Quantum State Sharing by Using Two-Mode and Single-Mode Squeezed State Lights *

ZHANG Jun-Xiang(张俊香)**, JING Jie-Tai(荆杰泰), XIE Chang-De(谢常德), PENG Kun-Chi(彭堃墀)

The State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-electronics, Shanxi University, Taiyuan 030006

(Received 9 June 2005)

We propose a quantum state sharing scheme for continuous variables using bright two-mode squeezed state and single-mode squeezed state light. The squeezing of a single-mode state is applied to enhance the security of information in quantum teleportation network. The signal-to-noise ratio of communication and the fidelity between the secret and reconstruction state are analysed. It is shown that both the receivers of Bob and Charlie cannot extract information with a high signal-to-noise ratio because of the large noise come from the other quadrature component of single mode squeezed state. Anyone of Bob and Charlie can retrieve the quantum state with a high signal-to-noise ratio if and only if the other one cooperates with the measurement.

In recent years, the quantum entanglement state has been proven to be an important resource for quantum information science.[1,2] One of the key applications of quantum entanglement is quantum state sharing,[3] in which the quantum information encoded in a quantum state at one sender (Alice) can be distributed to several remote receivers (Bobs) by using the multi-particle entangled state and then one of them is able to recover the information exactly if and only if all the other receivers agree to cooperate. The scheme further ensures secure transfer of an unknown quantum state by quantum teleportation,[4] in which an unknown quantum state can be transmitted from a sender to a remote receiver by using an entangled state. Quantum teleportation was originally proposed for discrete variables[4] using the Bell state and extended to continuous-variable systems[5,6] using the two-mode squeezed vacuum state. Experimental demonstrations have been realized for both discrete and continuous variables.[7−9]

The idea of quantum state sharing based on the method of teleportation was first described[3] for discrete variables using the maximally three-particle entangled state or GHZ state.[10] Later several related works based on the pure entangled state and entanglement swapping were proposed.[11−14] The first quantum state sharing experiment[15] for discrete variables has been accomplished by using the energy-time entangled pseudo-GHZ states.[16] Recently, Tyc and Sanders extended quantum state sharing in the continuous variables regime with Einstein–Podolsky–Rosen (EPR) entanglement.[17,18] Very recently, the continuous variables quantum state sharing in which a secret coherent state is encoded into a tripartite entangled state was investigated experimentally with fidelity as

high as 0.73.[19] It is known that the multipartite entanglement is needed in the traditional quantum state sharing protocol, however the experimental production of more than two entangled photons directly from the nonlinear process must suffer from low efficiency. In this Letter, we propose a system of quantum state sharing for continuous variables between one sender and two receivers, in which a bright two-mode squeezed state and a bright single-mode squeezed state light generated from nondegenerate optical parametric amplifier (NOPA) and degenerate OPA operating at deamplification[20] are used to constitute the multipartite entangled source. Hence the direct detection for Bell state[21,22] is utilized to make the proposed scheme valuable for performing experiments.

In the proposed quantum state sharing scheme (Fig. 1). A two-mode squeezed state and a single-mode squeezed state of the electromagnetic field are utilized to constitute a multipartite entangled state. In the Heisenberg representation the quadratures of a two-mode squeezed state (mode $\hat{a}_1$ and mode a_2) and a single-mode squeezed state (mode b) are expressed as follows:[23,24]

$$
\begin{aligned}
\hat{X}_1 &= (e^r \hat{X}_1^{(0)} + e^{-r} \hat{X}_2^{(0)})/\sqrt{2}, \\
\hat{Y}_1 &= (e^{-r} \hat{Y}_1^{(0)} + e^r \hat{Y}_2^{(0)})/\sqrt{2}, \\
\hat{X}_2 &= (-e^r \hat{X}_1^{(0)} + e^{-r} \hat{X}_2^{(0)})/\sqrt{2}, \\
\hat{Y}_2 &= (-e^{-r} \hat{Y}_1^{(0)} + e^r \hat{Y}_2^{(0)})/\sqrt{2}, \\
\hat{X}_b &= e^s \hat{X}_b^{(0)}, \quad \hat{Y}_b = e^{-s} \hat{Y}_b^{(0)}, \tag{1}
\end{aligned}
$$

