Multiparty quantum secret sharing of classical and quantum messages*

CHEN Pan[1], DENG Fuguo[2,3] and LONG Guilu[1,4**]

(1. Key Laboratory for Quantum Information and Measurements, and Department of Physics, Tsinghua University, Beijing 100084, China; 2. Key Laboratory of Beam Technology and Material Modification, MOE, Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, China; 3. Beijing Radiation Center, Beijing 100875, China; 4. Key Laboratory for Atomic and Molecular Nano-Sciences, Tsinghua University, Beijing 100084, China)

Accepted on June 8, 2006

Abstract A scheme for multiparty quantum secret sharing of classical and quantum messages is proposed by using entanglement swapping. This scheme can distribute not only the classical information but also the quantum information between N agents. The security of our scheme is also confirmed.

Keywords: quantum secret sharing, classical message, quantum message, EPR pair.

Suppose that the boss Alice wants to share a secret key with her some remote agents, and there may be one agent dishonest. She does not know who the dishonest man is, but Alice believes that the honest agents can prevent the dishonest man from stealing the secret information and doing harm to her belongings. For this goal, Blakley[1] and Shamir[2] independently proposed an original scheme for secret sharing in 1979. In their schemes, the secret key is divided into n pieces and distributed to n agents Bob_i ($i = 1, 2, \cdots, n$). Only when all the n agents cooperate can they reconstruct Alice's secret key $K_A = K_{B_1} \oplus K_{B_2} \oplus \cdots \oplus K_{B_n}$. Here K_{B_i} is the key obtained by the agent Bob_i. Because a classical signal can be copied fully and freely by a vicious eavesdropper, say Eve, it is difficult for the parties to create the key K_A securely only with the classical physics.

The quantum secret sharing (QSS) is the quantum counterpart of the classical secret sharing, and becomes an important branch of quantum communication. In 1999, Hillery et al.[3] proposed the first QSS scheme with a Greenberger-Horne-Zeilinger (GHZ) state, called HBB99 scheme. Up to now, many studies have been focused on QSS[3—23], including those for sharing an unknown quantum state[24—27]. Recently, Zhang and Man[22] introduced a multiparty quantum secret sharing (MQSS) protocol of classical messages by using entanglement swapping with Bell states. In their protocol, the boss Alice prepares three Einstein-Podolsky-Rosen (EPR) pairs and uses four local unitary operations to encode the secret messages on one of the three EPR pairs. She sends the two particles in two EPR pairs to her two agents, Bob and Charlie, respectively, and keeps the other two particles. Moreover, Alice should set up an entangled quantum channel for Bob and Charlie with an EPR pair. By performing a local unitary operation on one particle in her hand, Alice encodes her classical message in the quantum states and distributes it to her two agents with entanglement swapping by means that Alice takes a Bell-basis measurement on her two particles kept. Each of the two agents can get the secret key K_A when the other agent works together with him and each performs a Bell-basis measurements on his two particles.

In this paper, we will present a multiparty quantum secret sharing (MQSS) protocol with EPR pairs. This MQSS scheme has the advantage of using less physical resources.

1 MQSS scheme with two agents

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

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \qquad (1)$$

* Supported by the Major State Basic Research Development Program of China (Grant No. 001CB309308), National Natural Science Foundation of China (Grant Nos. 60433050, 10325521), and the Hang-Tian Science Fund, the SRFDP Program of Education Ministry of China

** To whom correspondence should be addressed. E-mail: gllong@mail.tsinghua.edu.cn

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \quad (2)$$

where $|0\rangle$ and $|1\rangle$ are the two eigenvectors of the measuring basis σ_z (for instance, the polarization of a single photon along the z-direction). We can transfer each of the four Bell states into another one by operating one particle in each EPR pair:

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

These four operations can represent two bits of classical information 00, 01, 10 and 11, respectively, in quantum communication.

