

Quantum public-key cryptosystem without quantum channel between any two users based on the Bell state measurement

Xiaoyu Li*, Dai Wang

School of Information Engineering, Zhengzhou University, Zhengzhou City, China

Received 1 March 2014, www.cmnt.lv

Abstract

In this paper, a quantum public-key cryptosystem without quantum channel between any two users based on the Bell state measurement is presented. A user Alice shares a set of Einstein-Podolsky-Rosen (EPR) pairs with key management centre (KMC) as the private key and the public key. By performing the Bell state measurement on the public key and the auxiliary qubits any other user can send encrypted message to Alice. On the other hand, digital signature can also be achieved by this public-key cryptosystem. 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 is easier to carry out in practice and more robust against possible attacks.

Keywords: public-key, quantum cryptography, EPR pair, the Bell state measurement, digital signature

1 Introduction

In cryptography, people integrate the original information (called “the plain text”) with some auxiliary information (called “the key”) to produce encrypted information (called “the cipher text”) by a cryptographic algorithm. Anyone who has not the key cannot recover the plain text from the cipher text. So the cipher text can be transmitted through an insecure channel without any danger to leak the plaintext. Two users can fulfil secret communications through an insecure channel as long as they have shared the key before. As a result key distribution becomes the most important and difficult problem for people to complete secret communication. In fact, there are nearly no unconditionally secure classical key distribution protocols in classical cryptography.

Quantum key distribution (QKD) protocol is a good solution to this problem. In QKD protocols people can achieve unconditional security using the special physical properties of quantum system. C. H. Bennett and G. Brassard provided the first quantum key distribution protocol [1] in 1984. Since then people have developed many quantum key distribution protocols, such as the EPR protocol [2], B92 protocol [3], Lo-Chau protocol [4], et al [5-10]. Experimental work for QKD has also been finished in laboratory. Bennett, Bessette and Brassard first realized BB84 protocol in 1992 [11]. Now QKD protocol in optical fibre has been completed beyond 150 km [12] while QKD protocol in free space has also been achieved over a distance of 1 km [13].

Traditional QKD protocols belong to symmetrical key protocols. But all symmetrical key protocols are faced with a serious problem: how to distribute and manage keys if there are a lot of users in the cryptosystem? If there are N

users, which need to communicate with each other, every user must share a key with any one of the other users. So every user should keep N-1 keys secret so that no one can steal them. At the same time, every user should complete key distribution with any one of the other N-1 user. Obviously, it is an arduous task when N is a large number! Furthermore, in practice maybe the users do not trust each other so that it is impossible for them to perform key distribution. It is known that public-key cryptosystem can overcome this difficulty in classical cryptography, such as RSA algorithm [14]. In public-key cryptosystem a user has (public key, private key) pair in which the public key and the private key cannot be deduced from each other. The private key is used to decrypt the message encrypted by the public key while the public key is used to decrypt the message encrypted by the private key. Every user keeps his private key secret so as that no one can get it. At the same time, a key management centre keeps all users' public keys, which are open to everyone. If a user Bob wants to send a secret message to another user Alice, he first asks KMC for Alice's public key and encrypts the message by the public key to get the cipher text. Then Bob sends the cipher text to Bob. When Bob receives the cipher text, he can decrypt it by his private key to recover the original message. Any eavesdropper who catches the cipher text cannot recover the original message because he or she does not hold Bob's private key. Public-key cryptography technology has become one of the most important tools to safeguard information security in modern society, such as commercial affairs, military affairs, network communications et al. But Peter Shor proved that RSA algorithm is unsafe on future quantum computer in 1994 [15]. So the classical public-key cryptosystem based on RSA algorithm will be crashed

* *Corresponding author* e-mail: iexyli@zzu.edu.cn

by attacks on quantum computer. Quantum public-key technology can provide a good alternative solution. In 2001 Gottesman first presented a quantum one-way function to design quantum digital signature protocol, which may be used in a public-key system. A similar scheme is provided in [17]. In 2008 Nikolopoulos put forward the first quantum public-key cryptosystem [18] based on the property of single-particle rotation of unknown quantum states which can provide unconditional security. Since then a few public-key protocols have been studied [19-22].

In this paper, we provide a quantum public-key cryptosystem based on the Bell state measurement. Users and KMC share EPR pairs as the public key and the private key. With the help of KMC, N users can communicate with each other securely. Moreover digital signature for message can be fulfilled naturally by the public-key cryptosystem. There are no quantum channels needed between any two users. So it's easy to carry out in practice. We prove that the cryptosystem is secure against possible attack.

