Eur. Phys. J. D **39**, 459–464 (2006)
DOI: 10.1140/epjd/e2006-00124-1

THE EUROPEAN
PHYSICAL JOURNAL D

Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements

F.-G. Deng[1,2,3,a], X.-H. Li[1,2], C.-Y. Li[1,2], P. Zhou[1,2], and H.-Y. Zhou[1,2,3]

[1] The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, P.R. China
[2] Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, P.R. China
[3] Beijing Radiation Center, Beijing 100875, P.R. China

Received 15 September 2005 / Received in final form 30 March 2006
Published online 13 June 2006 – © EDP Sciences, Società Italiana di Fisica, Springer-Verlag 2006

Abstract. Two schemes for sharing an arbitrary two-qubit state based on entanglement swapping are proposed with Bell-state measurements and local unitary operations. One is based on the quantum channel with four Einstein-Podolsky-Rosen (EPR) pairs shared in advance. The other is based on a circular topological structure, i.e., each user shares an EPR pair with his neighboring one. The advantage of the former is that the construction of the quantum channel between the agents is controlled by the sender Alice, which will improve the security of the scheme. The circular scheme reduces the quantum resource largely when the number of the agents is large. Both of those schemes have the property of high efficiency as almost all the instances can be used to split the quantum information. They are more convenient in application than the other schemes existing as they require only two-qubit entanglements and two-qubit joint measurements for sharing an arbitrary two-qubit state.

PACS. 03.67.Hk Quantum communication – 03.67.Dd Quantum cryptography – 03.65.Ud Entanglement and quantum nonlocality (e.g. EPR paradox, Bell's inequalities, GHZ states, etc.)

1 Introduction

The basic idea of secret sharing [1] in a simple case is that a secret (M_A) is divided by the sender Alice into two pieces which will be distributed to two parties, Bob and Charlie, respectively, and they can reconstruct the secret if and only if both act in concert. Each can get nothing about the message M_A. As classical signal can be copied freely and fully without leaving a track, there is no way for people to complete the task unconditionally securely with classical physics in principle. When quantum mechanics enters the field of information, the case is changed. Quantum secret sharing (QSS), an important branch of quantum communication, is the generalization of classical secret sharing into quantum scenario [2,3]. There are three main goals in QSS. The first one is used to distribute a private key among several parties, such as those in references [2–8]; the second is used for splitting a classical secret [2,3,9–15], and the third one can be used to share an unknown quantum state [16–18], which has to resort to quantum entanglement.

Certainly, quantum key distribution (QKD) provides a secure way for generating a private key between two remote parties and then can be used to complete the task for disturbing the key among several parties. The difference between QSS and QKD [19] is that the former can reduce the resource necessary to implement multiparty secret sharing tasks and is more convenient than that with QKD [5]. A pioneering QSS scheme was proposed by Hillery, Bužek and Berthiaume in 1999 by using three-particle and four-particle entangled Greenberger-Horne-Zeilinger (GHZ) states for sharing classical information, called HBB99 customarily for short. For sharing a quantum secret, almost all of the existing QSS protocols either are used to split a single qubit [16] or resorts to m-particle entanglements [18] and m-particle joint measurements ($m > 2$) [16,17]. The producing and measurement of m-particle entanglement both are not easy with present techniques [20–22].

From the view of security, sharing a quantum secret in QSS is similar to quantum secure direct communication (QSDC) [24–26] in which the secret message is transmitted directly without creating a private key and then encrypting the message as the quantum secret should not be

[a] e-mail: fgdeng@bnu.edu.cn

$$\begin{aligned}
|\Phi\rangle_{ab3456} \equiv\ & (\alpha|00\rangle+\beta|01\rangle+\gamma|10\rangle+\delta|11\rangle)_{ab}\otimes|\psi^-\rangle_{34}\otimes|\psi^-\rangle_{56}\\
=\ & \frac{1}{4}\{|\psi^-\rangle_{a3}[|\psi^-\rangle_{b5}(\alpha|00\rangle+\beta|01\rangle+\gamma|10\rangle+\delta|11\rangle)_{46}+|\psi^+\rangle_{b5}(\alpha|00\rangle-\beta|01\rangle+\gamma|10\rangle-\delta|11\rangle)_{46}\\
& -|\phi^-\rangle_{b5}(\alpha|01\rangle+\beta|00\rangle+\gamma|11\rangle+\delta|10\rangle)_{46}-|\phi^+\rangle_{b5}(\alpha|01\rangle-\beta|00\rangle+\gamma|11\rangle-\delta|10\rangle)_{46}]\\
& +|\psi^+\rangle_{a3}[|\psi^-\rangle_{b5}(\alpha|00\rangle+\beta|01\rangle-\gamma|10\rangle-\delta|11\rangle)_{46}+|\psi^+\rangle_{b5}(\alpha|00\rangle-\beta|01\rangle-\gamma|10\rangle+\delta|11\rangle)_{46}\\
& -|\phi^-\rangle_{b5}(\alpha|01\rangle+\beta|00\rangle-\gamma|11\rangle-\delta|10\rangle)_{46}-|\phi^+\rangle_{b5}(\alpha|01\rangle-\beta|00\rangle-\gamma|11\rangle+\delta|10\rangle)_{46}]\\
& -|\phi^-\rangle_{a3}[|\psi^-\rangle_{b5}(\alpha|10\rangle+\beta|11\rangle+\gamma|00\rangle+\delta|01\rangle)_{46}+|\psi^+\rangle_{b5}(\alpha|10\rangle-\beta|11\rangle+\gamma|00\rangle-\delta|01\rangle)_{46}\\
& -|\phi^-\rangle_{b5}(\alpha|11\rangle+\beta|10\rangle+\gamma|01\rangle+\delta|00\rangle)_{46}-|\phi^+\rangle_{b5}(\alpha|11\rangle-\beta|10\rangle+\gamma|01\rangle-\delta|00\rangle)_{46}]\\
& -|\phi^-\rangle_{a3}[|\psi^-\rangle_{b5}(\alpha|10\rangle+\beta|11\rangle-\gamma|00\rangle-\delta|01\rangle)_{46}+|\psi^+\rangle_{b5}(\alpha|10\rangle-\beta|11\rangle-\gamma|00\rangle+\delta|01\rangle)_{46}\\
& -|\phi^-\rangle_{b5}(\alpha|11\rangle+\beta|10\rangle-\gamma|01\rangle-\delta|00\rangle)_{46}-|\phi^+\rangle_{b5}(\alpha|11\rangle-\beta|10\rangle-\gamma|01\rangle+\delta|00\rangle)_{46}]\}
\end{aligned} \qquad (5)$$

