Journal of Theoretical and Applied Information Technology
10th March 2013. Vol. 49 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

QUANTUM INFORMATION DELAY SCHEME USING ORTHOGONAL PRODUCT STATES

[1]XIAOYU LI, [2]LIJU CHEN

[1]School of Information Engineering, Zhengzhou University, Zhengzhou City, 450001, P. R. China
[2]Xi'an Communication Institute, Xi'an City, 761000, P. R. China
E-mail: [1]iexyli@zzu.edu.cn , [2]chenliju0801@sina.com

ABSTRACT

In this paper we provide a quantum information delay scheme using orthogonal product states. By sharing orthogonal product states one person can give the other person some information which cannot be read until he or she lets the latter do. The fundamental Laws of quantum mechanics guarantee that the scheme is unconditionally secure. Our scheme is easy to carry out in practice because there are no entangled states or complex quantum operations needed. Moreover our scheme is robust against noise and possible attacks.

Keywords: *Information Delay, Quantum Cryptography, Orthogonal Product State, Non-locality, Security***.**

1. INTRODUCTION

Quantum information science is an ascendant research field which integrates quantum physics with information science. It may show surprising results which are impossible in classical information science so far, such as decomposing a large number in polynomial time(Shor's algorithm) [1], efficient database search(Grove's algorithm) [2] and so on. One of the most important fields of quantum information science is quantum cryptography. Unlike the classical cryptographic protocol based on the complexity of computation, the unconditional security of the quantum cryptographic protocol is guaranteed by the fundamental principles of quantum physics. The first quantum key distribution (OKD) scheme is proposed by C. H. Bennett and G. Brassard [3]. So it's called BB84 scheme. Since then much research work has been done in quantum cryptography, such as quantum key distribution [3-9], quantum authentication [10-13], quantum secret sharing [14-15], quantum information hiding [16,17], information theory for quantum cryptography [18] and so on. Experiments on QKD have also been accomplished successfully. In 1992 Bennett, Bessette and Brassard first realized BB84 protocol in laboratory [19]. Recently QKD in optical fiber has been achieved [20] beyond 150 km and in free space has been implemented over a distance of 1 km [21].

There is another interesting problem: information delay. Suppose that one person, for example, Alice, wants to give some information to the other one, Bob. But she hopes that Bob couldn't read the information at his hands until she lets him to do sometime in the future. Moreover Bob may be far away from Alice in space when Alice finally decides to let him read the information. Obviously it's an important problem which may appear in business and military affairs. In classical cryptography people often solve this problem by the following scheme. Alice encrypts the information and only gives Bob the cipher text. So Bob can't read the information because he hasn't the information to decrypt it. Only when Alice decides to let Bob get the information, does she send the information to Bob through a public channel. So Bob can read the information now. On the other hand, since the channel is public, an eavesdropper, Eve, can also get the information. But she can't get the information because she hasn't the cipher text. Obviously such schemes often depend a well-designed key management system [22-24]. However there is still a serious danger in this scheme. Bob must keep the cipher text until he gets the information Alice sends him. If Eve breaks in Bob's office while he isn't present, she can make a copy of the cipher text without being found by Bob. So she can get the information by decrypt the cipher text with the information, that is to say, the scheme above is insecure under such attack.

In this paper we provide an information delay protocol which can prevent such attacks. First Alice and Bob share a sequence of two-qutrit systems in orthogonal product states. When Alice decides to let Bob get the information, she declares the state of the qutrits at her hands and sends dictates to Bob. Then Bob creates auxiliary qutrits and brings them together with the qutrits at his hands. Finally Bob

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

get the information by performing measurement on the composed systems and doing according to Alice's dictates. The information doesn't exist until Alice decides to let Bob know it. Moreover quantum no-cloning theorem forbids anyone to copy unknown states. These facts prevent Eve from getting the information by taking the attack above. The principles of quantum mechanics guarantee that our protocol is unconditionally secure. It's easy to carry out in practice and robust against noise and attacks.

