Quantum Secret Sharing Among Four Players Using Multipartite Bound Entanglement of an Optical Field

Yaoyao Zhou, Juan Yu, Zhihui Yan, Xiaojun Jia,[*] Jing Zhang,[†] Changde Xie, and Kunchi Peng
State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China
and Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China

(Received 2 June 2017; published 12 October 2018)

Secret sharing is a conventional technique for realizing secure communications in information networks, where a dealer distributes to n players a secret, which can only be decoded through the cooperation of k ($n/2 < k \leq n$) players. In recent years, quantum resources have been employed to enhance security of secret sharing, which has been named quantum secret sharing (QSS). A multipartite bound entanglement (BE) state of an optical field, due to its special entanglement features, can be used in quantum networks to improve security and flexibility of communication. We design and experimentally demonstrate a QSS protocol, where the dealer modulates a secret on a four-partite BE state and then distributes the submodes of the BE state to four spatially separated players. The presented QSS scheme has the capability to protect secrets from eavesdropping and dishonest players, because a nonlocal and deterministic BE state is shared among four authorized players.

DOI: 10.1103/PhysRevLett.121.150502

Secret sharing is a multipartite cryptographic communication scheme, which was introduced independently by Shamir and Blakley in 1979 [1,2]. In the secret sharing protocol, a dealer first distributes secret messages to n players with some particular techniques. Then the secret can be extracted only when k players ($n/2 < k \leq n$) collaborate in forming the access structure, whereas the remaining $n - k$ players cannot obtain any secret even if they work together, thereby forming the adversary structure. Secret sharing provides a significant method for secure network communications and distributed computation. It has been demonstrated in various systems that the security of information networks can be enhanced if quantum resources [3–7] are applied, and the secret sharing protocol using quantum resources has been termed quantum secret sharing (QSS) [8–12]. Varieties of QSS protocols can be summarized by the following three tasks [12,13]: (CC): Classical information is shared among players through secure and private channels. (CQ): Classical information is shared through public or insecure channels. (QQ): A quantum state is shared by distributing QSS states through public channels, also known as quantum state sharing. S. Gaertner *et al.* have experimentally demonstrated a four-party QSS with four-photon entanglement [14]. Later, a five-photon graph-state-based QSS was experimentally realized for sharing both classical and quantum secrets [15]. Very recently, secret sharing of a quantum entangled state was accomplished by employing a six-photon entangled state [16]. Aside from the entangled states of single photons, continuous-variable (CV) entangled states of lights can also be used as quantum resources to implement QSS [17]. A secret coherent state was encoded into a tripartite CV Greenberger-Horne-Zeilinger (GHZ) entangled state of light for performing (2,3) threshold quantum state sharing [18]. In order to construct larger QSS networks with more players, entanglement resources with more entangled parties have to be required [19–22].

Here we design and experimentally demonstrate a new CC QSS protocol, in which a four-partite CV bound entanglement (BE) state is used as the quantum resource. For evaluating the performance of CC QSS tasks, we calculate the secret key rates—i.e., the amount of secure key distilled from the shared quantum states—in order to encode a classical secret [12]. Comparing the secret key rates using BE states and other kinds of entangled states, we show that our scheme has the clear advantage that the secret key rates extracted from two quadrature components are totally balanced. This is difficult in QSS systems based on GHZ and cluster entangled states, as their quantum correlation features are not balanced. A balanced secret sharing rate is important: In the CC QSS task, the balanced secret sharing rate can result in an optimal classical processing efficiency, while in the CQ and QQ QSS tasks, the balanced secret sharing rate can be easily used to find the possible eavesdropping, whichever basis is selected in the measurement.

