Quantum authentication protocol using entangled states

Xiaoyu Li
College of Information Engineering
Zhengzhou University
Zhengzhou City, 450052
the People’s Republic of China

Dexi Zhang
College of Computer Science and Technology
Xuchang University
Xuchang City, 461000
the People’s Republic of China

Abstract: In this paper we provide a quantum authentication protocol. The two parties share a sequence of EPR(Einstein-Podolsky-Rosen) pairs as the authentication key. To authenticate each other, one party creates auxiliary qubits and make them interact with the authentication key. After measurement in selected basis, he or she affirm the other’s identity. We shown that no one without the authentication key can pass the authentication process. So the protocol is secure. The authentication key is reusable if there are no eavesdroppers and errors in transmission.

Key–Words: Quantum cryptography, quantum authentication, EPR pair, CNOT operation, security, reusable.

1 Introduction

One of the most important applications of quantum information theory is quantum cryptography. Quantum cryptography is a field that integrates quantum mechanics with cryptograph. The fundamental principles of quantum physics guarantee its security. The first quantum key distribution (OKD) protocol is proposed by C. H. Bennett and G. Brassard [1]. Since then much research work has been done in quantum cryptography, such as quantum key distribution [2-6], quantum secret share [7,8,9], quantum bit commitment [10-11], quantum information hiding [12-14], and information theory for quantum cryptography [15]. Experimentes on QKD has also been accomplished successfully. In 1992, BennettBessette and Brassard first realized BB84 protocol in laboratory[16]. Recently QKD in optical fiber has been achieved [17] beyond 150 km and in free space has been implemented over a distance of 1 km [18].

There is another important problem in cryptography: authentication. If Alice and Bob want to build a key by classical or quantum key distribution protocol, they must affirm each other’s identity at first. So authentication key must be distributed to both sides in order to verify the counterpart’s identity. Quantum authentication is better than classical one in potential useful ways. For example, if an eavesdropper breaks in Alice’s office while she is not present. In classical cryptography the eavesdropper can make a copy of Alice’s authentication key without leaving any trace behind from which Alice may percept his existence. So he can pass the authentication. That is to say, the authentication protocol can no longer work. But in quantum authentication protocol, the authentication key is quantum states. Quantum no-cloning theorem forbids eavesdropper to copy the authentication key. So quantum authentication provides capacity of theft-detection much as quantum key distribution provides security against eavesdropping.

Recently several quantum authentication schemes [19-26] have been proposed. Zeng’s [19] protocol uses EPR pairs as the first authentication keys, and then uses classical keys distributed via quantum key distribution. Barnum’s [20] and Jensen and Schack’s [21] schemes use entanglement and catalysis. Zhang’s scheme [22] accomplishes the authentication using an auxiliary qubit. Ljunggren’s protocol [23] performs authentication integrated with quantum key distribution in virtue of an arbitrator. Li and Barnum’s scheme [24] takes EPR pair as identity token and uses auxiliary EPR pairs to fulfill the authentication. Barnum [25] and Kuhn [26] discussed quantum authentication using both quantum and classical key. In this paper we provide a scheme using EPR pairs as the authentication key. They create auxiliary qubits and have them interact with the authentication. Then the authentication is accomplished by a measurement in selected basis. There is no classical information exchange needed and the authentication key is reusable. In some sense our protocol is analogous to Zhang’s because both them use entangled states as authentication key and create auxiliary qubits to interact with the key. But Zhang’s scheme requires that the auxiliary qubits are sent twice between Alice and Bob. Alice creates auxiliary qubits and sends them to Bob. After Bob
receives the qubits and does some operations, he will send them back to Alice. The authentication process is finished by Alice’s operations in the end. Here we prove that it isn’t necessary at all. In our protocol auxiliary qubits are only sent from Alice to Bob for one times. Then they realize authentication successfully. So our protocol is simpler and more practicable than Zhang’s.

The paper is organized as follows. In section 2 we introduce the basic idea on which our authentication protocol is based. Then the protocol is present in section 3. Next in section 4 we prove that it’s secure. Finally we give some further discussions.

2 Basic Idea

An EPR pair is a two-qubit system which is in one of the four Bell states:

\[|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\]
\[|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)\]
\[|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\]
\[|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).\] (1)

The Bell state measurement is a measurement on a two-qubit system in which one uses the Bell states as the basis. Complete Bell state measurement has been realized recently [27,28].

