Quantum Identification Protocol with Trusted Author

Chih-Cheng Hsueh
Department of Information Enginerring
I-Shou University
jrcheng0203@gmail.com

Chien-Yuan Chen
Department of Information Enginerring
I-Shou University
cychen@ isu.edu.tw

Yu-Chin Dai
Department of Information Enginerring
I-Shou University
carlos@axtronics.com.tw

Abstract

In this paper, we propose a quantum identification protocol with trusted author between two entities in quantum channel. At first, the user deposits *n* different sets $\{S_1, S_2, \cdots, S_n\}$ of entangled states to trusted author. Whenever the verifier wants to verify the user's identity, the trusted author would give a set of the first qubits of entangled states to the verifier. The verifier chooses a random numbers $r = (r_1, r_2, \cdots, r_n)$ and applies the operator *X* or nothing to the shared entangled states according to the numbers *r*. Two entities both measure shared states and get two measured values. According to two measured values, the user determines the number *r'*. The verifier compares two numbers *r* and *r'* to determine the protocol which is success or fail. Moreover, our protocol relies on the usage of entanglement.

Keywords: identification, cryptography, quantum cryptography

1. Introduction

In 1995, Crépeau and Salvail presented the quantum identification protocol [2]. They used Bennett and Brassard's protocol [1] to exchange quantum information. In 1999, Dusek et al. designed a quantum identification protocol [3] that needs to share the common secret beforehand. According to the common secret, the information for identification is sent by quantum channels. However, the information of identification in these protocols cannot be used repeatedly. In 2002, Mihara used the property of quantum entanglement and the trusted author (TA) to design an identifiable protocol [4]. In 2003, Wim [5] proved that the security of Mihara's protocol does not rely on the usage of entanglement or any other quantum-mechanical properties. In [4], the trusted author creates the user's identity. However, in our protocol, the user creates information of identity by oneself and the trusted author maintains the user's information of identity by safekeeping, only. Moreover, our protocol relies on the usage of entanglement.

In our protocol, at first, the user deposits *n* different sets of entangled states $\{S_1, S_2, \cdots, S_n\}$ to the trusted author, where $S_j \in \{ \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)$, $\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle - \left|10\right\rangle\right)$ $\}$. Whenever the verifier wants to verify the user's identity, the trusted author would give the set of the first qubits of entangled states to the verifier. The verifier selects a random number $r = (r_1, r_2, \cdots, r_n)$, where $r_i \in \{0,1\}$. If $r_i = 1$, the verifier applies an operator *X* to the *i*-th shared entangled state. Otherwise, the verifier applies nothing to the *i*-th shared entangled state. Then, two

entities both measure the shared states and get two measured values. The verifier sends his measured to the user. According to two measured values and initial entangled states, the user gets a random number r_i' and sends it to the verifier. Finally, the verifier check r_i and r_i'. If $r_i' = r_i$, the quantum identification protocol is success; otherwise it is fail.

This paper is arranged as follows. We describe our quantum identification protocol and give a simple example in Section 2. Section 3 discusses and analyzes our protocol. Finally, conclusions are drawn in Section 4.

2. Our quantum identification protocol

We assume that two entities, called Alice and Bob. Alice must deposit *n* different sets $\{S_1, S_2, \cdots, S_n\}$ of entangled states to the trusted author, where $S_j \in \{ |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\}$. Alice controls the first qubits of all entangled states and the trusted author takes care of the second qubits of all entangled states.

Whenever Bob want to verify Alice's identity, Bob asks the trusted author to verify Alice's identity. In the following, our quantum identification protocol is given.

Step 1:

Bob asks the trusted author to verify Alice's identity. Then, the trusted author gives the second qubits of entangled states to Bob. Then, Alice and Bob perform the following Step 2 and Step 4 for the *i*-th entangled states from *i*=1 to *n*.

Step 2:

Bob selects a random numbers $r = (r_1, r_2, \cdots, r_n)$, where $r_i \in \{0,1\}$. If $r_i = 1$, Bob applies an operator $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ to the *i*-th entangled states. Otherwise, Bob applies nothing to the *i*-th entangled states. Thus, the shared state is changed to $|\Phi_i'\rangle = \begin{cases} X|\Phi_i\rangle, \text{if } r_i = 1 \\ |\Phi_i\rangle, \text{if } r_i = 0 \end{cases}$.

Step 3:

Bob and Alice measure the shared state $|\Phi_i'\rangle$, respectively. Thus, Bob gets the measured values B_i and Alice gets the measured values A_i. Then, Bob sends the measured value B_i to Alice.

Step 4:

According to A_i, B_i, and initial entangled state $|\Phi_i\rangle$, Alice computes the random numbers r_i' by Rule 1.

Rule 1:

① If $A_i = B_i$ and the initial entangled state is $|\Phi_i\rangle = |\Phi^+\rangle$, Alice computes the number r_i' =0.

