Vol 18 No 11, November 2009
1674-1056/2009/18(11)/4690-05

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

High-capacity three-party quantum secret sharing with superdense coding*

Gu Bin(顾 斌)†, Li Chuan-Qi(李传起),
Xu Fei(徐 飞), and Chen Yu-Lin(陈玉林)

College of Math and Physics, Nanjing University of Information Science and Technology (NUIST), Nanjing 210044, *China*

(Received 16 January 2009; revised manuscript received 13 February 2009)

This paper presents a scheme for high-capacity three-party quantum secret sharing with quantum superdense coding, following some ideas in the work by Liu *et al* (2002 *Phys. Rev.* A **65** 022304) and the quantum secret sharing scheme by Deng *et al* (2008 *Phys. Lett.* A **372** 1957). Instead of using two sets of nonorthogonal states, the boss Alice needs only to prepare a sequence of Einstein–Podolsky–Rosen pairs in d-dimension. The two agents Bob and Charlie encode their information with dense coding unitary operations, and security is checked by inserting decoy photons. The scheme has a high capacity and intrinsic efficiency as each pair can carry $2\mathrm{lb}d$ bits of information, and almost all the pairs can be used for carrying useful information.

Keywords: quantum secret sharing, three-party, high-capacity, superdense coding

PACC: 0367

Quantum entanglement provides some novel ways for quantum information transmission and processing, such as quantum key distribution (QKD),[1−6] quantum teleportation,[7] quantum dense coding,[8−11] and so on. QKD provides a secure way for two legitimate users, say the sender Alice and the receiver Bob, to create a private key. With a private key, Alice and Bob can communicate a secret message securely. Quantum teleportation[7] acts as an important role in a remote two-party quantum communication. Quantum dense coding[8−11] can be used to improve the capacity of quantum communication. All these branches of quantum communication have a common property, that is, the communication takes place between two legitimate users. Another important branch of quantum communication is called quantum secret sharing (QSS) which is used to share a secret message between the boss Alice and her agents. Unlike the branches of quantum communication above, Alice suspects that one of her agents may be dishonest, but she does not know whom the dishonest one is. She believes that the honest agents can prevent the dishonest agent from destroying her benefits if the agents act in concert.

In 1999, Hillery, Bužek and Berthiaume (HBB)[12] proposed the first QSS protocol based on three-particle Greenberger–Horne–Zeilinger (GHZ) states for three-party secret sharing of a private key. In this protocol, the three parties, Alice and her two agents Bob and Charlie, choose randomly one of the two measuring bases, say the measuring basis (MB) $X = (|H\rangle \pm |V\rangle)/\sqrt{2}$ and the MB $Y = (|H\rangle \pm \mathrm{i}|V\rangle)/\sqrt{2}$ to measure their particles in hand. Here $|H\rangle \equiv |0\rangle$ and $|V\rangle \equiv |1\rangle$ represent the horizontal polarization of photons and the vertical one, respectively. As there is a probability of 50% that the three parties choose uncorrelated MBs, which means they cannot deduce the private key $K_{\mathrm{A}} = K_{\mathrm{B}} \oplus K_{\mathrm{C}}$ and they should discard their instances in this time, the intrinsic efficiency of HBB QSS scheme is not more than 50%. Here K_{A}, K_{B} and K_{C} represent the keys obtained by Alice, Bob and Charlie, respectively. Subsequently, Karlsson, Koashi and Imoto (KKI)[13] proposed a QSS scheme with two-particle entanglement. Xiao *et al*[14] proposed two schemes for improving the efficiencies of both the HBB and KKI QSS schemes with some special quantum techniques[5] and extended QSS into multi-party and high dimensions. A concise form for the shared secret was first given in their work.[14] Moreover, it has been experimentally verified in nuclear magnetic resonance quantum systems.[15] In 2005, Deng, Zhou and Long presented a QSS scheme with Einstein–Podolsky–Rosen (EPR) pairs[16] and

*Project supported by the National Natural Science Foundation (NSF) of China (Grant No 10847147), the NSF of Jiangsu Province, China (Grant No BK2008437) and Jiangsu Provincial Universities (Grant No 07KJB510066) and the Science Foundation of NUIST, China.