The schematics of experimental principle and setup are shown in Figs. 1(a) and 1(b), respectively. According to the features of the multipartite BE state, no pure entanglement can be distilled between any two parties by means of local operation and classical communication [23–27]. The dealer prepares a four-partite BE state by combining two

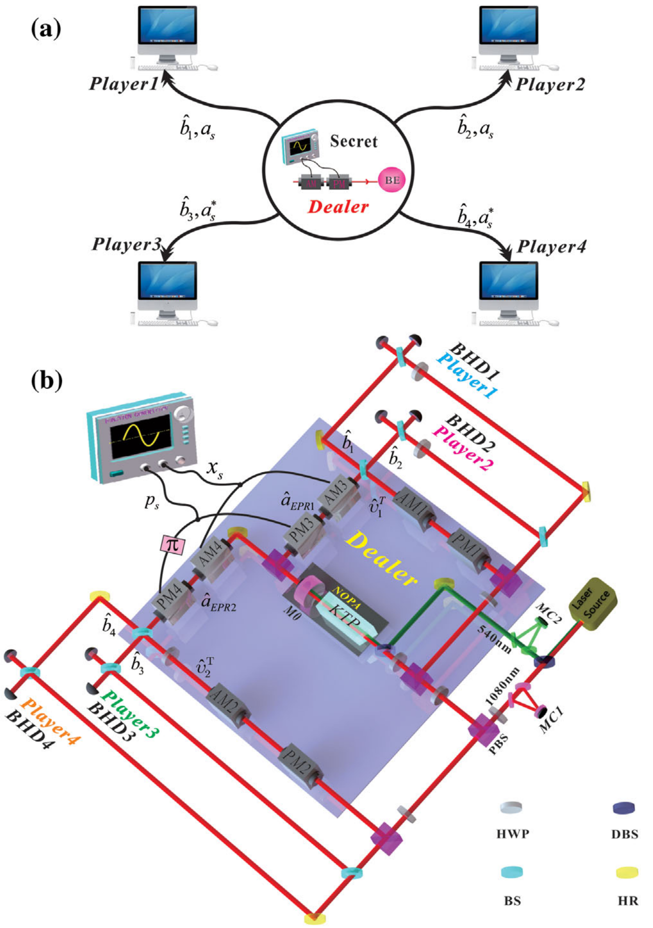

FIG. 1. Schematics of the experimental principle and setup for QSS using a four-partite BE state. (a) Diagram for the QSS. (b) Experimental setup for generating a four-partite BE state and implementing the QSS scheme. MC1 and MC2: Mode cleaner cavity. HWP: Half-wave plate. PBS: Polarization beam splitter. DBS: Dichroic beam splitter. BS: 50:50 beam splitter. HR: Mirror with high reflection. NOPA: Nondegenerate optical parametric amplifier. AM1–AM4: Amplitude modulator. PM1–PM4: Phase modulator. BHD1–BHD4: Balanced homodyne detector.

submodes of an Einstein-Podolsky-Rosen (EPR) entangled state ($\hat{a}_{\mathrm{EPR1}}$ and $\hat{a}_{\mathrm{EPR2}}$) and two thermal states of light ($\hat{\upsilon}_1^T$ and $\hat{\upsilon}_2^T$) on two 50:50 beam splitters (BSs), respectively. Then the four submodes ($\hat{b}_j$, $j = 1, 2, 3, 4$) of the obtained BE state are distributed to four players. The submode ($\hat{b}_j$) can be expressed in terms of the amplitude ($\hat{x}_j = \hat{b}_j + \hat{b}_j^+$) and phase [$\hat{p}_j = (\hat{b}_j - \hat{b}_j^+)/i$] quadratures with the canonical commutation relation $[\hat{x}_j, \hat{p}_j] = 2i$. The combination noises of quadrature amplitudes and phases among submodes of the BE state depend on the correlation factor r of the initial EPR entanglement [27]. If r is high, the noises of quadrature amplitudes [$\langle \Delta^2(\hat{x}_{b_1} + \hat{x}_{b_2} + \hat{x}_{b_3} + \hat{x}_{b_4})\rangle = 4e^{-2r}$] and phases [$\langle \Delta^2(\hat{p}_{b_1} + \hat{p}_{b_2} - \hat{p}_{b_3} - \hat{p}_{b_4})\rangle = 4e^{-2r}$] among submodes will be much lower than the corresponding quantum noise limit (QNL). The noise in quadrature amplitude (phase) of the thermal state [$\hat{x}(\hat{p})_{\upsilon^T_{1(2)}}$] should match the nondistillability requirement of the BE state, i.e., $V_T = \langle \Delta^2 \hat{x}(\hat{p})_{\upsilon_1^T}\rangle = \langle \Delta^2 \hat{x}(\hat{p})_{\upsilon_2^T}\rangle = \langle \Delta^2 \hat{x}(\hat{p})_{\upsilon^T}\rangle \geq 2\text{–}3e^{-2r} + 2\sqrt{1-2e^{-2r}+2e^{-4r}}$ [27,28]. For realizing QSS amongst four players, 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 submodes of an EPR entangled state ($\hat{a}_{\mathrm{EPR1}}$ and $\hat{a}_{\mathrm{EPR2}}$) by amplitude modulators (AM3 and AM4) and phase modulators (PM3 and PM4), respectively. The two components (x_s and p_s) are mutually independent, and the strengths of modulated signals ($V_{xs} = \langle x_s\rangle^2$ and $V_{ps} = \langle p_s\rangle^2$) can be controlled by the dealer. In our experiment, two sets of modulated signals have identical intensity: $V_s = V_{xs} = V_{ps}$. The nullifiers $\hat{N}_1$ and $\hat{N}_2$ of the CV BE state are expressed by [12]

