SCIENCE CHINA
Physics, Mechanics & Astronomy

• Research Paper •

December 2010 Vol.53 No.12: 2238–2244
doi: 10.1007/s11433-010-4181-0

Quantum secret sharing between multiparty and multiparty with Bell states and Bell measurements

SHI RunHua[1,2*], HUANG LiuSheng[1,3], YANG Wei[1,3] & ZHONG Hong[2]

[1] *National High Performance Computing Center at Hefei, Department of Computer Science and Technology, University of Science and Technology of China, Hefei, 230027, China;*
[2] *School of Computer Science and Technology, Anhui University, Hefei 230039, China;*
[3] *Suzhou Institute for Advanced Study, USTC, Suzhou 215123, China*

Received June 23, 2010; accepted September 1, 2010

We present a quantum secret sharing scheme between multiparty (*m* members in Group 1) and multiparty (*n* members in Group 2), and analyze its security. This scheme takes EPR pairs in Bell states as quantum resources. In order to obtain the shared key, all members only need to perform Bell measurements, rather than perform any local unitary operation. The total efficiency in this scheme approaches 100% as the classical information exchanged is not necessary except for the eavesdropping checks.

quantum information, quantum cryptography, quantum secret sharing

PACS: 03.67.Dd, 03.67.Ac

1 Introduction

In the last two decades, quantum cryptography has progressed quickly since the original work on quantum key distribution by Bennett and Brassard [1]. Especially, the first metropolitan quantum cryptography network for government administration has recently been field tested in Wuhu, China by researchers of Key Laboratory of Quantum Information [2,3]. Under the principle of quantum mechanics, other cryptographic tasks can be realized, such as quantum secret sharing (QSS).

The first QSS protocol was presented by Hillery, Bužek and Berthiaume [4] by using a three-particle or a four-particle entangled Greenberger-Horne-Zeilinger (GHZ) state for sharing a classical secret with three or four parties, and generalized by Xiao et al. [5] into arbitrary multiparties. Later Karlsson et al. proposed another QSS scheme [6] with a two-photon polarization-entangled state. Afterward, QSS has attracted widespread attention and many studies focus on QSS theoretically and experimentally [7–39].

QSS concentrates mainly on two kinds of research. One only deals with the QSS of classical information [13–28], in which a classical secret is shared among all participants based on quantum mechanics, and the other with the QSS of quantum information [29–39], in which the secret is an arbitrary unknown quantum state. This paper mainly focuses on the former.

Recently, a protocol for QSS between multiparty (*m* members in Group 1) and multiparty (*n* members in Group 2) has been proposed by Yan and Gao [24]. In their protocol, all members in Group 1 directly encode their respective keys on the states of single photons via unitary operations, and then the last one in Group 1 sends 1/*n* of the resulting qubits to each of Group 2. After each member in Group 2 measures the photons according to all members' measuring-basis sequences in Group 1, the two groups share the secret key. Unfortunately, Li et al. [25] and Han et al. [26] pointed out that this protocol is insecure. Later, Yan et al. [27] and Gao et al. [28] respectively presented two im-

*Corresponding author (email: hfsrh@sina.com)

© Science China Press and Springer-Verlag Berlin Heidelberg 2010

proved schemes for QSS between multiparty and multiparty. However, these improved schemes still make it necessary to use quantum memory and to publish much information about the measurement basis, so the total efficiency is low. In this paper, we will present a QSS scheme between multiparty and multiparty with Bell states and Bell measurements. Compared with these known schemes, the total efficiency of our scheme is higher, which approaches 100% as the classical information exchanged is not necessary except for the eavesdropping checks.

2 The quantum correlation property of Bell states and Bell measurements

We first introduce the quantum correlation property of Bell states and Bell measurements in multiparty protocols. For simplicity, we first consider the three-party scenario. Suppose there are three parties, say, Alice, Bob and Charlie, and they share 3 EPR pairs in Bell states. Four Bell states are defined as follows:

$$\left|\varphi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right), \tag{1}$$

$$\left|\varphi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right), \tag{2}$$

$$\left|\psi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right), \tag{3}$$

$$\left|\psi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle-\left|10\right\rangle\right). \tag{4}$$

Without a loss of generalization, we assume that 3 EPR pairs are in $\left|\varphi^{-}\right\rangle_{12}$, $\left|\psi^{+}\right\rangle_{34}$ and $\left|\psi^{-}\right\rangle_{56}$, respectively, where Alice holds two particles 1 and 6, Bob, two particles 2 and 3, and Charlie, two particles 4 and 5, respectively, as shown in Figure 1.

After the secure quantum channel is set up, if all participants measure their particles with Bell basis, the possible relationships of their measurement results are shown in eq. (5).

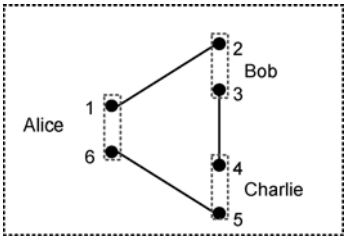

Figure 1 Three-party sharing 3 EPR pairs. The two particles linked with the bold lines are in Bell states. The panes with the dashed lines represent the Bell-state measurements.

