International Journal of u- and e- Service, Science and Technology
Vol.9, No. 10 (2016), pp.181-186
http://dx.doi.org/10.14257/ijunesst.2016.9.10.17

# Quantum Authentication of Classical Messages Using Non-orthogonal Qubits and Hash Function

Xiangjun Xin, Xiaolin Hua, Chaoyang Li and Dongsheng Chen

*School of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou 450002, China*
*xin_xiang_jun@126.com, xl_hua@126.com, lichaoyang2013@163.com*

***Abstract***

*Quantum authentication protocol can be used to authenticate classical messages in a secure manner. In this paper, by using the cryptographic hash function and non-orthogonal qubits, a quantum authentication protocol of classical messages is proposed. In our protocol, the classical messages and their corresponding tags are encoded as nonorthogonal qubits. The message receiver decodes the classical messages and their corresponding tags from the received qubits by using the authentication key. To verify the validity of the received classical messages, the message receiver verifies whether the hash values of the decoded classical messages are equal to the corresponding tags. Our scheme can be proved to be secure against forgery attack and measurement attack. On the other hand, the authentication key is a binary string, which can be securely obtained and easily saved. What is more, because the authentication key remains secure after executing the authentication protocol, it provides the possibility of reusing the authentication key.*

***Keywords****: Quantum authentication, Hash function, Qubit, Security*

## 1. Introduction

Message authentication is an important topic in the study of cryptography. In the past years, much attention has been paid to the authentication of classical messages using cryptographic tool, such as message authentication codes(MAC) and digital signatures based on unproven assumptions concerning the computational complexity of some algorithms, for example, factoring assumption and discrete logarithm problem [1-2]. However, with the development of quantum information and quantum computation, the security of the classical authentication protocols based on hardness assumptions of mathematics is more and more threatened [3-4]. How to authenticate the classical messages securely becomes an important and interesting topic.

Quantum authentication protocols can be used to authenticate both classical messages and quantum messages securely. The security of these protocols is based on fundamental properties of quantum mechanics, for example, the Heisenberg uncertainty principle and no-cloning theorem, instead of on unproven assumptions concerning the computational complexity of some algorithms. Now, there are two kinds of quantum authentication protocols for messages: quantum authentication protocol of classical messages [5] and the one of quantum messages [6].

On the other hand, quantum authentication protocols can be used to authenticate the identities of the message sender and the corresponding receiver [7-8].

To our knowledge, most of the quantum authentication protocols that have been proposed were used to authenticate quantum messages [6] and [9-12]. However, in the communication world, classical messages are widely used. So, it is more important to study the quantum authentication of classical messages. The quantum authentication protocols of classical messages can be more secure than the traditional authentication protocols, because the former has the properties of quantum authentication. The early

ISSN: 2005-4246 IJUNESST

quantum authentication protocols of classical messages were proposed by Curty *et. al.*, [5]. But, in Curty *et. al.*, protocol, the EPR states were used as the authentication key to authenticate classical messages, and the message sender and corresponding receiver had to share and save the EPR states before authenticating classical messages, then, for their protocol, the quantum storage should be used.

In this paper, a new quantum authentication of classical messages is proposed. In our scheme, instead of using EPR states as the authentication key, the message sender and the corresponding receiver share a binary string as their authentication key, which can be obtained by performing the key distribution protocol of BB84 [13]. Note that the key distribution protocol of BB84 has been proved to be secure against various attacks. Then, for our protocol, the authentication key can be securely obtained and easily saved. To authenticate a classical message, the message sender encodes the classical message and its corresponding tag as indistinguishable qubits selected from a set of non-orthogonal qubits. The message receiver decodes the classical message and its tag from the received qubits and verifies their validity by verifying whether the hash value of the decoded message is the equal to the tag. In our protocol, the hash function is used to generate a tag for the classical message. This is different from the use of constructing the quantum key distribution protocols based hash function [14-15]. Our protocol can be proved to be secure against forgery attack and message attack. On the other hand, this protocol provides the possibility of reusing the authentication key.

The rest of this paper is organized as follows. In the second section, the new quantum authentication protocol of classical messages is proposed. In the third section, we analyze the security of the proposed protocol. At last, we conclude.