where the superscript (0) denotes the initial modes; r and s are the squeezing parameters of two-mode and single-mode squeezed states; $\hat{X}$ and $\hat{Y}$ represent the operators of quadrature phase amplitudes of the

field modes. For the finite squeezing, when the uncertainty product for the variances of the two inferences $\langle \Delta^2 \hat{X}_{\text{inf}} \rangle \langle \Delta^2 \hat{Y}_{\text{inf}} \rangle = \langle \Delta^2 (\hat{X}_1 + g_x \hat{X}_2) \rangle \langle \Delta^2 (\hat{Y}_1 - g_y \hat{Y}_2) \rangle$ is less than the limit of unity associated with the Heisenberg uncertainty relation, the EPR paradox for continuous variables is demonstrated;[25] here $g_{x(y)}$ is the scaling factor for minimizing the variances. For infinite squeezing $r \to \text{infty}$, the zero fluctuations of the $\hat{X}_1 + \hat{X}_2$ and $\hat{Y}_1 - \hat{Y}_2$ show the fact that the two modes $(\hat{X}_1, \hat{Y}_1)$ and $(\hat{X}_2, \hat{Y}_2)$ consisting of the two-mode squeezed state approaches an ideal EPR entangled state with anticorrelation between phase quadrature components $\hat{X}$ and correlation between phase quadrature components $\hat{Y}$. In addition, $r = 0$ means no quantum entanglement, i.e. the classical limit.
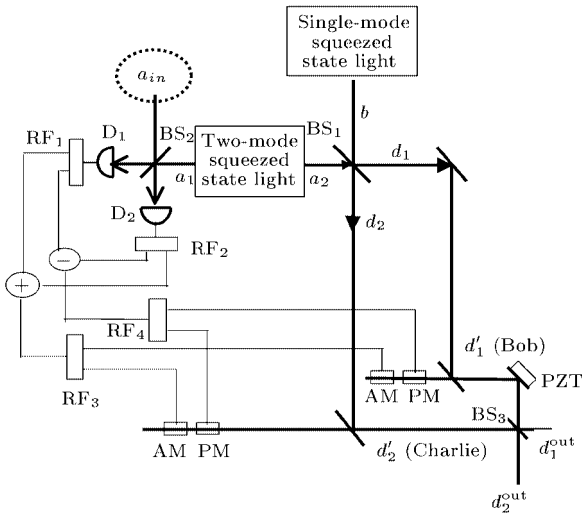

Fig. 1. Schematic of quantum secret sharing. BS: beamsplitter, $D_{1,2}$: photo detectors, RF: radio-frequency power splitters, AM: amplitude modulator, PM: phase modulator.

Firstly mixing one mode a_2 of the two-mode squeezed state with the mode b of single-mode squeezed state on the beamsplitter BS_1, the annihilation operators of the outcomes are given by

$$\hat{d}_1 = (\hat{a}_2 - \hat{b})/\sqrt{2},$$
$$\hat{d}_2 = (\hat{a}_2 + \hat{b})/\sqrt{2}. \tag{2}$$

As for the protocol of quantum state sharing, several parties, i.e. Alice (at the sending station), Bob and Charlie (at the receiving stations) in three systems, have been arranged to share an entangled state. In our scheme, mode a_1 is sent to Alice, mode d_1 and d_2 are sent to Bob and Charlie. We suppose that the quantum information teleported to and distributed secretly into remote stations named Bob and Charlie is encoded in an input quantum state at Alice. Then Alice performs a joint measurement on the input unknown quantum state and the mode a_1, and she communicates her measurement results to Bob and Charlie via classical channels. With the obtained classical

results, Bob and Charlie perform appropriate rotations on the modes d_1 and d_2 to make the quantum information be shared by the two stations Bob and Charlie secretly. When the two receivers agree to co-operation, both of them send their own rotated mode to a 50% beamsplitter (BS_3). In the following we demonstrate that one of the outcomes from BS_3 will recover the input quantum state at a certain phase difference between the two rotated modes.