†Corresponding author. E-mail: gubin@nuist.edu.cn

another two QSS schemes with single photons.[17,18] Zhang and Man introduced a QSS scheme with entanglement swapping.[19] Zhang, Li and Man proposed a QSS scheme with single photons and some unitary operation.[20] Deng *et al*[21] improved its security. Yan *et al* presented two QSS schemes between two groups with single photons.[22,23] Now, QSS is generalized to share quantum information, i.e., an unknown quantum state.[24−34] In this time, QSS is equivalent to controlled teleportation, shown by Deng *et al.*[35]

Recently, Deng, Li and Zhou (DLZ2008) proposed a novel QSS scheme[36] with EPR pairs based on quantum dense coding,[8] called it the DLZ2008 QSS scheme. Its security depends on the security of the transmission of some decoy photons.[37−39] That is, the parties exploit their decoy photons to prevent a dishonest agent or a malicious eavesdropper from stealing the information fully and freely, and use the entangled quantum systems to carry the useful information. The DLZ2008 QSS scheme has the advantage of high intrinsic efficiency and high capacity as almost all the entangled quantum systems can be used for creating their private key and each EPR pair can carry two bits of useful information in theory.

In this paper, we will present a QSS scheme based on quantum superdense coding, following some ideas in the work by Liu *et al*[9] and the DLZ2008 QSS scheme.[36] The boss Alice prepares a sequence of d-dimensional EPR pairs in a d-dimensional Bell-basis state and divides the pairs into two sequences $S_{\rm B}$ and $S_{\rm C}$ which are sent to her two agents Bob and Charlie, respectively. The agents code their information on the message photons with some unitary operations. Also, they should prevent an eavesdropper from eavesdropping with Trojan horse attack strategies[40] by adding a filter in front of their devices and sampling some photons to measure with a photon beam splitter (PBS: 50/50) and two MBs. The security of the transmission of the message photons running back to Alice depends on the decoy photons prepared by the agents. In this scheme, each d-dimensional entangled pair can carry 2lb$d$ bits of information and almost all the pairs can be used for carrying useful information in theory. Compared with the optimal QSS scheme by Deng, Li and Zhou,[36] this scheme is simpler in the preparation and the measurement of quantum signals, and it has a higher capacity. It also has a higher intrinsic efficiency than others.[12,13]

For two-particle quantum systems, d-dimensional Bell-basis states in a symmetric quantum channel are[7,9,11]

$$|\Psi_{nm}\rangle_{\rm BC}=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}{\rm e}^{\frac{2\pi {\rm i}jn}{d}}|j\rangle_{\rm B}\otimes|j+m \bmod d\rangle_{\rm C}, \quad (1)$$

where $n,m=0,1,...,d-1$. The unitary operations

$$U_{nm}^{\rm C}=\sum_{j=0}^{d-1}{\rm e}^{\frac{2\pi {\rm i}jn}{d}}|j+m \bmod d\rangle_{\rm C}\langle j| \quad (2)$$

can transform the Bell-basis state

$$|\Psi_{00}\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle_{\rm B}\otimes|j\rangle_{\rm C} \quad (3)$$

into the Bell-basis state $|\Psi_{nm}\rangle_{\rm BC}$, i.e.,

$$U_{nm}^{\rm C}|\Psi_{00}\rangle_{\rm BC}=|\Psi_{nm}\rangle_{\rm BC}. \quad (4)$$

Here $U_{nm}^{\rm C}$ represents the unitary operation performed on the particle C. If Bob and Charlie perform their unitary operations $U_{kl}^{\rm B}$ and $U_{k'l'}^{\rm C}$ on the particles B and C in the state $|\Psi_{00}\rangle_{\rm BC}$, respectively, the state $|\Psi_{00}\rangle_{\rm BC}$ is transformed into another one shown as follows

