http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (11): 1912-1915, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.1912.1915

Deterministic Key Distribution Protocol Based on the Non-locality of Quantum Entangled States

[1]Li Xiaoyu and [2]Liju Chen
[1]School of Information Engineering, Zhengzhou University, Zhengzhou City, 450001, People's Republic of China
[2]Xi'an Communication Institute, Xi'an City, 761000, People's Republic of China

Abstract: In traditional quantum key distribution protocols the key is a random string produced in process of key distribution. This study provides a quantum deterministic key distribution protocol based on the non-locality of quantum entangled states. A predetermined string can be distributed to two parts as the key by virtue of the property of EPR (Einstain-Rosen-Podolsky) pair. The laws of quantum mechanics guarantee that the protocol is unconditionally secure. All operations needed in the protocol have already been mature technology in laboratory. So, it is easy to carry out in practice. The protocol can be widely applied in military and commercial affairs.

Key words: Deterministic key distribution, quantum cryptography, entangled states, EPR pair, security

INTRODUCTION

Quantum cryptography is the integration of quantum physics and cryptography. Unlike classical cryptographic protocols based on complexity of computation, quantum cryptographic protocols are based on the laws of quantum mechanics. So they can be unconditionally secure. In classical cryptography how to distribute the key is the most difficult problem. Quantum Key Distribution (QKD) protocol can help people to solve such difficulty. The principles of quantum physics guarantee that OKD protocols can be unconditionally secure. C. H. Bennett and G. Brassard provided the first Quantum Key Distribution (QKD) protocol which is called BB84 protocol (Bennett and Brassard, 1984). After that many QKD protocols have been developed (Ekert, 1991; Bennett *et al*., 1992a; Lo and Chau, 1999; Qi *et al*., 2007; Zhao *et al*., 2008; Horodecki *et al*., 2008; Barrett *et al*., 2012). At the same time experimental work for OKD has also been accomplished. Bennett *et al*. (1992a) realized BB84 protocol in laboratory (Bennett *et al*., 1992b). Now in optical fiber people have realized QKD beyond 150 km (Kimura *et al*., 2004) while in free space people have realized QKD over a distance of 1 km (Buttler *et al*., 1998). To most of the precious quantum key distribution protocols, the key which is shared by the two parts at last is a random binary string produced in the key distribution process. That is to say, it's impossible for the two parts to share a predetermined string as the key. But in business and military affairs people often need to choose a string from a code-book and distribute it as the key, which make it necessary to develop deterministic key distribution protocol. In this study we provide a deterministic key distribution protocol which is based on the non-locality of quantum entangled states. First Alice and Bob share some EPR pairs. Then they measure their qubits respectively according to a group of well-designed rules. Finally, they establish a shared key which can be a random predetermined string. The security of this protocol is guaranteed by the principles of quantum physics. What people need to do in the protocol are transmitting qubits through a quantum channel and performing single-particle measurements, which have been mature technology for a long time. So the protocol is easy to carry out in practice.

BASIC IDEA

In quantum information science a quantum two-state system is often called a qubit. Such states are possible states of a qubit:

$$|0>, |1>, |+>, |-> \quad (1)$$

In which:

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

Corresponding Author: Li Xiaoyu, School of Information Engineering, Zhengzhou University, Zhengzhou City, 450001, People's Republic of China

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

It can be noticed that they aren't orthogonal to each other. As known the four states form two complete orthogonal basic vector sets:

$$B_{01} = \{|0>, |1>\}$$

$$B_{+-} = \{|+>, |->\} \quad (3)$$

in which people can measure the qubit. It's known that non-orthogonal quantum states can't be discriminated from each other with certainty, that is to say, no ways to determine in which state a qubit is from the four states in Eq. 1 with certainty. Then there is a coding rule which is established first.

Coding rule:

$$|0>\rightarrow 0, |1>\rightarrow 1, |+>\rightarrow 0, |->\rightarrow 1$$

A two-qubit system can be the following state:

$$|\Phi^+>=\frac{1}{\sqrt{2}}(|00>+|11>) \quad (4)$$

which is one of the maximumly-entangled states of a two-qubit system. Such a two-qubit system is often called an EPR pair. As known entangled states can show non-locality, that is to say, if people measure the two qubits respectively, the measurement results are correlated. This fact has been applied widely applied in quantum cryptography.