At the sending station Alice, the input state a_{in} is superimposed with the mode a_1 at a 50% beamsplitter (BS_2) for implementation of the joint detection of Bell-state. To accomplish the Bell-state detection via direct measurement of photo currents, a phase shift of $\pi/2$ is imposed between a_1 and a_{in} before they are injected into BS_2. The annihilation operators of two outputs from BS_2 equal to

$$\hat{c}_1 = (\hat{a}_{in} - i\hat{a}_1)/\sqrt{2},$$
$$\hat{c}_2 = (\hat{a}_{in} + i\hat{a}_1)/\sqrt{2}. \tag{3}$$

The two beams are directly detected by detectors D_1 and D_2, then the photocurrent of each detector is divided into two parts of identical intensity by rf power splitters $(RF_1$ and $RF_2)$, and the sum and difference of the divided ac photocurrents are expressed by[21]

$$i_+ = (X_{in} + X_1)/\sqrt{2},$$
$$i_- = (Y_{in} - Y_1)/\sqrt{2}. \tag{4}$$

In order to realize quantum secret sharing, both outcomes from beamsplitter BS_2 have to be transmitted to receivers Bob and Charlie simultaneously, thus the photocurrents from the power combiners $(+)$ and $(-)$ are split into two equal parts with rf power splitters $(RF_3$ and $RF_4)$, then are sent to Bob and Charlie to transform the beam d_1 and d_2 by means of the amplitude and phase modulators (AM and PM):

$$\hat{d}_1' = \hat{d}_1 + g_1(i_+ + ii_-),$$
$$\hat{d}_2' = \hat{d}_2 + g_2(i_+ + ii_-). \tag{5}$$

In Eq. (5) the parameter g_i $(i = 1, 2)$ describes a normalized gain for the transformation from classical values to complex amplitude. Substituting Eq. (2) and (4) into Eq. (5), we obtain

$$\hat{d}_1' = [(\hat{X}_2 + g_1 \hat{X}_1) + i(\hat{Y}_2 - g_1 \hat{Y}_1) + g_1(\hat{X}_{in} + i\hat{Y}_{in}) - (\hat{X}_b + i\hat{Y}_b)]/\sqrt{2},$$
$$\hat{d}_2' = [(\hat{X}_2 + g_2 \hat{X}_1) + i(\hat{Y}_2 - g_2 \hat{Y}_1) + g_2(X_{in} + i\hat{Y}_{in}) + (\hat{X}_b + i\hat{Y}_b)]/\sqrt{2}. \tag{6}$$

We take the classical unit gain, and the two-mode squeezed state is assumed to be perfectly squeezed, i.e. $\langle \delta^2 (\hat{X}_1 + \hat{X}_2) \rangle \to 0$, $\langle \delta^2 (\hat{Y}_2 - Y_1) \rangle \to 0$, then the above equations are simplified to

$$\hat{d}_1' = (\hat{X}_{in} + i\hat{Y}_{in} - (e^s \hat{X}_b^{(0)} + ie^{-s} \hat{Y}_b^{(0)}))/\sqrt{2},$$

$$\hat{d}_2' = (\hat{X}_{in} + i\hat{Y}_{in} + (e^s \hat{X}_b^{(0)} + ie^{-s}\hat{Y}_b^{(0)}))/\sqrt{2}. \tag{7}$$

It is obvious that the two receivers individually cannot recover the quantum information of the input state. Although they have received the quadrature phase amplitude information $\hat{X}_{in}$ and $\hat{Y}_{in}$ of a_{in} mode, due to the existence of huge noise in the noisy component of single-mode squeezed state $(e^s \hat{X}_b^{(0)})$, the quantum information $\hat{X}_{in}$ of a_{in} is submerged in noise background. Considering the finite squeezing of EPR beams and unit gain for classical channel, Bob or Charlie can extract some information of input state $\hat{a}_{in}$ with the signal-to-noise ratios (SNR):

$$SNR_{d_1', X} = \frac{\langle \delta^2 \hat{X}_{in} \rangle}{2e^{-2r}\delta^2 \hat{X}_2^{(0)} + e^{2s}\delta^2 \widehat{X}_b^{(0)}},$$