$$\begin{aligned}
&(U_{kl}^{\rm B}\otimes U_{k'l'}^{\rm C})|\Psi_{00}\rangle_{\rm BC}\\
=&\left\{\left(\sum_{r=0}^{d-1}{\rm e}^{\frac{2\pi {\rm i}rk}{d}}|r+l \bmod d\rangle_{\rm B}\langle r|\right)\otimes\left(\sum_{r'=0}^{d-1}{\rm e}^{\frac{2\pi {\rm i}r'k'}{d}}|r'+l' \bmod d\rangle_{\rm C}\langle r'|\right)\right\}\left(\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j\rangle_{\rm B}\otimes|j\rangle_{\rm C}\right)\\
=&\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}{\rm e}^{\frac{2\pi {\rm i}}{d}j(k'+k)}|j+l \bmod d\rangle_{\rm B}\otimes|j+l' \bmod d\rangle_{\rm C}\\
=&{\rm e}^{\frac{-2\pi {\rm i}}{d}l(k'+k)}\frac{1}{\sqrt{d}}\sum_{j'=0}^{d-1}{\rm e}^{\frac{2\pi {\rm i}}{d}j'(k'+k)}|j'\rangle_{\rm B}\otimes|j'+l'-l \bmod d\rangle_{\rm C}\\
=&A|\Psi_{k'+k,l'-l}\rangle_{\rm BC}. \quad (5)
\end{aligned}$$

Here $A = \exp(-2\pi \mathrm{i} l(k+k')/d)$ is a whole phase for the state $|\Psi_{k'+k,l'-l}\rangle_{\mathrm{BC}}$ and it does not have a physics effect. The subscripts $k'+k$ and $l'-l$ mean $(k'+k \bmod d)$ and $(l'-l \bmod d)$, respectively. In other words,

$$(U_{kl}^{\mathrm{B}} \otimes U_{k'l'}^{\mathrm{C}})|\Psi_{00}\rangle_{\mathrm{BC}} = |\Psi_{k'+k,l'-l}\rangle_{\mathrm{BC}}. \tag{6}$$

Our high-capacity three-party QSS scheme works with the following steps.

(S0) Alice and her agents encode the unitary operation U_{kl} as the information kl $(k,l \in \{0,1,2,\ldots,d-1\})$.

(S1) Alice prepares a sequence of d-dimensional two-photon quantum systems BC in the Bell-basis state $|\Psi_{00}\rangle_{\mathrm{BC}}$. Alice divides the photons into two sequences, S_{B} and S_{C}. S_{B} is made up of all the photons B in order and S_{C} is made up of all the photons C, similar to Ref.[4]. Alice sends the sequences S_{B} and S_{C} to Bob and Charlie, respectively.

(S2) After receiving the sequences S_{B} and S_{C}, Bob and Charlie choose some samples from their photon sequences independently and randomly check for eavesdropping. That is, each agent (Bob or Charlie) chooses the checking-eavesdropping mode with a small probability p_{c} $(< 1/2)$ and the coding mode with a large probability $1-p_c$, similar to Ref.[36]. When Bob (or Charlie) chooses the checking-eavesdropping mode, he measures his samples by choosing randomly two sets of single-photon measuring bases Z_d and X_d. Also, they should exploit some special quantum techniques for preventing an eavesdropper from eavesdropping with Trojan horse attack strategies.[40] When Bob (or Charlie) chooses the coding mode, he encodes his information on the message photons with unitary operations, say U_{kl}^{B} (or $U_{k'l'}^{\mathrm{C}}$).

(S3) In order to prevent an eavesdropper from eavesdropping on the quantum communication process freely when the message photons run back from Bob (or Charlie) to Alice, each agent (Bob and Charlie) prepares some d-dimensional decoy photons and inserts them into the positions from which he chooses the photons as samples for the eavesdropping check.

Bob and Charlie can choose two sets of measuring bases to prepare their decoy photons. That is, the MB Z_d is made up of the d eigenvectors as[39,41]

$$|0\rangle, \quad |1\rangle, \quad |2\rangle, \quad \ldots, \quad |d-1\rangle. \tag{7}$$

