Advanced Engineering Forum *Online: 2011-09-09*
ISSN: 2234-991X, Vol. 1, pp 178-182
doi:10.4028/www.scientific.net/AEF.1.178

Information delay protocol using non-orthogonal quantum states

Dexi Zhang[1,a] , Xiaoyu Li[2, b]

[1] College of Computer Science and Technology, Xuchang University, Xuchang City, 461000, the People's Republic of China

[2] School of Information Engineering, Zhengzhou University, Zhengzhou City, 450001, the People's Republic of China

[a]zdx@xcu.edu.cn, [b]iexyli@zzu.edu.cn

Keywords: information delay protocol; quantum cryptography; non-orthogonal states; quantum measurement; security.

Abstract. In this paper we provide an information delay protocol using non-orthogonal quantum states. One person can send the other person some information which cannot be read until he or she lets the latter do. The principles of quantum mechanics guarantee that the protocol is unconditionally secure. When the sender decides to let the other get the information, he or she need only to send the latter some dictates through a public classical channel. There are no entangled states and complex quantum operations except measurements needed in our protocol. So it is easier to carry out and more robust in practice.

1. Introduction

Quantum information science is the integration of quantum physics and 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 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) protocol is proposed by C. H. Bennett and G. Brassard [2]. So it's called BB84 protocol. Since then much research work has been done in quantum cryptography, such as quantum key distribution [3-7], quantum authentication [8-10], quantum bit commitment [11,12], quantum secret sharing [13-14], quantum information hiding [15-16], quantum obvious transfer[17,18], 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 Bob 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 key to decrypt it. Only when Alice decides to let Bob get the information, does she send the key 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 key. But she can't get the information because she hasn't the cipher text. However there is still a serious danger in this scheme. Bob must keep the cipher text until he gets the key 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 key, that is to say, the scheme above is insecure under such attack.

In [24] an information delay protocol using quantum entangled states is provided. But it needs that two sides share EPR pairs and keep them entangled for a long time which may be difficult in practice. In this paper we provide an information delay protocol which can prevent such attacks. First Alice send Bob some qubits. When Alice decides to let Bob get the information, she sends some dictates to Bob through a public classical channel. Finally Bob gets the information. The information doesn't exist until Alice decides to let Bob know it. Moreover quantum no-cloning theorem forbids anyone to copy unknown states. This facts prevent Eve from getting the information by taking the attack above. The principles of quantum mechanics guarantee that our protocol is unconditionally secure.

2. Basic idea

In quantum information science a quantum two-state system is often called a qubit. The state space of a qubit is a two-dimension Hilbert space. We can measure the state of the qubit in basis $\{|0>,|1>\}$ or basis $\{|+>,|->\}$ in which

$$|+>=\frac{1}{\sqrt{2}}(|0>+|1>)$$
$$|->=\frac{1}{\sqrt{2}}(|0>-|1>) \quad (1)$$

As known two non-orthogonal quantum states, such as |0> and |+>, or |1> and |-> and so on, can't be discriminated with certainty, or in other words, it's impossible to determine the state by doing any measurement form the state set $\{|0>,|1>,|+>,|->\}$. The famous BB84 QKD protocol is just based on this fact. Now we assume that Alice creates a qubit in one state of the state set $\{|0>,|1>,|+>,|->\}$ at random and records her choice. Then she sends the qubit to Bob. Obviously it's impossible for Bob to know what state the qubit is in. When Alice want to let Bob receive a bit of information '0', she does according to the following rule.

Rule 1: If the original state of the qubit is |0>, Alice ask Bob to measure it in basis {|0>,|1>}. When Bob gets result |0> or |1>, he records it respectfully as '0' or '1'.

If the original state of the qubit is |1>, Alice ask Bob to measure it in basis {|0>,|1>}. When Bob gets result |0> or |1>, he records it respectfully as '1' or '0'.

If the original state of the qubit is |+>, Alice ask Bob to measure it in basis {|+>,|->}. When Bob gets result |+> or |->, he records it respectfully as '0' or '1'.

If the original state of the qubit is |->, Alice ask Bob to measure it in basis {|+>,|->}. When Bob gets result |+> or |->, he records it respectfully as '1' or '0'.