## 2. New Construction of Quantum Authentication of Classical Messages

Assume Alice wants to send a certified classical message to Bob. The goal is to make Bob confident about the authenticity of the message and sender. In our protocol, a quantum channel is used. Then, to authenticate the classical message, it is necessary to encode the classical message into qubits. The quantum channel is used to transmit qubits carrying the classical message. On the other hand, to decode the classical messages from the qubits sent from Alice, a quantum decoding algorithm should be performed by Bob. All the encoding and decoding algorithms can be public. Also, to authenticate a classical message, a public cryptographic hash function $H$: $\{0, 1\}^{*}\rightarrow\{0, 1\}^{q}$, where $q$ is a secure parameter, is used. The symbol "||" is used to denote the concatenation of strings. In our protocol, we assume that, before authenticating a classical message, the message sender Alice and message receiver Bob have shared an authentication key, which is a binary string $s=s_1s_2\ldots,s_i,\ldots s_{n+q}$, where $s_i \in \{0, 1\}$ for $i$=0, 1, …,$n+q$, and this string can be securely obtained by executing the quantum key distribution protocol of BB84[13].

Now, by performing the authentication protocol as follow, Alice sends Bob a certified classical message $m=m_1m_2\ldots m_n$, where $m_i \in \{0, 1\}$ for $i$=1, …, $n$.

**Table 1. The State of $|a>$**

| $s_i$ \ $m_i$ | 0 | **1** |
|---|---|---|
| 0 | $\|a>=\|0>$ | $\|\boldsymbol{a}>=\|\mathbf{1}>$ |
| **1** | $\|a>=\|+>=\frac{1}{\sqrt{2}}(\|0>+\|1>)$ | $\|a>=\|->=\frac{1}{\sqrt{2}}(\|0>-\|1>)$ |

**Step 1.** First, Alice computes the hash value $H(m)= m_{n+1}m_{n+2}\ldots m_{n+q}$ of the message $m$, where $m_i \in \{0, 1\}$for $i=n+1, n+2\ldots, n+q$. Then, according the key bit $s_i$ of authentication

 

key $s$ and the message bit $m_i$ for $i$=1, 2…, $n+q$, Alice encodes the bit $m_i$ as the corresponding qubit $|a\rangle$, whose state is chosen from Table 1. For example, if $m_i$=0, $s_i$=1, then the bit $m_i$ of classical message $m$ is encoded as qubit $|a\rangle=|+\rangle$.

After finishing the encoding process, Alice sends Bob the qubit $|a\rangle$. Since the length of the binary string $m||H(m)=m_1m_2\ldots m_nm_{n+1}m_{n+2}\ldots m_{n+q}$ is $p+q$, Alice will send Bob the $p+q$ qubits encoded from $m||H(m)$.

**Step 2.** Once Bob receives the qubit $|a\rangle$, he first checks the key bit $s_i$ of his authentication key $s$. Then, according to Table 1, if $s_i$=0(or $s_i$=1), Bob knows that the qubit $|a\rangle \in \{|0\rangle, |1\rangle\}$(or $|a\rangle \in \{|+\rangle, |-\rangle\}$), so he makes an orthogonal measurement on the qubit $|a\rangle$ by using the corresponding orthogonal base. If the result of the measurement is $|0\rangle$ (or $|+\rangle$), he can decode the binary bit "0" from the qubit $|a\rangle$, or he can decode the binary bit "1". At last, Bob obtains all the $n+q$ binary bits $m_1'm_2'\cdots m_n'm_{n+1}'\cdots m_{n+q}'$ by decoding the received $n+q$ qubits. Then he checks whether $H(m')=m_{n+1}'\cdots m_{n+q}'$ holds, where $m'=m_1'm_2'\cdots m_n'$. If it holds, Bob believes that the message $m'$ decoded from the received qubits is from Alice and accepts it, or he rejects the message.

From the protocol described above, it is found that the measurements are performed on the corresponding orthogonal states, so the correctness of our protocol can be proved easily.

## 3. Security Analysis

From our protocol, it is found that the qubit $|a\rangle$ uniquely determine the classical message sent from Alice. Since Bob masters the authentication key, he can extract the classical message $m$ and its corresponding hash value $H(m)$ from the qubits received by performing correct orthogonal measurements. On the other hand, the string of the qubits encoded from the bits $m_{n+1}m_{n+2}\ldots m_{n+q}$ can be seemed as a tag for the first $n$ qubits encoded from $m_1m_2\ldots m_n$. Since Bob knows the correct orthogonal bases of the measurements, the tag will pass the verification in case of no forgery. That is, if a forgery can pass the measurement and verification of Bob, our protocol would fail.