The MB X_d is made up of the d eigenvectors as

$$\begin{aligned}
|0\rangle_x &= \frac{1}{\sqrt{d}}\left(|0\rangle + |1\rangle \ + \ldots \ + |d-1\rangle\right), \\
|1\rangle_x &= \frac{1}{\sqrt{d}}\left(|0\rangle + \mathrm{e}^{\frac{2\pi \mathrm{i}}{d}}|1\rangle + \ldots \right. \\
&\quad \left. + \mathrm{e}^{\frac{(d-1)2\pi \mathrm{i}}{d}}|d-1\rangle\right), \\
|2\rangle_x &= \frac{1}{\sqrt{d}}\left(|0\rangle + \mathrm{e}^{\frac{4\pi \mathrm{i}}{d}}|1\rangle + \ldots \right. \\
&\quad \left. + \mathrm{e}^{\frac{(d-1)4\pi \mathrm{i}}{d}}|d-1\rangle\right), \\
&\ldots \\
|d-1\rangle_x &= \frac{1}{\sqrt{d}}\left(|0\rangle + \mathrm{e}^{\frac{2(d-1)\pi \mathrm{i}}{d}}|1\rangle + \mathrm{e}^{\frac{2\times 2(d-1)\pi \mathrm{i}}{d}}|2\rangle \right. \\
&\quad \left. + \ldots + \mathrm{e}^{\frac{(d-1)\times 2(d-1)\pi \mathrm{i}}{d}}|d-1\rangle\right).
\end{aligned} \tag{8}$$

The vector $|k\rangle_z$ coming from the MB Z_d and the vector $|l\rangle_x$ coming from the MB X_d satisfy the relation $|{}_z\langle k|l\rangle_x|^2 = 1/d$. After coding on the message photons, Bob (Charlie) replaces the photons sampled for the eavesdropping check with his decoy photons and then sends the sequence S_{B} (S_{C}) back to Alice.

(S4) After receiving the two sequences S_{B} and S_{C}, Alice chooses some pairs as samples for an eavesdropping check with single-photon measurements by choosing randomly two sets of bases Z_d and X_d. She performs d-dimensional Bell-basis measurements on other pairs.

(S5) Alice, Bob and Charlie analyse the security of their transmission. If they confirm that their transmissions are secure, they can create a private key according to the correlation $U^{\mathrm{A}} = U^{\mathrm{B}} \otimes U^{\mathrm{C}}$.

The security analysis includes two steps. One is used for the transmission of the states $|\Psi_{00}\rangle_{\mathrm{BC}}$ from Alice to her two agents Bob and Charlie. The other is used for the transmission of the two sequences S_{B} and S_{C} from Bob and Charlie to Alice. In the first step, Alice should prevent an eavesdropper from stealing freely the information by inserting another spy photon, an invisible photon, or a delay one into the sequence S_{B} or S_{C}. To this end, she requires her two agents Bob and Charlie to insert a filter in front of their devices to filter out the photon signal with an illegitimate wavelength before they code their information on their photons, and then chooses a sufficiently large subset of photons randomly.[40] Each agent splits each sampling signal with a photon beam splitter (PBS: 50/50) and measures the two signals after the PBS by choosing the MB Z_d or X_d randomly. If the multiphoton rate is unreasonably high, Bob (Charlie) terminates the quantum communication and requires Alice to repeat the communication from the beginning. Otherwise, he continues to the next step. In the second

step, each agent first tells Alice which positions the decoy photons are and their states, and then Alice exploits the samples, for which she chooses a suitable MB for single-photon measurements, for the eavesdropping check. Moreover, she should picks up some outcomes from the Bell-basis measurements for checking eavesdropping.

With the first eavesdropping check, Alice and her agents can prevent an eavesdropper from stealing the message with Trojan horse attack strategies.[40] Also, it provides a way for checking the correlation of two photons in the Bell state $|\Psi_{00}\rangle_{\rm BC}$. The second eavesdropping check can prevent a dishonest agent from measuring the message-photon pairs freely with d-dimensional Bell-basis measurements when the pairs run from the honest agent back to Alice. It will make the replacement of the Bell state $|\Psi_{00}\rangle_{\rm BC}$ with another one done by the dishonest agent invalid. As the decoy photons are in some nonorthogonal states, the measurements on them will leave a trace in the outcomes obtained by Alice and her honest agent. If the two processes for the transmission of the photon sequences are secure, this scheme is secure in theory.