leaked to the dishonest one. It is necessary for QSS to set up a quantum channel securely in advance [2,3,11–14,16], which is same as QSDC in references [24–26]. The way for sharing a sequence of two-particle maximally entangled states, Einstein-Podolsky-Rosen (EPR) pairs is discussed in references [24,27].

In this paper, we will present a quantum state sharing (which is abbreviated as *QSTS* in reference [17], different from QSS for classical information) scheme for sharing an arbitrary two-qubit state $|\chi\rangle_{ab}=\alpha|00\rangle_{ab}+\beta|01\rangle_{ab}+\gamma|10\rangle_{ab}+\delta|11\rangle_{ab}$ based on entanglement swapping [28–30] with Bell-state measurements and local unitary operations. It will be shown that the state $|\chi\rangle_{ab}$ can be split by two agents with four EPR pairs shared in advance and four Bell-state measurements, not m-particle joint measurements ($m>2$). Any one in the two agents has the choice to reconstruct the original state $|\chi\rangle_{ab}$ with the help of the other. Moreover, we present a circular topological structure for splitting the state $|\chi\rangle_{ab}$ with EPR pairs and Bell-state measurements efficiently as it reduces the quantum resource largely when the number of the agents is large. Almost all the EPR pairs can be used for quantum communication in those two schemes, their efficiency for qubits approaches the maximal value, same as references [16–18]. They are more convenient in application than the other schemes existing as they require only two-qubit entanglements and two-qubit joint measurements, not GHZ states, for sharing an arbitrary two-qubit state.

2 QSTS protocol with EPR pairs and Bell-basis measurements

An EPR pair is in one of the four Bell states shown as follows:

$$|\psi^{\pm}\rangle_{AB}=\frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B\pm|1\rangle_A|0\rangle_B), \qquad (1)$$

$$|\phi^{\pm}\rangle_{AB}=\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B\pm|1\rangle_A|1\rangle_B). \qquad (2)$$

where $|0\rangle$ and $|1\rangle$ are the two eigenvectors of two-level quantum system, such as the polarizations of photon along the z-direction, say σ_z. The four local unitary operations U_i ($i=0,1,2,3$) can transform each one of the four Bell states into another

$$\begin{aligned}
U_0&=|0\rangle\langle 0|+|1\rangle\langle 1|, & U_1&=|0\rangle\langle 0|-|1\rangle\langle 1|,\\
U_2&=|1\rangle\langle 0|+|0\rangle\langle 1|, & U_3&=|0\rangle\langle 1|-|1\rangle\langle 0|.
\end{aligned} \qquad (3)$$

For example,

$$\begin{aligned}
I\otimes U_0|\psi^-\rangle&=|\psi^-\rangle, & I\otimes U_1|\psi^-\rangle&=-|\psi^+\rangle,\\
I\otimes U_2|\psi^-\rangle&=|\phi^-\rangle, & I\otimes U_3|\psi^-\rangle&=|\phi^+\rangle,
\end{aligned} \qquad (4)$$

where $I=U_0$ is the 2×2 identity operator which means doing nothing on the particle.

The basic idea of this QSTS scheme for splitting an entangled state $|\chi\rangle_{ab}=\alpha|00\rangle_{ab}+\beta|01\rangle_{ab}+\gamma|10\rangle_{ab}+\delta|11\rangle_{ab}$ based on entanglement swapping is shown in Figure 1. Alice shares two EPR photon pairs $|\psi^-\rangle_{12}$ and $|\psi^-\rangle_{34}$ with Bob, and another two pairs $|\psi^-\rangle_{56}$ and $|\psi^-\rangle_{78}$ with Charlie. She retains the photons 1, 3, 5, 7, and the two photons a and b in the entangled state $|\chi\rangle_{ab}$. Bob and Charlie keep the photons 2 and 4, and 6 and 8, respectively. The joint state of the quantum system composed of the six photons a, b, 3, 4, 5, and 6 can be written as

see equation (5) above.

