Vol 16 No 10, October 2007
1009-1963/2007/16(10)/2875-05

Chinese Physics

© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

A (2, 3) quantum threshold scheme based on Greenberger–Horne–Zeilinger state*

Li Yuan(李 渊)† and Zeng Gui-Hua(曾贵华)‡

Laboratory of Quantum Information and Communication Security,

Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200240, *China*

(Received 22 November 2006; revised manuscript received 1 March 2007)

In this paper, by using properties of quantum controlled-not manipulation and entanglement states, we have designed a novel (2, 3) quantum threshold scheme based on the Greenberger- Horne -Zeilinger (GHZ) state. The proposed scheme involves two phases, i.e. a secret sharing phase and a secret phase. Detailed proofs show that the proposed scheme is of unconditional security. Since the secret is shared among three participants, the proposed scheme may be applied to quantum key distribution and secret sharing.

Keywords: quantum threshold, controlled-not manipulation, secret sharing, GHZ state
PACC: 0367, 0365

1. Introduction

On some occasions, such as the control and launch of missile, the pass on an important occasion and validation of testament, the secret has to be protected or enhanced by several participants. The process of protecting secret message is called cryptographically secret sharing, which is, in essence, that the secret is taken apart appropriately, and then, let different participants each hold a portion of it. Furthermore, the single participant cannot individually resume the secret unless some shares are united symbiotically.

In 1977, Sykes suggested a concept of secret split. Its basic idea is that each detached secret share means nothing, and the secret is reconstituted when all shares united. Shamir[1] and Blakley[2] in 1979 proposed independently the concept of secret sharing. Their secret sharing schemes, respectively, are Lagrange interpolating polynomial scheme and vector scheme. By using the techniques of quantum key distribution[3,4] and the Greenberger–Horne–Zeilinger (GHZ) triplet states,[5] Hillery *et al* proposed first a quantum secret sharing scheme. Thereafter, the quantum secret sharing scheme has attracted much attention,[6−12] and a series of quantum secret sharing schemes is proposed by using the quantum nature such as the properties of 2-particle entangled state, the characters of quantum error correcting code, quantum computation, etc. In 2000, the quantum secret sharing scheme was first implemented experimentally by a research group in the University of Geneva.[13]

Generally, the secret sharing scheme is often called threshold scheme. Suppose that m and n are positive integers with $m < n$ and the secret S is distributed to a set of participators P. If n participants dispense the secret by the following means to share the secret S, i.e. m of n participants may resume cooperatively the secret S, but any set of m-1 or fewer shares contains absolutely no information about the secret, this kind of sharing scheme is called (m, n) threshold scheme. Naturally, if this kind of scheme is implemented by quantum technique, it is called (m, n) quantum threshold scheme.[14] By using the technique of quantum error correction coding, a discrete variable (m, n) quantum threshold scheme was proposed. After that, a continuous variable (m, n) quantum threshold scheme was also advanced.[15]

In this paper, we propose a novel quantum secret sharing scheme in Section 2. The proposed scheme is a (2, 3) quantum threshold scheme which is implemented by using the properties of GHZ states and simple quantum computation. Moreover, we also analyse the security of the scheme and conclude that it is of unconditionally security in Section 3. Finally we draw

*Project supported by the National Natural Science Foundation of China (Grant No 60472018).
†E-mail: yuanli@sjtu.edu.cn
‡E-mail: ghzeng@sjtu.edu.cn

a conclusion in Section 4.

2. Scheme descriptions

Suppose that the secret is $|\psi_c\rangle = \alpha|0_c\rangle + \beta|1_c\rangle$ and this state is carried by particle p_c. $|\psi_c\rangle$ may be a quantum message ($\alpha, \beta \neq 0$) or a classic message ($\alpha = 0$ or $\beta = 0$). The participants are Alice, Bob, and Charlie. The distribution of secret sharing fulfills the following steps.

