Circular quantum secret sharing

Institute of Physics Publishing Journal of Physics A: Mathematical and General

J. Phys. A: Math. Gen. **39** (2006) 14089–14099 doi:10.1088/0305-4470/39/45/018

Circular quantum secret sharing

Fu-Guo Deng[1,2,3,4], **Hong-Yu Zhou**[1,2,3] **and Gui Lu Long**[4,5]

[1] The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, People's Republic of China
[2] Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, People's Republic of China
[3] Beijing Radiation Center, Beijing 100875, People's Republic of China
[4] Key Laboratory For Quantum Information and Measurements of Ministry of Education, and Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China
[5] Key Laboratory for Atomic and Molecular Nanosciences, Tsinghua University, Beijing 100084, People's Republic of China

E-mail: fgdeng@bnu.edu.cn and gllong@tsinghua.edu.cn

Received 19 January 2006, in final form 18 August 2006
Published 24 October 2006
Online at stacks.iop.org/JPhysA/39/14089

Abstract
A circular quantum secret sharing protocol is proposed, which is useful and efficient when one of the parties of secret sharing is remote to the others who are in adjacent, especially the parties are more than three. We describe the process of this protocol and discuss its security when the quantum information carrying is polarized single photons running circularly. It will be shown that entanglement is not necessary for quantum secret sharing. Moreover, the theoretic efficiency is improved to approach 100% as almost all the instances can be used for generating the private key, and each photon can carry one bit of information without quantum storage. It is straightforwardly to utilize this topological structure to complete quantum secret sharing with multi-level two-particle entanglement in high capacity securely.

PACS numbers: 03.67.Hk, 03.67.Dd, 03.65.Ud, 89.70.+c

1. Introduction

Secret sharing is a useful tool in classical secure communication [1, 2]. It can be used to accomplish a special task. Suppose a president of a bank, Alice wants to send a secret message to her two agents, Bob and Charlie who are at a distant place for carrying out a business on her behalf. Alice cannot determine whether both of them are honest. There may be at most one dishonest agent among Bob and Charlie pair, but Alice does not know who is the dishonest one. She knows that the honest one will keep the dishonest one from destroying the business if they coexist in the process of the business. For the security of the secret message (S_A), she will split it into two pieces, S_B and S_C, and only sends one to Bob and another to

Charlie respectively. The two pieces of message can be used to reconstruct the secret message S_A when Bob and Charlie collaborate, otherwise none of them can get any useful information about S_A.

Cryptography can be used to complete the task if Alice created a private key K_B (K_C) with Bob (Charlie). For example, if Alice wants to send the message S_B to Bob securely, she can encrypt the message S_B with the private key K_B using the one time-pad crypt-system and then send the ciphertext $C_B = S_B \oplus K_B$ to Bob, where $\oplus$ means modulo 2 summation. With the key K_B, Bob can decrypt C_B to read out the message S_B, but any one else cannot obtain anything about it. Similarly, Alice can encrypt the message S_A with $K_A = K_B \oplus K_C$, i.e., $C_A = S_A \oplus K_A$, and then sends the ciphered text C_A to both of Bob and Charlie. They can get the original message S_A only when they collaborate. In essence, this is the classical secret sharing whose security depends on the privacy of the key K_B and K_C. The distribution of a private key between two remote parties or multi-parties is important for secure communication.

Quantum key distribution (QKD) is an important application of quantum mechanics within the field of information, and it provides a secure way for generating a private key between two remote parties since Bennett and Brassard (BB84) [3, 4]. The secret sharing has been generalized to the quantum scenario by using entanglement [2, 5], namely quantum secret sharing (QSS). Different from classical secret sharing, the shared information in QSS can be both classical and quantum. In particular, QSS is useful for creating a private key among multi-party of secure communications . There have been many theoretical and experimental interests in QSS [6–22]. A pioneering QSS scheme [2], called HBB99 scheme, was proposed by Hillery, Bužek and Berthiaume in 1999 by using three-particle entangled Greenberger–Horne–Zeilinger (GHZ) states. In this scheme, the bank president, Alice prepares a GHZ triplet state

$$|\psi\rangle_{abc} = \frac{1}{\sqrt{2}}(|000\rangle_{abc} + |111\rangle_{abc}), \tag{1}$$

where the state $|0\rangle$ and $|1\rangle$ are two eigenvectors of two-level quantum system, such as the polarization of single photons along the z-direction (σ_z). Alice sends the particle b and c to Bob and Charlie respectively, and keeps the particle a. They all agree that they choose randomly one of the two measuring bases (MBs), σ_x and σ_y to perform the measurement on their particles. When they all choose σ_x or one chooses σ_x and the others choose σ_y, their results are correlated and will be kept for key, otherwise they discard the results. Its intrinsic efficiency for qubits ϵ_q, the ratio of number of valid qubits to the number of transmitted qubits, is about 50% as half of the instances will be abandoned. Subsequently, Karlsson, Koashi and Imoto (KKI) put forward a QSS scheme [5] with two-photon polarization-entangled states, and its efficiency ϵ_q is also 50%.