For splitting the state $|\chi\rangle_{ab}$, Alice first performs Bell-state measurement on the photons a and 3, and then b and 5. She records the results R_{a3} and R_{b5}. In this way, the state $|\chi\rangle_{ab}$ is transferred to the particles 4 and 6 which are kept by Bob and Charlie, respectively. In order to set up a quantum channel for Bob and Charlie, Alice performs Bell-state measurement on the photons 1 and 7, and records the result R_{17}. With R_{17}, the state of the photons 2 and 8 can be determined as

$$\begin{aligned}
|\Phi\rangle_{1278}&\equiv|\psi^-\rangle_{12}\otimes|\psi^-\rangle_{78}\\
&=\frac{1}{2}(|\psi^-\rangle_{17}|\psi^-\rangle_{28}-|\psi^+\rangle_{17}|\psi^+\rangle_{28}\\
&\quad-|\phi^-\rangle_{17}|\phi^-\rangle_{28}+|\phi^+\rangle_{17}|\phi^+\rangle_{28}).
\end{aligned} \qquad (6)$$

For reconstructing the original state $|\chi\rangle_{ab}$, Bob or Charlie performs Bell-state measurement on his two photons and then tells the other one the result when they act in concert. We assume that Charlie will obtain the quantum secret

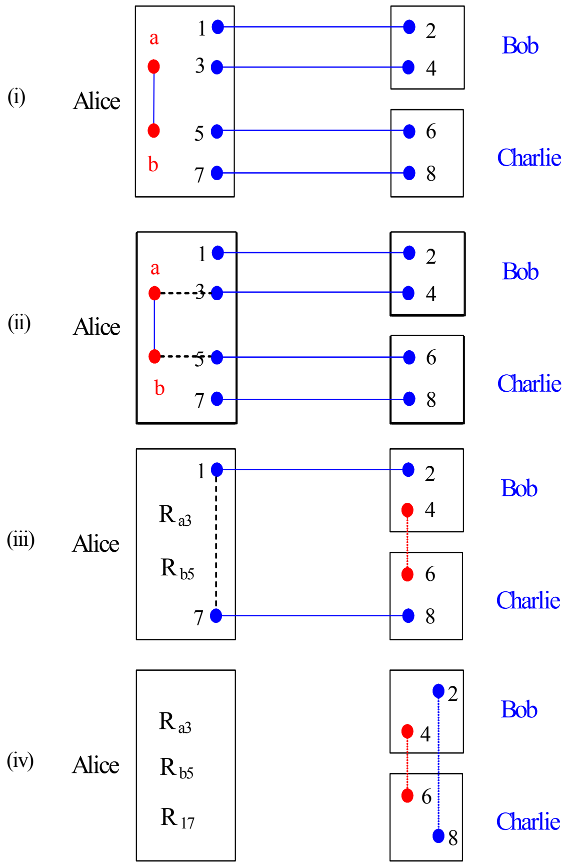

Fig. 1. Quantum secret sharing based on entanglement swapping with Bell-basis measurements and local unitary operation by using four EPR pairs as the quantum channel. The bold lines connect qubits in Bell states or the two-particle entangled state $|\chi\rangle_{ab}$, the dashed lines connect qubits on which a Bell measurement is made, and the diamond lines connect qubits in entangled states (or Bell state) induced by entanglement swapping, similar to that in reference [23]. R_{a3}, R_{b5} and R_{17} are the results of the Bell-basis measurements on the particles a and 3, b and 5, 1 and 7, respectively.

message $|\chi\rangle_{ab}$ with the help of Bob's. Due to symmetry, the other cases are the same as it with or without a little of modification. As an example, let us suppose that the results R_{a3}, R_{b5} and R_{17} published by Alice are $|\psi^-\rangle_{a3}$, $|\psi^-\rangle_{b5}$ and $|\psi^-\rangle_{17}$

$$\begin{aligned}|\Phi\rangle_{2846} &\equiv |\psi^-\rangle_{28} \otimes (\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{46}\\ &= \frac{1}{2}\{|\psi^-\rangle_{24}(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle)_{86}\\ &\quad -|\psi^+\rangle_{24}(\alpha|00\rangle + \beta|01\rangle - \gamma|10\rangle - \delta|11\rangle)_{86}\\ &\quad +|\phi^-\rangle_{24}(\alpha|10\rangle + \beta|11\rangle + \gamma|00\rangle + \delta|01\rangle)_{86}\\ &\quad +|\phi^+\rangle_{24}(\alpha|10\rangle + \beta|11\rangle - \gamma|00\rangle - \delta|01\rangle)_{86}\}.\end{aligned} \tag{7}$$

If the result of the Bell-state measurement R_{24} done by Bob is $|\psi^-\rangle_{24}$, $|\psi^+\rangle_{24}$, $|\phi^-\rangle_{24}$ or $|\phi^+\rangle_{24}$, Charlie needs to perform the local unitary operations $U_0 \otimes U_0$, $U_1 \otimes U_0$, $U_2 \otimes U_0$ or $U_3 \otimes U_0$ on the particles 8 and 6 respectively, and then reconstructs the state $|\chi\rangle_{ab}$.