$$\begin{aligned}
&\left|\varphi^{-}\right\rangle_{12}\left|\psi^{+}\right\rangle_{34}\left|\psi^{-}\right\rangle_{56}=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right)_{12}\otimes\frac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right)_{34}\\
&\otimes\frac{1}{\sqrt{2}}\left(\left|01\right\rangle-\left|10\right\rangle\right)_{56}\\
&=\frac{1}{2\sqrt{2}}\left(\left|000101\right\rangle-\left|000110\right\rangle+\left|001001\right\rangle-\left|001010\right\rangle\right.\\
&\quad\left.-\left|110101\right\rangle+\left|110110\right\rangle-\left|111001\right\rangle+\left|111010\right\rangle\right)_{123456}\\
&=\frac{1}{2\sqrt{2}}\left(\left|01\right\rangle_{16}\left|00\right\rangle_{23}\left|10\right\rangle_{45}-\left|00\right\rangle_{16}\left|00\right\rangle_{23}\left|11\right\rangle_{45}\right.\\
&\quad+\left|01\right\rangle_{16}\left|01\right\rangle_{23}\left|00\right\rangle_{45}-\left|00\right\rangle_{16}\left|01\right\rangle_{23}\left|01\right\rangle_{45}\\
&\quad-\left|11\right\rangle_{16}\left|10\right\rangle_{23}\left|10\right\rangle_{45}+\left|10\right\rangle_{16}\left|10\right\rangle_{23}\left|11\right\rangle_{45}\\
&\quad\left.-\left|11\right\rangle_{16}\left|11\right\rangle_{23}\left|00\right\rangle_{45}+\left|10\right\rangle_{16}\left|11\right\rangle_{23}\left|01\right\rangle_{45}\right)\\
&=\frac{1}{8}\left(\left(\left|\psi^{+}\right\rangle+\left|\psi^{-}\right\rangle\right)_{16}\left(\left|\varphi^{+}\right\rangle+\left|\varphi^{-}\right\rangle\right)_{23}\left(\left|\psi^{+}\right\rangle-\left|\psi^{-}\right\rangle\right)_{45}\right.\\
&\quad-\left(\left|\varphi^{+}\right\rangle+\left|\varphi^{-}\right\rangle\right)_{16}\left(\left|\varphi^{+}\right\rangle+\left|\varphi^{-}\right\rangle\right)_{23}\left(\left|\varphi^{+}\right\rangle-\left|\varphi^{-}\right\rangle\right)_{45}\\
&\quad+\left(\left|\psi^{+}\right\rangle+\left|\psi^{-}\right\rangle\right)_{16}\left(\left|\psi^{+}\right\rangle+\left|\psi^{-}\right\rangle\right)_{23}\left(\left|\varphi^{+}\right\rangle+\left|\varphi^{-}\right\rangle\right)_{45}\\
&\quad-\left(\left|\varphi^{+}\right\rangle+\left|\varphi^{-}\right\rangle\right)_{16}\left(\left|\psi^{+}\right\rangle+\left|\psi^{-}\right\rangle\right)_{23}\left(\left|\psi^{+}\right\rangle+\left|\psi^{-}\right\rangle\right)_{45}\\
&\quad-\left(\left|\varphi^{+}\right\rangle-\left|\varphi^{-}\right\rangle\right)_{16}\left(\left|\psi^{+}\right\rangle-\left|\psi^{-}\right\rangle\right)_{23}\left(\left|\psi^{+}\right\rangle-\left|\psi^{-}\right\rangle\right)_{45}\\
&\quad+\left(\left|\psi^{+}\right\rangle-\left|\psi^{-}\right\rangle\right)_{16}\left(\left|\psi^{+}\right\rangle-\left|\psi^{-}\right\rangle\right)_{23}\left(\left|\varphi^{+}\right\rangle-\left|\varphi^{-}\right\rangle\right)_{45}\\
&\quad-\left(\left|\varphi^{+}\right\rangle-\left|\varphi^{-}\right\rangle\right)_{16}\left(\left|\varphi^{+}\right\rangle-\left|\varphi^{-}\right\rangle\right)_{23}\left(\left|\varphi^{+}\right\rangle+\left|\varphi^{-}\right\rangle\right)_{45}\\
&\quad\left.+\left(\left|\psi^{+}\right\rangle-\left|\psi^{-}\right\rangle\right)_{16}\left(\left|\varphi^{+}\right\rangle-\left|\varphi^{-}\right\rangle\right)_{23}\left(\left|\psi^{+}\right\rangle+\left|\psi^{-}\right\rangle\right)_{45}\right)\\
&=\frac{1}{4}\left(\left|\psi^{+}\right\rangle_{16}\left|\varphi^{+}\right\rangle_{23}\left|\psi^{+}\right\rangle_{45}-\left|\psi^{+}\right\rangle_{16}\left|\varphi^{-}\right\rangle_{23}\left|\psi^{-}\right\rangle_{45}\right.\\
&\quad-\left|\psi^{-}\right\rangle_{16}\left|\varphi^{+}\right\rangle_{23}\left|\psi^{-}\right\rangle_{45}+\left|\psi^{-}\right\rangle_{16}\left|\varphi^{-}\right\rangle_{23}\left|\psi^{+}\right\rangle_{45}\\
&\quad-\left|\varphi^{+}\right\rangle_{16}\left|\varphi^{+}\right\rangle_{23}\left|\varphi^{+}\right\rangle_{45}+\left|\varphi^{+}\right\rangle_{16}\left|\varphi^{-}\right\rangle_{23}\left|\varphi^{-}\right\rangle_{45}\\
&\quad+\left|\varphi^{-}\right\rangle_{16}\left|\varphi^{+}\right\rangle_{23}\left|\varphi^{-}\right\rangle_{45}-\left|\varphi^{-}\right\rangle_{16}\left|\varphi^{-}\right\rangle_{23}\left|\varphi^{+}\right\rangle_{45}\\
&\quad+\left|\psi^{+}\right\rangle_{16}\left|\psi^{+}\right\rangle_{23}\left|\varphi^{+}\right\rangle_{45}+\left|\psi^{+}\right\rangle_{16}\left|\psi^{-}\right\rangle_{23}\left|\varphi^{-}\right\rangle_{45}\\
&\quad+\left|\psi^{-}\right\rangle_{16}\left|\psi^{+}\right\rangle_{23}\left|\varphi^{-}\right\rangle_{45}+\left|\psi^{-}\right\rangle_{16}\left|\psi^{-}\right\rangle_{23}\left|\varphi^{+}\right\rangle_{45}\\
&\quad-\left|\varphi^{+}\right\rangle_{16}\left|\psi^{+}\right\rangle_{23}\left|\psi^{+}\right\rangle_{45}-\left|\varphi^{+}\right\rangle_{16}\left|\psi^{-}\right\rangle_{23}\left|\psi^{-}\right\rangle_{45}\\
&\quad\left.-\left|\varphi^{-}\right\rangle_{16}\left|\psi^{+}\right\rangle_{23}\left|\psi^{-}\right\rangle_{45}-\left|\varphi^{-}\right\rangle_{16}\left|\psi^{-}\right\rangle_{23}\left|\psi^{+}\right\rangle_{45}\right).
\end{aligned} \tag{5}$$

Furthermore, if the participants code the state $\left|\varphi^{+}\right\rangle$ as '00', $\left|\varphi^{-}\right\rangle$ as '01', $\left|\psi^{+}\right\rangle$ as '10' and $\left|\psi^{-}\right\rangle$ as '11', the relationships between the possible measurement results and the original quantum resources will satisfy the following equation:

$$M_{16}\oplus M_{23}\oplus M_{45}=R_{12}\oplus R_{34}\oplus R_{56}, \tag{6}$$

where M_{ij} denotes the code of the Bell measurement re-

sult on two particles i and j, and R_{st} denotes the code of the original Bell state of two particles s and t. For example, in eq. (5), the possible measurement results of all participants must satisfy: $M_{16} \oplus M_{23} \oplus M_{45} = 00$, since $R_{12} = 01$, $R_{34} = 10$ and $R_{56} = 11$, that is, $R_{12} \oplus R_{34} \oplus R_{56} = 00$. Thus, the measurement result of any one of the three participants can be uniquely deduced by the remaining participant's measurement results without any announcement.