2 Basic idea

As known a quantum two-state system is called a qubit. A qubit may be in one of the four possible states

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

Obviously, the four states are not orthogonal to each other. Therefore, it is impossible to determine in which state a qubit is with certainty. On the other hand, they form two complete orthogonal bases in which we can measure a qubit:

$$B_{01} = \{|0\rangle, |1\rangle\}, \quad B_{+-} = \{|+\rangle, |-\rangle\}. \quad (2)$$

A two-qubit system can be in one of the four Bell states:

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \quad (3)$$

Such a two-qubit system is often called an EPR pair. It is easy to find that the four Bell states forms a complete orthogonal basic vector set in which people can measure a two-qubit system. Such measurement is called the Bell state measurement, which has been carried out [23].

We assume that Alice and Bob share M EPR pair in the state:

$$|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2), \quad (4)$$

in which qubit 1 is hold by Alice and qubit 2 is hold by Bob. Then to each EPR pair Bob creates an auxiliary (denoted as qubit B) in the state $|0\rangle$ and put it together with qubit 2. So the state of the whole three-qubit system is:

$$|S\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 |0\rangle_B + |1\rangle_1 |1\rangle_2 |0\rangle_B). \quad (5)$$

It can be rewritten as:

$$\begin{aligned} |S\rangle &= \frac{1}{\sqrt{2}}[|0\rangle_1 (|\Phi^+\rangle_{2B} + |\Phi^-\rangle_{2B}) + \\ &|1\rangle_1 (|\Psi^+\rangle_{2B} - |\Psi^-\rangle_{2B})]. \end{aligned} \quad (6)$$

Now Alice measures qubit 1 in basis $\{|0\rangle, |1\rangle\}$ while Bob performs the Bell state measures on the composed system of qubit 2 and qubit B. It is easy to find that Alice's measurement results and Bob's measurement result are correlated in Table 1.

TABLE 1 Correlation of their measurement results

Alice's measurement result	Bob's measurement result
$ 0\rangle_1$	$ \Phi^+\rangle_{2B}$
	$ \Phi^-\rangle_{2B}$
$ 1\rangle_1$	$ \Psi^+\rangle_{2B}$
	$ \Psi^-\rangle_{2B}$

So it's possible to establish a public-key cryptosystem based on the result above.

Now let us consider a public-key cryptosystem, which includes a key management centre (KMC) and N users. First, we have the Key Rule.

Key Rule:

$$\begin{aligned} |0\rangle \rightarrow 0, |1\rangle \rightarrow 1, |+\rangle \rightarrow 0, |-\rangle \rightarrow 1, \\ \Phi^+ \rightarrow 0, |\Phi^-\rangle \rightarrow 0, |\Psi^+\rangle \rightarrow 1, |\Psi^-\rangle \rightarrow 1. \end{aligned} \quad (7)$$

A user, e.g. Alice, creates M EPR pairs in which every EPR pair is in the state:

$$|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2). \quad (8)$$

Then Alice shares the EPR pairs with KMC in which qubit 1 of the EPR pair is hold by Alice and qubit 2 is hold by KMC. So the qubit sequence hold by Alice denoted as Q^A is just Alice's private key while the qubit sequence hold by Bob denoted as Q^K is just Alice's public key. The public key is open to every user while Alice keeps her private key secret in order that no one except herself can get it. Now another user, such as Bob, wants to send a secret message to Alice. E.g., the message may be an n-bit string denoted as P , which is just the plain text. To encrypt the plain text, Bob asks KMC for Alice's public key Q^K . After getting Q^K , to every qubit in Q^K Bob creates an auxiliary qubit in the state $|0\rangle$ and performs the Bell state measurement on the two qubits. At the same time Bob records his measurement result according to the Key Rule. Finally, Bob gets an M-bit string S . On the other hand, Alice measures Q^A in B_{01} and records her measurement

results according to the Key Rule. Finally Alice also gets an M-bit string denoted as S' . Alice and Bob mutually choose t bits from S' and S in which $t = M - n$ and compare them. If there are too many disagreements, they abandon the intention of communications and turn back to the beginning. Alternatively, they can be sure that no errors or eavesdroppers existing. So Alice has an n-bit string denoted as K' while Bob has an n-bit string denoted as K . It is obvious that $K' = K$. Next Bob perform an XOR operation on P and K to get a new n-bit string PS in which:

$$PS = P \oplus K. \quad (9)$$

Then Bob sends PS to Alice through the public classical channel. When Alice receives it, she performs an XOR operation on PS and K' to get P'

$$P' = PS \oplus K'. \quad (10)$$

From (9) and (10) we get

$$P' = P. \quad (11)$$

So Alice has gotten the plain text which Bob wants to send her. In section IV we will prove that no one except Alice and Bob can get the plain text. So Bob succeeds in sending a secret message to Alice. It is easy to find that Alice and Bob needn't exchange qubits at all. So no quantum channels are needed between them. This is a notable advantage of our public-key cryptosystem.