For the other cases, the relation between the local unitary operations with which Bob can recover the original state $|\chi\rangle_{ab}$ and the results R_{a3}, R_{b5}, R_{17} and R_{24} is shown in Table 1. Same as those in reference [18], we define V as the bit value of the Bell state, i.e., $V_{|\phi^\pm\rangle} \equiv 0$, $V_{|\psi^\pm\rangle} \equiv 1$; That is, the bit value $V = 0$ if the states of the two particles in a Bell state are parallel, otherwise $V = 1$. $V_{total} \equiv V_{a3} \oplus V_{b5} \oplus V_{17} \oplus V_{24}$. P denotes the parity of the result of the Bell-state measurement on the two-particle quantum system $R_i \in \{|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle, |\phi^-\rangle\}$, i.e., $P_{|\psi^\pm\rangle} \equiv \pm$, $P_{|\phi^\pm\rangle} \equiv \pm$ and $P_{total} \equiv \prod_{i=1} \otimes P_{R_i} = P_{R_{a3}} \otimes P_{R_{b5}} \otimes P_{R_{17}} \otimes P_{R_{24}}$; Φ_{86} is the state of the particles 8 and 6 after all the Bell-basis measurements are taken, $\oplus$ means summing modulo 2 and the unitary operations $U_i \otimes U_j$ $(i, j \in \{0, 1, 2, 3\})$ represents performing the unitary operation U_i on the particle 8 and the operation U_j on the particle 6, respectively. For instance, if the results of R_{a3}, R_{b5}, R_{17} and R_{24} are $|\psi^-\rangle_{a3}$, $|\phi^-\rangle_{b5}$, $|\psi^+\rangle_{17}$ and $|\psi^-\rangle_{24}$, then $V_{total} = 1 \oplus 0 \oplus 1 \oplus 1 = 1$, $V_{b5} = 0$, $P_{b5} = -$, and $P_{total} = (-) \otimes (-) \otimes (+) \otimes (-) = -$, and Charlie performs the unitary operations U_1 and U_2 on the particles 8 and 6 respectively for reconstructing the original state $|\chi\rangle_{ab}$.

In detail, Alice performs Bell-state measurements on the particles a and 3, b and 5, 1 and 7, and she publishes the results R_{b5} , $R_{a3} \oplus R_{b5} \oplus R_{17}$ with simple coding, i.e., 0 or 1, and the parities P_{b5} and $P = P_{a3} \otimes P_{b5} \otimes P_{17}$ (+ or $-$). She only pays four bits of classical information for announcing her results in public, not six bits. Subsequently, Bob takes Bell-state measurement on the particles 2 and 4, and records the result R_{24} including its bit value and its parity (two bits of classical information). With the four bits of information published by Alice, Charlie can reconstruct the original state $|\chi\rangle_{ab}$ according to the Table 1 with the help of Bob's. On the other hand, neither Bob nor Charlie can obtain the unknown two-qubit state if they do not cooperate even they get the information published by Alice. Let us suppose that the result of the measurement on particles b and 5 done by Alice is $|\phi^+\rangle_{b5}$. From Table 2, we can see that Charlie has only the probability 1/4 to choose two correct local unitary operations for reconstructing the two-qubit unknown state if he knows the information published by Alice after Bob performed the Bell-state measurement on his two particles. That is, the four results of Bob's measurements represent four kinds of combination of the two operations on the two particles kept by Charlie. Moreover, if Bob does not measures his two particles, Charlie can only obtain a random result, no useful information about the unknown state, as he gets only a part of the two-qubit quantum system $|\chi\rangle_{ab}$ after the entanglement swapping is performed by Alice.

Similar to the controlled teleportation [18], the original state $|\chi\rangle_{ab}$ is an arbitrary one for two-particle quantum system in the Hilbert space $H^2 \otimes H^2$, i.e., $|\chi\rangle_{ab} = \alpha|00\rangle_{ab} + \beta|01\rangle_{ab} + \gamma|10\rangle_{ab} + \delta|11\rangle_{ab}$. Moreover, this QSTS scheme is symmetric as each of the agents can act as the receiver with the help of the other. In essence, any

Table 1. The relation between the local unitary operations and the results R_{a3}, R_{b5}, R_{17} and R_{24}. Φ_{86} is the state of the two particles hold in the hand of Charlie after all the measurements are done by Alice and Bob; $U_i \otimes U_j$ are the local unitary operations with which Charlie can reconstruct the unknown state $|\chi\rangle_{ab}$.