2. BASIC IDEA

In quantum information science a two-state quantum system is often called a qubit while a three-state quantum system is called a qutrit. Once people thought that non-locality could only be found in entangled states system. But in [25] Bennett et al proved that a set of non-entangled orthogonal product states in a two-qutrit system can also show non-locality. There is a complete orthogonal set of states in such system

$$|\varphi_1>=|1>|1>,$$
$$|\varphi_2>=|0>\frac{1}{\sqrt{2}}(|0>+|1>),$$
$$|\varphi_3>=|0>\frac{1}{\sqrt{2}}(|0>-|1>),$$
$$|\varphi_4>=|2>\frac{1}{\sqrt{2}}(|1>+|2>),$$
$$|\varphi_5>=|2>\frac{1}{\sqrt{2}}(|1>-|2>),$$
$$|\varphi_6>=\frac{1}{\sqrt{2}}(|1>+|2>)|0>,$$
$$|\varphi_7>=\frac{1}{\sqrt{2}}(|1>-|2>)|0>,$$
$$|\varphi_8>=\frac{1}{\sqrt{2}}(|0>+|1>)|2>$$
$$|\varphi_9>=\frac{1}{\sqrt{2}}(|0>-|1>)|2> \quad (1)$$

in which we can perform a collective measurement on 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. We can design an information delay scheme based on this property as follows. First Alice and Bob agree to such coding rule.

Coding Rule:

$$|\varphi_2>\rightarrow 0 \quad |\varphi_3>\rightarrow 1$$
$$|\varphi_4>\rightarrow 0 \quad |\varphi_5>\rightarrow 1 \quad (2)$$

Alice creates a two-qutrit system in one of the nine states $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$ at random and records her choices. Then Alice sends the second qutrit to Bob and keeps the first qutrit at her hands. To discriminate the two qutrits, we mark them qutrit 1 and qutrit 2 respectively. When Bob receives qutrit 2, Alice declares the state of qutrit 1 while she still keeps the state of the two-qutrit system secret. If the state of two-qutrit system is $|\varphi_1>,|\varphi_6>,|\varphi_7>,|\varphi_8>$ or $|\varphi_9>$, Alice and Bob abandon it and turn to the first step, that is to say, Alice creates a new two-qutrit system again and repeat the following steps. If the state of two-qutrit system is $|\varphi_2>,|\varphi_3>,|\varphi_4>,$ or $|\varphi_5>$, Bob creates an auxiliary qutrit named qutrit E in the same state as qutrit 1. Then Bob performs collective measurement on the composed two-qutrit system consisting of qutri E and qutrit 2 in basis $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$. So Bob will get the state of the new two-qutrit system of qutri E and qutrit 1 which is just the same as the state of composed two-qutrit system of qutrit 1 and qutrit 2. From this fact we can come to an important conclusion as follows. If Alice wants to give Bob a bit "0", she only needs to do according to the following Rule 1.

Key Rule 1: If the state of the composed system of qutrit 1 and qutrit 2 is $|\varphi_2>,$ or $|\varphi_4>$, Alice asks Bob nothing to do but keep the bit he gets; If the state of the composed system of qutrit 1 and qutrit 2 is $|\varphi_3>,$ or $|\varphi_5>$, Alice asks Bo to reverse the bit he gets.

On the other hand, if Alice wants to give Bob a bit "1", she does according to Rule 2.

Key Rule 2: If the state of the composed system of qutrit 1 and qutrit 2 is $|\varphi_2>,$ or $|\varphi_4>$, Alice asks Bob to reverse the bit he gets. If the state of the composed system of qutrit 1 and qutrit 2 is $|\varphi_3>,$ or $|\varphi_5>$, Alice asks Bob nothing to do but keep the bit he gets.

Finally Bob is sure to get the bit which Alice wants to give him. The process of the coding rules can be summarized as following tables.

Table 1. Key Rule 1. ...

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

bit (Alice)	origin state	dictate	result (Bob)	bit (Bob)
0	$\|\varphi_2>$	nothing	$\|\varphi_2>$	0
	$\|\varphi_3>$	reverse	$\|\varphi_3>$	0
	$\|\varphi_4>$	nothing	$\|\varphi_4>$	0
	$\|\varphi_5>$	reverse	$\|\varphi_5>$	0

Table 2. Key Rule 2

bit (Alice)	origin state	dictate	result (Bob)	bit (Bob)
1	$\|\varphi_2>$	reverse	$\|\varphi_2>$	1
	$\|\varphi_3>$	nothing	$\|\varphi_3>$	1
	$\|\varphi_4>$	reverse	$\|\varphi_4>$	1
	$\|\varphi_5>$	nothing	$\|\varphi_5>$	1

In section 4 we will prove that by a well-designed error-checking process we can prevent anyone except Bob from getting the bit. So we can develop an information delay scheme based on these facts above.

