Quantum Public-Key Cryptosystem Based on Super Dense Coding Technology

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

Dexi Zhang
College of Computer Science and Technology, Xuchang University, Xuchang City, P. R. China
Email:zdx@xcu.edu.cn

***Abstract*—In this paper we provide a quantum public-key cryptosystem based on super dense coding technology. A user Alice shares a set of Einstein-Podolsky-Rosen (EPR) pairs with a key management center (KMC) in which the particles hold by Alice are the private key and the particle hold by KMC are the public key. By the help of the key management center any other user can send encrypted message to Alice. Any one including KMC except Alice can't recover the message. On the other hand digital signature can also be achieved by this public-key cryptosystem. In the cryptosystem one EPR pair can be used to encrypt two bits of the plain text. So it's efficient. Finally we prove that our cryptosystem is robust against possible attacks.**

***Index Terms*—public-key, quantum cryptography, EPR pair, super dense coding, the Bell state measurement.**

I. Introduction

Cryptography can help people to exchange secret information through an insecure channel. The original information to be submitted is called "the plain text". It is integrated with some auxiliary information which called "the key" to produce the encrypted information which is called "the cipher text". Then the cipher text can be transmitted though an unsecure channel. No one can recover the plain text except the authenticated user who has the key. Two users sharing the key can perform secret communications though there is only an insecure quantum channel between them. Obviously key distribution is the precondition for people to achieve secret communication. In classical cryptography it is the most difficult problem. In fact there are nearly no unconditionally secure classical key distribution protocols.

There is a good way to solve this problem: quantum key distribution protocol. In QKD protocols we need insecure quantum channel and an authenticated public classical channel. The laws of quantum physics guarantee that the protocols can be unconditionally secure. C. H. Bennett and G. Brassard provided the first quantum key distribution protocol in 1984 [1]. Then people developed many quantum key distribution protocols [2~10]. On the other hand experimental work for OKD has also succeeded. In 1992 Bennett, Bessette and Brassard first realized BB84 protocol in laboratory [11]. QKD in optical fiber has been achieved beyond 150 km [12] and in free space has been implemented over a distance of 1 km [13].

As known there are two kinds of cryptographic algorithms: symmetrical algorithms and asymmetrical algorithms. In asymmetrical algorithm encryption and decryption use the same key which is shared by the two parts involved in communication. If many users want to communicate with each other, key management will become very difficult. If there are N users in a cryptosystem, one user must share a key with every one of the other users. So every user must keep N-1 keys secret and remember which user they belong to, which needs the user to pay much cost. Moreover all the N(N-1)/2 key must be distributed before the cryptosystem begins to work. Obviously it's too tedious and too complex if N is a large number! On the other hand maybe the N users don't trust each other. So they can't establish shared key at all, which makes that the crypto-system can't work from the beginning. In cryptography a solution to overcome such difficulties is public-key cryptosystem, for example, RSA algorithm [14]. In public-cryptosystem every user has a pair of keys which are called the public key and the private key respectfully. The cipher text encrypted by the public key can only be decrypted by the private key while cipher text encrypted by the private key can only be decrypted by the public key. Moreover the public key and the private key are independent from each other, that is to say, it's impossible to deduce one key from the other. All users' public keys are kept by a key management center (KMC) in which they are open to every user. Every user keeps his or her private key secret so as that no other one can get it. When a user Alice wants to send a secret message to another user Bob, she first asks KMC for Bob's public key. The she encrypts the message by the public key and sends the encrypted message (named "the cipher text") to Bob. When Bob receives the cipher text, he decrypts the cipher text using his private key. Finally Bob gets the plain text. Any eavesdropper who catches the cipher text can't recover the plain text because he or she has no Bob's private key. Today public-key cryptosystem has

doi:10.4304/jcp.8.12.3168-3175

been widely used in modern society, which provides secure communications for military affairs, commercial affairs, government affairs and network transmissions. But as known Peter Shor found a quantum polynomial-time algorithm to RSA algorithm in 1994 [15]. So the classical public-key cryptosystem based on RSA algorithm will become unsafe in future if quantum computers are put into use. Quantum public-key cryptosystem may replace classical public-key cryptosystem to bring us security on future quantum computers. In 2001 Gottesman presented a quantum one-way function in his quantum digital signature protocol [16], which may be heuristic in quantum public-key crypto-system. A similar scheme was provided in [17]. In 2008 Nikolopoulos found the first unconditionally secure quantum public-key scheme [18]. It is based on single-particle rotation of unknown quantum states. Since then a few public-key schemes have been provided [19-22].