Step 1, the secret dealer first creates an entangled state,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0_a 1_b\rangle - |1_a 0_b\rangle), \tag{1}$$

where the subscripts a and b refer to different particles p_a and p_b respectively.

Step 2, the dealer combines the particle p_c and two entangled particles p_a and p_b into a mixed state,

$$\begin{aligned}|\varphi_0\rangle &= |\psi\rangle \otimes |\psi_c\rangle \\ &= \frac{1}{\sqrt{2}}(|0_a 1_b\rangle - |1_a 0_b\rangle)(\alpha|0_c\rangle + \beta|1_c\rangle) \\ &= \frac{1}{\sqrt{2}}(\alpha|0_a 1_b 0_c\rangle + \beta|0_a 1_b 1_c\rangle \\ &\quad - \alpha|1_a 0_b 0_c\rangle - \beta|1_a 0_b 1_c\rangle).\end{aligned} \tag{2}$$

Operating the generated mixed state with a quantum control-not gate C_{ac} generates an entangled triplet state

$$\begin{aligned}|\varphi_1\rangle &= C_{ac}(|\psi\rangle|\psi_c\rangle) \\ &= \frac{1}{\sqrt{2}}(\alpha|0_a 1_b 0_c\rangle + \beta|0_a 1_b 1_c\rangle \\ &\quad - \alpha|1_a 0_b 1_c\rangle - \beta|1_a 0_b 0_c\rangle),\end{aligned} \tag{3}$$

where the quantum control-not gate C_{ac} is defined as

$$C_{12}(|\varepsilon_1\rangle|\varepsilon_2\rangle) \to |\varepsilon_1\rangle|\varepsilon_2 \oplus \varepsilon_1\rangle, \quad \varepsilon_1, \varepsilon_2 \in \{0, 1\}. \tag{4}$$

Step 3, the secret dealer prepares three different registers R_1, R_2, R_3 and puts three particles p_a, p_b, p_c in the generated triplet state $|\varphi_1\rangle$ into registers R_1, R_2, R_3, respectively.

Step 4, according to expression (3), the dealer creates two entangled triplet states $|\widehat{\varphi}_1\rangle$ and $|\breve{\varphi}_1\rangle$ which are completely the same as $|\varphi_1\rangle$, namely, $|\varphi_1\rangle = |\widehat{\varphi}_1\rangle = |\breve{\varphi}_1\rangle$. The procedure is the same as the above. Put the three particles in $|\widehat{\varphi}_1\rangle$ and $|\breve{\varphi}_1\rangle$ into three registersR_1,R_2andR_3 according to the way presented in Table 1. From the table, we can learn that three registers each have particles p_a, p_b and p_c, but the marshaling sequences of the three particles in the three registers are different from each other.

Table 1.

	Register R_1	Register R_2	Register R_3
Quantum state $\|\varphi_1\rangle$	p_a	p_b	p_c
Quantum state $\|\widehat{\varphi}_1\rangle$	p_c	p_a	p_b
Quantum state $\|\breve{\varphi}_1\rangle$	p_b	p_c	p_a

From the above manipulation, we can learn that any one of the three participants owns a register which stores three particles. However, the three particles belong to the three different 3-particle entangled states. Therefore, the state of three particles in a register can be described as

$$|\phi\rangle = |\varphi_1\rangle \otimes |\widehat{\varphi}_1\rangle \otimes |\breve{\varphi}_1\rangle, \tag{5}$$

the above formula indicates that the three particles in the register are in direct states.

Step 5, the secret dealer distributes the different registers R_1, R_2 and R_3 containing particles to the participants Alice, Bob and Charlie, respectively. These shares will be the holder fragments. Despite the different registers and the particles that are distributed to the different participants, due to the entanglement of three corresponding particles, any aggressive action will destroy three entangled systems $|\varphi_1\rangle$, $|\widehat{\varphi}_1\rangle$ and $|\breve{\varphi}_1\rangle$ which are expressed in expression (3). Subsequently, the secret cannot be resumed.

