Hiding information in orthogonal product quantum states

Dexi Zhang
College of Computer Science and Technology
Xuchang University
Xuchang City, 461000
the People's Republic of China

Xiaoyu Li
College of Information Engineering
Zhengzhou University
Zhengzhou City, 450052
the People's Republic of China

Abstract: This paper provide a quantum information hiding protocol using orthogonal product states. It is based on the non-locality of an complete orthogonal set of product states in a two-particle quantum system in which each particle has three states. Information is coded in a integral state of the two-particle system. Then the two particles are distributed to two persons who can only perform local operations and classical communications. So the origin information is hidden and it's impossible for two persons to recover it. We show that our protocol is secure and give a detailed procedure to hide data in computers.

Key–Words: Typing manuscripts, LaTeX

Quantum information science is field which integrates quantum physics with information science. It may provide surprising force for people to do things which are impossible in classical information science so far, such as decomposing a large number in polynomial time(Shor's algorithm)[1] and so on. One of the most important applications of quantum information science is quantum cryptography. Quantum cryptography is a field that applies quantum mechanics into cryptograph. The fundamental principles of quantum physics guarantee its security. The first quantum key distribution (OKD) protocol is proposed by C. H. Bennett and G. Brassard [2]. Since then much research work has been done in quantum cryptography, such as quantum key distribution [3-7], quantum authentication [8-11], quantum bit commitment [12,13], quantum secret sharing [14-16] and information theory for quantum cryptography [17]. Experiments on QKD has also been accomplished successfully. In 1992 BennettBessette and Brassard first realized BB84 protocol in laboratory [18]. Recently QKD in optical fiber has been achieved [19] beyond 150 km and in free space has been implemented over a distance of 1 km [20].

There is another interesting problem: quantum information hiding. Unlike secret sharing information hiding is a particular technique in quantum cryptography which is impossible to fulfil in classical cryptography. Some classical information can be coded in a compound quantum system. Then we distribute the parts of the compound system to a group of people people who can only perform local operations and communicate with each other through a classical channel. It's impossible for these people to get the origin information. So we can say that the origin information has been hidden. In 2001 Terhal et al issued a quantum protocol hiding bits in Bell states[21]. DiVicenzo and Leung and Terhal's paper give a detailed discussion on information hiding using Bell states [22]. Eggelin and Werner present a scheme to hide data in entangled multiple-particle system [23]. Later quantum information hiding is extended by DiVicenzo et al to hide not only classical information but also quantum bits [24].

Most of the previous quantum information hiding protocols uses entangled states to fulfil information hiding because they are based on the non-locality of the entangled states. But in 1999 Bennett et al proved that non-entangled orthogonal product states can also show non-locality [25]. In this paper we provide a quantum information hiding protocol using non-entangled product states. As known product states are easier to produce and control. Our protocol is easier to apply in practice.

The paper is organized as follows. In section 2 we introduce the basic idea on which our information hiding protocol is based. Then the protocol is present in section 3. Next in section 4 we give some further discussions. Section 5 we come to our conclusion.

1 Basic Idea

In [25] Bennett et al proved that non-entangled orthogonal state can also show non-locality. They consider a two-particle system in which each particle has

three states. There is a complete orthogonal set of states in this system.

$$\begin{aligned}
|\varphi_1>&=|1>|1>\\
|\varphi_2>&=|0>\frac{1}{\sqrt{2}}(|0>+|1>),\\
|\varphi_3>&=|0>\frac{1}{\sqrt{2}}(|0>-|1>),\\
|\varphi_4>&=|2>\frac{1}{\sqrt{2}}(|1>+|2>),\\
|\varphi_5>&=|2>\frac{1}{\sqrt{2}}(|1>-|2>),\\
|\varphi_6>&=\frac{1}{\sqrt{2}}(|1>+|2>)|0>,\\
|\varphi_7>&=\frac{1}{\sqrt{2}}(|1>-|2>)|0>,\\
|\varphi_8>&=\frac{1}{\sqrt{2}}(|0>+|1>)|2>,\\
|\varphi_9>&=\frac{1}{\sqrt{2}}(|0>-|1>)|2>.
\end{aligned} \tag{1}$$