$$\hat{N}_1 = \hat{x}_{b_1} + \hat{x}_{b_2} + \hat{x}_{b_3} + \hat{x}_{b_4} + x_s,$$
$$\hat{N}_2 = \hat{p}_{b_1} + \hat{p}_{b_2} - \hat{p}_{b_3} - \hat{p}_{b_4} + p_s. \tag{1}$$

In principle, if we have an infinitely squeezed state, the secret can be protected from the adversary structure and extracted perfectly by the access structure. However, for the practical case of finite squeezing, the classical secret cannot be perfectly recovered by the access structure while partial information is leaked into the adversary structure. Thus, we need to calculate the secret key rate, which is usually used in CV quantum key distribution (QKD) to distill the secure secret key [29,30]. In Ref. [12], the derivation of the minimum secret key rate K is provided for a single-variable QSS. Although amplitude and phase components are used to share the secret in our proposal, these two components are completely independent, and only one quadrature is measured at a specified time. The minimum secret key rate K in our experiment can also be expressed by

$$K = I(D{:}A) - I(D{:}E), \tag{2}$$

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. The calculation details and results are given in the Supplemental Material [31–35]. The classical mutual information among all four players [$I(D{:}A)_4$] and any three players [$I(D{:}A)_3$] are expressed by [31]

$$I(D{:}A)_4 = \frac{1}{2}\log_2(1 + 2e^{2r}V_s), \tag{3}$$

$$I(D{:}A)_3 = \frac{1}{2}\log_2\left(1 + \frac{4e^{4(r+r')}V_s}{2e^{2r+4r'} + 2e^{-2r+2r'} + (e^{2(r+r')} + e^{-2r})^2 V_T}\right), \tag{4}$$

respectively, where $(r + r')$ is the antisqueezed parameter for the antisqueezed quadrature components of the initial EPR state. The value of the extra noise factor r' is not a constant, and it increases with the increase of r. Using the measured noise of quadrature components, we get $r' \simeq 2r/3$, which is used in our theoretical calculation. If four players collaborate, they form the access structure, and the secret key rate K_4 is equal to the mutual information obtained by the access structure, $I(D{:}A)_4$. For (3,4) threshold QSS, the access structure is the collaboration of any three players, and the adversary structure is the remaining one. Based on the special correlation characteristics of the BE state, $I(D{:}A)_3$ is almost kept at a specified value and $I(D{:}E)_1$ decreases with the increase of r. Thus, the secret key rate of any three players K_3 is able to be higher than 0, and (3, 4) threshold QSS can be realized. On the other hand, the cooperation of any two players should not obtain the shared secret, and thus the secret key rate with the collaboration of any two players K_2 should always be below zero [31].