There is a common feature in the existing QSS protocols, for instance, in [2, 5–18, 21], that the quantum information carrier (QIC) runs only between two parties among the participants, i.e., from Alice to Bob, and from Alice to Charlie in three-party secret sharing, no transmission between Bob and Charlie. In general, Alice is remote to both Bob and Charlie, and Bob and Charlie are likely two adjacent agents. Then they can complete a QSS by making the QIC run a circle, namely, the QIC runs from Alice to Bob, and then from Bob to Charlie, finally back to Alice. Though the change in the process seems small, but it reduces the resource requirement greatly and the intrinsic efficiency is also increased. In this paper, we will present a quantum secret sharing protocol of classical information based on the circular motion idea using polarized single photons. This basic circular transmission idea is not restricted to the use of single photons, but also could be used in other systems and the generalization of the protocol with entangled states is also presented.

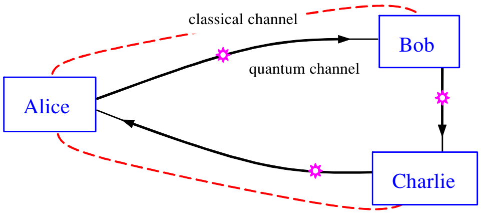

Figure 1. Circular quantum secret sharing. The quantum information carrier runs from Alice to Bob, then to Charlie, and finally back to Alice. Bob and Charlie randomly choose the control mode or the coding mode for each signal. The full line represents the quantum channel and the dashed line for classical channel.

2. Circular quantum secret sharing with polarized single photons

2.1. The circular-QSS protocol with single photons

The basic idea of the circular-QSS protocol with polarized single photons is shown in figure 1. The president, Alice prepares the QICs which are polarized single photons in this QSS protocol, using two sets of measuring basis (MB) into one of the following four states randomly

$$\{|+z\rangle, |-z\rangle, |+x\rangle, |-x\rangle\}, \tag{2}$$

where

$$|+z\rangle = |0\rangle, \qquad |-z\rangle = |1\rangle, \tag{3}$$

$$|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{4}$$

respectively. The states $|\pm z\rangle$ and $|\pm x\rangle$ are the eigenstates of σ_z and σ_x, respectively. Before the quantum communication, Alice, Bob and Charlie agree that Bob and Charlie choose randomly the control mode or the coding mode for the quantum signal received, similar to the Ping-Pong quantum key distribution scheme in [23, 24]. When they choose the control mode, they perform single-photon measurement on the signal using one of the two MBs, σ_z and σ_x randomly and record the MBs and outcomes of the measurements, denoted as R_B and R_C respectively. If they choose the coding mode, they perform randomly one of the two unitary operations, U_0 and U_1 which represent the bits 0 and 1 respectively, on the single photon received,

$$U_0 = |0\rangle\langle 0| + |1\rangle\langle 1|, \tag{5}$$

$$U_1 = |0\rangle\langle 1| - |1\rangle\langle 0|. \tag{6}$$

The operation U_0 is the identity operation and does nothing on the single photon. The nice feature of U_1 operation is that it flips the state in both measuring basis: U_1 negates the states in the two conjugate MBs [25, 26], i.e.,