In this paper we provide a quantum public-key cryptosystem based on super dense coding technology. 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. One EPR pair can be used to encrypt two bits of the message. So it's efficient. We prove that the cryptosystem is secure against possible attack.

II. Basic Idea

In quantum information science a quantum two-state particle is often called a qubit. A two-qubit system can be in one of the four Bell states

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

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

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

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

Such a two-qubit system is often called an EPR pair. It's 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]. As known we can perform one of the four operations in {I, σ_x, $i\sigma_y$, σ_z} on a qubit in which

$$I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \qquad \sigma_x=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

$$\sigma_y=\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}, \quad \sigma_z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}. \quad (2)$$

Now we assume that Alice and Bob share an EPR pair in the state

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

in which qubit 1 is hold by Alice and qubit 2 is bold by Bob. Alice can choose to perform one operation of {I, σ_z, σ_x, $i\sigma_y$} on qubit 1 at her hands, which will make the state of the EPR pair turn into $|\Phi^+>$, $|\Phi^->$, $|\Psi^+>$ or $|\Psi^->$. Then Alice sends qubit 1 to Bob. When Bob receives qubit 1, he performs the Bell state measurement on the composed system of qubit 1 and qubit 2 and explains his measurement result as Coding Rule. So Alice makes Bob to get two-bit classical information by sending only one qubit to Bob. This technology is called super dense coding [24]. It has been realized in laboratory [25].

Now let's consider a public-key cryptosystem which includes a key management center (KMC) and N users. KMC keeps every user's public key which anyone can get to encrypt the plain text while every user keeps his private key secret to decrypt cipher text. First we have the Key Rule.

Key Rule:

$$|\Phi^+>\rightarrow 00, \quad |\Phi^->\rightarrow 11$$

$$|\Psi^+>\rightarrow 01, \quad |\Psi^->\rightarrow 10 \quad (4)$$

A user, for example Alice, creates n EPR pairs in which every EPR pair is in the state

$$|\Phi^+>_{12}=\frac{1}{\sqrt{2}}(|0>_1|0>_2+|1>_1|1>_2). \quad (5)$$

Then Alice shares the EPR pairs with KMC in which qubit 1 of the EPR pair is hold by Alice and qubit 2 is bold by KMC. The qubits sequence hold by Alice is called Alice's private key while the qubits sequence hold by KMC is called 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. The message may be a 2n-bit string denoted P which we call the plain text. First Bob splits the 2n bits into n two-bit blocks. To encrypt the plain text to the cipher text, Bob asks KMC for Alice's public key. After getting the qubit sequence, he encrypts the plain text according to the following Encoding Rule.

Encoding Rule:

If the block is '00', Bob do nothing; if the block is '01', Bob performs a σ_x operation on qubit 1 of the EPR; if

the block is '10', Bob performs a $i\sigma_y$ operation on qubit 1 of the EPR pair; if the block is '11', Bob performs a σ_z operation on qubit 1 of the EPR pair.

It's easy to find that each qubit 2 of the EPR pair is used to encrypt a two-bit block. Then Bob sends the qubit sequence to Alice. When Alice receives the qubits, to each EPR pair she put the qubit 2 she received together with the qubit 1 at her hands. Next Bob performs the Bell state on the EPR pairs and records according to the Key Rule. Finally Alice gets a 2n-bit string denoted as *P*'. Obviously we have *P*'=*P*, or in other words, Alice gets the plain text that Bob wants to send her. In section 4 we will prove that by a well-designed scheme no one except Alice and Bob can get the plain text. So the communication process between Bob and Alice is secure.

There is still a problem left. The public key, or in other words, the n-qubit sequence is consumed after a communication process. So does the private key. The pair of keys can be used for only one time. If all the N-1 users want to send secret message to Alice, KMC must preserve at least N-1 public keys for Alice. In practice a user maybe needs to communicate with Alice for many times. So we can assume that KMC should keep M(M>>N) public key for Alice. So does every user in our cryptosystem. In order to discriminate the M public keys of Alice, every public key should be given a unique id number.

So we can design a feasible public-key cryptosystem based on this idea.

