Science in China Series G: Physics, Mechanics & Astronomy

An efficient quantum secret sharing protocol with orthogonal product states

YANG YuGuang[1,2†], WEN QiaoYan[3] & ZHU FuChen[4]

[1] School of Computer, Beijing University of Technology, Beijing 100022, China;
[2] State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100022, China;
[3] School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;
[4] National Key Laboratory for Modern Communications, Chengdu 610041, China

An efficient quantum secret sharing protocol with orthogonal product states in the $3\otimes 3$ Hilbert space is presented. The particles in the orthogonal product states form two particle sequences. One sequence is sent to Bob and the other is sent to Charlie after rearranging the particle orders. With the help of Alice, Bob and Charlie make the corresponding local measurement to obtain the information of the orthogonal product states prepared. This protocol has many distinct features such as great capacity and high efficiency.

quantum secret sharing, orthogonal product state, orthogonal measurement

Quantum secret sharing (QSS) is a quantum counterpart of classical secret sharing[1]. Now, there are many theoretical and experimental studies on QSS, for instance in refs. [2−16]. QSS provides a secure way for sharing not only classical information[2−10] but also a quantum secret[11−16]. Most existing QSS protocols use entangled states and the participants choose randomly one of two sets of measuring bases (MBs), for example the protocols proposed in refs. [2−7, 11, 12]. The intrinsic efficiency of some protocols is nearly 50%, for example the protocols in refs. [2,3]. Some techniques from quantum key distribution (QKD) for improving the intrinsic efficiency[6,17,18] can be used for improving their efficiency in some QSS protocols. For example, the favored-measuring-basis technique[17] and the measuring-basis-encrypted technique[18] are extended to the multiparty QSS schemes in ref. [7]. In the measuring-basis-encrypted QSS scheme, a three-party control key is generated first among the three parties, and it is used repeatedly to control the use of the alternative MBs. In ref. [19], Deng et al. proposed an efficient quantum secret sharing scheme with

Received September 6, 2006; accepted November 17, 2006
doi: 10.1007/s11433-007-0028-8
†Corresponding author (email: yangyang7357@sina.com)
Supported by the National High-Tech Research and Development Program of China (Grant Nos. 2006AA01Z419 & 2006AA01Z440), the Major Research Plan of the National Natural Science Foundation of China (Grant No. 90604023), the National Research Foundation for the Doctoral Program of Higher Education of China (Grant No. 20040013007), the National Laboratory for Modern Communications Science Foundation of China (Grant No. 9140C1101010601) and the Open Foundation of State Key Laboratory of Information Security (Graduate University of Chinese Academy of Sciences)

Einstein-Podolsky-Rosen pairs which employs dense coding[20] and an order-rearrangement idea[21]. The basic idea of order-rearrangement is that the sender, Alice, mixes up the correct correlation of the particles in the EPR pairs so that Eve does not know which two particles are the particles in an EPR pair and he cannot perform Bell-basis measurement to steal the secret information. Later Alice restores the correct correspondence of particles and obtains the result with Bell-basis measurement. The idea of order-rearrangement has been introduced into quantum secure direct communication, for example the protocols in refs. [22, 23].

Entanglement is not necessary in quantum secret sharing. In ref. [8], Guo et al. proposed a QSS protocol without entanglement based on a modified BB84 QKD protocol and the efficiency is improved to approach 100%, with the use of quantum data storage. In ref. [9], based on a quantum secure direct communication (QSDC) protocol[24], Zhang et al. proposed a (n, n)-threshold scheme of multiparty quantum secret sharing of classical messages (QSSCM) using only single photons. In ref. [25], Deng et al. presented quantum secret sharing and secret splitting protocols with single photons running forth and back between the participating parties. In ref. [26], Hsu et al. proposed three quantum secret sharing protocols using product states. The first two protocols adopt the quantum key distribution protocol using product states[27]. In the third proposed protocol, three-level Bell states are exploited for qutrit preparation via nonlocality swapping. However, about half of the outcomes have to be dropped.

