Secret Sharing of a Quantum State

He Lu,[1,2,4] Zhen Zhang,[3] Luo-Kan Chen,[1,2,4] Zheng-Da Li,[1,2,4] Chang Liu,[1,2,4] Li Li,[1,2,4,*] Nai-Le Liu,[1,2,4] Xiongfeng Ma,[3] Yu-Ao Chen,[1,2,4] and Jian-Wei Pan[1,2,4]

[1]*Shanghai Branch, National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Shanghai 201315, China*

[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China*

[3]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

[4]*CAS-Alibaba Quantum Computing Laboratory, Shanghai 201315, China*

(Received 27 April 2016; revised manuscript received 21 June 2016; published 13 July 2016)

Secret sharing of a quantum state, or quantum secret sharing, in which a dealer wants to share a certain amount of quantum information with a few players, has wide applications in quantum information. The critical criterion in a threshold secret sharing scheme is confidentiality: with less than the designated number of players, no information can be recovered. Furthermore, in a quantum scenario, one additional critical criterion exists: the capability of sharing entangled and unknown quantum information. Here, by employing a six-photon entangled state, we demonstrate a quantum threshold scheme, where the shared quantum secrecy can be efficiently reconstructed with a state fidelity as high as 93%. By observing that any one or two parties cannot recover the secrecy, we show that our scheme meets the confidentiality criterion. Meanwhile, we also demonstrate that entangled quantum information can be shared and recovered via our setting, which shows that our implemented scheme is fully quantum. Moreover, our experimental setup can be treated as a decoding circuit of the five-qubit quantum error-correcting code with two erasure errors.

DOI: 10.1103/PhysRevLett.117.030501

Suppose that two presidents have established a secure quantum channel via sharing of entangled states, such as many Einstein-Podolsky-Rosen (EPR) pairs. At some point, one president takes a vacation and does not trust her individual vice presidents entirely; she therefore decides to divide up her halves of the EPR pairs into shares and distributes to the vice presidents in a quantum secret sharing (QSS) scheme. Only when all of the vice presidents work together are they allowed to communicate with the other president. Hence, in quantum cryptography, for instance, QSS can help to establish a quantum key in a multipartite scenario. Moreover, in a long-distance quantum network, the quantum channels, by which a quantum state can be transmitted between remote nodes, are typically very lossy. QSS is an efficient error correction protocol against qubit losses as erasure errors. Furthermore, QSS provides a robust and secure solution for quantum state storage and computation [1].

A significant class of secret sharing schemes is the (k, n) threshold scheme, which is described as follows. The dealer encodes the initial secret into a large system composed of n parts, and sends each player a share. To recover the dealer's information, at least k (with $k \leq n$) players should combine their shares together. Any subgroup with less than k players is forbidden to decode any knowledge about the shared information. There are two criteria in a (k, n) threshold scheme. The first criterion is reliability; if more than k players combine their shared piece together, the information originating from the dealer can be faithfully recovered. The second criterion is confidentiality [2,3]; otherwise, with less than k players, no information can be recovered. The no-cloning theorem [4,5] implies that no quantum (k, n) threshold scheme exists for $2k \leq n$. In QSS, a third critical criterion exists, namely, the capability of sharing entangled and unknown quantum information, as required in the aforementioned quantum cryptography example. Note that the third criterion can also be understood as maintaining coherence of quantum states during processing, which is generally required in quantum communication and quantum information. Numerous attempts to realize QSS have been reported in the literature; however, none of them satisfies all three criteria. For instance, in many experiments, quantum means are employed to share classical information [6–9], none of which can satisfy the confidentiality criterion when used for sharing a quantum state. In other implemented schemes [10–12], pure-qubit state sharing has been demonstrated; however, entangled states have never been shared and recovered.

In their seminal work, Cleve, Gottesman, and Lo [1] showed that for any $k \leq n \leq 2k-1$, efficient constructions of quantum threshold schemes exist. The essential idea is that a quantum $(k, 2k-1)$ threshold scheme can be realized by a quantum error-correcting code that is capable of correcting $k-1$ erasure errors with a code length of $2k-1$. Intuitively, if an error-correcting code can correct $k-1$ erasure errors, any k shares can recover the initial state by treating the missing $k-1$ shares as erasure errors. Any

information gain of the unknown initial state by measuring $k-1$ shares leads to disturbance of the recovered state by the remaining k shares. Because k shares can be used to perfectly reconstruct the initial state, no information can be obtained by less than $k-1$ shares; otherwise, the principle of "information gain means disturbance" in quantum mechanics is violated [13]. Furthermore, for a general case with $n \leq 2k-1$, the quantum (k, n) threshold scheme can be constructed by discarding $2k-1-n$ shares from a quantum $(k, 2k-1)$ threshold scheme.