For the generalization of three-party to m-party, the quantum correlation property between the possible measurement results and the original quantum resources still exists. That is,

$$M_{1(2m)} \oplus M_{23} \oplus ... \oplus M_{(2m-2)(2m-1)} = R_{12} \oplus R_{34} \oplus ... \oplus R_{(2m-1)2m}, \quad (7)$$

where $R_{12} \oplus R_{34} \oplus ... \oplus R_{(2m-1)2m}$ is known in advance. Especially, let $R_{12} \oplus R_{34} \oplus ... \oplus R_{(2m-1)2m} = 00$, then $M_{1(2m)} \oplus M_{23} \oplus ... \oplus M_{(2m-2)(2m-1)} = 00$. If we can make use of the quantum correlation property appropriately, we will build a secret of classical information, which is shared among all participants.

3 Quantum secret sharing between m-party and n-party

Let A_1, A_2, …, A_m, and B_1, B_2, …, B_n all be members respectively of Group 1 and Group 2 in our following protocol. After executing this protocol, m members of Group 1 will share a classical secret key with n members of Group 2, such that all members of Group 1 or 2 can collaborate to infer the shared secret key, but fewer members than these cannot obtain any information about it. We assume that there is a trusted third party, say, Trent, who generates all quantum resources and distributes these particles to all participants in security. The basic ideas of our QSS between m-party and n-party can be seen in Figure 2.

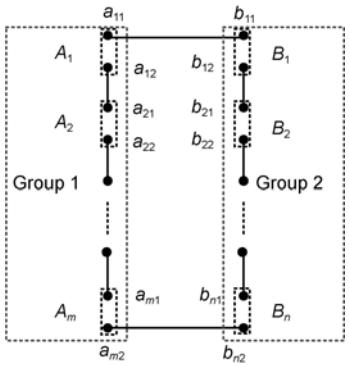

Figure 2 The rationale of our QSS between m-party and n-party. The two particles linked with the bold lines are in Bell states. The panes with the dashed lines represent the Bell-state measurements.

In the following we describe the scheme in detail.

(1) Trent prepares $(m+n)N$ EPR pairs. These EPR pairs are divided into N groups, and each group has $(m+n)$ EPR pairs, which can be used to share two classical bits of the secret. Here, the EPR pairs in each group must satisfy that the XOR result of their codes equals 00, that is, $R_{b_{11}a_{11}} \oplus R_{a_{12}a_{21}} \oplus ... \oplus R_{a_{m2}b_{n2}} \oplus ... \oplus R_{b_{21}b_{12}} = 00$ (see Figure 2). Moreover, he divides the particles into $2(m+n)$ sequences as follows:

$$\begin{aligned}
&[P_1(a_{11}), P_2(a_{11}), ..., P_N(a_{11})],\\
&[P_1(a_{12}), P_2(a_{12}), ..., P_N(a_{12})], \ \ \dots,\\
&[P_1(a_{m1}), P_2(a_{m1}), ..., P_N(a_{m1})],\\
&[P_1(a_{m2}), P_2(a_{m2}), ..., P_N(a_{m2})],\\
&[P_1(b_{11}), P_2(b_{11}), ..., P_N(b_{11})],\\
&[P_1(b_{12}), P_2(b_{12}), ..., P_N(b_{12})], \ \ \dots,\\
&[P_1(b_{n1}), P_2(b_{n1}), ..., P_N(b_{n1})],\\
&[P_1(b_{n2}), P_2(b_{n2}), ..., P_N(b_{n2})],
\end{aligned}$$

which are denoted as $S_{a_{11}}$, $S_{a_{12}}$, …, $S_{a_{m1}}$, $S_{a_{m2}}$, $S_{b_{11}}$, $S_{b_{12}}$, …, $S_{b_{n1}}$ and $S_{b_{n2}}$, respectively.

(2) Trent prepares $2(m+n)$ sets of decoy particles which are sufficient for a statistical analysis of eavesdropping as the sample sets, which are denoted as $R_{a_{11}}$, $R_{a_{12}}$, …, $R_{a_{m1}}$, $R_{a_{m2}}$, $R_{b_{11}}$, $R_{b_{12}}$, …, $R_{b_{n1}}$ and $R_{b_{n2}}$, respectively, where every decoy particle in sample sets is prepared randomly with either the Z-basis (i.e. $\{|0\rangle, |1\rangle\}$) or the X-basis (i.e. $\left\{|+x\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle), \ \ |-x\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)\right\}$). Then Trent inserts $R_{a_{11}}$, $R_{a_{12}}$, …, $R_{a_{m1}}$, $R_{a_{m2}}$, $R_{b_{11}}$, $R_{b_{12}}$, …, $R_{b_{n1}}$ and $R_{b_{n2}}$ randomly into $S_{a_{11}}$, $S_{a_{12}}$, …, $S_{a_{m1}}$, $S_{a_{m2}}$, $S_{b_{11}}$, $S_{b_{12}}$, …, $S_{b_{n1}}$ and $S_{b_{n2}}$, respectively. The new sequence is denoted as $S^*_{a_{11}}$, $S^*_{a_{12}}$, …, $S^*_{a_{m1}}$, $S^*_{a_{m2}}$, $S^*_{b_{11}}$, $S^*_{b_{12}}$, …, $S^*_{b_{n1}}$ and $S^*_{b_{n1}}$, respectively.