For simplification, we first consider the case with two agents, say Bob and Charlie. Our MQSS scheme works with the following steps:

① Alice prepares two sequences of EPR pairs, say S_1 and S_2. Each sequence is composed of N ordered EPR photon pairs in the same quantum state, say $|\Psi^-\rangle$. We denote the N ordered EPR pairs by $[(P_1(C), P_1(M)), (P_2(C), P_2(M)), (P_3(C), P_3(M)), \cdots, (P_N(C), P_N(M))]$. Alice takes one photon from each EPR pair to form an ordered EPR parter photon sequence, say $[P_1(C), P_2(C), P_3(C), \cdots, P_N(C)]$, which is called the checking sequence (S_C sequence). The remaining photons compose another sequence $[P_1(M), P_2(M), P_3(M), \cdots, P_N(M)]$, called the message-coding sequence (S_M sequence), being the same as that in Refs. [28, 29].

② Alice sends the two checking sequences, say S_{C1} and S_{C2} to her two agents Bob and Charlie, respectively, and always keeps the two corresponding message-coding sequences, S_{M1} and S_{M2}.

③ After the two agents received their sequences, Alice chooses a subset of EPR pairs as the samples for checking eavesdropping from each EPR-pair sequence. Alice can complete the process for eavesdropping check with each agent with the method introduced in Refs. [28, 29]. That is, Alice first picks out the positions where the photons will be used to check eavesdropping. She tells her agents which photons are to be measured with one of the two MBs, σ_z or σ_x. After the measurements are done by the agents, Alice performs the corresponding measurements on her sample photons. They analyze the error rate of the samples by comparing their results in public.

If the error rate is by far lower than the threshold value ε_t, the parties continue their quantum communication to the next step; otherwise, they will abort the whole transmission.

④ Alice encodes her message K_A on the photons in the sequence S_{M1} with one of the four local unitary operations U_i ($i = 0, 1, 2, 3$). Then she performs a Bell-basis measurement on every pair of photons composed of $P_j(M1)$ and $P_j(M2)$, which come from the two message-coding sequences S_{M1} and S_{M2}. Here $j = 1, 2, \cdots, N$. Alice publishes her outcomes of the measurement for each pair.

⑤ If Bob and Charlie collaborate after receiving Alice's information, they can perform a Bell measurement on the two corresponding photons $P_j(M1)$ and $P_j(M2)$ which come from the two checking sequences of S_{M1} and S_{M2}, respectively. Otherwise, neither of them can obtain the key K_A.

For example, if the local unitary operation chosen by Alice in step (4) is U_3, then the state of the photons $P_j(M1)$ and $P_j(C1)$ would be transferred into the state $|\Phi^+\rangle_{M1C1}$, i.e. $U_3|\Psi^-\rangle_{M1C1} = |\Phi^+\rangle_{M1C1}$. After the local unitary operation, the state of the photons $P_j(C1)$, $P_j(M1)$, $P_j(C2)$ and $P_j(M2)$ can be written as:

$$\begin{aligned} & U_3|\Psi^-\rangle_{M1C1} \oplus |\Psi^-\rangle_{M2C2} \\ &= |\Phi^+\rangle_{M1C1} \otimes |\Psi^-\rangle_{M2C2} \\ &= \frac{1}{2}(|\Phi^-\rangle_{M1M2}|\Psi^+\rangle_{C1C2} \\ &\quad - |\Psi^+\rangle_{M1M2}|\Phi^-\rangle_{C1C2} \\ &\quad - |\Psi^-\rangle_{M1M2}|\Phi^+\rangle_{C1C2} \\ &\quad + |\Phi^+\rangle_{M1M2}|\Psi^-\rangle_{C1C2}). \end{aligned} \quad (4)$$

When Alice performs a Bell-basis measurement on photons $P_j(M1)$ and $P_j(M2)$, the state of the photons $P_j(C1)$ and $P_j(C2)$ will collapse to a corresponding state. Supposed Alice's outcome is $|\Phi^+\rangle_{M1M2}$, then the two corresponding photons $P_j(C1)$ and $P_j(C2)$ controlled by Bob and Charlie, respectively, should be in the state $|\Psi^-\rangle_{C1C2}$ according to Eq. (4). That is, Bob and Charlie can deduce that the local unitary operation chosen by Alice is U_3

and the two-bit classical information distributed is 11.