$$U_1|+z\rangle = -|-z\rangle, \qquad U_1|-z\rangle = |+z\rangle, \tag{7}$$

$$U_1|+x\rangle = |-x\rangle, \qquad U_1|-x\rangle = -|+x\rangle. \tag{8}$$

For creating the private key K_A, Alice sends the quantum signal to Bob first, and Bob chooses the control mode or the coding mode randomly for each photon. If he chooses the control mode, Bob performs measurement on the photon using the MB σ_z or σ_x. Otherwise, he codes the photon with the two unitary operations U_0 and U_1 chosen randomly and then sends it to Charlie. Charlie performs the operation in a way similar to Bob. When he chooses control mode, he measures the photon with one of the two MBs. Otherwise, he sends the photon to Alice after coding with unitary operations. In order to preventing others from eavesdropping with fake signal and cheating [27], Bob should add a small trick. He replaces some photons with his own ones whose states are randomly in one of the four states $\{|+z\rangle, |-z\rangle, |+x\rangle, |-x\rangle\}$. He can produce his photons with an ideal single-photon source or operating some of the samples chosen with the control mode. That is, he performs one of the four operations $\{U_0, U_1, H', H' \otimes U_1\}$ (here H' is the Hadamard operation) on those photons and changes their states into those secret to others. For most of the photons received, Alice performs the single-photon measurement with the same MB as she prepares them. For others, she will measure the photons using one of the two MBs randomly. As the two unitary operations U_0 and U_1 do not change the MB, Alice can get a deterministic outcome for almost all the photons returned, e.g., $U_A = U_B \otimes U_C$, where U_B and U_C are the operations done by Bob and Charlie on the same photon respectively, U_A is the total operation on photon. After Alice receives all the photons, Charlie publishes the positions of his own photons. In this way, Alice can use the deterministic outcomes as a raw key for distilling a private if the quantum communication is secure.

In order to prevent any eavesdropper from getting the information about the key K_A which is represented by U_A when the parties confirm that the whole process of quantum communication is secure, Alice, Bob and Charlie should sample instances twice for analysing the error rates. The first sequence of the samples is those that has been chosen and measured by Bob or Charlie when they choose the control mode. It can be divided into two parts: one contains those measured by Bob, denoted by s_{1b}; the other contains those measured by Charlie, say s_{1c}. The second sample sequence consists of those measured by Alice using the two MBs randomly, say s_2. In this second sample sequence, Bob and Charlie both choose the coding mode, and hence accordingly their coding operations form two coding sequences denoted by s_{2b} and s_{2c}.

For analysing the error rate in samples s_{1b}, Bob publishes the information about the samples s_{1b}, including the positions of the measured photons in the photon sequence he receives from Alice, the MBs and the results of the measurements in s_{1b}, and Alice compares it with the information of these photons. In those cases where Bob has chosen the same measuring-basis as Alice's, Alice can determine the error rate ε_{1b}.

The error rate of the sample sequence s_{1c}, denoted as ε_{1c}, can be similarly determined by Alice and Charlie. But here Charlie first announces the positions of s_{1c} photons, and then Bob is asked to publish his unitary operations he performs on these photons, then Charlie publishes the outcome of his measurement and the corresponding measuring-basis.

To analyse the error rate in the second sample sequence s_2, Alice asks Bob and Charlie to publish the unitary operations of the sampled photons in the sequence. For s_{2b} (s_{2c}), Alice first requires Bob (Charlie) to publish his operations and then Charlie (Bob). If the photon is produced by Charlie, he also announces its state in public. Since Alice's result should be the product of unitary operations of Alice and Bob, Alice can determine the error rate from the announcement of Bob and Charlie.

With these eavesdropping checks, eavesdropper will be detected if he or she has monitored the quantum channel [28]. The details will be discussed shortly.

In essence, the security of this QSS protocol is ensured by the analysis of the error rates in a similar way to the BB84 QKD protocol [4] and its modified version [28]. As each sample for analysing error rate is prepared and measured with the two unbiased bases, the security of this QSS protocol is also the same as that in BB84 protocol and the modified version.

In practical, there are noise and loss in the quantum channel. The methods for error correction and privacy amplification are necessary for distilling the key $K_A = K_B \oplus K_C$, the same as QKD [3, 29].

2.2. Security analysis of the QSS protocol with single photons

Suppose the dishonest one between Bob and Charlie is denoted as Bob*. As discussed in [5], if the dishonest one Bob* can be detected by the other two parties, say Alice and Charlie* when he eavesdrops the quantum communication, then any eavesdropper can be found. We will discuss the security of this circular QSS protocol in two cases with Bob* being Bob, and Charlie respectively.

If Bob* is Bob, the security of this QSS protocol is simplified to prevent Bob from eavesdropping the secret key K_A. In fact, the task of eavesdropping check is to determine whether Bob obtained the information about the unitary operations U_C which is just the key K_C under ideal condition. Any other cheat done by Bob in the process of quantum communication will be found out in secret sharing if Bob cannot get the information about U_C. The fake information that Bob publishes about his operations U_B on s_{1c} will be exposed as it was announced before Charlie publishes the MBs and the results for s_{1c}. In this way, the process for security analysis between Alice and Charlie is equal to that in BB84 QKD [4], which is proved unconditionally secure; for example, see [30–32]. We can calculate the information I_B that Bob can obtain about the unitary operations U_C done by Charlie with the probability of being detected ε_B as follows, in a way similar to those used in [23, 33].