(3) Trent respectively sends two sequences $S^*_{a_{i1}}$, $S^*_{a_{i2}}$ to the member A_i ($1 \leqslant i \leqslant m$) and two sequences $S^*_{b_{j1}}$, $S^*_{b_{j2}}$ to the member B_j ($1 \leqslant j \leqslant n$).

(4) After confirming that each member A_i ($1 \leqslant i \leqslant m$) or B_j ($1 \leqslant j \leqslant n$) has received the two sequences ($S^*_{a_{i1}}$, $S^*_{a_{i2}}$) or ($S^*_{b_{j1}}$, $S^*_{b_{j2}}$), Trent announces the positions of the decoy particles and the corresponding measurement basis. All members measure the decoy particles according to Trent's announcements and tell Trent their measurement results. Trent compares the measurement results of the members with the initial states of the decoy particles in the sample

sets and analyzes the security of the transmissions. If the error rate is higher than the threshold determined by the channel noise, Trent cancels this protocol and restarts; or else all members of Group 1and Group 2 continue to the next step.

(5) The members A_i ($1 \leqslant i \leqslant m$) and B_j ($1 \leqslant j \leqslant n$) measure their l^{th} two-particle pair $(P_l(a_{i1}), P_l(a_{i2}))$ and $(P_l(b_{j1}), P_l(b_{j2}))$ respectively in the two sequences ($S_{a_{i1}}$, $S_{a_{i2}}$) and ($S_{b_{j1}}$, $S_{b_{j2}}$) with Bell basis for $l = 1, 2, \ldots N$. Each measured result with Bell basis defines the two bits of classical information: "00" if the result is $\left|\varphi^+\right\rangle$, "01" if it is $\left|\varphi^-\right\rangle$, "10" if it is $\left|\psi^+\right\rangle$, and "11" if it is $\left|\psi^-\right\rangle$. And then each member can transform her (his) measured result sequences into the classical bit strings k_{A_i} or k_{B_j}, where k_{A_i} is the shared sub-key of the member A_i ($1 \leqslant i \leqslant m$) and k_{B_j} is the shared sub-key of the member B_j ($1 \leqslant j \leqslant n$). Let $k = k_{A_1} \oplus k_{A_2} \oplus \ldots \oplus k_{A_m}$. Then k is the secret key shared between *m* members in Group 1 and *n* members of Group 2, since all k_{A_i} and k_{B_j} satisfy the relationship: $k_{A_1} \oplus k_{A_2} \oplus \ldots \oplus k_{A_m} \oplus k_{B_1} \oplus k_{B_2} \oplus \ldots \oplus k_{B_n} = 00\ldots00$, that is, $k_{A_1} \oplus k_{A_2} \oplus \ldots \oplus k_{A_m} = k_{B_1} \oplus k_{B_2} \oplus \ldots \oplus k_{B_n}$. Thus, all members of Group 1 (or Group 2) can infer the secret key k when they collaborate.

Please note that here we utilize the state coding and multi-step transmission and block transmission methods, which are first presented by Long et al. in ref. [40]. That is, four Bell states are defined as two classical bits of the secret respectively, and these EPR pairs are divided into two ordered sequences and then they are transmitted respectively.

4 Security analysis

Now we will prove that the present scheme is secure. A dishonest member generally has more power to attack than an outside eavesdropper, because he knows partial information legally and can tell a lie at the stage of eavesdropping detection to try to avoid introducing errors. Therefore, the main goal for the security of QSS is to prevent dishonest members from deception. In the following, we will mainly consider the cases, in which some dishonest members try to find the secret key by themselves without collaborating with other members.

4.1 The security of the scheme against the intercept-resend attack

Suppose that there is a dishonest member who can intercept the particle sequences transmitted from Trent to other members, and resend the fake sequences prepared by herself (himself) to other members (i.e. the intercept-resend attack). In our QSS scheme between multiparty and multiparty, the sender Trent and all members accomplish an honesty check before they found the shared secret. That is, Trent inserts randomly some decoy particles in the transmitted sequences, requires the members to measure them later, and checks their measurement results. In fact, if the dishonest member starts an intercept-resend attack, he does not know which are the decoy particles in the transmitted sequences and which state the decoy particle is in. Since each decoy particle is random in one of the four states $\{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle\}$, the probability of not being detected is $(1/4)^q$, where q is the number of the decoy particles in the sequences transmitted to other members.

4.2 The security of the scheme against the dishonest member's eavesdropping

Here we discuss a more complicated eavesdropping attack by a dishonest member who can prepare an ancilla and entangle the ancilla with the particles transmitted from Trent to other members by a unitary operation. At a later time, he can measure the ancilla to gain information about the secret. For simplicity, we mainly analyze the security of the special case, which involves one member in Group 1 and two members in Group 2. For example, Alice shares a classical secret with two members Bob and Charlie, as shown in Figure 1. Suppose Bob is the dishonest member, and Charlie is the honest member. We first analyze the effect of Bob's eavesdropping on the decoy particles in this scheme using the following equations [19,20]:

$$\hat{U}_B|0\rangle|\varepsilon\rangle_B = |0\rangle|\varepsilon_0\rangle_B + |1\rangle|\varepsilon_1\rangle_B, \tag{8}$$

$$\hat{U}_B|1\rangle|\varepsilon\rangle_B = |0\rangle|\varepsilon_0'\rangle_B + |1\rangle|\varepsilon_1'\rangle_B, \tag{9}$$

$$\begin{aligned}\hat{U}_B|+x\rangle|\varepsilon\rangle_B &= \frac{1}{\sqrt{2}}\left(|0\rangle|\varepsilon_0\rangle_B + |1\rangle|\varepsilon_1\rangle_B\right.\\ &\quad \left.+|0\rangle|\varepsilon_0'\rangle_B + |1\rangle|\varepsilon_1'\rangle_B\right)\\ &= \frac{1}{2}\left[|+x\rangle\left(|\varepsilon_0\rangle_B + |\varepsilon_1\rangle_B + |\varepsilon_0'\rangle_B + |\varepsilon_1'\rangle_B\right)\right.\\ &\quad \left.+|-x\rangle\left(|\varepsilon_0\rangle_B - |\varepsilon_1\rangle_B + |\varepsilon_0'\rangle_B - |\varepsilon_1'\rangle_B\right)\right],\end{aligned} \tag{10}$$