V_{total}	V_{b5}	P_{b5}	P_{total}	Φ_{86}	$U_i \otimes U_j$
0	1	$-$	$+$	$\alpha\|00\rangle + \beta\|01\rangle + \gamma\|10\rangle + \delta\|11\rangle$	$U_0 \otimes U_0$
0	1	$+$	$-$	$\alpha\|00\rangle - \beta\|01\rangle + \gamma\|10\rangle - \delta\|11\rangle$	$U_0 \otimes U_1$
1	0	$-$	$+$	$\alpha\|00\rangle + \beta\|01\rangle - \gamma\|10\rangle - \delta\|11\rangle$	$U_1 \otimes U_0$
1	0	$+$	$-$	$\alpha\|00\rangle - \beta\|01\rangle - \gamma\|10\rangle + \delta\|11\rangle$	$U_1 \otimes U_1$
0	1	$-$	$-$	$\alpha\|01\rangle + \beta\|00\rangle + \gamma\|11\rangle + \delta\|10\rangle$	$U_0 \otimes U_2$
0	1	$+$	$+$	$\alpha\|01\rangle - \beta\|00\rangle + \gamma\|11\rangle - \delta\|10\rangle$	$U_0 \otimes U_3$
1	0	$-$	$-$	$\alpha\|01\rangle + \beta\|00\rangle - \gamma\|11\rangle - \delta\|10\rangle$	$U_1 \otimes U_2$
1	0	$+$	$+$	$\alpha\|01\rangle - \beta\|00\rangle - \gamma\|11\rangle + \delta\|10\rangle$	$U_1 \otimes U_3$
1	1	$-$	$+$	$\alpha\|10\rangle + \beta\|11\rangle + \gamma\|00\rangle + \delta\|01\rangle$	$U_2 \otimes U_0$
1	1	$+$	$-$	$\alpha\|10\rangle - \beta\|11\rangle + \gamma\|00\rangle - \delta\|01\rangle$	$U_2 \otimes U_1$
0	0	$-$	$+$	$\alpha\|10\rangle + \beta\|11\rangle - \gamma\|00\rangle - \delta\|01\rangle$	$U_3 \otimes U_0$
0	0	$+$	$-$	$\alpha\|10\rangle - \beta\|11\rangle - \gamma\|00\rangle + \delta\|01\rangle$	$U_3 \otimes U_1$
1	1	$-$	$-$	$\alpha\|11\rangle + \beta\|10\rangle + \gamma\|01\rangle + \delta\|00\rangle$	$U_2 \otimes U_2$
1	1	$+$	$+$	$\alpha\|11\rangle - \beta\|10\rangle + \gamma\|01\rangle - \delta\|00\rangle$	$U_2 \otimes U_3$
0	0	$-$	$-$	$\alpha\|11\rangle + \beta\|10\rangle - \gamma\|01\rangle - \delta\|00\rangle$	$U_3 \otimes U_2$
0	0	$+$	$+$	$\alpha\|11\rangle - \beta\|10\rangle - \gamma\|01\rangle + \delta\|00\rangle$	$U_3 \otimes U_3$

Table 2. The relation between the local unitary operations and the results of the measurements done by Bob R_{Bob} after Alice published her information about her measurements. Here $V_{Alice} = V_{a3} \oplus V_{b5} \oplus V_{17}$, $P_{Alice} = P_{a3} \otimes P_{b5} \otimes P_{17}$, and $U_i \otimes U_j$ are the local unitary operations with which Charlie can reconstruct the unknown state $|\chi\rangle_{ab}$.

V_{Alice}	V_{b5}	P_{b5}	P_{Alice}	R_{Bob}	Φ_{86}	$U_i \otimes U_j$
0	0	$+$	$+$	ϕ^+	$\alpha\|11\rangle - \beta\|10\rangle - \gamma\|01\rangle + \delta\|00\rangle$	$U_3 \otimes U_3$
0	0	$+$	$+$	ϕ^-	$\alpha\|10\rangle - \beta\|11\rangle - \gamma\|00\rangle + \delta\|01\rangle$	$U_3 \otimes U_1$
0	0	$+$	$+$	ψ^+	$\alpha\|01\rangle - \beta\|00\rangle - \gamma\|11\rangle + \delta\|10\rangle$	$U_1 \otimes U_3$
0	0	$+$	$+$	ψ^-	$\alpha\|00\rangle - \beta\|01\rangle - \gamma\|10\rangle + \delta\|11\rangle$	$U_1 \otimes U_1$
0	0	$+$	$-$	ϕ^+	$\alpha\|10\rangle + \beta\|11\rangle - \gamma\|00\rangle - \delta\|01\rangle$	$U_3 \otimes U_0$
0	0	$+$	$-$	ϕ^-	$\alpha\|11\rangle + \beta\|10\rangle - \gamma\|01\rangle - \delta\|00\rangle$	$U_3 \otimes U_2$
0	0	$+$	$-$	ψ^+	$\alpha\|00\rangle + \beta\|01\rangle - \gamma\|10\rangle - \delta\|11\rangle$	$U_1 \otimes U_0$
0	0	$+$	$-$	ψ^-	$\alpha\|01\rangle + \beta\|00\rangle - \gamma\|11\rangle - \delta\|10\rangle$	$U_1 \otimes U_2$
1	0	$+$	$+$	ϕ^+	$\alpha\|01\rangle - \beta\|00\rangle + \gamma\|11\rangle - \delta\|10\rangle$	$U_0 \otimes U_3$
1	0	$+$	$+$	ϕ^-	$\alpha\|00\rangle - \beta\|01\rangle + \gamma\|10\rangle - \delta\|11\rangle$	$U_0 \otimes U_1$
1	0	$+$	$+$	ψ^-	$\alpha\|10\rangle - \beta\|11\rangle + \gamma\|00\rangle - \delta\|01\rangle$	$U_2 \otimes U_1$
1	0	$+$	$+$	ψ^+	$\alpha\|11\rangle - \beta\|10\rangle + \gamma\|01\rangle - \delta\|00\rangle$	$U_2 \otimes U_3$
1	0	$+$	$-$	ϕ^+	$\alpha\|00\rangle + \beta\|01\rangle + \gamma\|10\rangle + \delta\|11\rangle$	$U_0 \otimes U_0$
1	0	$+$	$-$	ϕ^-	$\alpha\|01\rangle + \beta\|00\rangle + \gamma\|11\rangle + \delta\|10\rangle$	$U_0 \otimes U_2$
1	0	$+$	$-$	ψ^+	$\alpha\|10\rangle + \beta\|11\rangle + \gamma\|00\rangle + \delta\|01\rangle$	$U_2 \otimes U_0$
1	0	$+$	$-$	ψ^-	$\alpha\|11\rangle + \beta\|10\rangle + \gamma\|01\rangle + \delta\|00\rangle$	$U_2 \otimes U_2$