III. Quantum Public-key Cryptosystem using based on Super Dense Coding Technology

Now we present our quantum public-key cryptosystem.

A. Building the Public-key Cryptosystem

First we assume that there are N users and a KMC in our public-key cryptosystem. They can communicate with each other through a classical channel and a quantum channel. Both the two channels are insecure which everyone can listen to. But the classical channel is authenticated so that one user can assure that the classical information he receives is really from the counterpart. KMC is trusted by every user while any two users don't trust each other. Every user creates M (M>>N) EPR pairs and shares with KMC in which the first qubit (qubit 1) is hold by user himself and the second qubit (qubit 2) is hold by KMC. So the public keys is denoted as

$$K_{PU} = \{ (i, Q_i), \quad i = 1,2,...M \} \qquad (6)$$

in which Q_i is an n-qubit sequence and *i* is the id number. On the other hand, the user keeps her private keys denoted as

$$K_{PR} = \{ (i, R_i), \quad i = 1,2,...M \}. \qquad (7)$$

All users' public keys are open to everyone, in other words, any user can asks KMC for any public key of any other user. But one public key can only be given to one user because it will be consumed and no longer exist. At the same time every user must keep his or her private keys absolutely secret. Similarly one private key can also be used for one time.

B. Process of the Secret Communication

If a user Bob wants to send a secret message denoted as a 2n-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) from Alice's K_{PU} at random and gives it to Bob.

Step 3: After receiving the public key, Bob gets the id number *j* and sends it to Alice through the classical channel.

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

Step 5: Bob encodes *P* on Q_j according to Encoding Rule. So he gets a new n-qubit sequence Q_j'. Then Bob sends Q_j' to Alice.

Step 6: When Alice receives Q_j', to each qubit in Q_j', she put it with the corresponding qubit in R_j. Then Alice performs the Bell state measurement on them and records according to Key Rule. Finally Alice will get a string *P*'. Obviously we have *P'=P*. So Alice gets the message which Bob sends her.

If Alice wants to send secret message to Bob, they need only exchange the roles in the process above. So any two users can achieve secret communications by our public-key cryptosystem.

C. Digital Signature

First all users agree to the following rule.

Signature Rule:

If the measurement result is |0>, we records it as "0"; If the measurement result is |1>, we records it as "1".

If Bob sends a secret message *P'* to Alice, he can sign the message to prove his identity 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 as 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 key at random, for example R_k. Then he measures the first m qubits of R_k in basis $\{|0>, |1>\}$ and records his results according to Signature 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 *k* with *P'*. So he gets a string *P* which is the plain text to be submitted to Alice.

Notice that now the length of *P* should be 2n. So the length of the original message *P*' added with the length of *k* should be 2n-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 as the steps in section III.

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

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

Step 2: After receive B_k, Alice measure Q_k in basis $\{|0>,|1>\}$. Then she takes the first m measurement results and records according to Signature Rule. Finally she gets an m-string *PK*' which is just equals 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*' by SHA-1 algorithm just as Bob does.

Step 6: Alice compare *PA*' and *PA*. If they are same, the verification succeeds. Alice can be sure that the message is just from Bob.

IV. Security of the Public-key Cryptosystem

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

Let's assume that an eavesdropper, for example, Eve, wants to get the message transmitted from Bob to Alice.

A. Impossibility for Eavesdroppesr to Get theMessage

Eve may listen to both the classical channel and the quantum channel, trying to get the message from Bob to Alice. She can get the n-qubit sequence Q_j' sent from Bob to Alice in step 5. On the other hand, she also knows that the plain text is encrypted by no. j public key. But she can't get the message *P* that Bob wants to send Alice at all because the message is encoded not in the states of the qubits of Q_j' but in the states of the whole EPR pairs. The other qubits of the EPR pairs are kept secret by Alice. Eve can't get them. So she can never get the message by performing the Bell state measurements on the EPR pairs just as Alice does. What Eve can do is to measure the qubits in Q_j'. It's easy to find from equation (1) that Eve can only get measurement result |0> or |1> with equal probability although the state may be any one in $\{|\Phi^+>, |\Phi^->, |\Psi^+>, |\Psi^->\}$. That is to say, Eve can't get any information about the EPR pair's state. The probability that she get a two-bit block of the message *P* is no more than 1/4. There are n blocks in *P*, so we have the probability for Eve to get *P* is