Now Alice wants to share a predetermined n-bit string (denoted as P) as the key with Bob. First Alice and Bob share N (N>2n) EPR pairs in the state:

$$|\Phi^+>=\frac{1}{\sqrt{2}}(|0>_1|0>_2+|1>_1|1>_2) \quad (5)$$

in which Alice holds qubit 1 and Bob holds qubit 2. Then to each EPR pair Alice chooses to measure qubit 1 in basis {|0>, |1>} or {|+>, |->} at random. She declares the base which she measures them through a public classical channel. It can be denoted as:

$$B = (B_1B_2...B_n) \quad (6)$$

in which $B_i \in \{B_{01}, B_{+-}\}$. After getting B, Bob measures qubit 2 to each EPR pair according to B. It's obvious that Alice and Bob are sure to get the same measurement results. To each bit of P, if it is '0', they perform according to Key Rule 1 and Key Rule 2.

Key rule 1: If Alice gets measurement result |0> or |+>, she tells Bob to record as Coding Rule.

Key rule 2: If Alice gets measurement result |1> or |->, Alice tells Bob to add his result to his error-checking sequence E_2 while she adds the result to her error-checking sequence E_1. Then they turn to the next EPR pair.

To each bit of P, if it is '1', they perform according to Key rule 3 and 4.

Key rule 3: If Alice and Bob get measurement result |1> or |->, she tells Bob to record as Coding Rule.

Key rule 4: If Alice gets measurement result |0> or |+>, she tells Bob to add his result to his error-checking sequence E_2 while she adds the result to her error-checking sequence E_1. Then they turn to the next EPR pair.

Alice and Bob repeat it until Bob gets an n-bit string P'. It's easy to find that Bob will get the bit which Alice wants to share with him with a probability 1/2 for each EPR pair. There are N (N>2n) EPR pairs. So they can always achieve it. If there are no eavesdroppers and errors existing, they can be sure that P' = P. This is just the key which Alice and Bob share. To confirm that no errors or eavesdroppers exit, Alice and Bob compare the error-checking sequence E1 and E2. If there are too many disagreements, they abandon the key distribution process and start it again. Or they can affirm that the key distribution has been accomplished successfully. In the following sections it will be proved that no one except Alice and Bob can get the key. So a deterministic key distribution protocol can be established based on this idea.

DETERMINISTIC KEY DISTRIBUTION PROTOCOL BASED ON THE NON-LOCALITY OF ENTANGLED STATES

Now the deterministic key distribution protocol is given as follows.

If Alice wants to share a predetermined n-bit string P is with Bob as the key, they do as the following steps:

Step 1: Alice creates N (N>2m) EPR pairs in the state $|\Phi^+>$. Then to each EPR pair she sends the second qubit to Bob and keeps the first qubit at her hands

Step 2: To each EPR pair Alice measures the qubit at her hands in basis {|0>, |1>} or {|+>, |->} at random. Then Alice declares the base to all EPR pairs which is denoted as a sequence B

Step 3: To each EPR pair Bob measures the qubit at his hand according to B

Step 4: To each bit of the string P Alice tells Bob what to do. If the bit is '0', Alice does according to Key Rule 1 and Key Rule 2 while Alice does according to Rule 3 and Rule 4 if the bit is '1'. Finally Bob also gets an n-bit string P'. On the other hand Bob gets a result sequence E_2 while Alice gets a result sequence E_1

Step 5: Alice and Bob compare E_1 and E_2. If there are too many disagreements, they abandon the protocol and turn back to step (1) to restart the key distribution. Or they can be sure P = P' which is just the key they have shared

So Alice and Bob have established a key. On the other hand if Bob wants to share a predetermined string with Alice as the key, they need only exchange their roles in the protocol.

SECURITY OF THE PROTOCOL

The protocol is secure. No one except Alice and Bob can get the key. It's proved it as follows.

Let's assume that an eavesdropper, for example, Eve, wants to get the key. At first Eve may catch the qubit sent from Alice to Bob. But she can't get any information about the key by measuring the qubits. If Eve measures them in {|0>, |1>}, she can only get measurement result |0> or |1> with the equal probability 1/2. If Eve measures them in {|0>, |1>}, she can only get measurement result |+> or |-> with the equal probability 1/2. What Eve gets has nothing about the key. So Eve's attack fails.