3. INFORMATION DELAY SCHEME USING ORTHOGONAL PRODUCT STATES

Now we present our information delay scheme. If Alice wants to give Bob an n-bit string denoted as K which Bob can't read only when Alice wants him to do. They do as follows.

3.1. Share The Orthogonal Product States

First Alice tries to share n two-qutrit systems with Bob. They perform following steps.

step 1: Alice creates N two-qutrit systems (N>>n) in one state in the set $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$ at random and records her choices.

step 2: Alice sends qutrit 2 of each two-qutrit system to Bob.

step 3: After Bob receives the qutrits, to each two-qutrit system Alice chooses it out and declares its state if it is in the state $|\varphi_1>,|\varphi_6>,|\varphi_7>,|\varphi_8>$ or $|\varphi_9>$ while Alice keep its state secret if it is in the state $|\varphi_2>,|\varphi_3>,|\varphi_4>,$ or $|\varphi_5>$. Let's assume that there are m two-qutrit systems chosen out. So there are N-m two-qutrit systems left whose states are still secret.

step 4: To each of the m two-qutrit system, Bob creates an auxiliary qutrit (qutrit E) in the same state as the qutrit 1 whose state is now public. Then Bob performs collective measurement on the composed system consisting of the qutrit E and qutrit 2 in basis $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$.

step 5(error-checking): To each composed system consisting of qutrit E and qutrit 2 Bob compares his measurement result with the state of corresponding two-qutrit system consisting of qutrit 1 and qutrit 2 which Alice has declared. If there are too many disagreements, Alice and Bob abandon the scheme and turn back to step 1. Else they continue to step 6.

step 6: Alice and Bob choose n two-qutrit systems out at random and discard the others. Because N>>n, so they can always accomplish it.

After finishing steps above, Alice and Bob share n two-qutrit systems.

3.2. The Information Delay Scheme

Whenever Alice wants to let Bob get an n-bit string, they perform the following steps.

step 7: To each one of the left n two-qutrit systems, Alice declares the state of qutrit 1 of every two-qutrit system and send dictates to Bob according to K as Rule 1 and Rule 2 ask.

step 8: To each one of these two-qutrit systems Bob creates an auxiliary qutrit (qutrit E) in the same state as the qutrit 1. Then Bob performs collective measurements on the composed systems consisting of qutrit E and qutrit 2 in basis $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$ and records his measurement results. Next Bob does as Alice's dictates ask. Finally he will get an n-bit string named K1.

step 9: Obviously we have K1=K. It is just the information that Alice want to let Bob get in our information delay scheme.

So in the end Alice lets Bob get a string as she wants. Notice it, Alice and Bob may be far away from each other in space now. For example, Alice is in New York while Bob is in London.

4. SECURITY OF THE SCHEME

Our scheme is secure. No one except Alice and Bob can get the information. We prove it as follows. Let's assume that an eavesdropper, for example, Eve, wants to get the information. She may catch the qutrits sent from Alice to Bob and try to get something about the information. We can prove that it's impossible. From equation (1) we can

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

notice that the possible states set of qutrit 2 is $\{|0>,|1>,|2>,\frac{1}{\sqrt{2}}(|0>+|1>),\frac{1}{\sqrt{2}}(|0>-|1>),$ $\frac{1}{\sqrt{2}}(|1>+|2>),\frac{1}{\sqrt{2}}(|1>-|2>)\}$ which contains seven states. These states aren't orthogonal to each other. As known non-orthogonal quantum states are indistinguishable. So Eve can't know the state of qutrit 2 with certainty whatever she does, or in other words, she can't get the information just as Bob. We can estimate the probability she fortunately gets a bit. Notice that if Eve chooses exact the correct basis to measure qutrit 2 she catches, she may know the state of qutrit with certainty and get a bit of the information at last. Moreover to the qutrit, Eve can get its state with certainty only when she chooses the correct basis to measure. It's easy to find that there are three possible bases

$$B1=\{|0>,|1>,|2>\},$$
$$B2=\{\frac{1}{\sqrt{2}}(|0>+|1>),\frac{1}{\sqrt{2}}(|0>-|1>),|2>\}$$
$$B3=\{|0>,\frac{1}{\sqrt{2}}(|1>+|2>),\frac{1}{\sqrt{2}}(|1>-|2>)\} \quad (3)$$