In this paper, we present an efficient quantum secret sharing protocol with orthogonal product states in the $3\otimes 3$ Hilbert space. Our protocol employs the order-rearrangement idea[21]. The particles in the orthogonal product states form two particle sequences. One sequence is sent to Bob and the other is sent to Charlie after rearranging the particle orders. Bob and Charlie make the corresponding local orthogonal measurement to obtain the information of the state sent by Alice. The information that Alice wants to send exists in the correlation of particles in the orthogonal product states. This protocol has many distinct features such as great capacity and high efficiency.

The proposed QSS scheme has three advantages. Firstly, there is no need to prepare any entanglement. Secondly, the intrinsic efficiency is nearly 100%, and all the particles in the orthogonal product states except those used for eavesdropping check are retained for secret sharing. Lastly, each orthogonal product state carries 3 bits of information because one state in a complete set is not used.

1 Quantum secret sharing scheme

For $3\otimes 3$ system, one of the two-qutrit bases in a complete set $\{|\Psi_l>\}$ is as follows:

$$\begin{aligned}
\Psi_1 &= |0>_B \frac{1}{\sqrt{2}}(|0>_C + |2>_C),\\
\Psi_2 &= \frac{1}{\sqrt{2}}(|1>_B + |2>_B)|2>_C,\\
\Psi_3 &= |2>_B \frac{1}{\sqrt{2}}(|0>_C + |1>_C),\\
\Psi_4 &= \frac{1}{\sqrt{2}}(|0>_B + |1>_B)|1>_C,\\
\Psi_5 &= \frac{1}{\sqrt{2}}(|0>_B - |1>_B)|1>_C,
\end{aligned} \tag{1}$$

$$\Psi_6 = |2\rangle_B \frac{1}{\sqrt{2}}(|0\rangle_C - |1\rangle_C),$$

$$\Psi_7 = \frac{1}{\sqrt{2}}(|1\rangle_B - |2\rangle_B)|2\rangle_C,$$

$$\Psi_8 = |0\rangle_B \frac{1}{\sqrt{2}}(|0\rangle_C - |2\rangle_C),$$

$$\Psi_9 = |1\rangle_B|0\rangle_C,$$

where the subscripts B, C denote the particles of Bob and Charlie, respectively.

For $3 \otimes 3$ system, we just write out one of the various complete base forms, and still 17 complete sets of product states possess nonlocality without entanglement[26].

An ordered N orthogonal product state sequence is denoted by [P_1(B); P_1(C); P_2(B); P_2(C);…; P_i(B); P_i(C);…;P_N(B); P_N(C)]. We denote P_i(B) for one particle for Bob in the ith orthogonal product state, and P_i(C) for Charlie, i = 1, 2,…, N. We can take one particle P_i(B) from each orthogonal product state (P_i(B); P_i(C)) to form the first particle sequence [P_1(B), P_2(B), P_3(B),..., P_N(B)]. The remaining particles form the second particle sequence [P_1(C), P_2(C), P_3(C),..., P_N(C)].

Because the information is encoded in the orthogonal product states, to guard the secret information from eavesdropping, Alice cannot allow Eve to acquire simultaneously both particles in the orthogonal product states. If the correct correspondences of particles in the orthogonal product states are mixed up, Eve cannot know which two particles are in the same orthogonal product state. For example, the order of the first particle sequence [P_1(B), P_2(B), P_3(B), ..., P_N(B)] is maintained throughout the transmission process. And the order of the second one [P_1(C), P_2(C), P_3(C), ..., P_N(C)] is rearranged according to the order-rearrangement operations performed by Alice. What he can do is just to guess this correspondence. Inevitably, he will cause significant errors in the data if he tries to eavesdrop. Depicted in Figure 1[21] is an example of four such rearrangement operations. Operation E0 = I is the identity operation and no change is made to the second particle sequence. If the rearrangement operation is E1, Alice exchanges the order of particles 1 and 2, and particles 3 and 4 in the second particle sequence. Without knowing the correct particle correspondence, Eve's joint orthogonal measurement will obtain no useful information and cause errors. This leaves his trace in the results, and the participants can find Eve by checking a subset of results of their measurement.