We discuss the security in the case that any eavesdropper can only make individual attacks. The reason is discussed in [34–37]. As discussed in [26], the limitation on the error rate introduced by Bob's eavesdropping is 25% for which Bob intercepts the quantum signal Alice sends to Charlie and sends a fake photon to him. The purpose that Bob eavesdrops the quantum signal is to learn more information about it and introduces as little error as possible into the results. The error rate introduced by Bob comes from the wrong MBs chosen, i.e., Alice prepares the quantum signal with σ_z, but Bob chooses σ_x for eavesdropping, or vice versa [34]. We assume that Alice prepares the quantum states with σ_z and Bob with σ_x for eavesdropping (the condition that Alice chooses σ_x and Bob σ_z is the same for the security analysis). In this way, the information stolen by Bob about the state of the photon coded is equal to that about the operation done by Charlie [23].

The optimal individual attack done by an eavesdropper can be realized by a unitary operation U_E on the photon [23, 29, 34–41] with an ancilla whose initial state is $|0\rangle$.

$$U_E|0\rangle|0\rangle = |0\rangle|0\rangle, \tag{9}$$

$$U_E|1\rangle|0\rangle = \cos\phi|1\rangle|0\rangle + \sin\phi|0\rangle|1\rangle, \tag{10}$$

where $\phi \in [0, \frac{\pi}{4}]$ characterizes the strength of Eve's attack [35].

The probability ε_B that Bob will be detected is the same as the error rate introduced by the eavesdropping [23, 29]. As Alice makes the photon in the four states $\{|+z\rangle, |-z\rangle, |+x\rangle, |-x\rangle\}$ with the same probability, then the error rate is [26, 35]

$$\varepsilon_B = \tfrac{1}{2}\sin^2\phi. \tag{11}$$

The state of the photon that Alice prepares can be described with a density matrix

$$\rho_A = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|. \tag{12}$$

After Bob's eavesdropping, the joint state $\psi_{\Im}$ of the system $\Im$ composed of the photon A and the ancilla [23, 29, 33] P can be written as

$$\begin{aligned}\rho_{AP} = \tfrac{1}{2}\{&|00\rangle\langle 00| + \cos^2\phi|10\rangle\langle 10| + \cos\phi\sin^*\phi|10\rangle\langle 01| \\ &+ \sin\phi\cos^*\phi|01\rangle\langle 10| + \sin^2\phi|01\rangle\langle 01|\},\end{aligned} \tag{13}$$

where $|ij\rangle \equiv |i\rangle_A|j\rangle_P, i, j \in \{0, 1\}$. The effect of the unitary operations done by Charlie is just to change the state of the photon A in ρ_{AP}. Suppose the probabilities that Charlie chooses U_0 and U_1 are P_{c0} and P_{c1}, respectively. After the coding, the state $\psi_{\Im}$ becomes

$$\begin{aligned}\rho'_{AP} = \tfrac{1}{2}\{&P_{c0}|00\rangle\langle 00| + P_{c1}|10\rangle\langle 10| + P_{c0}[\cos^2\phi|10\rangle\langle 10| + \cos\phi\sin^*\phi|10\rangle\langle 01| \\ &+ \sin\phi\cos^*\phi|01\rangle\langle 10| + \sin^2\phi|01\rangle\langle 01|] \\ &+ P_{c1}[\cos^2\phi|00\rangle\langle 00| - \cos\phi\sin^*\phi|00\rangle\langle 11| \\ &- \sin\phi\cos^*\phi|11\rangle\langle 00| + \sin^2\phi|11\rangle\langle 11|]\}.\end{aligned} \tag{14}$$

As Bob wants to eavesdrop the quantum communication for creating a private key, he should send the photon coded to Alice and only measure the ancilla, which is different to that for direct communication [23, 33]. We can trace out the state of the photon A from the joint state $\psi_{\Im}$ with MB σ_z ($\{|0\rangle, |1\rangle\}$) to get the state of the ancilla, ρ'_P,

$$\rho'_P = \tfrac{1}{2}\{(1 + \cos^2\phi)|0\rangle\langle 0| + \sin^2\phi|1\rangle\langle 1|\}, \tag{15}$$

which can be projected to orthogonal measuring basis $\{|0\rangle, |1\rangle\}$ (it is one of the best measurements for distilling the information from the state) and written as

$$\rho''_P = \frac{1}{2}\begin{pmatrix} 1 + \cos^2\phi & 0 \\ 0 & \sin^2\phi \end{pmatrix}. \tag{16}$$