As for the decoy photons, each agent can prepare them with a quantum source. Also Bob (Charlie) can obtain some decoy photons by requiring Charlie (Bob) to measure his photon C (B) in the state $|\Psi_{00}\rangle_{\rm BC}$ and then performing a unitary operation on the photon B (C), including the unitary operations $U_{nm}^{\rm C}$ and a d-dimensional Hadamard (H_d) operation.[39] As pointed out in Refs.[39] and [41], a d-dimensional Hadamard (H_d) operation can be written as follows:

$$H_d = \frac{1}{\sqrt{d}} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & {\rm e}^{2\pi {\rm i}/d} & \dots & {\rm e}^{(d-1)2\pi {\rm i}/d} \\ 1 & {\rm e}^{4\pi {\rm i}/d} & \dots & {\rm e}^{(d-1)4\pi {\rm i}/d} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & {\rm e}^{2(d-1)\pi {\rm i}/d} & \dots & {\rm e}^{(d-1)2(d-1)\pi {\rm i}/d} \end{pmatrix}, \quad (9)$$

i.e.,

$$H_d|j\rangle = |j\rangle_x. \quad (10)$$

Certainly, in order to adjust the positions of the decoy photons in the sequence $S_{\rm B}$ ($S_{\rm C}$), Bob (Charlie) can use some delay devices to delay the arrival time of a decoy photon, similar to Ref.[5].

In summary, we have presented a QSS scheme based on quantum superdense coding, following some ideas in Refs.[9] and [36]. This scheme has a higher capacity and intrinsic efficiency than others as each d-dimensional entangled pair can carry 2lb$d$ bits of information and almost all the pairs can be used for carrying useful information in theory.

We would like to thank Dr Deng Fu-Guo for many helpful discussions on this work.

References

[1] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[2] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[4] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302
[5] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315
[6] Li X H, Deng F G and Zhou H Y 2008 *Phys. Rev.* A **78** 022321
[7] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[8] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[9] Liu X S, Long G L, Tong D M and Li F 2002 *Phys. Rev.* A **65** 022304
[10] Grudka A and Wójcik A 2002 *Phys. Rev.* A **66** 014301
[11] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305
[12] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[13] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162
[14] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A **69** 052307
[15] Wei D X, Yang X D, Luo J, Sun X P, Zeng X Z and Liu M L 2004 *Chin. Sci. Bull.* **49** 423
[16] Deng F G, Long G L and Zhou H Y 2005 *Phys. Lett.* A **340** 43
[17] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329
[18] Deng F G, Zhou H Y and Long G L 2006 *J. Phys.* A **39** 14089
[19] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303
[20] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301
[21] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302
[22] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304
[23] Yan F L, Gao T and Li Y C 2008 *Chin. Phys. Lett.* **25** 1187
[24] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[25] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett.* A **324** 420
[26] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301

[27] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Europ. Phys. J.* D **39** 459
[28] Li X H, Zhou P, Li C Y, Zhou H Y and Deng F G 2006 *J. Phys.* B **39** 1975
[29] Zhang Y Q, Jin X R and Zhang S 2006 *Chin. Phys.* **15** 2252
[30] Cheung Y C 2006 *Phys. Scr.* **74** 459
[31] Sheng Y B 2008 *Europ. Phys. J.* D **48** 279
[32] Wang T J 2008 *Physica* A **387** 4716
[33] Man Z X, Xia Y J and An N B 2007 *Europ. Phys. J.* D **42** 333
[34] Wang Z Y, Yuan H, Shi S H and Zhang Z J 2007 *Europ. Phys. J.* D **41** 371
[35] Deng F G, Li C Y, Li Y S, Zhou H Y and Wang Y 2005 *Phys. Rev.* A **72** 022338
[36] Deng F G, Li X H and Zhou H Y 2008 *Phys. Lett.* A **372** 1957
[37] Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
[38] Li C Y, Li X H, Deng F G, Zhou P, Liang Y J and Zhou H Y 2006 *Chin. Phys. Lett.* **23** 2896
[39] Li X H, Deng F G, Li C Y, Liang Y J, Zhou P and Zhou H Y 2006 *J. Korean Phys. Soc.* **49** 1354
[40] Li X H, Deng F G and Zhou H Y 2006 *Phys. Rev.* A **74** 054302
[41] Chen P 2006 *Chin. Phys.* **15** 2228