If Eve choose the incorrect basis, she only get the state with a probability p(p<1). It can be summarized as the following table

Table 3. Probability

basis	B1	B2	B3
|0>	1	0	1
|1>	1	0	0
|2>	1	1	0
|s1>	0	1	0
|s2>	0	1	0
|s3>	0	0	1
|s4>	0	0	1

in which

$$s1=\frac{1}{\sqrt{2}}(|0>+|1>),\quad s2=\frac{1}{\sqrt{2}}(|0>-|1>),$$
$$s3=\frac{1}{\sqrt{2}}(|1>+|2>),\quad s4=\frac{1}{\sqrt{2}}(|1>-|2>).$$

Because no information can help Eve to choose correct basis, she has to measure qutrit 2 in one basis at random, or in other words, the probability that Eve choose any basis is 1/3. So from table 1 we can deduce that the probability that to the seven states Eve chooses the correct basis and get the bit are

$$p_1=1/3\times 2=2/3,\ p_2=1/3\times 1=1/3,$$
$$p_3=1/3\times 2=2/3,\ p_4=1/3\times 1=1/3$$
$$p_5=1/3\times 1=1/3,\ p_6=1/3\times 1=1/3,$$
$$p_7=1/3\times 1=1/3 \quad (4)$$

According to our scheme, Alice creates the two-qutrit systems in one state of the set $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$ at random. So for each state the probability is 1/9. From equation (1) and equation (4), the average probability which Eve get a bit without being found by Alice and Bob is

$$P=\frac{1}{9}\times(p_1\times 2+p_2+p_3\times 2 + p_4+p_5+p_6+p_7)$$
$$=\frac{13}{27} \quad (5)$$

The length of the information is n. So the probability for Eve to get the information is

$$P_{error}=p^n=\left(\frac{13}{27}\right)^n \quad (6)$$

If n=1000, we have

$$P_{error}=p^n=\left(\frac{13}{27}\right)^{1000}\approx 10^{-300} \quad (7)$$

It's a number too small to image. So Eve's attack can't succeed.

Since attacks by catching the qutrits fails, all that Eve can do is to listen to the public classical channel in which Alice sends her dictates to Bob. But she can just get the dictates that Alice tells Bob to perform operation on his strings from measurement results. The information is determined by not only Alice's dictates, but also Bob's measurement results which are kept secret by Bob. Eve can't get them. It's easy to prove that Eve could obtain no information about the information as follows. First the measurement results Bob gets is random, or in other words, Bob will get measurement results $|\varphi_2>,|\varphi_3>,|\varphi_4>,$ or $|\varphi_5>$ with equal probability 1/4 no matter what string Alice wants to send Bob. Then Alice sends dictates to Bob as the two key rules ask. We can easily deduct from the four tables in section 2 as follows. If Eve gets a dictate from Alice to Bob, for example, "nothing", she can't get any information about the string which Alice sends to Bob because it may be 0 or 1 with equal probability 1/2. The same result does she get if the dictate is "reverse". So Eve has no way to get the information than

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

random guessing. The probability she gets a correct two-bit string is

$$p_e = \frac{1}{2}. \quad (8)$$

Then the probability she gets the n-bit information is

$$P_{error} = p_e{}^n = \left(\frac{1}{2}\right)^n. \quad (9)$$

Let n=1000 which is a common length of a information. We have

$$P_{error} = \left(\frac{1}{2}\right)^{1000} \approx 10^{-300}. \quad (10)$$

It's also a number too small to image. So it's impossible foe Eve to get the information in fact, or in other words, Eve's attack fails.