In this section, we first analyze the security of our protocol under forgery attacks, then we analyze its security under measurement attack.

For the forgery attacks, we mainly consider two kinds of attacks: the no-message attack and the message attack. The first one is that, before Alice's sending any message to Bob, Eve attempts to prepare quantum states that pass the verification algorithm. For the message attack, we assume that Eve can access the quantum messages transmitted in the quantum channel, and she tries to manipulate the quantum messages transmitted in the quantum channel and produce a forged message.

For the measurement attack, Eve attempts to obtain the authentication key by performing some measurements on the quantum messages sent from Alice.

### 3.1. No-Message Attack

Assume Eve prepares a string of normalized pure quantum qubits encoded from a classical binary message $m_1''m_2''\cdots m_n''m_{n+1}''\cdots m_{n+q}''$ satisfying $H(m'')=m_{n+1}''\cdots m_{n+q}''$, where $m''=m_1''m_2''\cdots m_n''$ and $m_i'' \in \{0,1\}$ for $i$=1, 2, …, $p+q$. Then, Eve sends these qubits to Bob. Her goal is to make these particles pass the verification of Bob and to make Bob believe that the classical message decoded from these qubits comes from Alice. In fact, when Bob receives these qubits sent from Eve, he cannot know that they come from a forger, so he executes the step 2 of the protocol and tries to decode the binary message and verifies its validity. Then, according to the step 2 of our protocol, for any qubit $|a'\rangle$ from Eve, Bob will check his current key bit $s_i$. If $s_i$=0, Bob will make an orthogonal measurement on the qubit $|a'\rangle$ by using the orthogonal set $\{|0\rangle, |1\rangle\}$, or he will make the

 

measurement by using the orthogonal set {|+>, |−>}. Note that the key bit $s_i$ of the authentication key $s$ is independent of the choice of classical bit $m_i''$ forged by Eve. So, When Bob makes a measurement on |$a''$>, he can select the correct measurement bases with probability 1/2. Then, for any qubit |$a''$> from Eve, Bob can only get the corresponding binary bit $m_i''$ by decoding |$a''$> with a probability 3/4. Assume that, after decoding all the qubits from Eve, Bob obtains a classical message $m_1'''m_2'''\cdots m_n'''m_{n+1}'''\cdots m_{n+q}'''$. Let $m''' = m_1'''m_2'''\cdots m_n'''$. Then, according to the step 2 of the protocol, Eve can pass the verification of Bob only if $H(m''') = m_{n+1}'''\cdots m_{n+q}'''$, which happens with a negligible probability $(3/4)^{n+q}$. Then, Bob can detect the no-message attack with a probability $1-(3/4)^{n+q}$.

Now, we analyze the security of our protocol in a more complex case. That is, Eve could have prepared one general mixed state $\rho_{a''} = \sum_{i=0}^{1} p_i \mid a_i'' >< a_i'' \mid$ with $\sum_{i=0}^{1} p_i = 1$, instead of the pure quantum state |$a''$>, for the bit $\boldsymbol{m_i''}$. In this case, if Bob makes a measurement on the mixed state using the orthogonal set {|0>, |1>}, he will get the results |0> and |1> with probabilities $P_{|0>} = p_0 \left| < 0 \mid a_0'' > \right|^2 + p_1 \left| < 0 \mid a_1'' > \right|^2$ and $P_{|1>} = p_0 \left| < 1 \mid a_0'' > \right|^2 + p_1 \left| < 1 \mid a_1'' > \right|^2$, respectively. Note that $0<p_0<1$, $0<p_1<1$ and $p_0+p_1=1$. Then, we can obtain both $P_{|0>}<1$ and $P_{|1>}<1$. Similarly, if Bob makes a measurement on the mixed state using the orthogonal set {|+>, |−>}, he will get the results |+> and |−> with probabilities $P_{|+>}<1$ and $P_{|->}<1$, respectively. Note that the key bit $s_i$ of the authentication key $s$ is independent of the choice of classical bit $m_i''$. So, according to step 2 of our protocol, Bob decodes the binary bit "0" and "1" from the mixed state $\rho_{a''}$ with probabilities $P_0=(P_{|0>}+P_{|+>})/2$ and $P_1=(P_{|1>}+P_{|->})/2$, respectively. Since all the number $P_{|0>}$, $P_{|1>}$, $P_{|+>}$, $P_{|->}$ are strictly less than one, we can get $P_0<1$ and $P_1<1$, too. Then, for any mixed state $\rho_{a''}$ from Eve, Bob can only decode the corresponding binary bit $m_i''$ from the mix state designed by Eve with a probability less than $P \leq \max\{P_0, P_1\}<1$. Then, according to the analysis similar to the above paragraph, Eve can pass the verification of Bob only if $H(m''') = m_{n+1}'''\cdots m_{n+q}'''$, which happens with negligible probability not more than $P^{n+q}$. Then, Bob can detect the no-message attack with probability at least $1-P^{n+q}$.