Figure 2 presents the theoretical results of K_3 and K_4 as functions of the strength of modulated signals for various r. There, the dashed, solid, and dotted traces correspond to $r = 1.5$, 0.93, 0.5, respectively. (Note that $r = 0.93$ is the measured value in our experiment.) The blue and red traces depict the secret key rates of K_4 and K_3, respectively. We see that K_4 and K_3 are always positive, indicating that QSS of four players and of any three players can be realized in our system. Although CC QSS protocol can also be implemented with four-partite GHZ and linear cluster entangled states, only QSS based on a CV BE state shows the balanced feature between the secret key rates of amplitude quadrature and phase quadrature [31]).

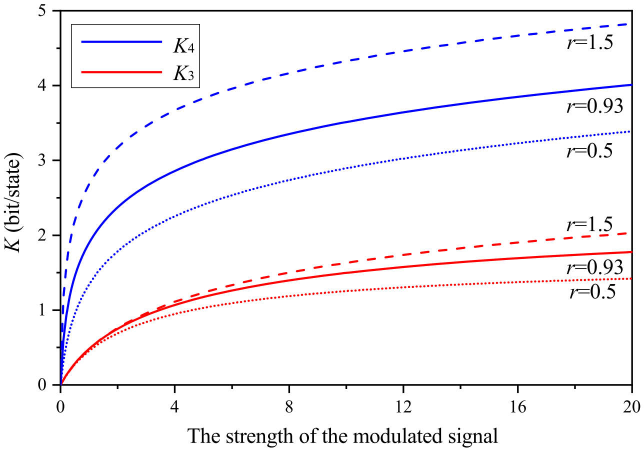

FIG. 2. The calculated dependences of the secure key rate K on the strength of a modulated signal for different correlation factors r. The blue and red traces are the corresponding traces for the collaboration of four players and of any three players, respectively. The dashed, solid, and dotted traces correspond to correlation factors r of 1.5, 0.93 and 0.5, respectively, where $r = 0.93$ corresponds to our experimental condition.

The schematic of the experimental setup is shown in Fig. 1(b). The laser source (CDPSSFG-VIB, made by the YuGuang company) is a solid-state single-frequency and stable-frequency continuous wave Nd:YAP/LBO laser with two output wavelengths at 540 and 1080 nm. The two output lasers are separated into two parts by a dichroic beam splitter (DBS) coated for high reflection (HR) at 540 nm and antireflection (AR) at 1080 nm. The mode cleaner MC1 (MC2) is a three-mirror ring cavity that provides the spatiotemporal filtering of the 1080 nm (540 nm) laser for the downstream experiment. The finesse of MC1 (MC2) is 500 (650) for 1080 nm (540 nm). The cleaned laser beam at 540 nm is injected into a nondegenerate optical parametric amplifier (NOPA) as the pump field. The cleaned laser at 1080 nm is separated into seven parts, four parts of which serve as local oscillators (LO) in each balanced homodyne detector (BHD$_j$, $j = 1$–4). The power and the polarization of LO in each BHD are adjusted by means of rotating the half-wave plate (HWP) in front of a polarization beam splitter (PBS). Two parts are used to generate the thermal states $(\hat{\nu}_1^T, \hat{\nu}_2^T)$ by modulating the amplitude and phase quadratures with noisy signals of Gaussian function distribution: The modulations are implemented by amplitude and phase modulators [AM1(2) and PM1(2)], respectively, connected to Gaussian random signal generators. The noises of thermal states in both quadratures are chosen as $\langle \Delta^2 \hat{x}_{\nu^T} \rangle = \langle \Delta^2 \hat{p}_{\nu^T} \rangle = 3.5$, which satisfies the requirement of nondistillability of the BE state [27]. The last part of the cleaned infrared beam is used as the seed beam injected into the NOPA. The NOPA consists of a wedged type-II noncritical phase matching a KTiOPO$_4$ (KTP) of dimensions $3 \times 3 \times 10\ \text{mm}^3$ and a concave mirror (M0) with a radius of curvature of 50 mm. M0 is coated for a transmission of $T = 12.5\%$ for 1080 nm and HR for 540 nm to be used as the output coupler of the NOPA. The front face of the KTP crystal is HR-coated for 1080 nm and $T_0 = 20\%$ for 540 nm, which serves as the input coupler of the NOPA. The end face of the KTP is AR-coated for both 1080 and 540 nm [36]. When the relative phase between the pump and the injected seed beam is locked to $\pi + 2m\pi$ (where m is an integer), the EPR entangled state with anticorrelation of quadrature amplitudes and correlation of quadrature phases is produced. When the relative phase between the signal beam and the corresponding LO in BHD$_j$ is controlled at $m\pi$ or $\pi/2 + m\pi$ (where m is an integer), the combination noises of the quadrature amplitude and quadrature phase of the signal beam are measured, respectively [36,37]. The measured noises of the two quadratures of the EPR entangled state are 8.1 ± 0.2 dB below the corresponding QNL, which means $\langle \Delta^2(\hat{x}_{a_{\text{EPR1}}} + \hat{x}_{a_{\text{EPR2}}}) \rangle = \langle \Delta^2(\hat{p}_{a_{\text{EPR1}}} - \hat{p}_{a_{\text{EPR2}}}) \rangle = 0.31 \pm 0.01$. The measured noise levels of the amplitude difference and phase sum for the EPR state are about 13.6 ± 0.2 dB above the corresponding QNL; i.e., $\langle \Delta^2(\hat{x}_{a_{\text{EPR1}}} - \hat{x}_{a_{\text{EPR2}}}) \rangle = \langle \Delta^2(\hat{p}_{a_{\text{EPR1}}} + \hat{p}_{a_{\text{EPR2}}}) \rangle = 45.7 \pm 2.3$, from which the correlation factor $r = 0.932$ and the extra noise factor $r' = 0.632$ [36].