QSTS scheme can be used for the controlled teleportation [18,31–33] by means that one of the two agents acts as the controller and the other recovers the unknown state according to the information published by the sender and the controller. That is, this QSTS scheme can be used to complete the task of controlled teleportation of an arbitrary two-qubit state more efficient than that in reference [18] as the quantum resource is only two-photon entanglements, not GHZ states which are not easy for producing [20–22]. On the other hand, the users should used at least four EPR pairs for sharing the state in this QSTS scheme. Two EPR pairs ($|\psi^-\rangle_{34}$ and $|\psi^-\rangle_{56}$) are used to transfer the original state and the other two pairs ($|\psi^-\rangle_{12}$ and $|\psi^-\rangle_{78}$) are used to set up the quantum channel between the two agents, Bob and Charlie, with the control of the sender Alice.

3 Circular QSTS scheme with entanglement swapping

In the QSTS scheme discussed above, the sender Alice should provide the resource for Bob and Charlie to set up the quantum channel, which will cost Alice a lot of quantum resource when the number of the agents increases largely. If the topological structure of the QSTS is circular, the resource can be reduced greatly. In this way, Alice shares the two-photon entanglement $|\psi^-\rangle_{34}$ with Bob, and $|\psi^-\rangle_{56}$ with Charlie, and then Bob shares the entanglement $|\psi^-\rangle_{78}$ with Charlie, shown in Figure 2. After the measurements on the photons a and 3, and b and 5, the original state $|\chi\rangle_{ab}$ is transferred to the photons 4 and 6. That is, the quantum information, the unknown state, is

Table 3. The relation between the local unitary operations and the results R_{a3}, R_{b5}, and $R_{2i+5,2i+6}$ $(1 \leq i \leq N-1)$. $\Phi_{2N+4,6}$ is the state of the two particles hold in the hand of Charlie after all the measurements are done by Alice and Bob$i$; $U_i \otimes U_j$ are the local unitary operations with which Charlie can reconstruct the unknown state $|\chi\rangle_{ab}$.

V_{total}	V_{b5}	P_{b5}	P_{total}	$\Phi_{2N+4,6}$	$U_i \otimes U_j$
1	1	$-$	$-$	$\alpha\|00\rangle+\beta\|01\rangle+\gamma\|10\rangle+\delta\|11\rangle$	$U_0 \otimes U_0$
1	1	$+$	$+$	$\alpha\|00\rangle-\beta\|01\rangle+\gamma\|10\rangle-\delta\|11\rangle$	$U_0 \otimes U_1$
0	0	$-$	$-$	$\alpha\|00\rangle+\beta\|01\rangle-\gamma\|10\rangle-\delta\|11\rangle$	$U_1 \otimes U_0$
0	0	$+$	$+$	$\alpha\|00\rangle-\beta\|01\rangle-\gamma\|10\rangle+\delta\|11\rangle$	$U_1 \otimes U_1$
1	1	$-$	$+$	$\alpha\|01\rangle+\beta\|00\rangle+\gamma\|11\rangle+\delta\|10\rangle$	$U_0 \otimes U_2$
1	1	$+$	$-$	$\alpha\|01\rangle-\beta\|00\rangle+\gamma\|11\rangle-\delta\|10\rangle$	$U_0 \otimes U_3$
0	0	$-$	$+$	$\alpha\|01\rangle+\beta\|00\rangle-\gamma\|11\rangle-\delta\|10\rangle$	$U_1 \otimes U_2$
0	0	$+$	$-$	$\alpha\|01\rangle-\beta\|00\rangle-\gamma\|11\rangle+\delta\|10\rangle$	$U_1 \otimes U_3$
0	1	$-$	$-$	$\alpha\|10\rangle+\beta\|11\rangle+\gamma\|00\rangle+\delta\|01\rangle$	$U_2 \otimes U_0$
0	1	$+$	$+$	$\alpha\|10\rangle-\beta\|11\rangle+\gamma\|00\rangle-\delta\|01\rangle$	$U_2 \otimes U_1$
1	0	$-$	$-$	$\alpha\|10\rangle+\beta\|11\rangle-\gamma\|00\rangle-\delta\|01\rangle$	$U_3 \otimes U_0$
1	0	$+$	$+$	$\alpha\|10\rangle-\beta\|11\rangle-\gamma\|00\rangle+\delta\|01\rangle$	$U_3 \otimes U_1$
0	1	$-$	$+$	$\alpha\|11\rangle+\beta\|10\rangle+\gamma\|01\rangle+\delta\|00\rangle$	$U_2 \otimes U_2$
0	1	$+$	$-$	$\alpha\|11\rangle-\beta\|10\rangle+\gamma\|01\rangle-\delta\|00\rangle$	$U_2 \otimes U_3$
1	0	$-$	$+$	$\alpha\|11\rangle+\beta\|10\rangle-\gamma\|01\rangle-\delta\|00\rangle$	$U_3 \otimes U_2$
1	0	$+$	$-$	$\alpha\|11\rangle-\beta\|10\rangle-\gamma\|01\rangle+\delta\|00\rangle$	$U_3 \otimes U_3$