From the discussion above, it is known that our protocol is secure against no-message attack.

### 3.2. Message Attack

There are two kinds of message attacks. In the first kind of attack called trace-preserving completely positive (TPCP) map [16-18], instead of directly forging quantum messages and sending them to Bob, Eve will wait for Alice's original messages and try to manipulate them. Her goal is to convert authentic messages into others so as to pass the verification of Bob. So, for our protocol, Eve tries to convert the states of the qubits sent from Alice into others so that the new states can pass the verification of Bob. Then, based on the knowledge of all the public aspects of the quantum authentication scheme used, Eve determines one unitary quantum operation and applies it to the particles sent from Alice. In the second kind of attack, called measurement attack, Eve tries to extract the information of authentication key by performing some measurements on the transmitted messages in the quantum channel. Especially, if Eve can extract the information of

 

authentication key from the results of the measurements, she may prepare some forged messages, which can pass the verification of Bob.

**3.2.1. TPCP Map:** Consider that Alice sends to Bob a quantum particle $|a\rangle$ whose state is chosen from Table 1 according the key bits $s_i$ shared by Alice and Bob. Eve tries to convert $|a\rangle$ into $|a'\rangle$ by performing some unitary operation $U$ (e.g., $U = i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$) such that $\langle a'|a\rangle=0$. In this case, Bob will extract a tampered bit $k \in \{0, 1\}$ from the tampered qubit $|a'\rangle$, instead of the valid bit $j \in \{0, 1\}$ ($j \neq k$) from the original qubit $|a\rangle$. Eve's goal is to tamper some states of the qubits sent from Alice and then to make the classical message decoded from qubits including the tampered ones can pass the verification of Bob. To achieve her aim, Eve sends all the qubits including the tampered ones to Bob. Assume the classical message decoded from the tampered qubits is $m'_1 m'_2 \cdots m'_n m'_{n+1} \cdots m'_{n+q}$. Note that in this kind of attack, the binary bits decoded from the tampered qubits must have been changed. Then, according to the analysis similar to section 3.1, we know that any change of the transmission will lead to that $H(m') \neq m'_{n+1} \cdots m'_{n+q}$, where $m' = m'_1 m'_2 \cdots m'_n$. Then, our scheme is secure against this kind of attack.

**3.2.2. Measurement:** In this kind of attack, instead of performing a predetermined quantum operation on the qubits sent from Alice, Eve makes measurements on the qubits from Alice and attempts to get some information about the authentication key. According to Table 1, if Eve were able to distinguish the states {|0>, |1>, |+>, |—>}, she could get the information about the authentication key by performing orthogonal measurements on the qubits sent from Alice. However, the states {|0>, |1>, |+>, |− >} are indistinguishable, and for any qubit $|a\rangle$ from Alice, Eve can only guess the key bit $s_i$ (or its corresponding orthogonal bases) correctly with a probability 1/2, then Eve can not obtain the information of the authentication key shared by Alice and Bob.

On the other hand, in our protocol, Alice and Bob need not publish any state of the transmitted qubits or any bit of the classical message. So, Eve cannot get any information of the authentication key from the public channel.

At last, since Eve cannot get the information about the authentication key from the public channel and measurement attack, the authentication key will be still secure after executing the authentication protocol. Then, an interesting property of our protocol is that, it provides the possibility of reusing the authentication key.