So Bob is sure to record a piece of information '0', that is to say, he knows the information is '0'.

On the contrary if Alice wants to give Bob a bit of information '1'. She does as the following rule.

Rule 2: If the original state of the qubit is |0>, Alice ask Bob to measure it in basis {|0>,|1>}. When Bob gets result |0> or |1>, he records it respectfully as '1' or '0'.

If the original state of the qubit is |1>, Alice ask Bob to measure it in basis {|0>,|1>}. When Bob gets result |0> or |1>, he records it respectfully as '0' or '1'.

If the original state of the qubit is |+>, Alice ask Bob to measure it in basis {|+>,|->}. When Bob gets result |+> or |->, he records it respectfully as '1' or '0'.

If the original state of the qubit is |->, Alice ask Bob to measure it in basis {|+>,|->}. When Bob gets result |+> or |->, he records it respectfully as '0' or '1'.

So Bob is sure to record a piece of information '1', that is to say, he knows the information is '1'.

Now Alice can let Bob get the information at anytime as long as she wants. So we can design a information delay protocol based on this idea.

3. Information protocol using quantum entangled states

Now we present our information delay protocol.

A. How to transmit the qubits from Alice to Bob

First Alice creates m qubits at random in one of the four states $\{|0>,|1>,|+>,|->\}$. Then Alice sends them to Bob. These qubits can be transmitted through an insecure quantum channel. We can prove that it's secure by the technology provided by BB84 protocol [1]. No eavesdroppers can intercept in this process without being found.

step 1: Alice creates m qubits (m>>n) in one state in the set $\{|0>,|1>,|+>,|->\}$ at random and records her choice.

step 2: Alice sends all the qubits to Bob.

step 3: When Bob receives them, Alice and Bob choose m1 qubits out. Then to each qubit, Bob measures it in basis {|0>, |1>} or {|+>, |1>} at random.

step 4: Bob declares the basis he choose to measure the qubits. If he just chooses the "right" basis, that is to say, {|0>, |1>} for original state |0> or |1>, {|+>, |->} for original state |+> or |->, the qubits are kept while the others of the m1 qubits are abandoned.

step 5: To each one of the left qubits Alice compares her records with Bob's measurement results. If there are too many disagreements, they can be sure that an eavesdropper exists and turn to step 1. Or the left m-m1 qubits are the ones Bob received from Alice.

The number m-m1 is usually larger than the number n because m>>n. So Alice and Bob choose n qubit from the left m-m1qubits. It is the qubits which is needed in our quantum information delay protocol.

B . The information delay protocol

Now we give our information delay protocol using orthogonal quantum states. Whenever Alice wants to let Bob get an n-bit string. They do as following steps.

(1)To each bit of the string Alice tells Bob what to do. If the bit is '0', Alice does according to Rule 1 while if the bit is '1', Alice does according to Rule 2.

(2)When Bob receives Alice's dictates and finished measurements, Bob gets an n-bit string at last. It is just the information which Alice wants to give him.

4. Security of the protocol

Our protocol is secure. Bob can't get the information until Alice wants him to do. On the other hand no one except Alice and Bob can know the information. We prove it as follows.

First it is easy to find that Bob can't get the information until Alice wants him to do. At first Bob receives the qubits from Alice. But Bob can't do anything to get the information because Alice hasn't encode the information in these qubits. If Bob measures the qubits he holds, he can only get results |0> and |1> at random, which contain no information. Only when Alice decides to let Bob get the information, does she indicates Bob what to do. Only when Bob receives these dictates, can he measure the qubits at his hands and get the information.

Second let's assume that an eavesdropper, for example, Eve, wants to get the information. At first the process that Alice sends the qubits to Bob is secure, which has been proved in [1]. Eve can't intercept. All that she can do is to listen to the public classical channel in which Alice sends her dictates to Bob. But she just gets the dictates that Alice tells Bob to measure their qubits in one basis. The information is determined by Bob's measurement outcomes which is kept secret by Bob so that Eve can never get it. On the other hand although if Eve breaks in Bob's office while Bob isn't present, she can't make a copy of Bob's qubits because quantum no-cloning theorem forbids her to do such things. So our protocol is unconditionally secure.