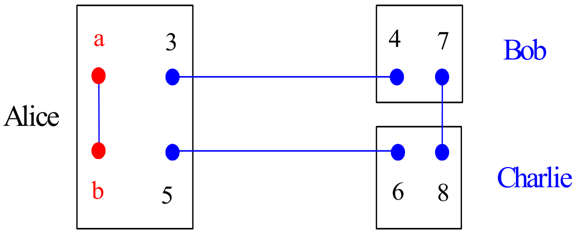

Fig. 2. The circular QSTS scheme with entanglement swapping in the case with two agents.

split by Bob and Charlie. The entanglement $|\psi^-\rangle_{78}$ is just used to transfer the unknown state $|\chi\rangle_{ab}$ to one of the two agents with the help of the other. The entanglement $|\psi^-\rangle_{12}$ is not necessary in this circular QSTS with two agents.

It is straightforwardly to generalize this circular QSTS scheme to the case with N agents, say Bob$_i$ $(i = 1, 2, ..., N-1)$ and Charlie. As the symmetry, we still assume that Charlie is the agent who will reconstruct the unknown state with the help of the other $N-1$ agents, Bob$_i$. To this end, Alice should share an EPR pairs $|\psi^-\rangle_{34}$ with Bob$_1$ and another pair $|\psi^-\rangle_{56}$ with Charlie. The ith agent Bob$_i$ shares an EPR pair $|\psi^-\rangle_{2i+5,2i+6}$ with the $(i+1)$th agent Bob$_{i+1}$ $(i = 1, 2, \ldots, N-2)$. [The $(N-1)$th agent Bob$_{N-1}$ shares the entanglement $|\psi^-\rangle_{2N+3,2N+4}$ with Charlie.] If an agent wants to act as a controller, he performs a Bell-state measurement on his two photons. That is, all the Bobs measure their photons and then tell the information of the outcomes to Charlie for reconstructing the original state $|\chi\rangle_{ab}$ when they cooperate.

Table 3 gives us the relation between the results and the local unitary operations. All the notations in Table 2 are as same as those in Table 1, see Section 2. We do not exploit the notation for the EPR pair $|\psi^-\rangle_{12}$, then the total value V_{total} is the sum of the values of the outcomes obtained by Alice and the $N-1$ controllers Bob$_i$. So does the total parity P_{total}.

In this circular QSTS scheme, each user should share an EPR pair with his neighboring one, and he performs Bell-state measurements on his photons if he wants to act as a controller. Alice's measurements will transfer the original two-qubit state $|\chi\rangle_{ab}$ to other photons with entanglement swapping. The measurements done by the controllers help to set up the quantum channel for sharing the state with their control. For the view of producing or measuring a m-particle entanglement, this circular QSTS scheme is an optimal one as it just exploits two-photon entanglement resource and Bell-state measurements. As almost all of the photons are useful for the quantum communication, its efficiency for qubits approaches the maximal value. Same as the QSTS scheme discussed in Section 2, any one of the agents cannot obtain the quantum information, the unknown two-qubit state unless he cooperate with all of the other agents even though Alice published the results of her measurements.

4 Discussion and summary

As discussed in references [2,3], if Alice can prevent the dishonest man (no more than one) in the agents from eavesdropping the quantum secret, the process for sharing an unknown state is secure for any eavesdropper. In these two QSTS schemes, their security depends on the process for setting up the quantum channel (sharing the maximally entangled states), i.e., the EPR pairs. Certainly, it is difficult for two users to share an EPR pairs securely, but easy to share a sequence of EPR pairs [24,27]. In a noise channel, the parties can exploit entanglement purification [35,36] to distill some maximally entangled states for improving the security of quantum communication. In this way, these two QSTS schemes for sharing an arbitrary two-qubit states are secure. Another feature of these two QSTS schemes is that two-particle Bell-state measurements are required, which is more efficient than those with m-particle joint measurement ($m > 2$).