$$\begin{aligned}\hat{U}_B|-x\rangle|\varepsilon\rangle_B &= \frac{1}{\sqrt{2}}\left(|0\rangle|\varepsilon_0\rangle_B + |1\rangle|\varepsilon_1\rangle_B\right.\\ &\quad \left.-|0\rangle|\varepsilon_0'\rangle_B - |1\rangle|\varepsilon_1'\rangle_B\right)\\ &= \frac{1}{2}\left[|+x\rangle\left(|\varepsilon_0\rangle_B + |\varepsilon_1\rangle_B - |\varepsilon_0'\rangle_B - |\varepsilon_1'\rangle_B\right)\right.\end{aligned}$$

$$+\left|-x\right\rangle\left(\left|\varepsilon_0\right\rangle_B-\left|\varepsilon_1\right\rangle_B-\left|\varepsilon_0'\right\rangle_B+\left|\varepsilon_1'\right\rangle_B\right)\Big], \tag{11}$$

where $\left|\varepsilon\right\rangle_B$ is the initial state of Bob's ancilla and $\left\{\left|\varepsilon_0\right\rangle,\left|\varepsilon_1\right\rangle,\left|\varepsilon_0'\right\rangle,\left|\varepsilon_1'\right\rangle\right\}$ are the pure ancilla's states determined uniquely by the unitary operation $\hat{U}_B$. Therefore, $\left|\varepsilon_0\right\rangle,\left|\varepsilon_1\right\rangle,\left|\varepsilon_0'\right\rangle,\left|\varepsilon_1'\right\rangle$ must satisfy the relationship $\hat{U}_B\hat{U}_B^+ = I$, i.e.

$$\begin{aligned}&\left\langle\varepsilon_0\middle|\varepsilon_0\right\rangle+\left\langle\varepsilon_1\middle|\varepsilon_1\right\rangle=1,\ \left\langle\varepsilon_0'\middle|\varepsilon_0'\right\rangle+\left\langle\varepsilon_1'\middle|\varepsilon_1'\right\rangle=1,\\&\left\langle\varepsilon_1\middle|\varepsilon_0\right\rangle+\left\langle\varepsilon_1'\middle|\varepsilon_0'\right\rangle=0,\ \left\langle\varepsilon_0\middle|\varepsilon_1\right\rangle+\left\langle\varepsilon_0'\middle|\varepsilon_1'\right\rangle=0.\end{aligned} \tag{12}$$

Given eqs. (8)–(11), we can see that the action of Bob's eavesdropping will introduce an error rate for every decoy particle at the stage of the honest check.

$$P_B^0=\left\langle\varepsilon_1\middle|\varepsilon_1\right\rangle=1-\left\langle\varepsilon_0\middle|\varepsilon_0\right\rangle, \tag{13}$$

$$P_B^1=\left\langle\varepsilon_0'\middle|\varepsilon_0'\right\rangle=1-\left\langle\varepsilon_1'\middle|\varepsilon_1'\right\rangle, \tag{14}$$

$$P_B^+=\frac{1}{2}\left(1+\left\langle\varepsilon_0\middle|\varepsilon_0'\right\rangle+\left\langle\varepsilon_1\middle|\varepsilon_1'\right\rangle-\left\langle\varepsilon_0\middle|\varepsilon_1'\right\rangle-\left\langle\varepsilon_1\middle|\varepsilon_0'\right\rangle\right), \tag{15}$$

$$P_B^-=\frac{1}{2}\left(1-\left\langle\varepsilon_0\middle|\varepsilon_0'\right\rangle-\left\langle\varepsilon_1\middle|\varepsilon_1'\right\rangle-\left\langle\varepsilon_0\middle|\varepsilon_1'\right\rangle-\left\langle\varepsilon_1\middle|\varepsilon_0'\right\rangle\right). \tag{16}$$

If Bob tries to achieve the eavesdropping without being detected in the stage of the honest check, the error rates P_B^0,P_B^1,P_B^+,P_B^- have to equal 0 in the ideal environment. Then, the states of the ancilla must satisfy the following equation.

$$\begin{aligned}&\left\langle\varepsilon_1\middle|\varepsilon_1\right\rangle=\left\langle\varepsilon_0'\middle|\varepsilon_0'\right\rangle=0,\\&\left\langle\varepsilon_0\middle|\varepsilon_0\right\rangle=\left\langle\varepsilon_1'\middle|\varepsilon_1'\right\rangle=1,\\&\left\langle\varepsilon_0\middle|\varepsilon_1'\right\rangle=1.\end{aligned} \tag{17}$$

Therefore, in this three-party case, the whole quantum systems shown in eq. (5) should be rewritten with the effect of Bob's eavesdropping below.