Finally let's consider the fake information attack. Eve may impersonate Alice to send some dictates to Bob so as to give Bob the fake information. It's easy to prove this attack can't succeed. When Bob receives the fake dictates, he measures his qubits as our protocol asks. But Eve doesn't know the oringnal state at all, she has no way to guarantee that Bob get a determined measurement result which she wants Bob to get. So Bob can only get random $|0\rangle$ and $|1\rangle$. So Bob will get a random binary string containing no information. Moreover he can assure that the dictates must be fake at once.

So we have proved that our protocol is unconditionally secure.

5. Discussion and conclusion

Notice that there are no entangled states and complex quantum operation except measurement in our protocol, so it's easy to be achieved in practice. On the other hand after Alice sends Bob the qubits, Alice can let Bob get the information at any time even they may be separated by a long distance in space. Now all that they need is only a public classical channel between them. Since no quantum channels are needed now, many difficulties such as decoherence and noise of the quantum channel no longer exist. So our protocol is more robust.

In this paper we provide an information delay protocol using orthogonal quantum states. The principles of quantum mechanics guarantee that the protocol is unconditionally secure. And the protocol is easier to carry out and more robust in practice.

Acknowledgment

This work is supported by Natural Science Foundation of China (Grants 61073023); Natural Science Foundation of the Education Department of Henan Province of China(Grants 2010B520025) ;Natural Science Foundation of China (Grants 60873039). We would thank Ruqian Lu for directing us into this research.

References

[1] C. H. Bennet and G. Brassard: Proceedings of IEEE International conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE Press, 1984, pp.175.

[2] A. K. Ekert: Physical Review Letters, 67, 1991, pp.661-663.

[3] C. H. Bennett, G. Brassard and N. D. Mermin: Physical Review Letters, 68, 1992, pp.557-559.

[4] H. K. Lo and H. F. Chau: Science, 283, 1999, pp.2050-2056.

[5] A. Cabello: Physical Review Letters, 85, 2000, pp.5635-5638.

[6] P. Xue, C. F. Li and G. C. Guo: Physical Review A, 64, 2001, 032305

[7] X. Y. Li: International Journal of Modern Physics C, 14(6), 2003, pp.757-763.

[8] F. G. Deng and G. L. Long: Physical Review A, 70,2004, 012311.

[9] R. Namiki and T. Hirano: Physical Review A, 74, 2006, 032301.

[10] B. Qi, Y. Zhao, X. F. Ma, H-K. Lo, and L. Qian: Physical Review A, 75, 2007, 052304.

[11] Y. Adachi, T. Yamamoto, M. Koashi and N. Imoto: Physical Review Letters, 99, 2007, pp.180503

[12] Z. Q. Yin, Z. F. Han, F. W. Sun and G. C. Guo: Physical Review A, 76, 2007, 014304.

[13] R. Matsumoto: Physical Review A, 76, 2007, 062316.

[14] O. Ahonen, M. Mottonen, and J. L. O'Brien: Physical Review A, 78, 2008, 032314.

[15] Y. Zhao,B. Qi, H-K. Lo: Physical Review A, 77, 2008, 052327.

[16] T. Choi and M. S. Choi: Journal of Physics: Condensed Matter, 20, 2008, pp.275242.

[17] K. M. Horodecki, P. Horodecki, D. Leung and J. Oppenheim: IEEE Transaction Information Theory, 54(6), 2008, pp.2604-2620.

[18] C. H. Bennett, F.Bessette, G.Brassard, L.Salvail and J.Smolin: Journal of Cryptology, 5(1) , 1992, pp.3-28.

[19] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka and K, Nakamura: eprints: quant-ph/0403104.

[20] W. T. Buttler *et al*.: Physical Review Letters, 81, 1998, pp.3283-3286.

[21] X. Y. Li, D. X. Zhang: International Conference on Networking and Digital Society, 1, 2009, pp.25-28.

[22] Y. H. Kim, S. P. Kulik and Y. Shih: Physical Review Letters, 86, 2001, pp.1370-1373.

[23] C. Cinelli, M. Barbieri, F. De Martini and P. Mataloni: International Journal of Laser Physics, 15(1), 2005, pp.124-128.

[24] X. Y. Li, D. X. Zhang, Advanced Research on Industry, Information System and Material Engineering, 204-210, 1274-1278.