$$SNR_{d_2', Y} = \frac{\langle \delta^2 \hat{Y}_{in} \rangle}{2e^{-2r}\delta^2 \widehat{Y}_1^{(0)} + e^{-2s}\delta^2 \widehat{Y}_b^{(0)}},$$

$$SNR_{d_2', X} = \frac{\langle \delta^2 \hat{X}_{in} \rangle}{2e^{-2r}\delta^2 \hat{X}_2^{(0)} + e^{2s}\delta^2 \widehat{X}_b^{(0)}},$$

$$SNR_{d_2', Y} = \frac{\langle \delta^2 \hat{Y}_{in} \rangle}{2e^{-2r}\delta^2 \widehat{Y}_1^{(0)} + e^{-2s}\delta^2 \widehat{Y}_b^{(0)}}. \tag{8}$$

In a single-mode squeezed state, the noise of one quadrature component, i.e. $e^{2s}\delta^2 \widehat{X}_b^{(0)}$, is higher than the other one $e^{-2s}\delta^2 \widehat{Y}_b^{(0)}$. Thus the $SNR_{d_1'(d_2'), X}$ of measurement quadrature component X at the receiving station of Bob or Charlie is poor; this leads to the fact that Bob or Charlie cannot obtain the exact information of input state though $SNR_{d_1'(d_2'), Y}$ for the other quadrature component Y is high. Therefore, the application of single-mode squeezed state (mode b) avoids the possibility to reconstruct completely the teleported quantum state a_{in} at either Bob or Charlie. It is noted that the quantum secret sharing protocol does not permit anyone of the two receivers Bob and Charlie to reconstruct the quantum state without communicating between themselves, and meanwhile it allows the honest one of them to recover it with the assistance of the other receivers.[3] Now we discuss how to meet this requirement. Assuming that the Bob is honest and Charlie agrees to cooperate, Charlie sends her possessive field to Bob, then Bob can combine the two modes at a 50% beamsplitter BS_3; the two modes emerging from the beamsplitter BS_3 are given by

$$\hat{d}_1^{out} = (\hat{d}_1' - \hat{d}_2' e^{i\theta})/\sqrt{2},$$
$$\hat{d}_2^{out} = (\hat{d}_1' + \hat{d}_2' e^{i\theta})/\sqrt{2}, \tag{9}$$

where θ is the relative optical phase between two input fields on BS_3. Taking $\theta = 0$ and combining Eqs. (1), (6) and (9) we obtain

$$\hat{d}_1^{out} = \frac{(g_1 - g_2)[(\hat{X}_1 - i\hat{Y}_1) + (\hat{X}_{in} + i\hat{Y}_{in})]}{2}$$
$$- (\hat{X}_b + i\hat{Y}_b),$$

$$d_2^{out} = \frac{\left(-1 + \dfrac{g_1 + g_2}{2}\right)e^r \hat{X}_1^{(0)} + \left(1 + \dfrac{g_1 + g_2}{2}\right)e^{-r}\hat{X}_2^{(0)}}{\sqrt{2}}$$
$$+ i\frac{\left(1 - \dfrac{g_1 + g_2}{2}\right)e^r \hat{Y}_2^{(0)} - \left(1 + \dfrac{g_1 + g_2}{2}\right)e^{-r}\hat{Y}_1^{(0)}}{\sqrt{2}}$$
$$+ \frac{g_1 + g_2}{2}(\hat{X}_{in} + i\hat{Y}_{in}). \tag{10}$$

From Eq. (10) it can be seen easily that in the case of the ideal situation of $g_1 + g_2 = 2$ and $r \to \infty$, the one output d_2^{out} of BS_3 retrieves the input state a_{in}:

$$\hat{d}_1^{out} = -\hat{b}, \quad \hat{d}_2^{out} = \hat{a}_{in}. \tag{11}$$

With a totally analogous calculation for $\theta = \pi$ we obtain

$$\hat{d}_1^{out} = \hat{a}_{in}, \quad \hat{d}_2^{out} = -\hat{b}. \tag{12}$$

i.e., the input state is retrieved at other output of BS_3.