To guarantee the public-key work, there is still a problem, which must be solved. The public key and the private key, which are all parts of the M EPR pairs lose correlations after Alice's and Bob's measurements. So both the public key and the private key no longer exist after a communication process, or in other words, the (public key, private key) pair can be used for only one time. But many users may need to communicate with Alice and one user may need to send a lot of secret messages to Alice. So KMC and Alice should share L ($L \gg N$) (public key, private key) pairs. Each (public key, private key) pair of Alice should be given unique id number. So does every user in the public-key cryptosystem.

So we can design a quantum public-key cryptosystem based on the idea above.

3 Quantum public-key cryptosystem without quantum channels using the Bell state measurement

3.1 BUILDING THE PUBLIC-KEY CRYPTOSYSTEM

First, we assume that there are N users and a KMC in our public-key cryptosystem. There are a classical channel and a quantum channel. The classical channel is open so that everyone can listen to it and send classical information to others. However, the classical channel is authenticated so that everyone can assure the identity of the counterpart who is communicating with him. The quantum channel is insecure. Everyone can catch the qubit transmitted through it and send fake qubits to any other one without being found. Every user, such as Alice, creates L EPR pairs and

share them with KMC in which the first qubit (qubit 1) is hold by herself and the second qubit (qubit 2) is hold by KMC. So the Alice's public keys set is denoted as:

$$K_{PK} = \{ (i, Q_i^K), i = 1, 2, \dots, L \}, \quad (12)$$

in which M-qubits sequence and i is the id number. On the other hand, Alice keeps her private keys denoted as

$$K_{PA} = \{ (i, Q_i^A), i = 1, 2, \dots, L \}. \quad (13)$$

All users' public keys are open to everyone, that is to say, any person can get any public key of any other user from KMC. But one public key can only be given to one user because it will be consumed and no longer exist. It must be pointed out that every user must keep his or her private keys absolutely secret. Certainly one private key can also be used for one time.

3.2 PROCESS OF THE SECRET COMMUNICATION

If user Bob wants to send a secret message denoted as an n-bit string P to another user Alice, they perform the following steps:

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

Step 2: KMC chooses a public key (j, Q_j^K) from Alice's K_{PK} at random and gives it to Bob through the quantum channel while KMC sends the id number j to Bob through the classical channel.

Step 3: After receiving (j, Q_j^K) and j , Bob sends j to Alice through the classical channel.

Step 4: After receiving the id number j , Alice queries it in her K_{PA} and gets the corresponding private key (j, Q_j^A) in order to decrypt the cipher text received.

Step 5 (error-checking): Alice chooses t qubits from (j, Q_j^A) , where $t = M - n$. Then she measures them in basis B_{01} or B_{+-} at random and declares her choice of each measurement basis. Bob chooses the corresponding qubits in (j, Q_j^K) and measures them in the identical basis just as Alice. Finally Alice and Bob compare their measurement results. If there are too many disagreements, they abandon it and turn back to step 1. Or they continue into the next step.

Step 6: To each of the left n qubits (denoted as qubit 2) in (j, Q_j^K) , Bob creates an auxiliary qubit (denoted as qubit B) and performs the Bell state measurement on the composed system of qubit 2 and qubit B. Bob records his measurement results according to the Key Rule. Finally, Bob gets an M-bit string K .

Step 7: To each of the left n qubit in (j, Q_j^A) , Alice measures it in basis $\{|0\rangle, |1\rangle\}$ and records her measurement results according to the Key Rule. Finally Alice gets a string K' .

Step 8: Bob performs XOR operation on K and P to get the cipher text PS . Then Bob sends PS to Alice through the classical channel.

Step 9: When Alice receives PS , she performs XOR operation on PS and K' to get the decrypted text P' .

Obviously $P' = P$. So Alice has gotten the secret message which Bob wants to send 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 fulfil secret communications by this public-key cryptosystem.