In summary, we present two QSTS schemes for sharing an arbitrary two-qubit state $|\chi\rangle_{ab} = \alpha|00\rangle_{ab} + \beta|01\rangle_{ab} + \gamma|10\rangle_{ab} + \delta|11\rangle_{ab}$ based on entanglement swapping with EPR pairs and Bell-state measurements. One is based on the quantum channel with four EPR pairs shared in advance, the other is based on a circular topological structure. Any one in the agents has the choice to reconstruct the original state $|\chi\rangle_{ab}$ with the help of the others. Moreover the circular QSTS scheme reduces the quantum resource needed largely when the number of the agents is large. Almost all the EPR pairs can be used for quantum communication in those two schemes, their efficiency for qubits approaches the maximal value, same as references [16–18]. They are more convenient in application than the other schemes existing as they require only two-qubit entanglements and two-qubit joint measurements for sharing an arbitrary two-qubit state.

This work is supported by the National Natural Science Foundation of China under Grant Nos. 10447106, 10435020, 10254002, A0325401 and 10374010, and Beijing Education Committee under Grant No. XK100270454.

References

1. G.R. Blakley, in *Proceedings of the American Federation of Information Processing 1979 National Computer Conference* (American Federation of Information Processing, Arlington, VA, 1979), pp. 313-317; A. Shamir, Commun. ACM **22**, 612 (1979)
2. M. Hillery, V. Bužek, A. Berthiaume, Phys. Rev. A **59**, 1829 (1999)
3. A. Karlsson, M. Koashi, N. Imoto, Phys. Rev. A **59**, 162 (1999)
4. L. Xiao et al., Phys. Rev. A **69**, 052307 (2004); F.G. Deng, H.Y. Zhou, G.L. long, Phys. Lett. A **337**, 329 (2005); F.G. Deng, G.L. Long, H.Y. Zhou, Phys. Lett. A **340**, 43 (2005); F.G. Deng et al., Chin. Phys. Lett. **21**, 2097 (2004)
5. G.P. Guo, G.C. Guo, Phys. Lett. A **310**, 247 (2003)
6. F.L. Yan, T. Gao, Phys. Rev. A **72**, 012304 (2005)
7. A. Cabello, e-print `arXiv:quant-ph/0009025`
8. C.P. Yang, J. Gea-Banacloche, J. Opt. B: Quant. Semiclass. Opt. **3**, 407 (2001)
9. Z.J. Zhang, Z.X. Man, Phys. Rev. A **72**, 022303 (2005)
10. D. Gottesman, Phys. Rev. A **61**, 042311 (2000)
11. R. Cleve, D. Gottesman, H.K. Lo, Phys. Rev. Lett. **83**, 648 (1999)
12. Z.J. Zhang, Phys. Lett. A **342**, 60 (2005)
13. S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000)
14. V. Karimipour, A. Bahraminasab, S. Bagherinezhad, Phys. Rev. A **65**, 042320 (2002)
15. Z.J. Zhang, Y.Li, Z.X. Man, Phys. Rev. A **71**, 044301 (2005); F.G. Deng, X.H. Li, H.Y. Zhou, Z. Zhang, Phys. Rev. A **72**, 044302 (2005)
16. Y.M. Li, K.S. Zhang, K.C. Peng, Phys. Lett. A **324**, 420 (2004)
17. F.G. Deng, X.H. Li, C.Y. Li, P. Zhou, H.Y. Zhou, Phys. Rev. A **72**, 044301 (2005)
18. F.G. Deng, C.Y. Li, Y.S. Li, H.Y. Zhou, Y. Wang, Phys. Rev. A **72**, 022338 (2005)
19. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
20. D. Bouwmeester, J.W. Pan, M. Daniell, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999)
21. J.W. Pan, M. Daniell, S. Gasparoni, G. Weihs, A. Zeilinger, Phys. Rev. Lett. **86**, 4435 (2001)
22. Z. Zhao, Y.A. Chen, A.N. Zhang, T. Yang, H.J. Briegel, J.W. Pan, Nature **430**, 54 (2004)
23. A. Cabello, Phys. Rev. A **61**, 052312 (2000)
24. F.G. Deng, G.L. Long, X.S. Liu, Phys. Rev. A **68**, 042317 (2003)
25. F.G. Deng, G.L. Long, Phys. Rev. A **69**, 052319 (2004); F.G. Deng, G.L. Long, e-print `arXiv:quant-ph/0408102`
26. C. Wang et al., Phys. Rev. A **71**, 044305 (2005)
27. C.P. Yang, G.C. Guo, Phys. Rev. A **59**, 4217 (1999)
28. M. Zukowski, A. Zeilinger, M.A. Horne, A.K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993)
29. S. Bose, V. Vedral, P.L. Knight, Phys. Rev. A **57**, 822 (1998)
30. J.W. Pan, D. Bouwmeester, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998)
31. A. Karlsson, M. Bourennane, Phys. Rev. A **58**, 4394 (1998)
32. F.L. Yan, D. Wang, Phys. Lett. A **316**, 297 (2003)
33. C.P. Yang, Shih-I Chu, S.Han, Phys. Rev. A **70**, 022329 (2004)
34. M.A. Nielsen, I.L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, UK, 2000)
35. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996)
36. M. Murao, M.B. Plenio, S. Popescu, V. Vedral, P.L. Knight, Phys. Rev. A **57**, R4075 (1998)