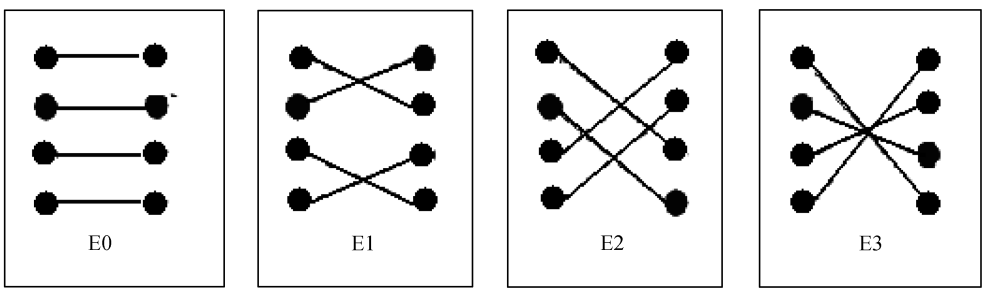

Figure 1 Order-rearrangement operation[21].

Now we first give the details of the QSS scheme. For simplicity, we fix the number of the orthogonal product states in each group to four, and the number of rearrangement operations is also restricted to four. There are two phases in this QSS scheme: preparation phase and revealing phase.

In this scheme, we do not use the state $|1>_B|0>_C$ because the nonlocality in the complete set in eq. (1) is preserved even if the $|1>_B|0>_C$ state is excluded[28]. So each product state can carry three-bit information.

Preparation phase:

(1) Alice, Bob and Charlie agree that Ψ_1, Ψ_2, Ψ_3, Ψ_4, Ψ_5, Ψ_6, Ψ_7, Ψ_8 represent classical information 000, 001, 010, 011, 100, 101, 110, 111, respectively.

(2) Alice prepares a sequence of particles [P_1(B); P_1(C); P_2(B); P_2(C);…; P_i(B); P_i(C);…; P_M(B); P_M(C)] randomly in one of the nine orthogonal product states except $|1>_B|0>_C$. Alice makes a record of the orthogonal product states. These particles are divided into groups, and each group has four orthogonal product states.

(3) Alice takes a particle from each orthogonal product state in a group and sends these four particles in its original order through the AB channel to Bob. Alice makes an order rearrangement operation to the remaining four particles using randomly one of four operations shown in Figure 1, and then sends them through the AC channel to Charlie.

(4) After Bob and Charlie receive the particles, Alice publishes the order rearrangement operation for each group. With this information, Bob and Charlie get the correct correspondences of their particles.

(5) According to her record of the orthogonal product states, Alice chooses the positions of particles randomly and firstly requires Bob(Charlie) to make a local orthogonal measurement on the basis of $\{|0>,|1>,|2>\}$ and publish his outcomes. According to the outcomes of measurement of Bob(Charlie), Charlie(Bob) makes the conditioned local orthogonal measurement and publishes his outcomes. For example, if the outcome obtained by Bob(Charlie) is $|2>$, Charlie(Bob) makes a conditioned local orthogonal measurement on the basis of $\left\{\frac{1}{\sqrt{2}}(|0>+|1>), \frac{1}{\sqrt{2}}(|0>-|1>), |2>\right\}$ $\left(\left\{|0>, \frac{1}{\sqrt{2}}(|1>+|2>), \frac{1}{\sqrt{2}}(|1>-|2>)\right\}\right)$.

(6) According to their outcomes, Alice makes the error rate analysis. If the error rate is lower than the threshold ε_{th}, Bob and Charlie retain the remaining particles for use in the revealing phase. Otherwise, Alice abandons this QSS scheme.