3.3 DIGITAL SIGNATURE

First all users agree to the following rule:

Signature Rule:

$$|0\rangle \rightarrow 0, \quad |1\rangle \rightarrow 1. \quad (14)$$

If Alice receives a secret message, which is claimed from Bob, how can she assure that it is really from Bob? Such problem can be solved by digital signature. Bob can sign the message to guarantee that it is just the message he wants to send Alice. Let us assume that Bob wants to send a string P to Alice. To produce the signed message, Bob performs as following steps:

Step 1: Bob produces an m -bit abstract PA of P using a hash algorithm, for example, SHA-1 algorithm.

Step 2: Bob chooses one of his private keys at random, such as (k, R_k^A) . Then he performs measurement on the first m qubits of (k, R_k^A) in basis $\{|0\rangle, |1\rangle\}$ and records his results according to the Signature Rule. Finally, Bob gets an m -bit string PK .

Step 3: Bob performs an operation $PA \oplus PK$. Finally, he gets an m -bit string PSD , which is just the signed message.

Step 4: Bob attaches PSD and the id number k with the message P . So he gets a string PX which is just the plain text to be submitted to Alice.

Notice that 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 cannot satisfy it, we can always make it by dividing it into several parts or adding supplementary bits to it.

Now Bob and Alice can finish the communication as the steps in section III.

After Alice gets the plain text PX , she extracts the original message P , the signed message PSD and the id number k . To verify the signature, she performs the following steps.

Step 1: Alice asks KMC for Bob's k public key (k, R_k^K) .

Step 2: Alice measure the first m qubits of (k, R_k^K) in basis $\{|0\rangle, |1\rangle\}$ and records her measurement results according to the Signature Rule. Finally she also gets an m -string PK' which is just equals to PK .

Step 3: Alice performs an operation $PSD \oplus PK'$. Finally she gets an m -bit string PA' .

Step 4: Alice produces the abstract PA of P by SHA-1 algorithm just as Bob does.

Step 5: Alice compares PA' and PA . If they are identical, the verification passes. Alice can be sure that the message is just from Bob.

4 Security of the public-key cryptosystem

This quantum public-key cryptosystem is secure. Two users can communicate with each other secretly. Any other people including KMC cannot get the message. We prove it as follows.

First, we assume that an eavesdropper, e.g., Eve, wants to get the message sent from Bob to Alice.

4.1 IMPOSSIBILITY FOR EAVESDROPPER TO GET THE MESSAGE

Eve can listen to both the classical channel and the quantum channel, trying to get the secret message from Bob to Alice. She can get the cipher text PS sent from Bob to Alice in step 5. At the identical time she also knows that the plain text is encrypted by Alice's j public key (j, Q_j^K) .

As known PS is produced from $P \oplus K$. It's easy to deduce that $P = PS \oplus K$. Since Bob has gotten PS , he can get P as long as he gets K . But K is kept secret by Bob so that he won't give K to anyone. What Eve can do is to monitor the process that Bob creates the cipher text, trying to get some information about K . First Eve can listen to all the classical information exchanged between Alice and Bob. But Alice's K' or Bob's K is from the measurement results on (j, Q_j^A) or (j, Q_j^K) , which Eve doesn't possess at all. So Eve can get no information about even one bit of K or K' .

Second Eve may catch (j, Q_j^K) when KMC sends it to Bob in step 2. But she can't measure (j, Q_j^K) because at

present (j, Q_j^K) contains no information about K which is produced by the random measurement results of Bob in step 5. If Eve measures (j, Q_j^K) now, she can only get a random string, which has nothing about K . Furthermore, if Eve measures (j, Q_j^K) , the qubits will collapse into eigenstates and no longer entangle with the qubits in (j, Q_j^A) . So Alice's measurement results on (j, Q_j^A) will have no correlations with Bob's measurements results on (j, Q_j^K) at all, that is to say, Alice and Bob will be sure to find too many disagreements between K or K' in step 5 and abandon the process of communication. Eve can get nothing by this attack method. The probability that Alice and Bob just get the identical value of the t bits, or in other words, Eve succeeds in getting K , is

$$P_{error} = \left(\frac{1}{2}\right)^t. \tag{15}$$

If $t = 200$, we have

$$P_{error} = \left(\frac{1}{2}\right)^{200} \approx 10^{-60}. \tag{16}$$

It is a number too small to imagine. So Eve's attack is sure to fail.

On the other hand, Eve may take the strategy of entanglement attack. First Eve catches (j, Q_j^K) in step 2.