The information I_B that Bob can obtain is equal to the Von Neumann entropy of the state of the ancilla. And the Von Neumann entropy can be calculate as follows [29, 26]:

$$I_B = S(\rho''_P) = -\mathrm{Tr}(\rho''_P \log_2 \rho''_P), \tag{17}$$

i.e.,

$$I_B = S(\rho''_P) = -\sum_{i=0}^{1} \lambda_i \log_2 \lambda_i, \tag{18}$$

where λ_i $(i = 0, 1)$ are the roots of the characteristic polynomial $\det(\rho''_P - \lambda I)$ [23], yielding the two eigenvalues

$$\lambda_0 = \tfrac{1}{2}(1 + \cos^2\phi), \tag{19}$$

$$\lambda_1 = \tfrac{1}{2}\sin^2\phi. \tag{20}$$

So we have

$$\begin{aligned}I_B &= 1 - \tfrac{1}{2}\{(1 + \cos^2\phi)\log_2(1 + \cos^2\phi) + \sin^2\phi\log_2\sin^2\phi\} \\ &= -\varepsilon_B\log_2\varepsilon_B - (1 - \varepsilon_B)\log_2(1 - \varepsilon_B).\end{aligned} \tag{21}$$

The relation between I_B and ε_B is shown in figure 2. It is shown in the figure that Bob has to face a detection probability $\varepsilon_B > 0$ if he wants to gain information $I_B > 0$. If I_B is not small, Bob will be detected, otherwise Alice and Charlie can distil the key K_C with privacy amplification.

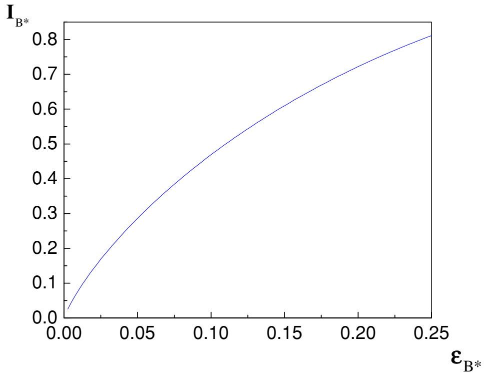

Figure 2. The relation between I_B and ε_B.

If the Bob* is Charlie, the process of eavesdropping check for the sample sequence s_{1b} is the same as in the BB84-QKD protocol [4, 30–32]. The state $\rho_{A''}$ of the photon prepared by Alice is random for Charlie as she chooses randomly one of the two MBs σ_z and σ_x for it.

$$\rho_{A''} = \frac{1}{4}|+z\rangle\langle+z| + \frac{1}{4}|-z\rangle\langle-z| + \frac{1}{4}|+x\rangle\langle+x| + \frac{1}{4}|-x\rangle\langle-x| = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}. \tag{22}$$

The operation U_B done by Bob on the photon does not change the character of the state for Charlie as

$$\rho_{A'''} = \frac{P_{b0}}{4}|+z\rangle\langle+z| + \frac{P_{b1}}{4}|-z\rangle\langle-z| + \frac{P_{b0}}{4}|-z\rangle\langle-z| + \frac{P_{b1}}{4}|+z\rangle\langle+z| + \frac{P_{b0}}{4}|+x\rangle\langle+x| \\ + \frac{P_{b1}}{4}|-x\rangle\langle-x| + \frac{P_{b0}}{4}|-x\rangle\langle-x| + \frac{P_{b1}}{4}|+x\rangle\langle+x| = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \rho_{A''}, \tag{23}$$

where P_{b0} and P_{b1} are the probabilities that Bob chooses the unitary operations U_0 and U_1, respectively. No matter what quantum signal Charlie eavesdrops, the security analysis is the same as BB84-QKD [4]. So this QSS is secure if Bob* is Charlie.