$$\begin{aligned}&\left|\varphi^-\right\rangle_{12}\otimes\hat{U}_B\left|\psi^+\right\rangle_{34}\left|\varepsilon\right\rangle_B\otimes\hat{U}_B\left|\psi^-\right\rangle_{56}\left|\varepsilon\right\rangle_B=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right)_{12}\\&\otimes\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_3\hat{U}_B\left|1\right\rangle_4\left|\varepsilon\right\rangle_B+\left|1\right\rangle_3\hat{U}_B\left|0\right\rangle_4\left|\varepsilon\right\rangle_B\right)\\&\otimes\frac{1}{\sqrt{2}}\left(\hat{U}_B\left|0\right\rangle_5\left|\varepsilon\right\rangle_B\left|1\right\rangle_6-\hat{U}_B\left|1\right\rangle_5\left|\varepsilon\right\rangle_B\left|0\right\rangle_6\right)\\&=\frac{1}{2\sqrt{2}}\left(\left|01\right\rangle_{16}\left|00\right\rangle_{23}\left|10\right\rangle_{45}\left|\varepsilon_1'\varepsilon_0\right\rangle_{BB}\right.\\&-\left|00\right\rangle_{16}\left|00\right\rangle_{23}\left|11\right\rangle_{45}\left|\varepsilon_1'\varepsilon_1'\right\rangle_{BB}+\left|01\right\rangle_{16}\left|01\right\rangle_{23}\left|00\right\rangle_{45}\left|\varepsilon_0\varepsilon_0\right\rangle_{BB}\\&-\left|00\right\rangle_{16}\left|01\right\rangle_{23}\left|01\right\rangle_{45}\left|\varepsilon_0\varepsilon_1'\right\rangle_{BB}-\left|11\right\rangle_{16}\left|10\right\rangle_{23}\left|10\right\rangle_{45}\left|\varepsilon_1'\varepsilon_0\right\rangle_{BB}\\&\left.+\left|10\right\rangle_{16}\left|10\right\rangle_{23}\left|11\right\rangle_{45}\left|\varepsilon_1'\varepsilon_1'\right\rangle_{BB}-\left|11\right\rangle_{16}\left|11\right\rangle_{23}\left|00\right\rangle_{45}\left|\varepsilon_0\varepsilon_0\right\rangle_{BB}\right)\\&=\frac{1}{2\sqrt{2}}\left(\left|01\right\rangle_{16}\left|00\right\rangle_{23}\left|10\right\rangle_{45}\left|\varepsilon_1'\varepsilon_0\right\rangle_{BB}\right.\\&-\left|00\right\rangle_{16}\left|00\right\rangle_{23}\left|11\right\rangle_{45}\left|\varepsilon_1'\varepsilon_1'\right\rangle_{BB}+\left|01\right\rangle_{16}\left|01\right\rangle_{23}\left|00\right\rangle_{45}\left|\varepsilon_0\varepsilon_0\right\rangle_{BB}\\&-\left|00\right\rangle_{16}\left|01\right\rangle_{23}\left|01\right\rangle_{45}\left|\varepsilon_0\varepsilon_1'\right\rangle_{BB}-\left|11\right\rangle_{16}\left|10\right\rangle_{23}\left|10\right\rangle_{45}\left|\varepsilon_1'\varepsilon_0\right\rangle_{BB}\\&\left.+\left|10\right\rangle_{16}\left|10\right\rangle_{23}\left|11\right\rangle_{45}\left|\varepsilon_1'\varepsilon_1'\right\rangle_{BB}-\left|11\right\rangle_{16}\left|11\right\rangle_{23}\left|00\right\rangle_{45}\left|\varepsilon_0\varepsilon_0\right\rangle_{BB}\right)\\&=\frac{1}{8}\left(\left(\left|\psi^+\right\rangle+\left|\psi^-\right\rangle\right)_{16}\left(\left|\phi^+\right\rangle+\left|\phi^-\right\rangle\right)_{23}\left(\left|\psi^+\right\rangle-\left|\psi^-\right\rangle\right)_{45}\left|\varepsilon_1'\varepsilon_0\right\rangle_{BB}\right.\\&-\left(\left|\phi^+\right\rangle+\left|\phi^-\right\rangle\right)_{16}\left(\left|\phi^+\right\rangle+\left|\phi^-\right\rangle\right)_{23}\left(\left|\phi^+\right\rangle-\left|\phi^-\right\rangle\right)_{45}\left|\varepsilon_1'\varepsilon_1'\right\rangle_{BB}\\&+\left(\left|\psi^+\right\rangle+\left|\psi^-\right\rangle\right)_{16}\left(\left|\psi^+\right\rangle+\left|\psi^-\right\rangle\right)_{23}\left(\left|\phi^+\right\rangle+\left|\phi^-\right\rangle\right)_{45}\left|\varepsilon_0\varepsilon_0\right\rangle_{BB}\\&-\left(\left|\phi^+\right\rangle+\left|\phi^-\right\rangle\right)_{16}\left(\left|\psi^+\right\rangle+\left|\psi^-\right\rangle\right)_{23}\left(\left|\psi^+\right\rangle+\left|\psi^-\right\rangle\right)_{45}\left|\varepsilon_0\varepsilon_1'\right\rangle_{BB}\\&-\left(\left|\phi^+\right\rangle-\left|\phi^-\right\rangle\right)_{16}\left(\left|\psi^+\right\rangle-\left|\psi^-\right\rangle\right)_{23}\left(\left|\psi^+\right\rangle-\left|\psi^-\right\rangle\right)_{45}\left|\varepsilon_1'\varepsilon_0\right\rangle_{BB}\\&+\left(\left|\psi^+\right\rangle-\left|\psi^-\right\rangle\right)_{16}\left(\left|\psi^+\right\rangle-\left|\psi^-\right\rangle\right)_{23}\left(\left|\phi^+\right\rangle-\left|\phi^-\right\rangle\right)_{45}\left|\varepsilon_1'\varepsilon_1'\right\rangle_{BB}\\&-\left(\left|\phi^+\right\rangle-\left|\phi^-\right\rangle\right)_{16}\left(\left|\phi^+\right\rangle-\left|\phi^-\right\rangle\right)_{23}\left(\left|\phi^+\right\rangle+\left|\phi^-\right\rangle\right)_{45}\left|\varepsilon_0\varepsilon_0\right\rangle_{BB}\\&\left.+\left(\left|\psi^+\right\rangle-\left|\psi^-\right\rangle\right)_{16}\left(\left|\phi^+\right\rangle-\left|\phi^-\right\rangle\right)_{23}\left(\left|\psi^+\right\rangle+\left|\psi^-\right\rangle\right)_{45}\left|\varepsilon_0\varepsilon_1'\right\rangle_{BB}\right).\end{aligned} \tag{18}$$

Given eq. (18), if Bob can distinguish between $\left\{\left|\varepsilon_0\varepsilon_0\right\rangle_{BB},\ \left|\varepsilon_1'\varepsilon_1'\right\rangle_{BB}\right\}$ and $\left\{\left|\varepsilon_0\varepsilon_1'\right\rangle_{BB},\ \left|\varepsilon_1'\varepsilon_0\right\rangle_{BB}\right\}$, he can deduce that Alice's measurement result is $\left|\phi^\pm\right\rangle$ or $\left|\psi^\pm\right\rangle$ with his measurement result. That is, he can secretly get the partial information about the secret (i.e. it is {00, 01} or {10, 11}). However, according to eq. (17), the elements in $\left\{\left|\varepsilon_0\varepsilon_0\right\rangle_{BB},\ \left|\varepsilon_0\varepsilon_1'\right\rangle_{BB},\ \left|\varepsilon_1'\varepsilon_0\right\rangle_{BB},\ \left|\varepsilon_1'\varepsilon_1'\right\rangle_{BB}\right\}$ are pairwise non-orthogonal.

