Extended Abstract of “Quantum public-key cryptosystem without quantum channels between any two users”

Xiaoyu Li
School of Information Engineering
Zhengzhou University
Zhengzhou City, P. R. China
iexyli@zzu.edu.cn

Yun Shang[1,2]
[1]Institute of Mathematics, Academy of Mathematics and System Science
Chinese Academy of Sciences
Beijing City, P. R. China
[2]NCMIS, Academy of Mathematics and System Science
Chinese Academy of Sciences
Beijing City, P. R. China
shangyun602@163.com

Traditional symmetrical encryption algorithms in which encryption and decryption use the same key are faced with a difficult problem: how to distribute and manage keys if there are many users in a cryptosystem? If N users want to communicate with each other, one user must share a key with any other user. So every user must keep N-1 keys secret to exchange information with the other N-1 users respectively. Moreover, N(N-1)/2 key distribution processes should be implemented before the cryptosystem begins to work. It’s very hard to guarantee it when N is a large number. On the other hand in practice maybe the users don’t trust each other, which make key distribution impossible from the beginning. As known in classical cryptography a solution to overcome such difficulties is public-key cryptosystem, such as RSA algorithm [1] et al. Every user has a (public key, private key) pair. The public key is kept open to every user by a key management center (KMC) while the private key is kept secret by the user. If a user Bob want to send a secret message to another user Alice, he uses Alice’s public key to encrypt the plain text while Alice uses her private key to decrypt the cipher text. Classical public-key cryptosystem has been widely used in modern society, such as commercial affairs, military affairs, network communications et al.

But in 1994 Peter Shor proved that RSA algorithm can be cracked in polynomial time on future quantum computer [2]. So the classical public-key cryptosystems based on RSA algorithm will collapse inevitably faced with a quantum computer. So do several most popular classical public-key cryptosystems. Quantum public-key technology may be a good solution to resist such danger. It originated form a paper of Gottesman which present a quantum one-way function to design quantum message authentication protocol [3]. This idea may be used in a public-key system. In 2008 Nikolopoulos presented the first unconditionally secure quantum public-key protocol [4] which based on the single-particle rotation of unknown quantum states. Since then people have developed several public-key protocols one after another [5-8].

Until now most of the quantum public-key protocols require that users accomplish communication by exchange qubits, which means that there must be a quantum channel between any two users. It may be difficult to guarantee in reality. Moreover quantum channel is more fragile, which reduces the robustness of quantum public-key cryptosystems. In this paper we provide a quantum public-key cryptosystem without quantum channels between any two users which is based on the non-locality of entangled states. It is based on the non-local correlation in an entangled quantum system. With the help of the key management center, N users can communicate with each other securely. Moreover message authentication can be fulfilled naturally by the public-key cryptosystem. No quantum channels are needed among users. So it’s easier to carry out and more robust in practice.

Let’s introduce our quantum public-key cryptosystem. First we have

Key Rule:

$$|0>\to 0, \quad |1>\to 1, \quad |+>\to 0, \quad |->\to 1 \tag{1}$$

and two measurement basis.

$$B_{01}=\{|0>,|1>\} \qquad B_{+-}=\{|+>,|->\}\ . \tag{2}$$

There are N users and a key management center (KMC) in the public-key cryptosystem. Any two users can exchange classical information through an authenticated public classical channel. The classical channel is public so that everyone can listen to it and catch the classical information transmitted through it. But a user can affirm the identity of the other at the end of the channel, or in other words, no one can impersonate other to send fake information through the classical channel. As known such an authenticated public classical channel is necessary to nearly all quantum cryptographic protocols including famous BB84 protocol et al. On the other hand every user can exchange qubits with KMC through an insecure quantum channel. But two users needn't to exchange qubits so that no quantum channels are needed to connect them. Every user creates $L \times M$ EPR pairs in the state $|\Phi^{+}>$ in which every M EPR pairs are given a unique id numbers as a (public key, private key) pair. Then she shares all the EPR pairs with KMC in which to each EPR pair the first qubit is hold by the user himself while the second qubit is hold by KMC. So a user's public keys set can be denoted as

$$K_{PK} = \{ \, (i, Q_i^{\,K}), \quad i = 1,2,..., L \, \} \tag{3}$$

in which $Q_i^{\,K}$ is a M-qubit sequence with the id number i. the user's private key set can be denoted as

$$K_{PA} = \{ \, (i, Q_i^{\,A}), \quad i = 1,2,..., L \, \} \tag{4}$$

in which $Q_i^{\,K}$ is the corresponding M-qubit sequence with the id number i. All users' public keys are kept by KMC and open to everyone who wants get them. But a user must keep his private keys absolutely secret by himself so that no other one including KMC can get.

The process of communication can be described as follows. If a user, such as Bob, wants to send an *n*-bit string *P* to another user Alice. They do according to the following steps.

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

Step 2: KMC chooses one public keys $(j, Q_j^{\,K})$ from Alice's public key set K_{PK} at random and sends it to Bob.

Step 3: When Bob receives $(j, Q_j^{\,K})$, he sends the id number *i* to Alice.

Step 4: When Alice receives the id number *i*, she measure the corresponding private key $(j, Q_j^{\,A})$ in basis B_{01} or B_{+-} at random and records her measurement basis sequence as *B*. Then Alice records her measurement results according to Key Rule. Finally she gets an *M*-bit string *S*'.

Step 5: Alice send her basis sequence *B* to Bob.

Step 6: When Bob receives *B*, he measures $(j, Q_j^{\,K})$ according to *B* and records his measurement basis according to Key Rule. Finally Bob also gets an *M*-bit string *S'*.

