Int J Theor Phys (2010) 49: 2852–2858
DOI 10.1007/s10773-010-0478-z

An Efficient Multiparty Quantum Secret Sharing Protocol Based on Bell States in the High Dimension Hilbert Space

Gan Gao · Li-ping Wang

Received: 21 June 2010 / Accepted: 20 August 2010 / Published online: 7 September 2010

Abstract We propose a quantum secret sharing protocol, in which Bell states in the high dimension Hilbert space are employed. The biggest advantage of our protocol is the high source capacity. Compared with the previous secret sharing protocol, ours has the higher controlling efficiency. In addition, as decoy states in the high dimension Hilbert space are used, we needn't destroy quantum entanglement for achieving the goal to check the channel security.

Keywords Bell state · Decoy particle · Quantum secret sharing

1 Introduction

In the last decade, the principles of quantum mechanics have supplied a lot of interesting applications in the field of information. Quantum key distribution (QKD) is one of these applications. The first quantum key distribution protocol [1] was proposed by Bennett and Brassard in 1984. Since then, all kinds of QKD protocols [2–14] have been put forward. In addition, utilizing the principle of quantum mechanics, the other cryptographic tasks have also progressed rapidly, such as quantum teleportation (QT), quantum secure direct communication (QSDC), quantum secret sharing (QSS) and so on. The QSS is an important branch of quantum communication and the generalization of classical secret sharing into a quantum scenario. In the QSS, the task that needs to be finished is which a secret message is splitted into several pieces by a boss, each agent holds a piece; and no subset of agents is sufficient to extract the message, but the entire set is. Obviously, the QSS may play an important role in protecting secret quantum information so that the works about QSS have attracted a lot of attention in theoretical and experimental ways [15–37]. All these works may be divided into two kinds, one only deals with the QSS of classical messages (i.e., bits) [15–24, 33, 34, 36, 37], or only deals with the QSS of quantum information [25–31] where the secret is an arbitrary unknown state in a qubit; and the other [32, 35] studies both, that is, deals

G. Gao (✉) · L.-p. Wang
Department of Electrical Engineering, Tongling University, Tongling 244000, China
e-mail: gaogan0556@163.com

with QSS of classical messages and QSS of quantum information simultaneously. In this paper, we only consider the sharing of classical messages and propose a feasible theoretical protocol about multiparty secret sharing of classical messages. In order to make it own the high capacity, we employ Bell states in the high dimension Hilbert space [38, 39]. Recently, that quantum communication protocols are proposed in the high dimension Hilbert space has been a hot point of research. For example, in 2003, Deng et al. [40] suggested a two-step quantum direct communication protocol; later on, Wang et al. expanded Deng et al.'s protocol to the high dimension case [38]. In 2005, Cola et al. [41] proposed a class of quantum protocols to teleport bipartite (entangled) states of two qubits ; subsequently, Nguyen generalized it to the case of arbitrary quNits [42]. In two-level system, Zhang et al. proposed a QSS protocol [35] based on the entanglement swapping of Bell states; before long, the QSS protocol of two-level system was generalized to that of three-level system [36]. Our QSS protocol in the high dimension Hilbert space isn't the expansion of the previous protocol, indeed, we design it out under the inspiring of Wang et al.'s protocol [37]. And all agents in our protocol have the higher controlling efficiency than those in Wang et al.'s protocol [37]. In addition, in order to check eavesdropping and to save quantum entanglement source, we utilize two batches of decoy states (particles), which are inserted into the two sequences. By making a single-particle measurement on decoy particle, whether the quantum channels are eavesdropped can be judged. At first, we give three-party case of this feasible theoretical QSS protocol, and then generalize it to the multiparty QSS case. Suppose Alice is the boss, and has two agents: Bob and Charlie in the distance. Alice herself knows that one of them, Bob or Charlie, is dishonest and not completely trusted. Also Alice knows that the honest agent will stop the dishonest one from doing any damage. Before describing our three-party QSS protocol, we define the Bell states in the $d \times d$-dimension Hilbert space as follows:

$$|\psi_{nm}\rangle_{ht} = \sum_{j=0} e^{\frac{2\pi ijn}{d}} |j\rangle_h \otimes |j + m \bmod d\rangle_t / \sqrt{d}, \tag{1}$$

where $n, m = 0, 1, 2, \ldots, d-1$. The unitary operators we need in this scheme:

$$U_{nm} = \sum_{j=0} e^{\frac{2\pi ijn}{d}} |j + m \bmod d\rangle \otimes \langle j|. \tag{2}$$

The number of unitary operators is d^2, and they can transfer the Bell state

$$|\psi_{00}\rangle_{ht} = \sum_{j=0} |j\rangle_h \otimes |j\rangle_t / \sqrt{d}, \tag{3}$$

into the Bell state $|\psi_{nm}\rangle_{ht}$, i.e., $(I \otimes U_{nm})|\psi_{00}\rangle_{ht} = |\psi_{nm}\rangle_{ht}$. Here I is the identity matrix which means doing nothing on the photon h. In addition, we put forward two sets of measuring basis (MB) in the high dimension Hilbert space. The Z-MB is composed of the following eigenvectors [39]:

$$|Z_0\rangle = |0\rangle, \quad |Z_1\rangle = |1\rangle, \quad |Z_2\rangle = |2\rangle \cdots |Z_{d-1}\rangle = |d-1\rangle. \tag{4}$$

The eigenvectors of the X-MB can be described as following:

$$|X_0\rangle = \frac{1}{\sqrt{d}}(|0\rangle + |1\rangle + \cdots + |d-1\rangle)$$

$$
\begin{aligned}
|X_1\rangle &= \frac{1}{\sqrt{d}}(|0\rangle + e^{\frac{2\pi i}{d}}|1\rangle + \cdots + e^{\frac{(d-1)2\pi i}{d}}|d-1\rangle) \\
|X_2\rangle &= \frac{1}{\sqrt{d}}(|0\rangle + e^{\frac{4\pi i}{d}}|1\rangle + \cdots + e^{\frac{(d-1)4\pi i}{d}}|d-1\rangle) \\
&\cdots \\
|X_{d-1}\rangle &= \frac{1}{\sqrt{d}}(|0\rangle + e^{\frac{2(d-1)\pi i}{d}}|1\rangle + e^{\frac{2\times 2(d-1)\pi i}{d}}|2\rangle + \\
&\quad \cdots + e^{\frac{(d-1)\times 2(d-1)\pi i}{d}}|d-1\rangle). \qquad (5)
\end{aligned}
$$

We still introduce one operator (Hadamard operator):

$$
H = \frac{1}{\sqrt{d}}\begin{pmatrix}
1 & 1 & \cdots & 1 \\
1 & e^{\frac{2\pi i}{d}} & \cdots & e^{\frac{(d-1)2\pi i}{d}} \\
1 & e^{\frac{4\pi i}{d}} & \cdots & e^{\frac{(d-1)4\pi i}{d}} \\
\vdots & \vdots & \cdots & \vdots \\
1 & e^{\frac{2(d-1)\pi i}{d}} & \cdots & e^{\frac{(d-1)2(d-1)\pi i}{d}}
\end{pmatrix} \qquad (6)
$$

which can realize the transformation between the two MBs.