In the study of quantum information just as that a two-state quantum particle is named a 'qubit', we usually call a three-state quantum particle a 'qutrit'. So the two-particle quantum system above can be called a two-qutrit system. It is proved in [25] that these nine states can't be distinguished reliably by local operations and classical communications, that is to say, it's impossible to confirm the state uniquely in this vector set by local operations and classical communications. So we can design a information hiding protocol based on this property of the compound system as follows. First we code some classical information in the two-qutrit system. Then the two qutrits is distributed to two persons, for example, Alice and Bob. They are restricted to only doing local operations and there is only a classical channel between them. Or in other words Alice and can only perform operations on the qutrit at her(or his) hand. They can't do any collective operation on the whole two-qutrit system including collective measurement. Moreover they can only exchange classical information through a classical channel, that is to say, they can't send quantum qutrit at hand to the other one. So Alice and Bob can't recover the origin information, in other words, the origin information is hidden to them.

Let's consider how to carry our idea. As known the nine states form a complete orthogonal basis $\{|\varphi_1>,|\varphi_2>,...,|\varphi_9>\}$ of the two-qutrit system. We can measure the two-qutrit system in this basis. It is easy to notice that we can distinguish all the nine states through by doing this collective measurement. So we can establish a rule of coding as follows.

Rule 1 (Coding):

$$\begin{aligned}
|\varphi_1>&\rightarrow 000, \quad |\varphi_2>\rightarrow 001,\\
|\varphi_3>&\rightarrow 010, \quad |\varphi_4>\rightarrow 011\\
|\varphi_5>&\rightarrow 100, \quad |\varphi_6>\rightarrow 101,\\
|\varphi_7>&\rightarrow 110, \quad |\varphi_8>\rightarrow 111.
\end{aligned} \tag{2}$$

Generally data in computers is usually a binary string. First we split it into many units which is composed of three bits. Then we will get a sequence of units. Obviously each unit can be coded as a state of the whole two-qutrit system according to Rule 1. Notice that the state $|\varphi_9>$ does'nt appear in Rule 1. The reason is that there are nine states in the complete orthogonal set while describing all possible values of a three-bit unit need only eight states. If we want to include all states in Rule 1, we have to use four-bit units. But there are sixteen possibilities of a four-bit unit now while we have only nine states of a two-qutrit system. If we split the origin string into four-bit units, there must be some code words which we have no quantum state to represent it. Of course it is will be impossible to finish coding. So we must split the origin string into three-bit units. On the other hand, is the state $|\varphi_9>$ is useless since it doesn't represent a coding word? The answer is NO. To accomplish information hiding $|\varphi_9>$ is indispensable. As known Bennett et al have proved that the nine vectors in the basic set $\{|\varphi_1>,|\varphi_2>,...,|\varphi_9>\}$ are indistinguishable under local operations and classical communications in their paper. But it's easy to find that the eight vectors in the vector set $\{|\varphi_1>,|\varphi_2>,...,|\varphi_8>\}$ are distinguishable under local operations and classical communications. That is to say, Alice and Bob will be able to confirm the state uniquely of the whole two-qutrit system under local operations and classical communications if we do coding with only eight states. Of course it's very dangerous. We have to make use of $|\varphi_9>$ so as to guarantee that Alice and Bob can't recover the origin data. So we can inert some tags in the sequence of units at random. It can be stipulated as follows.

Rule 2(Modified):
(1) To each unit, we create a two-qutrit system in the state $|\varphi>$, in which $|\varphi>\in\{|\varphi_1>,|\varphi_2>,...|\varphi_8>\}$ according to the Rule 1.
(2) To each tag, we create a two-qutrit system in the state $|\varphi_9>$.

So the sequence of two-qutrit systems which we get at last may contain system in any state in $\{|\varphi_1>,|\varphi_2>,...,|\varphi_9>\}$. Then we distribute the all the two-qutrit systems to Alice and Bob in which Alice hold the first qutrit and Bob hold the second one. It is impossible for Alice and Bob to distinguish the nine states under local operations and classical communications. So they can't confirm the state of any two-qutrit system.

There is another problem left. The binary string of origin information may contain random n bits which n can't be divided exactly by 3. So it may not be split into three-bit units exactly, in other words, there may be one or two bits left. To solve this problem we can make up the string with 'dictate bits'.

Rule 3(Making-up):
(1) If n can be divided exactly by 3, we add 000 to the end of the origin string;
(2) If n *Mod* 3=2, we first add 00 to the end of the origin string. Then we add '001' to the end;
(3) If n *Mod* 3=1, we first add 0 to the end of the origin string. Then we add 011 to the end.