In order to realize QSS, a classical secret message and its phase conjugate are first modulated, respectively, on two submodes of an EPR entangled state ($\hat{a}_{\mathrm{EPR1}}$ and $\hat{a}_{\mathrm{EPR2}}$). Then $\hat{a}_{\mathrm{EPR1}}$ ($\hat{a}_{\mathrm{EPR2}}$) and a thermal state $\hat{\upsilon}_1^T$ ($\hat{\upsilon}_2^T$) interfere on a BS, producing two output submodes, $\hat{b}_1$ and $\hat{b}_2$ ($\hat{b}_3$ and $\hat{b}_4$). Thus, the secret message is carried by all four submodes ($\hat{b}_1$, $\hat{b}_2$, $\hat{b}_3$, and $\hat{b}_4$), which are sent to four space-separated players. The noise spectra of their amplitude and phase quadratures are detected by BHD$_j$, consisting of a BS and two high-efficiency photodiodes. The submodes received by the four players are expressed by [28]

$$\hat{b}_{1(2)} = (\hat{a}_{\mathrm{EPR1}} \pm \hat{\upsilon}_1^T + a_s)/\sqrt{2}, \tag{5}$$

$$\hat{b}_{3(4)} = (\hat{a}_{\mathrm{EPR2}} \pm \hat{\upsilon}_2^T + a_s^*)/\sqrt{2}. \tag{6}$$