2 Construction of Quantum Secret Sharing Protocol

In our three-party QSS protocol, Bell states and decoy states in the high dimension Hilbert space will be employed; Alice is the boss, that is the sender of secret messages, and both Bob and Charlie are the agents. Next, let us detailedly describe this protocol, and its main steps are as follows:

(1) Alice prepares an ordered EPR pair sequence, in which all EPR pairs are in the $|\psi\rangle_{00}$. We denote the ordered EPR pair sequence with $[P_1^a, P_1^b, P_2^a, P_2^b, P_3^a, P_3^b, P_4^a, P_4^b, P_5^a, P_5^b, \ldots, P_n^a, P_n^b]$ (simply say P sequence). Here, a and b represent two particles in one EPR pair; and the subscripts "$1, 2, 3, 4, 5, \ldots, n$" indicate the orders of EPR pairs in the P sequence. Alice takes one particle from each EPR pair to form an ordered particle sequence, $[P_1^a, P_2^a, P_3^a, P_4^a, P_5^a, P_6^a, \ldots, P_n^a]$ (simply say P_t sequence). The remaining partner particles form another ordered particle sequence, $[P_1^b, P_2^b, P_3^b, P_4^b, P_5^b, P_6^b, \ldots, P_n^b]$ (simply say P_h sequence). In addition, Alice still prepares a batch of decoy particles, say d particles. Every d particle is randomly in one of these states: $|Z_0\rangle, |Z_1\rangle, \ldots, |Z_{d-1}\rangle$, $|X_0\rangle, |X_1\rangle, \ldots, |X_{d-1}\rangle$. Next, she inserts the d particles into the P_t sequence. So the P_t sequence is changed into $[P_1^a, P^d, P_2^a, P^d, P_3^a, P_4^a, P^d, P_5^a, P_6^a, \ldots, P^d, P_n^a]$ (simply say P_t' sequence). The position of each d particle in the P_t' sequence is secret, only known by Alice. And then, she sends the P_t' sequence to Bob.

(2) After receiving the P_t' sequence, Bob selects one of d^2+1 operators and performs it on each received particle. Here, d^2+1 operators include d^2 unitary operators and one Hadamard operator. By the way, the probability that Bob selects the Hadamard operator is $\frac{1}{2}$, and the probability of selecting each unitary operator is $\frac{1}{2d^2}$. And then, Bob sends the P_t' sequence to Charlie. Next, what Charlie does is the same as Bob's. In the end, Charlie sends the P_t' sequence back to Alice.

(3) After receiving the P_t' sequence from Charlie, Alice randomly selects Z-MB or X-MB to measure each d particle. Then, she publishes the position of each d particle in the P_t' sequence, and requires Bob and Charlie to tell her their performing operators on each d particle. So Alice can analyze the error rate of the P_t' sequence transmission by comparing her measurement outcomes with her deducing outcomes. By the way, since Alice can't select the correct measuring basis for all d particles, half d particles are wasted and useless for the security analysis. In other words, Alice can't judge whether the quantum channel is secure by analysing this half d particles. Similarly, part K sample photons in the protocol [37] are also useless as the incorrect selection of measuring basis. But, depending on another part d particles, Alice can decide the error rate of the P_t' sequence transmission. If the error rate goes beyond the threshold, the process is aborted. Otherwise, the process goes on to the next step.

(4) Getting rid of the d particles, the P_t' sequence is changed back to the P_t sequence. Next, Alice encodes her secret messages by performing the unitary operators (U_{nm}) on the particles in the P_h sequence. In advance, Alice, Bob and Charlie have an agreement that each unitary operator corresponds to two-Nit ($N = d$) classical messages. After encoding, Alice rearranges the P_t and P_h sequences back to the P sequence. Before sending it to Bob, Alice inserts another batch of decoy particles, say d' particles, into the encoded P sequence. So the P sequence is changed into $[P_1^a, P^{d'}, P_1^b, P^{d'}, P_2^a, P_2^b, P^{d'}, P_3^a, P_3^b, P^{d'}, P_4^a, P_4^b, P_5^a, P^{d'}, P_5^b, \ldots, P_n^a, P^{d'}, P_n^b]$ (simply say P' sequence). Similarly, also every d' particle is randomly in one of these states: $|Z_0\rangle, |Z_1\rangle, \ldots, |Z_{d-1}\rangle, |X_0\rangle, |X_1\rangle, \ldots, |X_{d-1}\rangle$; and the positions of the d' particles in the P' sequence are also secret, only known by Alice. Whereafter, Alice sends the P' sequence to Bob.