Then to each qubit (denoted as qubit 2) in (j, Q_j^K) , she creates an auxiliary qubit (denoted as qubit E) and performs CNOT operation on qubit 2 and qubit E in which qubit 2 is the control qubit and qubit E is the target qubit. So qubit E is also entangled with the EPR pair (qubit 1, qubit 2). Then Eve tries to get K from the correlated collapse of qubit E and qubit 2. It's easy to prove that such strategy can't succeed. After Eve's CNOT operation, the state of the whole three-qubit system turns into:

$$|T\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2|0\rangle_E + |1\rangle_1|1\rangle_2|1\rangle_E). \tag{17}$$

Then in step 5 Alice and Bob perform error-checking. They measure qubit 1 and qubit 2 in the identical basis. If the basis is B_{01} , Alice and Bob will get the identical result. So Eve escapes from being found by Alice and Bob. On the other hand, Equation (17) can be rewritten as:

$$|S\rangle = \frac{1}{2\sqrt{2}}[(|+\rangle_1|+\rangle_2 + |+\rangle_1|-\rangle_2 + |-\rangle_1|+\rangle_2 + |-\rangle_1|-\rangle_2) |0\rangle_E + (|+\rangle_1|+\rangle_2 - |+\rangle_1|-\rangle_2 + |-\rangle_1|+\rangle_2 - |-\rangle_1|-\rangle_2) |1\rangle_E]. \tag{18}$$

If the basis is B_{+-} , the probability that Alice and Bob get the identical result is 1/2. Since Alice chooses the basis B_{01} or B_{+-} at random, the average probability that Alice and Bob get the identical probability for one qubit is:

$$p = \frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}. \tag{19}$$

So the probability that all the measurement results for the t qubits, or in other words, the probability that Eve escapes from being found is:

$$P_{error} = \left(\frac{3}{4}\right)^t. \tag{20}$$

If $t=200$:

$$P_{error} = \left(\frac{3}{4}\right)^{200} \approx 10^{-25}. \tag{21}$$

It is a very small probability, which can be ignored. So the strategy of entanglement attack is also invalid.

4.2 IMPOSSIBILITY FOR KMC TO GET THE MESSAGE

Just like Eve, KMC cannot get the message that Bob sends to Alice although it keeps the public keys and joins in the communications process. KMC cannot measure (j, Q_j^K) and cannot perform attack of entanglement because it can do nothing more than Eve can do. We have proved that such attacks cannot succeed.

On the other hand, KMC may also take a complex strategy of attack. To Alice's public key (j, Q_j^K) , KMC creates M EPR pair and split them into two M -qubit sequence: (j, FQ_j^K) and (j, FQ_j^A) . When Bob asks for Alice's public key, it gives (j, FQ_j^K) to Bob. Then KMC measures (j, FQ_j^A) while Bob measures (j, FQ_j^K) . On the other hand KMC measures (j, Q_j^K) while Alice measures (j, Q_j^A) . KMC tries to get some information about K or K' by this method. Obviously Bob's measurement results on (j, FQ_j^K) and KMC's measurement results on (j, FQ_j^A) are identical. KMC's measurement results on (j, Q_j^K) and Alice's measurement results on (j, Q_j^A) are identical. However in step 5 Alice and Bob perform error-checking in which they compare Alice's measurement results on (j, Q_j^A) and Bob's measurement results on (j, FQ_j^K) . It is easy to find that there are no correlations between Alice's results and Bob's results because (j, Q_j^A) and (j, FQ_j^K) are not entangled with each other. So the probability that Alice and Bob get the identical measurement result for one qubit is 1/2. Alice and Bob measure t qubits respectively in step 5. So the probability that they just get identical results for all the t qubits is:

$$P_{error} = \left(\frac{1}{2}\right)^t. \tag{22}$$

If $t = 200$:

$$P_{error} = \left(\frac{1}{2}\right)^{200} \approx 10^{-60}. \tag{23}$$

So we can conclude that Alice and Bob are sure to find something wrong and abandon the process of

communication, that is to say, KMC can't succeeds in getting the secret messages.

4.3 SECURITY AGAINST FAKE MESSAGE ATTACK FROM EVE

Since Eve cannot get the secret message, can she make Alice to receive a fake message? We prove that it is impossible. Eve may try to catch the cipher text PS from Bob to Alice and produce a fake message to send to Alice. But Alice will perform XOR operation on PS and K' to recover the plain text. Although Eve can send Alice any fake cipher text, she can never make Alice to get the message that she wants Alice to accept because she does not hold K (or K'). Whatever Eve does, the probability that she make Alice to accept a specified message is no more than the probability that she guess all the bits of K correctly, which is

$$P_{error} = \left(\frac{1}{2}\right)^n. \tag{24}$$

If $n = 1000$:

$$P_{error} = \left(\frac{1}{2}\right)^{1000} \approx 10^{-300}. \tag{25}$$

That is to say, such attack also fails.