To resume the secret, the participants fulfil the following steps:

Step1, any two participants pick out the corresponding particles. For example, if Bob and Charlie want to resume the secret, they select the particles in the first or final row in Table 1. If Alice and Charlie want to resume the secret, they should select the particles in the first row or the second row.

Step 2, the participants apply a quantum controlled-not gate to the selected particles. For example, when Bob and Charlie resume the secret, and they have selected their particles in the first row in Table 1,

the manipulation can be described as follows:

$$C_{bc}|\varphi_1\rangle = \frac{1}{\sqrt{2}}(\alpha|0_a1_b1_c\rangle + \beta|0_a1_b0_c\rangle - \alpha|1_a0_b1_c\rangle - \beta|1_a0_b0_c\rangle) = |\psi\rangle \otimes |\psi_c\rangle, \quad (6)$$

where C_{bc} denotes the quantum controlled-not gate which is applied by the participants Bob and Charlie to the particles p_b and p_c. Expression (4) shows that the secret state $|\psi_c\rangle$ and the entangled state $|\psi\rangle$ are product states. Therefore, the secret $|\psi_c\rangle$ can be gained. Similarly, the participants Alice and Charlie also can acquire the secret only according to a similar method cooperatively,

$$C_{ac}|\varphi_1\rangle = |\psi\rangle \otimes |\psi_c\rangle, \quad (7)$$

where C_{ac} denotes the quantum controlled-not applied by participator Alice and Charlie to the particles p_a and p_c.

We note here that if only $|\varphi_1\rangle$ is employed, one can also design a quantum secret sharing scheme. However, since the particle p_c is only held by one participant in this case, the participant who holds the particle p_c must join in each process of secret resumption. For instance, even A and B can extract the secret, the secret will be stored in the particle C held by participant C so that A and B cannot obtain the secret. This kind of scheme is definitely different from the usual secret sharing ways. But in some particular cases, this kind of scheme is useful. For example, in a company, if the boss wants to control the action of employees the scheme can be adopted.

3. Analysis of security

Now, we analyse the security of the proposed scheme. The requirement for the (m, n) threshold scheme is that any m participants can resume the secret but any m-1 participants cannot resume the secret. According to this requirement we prove that the proposed scheme is of the unconditional security.

Theorem 1 Any one of the participants cannot resume the secret by employing only one particle.

Proof Now suppose that the first particle among the participants has been measured and the state is $|x\rangle$. Because after measuring any one of the GHZ triplet states, three-particle entangled state will be relieved, the other two particles compose a two-particle entangled state system, and their possible values are as follows:

$$|\psi^1\rangle_{23} = \frac{1}{\sqrt{2}}((\alpha-\beta)|+x\rangle_b|+x\rangle_c + (\alpha+\beta)|-x\rangle_b|+x\rangle_c),$$
$$|\psi^2\rangle_{23} = \frac{1}{\sqrt{2}}((\alpha+\beta)|-x\rangle_b|-x\rangle_c - (\alpha-\beta)|+x\rangle_b|-x\rangle_c),$$
$$|\psi^3\rangle_{23} = \frac{1}{\sqrt{2}}((\mathrm{i}\alpha-\beta)|-x\rangle_b|+y\rangle_c - (i\alpha+\beta)|-x\rangle_b|-y\rangle_c),$$
$$|\psi^4\rangle_{23} = \frac{1}{\sqrt{2}}((\alpha+\beta)|+x\rangle_b|-y\rangle_c - (\alpha-\beta)|+x\rangle_b|+y\rangle_c). \quad (8)$$

From the above formula, we know that the state of two-particle entangled system cannot be ascertained after the GHZ entangled bit has collapsed, and it is maybe one of the four states with equal possibility. Even if the entangled state of two-particle system has been confirmed, the state of two-particle system is still not ascertained because the state of Alice' particle maybe is $|+x\rangle$ or $|-x\rangle$. Therefore, if only a particle has been measured, the secret will not be given away.

Theorem 2 No less than two of participants can resume the secret by employing their particles.

Proof Now we still suppose that Bob and Charlie are to resume the secret by employing their particles. The triplet state is

$$C_{bc}|\varphi_1\rangle = \frac{1}{\sqrt{2}}(\alpha|0_a1_b1_c\rangle + \beta|0_a1_b0_c\rangle - \alpha|1_a0_b1_c\rangle - \beta|1_a0_b0_c\rangle),$$

where a, b, c still denote respectively the three particles. Define two eigenstates $|x\rangle$ and $|y\rangle$ expressed by vectors $|0\rangle$, $|1\rangle$ as

$$|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$
$$|+y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \mathrm{i}|1\rangle), \quad |-y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - \mathrm{i}|1\rangle). \quad (9)$$

As is well known, three exist the following relationships:

$$|0\rangle = \frac{1}{\sqrt{2}}(|+x\rangle + |-x\rangle), \quad |1\rangle = \frac{1}{\sqrt{2}}(|+x\rangle - |-x\rangle). \quad (10)$$

Therefore, GHZ triplet state is

$$|\psi\rangle = \frac{1}{\sqrt{2}}\{(|0\rangle_a + |1\rangle_a)((\alpha-\beta)|+x\rangle_b|+x\rangle_c - (\alpha+\beta)|-x\rangle_b|+x\rangle_c) + (|0\rangle_a - |1\rangle_a)((\alpha+\beta)|-x\rangle_b|-x\rangle_c$$

$$-(\alpha-\beta)|+x\rangle_b|-x\rangle_c)\}. \tag{11}$$

From the above formula, we can learn that measurements of p_b and p_c can determine that of p_a. For example, if Bob's particle in the $-x$ direction, Charlie's in the $+x$ direction, we can learn that Alice's state is $(-1/\sqrt{2})(\alpha+\beta)(|0\rangle_a+|1\rangle_a)$.

As for the eavesdropper (maybe a participant) Eve, he can take two attacking strategies, intercept–resend attack[16,17] and entangled state attack.[18−20] In fact, they are all ineffective on this scheme.

Theorem 3 Any participant cannot resume the secret by employing the intercept–resend attack strategy.

Proof Assume that Bob is dishonest, he wants to intercept the particles which Charlie send to Alice and measure the two particles which he had. Then, he sends one of them to Alice, and hopes to gain the information and be not found by the other two particles that he had known are Charlie's particles. This attack method is called intercept–resend attack.

In fact, GHZ secret sharing is secure for the intercept–resend attack. Because Charlie measured randomly his particles by using x or y basis, but Bob does not know the basis that Charlie has used, he just has half the probability to measure it correctly. However, a message is described by a large number of particle states, therefore, for this attack the protocol is secure.

Theorem 4 Any participants cannot resume the secret by employing the entangled state attack.

Proof If Eve or a dishonest participant tries to attack the scheme by entangling his own particles as an ancilla with the GHZ state. After the legal correspondents have measured their own particles, Eve tries to obtain the useful information by measuring his ancilla. This method is called entangled state attack.

According to the requirement for the secret sharing system, the analysis of security on quantum (2, 3) threshold system security is presented in this paper. This can be described by the following process.

If Eve obtains a register, which is any one of three registers R_1, R_2 and R_3, and makes an ancilla $|R_{ijn}\rangle$ and the three particles entangled, in fact, it is useless to do that, because in formula (5) we all know that $|\phi\rangle$, the state of three particles in any register, is the direct state of $|\varphi_1\rangle$, $|\widetilde{\varphi}_1\rangle$ and $|\breve{\varphi}_1\rangle$, what Eve has had are some useless shares. Given that Eve obtains the GHZ state from the secret dealer, here, supposing it to be $|\varphi_1\rangle$, he takes the entangled state manipulation, namely, he makes $|R_{ijn}\rangle$ and the GHZ state entangled. Suppose that the quantum state includes three particles, after the particles in ancilla and in GHZ triplet state have been entangled, the constituted hybrid state is as follows:

$$|\Psi\rangle=\frac{1}{\sqrt{2}}\sum_{i,j,n=0}^{1}\Gamma|ijn\rangle_3|R_{ijn}\rangle, \tag{12}$$

where $|ijn\rangle_3$ is the entangled 3-particle state and $\Gamma=\alpha,\beta$. We prove that $|\Psi\rangle$ is a direct state between GHZ triplet state and arbitrary 3-particle state as follows.

In fact, firstly, suppose that Alice, Bob and Charlie measure their particles by using x basis. From Theorem 2, we can learn that any two of participants can resume the secret by employing their particles and according to the GHZ's correlation,[5] the condition under which Eve will not cause the error is

$$\begin{aligned}&p(C=+x|A=\pm x,B=\mp x)=1,\\&p(C=-x|A=\pm x,B=\pm x)=1.\end{aligned} \tag{13}$$

In the above formula, $p(C=+x|A=+x,B=-x)=1$ is the probability for Bob to measure $-x$ and for Alice and Charlie to measure $+x$, and other forms can be defined similarly. From the above expressions we have

$$\begin{aligned}&P(-x,+x,-x)|\Psi\rangle=0,\quad P(+x,-x,-x)|\Psi\rangle=0,\\&P(-x,-x,+x)|\Psi\rangle=0,\quad P(+x,+x,+x)|\Psi\rangle=0,\end{aligned} \tag{14}$$

where $P(-x,+x,-x)=0$ denotes the projection operator of a mixed state $|\Psi\rangle$ projected into any 3-particle state. Among them, the particles of Alice, Bob and Charlie are respectively in the three directions $-x$, $+x$ and $-x$. Similarly, the other projection operators can be defined. If $|0\rangle$ and $|1\rangle$ denote the projection operators, the state vectors corresponding to the projection operators are

$$\begin{aligned}|\psi_1\rangle=&\frac{1}{\sqrt{2}}(\alpha|000\rangle_3+\beta|010\rangle_3\\&-\alpha|111\rangle_3-\beta|101\rangle_3),\\|\psi_2\rangle=&\frac{1}{\sqrt{2}}(\alpha|110\rangle_3+\beta|011\rangle_3\\&-\alpha|001\rangle_3-\beta|100\rangle_3),\\|\psi_3\rangle=&\frac{1}{\sqrt{2}}(\alpha|011\rangle_3+\beta|001\rangle_3\\&-\alpha|100\rangle_3-\beta|110\rangle_3),\end{aligned}$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(\alpha|100\rangle_3 + \beta|101\rangle_3 - \alpha|011\rangle_3 - \beta|010\rangle_3). \quad (15)$$

Other projection operators can be deduced in a similar manner. In this case, the condition under which any operation of an eavesdropper will not bring any errors is that the adopted quantum state vector should choose the above forms corresponding to projection operators.

Secondly, if Alice measures his particles by using x basis, and Bob and Charlie measure their particles by using y basis for the same reason, the condition under which no error can be described is as follows:

$$p(C = -y|A = \pm x, B = \mp y) = 1,$$
$$p(C = +y|A = \pm x, B = \pm y) = 1. \quad (16)$$

The above expressions present

$$P(-x, +y, +y)|\Psi\rangle = 0, \quad P(+x, -y, +y)|\Psi\rangle = 0,$$
$$P(-x, -y, -y)|\Psi\rangle = 0, \quad P(+x, +y, -y)|\Psi\rangle = 0. \quad (17)$$

Denote the projection operators by using $|0\rangle$ and $|1\rangle$, then the state vectors corresponding to the four projection operators, respectively, will be

$$|\tilde{\psi}_1\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle_3 + \beta|010\rangle_3 + \alpha|111\rangle_3 + \beta|101\rangle_3),$$
$$|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{2}}(\alpha 110\rangle)_3 + \beta|011\rangle_3 + \alpha|001\rangle_3 + \beta|100\rangle_3),$$
$$|\tilde{\psi}_3\rangle = \frac{1}{\sqrt{2}}(\alpha|011\rangle_3 + \beta|001\rangle_3 + \alpha|100\rangle_3 + \beta|110\rangle_3),$$
$$|\tilde{\psi}_2\rangle = \frac{1}{\sqrt{2}}(\alpha|100\rangle_3 + \beta|101\rangle_3 + \alpha|011\rangle_3 + \beta|010\rangle_3). \quad (18)$$

Actually, there exist only two projection operators that are different from formula (4). It is easy to see that $|\psi_i\rangle\,(i = 1, 2, 3, 4)$ and $|\tilde{\psi}_j\rangle(j = 1, 2, 3, 4)$ are mutual orthogonal.

Thirdly, if Alice and Bob measure their particles by using y basis and Charlie measures his particles by using x basis, according to the same analysis as the above, the condition under which there exists no error is to adopt a projection operator, and the corresponding vector is

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{2}}(\alpha|010\rangle_3 + \beta|110\rangle_3 - \alpha|101\rangle_3 - \beta|001\rangle_3). \quad (19)$$

According to the above three cases, in a word, the form of $|\psi\rangle$ may be confirmed as follows:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(\alpha|010\rangle_3 + \beta|011\rangle_3 - \alpha|101\rangle_3 - \beta|100\rangle_3) \otimes |R_{ijn}\rangle = \varphi_1 \otimes |R_{ijn}\rangle, \quad (20)$$

namely, $|\Psi\rangle$ is a direct state of GHZ triplet state and auxiliary quantum state, so Eve cannot obtain any information from $|\Psi\rangle$ if he did not cause any disturbance in the measurement of particles in register. Therefore, the entangled state attack will not be successful.

4. Conclusion

In this paper, a (2, 3) quantum threshold system is proposed. From the analyses in Section 3, we can conclude that the designed secret sharing scheme which is based on a (2, 3) quantum threshold system is unconditionally secure.

References

[1] Shamir A 1979 *Commun A CM* **22** 612
[2] Blakley G 1979 *Proc AFIPS* **48** 313
[3] Bennett C H and Brassard G and Mermin N 1992 *Phys. Rev. Lett.* **68** 557
[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[5] Hillery M, Buzek V and Andre Berthiaume 1999 *Phys. Rev.* A **59** 1829
[6] Song K H, Zhang W J and Guo G C 2002 *Chin. Phys.* **11** 0218
[7] Huang Z P and Lin H C 2005 *Chin. Phys.* **14** 0974
[8] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304
[9] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303
[10] Singh S K and Srikanth R 2005 *Phys. Rev.* A **71** 012328
[11] Zhang Y Q and Jin X R and Zhang S 2006 *Chin. Phys.* **15** 2252
[12] Chen Z H and Lin X M 2005 *Chin. Phys.* **14** 1821
[13] Tittel W, Zbinden H and Gisin N 2001 *Phys. Rev.* A **63** 042301
[14] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[15] Levvaidman T 1994 *Phys. Rev.* A **49** 1473
[16] Namiki R and Hirano T 2003 *Phys. Rev.* A **67** 022308
[17] Wang X B 2004 *Phys. Rev. Lett.* **92** 077902
[18] Tittel W, Brendel J, Zbinden H and Gisin N 2000 *Phys. Rev. Lett.* **84** 4737
[19] Shimizu K and Imoto N 2002 *Phys. Rev.* A **65** 032324
[20] Song D 2004 *Phys. Rev.* A **69** 034301