Revealing phase:

(7) To recover the full secret, Bob and Charlie have to need Alice's help. According to her record of the orthogonal product states, Alice firstly requires Bob(Charlie) to make a local orthogonal measurement on the basis of $\{|0>,|1>,|2>\}$. After Bob(Charlie) makes an orthogonal measurement, he tells his outcomes to the other receiver secretly.

(8) The other receiver, Charlie(Bob), performs the conditioned local measurement and keeps his outcomes secretly.

(9) To check if the possible dishonest receiver exists, Alice divides their outcomes into two subsets: one subset, Bob performs the first local measurement; and the other subset, Charlie performs the first local measurement. Alice chooses some outcomes from each subset randomly, respectively and requires them to publish their outcomes. If the error rates are tolerable, Alice considers that no dishonest receiver exists. Otherwise, she abandons this QSS scheme.

Now we will describe this scheme in detail. Steps (1) and (2) are obvious. Let us explain step (3). The goal of step (3) is to mix up the correct correspondences of particles in the orthogonal product states so that Eve cannot know which two particles are in the same orthogonal product state. Suppose Eve intercepts the qutrits $P_i(B)$ and $P_j(C)$, then Eve can perform some joint measurement on the qutrits $P_i(B)$ and $P_j(C)$ on the basis of eq. (1). However, possibly the qutrits $P_i(B)$ and $P_j(C)$ are not an orthogonal product state in eq. (1) and his measurement will cause errors. Eve still takes another strategy to obtain the information of single particle $P_i(B)$ ($P_j(C)$) by performing the local measurement on $P_i(B)$ ($P_j(C)$). However, because the qutrit $P_i(B)$ ($P_j(C)$) is chosen from the nonorthogonal set $\left\{|0>_B, \frac{1}{\sqrt{2}}(|1>_B+|2>_B), \quad |2>_B, \frac{1}{\sqrt{2}}(|0>_B+|1>_B), \quad \frac{1}{\sqrt{2}}(|0>_B-|1>_B), \right.$ $\left. \frac{1}{\sqrt{2}}(|1>_B-|2>_B)\right\}$ $\left(\left\{ \frac{1}{\sqrt{2}}(|0>_C+|2>_C), |2>_C, \frac{1}{\sqrt{2}}(|0>_C+|1>_C), |1>_C, \frac{1}{\sqrt{2}}(|0>_C-|1>_C), \right.\right.$ $\left.\left. \frac{1}{\sqrt{2}}(|0>_C-|2>_C)\right\}\right)$, according to the Heisenberg uncertainty principle of quantum mechanics, Eve's local measurement will obtain no useful information and cause errors. In step (4), Bob and Charlie get the correct correspondences of their particles. That is, Bob and Charlie's *i*th qutrits are $P_i(B)$ and $P_i(C)$, respectively. Step (5) is used to detect possible eavesdropping attack. Suppose Alice announces the state information for the *i*th qutrit pair. For the present discussion, we suppose Bob is honest. In the error-free case, Alice expects that Bob and Charlie can find some $P_i(B)$ and $P_i(C)$. However, deception can be detected if receivers announce wrong outcomes on the appropriate measurement basis. For example, if the state prepared is Ψ_2, then Alice firstly requires Charlie to make a local measurement on the basis of $\{|0>,|1>,|2>\}$ and publish his outcome. In the error-free case, Charlie obtains the $|2>$. If Charlie obtains the $|0>$ or $|1>$, Alice considers that either Eve exists or Charlie is dishonest. This QSS scheme fails. If Charlie obtains the $|2>$, according to the outcome of measurement of Charlie, Bob makes the conditioned local orthogonal measurement on the basis of $\left\{\frac{1}{\sqrt{2}}(|1>+|2>), \frac{1}{\sqrt{2}}(|1>-|2>), |0>\right\}$ and publishes his outcome. If Bob obtains the $\frac{1}{\sqrt{2}}(|1>-|2>)$ or $|0>$, then Alice considers that either Eve exists or Charlie is dishonest. In the cases for the other states prepared by Alice, the analysis is similar. In step (6), Alice makes the error rate analysis. In the revealing phase, we can suppose that no eavesdropper, Eve, but a dishonest agent possibly exists. Here, we still suppose Bob is honest. Steps (7) and (8) are used to recover the secret by Bob and Charlie with the help of Alice. In step (9), Alice checks if the possible dishonest agent exists. Similar to the above example, Bob knows Charlie's measurement outcome is $|2>$. If his outcome is $|0>$, then Bob immediately knows that Charlie is dishonest. For the case with the outcome $\frac{1}{\sqrt{2}}(|1>-|2>)$ of Bob, Alice can check dishonest agent's existence by further comparing some outcomes. If Charlie himself wants to obtain the state information prepared only by guessing after he performs the first local measurement without the help or authorization of Bob, he obtains either three-bit full information or zero-bit information. For example, if Charlie's measurement outcome is $|2>$, he guesses the state prepared is Ψ_2 or