On the other hand, Eve may catch Alice's public key (j, Q_j^K) when it is transmitted from KMC to Bob. Then she sends Bob a fake key (j, FQ_j^K) with the intention to make Bob to get a fake string PK to encrypt the plain text. But Alice and Bob performs error-checking in step 5. Since (j, FQ_j^K) isn't entangled with (j, Q_j^A) , Bob's measurement results on (j, FQ_j^K) have no correlations with Alice's measurement results on (j, Q_j^A) . The probability they just get the identical result for one qubit is $1/2$. So the probability that they get the identical results for all the t qubits is:

$$P_{error} = \left(\frac{1}{2}\right)^t. \tag{26}$$

If $t = 200$:

$$P_{error} = \left(\frac{1}{2}\right)^{200} \approx 10^{-60}. \tag{27}$$

So Eve still fails.

4.4 SECURITY AGAINST FAKE MESSAGE ATTACK FROM KMC

It is easy to prove that KMC cannot make Alice to get a fake message, either. KMC can catch PS and send a fake

cipher text to Alice just as Eve. On the other hand, KMC can give Bob a fake key (j, FQ_j^K) just as Eve. Obviously, what KMC can do is no more than what Eve can do. We have proved that Eve cannot make Alice to accept his fake message. So KMC cannot make it, either.

4.5 SECURITY OF DIGITAL SIGNATURE

Now we prove that our cryptosystem can solve digital signature problem. Alice can affirm that the message she receives is really from Bob and the message is integral without being tempered. After Alice receives the cipher text, she decrypts it and extracts the original message P , the signed message PS and the id number k . Then Alice verifies the signature. First she asks KMC for Bob's k public key (k, R_k^K) and measures the first m qubits to get a string PK' . Then she performs XOR operation to recover PA' , where:

$$PA' = PS \oplus PK'. \tag{28}$$

On the other hand, Alice produces the abstract of P by SHA-1 algorithm. Finally, she gets PA . Notice that

$$PS = PA \oplus PK. \tag{29}$$

If Alice find $PA = PA'$, she gets

$$PK = PK'. \tag{30}$$

Such fact shows that the one who sends the message to Alice should be able to get a string identical to PK' which is produced by Alice's measurement result on (k, R_k^K) . For a man who hasn't hold Bob's k private key (k, R_k^A) , the probability that he just guess all the m bits of PK' is:

$$P_{error} = \left(\frac{1}{2}\right)^m. \tag{31}$$

If $m = 100$:

$$P_{error} = \left(\frac{1}{2}\right)^{100} \approx 10^{-30}. \tag{32}$$

It is an extremely small probability. So Alice can assure that the one must have Bob's k private key (k, R_k^A) , or in other words, the one must be Bob. On the other hand, SHA-1 algorithm guarantees that any string except P cannot produce the abstract PA . The message P must be integral and unchanged. So this public-key cryptosystem provides a reliable digital signature method.

4.6 SECURITY AGAINST FORWARD SEARCH ATTACK

The forward search attack is a serous danger to classical public-key cryptosystems. Since Alice's public key is kept open by KMC, everyone can ask KMC for it. So Eve may

encrypt a large number of plain texts by Alice's public key to produce the same number of cipher texts and save them in her database. Then Eve catches every cipher text sent to Alice and queries them in her database. If she just finds that a cipher text, which she catches, is identical to one cipher text in her database, she can affirm that the corresponding plain text in her database is just the secret message sent to Alice. So Eve gets the secret message without being found. However, in our quantum public-key cryptosystem, the forward search attack is invalid because KMC keeps many public-key for Alice in which one public-key can be used for one time. Two cipher texts, which are produced from the identical plain texts, are completely different. Eve's database is useless. She can never find the correct plain text in her database from a cipher text, which she catches.

So the forward search attack is sure to fail. This is a big advantage of this quantum public-key system.

4.7 SECURITY AGAINST RESEND ATTACK

In classical public-key cryptosystem, Eve may perform resend attack. She can catch a message sent from Bob to Alice and make a copy of it. After some time she resends the message to Bob again. When Alice receives the cipher text, she can decrypt it to the plain text without finding anything wrong. Therefore, Eve makes Alice to accept an outdated and repeated message although Eve completely knows nothing about the message at all. In classical public-key cryptosystem, to defeat resend attack people should add a timestamp to the original plain text so as Alice can find that the message is repeated. But to produce and verify the timestamp user need pay more cost.