$$P_{error} = \left(\frac{1}{4}\right)^n. \tag{8}$$

If *n=1000,* we have

$$P_{error} = \left(\frac{1}{4}\right)^{1000} \approx 10^{-600}. \tag{8}$$

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

Let's consider the strategy of entanglement attack. First Eve catches Q_j'. Then to each qubit (denoted qubit 2) in Q_j', she creates an auxiliary qubit (named qubit E) and performs CNOT operation on the composed system of qubit 2 and qubit E in which qubit 2 is the control qubit and qubit E is the target qubit. If the state of the EPR pair is $|\Phi^+>$, the state of the whole three-qubit system turns into

$$|S>=\frac{1}{\sqrt{2}}(|0>_1|0>_2|0>_E+|1>_1|1>_2|1>_E) \tag{9}$$

which can be rewritten as

$$|S>=\frac{1}{\sqrt{2}}[(|\Phi^+>_{12}+|\Phi^->_{12})|0>_E + (|\Phi^+>_{12}-|\Phi^->_{12})|1>_E] \tag{10}$$

When Alice received qubit 2 and performs the Bell state measurement on the EPR pair in step 6, she will get $|\Phi^+>$ or $|\Phi^->$ with equal probability 1/2. Or in other words, the message sent from Bob is damaged. If the state of the EPR pair is $|\Phi^->$, $|\Psi^+>$ or $|\Psi^->$, we have the same conclusion. So Alice is sure to find Eve's existing. On the other hand Eve can only get |0> or |1> with equal probability 1/2 which contains no information about the message from Bob to Alice. So the strategy of entanglement attack can't succeed.

B. Impossibility for KMC to Get theMessage

It's easy to prove that KMC can't get message that Bob sends to Alice even though it keeps the public keys and join in the communications process. Alice's public key is a qubit sequence in which every qubit belongs to an EPR pair in the state $|\Phi^+>$. KMC holds all the public key of Alice. But the other qubit of each EPR pair, or in other words, the private key, is kept by Alice which no one can get it including KMC. So KMC can't get the EPR pairs and perform the Bell state measurement to get the message just as Alice does.

On the other hand KMC may also take strategy of entanglement attack. To each qubit (denoted qubit 2) in Q_j, KMC creates an auxiliary qubit (named qubit K) performs CNOT operation on the composed system of qubit 2 and qubit E in which qubit 2 is the control qubit

and qubit K is the target qubit. As known the state of the EPR pair is $|\Phi^+>$, the state of the whole three-qubit system turns into

$$|S>=\frac{1}{\sqrt{2}}(|0>_1|0>_2|0>_K+|1>_1|1>_2|1>_K) \tag{10}$$

When Bob get Q_j and encodes it by perfoming one of the four operations in {*I*, σ_x, $i\sigma_y$, σ_z} on qubit 2. For example, if Bob performs σ_x operation on qubit 2, the state of the whole three-qubit system turns into

$$\begin{aligned}|S>&=\frac{1}{\sqrt{2}}(|0>_1|1>_2|0>_K+|1>_1|0>_2|1>_K)\\&=\frac{1}{\sqrt{2}}[(|\Psi^+>_{12}+|\Psi^->_{12})|0>_K\\&\quad+(|\Psi^+>_{12}-|\Psi^->_{12})|1>_E]\end{aligned} \tag{11}$$

When Alice received qubit 2 and performs the Bell state measurement on the EPR pair in step 6, she will get $\Psi^+>$ or $|\Psi^->$ with equal probability 1/2. Or in other words, the message sent from Bob is damaged. So Alice can find that someone is cheating. On the other hand if KMC measures qubit K, it can only get |0> or |1> with equal probability 1/2 which contains no information about the message from Bob to Alice. So we have the same conclusion that the entanglement attack also fails.