Now the string can be split into three-bit units exactly. For simplicity we should make up the origin string before we insert tags in it. So the origin data is coded in a sequence of two-qutrit systems. It's hidden to Alice and Bob. If we want to recover it. We just need to combine the two qutrits from Alice and Bob up and do collective measurements on them. Obviously it is impossible for Alice and Bob to do such things. To recover the origin information we just do as follows.

Rule 4(Decoding):
(1) Measurement: We measure all the two-qutrit systems in basis $\{|\varphi_1>, |\varphi_2>, ..., |\varphi_9>\}$ in turn.
(2) Decoding: We translate the measurement results into code words according to following rule. If the result is $|\varphi_9>$, we ignore it, or in other words, it does't produce code words; If the result is $|\varphi>, |\varphi> \in \{|\varphi_1>, |\varphi_2>, ..., |\varphi_8>\}$, we translate it into a code word according Rule 1. Finally we will get a binary string.
(3) Deleting dictate bits: If the last three bits of the string are 000, we delete them; If the last three bits of the string are 001, we delete the last four bits; If the last three bits of the string are 011, we delete the last five bits.

Now the left string is the origin information.

2 Quantum information hiding protocol using orthogonal product states

It's easy to find that people can design a information hiding protocol based on the basic idea in section 2. Assuming that a third party named Carol wants to hide some classical information, she create two-qutrit systems and encode the data in them. Then she send the two qutrits of each system to Alice and Bob separately who can only perform local operation and classical channel. So the information is hidden to Alice and bob.

Now we give our quantum information hiding protocol in detail.
(1) Carol split her information(a binary string) into a sequence of three-bit units and add dictate bits to the end. If n can be divided exactly by 3, she add '000' to the end; If n *Mod 3*=1, she add '001' to the end; If n *Mod 3*=2, she add '011' to the end.
(2) Carol insert some tags in the sequence at random.
(3) Carol creates two-qutrit systems according to the following rule. To each unit she creates a two-qutrit system according to equation (1); To each tags she creates a two-qutrit system in $|\varphi_9>$. Finally she has a sequence of two-qutrit systems.
(4) Carol sends the first qutrit of each two-qutrit system to Alice and the second ones to Bob.
So the origin information is hidden. Alice and Bob can't obtain it without Carol's help.

To recover the data Alice and Bob must send their qutrits to Carol. After receiving them, Carol combines them up and does a collective measurement on the two-qutrit systems in basis $\{|\varphi_1>, |\varphi_2>, ..., |\varphi_9>\}$. Then she transform the measurement results into a sequence of coding words. That is to say, if the result is $|\varphi_9>$, she ignores it; if the result is any state of $\{|\varphi_1>, |\varphi_2>, ..., |\varphi_9>\}$, she translates it into coding words according to equation(1). So Carol get a binary string. Finally she trim the dictate bits as follows. If the last three bits are '000', she delete them; If the three bits are '001', she delete the last four bits of the string; If the three bits are '011', she delete the last five bits of the string. So the left string is the origin information.

3 Discussion

It's easy to show that our quantum information hiding protocol is secure. Since Bennett et al has proved in their paper that the nine states in $\{|\varphi_1>, |\varphi_2>, ..., |\varphi_9>\}$ can't be distinguished from each other reliably under local operations and classical communications. So Alice and Bob can't confirm the state of the two-qutrits system uniquely, in other words, they can't get the origin information exactly.

But there is still a problem left. Do Alice and Bob recover the origin information with a relative high probability although they can't get it exactly? Let's consider it. There are nine states in the basic vector set $\{|\varphi_1>, |\varphi_2>, ..., |\varphi_9>\}$. So Alice and Bob can guess the correct state of a two-qutrit system with a probability 1/9 at least while she has to do nothing. Moreover according to our protocol they can perform local operations(including local measurements) on her(or his) qutrit and tell the other one the measurement result through the classical channel. So the probability success for Alice and Bob to guess correctly can be improved. For example, if Alice and Bob measure the qutrit at her(or his) hand separately in basis

$\{|0>,|1>,|2>\}$, they can confirm that the state of the two-qutrit system must be in a smaller scope. The result can be summarized into the following table.