In this quantum public-key cryptosystem, resend attack is also invalid. First Eve can catch PS and make a copy of it when it is sent from Bob to Alice. But resending it is pointless. The public key and private key to be used to encrypt and decrypt the original message have been consumed. When Eve wants to send Alice a message, they must perform all the steps in the communication process. So Alice will ask Eve for the id number for the key. However, the private (j, Q_j^A) no longer exists. If Eve still gives Alice the id number j , Alice will find that this is a resend attack at once. If Eve provides another id number, such as j' , in step 5 (error-checking) Alice will perform measurement on t qubits of $(j', Q_{j'}^A)$. Then Eve must provide her measurement results of $(j', Q_{j'}^K)$ which must be identical to Alice's measurement results. If Eve can't provide them, she is found by Alice right away. Even if Eve has gotten $(j', Q_{j'}^K)$ from KMC, she can't succeed, either. In step 7 Alice gets a string NK' , which she will use it to decrypt the cipher text which she receives. But the string NK' has nothing to with the string K' , which Bob used to encrypt the plain text. When Alice gets PS which is resent by Eve, she tries to decrypt PS with NK' .

Obviously, Alice can get nothing but a garbled string so that she can be sure this message is unreal. So Eve has no chance to resend the repeated message to Alice at all.

4.8 SECURITY AGAINST CHOSEN PLAIN TEXT ATTACK

In a chosen plain text attack, Eve can obtain a random number of (plain text, cipher text) pairs of her choices, or in other words, she can get random cipher text for a specified plain text. Then Eve tries to find some information about the key by analyze the (plain text, cipher text) pairs. Chosen plain text attack is a power tool to crash many classical cryptographic algorithms if the number is large enough. But in our public-key cryptosystem one public key can be used for only one time. Any two cipher texts are produced by two different public keys. Furthermore, two identical plain texts are sure to be converted to completely different cipher texts. So Eve can find no laws which can help her to get something information about the key. In fact no matter how many (plain text, cipher text) pairs Eve may get, she can get nothing helpful to break the public-key cryptosystem. So the chosen plain text attack is impossible to succeed.

Now we have proved that our public-key cryptosystem is unconditionally secure.

5 Feasibility analysis of the public-key cryptosystem

First in this quantum public-key cryptosystem all that users need to do are performing the Bell state measurement on an EPR pair, performing single-particle measurements on a qubit and transmitting qubits through a quantum channel. All these have been realized in laboratory for many years. There are no unsolved technical difficulties at all. So it is easier to carry out in practice. On the other hand any two users need only to exchange classical information through a public classical channel. They don't need exchanging qubits at all. There are no quantum channels needed to connecting two users, which reduces the resource requirements and technical complexity greatly. So it is a big advantage of our quantum public-key cryptosystem.

Second, it is known that quantum cryptographic technology depends on the special physical properties of quantum systems. But quantum systems will inevitably undergo decoherence as time goes on. Once decoherence happens, it makes quantum to lose quantum coherence and to turn into classical systems so that all quantum cryptographic technology lose effectiveness. It's the most important threat to quantum cryptographic technology. In traditional quantum cryptographic protocols, such as quantum key distribution, we can complete the protocol as soon as possible before decoherence occurs. But in public-key cryptosystem, KMC needs to keep every user's public keys for a relative long time until a user asks for them. So decoherence is a problem which can not be avoided. To solve this problem, we can use the quantum system which has bigger time length of decoherence, for example,

photon in resonator. Another method is to make users to update their public keys periodically before decoherence happens. Using such methods this cryptosystem can work well to satisfy all users.

Third, in the public-key cryptosystem there is a public classical channel and a quantum channel needed. We have proved that eavesdroppers cannot get the secret message without being found. How about noise in these channels? Does it make the process of communication to error even fail? First, let us consider noisy classical channel. In step 3, Bob sends the id number j to Alice, which is necessary to go into the next step. If there are errors in transmission which cause a mistaken number j' , communication between Bob and Alice is sure to fail. Likewise, in step 5 Alice and Bob need to exchange classical information for error-checking. The noisy information may cause mistaken results. Fortunately, classical error-correcting coding technology has been mature and powerful to deal with noisy channel. By error-correcting coding technology, it is easy to guarantee that classical information is transmitted with a very low error rate. So noise in classical channel doesn't affect our quantum public-key cryptosystem. On the other hand, in step 2 KMC sends Alice's public key (j, Q_j^K) to Bob through the quantum channel. If there are random errors existing, Bob will get mistaken bits in step 5 and step 6, which also cause communication to fail. The solution is quantum error-correcting coding technology. Although quantum error-correcting coding technology still cannot work as well as classical error-correcting coding technology, it is

sufficient to accomplish reliable communications through most quantum channels.