Let's consider resend attack. Eve may catch all the qutrits sent from Alice to Bob and send fake qutrit to let Bob get fake information. But in step 5 of our scheme Alice and Bob perform error-checking. Because Eve doesn't know the states of the original two-qutrit systems created by Alice, she can only create two-qutrit systems at random in one state of $\{|\varphi_1>,|\varphi_2>,....,|\varphi_9>\}$ and send the second qutrits to Bob. So when Bob gets these qutrits and performs error-checking with Alice, they are sure to find many disagreements. The probability that Eve succeeds in cheating is equals to the probability that she just chooses the same state as Alice's two-qutrit system, which is 1/9. There are m two-qutrit systems for error-checking. So the probability for Eve to escape from being found by Alice and Bob is

$$P_{error} = \left(\frac{1}{9}\right)^m \quad (11)$$

If m=100, we have

$$P_{error} = \left(\frac{1}{9}\right)^{100} \approx 10^{-95} \quad (12)$$

So Alice and Bob are sure to find Eve's existing. They abandon the scheme and turn back to step 1. That is to say, Eve's attack fails.

Now we have proved that our scheme is unconditionally secure.

5. FESIBILITY ANALYSIS OF THE SCHEME

Notice that there are no entangled states and complex quantum operations needed in our scheme. All that people need to do is performing measurement on a qutrit and performing collective measurement on a two-qutrit system which have been mature technology in laboratory. So it's easier to carry out in practice. On the other hand in our scheme there are no producing and controlling entangled states and no complex quantum operations at all, which makes our scheme to have less fragility from noise, decoherence effects and possible attacks. So our scheme is more robust.

Second as known in quantum cryptographic schemes to keep quantum coherence is the most important and most difficult task. Especially in schemes using entangled states, the scheme is sure to fail if the entangled qubits lose coherence, or in other words, lose correlations between them. In practice quantum systems often undergo decoherence over time which make them lose quantum coherence and turn into classical systems inevitably. So the more work to handle and control quantum systems does a quantum cryptographic scheme need, the more difficult to accomplish is it. In our scheme the qutrits need to be tansfered for one time. To Alice, she won't handle quantum at all after step 2, which means that decoherence no longer affects Alice's work. It will reduce the risk of decoherence much for our scheme. On the other hand Alice and Bob don't exchange quantum information after step 2. What they need is only to exchange classical information. Or in other words, the quantum channel is no longer needed, which reduce the risk of decoherence of the quantum channel, too. So our scheme is easier to carry out in practice. This is a significant advantage of our scheme.

All that above discussions are based on the fact that Alice and Bob always use noiseless channels to send classical information and qutrits in our scheme. If there are no noiseless channels, can this scheme work? In our scheme they need an unjamed classical channel and a quantum channel. The quantum channel can be insecure. An eavesdropper can control it, which we have discussed in section 4. At the same time it can be a noisy channel in which occasional mistakes may occur at random. When a qutrit is affected by channel noise and changes its state, it seems that such accident will threaten our scheme. We can prove that such error can't cause our scheme fail. In step 4 of our scheme Alice and Bob do error-checking by comparing measurement results of m qutrits. If the error qutrit is in the m chosen qutrits, it will be found in the error-cheking and doesn't affect the process of information building. Only when the error qutrit isn't in the m chosen qutrits, it may be left to contribute a mistaken bit to the information. On the other hand

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

we can estimate the maximum probability that qutrit errors cause to the failure of the scheme. Let's assume that the error rate of the channel is e. Alice and Bob choose m two-qutrit systems to do error-checking from N two-qutrit system. So the probability that an error qubit is chosen out for error-checking is m/N. We can conclude that a qutrit error is from being found is