Alice's	Bob's	state	probability
$\|0>$	$\|0>$	$\|\varphi_2>,\|\varphi_3>$	1/2
$\|0>$	$\|1>$	$\|\varphi_3>,\|\varphi_2>$	1/2
$\|0>$	$\|2>$	$\|\varphi_8>,\|\varphi_9>$	1/2
$\|1>$	$\|0>$	$\|\varphi_6>,\|\varphi_7>$	1/2
$\|1>$	$\|1>$	$\|\varphi_1>$	1
$\|1>$	$\|2>$	$\|\varphi_8>,\|\varphi_9>$	1/2
$\|2>$	$\|0>$	$\|\varphi_6>,\|\varphi_7>$	1/2
$\|2>$	$\|1>$	$\|\varphi_4>,\|\varphi_5>$	1/2
$\|2>$	$\|2>$	$\|\varphi_4>,\|\varphi_5>$	1/2

table 1

From table 1 we can find that the probability with which Alice and Bob confirm the state uniquely is only 1/2 except when the state of the two-qutrit system is $|\varphi_1>$. Only when when the state of the two-qutrit system is $|\varphi_1>$, they can guess correct with probability 1. Without losing generality, we assume that the probability for all nine states to appear in the sequence is equal. So to a two-qutrit system, the average probability that Alice and Bob guess its state should be

$$P = 8 \times \frac{1}{9} \times \frac{1}{2} + \frac{1}{9} = \frac{5}{9}. \tag{3}$$

This conclusion is deduced based on the precondition that we use a two-qutrit system to represent a code word according to equation(1). To depress the probability that the hidden information is revealed to Alice and Bob, we can use multiple two-qutrit systems to represent a code word just as follows.

$$\begin{aligned}
&\overbrace{|\varphi_1>|\varphi_1>...|\varphi_1>}^{m} \longrightarrow 000\\
&\overbrace{|\varphi_2>|\varphi_2>...|\varphi_2>}^{m} \longrightarrow 001\\
&\overbrace{|\varphi_3>|\varphi_3>...|\varphi_3>}^{m} \longrightarrow 010\\
&\overbrace{|\varphi_4>|\varphi_4>...|\varphi_4>}^{m} \longrightarrow 011\\
&\overbrace{|\varphi_5>|\varphi_5>...|\varphi_5>}^{m} \longrightarrow 100\\
&\overbrace{|\varphi_6>|\varphi_6>...|\varphi_6>}^{m} \longrightarrow 101\\
&\overbrace{|\varphi_7>|\varphi_7>...|\varphi_7>}^{m} \longrightarrow 110\\
&\overbrace{|\varphi_8>|\varphi_8>...|\varphi_8>}^{m} \longrightarrow 111.
\end{aligned} \tag{4}$$

Similarly we use m qutrits to represent a tag.

$$\overbrace{|\varphi_9>|\varphi_9>...,|\varphi_9>}^{m} \longrightarrow tag. \tag{5}$$

So the probability that Alice and Bob guess the correct code word is

$$P = (\frac{5}{9})^m. \tag{6}$$

If the sequence of the two-qutrit systems are composed of k units and tags, the probability that Alice and Bob get the origin data is only

$$P = (\frac{5}{9})^{mk}. \tag{7}$$

Obviously the number k is related to the length of the origin data n, that is

$$k \approx n/3 + n_{tags} \tag{8}$$

in which n_{tags} is the number of the tags which Carol has inserted. So Carol can choose a fit number m so as to make it impossible for Alice and Bob to find the origin information even using the best computers in the world. On the other hand Carol can choose m neatly according to the length of the origin data and the degree of secret which she needs.

So we come to a conclusion that to improve the security of our protocol we can modify it by changing the 'two-qutrit system' in the protocol into 'm two-qutrit systems'.

4 Conclusion

In this paper we present a quantum information hiding protocol using orthogonal product states. It is based on the non-locality of the two-particle system in which each particle has three states, or the two-qutrit system. We can encode some classical information in the integral state of two-qutrit systems and distribute the two qutrits to different users who can perform local operation and classical communications. Law of quantum mechanics guarantees that the users can't recover the origin information. So the origin information is hidden effectively. We provide a detailed protocol to hide data in computers and show that it's secure. Because product state is easier to produce and control, our protocol is more practicable than previous protocols using entangled states.