(5) After confirming that Bob has received the P' sequence, Alice publishes the positions of d' particles in the P' sequence and the state of each d' particle. According to Alice's publishing information, Bob uses proper measuring basis to measure each d' particle. So they can judge whether the P' sequence is attacked from Alice to Bob. Even if it is attacked, the eavesdropper can't get any useful messages but destroys the sequence transmission. If it isn't attacked, getting rid of the d' particles and making the P' sequence change back to the encode P sequence, Bob and Charlie collaborate to perform the Bell state measurement on each two particles in the P sequence in order. By the way, they have to collaborate in order to correctly make the Bell state measurement. This is because some EPR pairs in the encode P sequence are in the superposition of two different Bell states after Bob' and Charlie's performing operators. If the number of the H (Hadamard) operator in their performing operators is even, Bob may directly make the Bell state measurement. On the contrary, if the number is odd, firstly, Bob must perform H^{-1} operator (Here, $HH^{-1} = I$). And then, he makes the Bell state measurement. Clearly, the parity of the H number is decided together by Bob and Charlie. Until Charlie tells Bob of his performing exact operator, Bob isn't able to make the Bell state measurement correctly. Therefore, Bob and Charlie want to extract Alice's secret messages, they must collaborate honestly. Otherwise, neither of them can get Alice's secret messages with 100% certainty.

So far we have proposed three-party QSS protocol using Bell states and decoy states in the high dimension Hilbert space. In this protocol, the securities of the two sequences (P_t' and P') transmission are assured by two batches of decoy particles (d and d'). By measuring decoy particles, it can be judged whether the two sequences are transmitted securely, as if the decoy particles act as a bodyguard role here. In Step (2), we can see that the $d^2 + 1$ operators are utilized, moreover, the probability that each agent selects the H operator is $\frac{1}{2}$,

and the probability of selecting each unitary operator is $\frac{1}{2d^2}$. If one agent performs each of the d^2+1 operators on a particle that is in $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{d-1}|d-1\rangle$ (here, $|\alpha_0|^2 + |\alpha_1|^2 + \cdots + |\alpha_{d-1}|^2 = 1$), he (she) will obtain d^2+1 states. Obviously, these d^2+1 states aren't completely orthogonal. As is well known, none is able to distinguish them perfectly according to the quantum no-distinguishing theorem. Further, also the d^2+1 operators can't be distinguished perfectly. In these operators, the H operator is indispensable. If it doesn't exist, the eavesdropper (the dishonest agent or the outside eavesdropper) very easily distinguishes the d^2 unitary operators using a set of orthogonal basis to make a measurement. As a matter of fact, the H operator exists, so the eavesdropper can't eavesdrop the information which operator is performed. In our QSS protocol, the P_t' sequence is sent out by Alice, and through a round trip, it returns to Alice again. For the outside eavesdropper, it is impossible to extract Alice's secret messages by intercepting the P_t' sequence, because this sequence is composed of one particle of EPR pair. As is well known, nobody can read out any information from one particle of EPR pair. Only if the P_t' sequence returns to Alice securely, no matter what the eavesdropping trick the outside eavesdropper does in the latter steps, her doing is worthless. Subsequently, even if she intercepts the P' sequence, and rearranges the sequence to the P sequence according to Alice publishing information, she can't read out Alice's secret messages either. And she is only able to know the relation among Alice's, Bob's and Charlie's operators. If Bob (Charlie) eavesdropping, similarly, he only knows the relation between Alice's and Charlie's (Bob's) operators. In essence, the security proof of our QSS protocol is similar to that of Wang et al.'s protocol [37] though the dimension number of two protocols is different. Wang et al.'s protocol [37] has been proved to be secure, hence our QSS protocol is also secure. Next, let us think why this QSS protocol is put forward in the high dimension Hilbert space? The key of the question is gotten easily, that is, the proposed protocol has the high source capacity. In our QSS protocol, Alice uses the d^2 unitary operators to encode her secret messages. Obviously, each particle that is sent out by her can load $\log_2 d$ bits information. However, in Wang et al.'s QSS protocol [37], every photon loads only 1 bit. In the case of $d > 2$, our protocol has the higher source capacity than Wang et al.'s. In addition, from the ahead content, we can see that the number of Alice's unitary operators to encode her secret messages is d^2, and the number of the operators that each agent may select in order to obtain the sharing right is d^2+1. Here, we define the controlling efficiency $\eta = \frac{\log d^2}{\log(d^2+1)}$. When d in our protocol reduces to 2, the η_{our} equals to $\frac{2}{\log 5}$. However, in Wang et al.'s protocol, the η_{wang} equals to $\frac{1}{\log 5}$. Clearly, $\eta_{our} = \frac{2}{\log 5} > \eta_{wang} = \frac{1}{\log 5}$, so the agents in our QSS protocol have the higher controlling efficiency than those in Wang et al.'s.