Now let’s introduce the basic idea of our authentication protocol. Assuming that Alice and Bob share n EPR pairs as the authentication key in which any pair is in one of the four Bell states. For example, an EPR pair is in the state

\[|\Phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})\] (2)

in which the subscript ‘A’ expresses that the qubit is at Alice’s hands and ‘B’ expresses that it is at Bob’s hands. Alice creates an auxiliary qubit (called qubit X) in the state

\[|\varphi\rangle = |0\rangle_0 |0\rangle_1.\] (3)

Then she performs a CNOT operation on qubit X and qubit A at her hands in which the control qubit is qubit X and the target qubit is qubit A. So the state of the whole three-qubits system (qubit A, qubit B, qubit X) is

\[S = \frac{1}{2}(|0\rangle_X |0\rangle_A |0\rangle_B + |0\rangle_X |1\rangle_A |1\rangle_B + |1\rangle_X |1\rangle_A |0\rangle_B + |1\rangle_X |0\rangle_A |1\rangle_B).\] (4)

Then Alice sends qubit X to Bob. When Bob receives it, he does a CNOT operation on qubit B and qubit X in which the control qubit is qubit X and the target qubit is qubit B. So the state of the whole three-qubits system is turned into

\[S = \frac{1}{2}(|0\rangle_X |0\rangle_A |0\rangle_B + |0\rangle_X |1\rangle_A |1\rangle_B + |1\rangle_X |1\rangle_A |0\rangle_B + |1\rangle_X |0\rangle_A |1\rangle_B)\] (5)

Obviously we can see that it comes back as origin. Alice and Bob share the EPR pair in |\Phi^+\rangle and the auxiliary qubit is in |\varphi\rangle. Bob can measures qubit X in basis \{\frac{1}{\sqrt{2}}(|0\rangle_X + |1\rangle_X), \frac{1}{\sqrt{2}}(|0\rangle_X - |1\rangle_X)\}. For simplicity, we rewrite the basis as \{+ \langle X, - \langle X\rangle\}. So Bob will get measurement outcome + \langle X with certainty. Similarly it is easy to prove that if the EPR pair in |\Phi^-\rangle, |\Psi^+\rangle or |\Psi^-\rangle, we get the same result. Later in section IV we will prove that Bob can affirm with a great probability that the one on the other side must be Alice if he always get + \langle X to n EPR pairs. Nobody except Alice and Bob can fulfill the authentication process. So we can design an authentication protocol based on the idea above. Noting that the state of any EPR pair is unchanged after the authentication process, so the authentication key can be reused for next authentication process.

3 Quantum authentication protocol using entangle states

Now we provide our quantum authentication protocol. Alice and Bob share n EPR pairs as the authentication key which is in any state of the set \{\Phi^+_{AB}, \Phi^-_{AB}, \Psi^+_{AB}, \Psi^-_{AB}\}. Alice holds qubit A while Bob holds qubit B. So the sequence of the n states can be written as \psi = (\psi^1_{AB}, \psi^2_{AB}, \ldots, \psi^n_{AB}). Alice and Bob even don’t need to know about the sequence \psi. They only hold qubit A and qubit B of each EPR pairs respectively. If Alice want to prove her identity to Bob, they do as follows.

(1) Alice creates n auxiliary qubits in the state

\[|\varphi\rangle = |+\rangle_X.\]

Then she performs CNOT operation on qubit A and qubit X to each EPR pair in which qubit A is the target qubit and qubit X is the control qubit.

(2) Alice sends all the auxiliary qubits to Bob in sequence.
B is the target qubit and qubit E is the control qubit. From Eve, he performs CNOT operation on qubit E and Bob gets the mixed state. If all the measurement outcomes are \(| >_X \rangle\), the authentication succeeds. Bob is sure that the one on the other side is Alice. If there are too many measurement outcomes \(| >_X \rangle\), the authentication fails. Bob affirms that the one on the other side isn’t Alice.

Similarly if Bob wants to prove his identity to Alice, the two parties just perform the same steps as above except that they exchange their roles in the authentication process.

## 4 Security of the protocol

In this section we prove that no one who hasn’t the authentication key could pass the authentication process. So our protocol is secure.

Now we are assuming that an eavesdropper, for example Eve, wants to impersonate Alice to pass the authentication while Alice is not present. According to our protocol she must sends n qubits to Bob. Eve can only create fake qubits and send them to Bob because she has no authentication key. In general the state of the any qubit which Eve sends to Bob can be described as

$$\rho_E = \sum_{i=1}^{2} p_i |\varphi_i \rangle_E \langle E \varphi_i|$$

in which \(|\varphi_i \rangle_E = a_i |0 \rangle_E + b_i |1 \rangle_E\), \(p_1 + p_2 = 1\), and \(|a_i|^2 + |b_i|^2 = 1\). As known a mixed state is composed of some pure states. So the measurement outcome of the mixed state is the sum of the measurement outcomes of these pure states when we measure these pure states respectively. So what we need to do is to consider \(|\varphi_1 \rangle_E = a_1 |0 \rangle_E + b_1 |1 \rangle_E\) and \(|\varphi_2 \rangle_E = a_2 |0 \rangle_E + b_2 |1 \rangle_E\) respectively and sum the outcomes up. Now we discuss it in detail.