Ψ_7. These two states Ψ_2 and Ψ_7 represent 001, 110, respectively. The encoding of the states prepared different from that in ref. [26] reduces the eavesdropper's mutual information.

2 Security analysis

Now, we consider the security of the present scheme. Recall that four possible states $\left(\left\{|0>, |1>, \frac{1}{\sqrt{2}}(|0>-|1>), \frac{1}{\sqrt{2}}(|0>+|1>)\right\}\right)$ are exploited in the BB84 protocol. This scheme can be regarded as the hybrid of three BB84 protocols based on three different sets of four states $\left\{|i>, |j>, \frac{1}{\sqrt{2}}(|i>-|j>), \frac{1}{\sqrt{2}}(|i>+|j>)\right\}$, where (i, j) are (0,1), (1,2), (2,0), respectively. The permutation of particles and the eavesdropping check in steps (5) and (9) can find the possible eavesdropping with higher probability than the BB84 protocol.

Now we just consider some possible attacks.

2.1 Misstate strategy

Since Bob and Charlie have to discuss Alice's preparation, the intuitive cheating is to lie to the honest receiver. If the eavesdropper is Charlie, the simplest method of cheating is to misstate local measurement outcomes to the other receiver. However, such deception can be detected in steps (9) (Note that Charlie can only take this strategy in the revealing phase) because Alice can choose a portion of such outcomes to compare.

2.2 Intercept-resend strategy

In the present scheme, the eavesdropper can perform any joint measurement. However, only when the eavesdropper performs a correct collective or local measurement on these two intercepted qutrits can the eavesdropper access full secret information. Otherwise, the eavesdropper will fail to know the secret. For example, the eavesdropper intercepts the qutrits P_i(B) and P_j(C) with the state $|0>\otimes|2>$. If the eavesdropper performs the measurement on the basis of eq. (1), then he will get $|0>\frac{1}{\sqrt{2}}(|0>\pm|2>)$ with equal probability $\frac{1}{2}$ and his measurement will cause error.

Moreover, the no-cloning theorem guarantees that a perfect clone of possible nonorthogonal states is impossible.

2.3 Coherent measurement attack strategy

For the eavesdropper, the possible states after Alice's order-rearrangement operation are non-orthogonal and he never distinguishes them deterministically. So this scheme indeed has the same essence as BB84-type protocols. Next we consider the case of coherent measurement attack. Coherent measurement attack for BB84-type protocols has been discussed in refs. [29, 30] where they are proved to be secure. So this scheme is also secure.

In addition, under practical conditions, the detection efficiency is not equal to 1, and the quantum channel is noisy. These details of security analysis are important and merit detailed analysis,

and will not be studied in this paper.