$$\begin{aligned}&\left\langle\varepsilon_0\varepsilon_0\middle|\varepsilon_0\varepsilon_1'\right\rangle=\left\langle\varepsilon_0\middle|\varepsilon_0\right\rangle\left\langle\varepsilon_0\middle|\varepsilon_1'\right\rangle=1,\\&\left\langle\varepsilon_0\varepsilon_0\middle|\varepsilon_1'\varepsilon_0\right\rangle=\left\langle\varepsilon_0\middle|\varepsilon_1'\right\rangle\left\langle\varepsilon_0\middle|\varepsilon_0\right\rangle=1,\\&\left\langle\varepsilon_1'\varepsilon_1'\middle|\varepsilon_0\varepsilon_1'\right\rangle=\left\langle\varepsilon_1'\middle|\varepsilon_0\right\rangle\left\langle\varepsilon_1'\middle|\varepsilon_1'\right\rangle=1,\\&\left\langle\varepsilon_1'\varepsilon_1'\middle|\varepsilon_1'\varepsilon_0\right\rangle=\left\langle\varepsilon_1'\middle|\varepsilon_1'\right\rangle\left\langle\varepsilon_1'\middle|\varepsilon_0\right\rangle=1.\end{aligned} \tag{19}$$

So, it is impossible for Bob to distinguish the elements in $\left\{\left|\varepsilon_0\varepsilon_0\right\rangle_{BB},\ \left|\varepsilon_0\varepsilon_1'\right\rangle_{BB},\ \left|\varepsilon_1'\varepsilon_0\right\rangle_{BB},\ \left|\varepsilon_1'\varepsilon_1'\right\rangle_{BB}\right\}$ and thus he can't obtain any information about the shared secret.

4.3 The security of the scheme against the collusion attack

In real life there may be two or more dishonest members, and they can collude to perform an attack (i.e. the collusion attack). Obviously, the two members B_1 and B_n in Group 2 are most likely to perform the collusion attack, as shown in Figure 3. For simplicity, we only consider the special case of $N=1$. Their attack works as follows: in step (5), B_1 and B_n do not perform the Bell-state measurements on their two-particle pair (b_{11},b_{12}) and (b_{n1},b_{n2}) respectively as they should. In reverse, they respectively measure the other two-particle pair (b_{11},b_{n2}) and (b_{12},b_{n1}) with Bell basis after exchanging two particles b_{12} and b_{n2}.

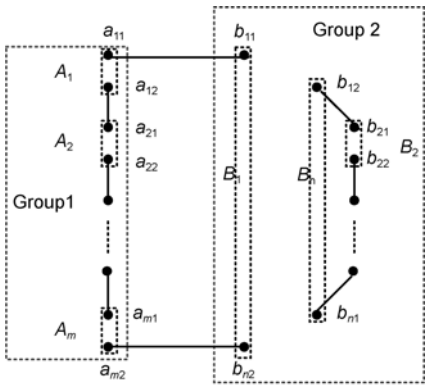

Figure 3 The collusion attack of two dishonest members B_1 and B_n. The two particles linked with the bold lines are in Bell states. The panes with the dashed lines represent the Bell-state measurements.

Here, $k_{B_1}^*$ and $k_{B_n}^*$ respectively denote the codes of measured results of (b_{11}, b_{n2}) and (b_{12}, b_{n1}). Then there exist the following equations by eq. (7):

$$k_{A_1} \oplus k_{A_2} \oplus ... \oplus k_{A_m} \oplus k_{B_1}^* = R_{b_{11}a_{11}} \oplus R_{a_{12}a_{21}} \oplus ... \oplus R_{a_{m2}b_{n2}}, \quad (20)$$

$$\begin{aligned} & k \oplus k_{B_1}^* = R_{b_{11}a_{11}} \oplus R_{a_{12}a_{21}} \oplus ... \oplus R_{a_{m2}b_{n2}} \\ & (\text{as } k = k_{A_1} \oplus k_{A_2} \oplus ... \oplus k_{A_m}), \end{aligned} \quad (21)$$

$$(k_{B_2} \oplus k_{B_3} \oplus ... k_{B_{n-1}}) \oplus k_{B_n}^* = R_{b_{n1}b_{(n-1)2}} \oplus ... \oplus R_{b_{21}b_{12}}, \quad (22)$$

$$\begin{aligned} & (k \oplus k_{B_1}^*) \oplus ((k_{B_2} \oplus k_{B_3} \oplus ... k_{B_{n-1}}) \oplus k_{B_n}^*) \\ & = (R_{b_{11}a_{11}} \oplus R_{a_{12}a_{21}} \oplus ... \oplus R_{a_{m2}b_{n2}}) \oplus (R_{b_{n1}b_{(n-1)2}} \oplus ... \oplus R_{b_{21}b_{12}}), \end{aligned} \quad (23)$$

$$k \oplus k_{B_1}^* \oplus k_{B_2} \oplus k_{B_3} \oplus ... k_{B_{n-1}} \oplus k_{B_n}^* = 00, \quad (24)$$

$$k = (k_{B_1}^* \oplus k_{B_n}^*) \oplus (k_{B_2} \oplus k_{B_3} \oplus ... k_{B_{n-1}}). \quad (25)$$

Since $k_{B_2} \oplus k_{B_3} \oplus ... k_{B_{n-1}}$ is not known to two members B_1 and B_n, they do not obtain any information about the secret key k from eq. (25). That is, our scheme is secure against the collusion attack of two dishonest members B_1 and B_n. In fact, it is still secure even if more dishonest members perform the collusion attack (as long as there is an honest member in Group 1 and Group 2, respectively), because the original states of the quantum resources in our system are not public.

5 Conclusion

We have presented a way for quantum secret sharing between *m*-party and *n*-party with Bell states and Bell measurements and analyzed its security. In this scheme, the efficiency for qubits $\eta_q = q_u / q_t$ approaches the maximal value 100% as almost all the EPR pairs are useful for carrying the message in principle, and here q_u is the useful qubits and q_t is the total qubits transmitted. The total efficiency η_t in this scheme also approaches 100% as the classical information exchanged is not necessary except for the eavesdropping checks.

Compared with the previous schemes, our scheme has the following advantages.

1) Since all Bell states are generated by the trusted third party, the members are not required to prepare entangled states or perform any local unitary operation.

2) By using only Bell measurements, all members can found and recover the shared secret key when they collaborate.

3) No classical bit needs to be exchanged except for the eavesdropping checks, i.e., the total efficiency of the scheme approaches 100%.

The implementation of this scheme only needs exploiting EPR pairs and Bell state measurements. With the present techniques, the EPR pairs may be one of the optimal entangled quantum resources for quantum secret sharing. We can deduce that this scheme is feasible.

This work was supported by the Major Research Plan of the National Natural Science Foundation of China (Grant No. 90818005), the National Natural Science Foundation of China (Grant Nos. 60903217, 60773032 and 60773114), and the Ph.D. Program Foundation of Ministry of Education of China (Grant No. 20060358014).

1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India. New York: IEEE, 1984. 175–179
2 Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chin Sci Bull, 2009, 54(17): 2991–2997
3 Li C Z. Real applications of quantum communications in China. Chin Sci Bull, 2009, 54(17): 2976–2977
4 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59(3): 1829–1834
5 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69: 052307
6 Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59(1): 162–168
7 Gottesman D. Theory of quantum secret sharing. Phys Rev A, 2000, 61: 042311
8 Hideki I, Jörn M Q, Anderson C A N, et al. A quantum information theoretical model for quantum secret sharing schemes. arXiv: quant-ph/0311136v1
9 Sudhir K S, Srikanth R. Generalized quantum secret sharing. Phys Rev A, 2005, 71: 012328
10 Tittel W, Zbinden H, Gisin N. Experimental demonstration of quantum secret sharing. Phys Rev A, 2001, 63: 042301
11 Lance A M, Symul T, Bowen W P, et al. Tripartite quantum state sharing. Phys Rev Lett, 2004, 92: 177903
12 Hsu L Y. Quantum secret-sharing protocol based on Grover's algorithm. Phys Rev A, 2003, 68: 022306
13 Deng F G, Zhou H Y, Long G L. Bidirectional quantum secret sharing and secret splitting with polarized single photons. Phys Lett A, 2005, 337(4-6): 329–334

14 Deng F G, Long G L, Zhou H Y. An efficient quantum secret sharing scheme with Einstein-Podolsky-Rosen pairs. Phys Lett A, 2005, 340(1-4): 43–50
15 Zhang Z J. Multiparty quantum secret sharing of secure direct communication. Phys Lett A, 2005, 342(1,2): 60–66
16 Zhang Z J, Man Z X. Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys Rev A, 2005, 72: 022303
17 Zhang Z J, Li Y, Man Z X. Multiparty quantum secret sharing. Phys Rev A, 2005, 71: 044301
18 Deng F G, Li X H, Zhou H Y. Efficient high-capacity quantum secret sharing with two-photon entanglement. Phys Lett A, 2008, 372(12): 1957–1962
19 Wang T Y, Wen Q Y, Chen X B, et al. An efficient and secure multiparty quantum secret sharing scheme based on single photons. Opt Commun, 2008, 281(24): 6130–6134
20 Sun Y, Wen Q Y, Gao F, et al. Multiparty quantum secret sharing based on Bell measurement. Opt Commun, 2009, 282(17): 3647–3651
21 Gao G. Reexamining the security of the improved quantum secret sharing scheme. Opt Commun, 2009, 282(22): 4464–4466
22 Zhang X L, Ji D Y. Analysis of a kind of quantum cryptographic schemes based on secret sharing. Sci China Ser G-Phy Mech Astron, 2009, 52(9): 1313–1316
23 Hao L, Li J L, Long G L. Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution. Sci China-Phy Mech Astron, 2010, 53(3): 491–495
24 Yan F L, Gao T. Quantum secret sharing between multiparty and multiparty without entanglement. Phys Rev A, 2005, 72: 012304
25 Li C M, Chang C C, Hwang T. Comment on quantum secret sharing between multiparty and multiparty without entanglement. Phys Rev A, 2006, 73: 016301
26 Han L F, Liu Y M, Shi S H, et al. Improving the security of a quantum secret sharing between multiparty and multiparty without entanglement. Phys Lett A, 2007, 361(1,2): 24–28
27 Yan F L, Gao T, Li Y C. Quantum secret sharing between multiparty and multiparty with four states. Sci China Ser G-Phys Mech Astron, 2007, 50(5): 572–580
28 Gao T, Yan F L, Li Y C. Quantum secret sharing between m-party and n-party with six states. Sci China Ser G-Phys Mech Astron, 2009, 52(8): 1191–1202
29 Bandyopadhyay S. Teleportation and secret sharing with pure entangled states. Phys Rev A, 2000, 62: 012308
30 Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys Rev Lett, 1999, 83(3): 648–651
31 Li Y M, Zhang K S, Peng K C. Multiparty secret sharing of quantum information based on entanglement swapping. Phys Lett A, 2004, 324(5,6): 420–424
32 Zhang Z J, Yang J, Man Z X, et al. Multiparty secret sharing of quantum information using and identifying Bell states. Eur Phys J D, 2005, 33(1): 133–136
33 Deng F G, Li C Y, Li Y S, et al. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys Rev A, 2005, 72: 022338
34 Deng F G, Li X H, Li C Y, et al. Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs. Phys Rev A, 2005, 72: 044301
35 Deng F G, Li X H, Li C Y, et al. Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements. Eur Phys J D, 2006, 39(3): 459–464
36 Li X H, Zhou P, Li C Y, et al. Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J Phys B-At Mol Opt Phys, 2006, 39(8): 1975–1983
37 Wang Y H, Song H S. Preparation of multi-atom specially entangled W-class state and splitting quantum information. Chin Sci Bull, 2009, 54(15): 2599–2605
38 Zhang W, Liu Y M, Yin X F, et al. Partition of arbitrary single-qubit information among n recipients via asymmetric $(n+1)$-qubit W state. Sci China Ser G-Phy Mech Astron, 2009, 52(10): 1611–1617
39 Zuo X Q, Liu Y M, Zhang W, et al. Simpler criterion on W state for perfect quantum state splitting and quantum teleportation. Sci China Ser G-Phy Mech Astron, 2009, 52(12): 1906–1912
40 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302