Without losing generality, we assume that the states of the EPR pair is \(|\Phi_{AB} \rangle\). First let’s consider pure states \(|\varphi_1 \rangle_E\). When Bob receives the qubit E from Eve, he performs CNOT operation on qubit E and qubit B according to our protocol in which qubit B is the target qubit and qubit E is the control qubit. So the state of the whole three-qubit system turns into

$$S_1 = \frac{1}{\sqrt{2}} (a_1 |0 \rangle_E |0 \rangle_A |0 \rangle_B + a_1 |0 \rangle_E |1 \rangle_A |1 \rangle_B + b_1 |1 \rangle_E |0 \rangle_A |1 \rangle_B + b_1 |1 \rangle_E |1 \rangle_A |0 \rangle_B).$$

Then Bob measures qubit E in basis \(|+ \rangle_E, |− \rangle_E\) according to the protocol. As known

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

$$|− \rangle_E = \frac{1}{\sqrt{2}} (|0 \rangle_E − |1 \rangle_E).$$

From equation (8) we have

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

$$|1 \rangle_E = \frac{1}{\sqrt{2}} (|+ \rangle_E − |− \rangle_E).$$

Obviously equation (7) can be turned into

$$S_1 = \frac{1}{2} [a_1 (|+ \rangle_E + |− \rangle_E) |0 \rangle_A |0 \rangle_B + a_1 (|+ \rangle_E − |− \rangle_E) |1 \rangle_A |1 \rangle_B + b_1 (|+ \rangle_E − |− \rangle_E) |0 \rangle_A |1 \rangle_B + b_1 (|+ \rangle_E − |− \rangle_E) |1 \rangle_A |0 \rangle_B].$$

If Bob measures it, the probabilities that he gets outcomes \(|+ \rangle_E\) and \(|− \rangle_E\) are

$$P^+_1 = |E < + |S_1 >|^2 = (\frac{1}{2})^2 (|a_1|^2 + |a_1|^2 + |b_1|^2 + |b_1|^2)$$

$$= \frac{1}{4}.$$  

$$P^-_1 = |E < − |S_1 >|^2 = (\frac{1}{2})^2 (|a_1|^2 + |a_1|^2 + |b_1|^2 + |b_1|^2)$$

$$= \frac{1}{4}. $$

So the probability that Bob gets the correct result \(|+ \rangle_E\) is \(1/2\). Doing the same reasoning, to pure state \(|\varphi_2 \rangle_E\), the probability that Bob gets the outcomes \(|+ \rangle_E\) and \(|− \rangle_E\) is

$$P^+_2 = |E < + |S_2 >|^2 = (\frac{1}{2})^2 (|a_2|^2 + |a_2|^2 + |b_2|^2 + |b_2|^2)$$

$$= \frac{1}{4}.$$  

$$P^-_2 = |E < − |S_2 >|^2 = (\frac{1}{2})^2 (|a_2|^2 + |a_2|^2 + |b_2|^2 + |b_2|^2)$$

$$= \frac{1}{4}. $$

Similarly the probability that Bob gets the correct result is also \(1/2\). So we are taking one with another the probability that Bob gets the correct result for \(\rho_E\) is

$$P = p_1 P^+_1 + p_2 P^+_2 = \frac{1}{2} p_1 + \frac{1}{2} p_2 = \frac{1}{2}. $$

If the states of the EPR pair is \(|\Phi_{AB} \rangle\), \(|\Psi_{AB}^+ \rangle\), or \(|\Phi_{AB}^- \rangle\), performing the same reasoning we can get that the probability for Bob to gets the correct result is also \(1/2\). So we come to a conclusion that the probability that Bob gets the correct result to each EPR pair is \(1/2\). There are n EPR pairs in the authentication key. So
Obviously it's a maximally mixed state of one qubit.