$$p = \frac{m}{N} \tag{13}$$

Then the probability that all error qubit escapes from being found is

$$P_{error} = (1 - \frac{m}{N})^{Ne} \tag{14}$$

Let e=0.1, m=200, N=2000, which is a reasonable assumption, we have

$$P_{error} = (1 - 0.1)^{200} \approx 0.000035 \tag{15}$$

It's an acceptable error rate for a noisy channel. If we need lower error-rate, we can use quantum error-correcting coding scheme which will be discussed in future work. So we can say that our scheme works well in a noisy quantum channel. However how about a noisy classical channel in our scheme? We can discuss it, too. In the step 2 in which Alice sends qutrits to Bob, the classical channel must be unjamed and error-free because Alice and Bob's error-checking needs to exchange classical information. On a noisy classical channel, it can't be accomplish to build shared the two-qutrit systems between Alice and Bob. Fortunately classical error-correcting coding technology has been a mature and powerful technology now. We can fulfill information transmission through a noisy classical channel with very low error rate by error-correcting coding. On the other hand in step 7 in which Alice sends dictates to Bob, we also need a classical channel. This channel can be unsecure. Eavesdroppers can control it and catch the dictates form Alice to Bob. They can even sends fake dictates to Bob. All this can't make Bob to get the faked information, which we have proved in section 4. But if there are noise in this channel which make a dictate error, Bob will be unable to get the correct information. So we need try to avoid the error caused by the channel noise. The solution to it is still error-correcting coding. We can guarantee that Bob get the correct dictates by transmitting them using error-correcting coding.

6. DISCUSSION AND CONCLUSION

In fact there are several variants of information delay scheme using orthogonal product states. For example, in the scheme Alice declares the state of qutrit 1 at her hands after Bob receiving qutrit 2. But Bob doesn't create auxiliary qutrits to build two-qutrit system and perform collective measurement on the composed two-qutrit system. Instead Alice ask Bob to measure the qubit at his hands directly in basis B2 or B3 in which

$$B2 = \{\frac{1}{\sqrt{2}}(|0> + |1>), \frac{1}{\sqrt{2}}(|0> - |1>), |2>\}$$
$$B3 = \{|0>, \frac{1}{\sqrt{2}}(|1> + |2>), \frac{1}{\sqrt{2}}(|1> - |2>)\} \tag{16}$$

On the other hand they agree to another coding rule.

Coding Rule(modified):

$$\frac{1}{\sqrt{2}}(|0> + |1>) \to 0, \frac{1}{\sqrt{2}}(|0> - |1>) \to 1$$
$$\frac{1}{\sqrt{2}}(|1> + |2>) \to 0, \frac{1}{\sqrt{2}}(|1> - |2>) \to 1 \tag{17}$$

It's easy to find that Alice and Bob will get the same result with certainty. If Alice wants to give Bob a bit "0", she only needs to do according to the following modified Rule 1.

Key Rule 1(modified): If the state qutrit 2 is $\frac{1}{\sqrt{2}}(|0> + |1>)$ or $\frac{1}{\sqrt{2}}(|1> + |2>)$, Alice asks Bob nothing to do but keep the bit he gets; If the state of the composed system of qutrit 1 and qutrit 2 is $\frac{1}{\sqrt{2}}(|0> - |1>)$ or $\frac{1}{\sqrt{2}}(|1> - |2>)$, Alice asks Bo to reverse the bit he gets.

On the other hand, if Alice wants to give Bob a bit "1", she does according to modified Rule 2.

Key Rule 2(modified): If the state of the composed system of qutrit 1 and qutrit 2 is $\frac{1}{\sqrt{2}}(|0> + |1>)$ or $\frac{1}{\sqrt{2}}(|1> + |2>)$, Alice asks Bob to reverse the bit he gets. If the state of the composed system of qutrit 1 and qutrit 2 is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$\frac{1}{\sqrt{2}}(|0>-|1>)$ or $\frac{1}{\sqrt{2}}(|1>-|2>)$, Alice asks Bob nothing to do but keep the bit he gets.

So we can design a modified information delay scheme just as in section 3. It also works well. We can issue some other methods to build information delay scheme. They have the same power and security as the first scheme we present in section 3.

An information delay scheme using orthogonal product states is present. By sharing orthogonal product states one person can give the other person some information which cannot be read until he or she lets the latter do. We prove that the scheme is unconditionally secure. There are no entangled states or complex quantum operations needed in our scheme. So it's easy to carry out in practice and robust against possible noise and attacks.

ACKNOWLEDGEMENT

This work is supported by Natural Science Foundation of China (Grants 61073023); we would thank Ruqian Lu for directing us into this research.

