polarization disturbance, Phys. Rev. A **102**, 032625 (2020).

[50] Y. Pan, H. Wang, Y. Shao, Y. Pi, T. Ye, S. Zhang, Y. Li, W. Huang, and B. Xu, Simple and fast polarization tracking algorithm for continuous-variable quantum key distribution system using orthogonal pilot tone, J. Light. Technol. **41**, 6169 (2023)

[51] 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).

[52] I. Kogias, Y. Xiang, Q. He, and G. Adesso, Unconditional security of entanglement-based continuous-variable quantum secret sharing, Phys. Rev. A **95**, 012315 (2017).

[53] A. S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, Probl. Peredachi Inf. **9**, 3 (1973).

[54] J. Qin, J. Cheng, S. Liang, Z. Yan, H. Lu, and X. Jia, Noiseless and efficient quantum information transmission for fiber-based continuous-variable quantum networks, Phys. Rev. Appl. **21**, 064026 (2024).