On the other hand let's consider another strategy of attack. Eve may perform attack of entanglement, that is to say, Eve creates an auxiliary qubit (called qubit E) in the state |0>. Then she makes it entangled with the qubit (qubit 2) sent form Alice to Bob. For example, Eve may do CNOT operation on them in which the qubit 2 the target qubit and qubit E is the control qubit. So the state of the four-qubit system turns to:

$$|S>=\frac{1}{\sqrt{2}}(|0>_1|0>_2|0>_E+|1>_1|1>_2|1>_E) \tag{7}$$

When Alice and Bob measure their qubits, the auxiliary qubit also collapses from which Eve may try to get some information about the key by measuring qubit E. But in the protocol entanglement attack can't succeed because Alice and Bob will measure the qubits in basis {|0>, |1>} or in basis {|+>, |->} with the equal probability 1/2. If Alice measures qubit 1 in basis {|0>, |1>}, Eve can get the same result as Alice. It's easy to find that Eq. 7 can be rewritten as:

$$|S>=\frac{1}{\sqrt{2}}(|+>_1|+>_2|+>_E+|+>_1|->_2|->_E +|->_1|+>_2|->_E+|->_1|->_2|+>_E) \tag{8}$$

If Alice measures qubit 1 in basis {|+>, |->}, Eve will get the same result or the contrast result as Alice with the equal probability 1/2. So the probability that Eve just get the same result as Alice to each EPR pair is:

$$P=\frac{1}{2}\times 1+\frac{1}{2}\times\frac{1}{2}=\frac{3}{4} \tag{9}$$

In the protocol Alice and Bob perform error-checking by compare result sequence E_1 and E_2. If there are k items in E_1 or E_2, the probability that Eve escapes from being found is:

$$P_{error}=\left(\frac{3}{4}\right)^k \tag{10}$$

If k = 200

$$P_{error}=\left(\frac{3}{4}\right)^{200}\approx 10^{-25} \tag{11}$$

It's a number too small to imagine. So we can affirmatively say that Eve is sure to be found by Alice and Bob, or in other words, such attack also fails.

Now, it has been proved that this protocol is unconditionally secure.

CONCLUSION

In the protocol Alice and Bob need only do single-particle measure and exchange qubits which have been carried out in laboratory for many years. The protocol can be accomplished without any technical difficulties. So it's easy to carry out in practice.

In this study a deterministic key distribution protocol based on the non-locality of quantum entangled states is presented. The laws of quantum mechanics guarantee that the protocol is unconditionally secure. No one except Alice and Bob can get the key. On the other hand the protocol is easy to fulfill in practice.

ACKNOWLEDGMENT

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

REFERENCES

Barrett, J., R. Colbeck and A. Kent, 2012. Unconditionally secure device-independent quantum key distribution with only two devices. Phys. Rev. A, Vol. 86.

Bennett, C.H. and G. Brassard, 1984. Quantum cryptography: Public-key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, December 1984, Bangalore, India, pp: 175-179.

Bennett, C.H., F. Bessette, G. Brassard, L. Salvail and J. Smolin, 1992a. Experimental quantum cryptography. J. Cryptol., 5: 3-28.

Bennett, C.H., G. Brassard and N.D. Mermin, 1992b. Quantum cryptography without Bell's theorem. Phys. Rev. Lett., 68: 557-559.

Buttler, W.T., R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux and G.G. Luther *et al*., 1998. Practical free-space quantum key distribution over 1 km Phys. Rev. Lett., 81: 3283-3286.

Ekert, A.K., 1991. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 67: 661-663.

Horodecki, K., M. Horodecki, P. Horodecki, D. Leung and J. Oppenheim, 2008. Quantum key distribution based on private states: Unconditional security over untrusted channels with zero quantum capacity. IEEE Trans. Inform. Theory, 54: 2604-2620.

Kimura, T., Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, K and K. Nakamura, 2004. Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum. Jpn. J. Appl. Phys., 43: L1217-L1219.

Lo, H.K. and H.F. Chau, 1999. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283: 2050-2056.

Qi, B., Y. Zhao, X.F. Ma, H.K. Lo and L. Qian, 2007. Quantum key distribution with dual detectors. Phys. Rev. A, Vol. 75.

Zhao, Y., B. Qi and H.K. Lo, 2008. Quantum key distribution with an unknown and untrusted Phys. Rev. A, Vol. 77. 10.1103/PhysRevA.77.052327.