Step 7(error-checking): Alice chooses *t* bits (*t*=*M*-*n*) at random from *S* and Bob chooses the corresponding bits from *S*' respectively. Then they compare them. If there are too many disagreements, they abandon the communication process and turn back to step 1. Or Alice and Bob keep the left *n*-bit string *K* and *K*' respectively and continue into next step.

Step 8: Bob performs an XOR operation on *P* and *K*' to get the cipher text *EP*. Then Bob sends *EP* to Alice.

Step 9: When Alice receives *EP*, she performs an XOR operation on *EP* and *K* to get a string *P*'.

Obviously they know *P*'=*P*. So Alice has obtained the message that Bob sends her. If Alice wants to send a secret message to Bob, they need only exchange the roles in the process above. So any two users can achieve secret communications by this public-key cryptosystem.

The message authentication and verification can be described as follows. If Bob sends a secret message *P* to Alice, he can sign the message to prove his identity and the integrity of the message to Alice. What Bob needs to do is to attach a classical message (the signed message) with the original message that he wants send to Alice. To produce the signed message, Bob performs the following steps.

Step 1: Bob produces an m-bit abstract *PA* from *P* which he wants to send Alice by a hash algorithm, such as SHA-1 algorithm.

Step 2: Bob chooses one of his private keys at random, such as (i, R_i^A). Then he performs measurement the first m qubits of (i, R_i^A) in basis $\{|0>, |1>\}$ and records his results according to Key Rule. So Bob gets a string *PK*.

Step 3: Bob performs XOR operation between *PA* and *PK*. Finally he gets an *m*-bit string *PS* which is just the signed message.

Step 4: Bob attaches *PS* and the id number *i* with *P*. So he gets a string *PX* which is the plain text to be submitted to Alice.

Notice that now the length of *PX* should be *n*. So the length of the original message *P* added with the length of *k* should be *n-m*. If *P* can't satisfy it, we can always make it by dividing it into several parts or adding supplementary bits.

Then Bob and Alice can finish the communication process.

After Alice gets the plain text *PX*, she can extract the original message *P*, the signed message *PS* and the id number *i.* To verify the message, she does the following steps.

Step 1: Alice asks KMC for Bob's no. *i* public key (i, R_i^K) .

Step2: Alice measure (i, R_i^K) in basis $\{|0>, |1>\}$. Then she takes the first m measurement results and records according to Key Rule. Finally she gets an *m*-string *PK*' which is just equal to *PK*.

Step 4: Alice performs XOR operation between *PK*' and *PS*. So she gets an *m*-bit string *PA*'.

Step 5: Alice produces the abstract *PA* of *P* using SHA-1 algorithm just as Bob does.

Step 6: Alice compare *PA*' and *PA*. If they are identical, the verification succeeds. Alice can be sure that the message is really from Bob without being distorted.

This quantum public-key cryptosystem can be proved unconditionally secure. Two users can exchange secret message while any other one including KMC can't get the message. User can perform message authentication on the message to guarantee the message's authenticity and integrity. So this quantum public-key cryptosystem can show the same power as classical cryptosystem. Moreover it can gain higher security over classical public-key cryptosystem just like all quantum cryptographic protocol.

On the other hand this quantum public-key cryptosystem has some advantages which make it feasible in practice and prior to the previous quantum public-key cryptosystems. First an advantage of this public-key cryptosystem is that what the users need to do are performing the single particle measurement on a qubit and transmitting qubit through a quantum channel, which have been realized in laboratory for many years. So there are no fundamental technical difficulties which prevent this quantum public-key cryptosystem from coming into practice. Second another significant advantage is that two user needn't exchange quantum information in this cryptosystem. So there are no quantum channels needed between them, which greatly depresses the resource requirements. So our cryptosystem is easier to carry out. Moreover no quantum channels needed means that it doesn't need to face a series of technical problem, such as control of quantum system, quantum decoherence, quantum noise et al. So it's more robust.

Acknowledgment

This work is supported by Natural Science Foundation of China (Grants 61472412) and Natural Science Foundation of the Education Department of Henan Province of China (Grants 14A520012). The authors wish to thank Ruqian Lu for directing us into this research.

References

[1] R. Rivest, A. Sharmir, L. Adleman, "A Method for Obstaining Message authentication and Public-Key Cryptosystem", Communications of ACM, vol. 21, no. 2, pp. 120-126(1978).

[2] 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, pp. 124-134(1994).

[3] D. Gottesman, I. Chuang, "Quantum Message authentications", arXiv:quant-ph/0105032(2010).

[4] G. Nikolopoulos, "Applications of single-qubit rotations in quantum public-key cryptography", Physical Review A, 77, pp. 032348(2008).

[5] G. Nikolopoulos, L. Ioannou, "Deterministic quantum-public-key encryption: forward search attack and randomization", Physical Review A, vol. 79, pp. 042327(2009).

[6] L. Ioannou, M. Mosca, "Public-key cryptography based on bounded quantum reference frames", *arXiv*:quant-ph/0903.5156(2009).

[7] L. Ioannou, M. Mosca, "Unconditionally-secure and reusable public-key authentication", Proceedings of the 6th Conference on the Theory of Quantum Computation, Communication and Cryptography, pp.13-27(2011).

[8] U. Seyfarth, G. Nikolopoulos, G. Alber ,"Symmetries and security of a quantum-public-key encryption based on single-qubit rotations", Physical Review A, vol. 85, pp. 022342(2012).