Ideal quantum state sharing [Eqs. (11) and (12)] should mean that the output state emerging at one of the receiving stations is the same as the input state. However, in a real experiment for continuous variables the ideal quantum secret sharing may not be accomplished since a non-ideal EPR pair is used by the two-mode squeezed states. Thus it is necessary to discuss the criteria for evaluating the efficiency of a realistic- and thus imperfect-quantum state sharing system. For our teleportation system, the fidelity quantifying the quality of teleportation is defined for a coherent input state $(|\alpha\rangle)$ by $F = \langle \alpha | \hat{\rho}_{out} | \alpha \rangle$[26,27], and it describes the matching between the input and teleported states. According to the discussion in teleportation, the quantum secret sharing fidelity for a coherent state input α_{in} reads

$$F = \frac{2}{\sqrt{(\langle \delta^2 \hat{X}_{out} \rangle + 1)(\langle \delta^2 \hat{Y}_{out} \rangle + 1)}}$$
$$\cdot \exp\left[-2\frac{(1 - g)^2 |\alpha_{in}|^2}{\sqrt{(\langle \delta^2 \hat{X}_{out} \rangle + 1)(\langle \delta^2 \hat{Y}_{out} \rangle + 1)}} \right], \tag{13}$$

where $\delta^2 \hat{X}_{out}$ and $\delta^2 \hat{Y}_{out}$ are the variance of in-phase quadrature and out-of-phase quadrature phases of the output mode, and g describes a normalized gain for the transformation from classical values to complex field amplitude performed by Bob, it takes the value $\dfrac{g_1 + g_2}{2}$ in our calculation. Using Eq. (10), this is given by

$$\langle \delta^2 \hat{X}_{out} \rangle = \frac{(g_1 + g_2)^2}{4}\langle \delta^2 \hat{X}_{in} \rangle + \frac{\left(1 + \dfrac{g_1 + g_2}{2}\right)^2}{2}e^{-2r}$$
$$+ \frac{\left(1 - \dfrac{g_1 + g_2}{2}\right)^2}{2}e^{2r},$$

$$\langle \delta^2 \hat{Y}_{out} \rangle = \frac{(g_1 + g_2)^2}{4}\langle \delta^2 \hat{Y}_{in} \rangle + \frac{\left(1 + \dfrac{g_1 + g_2}{2}\right)^2}{2}e^{-2r}$$

$$+ \frac{\left(1 - \dfrac{g_1 + g_2}{2}\right)^2}{2} e^{2r}, \tag{14}$$

where $\langle \delta^2 \hat{X}_{in} \rangle$ and $\langle \delta^2 \hat{Y}_{in} \rangle$ are the variances of the input coherent state, and then we have $\langle \delta^2 \hat{X}_{in} \rangle = \langle \delta^2 \hat{Y}_{in} \rangle = 1$.

According to Eqs. (13) and (14), the best optimal fidelity for quantum secret sharing occurs around $g_1 = g_2 = 1$. In this case the fidelity becomes

$$F = \frac{1}{1 + e^{-2r}}. \tag{15}$$

In the classical system without quantum correlation $r = 0$, we obtain $F = 1/2$ for the normalized gain $g_{1(2)} = 1$. In order to meet the requirement of the quantum region $F > 1/2$, it requires that $r > 0$. On the other hand, for a strict no-cloning measurement, the fidelity which warrants that no other copy of the input state can remain is described[28] as $F = \dfrac{1}{2 + e^{-2r}}$, thus the $F > 2/3$ criteria can be taken for non-cloning quantum state sharing.