It is very easy to generalize this three-party QSS protocol to the n-party QSS protocol ($n \geq 4$). In the three-party case, the agents are only Bob and Charlie. However, in the n-party case ($n \geq 4$), the number of the agents is added greatly, and we assume that they are Bob, Charlie, Dick, ..., York and Zach (there are totally $n-1$ agents), respectively. Each agent, as well as Bob in the three-party QSS protocol, performs one of the d^2+1 operators on every particle in the P_t' sequence, until Zach sends the P_t' sequence back to Alice. After receiving the sequence, Alice first checks the security of the P_t' sequence transmission, and then encodes her secret messages by performing the unitary operators, in the end, she sends the encoded P' sequence to any agent. After receiving the P' sequence, first, this agent and Alice finish the security check of the P' sequence transmission. And then, this agent and the other agents collaborate to make the Bell state measurements, and deduce Alice's secret messages together. Similarly, in the n-party QSS protocol ($n \geq 4$), all agents must collaborate honestly, otherwise, none can extract Alice's secret messages by oneself.

3 Discussion and Conclusion

Making use of the Bell states and the decoy states in high dimension Hilbert space, we have put forward an efficient multiparty QSS protocol, whose advantages is the high source capacity, and in which all agents have the higher controlling efficiency than ones in the previous QSS protocol [37]. In addition, in the process of the particle transmission, we employ the "sequence transmission" idea [12]. Firstly, the whole EPR pair sequence (the P sequence) is divided into two sequences, P_t and P_h. And then, the P_t sequence containing the d particles (the P_t' sequence) is sent out by Alice. Note that, all agents obtain the sharing rights by performing operators. Through a round trip, the P_t' sequence returns to Alice again. At last, Alice sends out the encoded P' sequence. By the way, in this QSS protocol, we employ two batches of decoy particles, that is, the d particles and the d' particles. Depending on these decoy particles, the securities of the quantum channels are analyzed successfully. As they are used, we save the expensive quantum entanglement sources.

Acknowledgements The author Gan Gao thanks his parents for their encouragements. This work is supported by the Natural Science Foundation of Anhui Province under Grant No. KJ2010B236.