The noise power spectra of the quadrature amplitude and phase from 2.0 to 2.5 MHz for different collaborations of players measured by spectrum analyzers (SAs) are shown in Figs. 3(a) and 3(b), where the modulated sinusoidal signals at 2.25 MHz with 1.52 Vpp are generated from the arbitrary signal generators (the corresponding V_s is 2.40). The blue traces are the noise with the collaboration of four players $\{1,2,3,4\}$, which are 7.8 ± 0.2 dB below the corresponding QNL, i.e., $\langle \Delta^2(\hat{x}_{b_1} + \hat{x}_{b_2} + \hat{x}_{b_3} + \hat{x}_{b_4})\rangle = \langle \Delta^2(\hat{p}_{b_1} + \hat{p}_{b_2} - \hat{p}_{b_3} - \hat{p}_{b_4})\rangle = 0.66 \pm 0.03$. The red traces are the noise with the collaboration of any three players, which are 1.0 ± 0.2 dB above the corresponding QNL, i.e., $\langle \Delta^2(g_1^{xopt}\hat{x}_{b_1} + g_2^{xopt}\hat{x}_{b_2} + \hat{x}_{b_{3(4)}})\rangle = \langle \Delta^2(\hat{x}_{b_{1(2)}} + g_3^{xopt}\hat{x}_{b_3} + g_4^{xopt}\hat{x}_{b_4})\rangle = 1.90 \pm 0.08$ and $\langle \Delta^2(g_1^{popt}\hat{p}_{b_1} + g_2^{popt}\hat{p}_{b_2} - \hat{p}_{b_{3(4)}})\rangle = \langle \Delta^2(\hat{p}_{b_{1(2)}} - g_3^{popt}\hat{p}_{b_3} - g_4^{popt}\hat{p}_{b_4})\rangle = 1.90 \pm 0.08$, where $g_j^{xopt} = 0.493$ and $g_j^{popt} = 0.493$ ($j = 1, 2, 3, 4$) are the optimal classical gains for minimizing the noises. The black traces are the noise of submodes $\hat{b}_1$ and $\hat{b}_2$ as well as $\hat{b}_3$ and $\hat{b}_4$, which are 10.5 ± 0.2 dB above the QNL. The pink traces correspond to the noise with other combinations of two players [the collaborations of player 1 and player 3, player 1 and player 4, player 2 and player 3, as well as player 2 and player 4 are labeled by $\{1(2), 3(4)\}$], which are 4.5 ± 0.2 dB above the QNL. The green traces correspond to the noise measured by any individual player, which are 8.7 ± 0.2 dB above the corresponding QNL. The signal-noise ratio (SNR)—i.e., the ratio of signal power to noise power as denoted by Σ—depends on both the amplitude of the signal and the noise power level [38,39]. We can see that the modulated secret signals can be extracted when four players or any three players cooperate, with the corresponding SNRs being $\Sigma_4 = 30.8$ and $\Sigma_3 = 1.2$, respectively. It is natural that the secret key rate among four players is higher than that for the collaboration of any three players in QSS, as quantum correlation among four submodes is much better than that among any three.

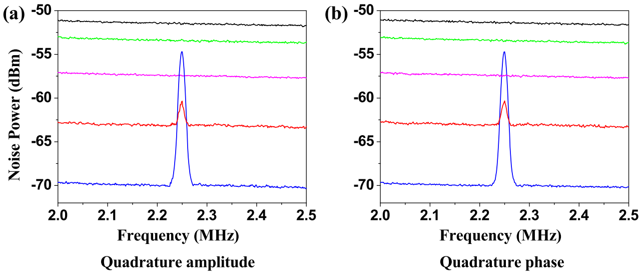

FIG. 3. The measured noise power spectra with different combinations of players for QSS. (a) The measured noises of quadrature amplitude. (b) The measured noises of the quadrature phase. The blue traces are the noise with the collaboration of four players $\{1,2,3,4\}$. The red traces are the noise with the collaboration of any three players. The black traces correspond to the noise with the collaboration of $\{1,2\}$ as well as $\{3,4\}$, and the pink traces correspond to the noise with the collaboration of $\{1(2), 3(4)\}$. The green traces correspond to the noise measured by any individual player. The value of the peak at the frequency of 2.25 MHz represents the strength of the measured signal power. The measurement parameters are as follows for the spectrum analyzer (SA): Resolution bandwidth (RBW): 10 kHz. Video bandwidth (VBW): 100 Hz.

For visualizing the performance of the QSS system, a simple communication paradigm with a modulated information string is shown in Fig. 4. The dealer modulates randomly a set of keys [Fig. 4(a)], which correspond to different modulation voltages given by the arbitrary signal generator, on the amplitude quadrature of an EPR state. Then the dealer distributes four submodes of the BE state to