Bob* may cheat in the communication, for instance he publishes a wrong information about his unitary operations U_{B*}, or he does not use the right key K_{B*} in secret sharing. Inevitably, his action can be detected. For example, the wrong information about his unitary operations will be found out when Alice and Charlie compare the results in s_{2c*} in quantum secret sharing. After the key $K_A = K_B \oplus K_C$ is created, the cheat that Bob* does not use K_{B*} for decrypting the ciphered text $C_A = S_A \oplus K_A$ can also be detected before C_A is transmitted. Alice, Bob and Charlie need only determine whether the key $K'_A = K'_B \oplus K'_C$ obtained by combining Bob's key and Charlie's key when they cooperate is identical to her key K_A obtained by Alice's measurement before she sends a secret message to her two remote assistants, Bob and Charlie. The process can be achieved by choosing at random a sufficiently large subset of bits in the key K'_A to compare the results with those in the key K_A. If the error rate is zero, Alice confirms that there is no dishonest one in Bob and Charlie pair, and she sends the secret message to them after encrypting it with the key K_A; otherwise she has to abort the secret message communication.

The parties encode the photons with unitary operations and each photon can carry one bit of information in K_A in principle. The efficiency for qubit is improved to approach 100%. Moreover, they do not exchange the information about the MBs for almost all the instances, and they also need not store the single photons.

3. Circular quantum secret sharing with multi-level two-particle entanglement

For two-particle quantum system, *d*-dimension Bell-basis states in a symmetric quantum channel are [42–46]

$$|\Psi_{nm}\rangle = \sum_j \mathrm{e}^{2\pi ijn/d}|j\rangle \otimes |j+m \bmod d\rangle/\sqrt{d}, \tag{24}$$

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

$$U_{nm} = \sum_j \mathrm{e}^{2\pi ijn/d}|j+m \bmod d\rangle\langle j| \tag{25}$$

can transform the Bell-basis state

$$|\Psi_{00}\rangle = \sum_j |j\rangle \otimes |j\rangle/\sqrt{d} \tag{26}$$

into the Bell-basis state $|\Psi_{nm}\rangle$, i.e., $U_{nm}|\Psi_{00}\rangle = |\Psi_{nm}\rangle$. For two-party communication, one particle can carry $\log_2 d^2$ bits of information while running forth and back. In a more generalized case, non-symmetric quantum channel is possible where the two particles of the entangled quantum system have the different dimensions [46, 47], for example, the first particle has p dimensions and the second one has q dimensions. Then the capacity is $\log_2 pq$.

The source coding capacity of this circular QSS can be improved largely with superdense coding [42, 45, 46] and quantum state storage [48–50]. We will generalize this circular QSS with Einstein–Podolsky–Rosen (EPR) pairs, two-particle maximally entangled states, following the ideas in dense coding [42]. The case for other multi-level two-particle entanglement is just the same as it.

An EPR pair can be in one of the four Bell states [29, 51],

$$|\psi^-\rangle_{HT} = \tfrac{1}{\sqrt{2}}(|0\rangle_H|1\rangle_T - |1\rangle_H|0\rangle_T), \tag{27}$$

$$|\psi^+\rangle_{HT} = \tfrac{1}{\sqrt{2}}(|0\rangle_H|1\rangle_T + |1\rangle_H|0\rangle_T), \tag{28}$$

$$|\phi^-\rangle_{HT} = \tfrac{1}{\sqrt{2}}(|0\rangle_H|0\rangle_T - |1\rangle_H|1\rangle_T), \tag{29}$$

$$|\phi^+\rangle_{HT} = \tfrac{1}{\sqrt{2}}(|0\rangle_H|0\rangle_T + |1\rangle_H|1\rangle_T). \tag{30}$$

The four local unitary operations U_{Li} ($i = 0, 1, 2, 3$) can transfer the four Bell states into each other.

$$U_{L0} = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \tag{31}$$

$$U_{L1} = \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|, \tag{32}$$

$$U_{L2} = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|, \tag{33}$$

$$U_{L3} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{34}$$

i.e.,

$$I \otimes U_{L0}|\psi^\pm\rangle = |\psi^\pm\rangle, \qquad I \otimes U_{L0}|\phi^\pm\rangle = |\phi^\pm\rangle, \tag{35}$$

$$I \otimes U_{L1}|\psi^\pm\rangle = |\phi^\mp\rangle, \qquad I \otimes U_{L1}|\phi^\pm\rangle = -|\psi^\mp\rangle, \tag{36}$$

$$I \otimes U_{L2}|\psi^\pm\rangle = |\phi^\pm\rangle, \qquad I \otimes U_{L2}|\phi^\pm\rangle = |\psi^\pm\rangle, \tag{37}$$

$$I \otimes U_{L3}|\psi^\pm\rangle = -|\psi^\mp\rangle, \qquad I \otimes U_{L3}|\phi^\pm\rangle = |\phi^\mp\rangle. \tag{38}$$