6 Discussions and conclusion

In this quantum, public-key cryptosystem a public key can be used for only one time, which is a limit to the cryptosystem's capacity for work. If a user's public keys have been used up, no one can send message to him again. Developing cryptosystem with reusable public key is a solution to this problem. Replenish public keys periodically is another solution. We will discuss them in future work.

In this paper, we provide a quantum public-key cryptosystem without quantum channels between any two users based the Bell state measurement. Users use EPR pairs as public key and private key. The laws of quantum physics guarantee that no one except the two parts involved in communication can get the secret message. So it's unconditionally secure. At the same time the integrality and truth of the message exchanged can be verified by digital signature. There are no quantum channels needed between any two users. So it is easier to carry out in practice.

Acknowledgements

The authors wish to thank Ruqian Lu for directing us into this research. This work is supported by Natural Science Foundation of China (Grants 61073023).

References

- [1] Bennett C H, Brassard G 1984 *Proceedings of IEEE International conference on Computers Systems and Signal Processing* 175-9
- [2] Ekert A K 1991 *Physical Review Letters* **67**(6) 661-3
- [3] Bennett C H, Brassard G, Mermin N D 1992 *Physical Review Letters* **68**(5) 557-9
- [4] Lo H K, Chau H F 1999 *Science* **283**(5410) 2050-6
- [5] Nguyen T, Sfaxi M A, Ghernaoui-Hélie S 2006 *Journal of Networks* **1**(5) 9-20
- [6] Qi B, Zhao Y, Ma X F, Lo H K, Qian L 2007 *Physical Review A* **75**(5) 052304
- [7] Matsumoto R 2007 *Physical Review A* **76**(6) 062316
- [8] Zhao Y, Qi B, Lo H K 2008 *Physical Review A* **77**(5) 052327
- [9] Horodecki K, Horodecki M, Horodecki P, Leung D, Oppenheim J 2008 *IEEE Transaction on Information Theory* **54**(6) 2604-20
- [10] Barrett J, Colbeck R, Kent A 2012 *Physical Review A* **86** 062326.
- [11] Bennett C H, Bessette F, Brassard G, Salvail L, Smolin J 1992 *Journal of Cryptology* **5**(1) 3-28
- [12] Kimura T, Nambu Y, Hatanaka T, Tomita A, Kosaka H, Nakamura K 2004 *Japanese Journal of Applied Physics* **43** L1109
- [13] Buttler W T, Hughes, R J, Kwiat P G, Lamoreaux SK, Luther G G, Morgan G L, Nordholt J E, Peterson C G, Simmons C M 1998 *Physical Review Letters* **81**(15) 3283-6
- [14] Rivest R, Sharmir A, Adleman L 1978 **21**(2) 120-6
- [15] Shor P W 1994 *Proceedings of 35th Annual IEEE Symposium on Foundations of Computer Science* 124-34
- [16] Gottesman D, Chuang I 2001 *Technical Report* arXiv:quant-ph/0105032
- [17] Zhang J 2012 *Journal of Networks* **7**(11) 1803-10
- [18] Nikolopoulos G 2008 *Physical Review A* **77** 032348
- [19] Nikolopoulos G, Ioannou L 2009 *Physical Review A* **79** 042327
- [20] Ioannou L, Mosca M 2009 arXiv:quant-ph/0903.5156
- [21] Ioannou L, Mosca M 2011 *Proceedings of the 6th Conference on the Theory of Quantum Computation, Communication and Cryptography* 13-27
- [22] Seyfarth U, Nikolopoulos G, Alber G 2012 *Physical Review A* **85** 022342
- [23] Michler M, Mattle K, Weinfurter H, Zeilinger A 1996 *Physical Review A* **53**(3) 1209-12

Authors



Xiaoyu Li

Current position, grades: associate professor at the School of Information Engineering, Zhengzhou University, China.
University studies: Graduated from the Institute of Computing Technology, Chinese Academy of Sciences in 2004.
Scientific interest: quantum information and quantum computation.
Publications: more than 20.



Dai wang

Current position, grades: graduate student at the School of Information Engineering, Zhengzhou University, China.
University studies: School of Information Engineering after graduation at the School of Software, Zhengzhou University.
Scientific interest: quantum information and quantum computation.