## 4. Conclusions

In this paper, a new quantum authentication protocol of classical message is proposed. From the security analysis, it is found that our protocol is secure against the forgery attack and measurement attack. Then, the classical message can be authenticated in a secure manner. On the other hand, because Eve cannot get any information about the authentication key, the authentication key will be still secure after executing the authentication protocol. So, it provides the possibility of reusing the authentication key. At the same time, because the single qubits are much easier to be prepared and implemented, we use single qubits instead of EPR state to transmit the classical message in our protocol. What is more, in our protocol, the authentication key is a binary string, and it can be securely obtained and easily saved.

## Acknowledgments

This work is supported by the Natural Science Foundation of China (Grant No. 61272525), the Foundation for Doctors of Zhengzhou University of Light Industry (NO. 20080014) and the Fundamental and Advanced Technology Research Project of Henan province (Grant No. 152300410129).

## References

[1] R. L. Rivest, A. Shamir and L. Adelman, "A Method for Obtain Digital Signatures and Public-key Cryptosystem", Common. ACM, vol. 21, no. 2, **(1978)**, pp.120-126.
[2] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards", Edited G. Brassard, Springer-Verlag , Berlin, vol. 435, **(1990)**, pp. 239-252.
[3] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithm and Factoring", Proc. of the 35th Annual Symposium on the Foundations of Computer Science, Santa Fe, New Mexico, **(1994)** November 20- 22.
[4] L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack", Phys. Rev. Lett., vol. 79, no. 2, **(1997)**, pp. 325-328.
[5] M. Curty and D. J. Santos, "Quantum Authentication of Classical Messages", Phys. Rev. A, vol. 64, no. 6, **(2001)**, pp. 062309.
[6] M. Curty, D. J. Santos and E. Pérez, "Qubit Authentication", Phys. Rev. A, vol. 66, no. 2, **(2002)**, pp. 022301.
[7] X. Li and L. Chen, "Quantum Authentication Protocol Using Bell States", The First International Symposium on Data, Privacy, and E-Commerce, Chengdu, China, **(2007)** November 1-3.
[8] Y. Kanamori, S. M. Yoo, D. A. Greogry and F. T. Sheldon, "On Quantum Authentication Protocols", Global Telecommunications Conference, St. Louis, Missouni, USA, **(2005)** November 28 - December 2.
[9] W. M, Shi, "Quantum Deniable Authentication Protocol", Quantum Information Processing, vol. 13, no. 7, **(2014)**, pp. 1501-1510.
[10] M. Li, "Public-key Encryption and Authentication of Quantum Information", Science China: Physics, Mechanics and Astronomy, vol. 55, no. 9, **(2012)**, pp. 1618-1629.
[11] T. Hwang, "Quantum Authencryption: One-step Authenticated Quantum Secure Direct Communications for Off-line Communicants", Quantum Information Processing, vol. 13, no. 4, **(2014)**, pp. 925-933.
[12] T. Yan and F. Yan, "Quantum Key Distribution Using Four-level Particles", Chinese Science Bulletin, vol. 56, no. 1 , **(2011)**, pp. 24-28.
[13] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proc. of IEEE Int. Conf. on Computer, System and Signal Processing, Bangalore, India, **(1984)** December 10-12.
[14] K. A. S. Al-Khateeb, M. M. Saeb, M. M. A. Majeed and M. R. Wahiddin, "A Secure Protocol Using 6DP for Quantum Authentication and Hash Functions for Key Distribution (KDP-6DP)", 2010 International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, Malaysia, **(2010)** May 11-12.
[15] M. M. A. Majeed, K. A. S. Al-Khateeb, M. R. Wahiddin and M. M. Saeb, "Protocol of Secure Key Distribution Using Hash Functions and Quantum Authenticated Channels (KDP-6DP)", Journal of Computer Science, vol. 6, no. 10, **(2010)**, pp. 1123-1129.
[16] M. A. Nielsen and C. M. Caves, "Reversible Quantum Operations and Their Application to Teleportation", Phys. Rev. A, vol. 55, no. 4, **(1997)**, pp. 2547 -2556.
[17] M. A. Nielsen, C. M. Caves, B. Schumacher and H. Barnum, "Information-theoretic Approach to Quantum Error Correction and Reversible Measurement", Proc. R. Soc. London, Ser. A, vol. 454, no. 1969, **(1998)**, pp. 277-304.
[18] C. M. Caves, "Quantum Error Correction and Reversible Operations", Supercond., vol. 12, no. 6, **(1999)**, pp. 707 -718.

 