The process of this QSS with EPR pairs is similar to that with single photons discussed above. The president, Alice prepares the two-particle entangled state $|\psi^-\rangle_{HT}$, and she keeps the particle H and sends the particle T to Bob first, shown in figure 1. He chooses the control mode and the coding mode randomly. When Bob chooses the coding mode, he performs one of the four unitary operations U_{Li} ($i = 0, 1, 2, 3$) which represent the bits 00, 01, 10 and 11 respectively, on the particle T randomly. Otherwise, he chooses the two MBs, σ_z and σ_x to measure the particle T, and tells Alice which particle he chooses the control mode. Alice does the correlated measurement on the particle H in the EPR pair in which Bob measures the particle T, that is, Bob tells Alice the position of the particle and his MB for it, and Alice performs the measurement with the same MB as Bob on the particle H.

As for Charlie, after he receives the particle that Bob sends to him after coding with an unitary operation, Charlie chooses randomly the control mode and the coding mode. If he chooses the coding mode, he performs randomly one of the four coding operations and then sends the particle to Alice (he also replaces some photons with his own ones). When Bob chooses the control mode, he measures the particle choosing randomly one of the two MBs σ_z and σ_x.

The eavesdropping check can be adapted here straightforwardly. In fact, no matter who the dishonest Bob* is, the way for checking the security of quantum communication is the same as that for the BBM-QKD [52] which has been proven unconditionally secure for key generation [36, 53]. As pointed out by Bechmann-Pasquinucci and Peres [54], the QKD with multi-level quantum system is more secure than that with two-level one.

4. Discussion and conclusion

In general, QSS is accomplished with entanglement, which normally requires more complicated experimental set-ups. Though big progress has been made for producing and measuring entanglement, the efficiency is still low [55–57]. QSS with single photons will be more convenient for being implemented in laboratory and practical application. On the other hand, the source coding capacity of QSS can be improved largely with super-dense coding in which entanglement is necessary. With development of technology, it is likely feasible to implement QSS based on entanglement, especially with multi-level entanglement in high capacity.

Certainly, another important function of QSS is to split a secret message into n pieces and completes the task of an $m - out - of - n$ quantum secret splitting scheme, or so-called (m, n) threshold scheme [5]. Unfortunately, this circular QSS scheme cannot be used to accomplish the full goal of quantum secret splitting. That is, it cannot be used for $m - out - of - n$ scheme in which any m parties can reconstruct the secret message when they collaborate. However, it is useful for accomplish a partial goal, $n - out - of - n$ scheme. In other words, the circular QSS can be used to reconstruct the secret message when all of the other n parties cooperate with some classical information published by Alice, the president.

In summary, a circular QSS scheme is proposed. It is useful and efficient when the president Alice is remote to all her agents, Bobs who are in adjacent, especially the parties of secret sharing are more than three. In this scheme, the quantum information carrier, single photons or entangled particles, will run circularly, and the parties choose randomly the control mode or coding mode to operate the QIC. They measure the QIC only when they choose control mode, otherwise, they encode the QIC with some unitary operations. If the QIC is single photon, all the parties of communication including Alice do not need to store the quantum state. If the QIC is entangled quantum system, only Alice is required to possess the technique of quantum storage, others need not. This is convenient for realizing QSS in practical application. Moreover, each QIC can be used to carry information except for the samples for eavesdropping check, and classical information exchanged is reduced largely as the parties need not announce the MBs for the QIC.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under grant nos. 10604008, 10435020, 10254002, A0325401, 60433050 and 10325521, the National Fundamental Research Program under grant no. 001CB309308, the SRFDP program of Education Ministry of China.