3 Conclusion

An efficient quantum secret sharing protocol with orthogonal product states in the $3 \otimes 3$ Hilbert space is presented. The particles in the orthogonal product states form two particle sequences. One sequence is sent to Bob and the other is sent to Charlie after rearranging the particle orders. Bob and Charlie make local measurement and cooperate to obtain the full information of the orthogonal product states sent by Alice. This protocol has many distinct features such as great capacity and high efficiency.

In addition, using the idea of order-rearrangement[21], the orthogonal product states can be replaced with other states such as EPR entangled states.

1 Shamir A. How to share a secret. Commun ACM, 1979, 22(11): 612－613
2 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829－1834
3 Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59: 162－168
4 Bandyopadhyay S. Teleportation and secret sharing with pure entangled states. Phys Rev A, 2000, 62: 012308－012312
5 Karimipour V, Bahraminasab A, Bagherinezhad S. Entanglement swapping of generalized cat states and secret sharing. Phys Rev A, 2002, 65: 042320－042324
6 Deng F G, Long G L, Wang Y, et al. Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement. Chin Phys Lett, 2004, 21: 2097－2100
7 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69: 052307－052311
8 Guo G P, Guo G C. Quantum secret sharing without entanglement. Phys Lett A, 2003, 310: 247－251
9 Zhang Z J, Man Z X. Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys Rev A, 2005, 72: 022303－022306
10 Zhang Z J, Li Y, Man Z X. Multiparty quantum secret sharing. Phys Rev A, 2005, 71: 044301－044304
11 Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys Rev Lett, 1999, 83: 648－651
12 Li Y M, Zhang K S, Peng K C. Multiparty secret sharing of quantum information based on entanglement swapping. Phys Lett A, 2004, 324: 420－424
13 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: 044301－044304
14 Deng F G, Li C Y, Li Y S, et al. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys Rev A, 2005, 72: 022338－022345
15 Yan F L, Gao T. Quantum secret sharing between multiparty and multiparty without entanglement. Phys Rev A, 2005, 72: 012304－012308
16 Tittel W, Zbinden H, Gisin N. Experimental demonstration of quantum secret sharing. Phys Rev A, 2001, 63: 042301－042306
17 Lo H K, Chau H F, Ardehali M. Efficient quantum key distribution scheme and proof of its unconditional security. J Cryptology, 2005, 18: 133－164
18 Hwang W Y, Koh I G, Han Y D. Quantum cryptography without. public announcement of bases. Phys Lett A, 1998, 244: 489－493
19 Deng F G, Long G L, Zhou H Y. An efficient quantum secret sharing scheme with Einstein-Podolsky-Rosen Pairs, arxiv: quant-ph/0504120
20 Bennett C H, Wiesner S J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys Rev Lett, 1992, 69: 2881－2884
21 Deng F G, Long G L. Controlled order rearrangement encryption for quantum key distribution. Phys Rev A, 2003, 68: 042315－042318

22 Zhu A D, Xia Y, Fan Q B, et al. Secure direct communication based on secret transmitting order of particles. Phys Rev A, 2006, 73: 022338－022341
23 Wang J, Zhang Q, Tang C J. Quantum secure direct communication based on order rearrangement of single photons. Phys Lett A, 2006, 358: 256－260
24 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319－052322
25 Deng F G, Long G L. Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys Rev A, 2004, 70: 012311－012317
26 Hsu L Y, Li C M. Quantum secret sharing using product states. Phys Rev A, 2005, 71: 022321－022329
27 Guo G P, Li C F, Shi B S, et al. Quantum key distribution scheme with orthogonal product states. Phys Rev A, 2001, 64: 042301－042304
28 Bennett C H, DiVincenzo D P, Fuchs C A, et al. Quantum nonlocality without entanglement. Phys Rev A, 1999, 59: 1070－1091
29 Cirac J I, Gisin N. Coherent eavesdropping strategies for the 4 state quantum cryptography protocol, arXiv: quant-ph/9702002 v1
30 Bechmann-Pasquinucci H, Gisin N. Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography, arXiv:quant-ph/9807041 v2