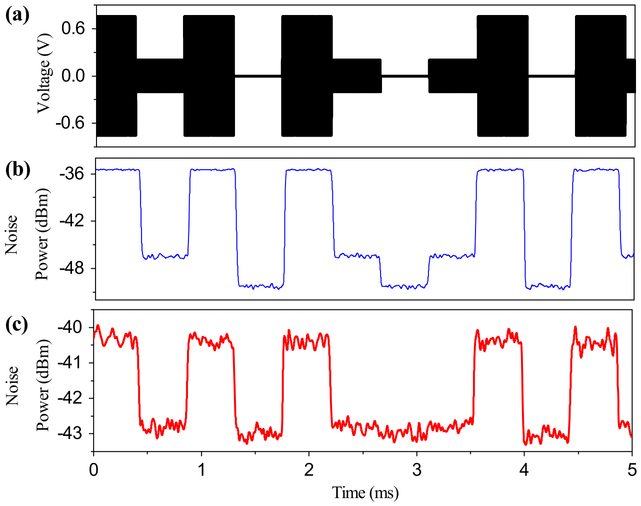

FIG. 4. Schematic of a secret string communication. (a) Modulated secret string by dealer. (b) and (c) The measured results by the collaboration of four players and by any three players, respectively. The measurement parameters are as follows for the SA: RBW: 300 kHz. VBW: 100 kHz.

four players as described before. Figures 4(b) and 4(c) are the measured results with QSS schemes by the collaborations of four players and three players, respectively. When the strength of modulated signals is higher (the modulation voltage of the signal generators is 1.52 Vpp, and the corresponding V_s is 2.40), the shared secrets can be easily extracted by the collaboration of four players or by any three players. When the modulation voltage is reduced to 0.40 Vpp (the corresponding V_s is 0.63), the shared secrets still can be extracted by the collaboration of all four players, but it is difficult for the collaboration of any three players. The duration time of 2.25 MHz modulated signals is 0.444 ms, and the estimated speed rate of QSS communication is about 2.25 kbit/s, which is limited by the squeezed bandwidth of the initial EPR state.

In conclusion, we have experimentally implemented a four-player-threshold CC QSS based on a CV four-partite BE state. Although the size of the present experimental setup is $0.9 \times 1.2\ \mathrm{m}^2$, the spatial distances among players can be distant when the quantum entanglement distributed among them has not been totally destroyed by transmission losses or extra noise. When a BE state with more submodes is available, the presented QSS scheme can be directly extended to larger systems with many more players. While we merely demonstrated CC QSS protocol, CQ and QQ QSS can be also implemented based on the BE in a similar fashion. The basic communication techniques of the presented QSS scheme, except for an offline prepared BE state, are compatible with that of classical secret sharing, which thus opens a convenient and favorable path for practical applications of QSS.

The authors wish to thank Hoi-Kwan Lau, Christian Weedbrook, and Xuyang Wang for helpful discussions. Our work was supported by the Key Project of the National Key R&D program of China (Grants No. 2016YFA0301402 and No. 2016YFA0301602), the National Natural Science Foundation of China (Grants No. 11474190, No. 11804246, No. 61775127, and No. 11654002), the Program for Sanjin Scholars of Shanxi Province, and the fund for Shanxi "1331 Project" Key Subjects Construction.

[*] jiaxj@sxu.edu.cn
[†] jzhang74@sxu.edu.cn

[1] A. Shamir, How to share a secret, Commun. ACM **22**, 612 (1979).

[2] G. R. Blakley, Safeguarding cryptographic keys, Proc. of AFIPS 1979 Nat. Computer Conf. **48**, 313 (1979).

[3] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, Advances in quantum teleportation, Nat. Photonics **9**, 641 (2015).

[4] T. C. Ralph and P. K. Lam, A bright future for quantum communications, Nat. Photonics **3**, 671 (2009).

[5] X. L. Su, S. H. Hao, X. W. Deng, L. Y. Ma, M. H. Wang, X. J. Jia, C. D. Xie, and K. C. Peng, Gate sequence for continuous variable one-way quantum computation, Nat. Commun. **4**, 2828 (2013).

[6] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, Detection of 15 dB Squeezed States of Light and Their Application for the Absolute Calibration of Photoelectric Quantum Efficiency, Phys. Rev. Lett. **117**, 110801 (2016).

[7] X. L. Su, C. Tian, X. Deng, Q. Li, C. D. Xie, and K. C. Peng, Quantum Entanglement Swapping between Two Multipartite Entangled States, Phys. Rev. Lett. **117**, 240503 (2016).