② If $A_i = B_i$ and the initial entangled state is $|\Phi_i\rangle = |\Phi^-\rangle$, Alice computes the number r_i' =1.

③ If $A_i \neq B_i$ and the initial entangled state is $|\Phi_i\rangle = |\Phi^+\rangle$, Alice computes the number r_i' =1.

④ If $A_i \neq B_i$ and the initial entangled state is $|\Phi_i\rangle = |\Phi^-\rangle$, Alice computes the number r_i' =0.

Then, Alice sends the number r_i' to Bob.

Step 5:

Bob verifies the received numbers $r' = (r_1, r_2, \cdots, r_n)$. If $r_i = r_i'$, the quantum identification protocol is success; otherwise,

the protocol is fail.

***Example*:**

Assume that Bob wants to verify Alice's identity by using our quantum identification with trusted author. Assume that Alice's entangled states is $S=\{|\Phi_1\rangle,|\Phi_2\rangle,|\Phi_3\rangle,|\Phi_4\rangle\}=\{|\Phi^+\rangle,|\Phi^-\rangle,|\Phi^+\rangle,|\Phi^-\rangle\}$.

Then, Alice, Bob and the trusted author performs the following steps.

Step 1:

The trusted author sends the second qubits of $S=\{|\Phi_1\rangle,|\Phi_2\rangle,|\Phi_3\rangle,|\Phi_4\rangle\}$ to Bob. Then, Alice and Bob perform the following Step 2 and Step 3 for the *i*-th entangled states from *i*=1 to 4.

Step 2: (*i*=1)

Bob selects a random number $r=(0,0,1,1)$. According to $r_1=0$, Bob applies nothing to the entangled state $|\Phi_1\rangle$. Thus, the shared state is $|\Phi_1'\rangle=|\Phi_1\rangle=|\Phi^+\rangle$.

Step 3: (*i*=1)

Bob and Alice measure the shared state $|\Phi_1'\rangle$, respectively. Assume that Bob's measured value B_1 is 1 and Alice's measured value A_1 is 1. Then, Bob sends B_1=1 to Alice.

Step 2: (*i*=2)

According to $r_2=0$, Bob applies nothing to the entangled state $|\Phi_2\rangle$. Thus, the shared state is $|\Phi_2'\rangle=|\Phi_2\rangle=|\Phi^-\rangle$.

Step 3: (*i*=2)

Bob and Alice measure the shared state $|\Phi_2'\rangle$, respectively. Assume that Bob's measured value B_2 is 0 and Alice's measured value A_2 is 1. Then, Bob sends B_2=0 to Alice.

Step 2: (*i*=3)

According to r_3=1, Bob applies $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ to the entangled state $|\Phi_3\rangle$. Thus, the shared state is changed to $|\Phi_3'\rangle=X|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$.

Step 3: (*i*=3)

Bob and Alice measure the shared state $|\Phi_3'\rangle$, respectively. Assume that Bob's measured value B_3 is 0 and Alice's measured value A_3 is 1. Then, Bob sends B_3=0 to Alice.

Step 2: (*i*=4)

According to r_4=1, Bob applies $X=\begin{pmatrix}0&1\\1&0\end{pmatrix}$ to the entangled state $|\Phi_4\rangle$. Thus, the shared state is changed to $|\Phi_4'\rangle=X|\Phi^-\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$.

Step 3: (*i*=4)

Bob and Alice measure the shared state $|\Phi_4'\rangle$, respectively. Assume that Bob's measured value B_4 is 0 and Alice's measured value A_4 is 0. Then, Bob sends B_4=0 to Alice.

Step 4:

According to Table 1, Alice computes the verified value r'. When *i*=1, A_1=1, B_1=1 and the initial entangled state is $|\Phi_1\rangle=|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$. Then, Alice guesses that Bob applied nothing to $|\Phi_1\rangle$. Thus, Alice computes the value $r_1'=0$. Similarly, Alice computes the values $r_2'=0$, $r_3'=1$, and $r_4'=1$. Finally, Alice sends the verified values $r'=\{0,0,1,1\}$ to Bob.

Alice			
Initial entangled states	*Measured value B*	*Measured value A*	*The verified value r'*
$\|\Phi^+\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	1	1	0
$\|\Phi^-\rangle = \frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$	0	1	0
$\|\Phi^+\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	0	1	1
$\|\Phi^-\rangle = \frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$	0	0	1

Table 1 : Computing the verified value

Step 5:

According to Alice's verified values $r' = \{0, 0, 1, 1\}$, Bob verifies $r' = r$. Thus, Bob verifies Alice's identity successfully.

3. Discussion and Analysis

In this section, we give correctness and security analysis of our protocol. First, we describe the correctness of our protocol.

We use four cases to discuss our correctness.