Different from the Zhang-Man protocol[22], it is unnecessary for the boss Alice to set up another quantum channel for the two agents. The agents can read out the message encoded by Alice if and only if they work together and measure their photons. In this scheme, Alice can prevent a dishonest man from stealing the information by using check mode, the same as the two-step protocol[28,29]. So it is also secure against other quantum techniques. Because almost all the entangled states are useful for quantum communication, the intrinsic efficiency for qubits $\eta_q \equiv \frac{q_u}{q_t}$ approaches 100%, the same as that in Refs. [28—31]. Here q_u and q_t are the useful qubits and the total qubits transmitted, respectively. The total efficiency η_t in this scheme approaches 50% as two bits of classical information are exchanged for two qubits. η is defined as[32,33]

$$\eta_t = \frac{q_u}{q_t + b_t}, \tag{5}$$

where b_t is the classical bits exchanged between the parties in the quantum communication. Even though the total efficiency η_t is lower than that in Refs. [17, 18], it is unnecessary for the photons to run forth and back from Alice to her agents.

2 MQSS scheme with N agents

We use $N = 3$ as an example to describe the principle of our MQSS scheme with N agents.

Firstly, we introduce a complete orthonormal basis of the combined Hilbert space of the three particles as follows:

$$\begin{aligned}
|\Omega^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle) \\
|\Pi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle) \\
|K^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle) \\
|\Gamma^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle).
\end{aligned} \tag{6}$$

We give the specific steps of the QSDC protocol as follows:

① Alice creates a string A of $3N$ random classical bits and divides this string into groups of three bits.

Then she prepares three sequences of EPR pairs, say S_1, S_2 and S_3. Each sequence is composed of N ordered EPR photon pairs in state $|\Psi^-\rangle$. Similar to Section 1, we also denote the N ordered EPR pairs with $[(P_1(C), P_1(M)), (P_2(C), P_2(M)), (P_3(C), P_3(M)), \cdots, (P_N(C), P_N(M))]$ and form three checking sequence S_{C1}, S_{C2}, S_{C3}, and three messagecoding sequence S_{M1}, S_{M2}, S_{M3}.

② Alice sends S_{C1}, S_{C2} and S_{C3} to her three agents, Bob_1, Bob_2 and Charlie, respectively, and keeps the three message-coding sequence S_{M1}, S_{M2}, S_{M3}.

③ After all the agents receive their sequences, Alice preforms the security checking with the same method in step(3) of Section 1. If the transmission is secure, she will continue to the next step.

④ Alice discards the photons which has been chosen for security checking and picks out three photons $P_j(M1)$, $P_j(M2)$ and $P_j(M3)$ from the three message-coding sequences S_{M1}, S_{M2} and S_{M3}, respectively. Then, according to the corresponding group A_j in the string A, Alice encodes her message K_A on the three particles. For example, if $A_j = 010$, then Alice performs a local unitary operation $U_i (i = 0, 1, 2, 3)$ which is previously selected by Alice and her agents on the photon $P_j(M2)$; if $A_j = 101$, then Alice performs a local unitary operation U_i on the photons $P_j(M1)$ and $P_j(M3)$, etc. Here, $j = 1, 2, \cdots, N$.

After doing that, Alice performs a three-particle GHZ state joint measurement on $P_j(M1)$, $P_j(M2)$ and $P_j(M3)$ and publishes her measurement outcomes.

⑤ If Bob_1, Bob_2 and Charlie collaborate, they can perform a three-particle GHZ state joint measurement on the three corresponding photons $P_j(C1)$, $P_j(C2)$ and $P_j(C3)$ which come from the three checking sequences S_{C1}, S_{C2} and S_{C3}, respectively. According to their measurement outcomes, they can get Alice's message K_A. Otherwise, none of them can obtain the key K_A.

For example, if Alice chose the local unitary operation U_3 in step ④, and the corresponding group $A_j = 010$, then the state of the photons $P_j(M2)$ and

$P_j(C2)$ would be transferred into the state $|\Phi^+\rangle_{M2C2}$.

After the local unitary operation, the state of the photons $P_j(C1)$, $P_j(M1)$, $P_j(C2)$, $P_j(M2)$, $P_j(C3)$ and $P_j(M3)$ can be written as:

$$\begin{aligned}
&|\Psi^-\rangle_{C1M1}\otimes(U_3|\Psi^-\rangle_{C2M2})\otimes|\Psi^-\rangle_{C3M3}\\
&=|\Psi^-\rangle_{C1M1}\otimes|\Phi^+\rangle_{C2M2}\otimes|\Psi^-\rangle_{C3M3}\\
&=\frac{1}{\sqrt{8}}(|K^+\rangle_{C1C2C3}|\Pi^+\rangle_{M1M2M3}\\
&\quad+|K^-\rangle_{C1C2C3}|\Pi^-\rangle_{M1M2M3})\\
&\quad-(|\Pi^+\rangle_{C1C2C3}|\Omega^+\rangle_{M1M2M3}\\
&\quad+|\Omega^-\rangle_{C1C2C3}|K^-\rangle_{M1M2M3})\\
&\quad-(|K^+\rangle_{C1C2C3}|\Pi^+\rangle_{M1M2M3}\\
&\quad+|K^-\rangle_{C1C2C3}|\Pi^-\rangle_{M1M2M3})\\
&\quad+(|\Gamma^+\rangle_{C1C2C3}|\Omega^+\rangle_{M1M2M3}\\
&\quad+|\Gamma^-\rangle_{C1C2C3}|\Omega^-\rangle_{M1M2M3}).
\end{aligned}\tag{7}$$

When Alice performs a three-particle GHZ state joint measurement on photons $P_j(M1)$, $P_j(M2)$ and $P_j(M3)$, the state of the photons $P_j(C1)$, $P_j(C2)$ and $P_j(C3)$ will collapse to a corresponding state. Supposed Alice's outcome is $|\Gamma^-\rangle_{M1M2M3}$, then the three corresponding photons $P_j(C1)$, $P_j(C2)$ and $P_j(C3)$ controlled by Bob_1, Bob_2 and Charlie, respectively, should be in the state $|\Omega^-\rangle_{C1C2C3}$ according to Eq. (7). That is, Bob_1, Bob_2 and Charlie can deduce that the three-bit classical information distributed by Alice is 010.

It is easily to generalize this MQSS scheme to arbitrary multiparty case.

Assume that there are N agents, Bob_i ($i=1,2,\cdots,N-1$) and Charlie, and Alice wants to distribute her secret information among the N agents. Then, Alice creates a string A of N^2 random classical bits and divides this string into groups of N bits. She prepares N sequences of EPR pairs $S_1, S_2, \cdots, S_N$. Each EPR photon pair is in state $|\Psi^-\rangle$. Alice sends S_{C1}, $S_{C2}, \cdots, S_{CN}$ to her N agents and keeps the N message-coding sequence $S_{M1}, S_{M2}, \cdots, S_{MN}$.

After all the agents received their sequences, Alice performs the security checking with the same method as in step ③ of Section 1. If the transmission is secure, they will continue to the next step.

Alice discards the photons which have been chosen for security checking and picks out N photons $P_j(M1), P_j(M2), \cdots, P_j(MN)$ from the N message-coding sequences $S_{M1}, S_{M2}, \cdots, S_{MN}$, respectively. Alice encodes her message K_A according to the corresponding group A_j in the string A, the same as the step ④. After doing that, Alice performs an N-particle GHZ state joint measurement on $P_j(M1)$, $P_j(M2), \cdots, P_j(MN)$ and publishes her measurement outcomes.

If the Bobs and Charlie collaborate, they can perform an N-particle GHZ state joint measurement on the N corresponding photons $P_j(C1), P_j(C2), \cdots, P_j(CN)$ which come from the N checking sequences $S_{C1}, S_{C2}, \cdots, S_{CN}$, respectively. According to their measurement outcomes, they can get Alice's message K_A. Otherwise, none of them can obtain the key K_A.

In this scheme, we distribute N bits of classical message among the N agents with N-particle GHZ-state measurement. It has a higher capacity. On the other hand, this scheme can save the entanglement resource, too.

3 MQSS scheme for sharing an unknown arbitrary n-qubit state

In this section, we will present a scheme for sharing an unknown arbitrary n-qubit state with entanglement swapping. For simplicity, we will describe the 2-qubit state 2-agent case firstly.

We assume that there are two agents, Bob and Charlie. Alice, the sender, wants to distribute an unknown arbitrary two-particle state between Bob and Charlie. Firstly, Alice has 6 particles, particle 1, 2, 3, 4, x and y, in her hand. Particles 1, 2 and particles 3, 4 are both prepared by Alice in the Bell basis state $|\Psi^-\rangle$. Particle x and y are in an unknown arbitrary two-particles state which can be described as

$$\begin{aligned}
|X\rangle_{xy}&=\alpha|00\rangle_{xy}+\beta|01\rangle_{xy}\\
&\quad+\gamma|10\rangle_{xy}+\delta|11\rangle_{xy},
\end{aligned}\tag{8}$$

where

$$|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2=1.\tag{9}$$

Alice sends particles 2 and 4 to Bob and Charlie, respectively, and keeps particls 1, 3, x and y for herself. After both Bob and Charlie receive the particles, Alice performs a Bell measurement on particles

x, 1 and y, 3, respectively, and announces the measurement outcomes. Then, if Bob and Charlie cooperate, they can recover the original state $|X\rangle_{xy}$.

Let us use an example to explain our scheme in detail. Firstly, we assume that both the EPR pairs are originally prepared in one of the four Bell states $|\Psi^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$. Then, before Alice's measurement, the state of the composite quantum system of the 6 particles can be written as

$$|\Omega\rangle_s = |X\rangle_{xy} \otimes |\Psi^-\rangle_{12} \otimes |\Psi^-\rangle_{34}. \quad (10)$$

If Alice performs a Bell measurement on particles x, 1 and the measurement outcome is $|\Phi^+\rangle_{x1}$, which will occur with probability $\frac{1}{4}$, then the state of the subsystem with particles y, 3, 2 and 4 becomes

$$\begin{aligned}|\Omega\rangle_{sub} = (&\alpha|0011\rangle - \alpha|0110\rangle + \beta|1011\rangle \\ &- \beta|1110\rangle + \gamma|0100\rangle - \gamma|0001\rangle \\ &- \delta|1001\rangle + \delta|1100\rangle)_{y324}, \end{aligned} \quad (11)$$

and then, the state can be rewritten as

$$\begin{aligned}|\Omega\rangle_{sub} = &|\Phi^+\rangle_{y3}(\alpha|11\rangle - \beta|10\rangle \\ &- \gamma|01\rangle + \delta|00\rangle)_{24} \\ &+|\Phi^-\rangle_{y3}(\alpha|11\rangle + \beta|10\rangle \\ &- \gamma|01\rangle - \delta|00\rangle)_{24} \\ &+|\Psi^+\rangle_{y3}(-\alpha|10\rangle + \beta|11\rangle \\ &+ \gamma|00\rangle - \delta|01\rangle)_{24} \\ &+|\Psi^-\rangle_{y3}(-\alpha|10\rangle - \beta|11\rangle \\ &+ \gamma|00\rangle + \delta|01\rangle)_{24}. \end{aligned} \quad (12)$$

Therefore, if Alice performs another Bell measurement on particles y and 3, the quantum information of the state $|X\rangle_{xy}$ will be transferred to particles 2 and 4 which are controlled by Bob and Charlie. Suppose Bob and Charlie agree to cooperate, they can recover the unknown state by performing some unitary operations according to the Alice's measurement outcomes. For example, if Alice's measurement results are $|\Phi^+\rangle_{y3}$, $|\Phi^-\rangle_{y3}$, $|\Psi^+\rangle_{y3}$ or $|\Psi^-\rangle_{y3}$, respectively, Bob and Charlie can perform the unitary operations $U_3 \otimes U_3$, $U_3 \otimes U_2$, $-U_3 \otimes U_1$ or $-U_3 \otimes U_0$ on particles 2 and 4, respectively, and reconstruct the unknown state $|X\rangle_{xy}$.

It is easy to generalize this MQSS scheme to the N party case. We also suppose that there are N agents, Bob_i $(i = 1, 2, \cdots, N-1)$ and Charlie, and Alice wants to distribute an unknown arbitrary two-particle state $|X\rangle_{xy}$ among the N agents.

Then, Alice prepares N EPR pairs in the Bell state $|\Psi^-\rangle$ and sends one particle of each EPR pair to Bob_i and Charlie, retains other particles for herself. After all the agents receive the particles, Alice randomly selects one particle from particles which are held in her hand, and performs a Bell measurement on this particle and particle y, and then she performs a joint measurement on particle x and the others which held in her hand and announces the measurement results. Hence, if Bob_is and Charlie collaborate, they can perform a joint measurement on $N-2$ particles which controlled by them. As a result, the information of the unknown state has been distributed to the remaining two particles. And then, they can recover the unknown state by performing a corresponding unitary operation according to their and Alice's measurement outcomes. If Bob_is and Charlie do not collaborate, none of them can get the quantum information.

Similar to the above scheme, we can also distribute an unknown arbitrary n-qubit state among n agents.

An arbitrary n-qubit state can be written as

$$|X\rangle_n = \sum_{i_1 i_2 \cdots i_n} \alpha_{i_1 i_2 \cdots i_n} |i_1 i_2 \cdots i_n\rangle_{x_1 x_2 \cdots x_n}, \quad (13)$$

where $i_1, i_2, \cdots, i_n \in \{0, 1\}$, and $x_1, x_2, \cdots, x_n$ are the n particles which carry the quantum information. In order to distribute the above state, Alice will prepare n EPR pairs and share them with her n agents securely. Each EPR pair has been prepared in the state $|\Psi\rangle_{a_j b_j} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{a_j b_j}$ (where $j = 1, 2, \cdots, n$, and a_j, b_j are the two particles of the jth EPR pair). Then, Alice sends one particle of the jth EPR pair, say b_j to the jth agent Bob_j, and keeps the particle a_j $(j = 1, 2, \cdots, n)$. After all the agents receive the particles, the state of the composite quantum system can be described as

$$\begin{aligned}|\Omega\rangle_s = &\left(\sum_{i_1 i_2 \cdots i_n} \alpha_{i_1 i_2 \cdots i_n} |i_1 i_2 \cdots i_n\rangle_{x_1 x_2 \cdots x_n}\right) \\ &\otimes \prod_{j=1}^{n} \left[\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{a_j b_j}\right]. \end{aligned} \quad (14)$$

Then, Alice performs the Bell measurements on the particles x_j and a_j, and announces all the measurement outcomes. After doing these, the unknown n-qubit state will be transferred to the n particles which are controlled by n agents Bob_is $(i = 1, 2, \cdots, n)$. If and only if all the n agents cooperate, they

can recover the unknown n-qubit state. Otherwise, none of them can get the quantum information of the unknown n-qubit state.

In this scheme, we use EPR pairs to share an unknown arbitrary n-qubit state with n agents, and the security of the sharing EPR pairs between two agents has been discussed in Refs. [20, 22, 28—31]. Thus, the proposed scheme is secure.

4 Summary

In this paper we have proposed a scheme for multiparty quantum secret sharing of classical and quantum messages by using entanglement swapping. With our scheme, not only the classical information but also the quantum information can be transmitted to N agents. The security of our scheme is also confirmed.

References

1 Blakley G. R. How to share a secret. In: Proceedings of the American Federation of Information Processing 1979 National Computer Conference (American Federation of Information Processing, Arlington, VA)1979, 313—315.

2 Shamir A. How to share a secret. Commun. ACM, 1979, 22: 612—613.

3 Hillery M., Bužek V. and Berthiaume A. Quantum secret sharing. Phys. Rev. A, 1999, 59: 1829—1834.

4 Karlsson A., Koashi M. and Imoto N. Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A, 1999, 59: 162—168.

5 Gottesman D. Theory of quantum secret sharing. Phys. Rev. A, 2000, 61: 042311(1)—(8).

6 Bandyopadhyay S. Teleportation and secret sharing with pure entangled states. Phys. Rev. A, 2000, 62: 012308(1)—(7).

7 Nascimento A. C. A., Mueller-Quade J. and Imai H. Improving quantum secret-sharing schemes. Phys. Rev. A, 2001, 64: 042311(1)—(5).

8 Yang C. P. and Gea-Banacloche J. Teleportation of rotations and receiver-encoded secret sharing. J. Opt. B: Quantum Semiclass. Opt., 2001, 3: 407—411.

9 Karimipour V., Bahraminasab A. and Bagherinezhad S. Entanglement swapping of generalized cat states and secret sharing. Phys. Rev. A, 2002, 65: 042320(1)—(5).

10 Bagherinezhad S. and arimipour V. K. Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers. Phys. Rev. A, 2003, 67: 044302(1)—(4).

11 Tyc T. and Sanders B. C. How to share a continuous-variable quantum secret by optical interferometry. Phys. Rev. A, 2002, 65: 042310(1)—(5).

12 Guo G. P. and Guo G. C. Quantum secret sharing without entanglement. Phys. Lett. A, 2003, 310: 247—251.

13 Lance A. M., Symul T., Bowen W. P. et al. Continuous variable (2, 3) threshold quantum secret sharing schemes. New J. Phys., 2003, 5: 4—8.

14 Tyc T., Rowe D. J. and Sanders B. C. Efficient sharing of a continuous-variable quantum secret. J. Phys. A: Math. Gen., 2003, 36: 7625—7637.

15 Sen A., Sen U. and Zukowski M. Unified criterion for security of secret sharing in terms of violation of Bell inequalities. Phys. Rev. A, 2003, 68: 032309(1)—(7).

16 Xiao Li, Long G. L., Deng F. G. et al. Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A, 2004, 69: 052307(1)—(5).

17 Deng F. G., Zhou H. Y. and Long G. L. Bidirectional quantum secret sharing and secret splitting with polarized single photons. Phys. Lett. A, 2005, 337: 329—334.

18 Deng F. G., Zhou H. Y. and Long G. L. An efficient quantum secret sharing scheme with Einstein-Podolsky-Rosen pairs. Phys. Lett. A, 2005, 340: 43—50.

19 Zhang Z. J., Li Y. and Man Z. X. Multiparty quantum secret sharing. Phys. Rev. A, 2005, 71: 044301(1)—(4).

20 Deng F. G., Li X. H., Zhou H. Y. et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A, 2005, 72: 044302(1)—(5).

21 Yan F. L. and Gao T. Entanglement concentration for unknown atomic entangled states via entanglement swapping. Phys. Rev. A, 2005, 72: 012304(1)—(5).

22 Zhang Z. J. and Man Z. X. Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A, 2005, 72: 022303(1)—(4).

23 Wang J., Zhang Q. and Tang C. J. Efficient multiparty quantum secret sharing of secure direct communication. Quantum Physics, 0510212(1)—(6).

24 Cleve R., Gottesman D. and Lo H. K. How to share a quantum secret. Phys. Rev. Lett., 1999, 83: 648—651.

25 Li Y. M., Zhang K. S. and Peng K. C. Multiparty secret sharing of quantum information based on entanglement swapping. Phys. Lett. A, 2004, 324: 420—424.

26 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(1)—(4).

27 Deng F. G., Li C. L., Li Y. S. et al. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys. Rev. A., 2005, 72: 022338(1)—(8).

28 Deng F. G., Long G. L. and Liu X. S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A, 2003, 68: 042317(1)—(5).

29 Li X. H., Zhou P., Liang Y. J. et al. Quantum secure direct communication network with two-Step protocol. Chin. Phys. Lett., 2006, 23: 1080—1084.

30 Deng F. G. and Long G. L. Secure direct communication with a quantum one-time pad. Phys. Rev. A, 2004, 69: 052319(1)—(4).

31 Deng F. G. and Long G. L. Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys. Rev. A, 2004, 70: 012311(1)—(7).

32 Cabello A. Quantum key distribution in the Holevo limit. Phys. Rev. Lett., 2000, 85: 5635—5638.

33 Li C. Y., Zhou H. Y., Wang Y. et al. Secure quantum key distribution network with Bell States and Local Unitary Operations. Chin. Phys. Lett., 2005, 22: 1049—1052.