C. Impossibility for Eavesdropper to Distort the Message

We prove that the Eve can't distort the secret message from Bob to Alice. Eve may catch the qubit sequence Q_j' from Bob to Alice and try to produce a fake message to send to Alice. Obviously she can perform any operation in {*I*, σ_x, $i\sigma_y$, σ_z} on the qubits of Q_j' as she wants. Finally Alice will get a qubit sequence Q_j''. But Eve can't make Alice get the specified fake message because Bob has finished encoding in step 5, every EPR pair may not be in the original state $|\Phi^+>$. It may be in any state of $\{|\Phi^+>,|\Phi^->,|\Psi^+>,|\Psi^->\}$ which Eve doesn't know. So Eve can't know what the state of the EPR pair is after she performs any operation. That is to say, she can't make the EPR pair turns into a state which she wants it to be. This makes it impossible for Eve to make Alice to get a measurement result which she wanted Alice to get. In fact Eve can only choose to perform an operation at random with a wish that the state EPR chances to turn to the state she wants it to be. The probability for one EPR pair is

$$P=(\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4})\times\frac{1}{4}=\frac{1}{4}. \tag{12}$$

There are n EPR pairs. So the probability which Eve achieves her goal for all the EPR pairs is

$$P_{error}=\left(\frac{1}{4}\right)^n. \tag{13}$$

If *n=1000*, we have

$$P_{error}=\left(\frac{1}{4}\right)^{1000}\approx 10^{-600}. \tag{12}$$

That is to say, such attack also fails.

D. Impossibility for KMC to distort the Message

We can prove that the KMC can't distort the secret message from Bob to Alice, too. KMC may also catch the qubit sequence Q_j' from Bob to Alice and try to produce a fake message to Alice. It's obvious that KMC encounter the same problem as Eve does. It's impossible for KMC to make the EPR pair to turn into a state which it hopes because KMC doesn't know the state of the EPR pair after Bob finishes encoding. So KMC can't make Alice to get the measurement result which it wants whatever it does. Or in other words, KMC can't make Alice to accept a fake message.

On the other hand KMC may try to produce a distort message by providing fake public key to Bob. We can prove that such attack can't succeed, either. First KMC produces a fake public key (j, FQ_j). When Bob asks KMC for Alice's public key, KMC give (j, FQ_j) to him. Then Bob encodes *P* on FQ_j and gets FQ_j'. But FQ_j' isn't entangled with Alice's private key R_j at all. When Alice put FQ_j' together with R_j and performs the Bell state measurement in step 6, she can only get random measurement results which contain no information. It's impossible for KMC to make Alice to get the distort message that it wants Alice to get. So KMC can't succeeds in cheating.

E. Security against Forward Search Attack

In classical public-key cryptosystem, how to defeat forward search attack is an important problem which can't be ignored. The forward search attack can be described as follows. Since Alice's public key is kept by KMC, every user who wants to sends message to Alice must ask KMC for Alice's public key. All cipher texts are encrypted by Alice's public key. So Eve may encrypt many plain texts by Alice's public key to produce many cipher texts and save them in her database. Then Eve catches all cipher texts sent to Alice and queries them in her database. If she just finds that a cipher text which a user sends to Alice is the same as one cipher text in her database, she can conclude that the plain text which the user wants to send Alice is just the plain text she used to produce the cipher text in her database. Finally Eve gets the secret message transmitted to Alice. But in our quantum public-key cryptosystem, forward search attack is meaningless because Alice has many public keys in which a public key can be used only one time. Encrypting

the same plain texts by different public keys of course produces different cipher texts.

So forward search attack is sure to be unsuccessful. This is a big advantage of our public-key system.

F. Security of Digital Signature

Finally we prove that our cryptosystem can solve digital signature problem, too. How does Alice assure that the message is really from Bob? If Eve wants to impersonate Bob, she must produce signed message to cheat Alice. It's easy for Eve to produce the abstract *PA* from the message she wants to send Alice by SHA-1 algorithm. But Eve doesn't know Bob's private key at all which it's necessary to produce the signed message *PS*. Since Bob keeps his private key secret, what Eve can do is only to guess *PK*. So the probability for Eve to guess correctly for all the m bit of *PK* is

$$P_{error} = \left(\frac{1}{2}\right)^m . \tag{13}$$

If *m=100*, we have

$$P_{error} = \left(\frac{1}{2}\right)^{100} \approx 10^{-30} . \tag{14}$$

It's such a small probability. So Eve has no chances to cheat Alice successfully. Or in other words, Alice can assure that the message is from Bob. So we can say that our public-key cryptosystem provides a reliable signature method.

G. Security against Resend Attcak

In classical public-key cryptosystem, Eve may take the strategy of resend attack. She can catch the message sent form Bob to Alice and make a copy of it. Then she resends the message after some time, for example two days or two months. Obviously Alice has no means to percept such attack because the message is indeed from Bob. So Eve can make Alice to receive an outdated and repeated message although Eve doesn't know the message at all. To solve this problem, people should add timestamp to the original plain text so as Alice can find that the message is outdated. Obviously users have to pay more cost to producing and verifying timestamp.

In our quantum public-key cryptosystem, resend attack is not a threat at all. First Eve can catch Q_j' when it is sent from Bob to Alice. Obviously the states of the qubits in Q_j' are unknown to Eve. So Eve can't make a copy of Q_j' so as to resend it in future because quantum no-cloning theorem forbids any one to copy an unknown quantum state. Then Eve may measure Q_j' wishing to find the states of qubits in Q_j' so as to avoid the restriction of quantum no-cloning theorem. But we have prove that it's impossible in this section, subsection A. By performing measurements on the qubits in Q_j', Eve not only can't get anything about the qubits' states but also will be found by Alice. Moreover Eve can't succeeds in resend attack even though she can get a copy of Q_j'! The reason is that in our public-key cryptosystem the public key Q_j and the private key R_j are also used for one time. When Alice receives Q_j' which Eve resends, she can't decode it because the private R_j has been consumed. So resend attack can't succeed in our public-key cryptosystem.

H. Security against Chosen Plain Text Attack

Our public-key cryptosystem is secure under chosen plain text attack. We prove it as follows.

In a chosen plain text attack, Eve is allowed to obtain a random number (plain text, cipher text) pairs of her choice. Then she tries to find some information about the key. In classical cryptography chosen plain text attack is a power tool to crash the cryptographic system if the number is large enough. But in our public-key cryptosystem the public key can be used for only one time. Different cipher texts are produced by different public keys. So there are no correlations between them. Eve can't find any laws which can help her to find something about the key. Although Eve may get as many as possible (plain text, cipher text) pairs, she is still unable to get anything helpful to break our public-key cryptosystem. So chosen plain text attack is invalid to our public-key cryptosystem.

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

V. Feasibility Analysis of the Public-key Cryptosystem

First our public-key cryptosystem isn't an imaginary plan based on the technology which doesn't exist now or the technology difficult to carry out. All that the users need to do are performing the Bell state measurement on an EPR pair, performing operation on a qubit and transmitting qubits through a quantum channel, which have been all realized in laboratory for a long time. So it is easier to carry out in practice.

Second as known quantum cryptography depends on the special properties of quantum system. But in practice quantum systems often undergo decoherence over time which makes them to lose quantum coherence and to turn into classical systems inevitably. It's the most important problem for quantum cryptographic protocol to work in practice. Especially in public-key cryptosystem, KMC needs to keep all users' public keys which are just quantum systems for some time until a user asks for them. This brings a serious challenge for public-key cryptosystem. To overcome this difficulty, we can use the quantum system which has bigger time length of decoherence, such as photon in Single-mode fiber. On the other hand users can update their public keys periodically. By means of such methods, our cryptosystem can perform well to satisfy all users.

Third all that above discussions are based on that Alice and Bob always using noiseless channels to build a key in our protocol. If there are no noiseless channels, can this protocol work? We can study it, too. Let's consider noisy classical channel first. In step 3, Bob sends the id number j to Alice, which is necessary to the next step. If there errors in transmission, Bob is sure to fail. Fortunately classical error-correcting coding technology has been a mature and powerful system. We can fulfill information transmission through a noisy classical channel with very low error rate by error-correcting coding, which guarantees the classical information correct between Alice and Bob.

On the other hand, in step 6 Bob sends the qubit sequence Q_j' to Alice through the quantum channel. If there are random errors existing, Alice will get mistaken bits, which also means communication failure. The solution is error-correcting coding, too. Although quantum error-correcting coding technology is not as mature as classical error-correcting coding technology, it can provide rather satisfying results for most quantum channel.

VI. Discussion and Conclusion

We have pointed out that a public key can be used for only one time in our cryptosystem. This limits the number of user. If KMC keeps M public keys for Alice, M users can send message to Alice at most. If one user needs to communicate with Alice for many times, the number who can exchange information with Alice will be further depressed. Such limit can be removed by developing cryptosystem in which public key can be reused. We will discuss it in future work.

In this paper we provide a quantum public-key cryptosystem based on super dense coding technology. N users can achieve secret communications by the help of a key manage center. The principles of quantum mechanics guarantee that our cryptosystem is unconditionally secure. No one except the two parts involved in communication can get the message. The message can be signed so that the sender's identity can be verified. One qubit in the public key can be used to encrypt two bits of classical information. So our cryptosystem is efficient. Moreover it is more secure against possible attacks.

Acknowledgment

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] C H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and tossing", P*roceedings of IEEE International conference on Computers, Systems and Signal Processing,* Bangalore, India, pp.175, December 1984.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Physical Review Letters*, vol. 67, no. 6, pp.661-663, August 1991.

[3] C. H. Bennett, G. Brassard and N. D. Mermin, "Quantum cryptography without Bell's theorem", *Physical Review Letters*, vol. 68, no. 5, pp.557-559, February 1992.

[4] Hoi-Kwong Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over arbitrarily long distances", *Science*, vol. 283, pp.2050-2056, February 1999.

[5] T. Nguyen, M. A. Sfaxi, S. Ghernaouti-Hélie, "802.11i encryption key distribution using quantum cryptography", *Journal of Networks*, v 1, nol. 5, pp. 9-20, September 2006.

[6] B. Qi, Y. Zhao, X. F. Ma, H. K. Lo, L. Qian, "Quantum key distribution with dual detectors", *Physical Review* A, vol. 75, no. 5, pp.052304, May 2007.

[7] R. Matsumoto, "Quantum multiparty key distribution protocol without use of entanglement", *Physical Review* A, vol. 76, no. 6, pp.062316, June 2007.

[8] Y. Zhao, B. Qi, H. K. Lo, "Quantum key distribution with an unknown and untrusted source", *Physical Review* A, vol. 77, no. 5, pp.052327, May 2008.

[9] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, J. Oppenheim, "Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity", *IEEE Transaction on Information Theory*, vol. 54, no. 6, pp.2604-2620, June 2008.

[10] J. Barrett, R. Colbeck, A. Kent, "Unconditionally secure device-independent quantum key distribution with only two devices", *Physical Review* A 86, pp. 062326, December 2012.

[11] Charles H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, "Experimental quantum cryptography", *Journal of Cryptology*, vol. 5, no.1, pp.3-28, January 1992.

[12] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, K. Nakamura, "Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography", *arXiv:quant-ph*/0403104, March 2004..

[13] W. T. Buttler et al., "Practical Free-Space Quantum Key Distribution over 1 km", *Physical Review Letters*, vol. 81, no. 15, pp.3283-3286, October 1998.

[14] R. Rivest, A. Sharmir, L. Adleman, "A Method for Obstaining Digital Signature and Public-Key Cryptosystem", *Communications of ACM,* vol. 21, no. 2, pp. 120-126, February 1978.

[15] 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.

[16] D. Gottesman, I. Chuang, "Quantum Digital Signatures", *arXiv:quant-ph*/0105032, May 2001.

[17] J. Zhang, "Arbitrated quantum signature protocol using EPR Pairs", *Journal of Networks*, vol. 7, no. 11, p 1803-1810, November 2012.

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

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

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

[21] 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, May 2011.

[22] U. Seyfarth, G. Nikolopoulos, G. Alber, "Symmetries and security of a quantum-public-key encryption based on

single-qubit rotations", *Physical Review* A, 85, pp. 022342, February 2012.
[23] M. Michler, K. Mattle, H. Weinfurter, A. Zeilinger, "Interferometric Bell-state analysis", *Physical Review A*, vol. 53, no. 3, pp. R1209~R1212, March 1996.
[24] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states", *Physical Review Letters*, vol. 69, no. 20, pp. 2881-2884, November 1992.
[25] K. Mattle, H. Weinfurter, P. Kwait et al, "Dense Coding in Experimental Quantum Communication", *Physical Review Letters*, vol. 76, no. 25, pp. 4656-4659, June 1996.

Xiaoyu Li was born in Nanyang, China in 1974. He received the Ph. D. degree in computer software and theory from Institute of Computing Technology, Chinese Academy of Sciences, China in 2004. He majors in quantum information and quantum computing; mobile computing.

He is an associate professor at School of Information Engineering, Zhengzhou University, China.

Dr Li is now the member of Chinese Computer Federation.

Dexi Zhang was born in Lushan, China in 1966. He received the master degree in electric information from Central China Normal University, China in 1999. He majors in quantum information and quantum computing; intelligent information processing.

He is a professor at College of Computer Science and technology, Xuchang University, China.