Case 1:

If the random number $r_i = 1$, Bob applies X to $|\Phi_i\rangle = |\Phi^+\rangle$. Thus, the entangled state is changed to $|\Phi_i'\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Bob and Alice measure the shared state $|\Phi_i'\rangle$. Assume that Bob gets the measured value B_i=0 and Alice gets the measured value A_i=1. Because $A_i \neq B_i$, Alice guesses that Bob applied X to the entangled state. That is, $r_i' = 1$. Similarly, if Bob gets the measured value B_i=1, then Alice gets the verified value A_i=0. Alice also gets $r_i' = 1$.

Case 2:

If the random number $r_i = 0$, Bob applies nothing to $|\Phi_i\rangle = |\Phi^+\rangle$. Thus, the entangled state is $|\Phi_i'\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Bob and Alice measure the shared state $|\Phi_i'\rangle$. If Bob gets the measured value B_i=1 and Alice gets the measured value A_i=1. Because $A_i = B_i$, Alice guesses that Bob applied nothing to the entangled state. That is, $r_i' = 0$. Similarly, if Bob gets the measured value B_i=0 and Alice gets the measured value A_i=0. Alice also gets $r_i' = 0$.

Case 3:

If the random number $r_i = 1$, Bob applies X to $|\Phi_i\rangle = |\Phi^-\rangle$. Thus, the entangled state is changed to $|\Phi_i'\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. Bob and Alice measure the shared state $|\Phi_i'\rangle$. If Bob gets the measured value B_i=0 and Alice gets the measured value A_i=0. Because $A_i = B_i$, Alice guesses that Bob had applied X to the entangled state. That is, $r_i' = 1$. Similarly, if Bob gets the measured value B_i=1 and Alice gets the measured value A_i=1. Alice also gets $r_i' = 1$.

Case 4:

If the random number $r_i = 0$, Bob applies nothing to $|\Phi_i\rangle = |\Phi^-\rangle$. Thus, the entangled state is $|\Phi_i'\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Bob and Alice measure the shared state $|\Phi_i'\rangle$. If Bob gets the measured value B_i=0 and Alice gets the measured value A_i=1. Because $A_i \neq B_i$, Alice guesses that Bob applied nothing to the entangled state. That is, $r_i' = 0$. Similarly, if Bob gets the measured value B_i=1 and Alice gets the measured value A_i=0. Alice also gets $r_i' = 0$.

From Case 1 to Case 4, we describe that our protocol is correct.

Second, we analyze the security of our protocol. Assume that Nancy wants to impersonate Alice. Because Alice must deposit quantum entangled states

to the trusted author, Nancy cannot impersonate Alice.

If Nancy wants to impersonate Bob, Nancy steals the contents of entangled states from Alice and modifies the contents of entangled states. In our protocol, the set of entangled states *S* is used once. Thus, Nancy gets useless entangled states. Obviously, our protocol need deposit quantum qubits to trusted author, so it is necessary of quantum computer.

4. Conclusions

In this paper, we don't share any secret and achieve identification. In our protocol, at first, Alice deposits *n* different sets of entangled states $\{S_1, S_2, \cdots, S_n\}$ to the trusted author where $S_j \in \{ \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle), \left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle - \left|10\right\rangle)\}$. Whenever Bob wants to verify Alice's identity, the trusted author would give a set of the first qubits of entangled states to Bob. Bob selects a random number $r = (r_1, r_2, \cdots, r_n)$ where $r_i \in \{0,1\}$. If $r_i = 1$, Bob applies an operator *X* to the *i*-th shared entangled state. Otherwise, Bob applies nothing to the *i*-th shared entangled state. Then, Alice and Bob measure the shared states and get two measured values $A = (A_1, A_2, \cdots, A_n)$ and $B = (B_1, B_2, \cdots, B_n)$. Then, Bob sends $B = (B_1, B_2, \cdots, B_n)$ to Alice. According to $A = (A_1, A_2, \cdots, A_n)$, $B = (B_1, B_2, \cdots, B_n)$, and initial entangled state $\left|\Phi_i\right\rangle$, Alice computes the random numbers $r' = (r_1', r_2', \cdots, r_n')$ and sends it to Bob. If $r = r'$, the quantum identification protocol is successfully; otherwise, the protocol is fail.

Acknowledgement

This work was supported in part by the National Science Council of the Republic of China under contract NSC94-2213-E-214-029.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, p. 175, 1984.

[2]C. Crepeau and L. Salvail, "Quantum oblivious mutual identification," *in Advances in Cryptology: Proceedings of Eurocrypt '95 (Springer-Verlag, Berlin, 1995)*, p. 133

[3]M. Dusek, O. Haderka, M. Hendrych, and R. Myska, "Quantum identification system," *Phys. Rev. A*, **60**, 149, 1999.

[4] T. Mihara, "Quantum identification schemes with entanglements," *Phys. Rev. A* **65**, 052326, 2002.

[5] Wim van Dam, "Comment on "Quantum identification schemes with entanglements"", Phys. Rev. A **68**, 026301, 2003.