References

1. Bennett, C.H., Brassard, G.: In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings, Bangalore, India, p. 175. IEEE, New York (1984)
2. Ekert, A.K.: Phys. Rev. Lett. **67**, 661 (1991)
3. Bennett, C.H.: Phys. Rev. Lett. **68**, 3121 (1992)
4. Bennett, C.H., Brassard, G., Mermin, N.D.: Phys. Rev. Lett. **68**, 557 (1992)
5. Bennett, C.H., Wiesner, S.J.: Phys. Rev. Lett. **69**, 2881 (1992)
6. Shi, B.S., Li, J., Liu, J.M., Fan, X.F., Guo, G.C.: Phys. Lett. A **281**, 83 (2001)
7. Zhang, Y.S., Li, C.F., Guo, G.C.: Phys. Rev. A **63**, 036301 (2001)
8. Guo, G.P., Li, C.F., Shi, B.S., Guo, G.C.: Phys. Rev. A **64**, 042301 (2001)
9. Pan, J.W., Daniell, M., Gasparoni, S., Weihs, G., Zeilinger, A.: Phys. Rev. Lett. **86**, 4435 (2001)
10. Wang, X.B.: Phys. Rev. Lett. **92**, 077902 (2004)
11. Li, C., Song, H.S., Zhou, L.: J. Opt., B Quantum Semiclass. Opt. **5**, 155 (2003)
12. Long, G.L., Liu, X.X.: Phys. Rev. A **65**, 032302 (2002)
13. Gao, G.: Opt. Commun. **281**, 876 (2008)
14. Gao, G.: Phys. Scr. **81**, 065005 (2010)
15. Hillery, M., Buzk, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
16. Li, Y.M., Zhang, K.S., Peng, K.C.: Phys. Lett. A **324**, 420 (2004)
17. Gottesman, D.: Phys. Rev. A **61**, 042311 (1999)
18. Liu, W.T., Liang, L.M., Li, C.Z., Yuan, J.M.: Chin. Phys. Lett. **23**, 3148 (2006)
19. Chau, H.F.: Phys. Rev. A **66**, 060302 (2002)
20. Song, J., Zhang, S.: Chin. Phys. Lett. **23**, 1383 (2006)
21. Guo, G.P., Guo, G.C.: Phys. Lett. A **310**, 247 (2003)
22. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Phys. Rev. A **69**, 052307 (2004)
23. Yan, F.L., Gao, T., Li, Y.C.: Chin. Phys. Lett. **25**, 1187 (2008)
24. Deng, F.G., Li, X.H., et al.: Phys. Lett. A **354**, 190 (2006)
25. Cleve, R., Gottesman, D., Lo, H.K.: Phys. Rev. Lett. **83**, 648 (1999)
26. Bandyopadhyay, S.: Phys. Rev. A **62**, 012308 (2000)
27. Hsu, L.Y.: Phys. Rev. A **68**, 022306 (2003)
28. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Phys. Rev. Lett. **92**, 177903 (2004)
29. Zhang, Y.Q., Jin, X.R., Zhang, S.: Phys. Lett. A **341**, 380 (2005)
30. Zhang, Z.J., Yang, J., Man, Z.X., Li, Y.: Eur. Phys. J. D **33**, 133 (2005)
31. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**, 042317 (2003)
32. Zhang, Z.J., Li, Y., Man, Z.X.: Phys. Rev. A **71**, 044301 (2005)
33. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Phys. Rev. A **72**, 044302 (2005)
34. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Phys. Rev. A **73**, 049901(E) (2005)
35. Zhang, Z.J., Man, Z.X.: Phys. Rev. A **72**, 022303 (2005)

36. Zhang, Z.J., Liu, Y.M., Fang, M., Wang, D.: Int. J. Mod. Phys. C **18**, 1885 (2007)
37. Wang, T.Y., Wen, Q.Y., Chen, X.B., Guo, F.Z., Zhu, F.C.: Opt. Commun. **281**, 6130 (2008)
38. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Phys. Rev. A **71**, 044305 (2005)
39. Bechmann-Pasquinucci, H., Peres, A.: Phys. Rev. Lett. **85**, 3313 (2000)
40. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**, 042317 (2003)
41. Cola, M.M., Paris, M.G.A.: Phys. Lett. A **337**, 10 (2005)
42. Ba An, N.: Phys. Lett. A **341**, 9 (2005)