If n=1000, we get

\[ P_{error} = (\frac{1}{2})^{1000} \approx 10^{-300}. \]  

(15)

It can be rewritten as

\[ \Gamma = \frac{1}{2} \left( \begin{array}{c|ccc} \left|0 > \right. X & \left|0 > E\right. & \left|0 > A\right. & \left|0 > B\right. \\ \hline \left|0 > X\right. & 0 & 0 & 0 & 0 \\ \left|1 > X\right. & 0 & 1 & 0 & 0 \\ \left|1 > X\right. & 0 & 0 & 1 & 0 \\ \end{array} \right). \]  

(18)

Then Eve sends qubit X to Bob. When receiving it, Bob does CNOT operation according to our protocol in which qubit X is the control qubit and qubit B is the target qubit. So we have

\[ \Gamma = \frac{1}{2} \left( \begin{array}{c|ccc} \left|0 > X\right. & \left|0 > E\right. & \left|0 > A\right. & \left|0 > B\right. \\ \hline \left|0 > X\right. & 0 & 0 & 0 & 0 \\ \left|1 > X\right. & 0 & 1 & 0 & 0 \\ \left|1 > X\right. & 0 & 0 & 1 & 0 \\ \end{array} \right). \]  

(19)

It can be rewritten as

\[ \Gamma = \frac{1}{2\sqrt{2}} \left( \begin{array}{c|ccc} \left|+ > X\right. & \left|+ > X\right. & \left|- > X\right. & \left|+ > X\right. \\ \hline \left|+ > X\right. & 0 & 0 & 0 & 0 \\ \left|+ > X\right. & 0 & 1 & 0 & 0 \\ \left|+ > X\right. & 0 & 0 & 1 & 0 \\ \left|- > X\right. & 0 & 0 & 0 & 0 \\ \end{array} \right). \]  

(20)

From equation(20) we can conclude that Bob will get \(|+ > X\) and \(|- > X\) with equal probability if he measure qubit X in basis \(|+ > X, - > X\) according to our protocol. If the state of the EPR pair is \(|\Phi_{AB}^+\rangle\), \(|\Psi_{AB}^+\rangle\) or \(|\Psi_{AB}^-\rangle\), Bob gets the same results. Taking one with another, the probability for Bob to get correct result required by the protocol is only \(1/2\). So to n EPR pairs the probability that Eve escapes from being found by Alice and Bob is

\[ P_{error} = (\frac{1}{2})^{1000} \approx 10^{-300}. \]  

(22)

It can be rewritten as

\[ \Gamma = \frac{1}{2\sqrt{2}} \left( \begin{array}{c|ccc} \left|+ > X\right. & \left|+ > X\right. & \left|- > X\right. & \left|+ > X\right. \\ \hline \left|+ > X\right. & 0 & 0 & 0 & 0 \\ \left|+ > X\right. & 0 & 1 & 0 & 0 \\ \left|+ > X\right. & 0 & 0 & 1 & 0 \\ \left|- > X\right. & 0 & 0 & 0 & 0 \\ \end{array} \right). \]  

(20)

From equation(20) we can conclude that Bob will get \(|+ > X\) and \(|- > X\) with equal probability if he measure qubit X in basis \(|+ > X, - > X\) according to our protocol. If the state of the EPR pair is \(|\Phi_{AB}^+\rangle\), \(|\Psi_{AB}^+\rangle\) or \(|\Psi_{AB}^-\rangle\), Bob gets the same results. Taking one with another, the probability for Bob to get correct result required by the protocol is only \(1/2\). So to n EPR pairs the probability that Eve escapes from being found by Alice and Bob is

\[ P_{error} = (\frac{1}{2})^{1000} \approx 10^{-300}. \]  

(22)

In other words, this kind of attack can’t succeed yet. So we come to a conclusion that Eve can’t breach our quantum authentication protocol by monitoring the the authentication process between Alice and Bob.

So far we have showed that this quantum authentication protocol is secure.

5 Discussion and conclusion

We must point out that in our protocol the authentication key is reusable only when the authentication
succeeds. That is to say, if an eavesdropper impersonates Alice in the authentication process, he or she will destroy the authentication key though he is sure to be found. So the authentication key is no longer valid. The two parties have to rebuild their key after an eavesdropper’s attack. Similarly if there are some errors in the transmission of the auxiliary qubits although no eavesdropper exists, the authentication key is destroyed, too. These problems are limits to our protocol. They may be solved by error-checking code in the authentication scheme. We will discuss it in future work.

We provide a quantum authentication scheme using EPR pairs as the authentication key. The two parties create auxiliary qubits to interact with the key. At last one party verify the identity of the other through measuring the qubits. The protocol is proved to be secure. No one without the authentication key can pass the authentication. There is no classical information exchange needed in the authentication process. When the authentication is successfully completed, the authentication key is unchanged. So it can be reused.

Acknowledgements: This work is supported by the National Natural Science Foundation of China (NSFC Major Research Program 60496324); the National Natural Science Foundation of China (Grants 60402016). We would thank Ruqian Lu for directing us into this research.

References:


