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 12 (16): 3820-3824, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.3820.3824

Unconditionally Secure Public-key Cryptosystem using Entangled Quantum States

Xiaoyu Li, Yuqing Ma
School of Information Engineering, Zhengzhou University,
Zhengzhou City, 450001, People's Republic of China

Abstract: This study presents an unconditionally secure public-key cryptosystem using entangled quantum states. Users share a group of entangled quantum systems with a Key Management Center (KMC) as the private key and the public key. Any two users can exchange secret information by the help of KMC. At the same time a user can also perform digital signature on the information to be transmitted. The principles of quantum physics guarantee that this public-key cryptosystem is unconditionally secure. No quantum channels are needed between two users. On the other hand users needn't perform complex quantum operations. So, the cryptosystem is easy to carry out in practice and more robust against attacks.

Key words: Public-key cryptosystem, quantum cryptography, entangled quantum states, the bell state measurement, digital signature

INTRODUCTION

Public-key cryptosystem is widely applied in modern society. In fact it's the base of network security, e-commerce and digital society technology *et al.* As known classical public-key cryptosystems are based on the complexity of computation, such as RSA algorithm (Rivest *et al.*, 1978), DH algorithm (Diffie and Hellman, 1976) and ECC algorithm (Koblitz, 1987) But P. Shor proved that RSA algorithm is insecure on future quantum computer (Shor, 1994). So, do almost all classical public-key algorithms. A possible solution to this threat is quantum public-key algorithm which is a field in quantum cryptography. Quantum cryptography is the integration of classical cryptography and quantum physics in which its unconditional security is guaranteed by not the complexity of computation but the principles of quantum physics. In 1984 Bennett *et al.* presented the first quantum key distribution protocol (Bennett and Brassard, 1984). Since then much theoretical and experimental work has been done in quantum cryptography (Ekert, 1991; Zhao *et al.*, 2008; Horodecki *et al.*, 2008; Barrett *et al.*, 2012). Recently the first quantum public-key scheme based on the rotation of single particle is provided (Nikolopoulos, 2008). Then several quantum public-key cryptosystems have been developed (Nikolopoulos and Ioannou, 2009; Ioannou and Mosca, 2009, 2011; Seyfarth *et al.*, 2012).

In this study, an unconditionally secure public-key cryptosystem using entangled states is presented. It's based on the non-locality of entangled quantum states. By sharing entangled states with KMC as the private keys and the public keys, users can achieve secret communications and digital signature. The laws of quantum physics guarantee the unconditional security of this public-key cryptosystem. No quantum channels are needed between any two users. So, it's easier to carry out in practice and more robust against possible attacks.

BASIC IDEA

A quantum two-state system is often called a qubit in quantum information science. A two-qubit system can be in one of the four maximumlly entangled states:

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

$$|\Phi^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$$

$$|\Psi^+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$$

$$|\Psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) \quad (1)$$

They are also called Bell states while such a two-qubit system is called an EPR (Einstain-Podolsky-Rosen) pair. As known the four Bell states form a complete orthogonal basic vector set $\{|\Phi^+\rangle,|\Phi^-\rangle,|\Psi^+\rangle,|\Psi^-\rangle\}$ in

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

which people can measure a two-qubit system. Such measurement is called the Bell state measurement which has been carried in Laboratory (Bennett and Wiesner, 1992).

Now let's assume a public-key cryptosystem including N users and a key management center. A user, such as Alice, shares M EPR pair with KMC in the state:

$$|\Phi^+>_{12}=\frac{1}{\sqrt{2}}(|0>_1|0>_2+|1>_1|1>_2) \quad (2)$$

in which Alice holds qubit 1 and KMC holds qubit 2. So, the M-qubit sequence (denoted as Q^R) hold by Alice is called the private key while the M-qubit sequence hold by KMC (denoted as Q^U) is called the public key. Every user can exchange qubits with KMC through an insecure quantum channel which can be controlled by any person. On other hand there an authenticated public classical channel through which everyone can exchange classical information. But no one can disguise as others to send some information. If another user, such as Bob, wants to sends a message (denoted as an n-bit string P) to Alice, he first asks KMC for Alice's public key. After getting Q^U, Bob creates an auxiliary qubit (denoted as qubit A) in the state $|1>$ to each qubit in Q^U. Then he performs a CNOT (controlled not) operation on the composed system of qubit 2 and qubit A in which the former is the target qubit and the latter is the control qubit. So, the state of the whole three-qubit system turns into:

$$|S>_{12A}=\frac{1}{\sqrt{2}}(|0>_1|1>_2|1>_A+|1>_1|0>_2|1>_A) \quad (3)$$

It can be rewritten as:

$$|S>_{12A}=\frac{1}{\sqrt{2}}[|0>_1(|\Phi^+>_{2A}-|\Phi^->_{2A})$$

$$|1>_1(|\Psi^+>_{2A}-|\Psi^->_{2A})] \quad (4)$$

Now if Alice measures each qubit 1 in Q_R and Bob performs the Bell state measure on the composed system of qubit 2 and qubit A, their measurement results are correlated with each other. It can be showed in the following Table 1.

Alice and Bob agree to the following coding rule.

Coding rule:

$$|0>\rightarrow 0, \qquad |1>\rightarrow 1$$

$$|\Phi^+>,|\Phi^->\rightarrow 0, \quad |\Psi^+>,|\Psi^->\rightarrow 1$$

Table 1: Correlations of measurement results

Alice's result	$\|0>$	$\|1>$
Bob's result	$\|\Phi^+>$	$\|\Psi^+>$
	$\|\Phi^->$	$\|\Psi^->$

Then Alice and Bob record their measurement results respectfully according to Coding Rule. It's obviously to find that they will get an identical n-bit string denoted as K. Then Bob encrypts the plain text P by perform an XOR operation on P and K to get:

$$EP = P \oplus K \quad (4)$$

in which EP is just the cipher text. Next Bob sends EP to Alice through the classical channel. When Alice receives EP, she performs XOR operation on EP and K. Finally Alice gets:

$$DP = K \oplus EP = K \oplus (P \oplus K) = P \quad (5)$$

So, Alice gets the message which Bob wants to send her. Later we will prove that any other one including KMC can't get the message. So, users can achieve secret communications by the public-key cryptosystem.

There is a problem left. Both the public key and the private key are consumed after the communication finishes. So, a user must share many (private key, public key) pairs with KMC if more than one user want to send message to Alice or a user wants to send message to Alice for more than one time. Every (private key, public key) pair should be given a unique id number to discriminate them.

UNCONDITIONLLY SECURE PUBLIC-KEY CRYPTOSYSTEM USING ENTANGLED QUANTUM STATES

Now the public-key cryptosystem is given as follows. There are N users and a KMC in the public-key cryptosystem. Every user, such Alice, creates L (private key, public key) pairs in which every pair includes M EPR pairs in the state:

$$|\Phi^+>_{12}=\frac{1}{\sqrt{2}}(|0>_1|0>_2+|1>_1|1>_2) \quad (6)$$

To each EPR pair Alice holds qubit 1 and KMC holds qubit 2. So, the public keys set of Alice is denoted as:

$$K_{PU}=\{(i,Q_i^U), \quad i=1,2,...L\} \quad (7)$$

The public key set of Alice is denoted as:

$$K_{PR}=\{(i,Q_i^R), \quad i=1,2,...L\} \quad (8)$$

There is a quantum channel through which a user asks KMC for another user's public key. The quantum channel is insecure so that every one can control it. On the other hand every user including KMC can exchanged classical information through an authenticated public classical channel. Every one can listen to the classical channel but no one can impersonate others to send fake message. Now if another user, such Bob, wants to send Alice an n-bit string (denoted as P), they perform the following steps.

Step 1: Bob asks KMC for one of Alice's public keys

Step 2: KMC chooses Alice's no. j public key Q_j^U at random and sends it to Bob

Step 3: (error checking) After receiving Q_j^U, Bob chooses t qubits (t = M-n) and measure them in basis {|0>, |1>} or in basis:

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

at random. Then Alice measures the corresponding qubits of Q_j^R in the same base as Bob. If there are too many disagreements, they abandon the process of communication and turn to step 1. Else they continue into the next step

Step 4: To each left n qubit(denoted as qubit 2) in Q_j^U Bob creates an auxiliary qubit (denoted as qubit A) in the state |1> and performs a CNOT operation on them in which qubit A is the control qubit and qubit 2 is the target qubit. At the same time Bob records his measurement results according to Coding Rule. Finally he gets an n-bit string K

Step 4: Bob performs an XOR operation on the plain text P and K to get the cipher text EP. Then Bob sends EP to Alice through the classical channel

Step 6: When Alice receives EP, she measures the left n qubits of Q_j^R in basis {|0>, |1>}. At the same time Alice records her measurement results according to Coding Rule. Finally she also gets an n-bit string K'. Obviously K' = K

Step 7: Alice performs an XOR operation on EP and K. Finally she get an n-bit string P' which is just identical to P

So, Alice has gets the secret message which Bob wants to send her.

On the other hand, Bob can perform digital signature on the message so that, Alice can affirm that the message is really from Bob and hasn't been tempered. If Bob wants to send a message P' to Alice, he first signed it according the following steps:

Step 1: Bob produces an abstract PA from P' by a hash algorithm, for example, SHA-1 algorithm. Let's assume that the length of PA is m

Step 2: Bob chooses one of his private keys, such as no. k private key Q_k^R at random. Then he measure the first m qubits of Q_k^R in basis {|0>, |1>} and records his measurement results according Coding Rule. Finally he gets an m-bit string PK

Step 3: Bob performs an XOR operation on PA and PK to get an m-bit string PE. Then he puts put P', k and PE together to form an n-bit string P

So, P is just the plain text which Bob will send to Alice. It must be pointed out that the length of P should be n, or in other words, the sum of the length of P', the length of PE and the length of k must be n. If it doesn't satisfy, people can always make it by dividing P' into a few parts or supplementing P' by redundant bits. When Alice receives the plain text P, she first decodes it and gets P', PE and k. Then Alice and Bob perform the following steps to verify the signature.

Step 1: Alice asks KMC for Bob's no. k public key Q_k^R

Step 2: Alice measures the first m qubit of Q_k^U and records his measurement results according to Coding Rule. Finally she gets an m-bit string PK'

Step 3: Alice performs an XOR operation on PE and PK' to gets a string PA''

Step 4: Alice also produces an abstract PA' from P' by SHA-1 algorithm. If PA' = PA'', the signature verification passes. Or it fails

So, Alice can assure that the message is really from Bob and hasn't been tempered.

SECURITY OF THE CRYPTOSYSTEM

This public-key cryptosystem is secure. It's proved as follows.

Let's assume that an eavesdropper, such as Eve, wants to get the message. First Eve can catch the cipher text EP sent from Bob to Alice. But the cipher text EP is produced by P⊕K. Since Eve has no K, she can't recover the plain text P. As known K is a random string produced from the measurement results of Alice and Bob. So, the probability that Eve gets P without K is no more than just guessing every bit of P in which:

$$p=(\frac{1}{2})^n \quad (9)$$

If n = 1000:

$$p = (\frac{1}{2})^{1000} \approx 10^{-300} \quad (10)$$

It's a number too small to imagine. So, Eve can't get message at all.

Second Eve may try to get K to help her decoding EP. For example Eve may catch Alice's public key Q_j^U when it's sent from KMC to Bob. But now Q_j^U is only a qubit sequence in which every bit is a part of an EPR pair. It contains no information about the string K which is produced by Alice's and Bob's measurement results on Q_j^R and Q_j^U later. Moreover Eve is sure to be found in step 3 in which Alice and Bob perform error-checking.

Third Eve may take attack of entanglement. When Q_j^U is sent from KMC to Bob, Eve catches it. Then Eve creates an auxiliary qubit in the state $|0\rangle$ to every qubit in Q_j^U and performs CNOT operation on them in which the former is the target qubit and the latter is the control qubit. Eve may try to get some information about key by measuring the auxiliary qubits after Alice's and Bob's measurements. It's easy to prove that Eve will be found by Alice and Bob in the error checking process. So, this attack also fails.

Fourth it can be proved that the digital signature is secure. It's based on the correlations of EPR pairs, or in other word, Bob's Q_k^R and Q_k^U. No one except Bob can produce the signature to pass Alice's verification. On the other hand SHA-1 algorithm guarantees that the plain text can not be tempered.

Sixth it is easy to find that KMC can do nothing more than Eve. So, KMC also can't get the message.

Finally since in this public-key cryptosystem one (private key, public key) pair can be used for only one time, it is immune to many kinds of attacks, such as forward search attack, resend attack and chosen text attack.

DISCUSSION AND CONCLUSION

There are no quantum channels needed between any two users because they needn't exchange qubits at all. So, the public-key cryptosystem is easier to carry out in practice. Obviously it's a significant advantage.

The public-key cryptosystem depends on the special properties of quantum systems. But a quantum systems always undergoes decoherence with time which makes it lose quantum coherence inevitably. So, the public-key cryptosystem doesn't work. This problem can be solved by two methods. One is using the system which has a long time of docoherence, such as photon in optical fiber. The other one is that users can update their (private key, public key) pairs periodically before they undergoes decoherence.

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. and S.J. Wiesner, 1992. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. Phys. Rev. Lett., 69: 2881-2884.

Diffie, W. and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654.

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.

Ioannou, L. and M. Mosca, 2009. Public-key cryptography based on bounded quantum reference frames. ArXiv:quant-ph/0903.5156, August, 2011. http://arxiv.org/pdf/0903.5156.pdf.

Ioannou, L. and M. Mosca, 2011. Unconditionally-secure and reusable public-key authentication. Proceedings of the 6th Conference on the Theory of Quantum Computation, Communication and Cryptography, May 24-26, 2011, San Diego, CA., pp: 13-27.

Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209.

Nikolopoulos, G.M. and L. Ioannou, 2009. Deterministic quantum-public-key encryption: Forward search attack and randomization. Phys. Revi. A, Vol. 79.

Nikolopoulos, G.M., 2008. Applications of single-qubit rotations in quantum public-key cryptography. Phys. Rev. A, Vol. 77. 10.1103/PhysRevA.78.019903

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM., 21: 120-126.

Seyfarth, U., G.M. Nikolopoulos and G. Alber, 2012. Symmetries and security of a quantum-public-key encryption based on single-qubit rotations. Phys. Rev. A, Vol. 85. 10.1103/PhysRevA.85.022342

Shor, P.W., 1994. Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, November 20-22, 1994, Santa Fe, NM., pp: 124-134.

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.