In conclusion, we have proposed an quantum secret sharing scheme for continuous variables, in which a bright two-mode squeezed state and a single-mode squeezed state of electromagnetic field are used to constitute the three partite entanglement. The two-mode squeezing provides the squeezed state entanglement distributed between a sender (Alice) and two receivers (Bob and Charlie) and the single-mode squeezing offers the performance of secret sharing of the system. If without the single-mode squeezed state, half of the EPR beam a_2 from two-mode squeezed state is combined with a vacuum field at the beamsplitter BS_1 and then the quantum entanglement between mode a_1 and mode a_2 is distributed in modes a_1, d_1 and d_2 with lower correlation.[29,30] Thus once $r \neq 0$, the fidelity between the output state $(\hat{X}_{out}, \hat{Y}_{out})$ from either output ports of BS_3 and the input state $(\hat{X}_{in}, \hat{Y}_{in})$ will surpass the classical limitation $(F > 1/2)$. Only when the single-mode squeezed state is applied, the noisy component $(e^s \hat{X}_b^{(0)})$ protects from that the information of the same quadrature in the input state [$\hat{X}_{in}$ in Eqs. (7) and (8)] is extracted independently by Bob or Charlie without cooperation. The appointed relative phase difference between two input fields on BS_3 (θ) confirms that the input state is retrieved at an honest receiver (for example, $\theta = 0$ at Charlie, $\hat{d}_2^{out} = \hat{a}_{in}$; $\theta = \pi$ at Bob, $\hat{d}_1^{out} = \hat{a}_{in}$). The other features of the system are that instead of usually used two balanced homodyne detectors[21] at Alice, a direct detection scheme for Bell-state is utilized and the bright squeezed state light[31] with in-phase quadrature anti-correlation and out-of-phase quadrature correlation is chosen. The mature technique to produce the bright squeezed state light and the simplification of direct detection[21] make the proposed scheme easier to be realized experimentally.

References

[1] Bennett C H 1995 *Phys. Today* **48** 24
[2] Lloyd S and Braunstein S L 1999 *Phys. Rev. Lett.* **82** 1784
[3] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[4] Bennett C H, Brassard G, Crepeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[5] Vaidmann L 1994 *Phys. Rev. A* **49** 1473
[6] Braunstein S L and Kimble H J 1998 *Phys. Rev. Lett.* **80** 869
[7] Boumeester D, Pan J W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 *Nature* **390** 575
[8] Boschi D, Branca S, Martini F D, Hardy L and Popescu S 1998 *Phys. Rev. Lett.* **80** 1121
[9] Furusawa A, Sorensen J L, Braunstein S L, Fuchs C A, Kimble H J and Polzik E S 1998 *Science* **282** 706
[10] Bagherinezhad S and Karimipour V 2003 *Phys. Rev. A* **67** 044302
[11] Gottesman D 2000 *Phys. Rev. A* **61** 042311
[12] Bandyopadhyay S 2000 *Phys. Rev. A* **62** 012308
[13] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[14] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev. A* **59** 162
[15] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev. A* **63** 042301
[16] Brendel J, Gisin N, Tittel W and Zbinden H 1999 *Phys. Rev. Lett.* **82** 2594
[17] Tyc T and Sanders B C 2002 *Phys. Rev. A* **65** 042310
[18] Tyc T, Rowe D J and Sanders B C 2003 *J. Phys. A* **36** 7625
[19] Lance A M, Symul T, Bowen W P, Sanders B C, Tyc T, Ralph T C and Lam P K 2005 *Phys. Rev. A* **71** 033814
[20] Zhang Y, Su H, Xie C D and Peng K C 1999 *Phys. Lett. A* **259** 171
[21] Zhang J and Peng K C 2000 *Phys. Rev. A* **62** 064302
[22] Li X Y, Pan Q, Jin J T, Zhang J, Xie C D and Peng K C 2002 *Phys. Rev. Lett.* **88** 047904
[23] Loock P and Braunstein S L 1999 *Phys. Rev. A* **61** 010302
[24] Walls D F and Milburn G J 1994 *Quantum Optics* (Berlin: Springer)
[25] Reid M D 1989 *Phys. Rev. A* **40** 913
[26] Braunstein S L, Fuchs C A and Kimble H J 2000 *J. Mod. Opt.* **47** 267
[27] Polkinghorne R E S and Ralph T C 1999 *Phys. Rev. Lett.* **83** 2095
[28] Grosshans F and Philippe P 2001 *Phys. Rev. A* **64** 010301
[29] Paris M G A 1999 *Phys. Rev. A* **59** 1615
[30] Loock P and Braunstein S L 1999 *Phys. Rev. A* **61** 010302
[31] Schneider K, Bruckmeier R, Hansen H, Schiller S and Mlynek J 1996 *Opt. Lett.* **21** 1396