According to the Cleve-Gottesman-Lo secret sharing theory [1], the (3,3) threshold scheme is inherited from the five-qubit quantum error-correcting code [14]. The derivations are reviewed in Sec. I of the Supplemental Material [15]. The dealer holds the to-be-shared quantum state $\alpha|H\rangle+\beta|V\rangle$, which, in principle, could be unknown to the dealer, and encodes it into a three-photon mixed state

$$\rho_{\mathrm{QSS}}=\frac{1}{4}\sum_{i,j=0}^{1}|\phi_{ij}\rangle\langle\phi_{ij}| \tag{1}$$

with

$$\begin{aligned}
|\phi_{00}\rangle &= \frac{1}{\sqrt{2}}(\alpha|H\rangle+\beta|V\rangle)_A(|HH\rangle-|VV\rangle)_{BC}-\frac{1}{\sqrt{2}}(\beta|H\rangle-\alpha|V\rangle)_A(|HH\rangle+|VV\rangle)_{BC},\\
|\phi_{01}\rangle &= \frac{1}{\sqrt{2}}(\alpha|H\rangle+\beta|V\rangle)_A(|HH\rangle-|VV\rangle)_{BC}+\frac{1}{\sqrt{2}}(\beta|H\rangle-\alpha|V\rangle)_A(|HH\rangle+|VV\rangle)_{BC},\\
|\phi_{10}\rangle &= \frac{1}{\sqrt{2}}(\alpha|V\rangle+\beta|H\rangle)_A(|HV\rangle-|VH\rangle)_{BC}-\frac{1}{\sqrt{2}}(\alpha|H\rangle-\beta|V\rangle)_A(|VH\rangle+|HV\rangle)_{BC},\\
|\phi_{11}\rangle &= \frac{1}{\sqrt{2}}(\alpha|V\rangle+\beta|H\rangle)_A(|HV\rangle-|VH\rangle)_{BC}+\frac{1}{\sqrt{2}}(\alpha|H\rangle-\beta|V\rangle)_A(|VH\rangle+|HV\rangle)_{BC},
\end{aligned} \tag{2}$$

where $|H\rangle$ and $|V\rangle$ denote horizontal and vertical polarization, respectively. The subscripts A, B, and C represent the three players Alice, Bob, and Charlie in the scheme. Note that the to-be-shared quantum state can be unknown to the dealer. In fact, it can be a part of a large entangled state.

The quantum state of Eq. (1) can also be treated as the five-qubit code state after two erasure errors. Thus, if we can show that the original qubit can be recovered from Eq. (1), we can conclude that the five-qubit code is capable of correcting two erasure errors, which has been proven to be equivalent to correcting an arbitrary error [16]. Hence, such decoding circuits could also demonstrate that the five-qubit code is capable of correcting an arbitrary qubit error.

To generate the three-photon mixed state ρ_{QSS}, we employ a six-photon entangled state. A schematic of the experimental setup is shown in Fig. 1. An ultraviolet laser pulse (~140 fs, 76 MHz, 390 nm) successively passes through three 2-mm-thick β-barium borate (BBO) crystals to generate three entangled photon pairs [17]. We then overlap the two generated photons on a polarizing beam splitter (PBS) to generate an ultrabright entangled photon pair [18]. For paths i, j, the entangled pair state is $|\Phi^+\rangle_{ij}=(|HH\rangle_{ij}+|VV\rangle_{ij})/\sqrt{2}$. Details of the photon source are presented in Supplemental Material [15]. Using three entangled pairs, we prepare the state shown in Eq. (1) for the (3,3) threshold scheme. In Fig. 1, X, Y, and Z are denoted as the Pauli operators and H is denoted as the Hadamard operation.