Acknowlegements

This work is supported by Natural Science Foundation of China (Grants 60603002);the National Natural Science Foundation of China 60496324(NSFC Major Research Program 60496324);the National Natural Science Foundation of China (Grants 60402016);the National Natural Science Foundation of China

(Grants 60503047).
We would thank Ruqian Lu for directing us into this research.

References:

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring", In: *Proc of the 35th Annual Symp on Foudations of Computer Science*, 1994: 124-134.

[2] C. H. Bennet and G. Brassard, "Quantum cryptography: Public-key distribution and tossing", In: *Proceedings of IEEE International conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984, (IEEE Press, 1984), pp. 175.

[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.* 67(1991) 661-663.

[4] C. H. Bennett, G. Brassard and N. D. Mermin, "Quantum cryptography without Bell's theorem", *Phys. Rev. Lett.* 68(1992) 557-559.

[5] Lo, H. K. and H. F. Chau, "Unconditional Security of Quantum Key Distribution over arbitrarily long distances", *Science*, 283(1999) 2050-2056.

[6] A. Cabello, "Quantum Key Distribution in the Holevo Limit". *Phys, Rev. Lett.* 85(2000) 5635-5638.

[7] P. Xue, C. F. Li and G. C. Guo, "Efficient quantum-key-distribution protocol with nonmXimally entangled states", *Phys. Rev. A* 64(2001) 032305.

[8] G. Zeng and W. Zhang, "Identity verification in quantum key distribution", *Phys. Rev. A* 61(2000) 022303.

[9] Y. S. Zhang, C. F. Li, and G. C. Guo, "Quantum authentication using entangled state", *e-print arXiv*: quant-ph/0008044.

[10] D. Ljunggren, M. Bourennane and Anders Karlsson, "Authority-based user authentication in quantum key distribution", *Phys. Rev. A* 62(2000), 022305.

[11] Xiaoyu Li and H. Branum, "Quanum authencation using entangled states", *International Journal of Foundation of Computer Science*, Vol 15, No.4, (2004) 609-617.

[12] H.-k. Lo, H. F. Chau (1998), *Why quantum bit commitment and ideal quantum coin tossing are impossible*, Physica D, 120, pp. 177-187.

[13] A. Kent, "Coin Tossing is Strictly Weaker than Bit Commitment", *Phys. Rev. Lett.* 83(1999) 5382-5384.

[14] R. Cleve, D. Gottesman, and H.-K. Lo, "How to Share a Quantum Secret", *Phys. Rev. Lett.* 83(1999) 648-651 .

[15] D. Gottesman, "Theory of quantum secret sharing", *Phys. Rev. A* 61(2000) 042311.

[16] M. Hillery, V. Buzek and A. Berthiasiaume, "Quantum secret sharing", *Phys. Rev. A* 59(1999) 1829-1834.

[17] B. Schumacher, Quantum Privacy and Quantum Coherence, Phys. Rev. Lett. 80(1998) 5695-5697.

[18] C.H.Bennett, F.Bessette, G.Brassard, L.Salvail and J.Smolin, "Experimental quantum cryptography", *Journal of Cryptology*, Vol.5 (1992) No.1 3 - 28.

[19] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka and K, Nakamura, "Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography", *eprints*: quant-ph/0403104.

[20] W. T. Buttler et al, "Practical Free-Space Quantum Key Distribution over 1 km", *Phys. Rev. Lett.* 81(1998) 3283-3286.

[21] B. M. Terhal, D. P. DiVincenzo and D. W. Leung, "Hiding Bits in Bell States", *Physical Review Letters*, 2001, 86: 5807-5810.

[22] D. P. DiVicenzo, D. W. Leung, and B. M. Terhal, "Quantum data hiding", *IEEE Transactions on Information Theory* Vol.48(2002) No.3 580-599.

[23] T. Eggeling and R. F. Werner, "Hiding Classical Data in Multipartite Quantum States", *Phys. Rev. Lett.* 89(2002) 097905.

[24] D. P. DiVincenzo, P. Hayden and B. M. Terhal, "Hiding Quantum Data", *e-prints*: quant-ph/0207147.

[25] C. H. Bennett, D. P. Divicenzo and C. A. Fuchs et al, "Quantum nonlocality without entanglement", *Physical Review A*, 1999, 59: 1070-1091.