References

[1] Blakley G R 1979 *Proc. American Federation of Information Processing 1979 National Computer Conference (American Federation of Information Processing, Arlington, VA, 1979)* pp 313–7
Shamir A 1979 *Commun. ACM* **22** 612
[2] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[4] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York)* pp 175–9
[5] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162
[6] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[7] Gottesman D 2000 *Phys. Rev.* A **61** 042311
[8] Bandyopadhyay S 2000 *Phys. Rev.* A **62** 012308
[9] Nascimento A C A, Mueller-Quade J and Imai H 2001 *Phys. Rev.* A **64** 042311
[10] Karimipour V, Bahraminasab A and Bagherinezhad S 2002 *Phys. Rev.* A **65** 042320
[11] Tyc T and Sanders B C 2002 *Phys. Rev.* A **65** 042310
[12] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247
[13] Bagherinezhad S and Karimipour V 2003 *Phys. Rev.* A **67** 044302
[14] Sen A, Sen U and Zukowski M 2003 *Phys. Rev.* A **68** 032309
[15] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A **69** 052307
Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329
Deng F G, Long G L and Zhou H Y 2005 *Phys. Lett.* A **340** 43
[16] Deng F G, Long G L, Wang Y and Xiao L 2004 *Chin. Phys. Lett.* **21** 2097
[17] Zhang Z J, Li Y and Man Z X 2005 *Phys. Rev.* A **71** 044301
Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302
[18] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett.* A **324** 420
[19] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301
Deng F G *et al* 2006 *Euro. Phys. J.* D **39** 459
[20] Deng F G, Li C Y, Li Y S, Zhou H Y and Wang Y 2005 *Phys. Rev.* A **72** 022338
Li X H *et al* 2006 *J. Phys. B: At. Mol. Opt. Phys.* **39** 1975
[21] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev.* A **63** 042301
[22] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 *Phys. Rev. Lett.* **92** 177903
Lance A M, Symul T, Bowen W P, Sanders B C, Tyc T, Ralph T C and Lam P K 2005 *Phys. Rev.* A **71** 033814
[23] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[24] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601
[25] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
[26] Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311
[27] Deng F G *et al* 2006 *Preprint* quant-ph/0604060
[28] Lo H K *et al* 2005 *J. Crytool.* **18** 133
[29] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge, UK: Cambridge University Press)
[30] Lo H K and Chau H F 1999 *Science* **283** 2050
[31] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[32] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304
[33] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[34] Fuchs C A, Gisin N, Griffiths R B, Niu C S and Peres A 1997 *Phys. Rev.* A **56** 1163
Griffiths R B and Niu C S 1997 *Phys. Rev.* A **56** 1173
Niu C S and Griffiths R B 1999 *Phys. Rev.* A **60** 276
[35] Scarani V and Gisin N 2001 *Phys. Rev. Lett.* **87** 117901
[36] Inamori H, Rallan L and Vedral V 2001 *J. Phys. A: Math. Gen.* **34** 6913
[37] Sen(De) A, Sen U and Żukowski M 2003 *Phys. Rev.* A **68** 032309
[38] Preskill J http://www.theory.caltech.edu/preskill/ph229
[39] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901
[40] Degiovanni I P, Berchera I R, Castelletto S, Rastello M L, Bovino F A, Colla A M and Castagnoli G 2004 *Phys. Rev.* A **69** 032310
Wójcik A 2005 *Phys. Rev.* A **71** 016301
Degiovanni I P, Berchera I R, Castelletto S, Rastello M L, Bovino F A, Colla A M and Castagnoli G 2005 *Phys. Rev.* A **71** 016302
[41] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[42] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[43] Bennett C H *et al* 1993 *Phys. Rev. Lett.* **70** 1895
[44] Zeng B, Liu X S, Li Y S and Long G L 2002 *Commun. Theor. Phys.* **38** 537
[45] Liu X S, Long G L, Tong D M and Li F 2002 *Phys. Rev.* A **65** 022304
[46] Grudka A and Wójcik A 2002 *Phys. Rev.* A **66** 014301
[47] Yan F L and Wang M Y 2004 *Chin. Phys. Lett.* **21** 1195
[48] Liu C, Dutton Z, Behroozi C H and Hau L V 2001 *Nature (London)* **409** 490
[49] Philips D F, Fleischhauer A, Mair A, Walsworth R L and Lukin M D 2001 *Phys. Rev. Lett.* **86** 783
[50] Sun C P, Li Y and Liu X F 2003 *Phys. Rev. Lett.* **91** 147903
[51] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302
Deng F G, Liu X S, Ma Y J, Xiao L and Long G L 2002 *Chin. Phys. Lett.* **19** 893
Li C Y, Zhou H Y, Wang Y and Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
[52] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[53] Waks E, Zeevi A and Yanamoto Y 2002 *Phys. Rev.* A **65** 052310
[54] Bechmann-Pasquinucci H and Peres A 2000 *Phys. Rev. Lett.* **85** 3313
[55] Bouwmeester D *et al* 1999 *Phys. Rev. Lett.* **82** 1345
[56] Pan J -W *et al* 2001 *Phys. Rev. Lett.* **86** 4435
[57] Zhao Z *et al* 2004 *Nature* **430** 54