The dealer (photon 2) holds the quantum secret $\alpha|H\rangle_2+\beta|V\rangle_2$ heralded by projecting photon 1 on the state $\alpha^*|H\rangle+\beta^*|V\rangle$. Photons 4 and 5 overlap on PBS_1, which leads the outgoing state to a four-photon Greenberger-Horne-Zeilinger (GHZ) state $|\mathrm{GHZ}\rangle_4=(|HHHH\rangle_{34'5'6}+|VVVV\rangle_{34'5'6})/\sqrt{2}$. By projecting photon $4'$ on the state $|+\rangle=(|H\rangle+|V\rangle)/\sqrt{2}$, $|\mathrm{GHZ}\rangle_3=(|HHH\rangle_{35'6}+|VVV\rangle_{34'5'})/\sqrt{2}$ is obtained. A rotation XHX, which is realized by a half-wave plate (HWP) set at 67.5°, is applied to photon 3 to convert the state $|\mathrm{GHZ}\rangle_3$ into $(|-HH\rangle_{34'5'}-|+VV\rangle_{34'5'})/\sqrt{2}$, where $|+\rangle=(|H\rangle+|V\rangle)/\sqrt{2}$ and $|-\rangle=(|H\rangle-|V\rangle)/\sqrt{2}$. A controlled-$ZX$ gate, which can be decomposed into three phase shift gates [i.e., two Hadamard gates and a controlled-Z (C-PHASE) gate; the decomposition of the controlled-ZX gate is shown in Sec. I D of the Supplemental Material [15]], is applied on target photon 2 and control photon 3. The phase shift gate $R(\theta)$ keeps $|H\rangle$ unchanged but adds a phase $e^{i\theta}$ on $|V\rangle$, i.e., $R(\theta)|H\rangle=|H\rangle$, $R(\theta)|V\rangle=e^{i\theta}|V\rangle$. The sequence of the three phase shift gates is shown in Fig. 1, and the value of three phase shifts in our experiment is set to $\theta_1=-\pi/2$ and $\theta_2=\theta_3=\pi/2$. $R(\pi/2)$ and $R(-\pi/2)$ are achieved by setting the quarter-wave plates (QWPs) at 0° and 90°. Two Hadamard gates (HWPs set at 22.5°) are applied on target photon 2 and $2'$ before and after the C-PHASE gate. The C-PHASE gate is implemented by overlapping photons 2 and 3 on a polarization-dependent beam splitter (PDBS) ($T_H=1$ and $T_V=1/3$) with two supplemental PDBSs ($T_V=1$ and $T_H=1/3$) at each exit port of the overlapping PDBS [19]. After the controlled-ZX gate, the state becomes

$$\frac{1}{\sqrt{2}}(|-HH\rangle_{35'6}-|+VV\rangle_{34'5'})\otimes(\alpha|H_2\rangle+\beta|V\rangle_2)$$
$$\xrightarrow{C\text{-}ZX(3\text{-}2)}\frac{1}{\sqrt{2}}|H\rangle_{3'}(|HH\rangle_{5'6}-|VV\rangle_{5'6})(\alpha|H\rangle_{2'}+\beta|V\rangle_{2'})-\frac{1}{\sqrt{2}}|V\rangle_{3'}(|HH\rangle_{5'6}+|VV\rangle_{5'6})(\beta|H\rangle_{2'}-\alpha|V\rangle_{2'}). \quad (3)$$

From Eq. (3), we can obtain $|\phi_{00}\rangle$ and $|\phi_{01}\rangle$ by projecting photon $3'$ onto the states $|+\rangle$ and $|-\rangle$, respectively. From Eq. (2), we find that $|\phi_{00}\rangle(|\phi_{01}\rangle)$ can be transformed into $|\phi_{11}\rangle(|\phi_{10}\rangle)$ by the operation $X_A\otimes X_B\otimes I_C$, i.e., $X_A\otimes X_B\otimes I_C|\phi_{00}\rangle(|\phi_{01}\rangle)=|\phi_{11}\rangle(|\phi_{10}\rangle)$. Thus, by randomly setting the degree of polarizer on photon $3'$ at $45°(|+\rangle)$ and $-45°(|-\rangle)$ and randomly inserting two HWPs set at $45°(X)$ on path $2'$ and $5'$, we obtain the mixed state ρ_{QSS} upon sixfold coincidence postselection. Three photons, $2'$, $5'$, and 6, are distributed to Alice, Bob, and Charlie, respectively. Note that this method used to generate ρ_{QSS} is rather universal; thus, it can not only be used in linear optics systems, but also in other quantum systems as well. The detailed quantum circuit is provided in Sec. I D of the Supplemental Material [15].

After preparing the quantum state for the (3,3) threshold scheme, we test the reliability and confidentiality on ρ_{QSS}. We confirm the reliability of the (3,3) threshold scheme by showing that the initial quantum information $\alpha|H\rangle+\beta|V\rangle$ issued by the dealer can be faithfully recovered by the three players. To do so, a Bell-state measurement (BSM) is first applied on Bob's and Charlie's photons. Then, conditioned on the outcome of BSM $\in\{|\Phi^+\rangle,|\Phi^-\rangle,|\Psi^+\rangle,|\Psi^-\rangle\}$, an operation $U\in\{XZ,I,Z,X\}$ is applied on Alice's photon to recover $|\psi\rangle$, where $|\Phi^\pm\rangle=(|HH\rangle\pm|VV\rangle)/\sqrt{2}$ and $|\Psi^\pm\rangle=(|HV\rangle\pm|VH\rangle)/\sqrt{2}$ are Bell states. As shown in Fig. 1, the BSM is realized by interfering photons $5'$ and 6 on a PBS and analyzed by the BSM analyzer [20] on photon $5''$ and photon $6'$. The correcting unitary U is realized by HWPs. On the basis of the result from the BSM analyzer, we choose the corresponding unitary operation on photon $2'$. In our experiment, we project photon $5'$ and 6 onto one of the four Bell states, and employ the corresponding U on photon $2'$ to obtain the initial state. The recovery results under different BSM results are presented in Sec. II B of the Supplemental Material [15]. In principle, Charlie and Bob could feed the outcome of the BSM forward to Alice, according to which Alice can apply the corresponding unitary on the photon in her hand to obtain the secret state.

In the experiment, we choose eight different input quantum states, in the form of $|\psi\rangle=\alpha|H\rangle+\beta|V\rangle$, and measure the fidelity between the input and decoded states for each case. The best fidelity achieved is 0.93 ± 0.02 and the average fidelity is 0.82 ± 0.01. More details on data processing are shown in Sec. II B of the Supplemental Material [15]. The results are presented in Fig. 2. Each of the eight fidelities is beyond the classical limit $2/3$ for more than three standard deviations.

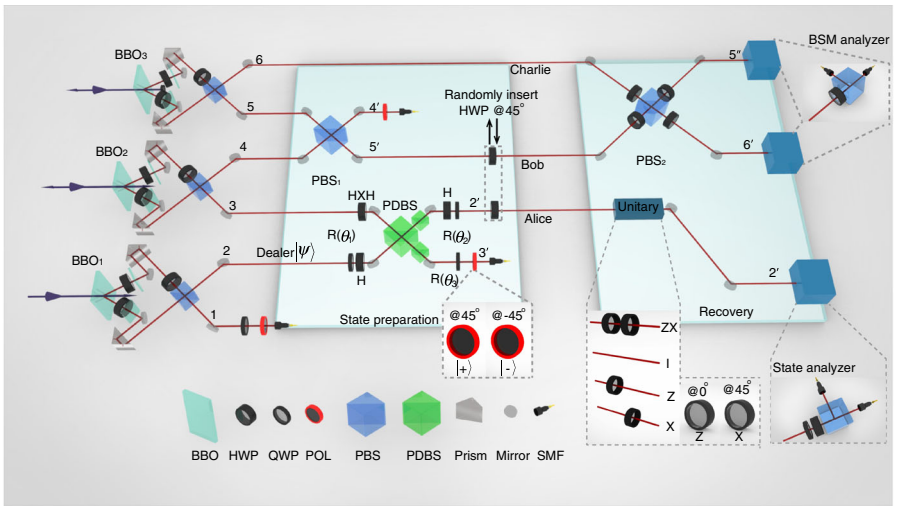

FIG. 1. Illustration of the experimental setup. An ultraviolet (UV) pulse passes through BBO_1, BBO_2, and BBO_3 successively. After pumping on BBO_1 (BBO_2), the UV pulse is refocused by lenses and directed to BBO_2 (BBO_3) by mirrors (not shown here). The interference on PBS_1, PDBS, and PBS_2 is obtained by finely adjusting the path length of the two input photons. To achieve good visibility of interference, we filter the photons temporally by narrow band filters and spatially by single-mode fibers (SMFs). Only sixfold coincidence events, among paths 1, 2', 3', 4', 5", and 6', are postselected, with rates of 75 counts per hour in the confidentiality test and 14 counts per hour in the reliability test. Polarizers (POL) are used for projection-valued measures.

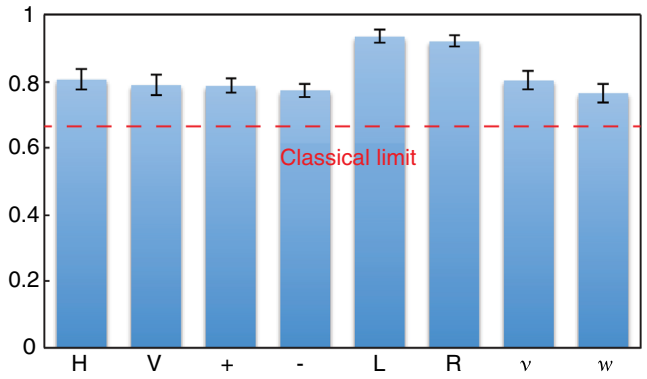

FIG. 2. Quantum secret recovery by three players. The column represents the corresponding fidelity of the recovered state when the initial state is prepared into $|H(V)\rangle$, $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$, $|L(R)\rangle = (|H\rangle \pm i|V\rangle)/\sqrt{2}$ and $|v(w)\rangle = (|H\rangle \pm \sqrt{3}|V\rangle)/2$. The error bars are calculated by assuming that our experimental data follow a normal distribution. The red dashed line represents the classical limit of 2/3.

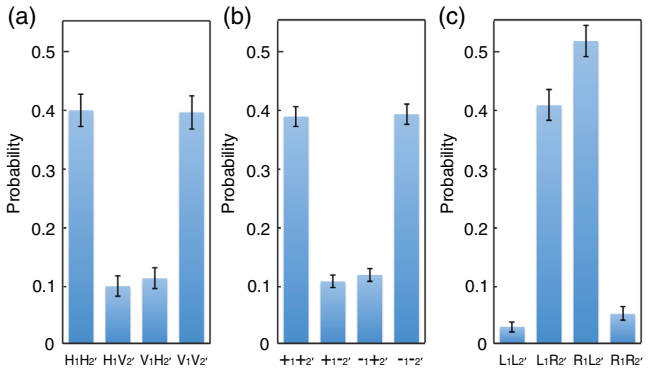

FIG. 3. Entanglement witness results as local measurements in the Z, X, and Y bases. (a) Coincidence detections in the Z basis, projecting to H and V, $P(H_1, H_{2'}) = 0.40(3)$, $P(H_1, V_{2'}) = 0.10(2)$, $P(V_1, H_{2'}) = 0.11(2)$ and $P(V_1, V_{2'}) = 0.40(3)$. In Eq. (4), $\langle Z_1 Z_{2'}\rangle = P(H_1, H_{2'}) - P(H_1, V_{2'}) - P(V_1, H_{2'}) + P(V_1, V_{2'}) = 0.59$. (b) X basis, projecting to $+$ and $-$, $P(+,+_{2'})=0.40(2)$, $P(+_1,-_{2'})=0.11(1)$, $P(-_1,+_{2'})=0.12(1)$, and $P(-_1,-_{2'}) = 0.39(2)$. (c) Y basis, projecting to L and R, $P(L_1,L_{2'})=0.03(1)$, $P(L_1,R_{2'})=0.41(3)$, $P(R_1,L_{2'})=0.52(3)$, and $P(R_1,R_{2'}) = 0.05(1)$.

Furthermore, we show that entangled quantum states can also be shared and recovered by our setup. As shown in Fig. 1, photons 1 and 2 are in a maximally entangled state $|\Phi_{12}^+\rangle = (|HH\rangle_{12} + |VV\rangle_{12})/\sqrt{2}$. Photon 2 is divided into three shares that are distributed to Alice, Bob, and Charlie and is recovered by collaboration of all three shares. We then analyze the entanglement between photon 1 and the recovered photon $2'$, i.e., $\rho_{12'}$, by an entanglement witness $\mathcal{W} = \frac{1}{2}I - |\Phi_{12'}^+\rangle\langle\Phi_{12'}^+|$. The expectation value of $\mathcal{W}$ can be decomposed into a linear combination of the expectation values of local observables,

$$\langle\mathcal{W}\rangle = \mathrm{Tr}(\mathcal{W}\rho_{12'}) = \frac{1}{4}(1 - \langle Z_1 Z_{2'}\rangle - \langle X_1 X_{2'}\rangle + \langle Y_1 Y_{2'}\rangle). \tag{4}$$

The measurement results are shown in Fig. 3. From the measured coincidence count probabilities, we calculate that $\langle\mathcal{W}\rangle = -0.24 \pm 0.02$, from which we further obtain the fidelity of the recovered $\rho_{12'}$ of $F_{\mathrm{exp}} = \mathrm{Tr}(|\Phi^+\rangle\langle\Phi^+|\rho_{12'}) = \frac{1}{2} - \mathrm{Tr}(\mathcal{W}\rho_{12'}) = 0.74 \pm 0.02$ [21]. More details on data processing are shown in Sec. II C of the Supplemental Material [15]. Clearly, the recovered quantum state is still entangled with the other half of the EPR pair because $\langle\mathcal{W}\rangle < 0$. Thus, we have shown that our QSS setup is capable of sharing entangled states.

From the viewpoint of error correction, the quantum state ρ_{QSS} we prepared can be treated as the five-qubit code after going through two erasure errors. The decoding circuit shown in Fig. 1 is the same as that for the five-qubit quantum erasure error-correcting code. Thus, we have successfully demonstrated that the five-qubit code is capable of correcting two erasure errors with a fidelity as high as 93%. Correcting two erasure errors has been proven to be equivalent to correcting an arbitrary error [16,22] (details are provided in Sec. I E of the Supplemental Material [15]). Thus, for the first time, we have experimentally verified that a general error can be corrected in a linear optics quantum computing system.

The confidentiality of the scheme is shown by the fact that the quantum state of any one or two of the three players is independent of the secret quantum information $|\psi\rangle$. In an ideal implementation, from Eq. (1), we can easily find that the density matrix of each player's qubit is $I/2$ and that the density matrix of any two players' joint state is $I \otimes I/4$. Thus, no information can be obtained unless three players' shares are combined. In the experiments, we verify single-player and two-player cases separately.

In the single-player case, the encoding process can be represented by a quantum channel [23], i.e., $\rho_k = \mathcal{E}_k(\rho_D)$, where ρ_k denotes the reduced density matrix of player k and $\rho_D = |\psi\rangle\langle\psi|$ is the initial secret quantum state. The ideal-implementation channel $\mathcal{E}_{\mathrm{ideal}}$ from the dealer to a single player is a depolarizing channel $\rho_D \to I/2$. Experimentally, we remove the PBS_2 and BSM analyzer, and reconstruct $\mathcal{E}_k$ using the quantum process tomography technology [23]. For example, when we reconstruct $\mathcal{E}_A$, we perform tomographic measurements on Alice while treating Bob and Charlie's qubits as trigger photons without measuring their polarization information. The geometry interpretation of $\mathcal{E}_k$ is shown in Fig. 4. We calculate the process fidelity between ideal $\mathcal{E}_{\mathrm{ideal}}$ and reconstructed $\mathcal{E}_k$, namely, $F_k = \mathrm{Tr}(\sqrt{\sqrt{\mathcal{E}_{\mathrm{ideal}}}\mathcal{E}_k\sqrt{\mathcal{E}_{\mathrm{ideal}}}})^2$ and discover that $F_{\mathrm{Alice}} = 0.90 \pm 0.03$, $F_{\mathrm{Bob}} = 0.97 \pm 0.01$, and $F_{\mathrm{Charlie}} = 0.89 \pm 0.03$. More details on data processing are shown in Sec. II D of the Supplemental Material [15]. We test the confidentiality of two players by measuring the minimum error probability to distinguish two orthogonal secret states

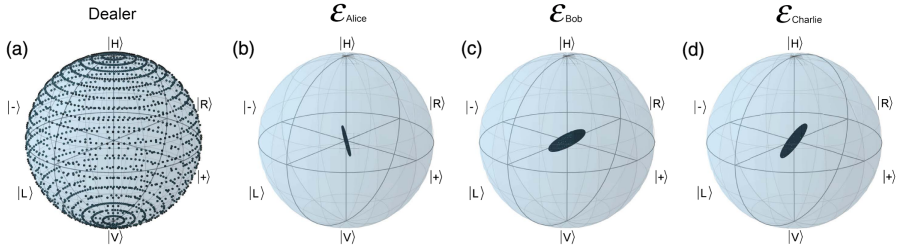

FIG. 4. The geometric interpretation of the channel $\mathcal{E}_i$ on a Bloch sphere. Qubit states can be represented in a Bloch sphere. A pure state is on the sphere and a mixed state is in the ball. The ideal $\mathcal{E}_{\text{ideal}}$ of the quantum (3,3) threshold scheme maps each point on the surface (pure state) to the origin (the maximally mixed state $I/2$). (a) Geometric interpretation of the initial pure states possibly prepared by the dealer. [(b)–(d)] Geometric interpretations of the channel $\mathcal{E}_{\text{Alice}}$, $\mathcal{E}_{\text{Bob}}$, and $\mathcal{E}_{\text{Charlie}}$, respectively. We observe that $F_{\text{Alice}} = 0.90 \pm 0.03$, $F_{\text{Bob}} = 0.97 \pm 0.02$, and $F_{\text{Charlie}} = 0.89 \pm 0.03$, where the error bars are calculated by performing 500 runs of channel operator matrix reconstructions and assuming white noise.

[24]. The two-player results are presented in Sec. II E of the Supplemental Material [15].

By designing a linear optical quantum circuit, we experimentally demonstrate the quantum (3,3) threshold scheme, satisfying the three criteria for the fully quantum secret sharing: reliability, confidentiality, and capability of sharing entangled states. Our setup provides a practical QSS architecture. With the assistance of entanglement purification and nested entanglement swapping, a long-distance QSS scheme can be achieved to protect the secrets. Such a scheme can serve as one of the founding blocks in many quantum information tasks, such as all-photonic quantum repeater [25,26], distributed quantum information processing [27], and lossy quantum memory [28].

We acknowledge H.-K. Lo, B. C. Sanders, and X. Yuan for insightful discussions. This work has been supported by the National Natural Science Foundation of China and the CAS.

H. L. and Z. Z. contributed equally to this work.

*eidos@ustc.edu.cn

[1] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[2] A. Shamir, Commun. ACM **22**, 612 (1979).
[3] G. R. Blakley, Safeguarding cryptographic keys, in *Proc. of the National Computer Conference, 1979*, Vol. 48 (1979), p. 313.
[4] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[5] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[6] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[7] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **95**, 200502 (2005).
[8] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
[9] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007).
[10] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[11] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, T. Tyc, T. C. Ralph, and P. K. Lam, Phys. Rev. A **71**, 033814 (2005).
[12] B. A. Bell, D. Markham, D. A. Herrera-Mart, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, Nat. Commun. **5**, 5480 (2014).
[13] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[14] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).
[15] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.117.030501 for the further details of the QSS scheme and its experiment implementation.
[16] M. Grassl, T. Beth, and T. Pellizzari, Phys. Rev. A **56**, 33 (1997).
[17] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[18] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, Nat. Photonics **6**, 225 (2012).
[19] N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter, Phys. Rev. Lett. **95**, 210505 (2005).
[20] J.-W. Pan and A. Zeilinger, Phys. Rev. A **57**, 2208 (1998).
[21] O. Gühne, C.-Y. Lu, W.-B. Gao, and J.-W. Pan, Phys. Rev. A **76**, 030305 (2007).
[22] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[23] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[24] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, New York, 2013).
[25] K. Azuma, K. Tamaki, and H.-K. Lo, Nat. Commun. **6**, 10171 (2015).
[26] R. Namiki, O. Gittsovich, S. Guha, and N. Lütkenhaus, Phys. Rev. A **90**, 062316 (2014).
[27] Y. L. Lim, A. Beige, and L. C. Kwek, Phys. Rev. Lett. **95**, 030505 (2005).
[28] W. Tittel, M. Afzelius, T. Chaneli, R. Cone, S. Krll, S. Moiseev, and M. Sellars, Laser Photonics Rev. **4**, 244 (2010).