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

[9] A. Karlsson, M. Koashi, and N. Imoto, Quantum entanglement for secret sharing and secret splitting, Phys. Rev. A **59**, 162 (1999).

[10] W. Tittel, H. Zbinden, and N. Gisin, Experimental demonstration of quantum secret sharing, Phys. Rev. A **63**, 042301 (2001).

[11] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography, Phys. Rev. Lett. **95**, 200502 (2005).

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

[13] D. Markham and B. C. Sanders, Graph states for quantum secret sharing, Phys. Rev. A **78**, 042309 (2008).

[14] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Experimental Demonstration of Four-Party Quantum Secret Sharing, Phys. Rev. Lett. **98**, 020503 (2007).

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

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

[17] T. Tyc and B. C. Sanders, How to share a continuous-variable quantum secret by optical interferometry, Phys. Rev. A **65**, 042310 (2002).

[18] 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).

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

[20] V. Karimipour and M. Asoudeh, Quantum secret sharing and random hopping: Using single states instead of entanglement, Phys. Rev. A **92**, 030301 (2015).

[21] A. Tavakoli, I. Herbauts, M. Żukowski, and M. Bourennane, Secret sharing with a single d-level quantum system, Phys. Rev. A **92**, 030302 (2015).

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

[23] M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-State Entanglement and Distillation: Is there a "Bound" Entanglement in Nature?, Phys. Rev. Lett. **80**, 5239 (1998).

[24] M. Murao and V. Vedral, Remote Information Concentration Using a Bound Entangled State, Phys. Rev. Lett. **86**, 352 (2001).

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

[26] A. Acín, J. I. Cirac, and Ll. Masanes, Multipartite Bound Information Exists and can be Activated, Phys. Rev. Lett. **92**, 107903 (2004).

[27] X. J. Jia, J. Zhang, Y. Wang, Y. P. Zhao, C. D. Xie, and K. C. Peng, Superactivation of Multipartite Unlockable Bound Entanglement, Phys. Rev. Lett. **108**, 190501 (2012).

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

[29] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

[30] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of longdistance continuous-variable quantum key distribution, Nat. Photonics **7**, 378 (2013).

[31] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.121.150502 for the noise of combinations among submodes of a BE state, the secret key rate *K* for our QSS protocols, and the secret key rate *K* for QSS protocols with other quadripartite entangled states, which includes Refs. [32–35].

[32] M. D. Reid, Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification., Phys. Rev. A **40**, 913 (1989).

[33] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Realization of the Einstein-Podolsky-Rosen Paradox for Continuous Variables., Phys. Rev. Lett. **68**, 3663 (1992).

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

[35] X. L. Su, A. H. Tan, X. J. Jia, J. Zhang, C. D. Xie, and K. C. Peng, Experimental Preparation of Quadripartite Cluster and Greenberger-Horne-Zeilinger Entangled States for Continuous Variables., Phys. Rev. Lett. **98**, 070502 (2007).

[36] Y. Y. Zhou, X. J. Jia, F. Li, C. D. Xie, and K. C. Peng, Experimental generation of 8.4 dB entangled state with an optical cavity involving a wedged type-II nonlinear crystal, Opt. Express **23**, 4952 (2015).

[37] G. Hétet, O. Glöckl, K. A. Pilypas, C. C. Harb, B. C. Buchler, H.-A. Bachor, and P. K. Lam, Squeezed light for bandwidth-limited atom optics experiments at the rubidium D1 line, J. Phys. B **40**, 221 (2007).

[38] N. Treps, N. Grosse, W. P. Bowen, M. T. L. Hsu, A. Maitre, C. Fabre, H-A Bachor, and P. K. Lam, Nano-displacement measurements using spatially multimode squeezed light, J. Opt. B **6**, S664 (2004).

[39] H. X. Sun, K. Liu, Z. L. Liu, P. L. Guo, J. X. Zhang, and J. R. Gao, Small-displacement measurements using high-order Hermite-Gauss modes, Appl. Phys. Lett. **104**, 121908 (2014).