REFRENCES:

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithm and Factoring", Proceedings of 35th Annual IEEE Symposium on Foundations of Computer Science, Santa Fe, US, 1994, pp. 124-134.

[2] L. K. Grover, "A fast quantum mechanical algorithm for data search", Proceedings of the 28th ACM Symposium on Theory of Computing, 1996, pp. 212-219.

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

[4] A. K. Ekert, "Quantum cryptography based on Bell's theorem", Physical Review Letters, Vol. 67, 1991, pp. 661-663.

[5] C. H. Bennett, G. Brassard and N. D. Mermin, "Quantum cryptography without Bell's theorem", Physical Review Letters, Vol. 68, 1992, pp. 557-559.

[6] H. K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over arbitrarily long distances", Science, Vol. 283, 1999, pp. 2050-2056.

[7] B. Qi, Y. Zhao, X. F. Ma, H-K. Lo, and L. Qian, "Quantum key distribution with "dual detectors", Physical Review A, 2007, Vol. 75, pp. 052304.

[8] Y. Zhao,B. Qi, H-K. Lo, "Quantum key distribution with an unknown and untrusted source", Physical Review A, Vol. 77, pp. 052327, 2008.

[9] K. M. Horodecki, P. Horodecki, D. Leung and J. Oppenheim, "Quantum information distribution based on private states: unconditional security over untrusted channels with zero quantum capacity", IEEE Transaction Information Theory, Vol. 54, No. 6, 2008, pp.2604-2620.

[10] G. Zeng and W. Zhang, "Identity verification in quantum key distribution", Physical Review A, Vol. 61, 2000, pp. 022303.

[11] D. Ljunggren, M. Bourennane and Anders Karlsson, "Authority-based user authentication in quantum key distribution", Physical. Review A, Vol. 62, 2000, pp. 022305.

[12] Xiaoyu Li and H. Branum, "Quantum authentication using entangled states", International Journal of Foundation of Computer Science, Vol. 15, No. 4, 2004, pp. 609-617.

[13] A. Kent, W. Munro, T. Spiller, "Quantum Tagging: Authenticating Location via Quantum Information and Relativistic Signalling Constraints", Physical Review A, Vol. 84, 2011, pp. 012326.

[14] D. Gottesman, "Theory of quantum secret sharing", Physical Review A, Vol. 61, 2000, pp. 042311.

[15] P. Sarvepalli, "Non-Threshold Quantum Secret Sharing Schemes in the Graph State Formalism", Physical Review A, Vol. 86, 2012, pp. 042303.

[16] B. M. Terhal, D. P. DiVincenzo, D. W. Leung, "Hiding Bits in Bell States", Physical Review Letters, Vol. 86, 2001, pp.5807-5810.

[17] I. Chattopadhyay, D. Sarkar, "Local Indistinguishability and Possibility of Hiding cbits in Activable Bound Entangled States", Physics Letters A, Vol. 365, 2007, pp. 273-277.

[18] B. Schumacher, "Quantum Privacy and Quantum Coherence", Physical Review Letters, Vol. 80, 1998, pp.5695-5697.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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

[20] 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", 2004, eprints: quant-ph/0403104.

[21] W. T. Buttler et al., "Practical Free-Space Quantum Information Distribution over 1 km", Physical Review Letters, Vol. 81, 1998, pp.3283-3286.

[22]. V. Kalaichelvi, ”Design and analysis of secured electronic voting protocol”, Journal of Theoretical and Applied Information Technology, Vol. 34, No. 2, 2011, pp. 151-157.

[23] J. Sridhar, R. Senthil Kumar, S. Arun Kumar, “An optimal and cost effective key management scheme for secure multicast communication”, Journal of Theoretical and Applied Information Technology, Vol. 40, No. 2, 2012, p p. 202-207.

[24] K. Thair, A, Abdullah, “A hybrid schema zone-based key management for MANETs”, Journal of Theoretical and Applied Information Technology, Vol. 35, No. 2, 2012, pp. 175-183.

[25] C. Bennett, D. Divicenzo, C. Fuchs, *et al.*, “Quantum nonlocality without entanglement”, Physical Review A, Vol. 59, 1999, pp. 1070-1091.