International Journal of Future Generation Communication and Networking
Vol. 9, No. 5 (2016), pp. 123-130
http://dx.doi.org/10.14257/ijfgcn.2016.9.5.12

Quantum Authentication Protocol of Classical Messages Based on Different Sets of Orthogonal Quantum States

Xiangjun[1], Chaoyang Li[1], Dongsheng Chen[1] and Fagen Li[2]

[1]*School of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou 450002, China*
[2]*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China*
xin_xiang_jun@126.com

Abstract

Most of the quantum authentication protocols are used to authenticate quantum messages. In this paper, by using a pair of non-entangled qubits, a quantum authentication protocol of classical messages is proposed. In the pair of qubits, the first one is used to carry a bit message, and the second one is used as a tag to authenticate the classical message. In our protocol, a bit string instead of a sequence of maximally entangled states is used directly as an authentication key, so the authentication key can be easily stored offline. On the other hand, in our protocol, a unitary operation U_A is chosen to encrypt the qubits so that the successful probability of all attacks analyzed is less than one. Our quantum authentication protocol is secure against various attacks such as the no-message attack and message attacks.

Keywords: *authentication, quantum authentication, qubit, unitary operation, security*

1. Introduction

During the network communication, the message authentication is very important. A secure message authentication protocol can be used to ensure the legitimacy of the transmitted data as well as the communicating parties. In general, both digital signatures [1, 2] and message authentication codes (MACs) [3] have the function of authenticating the classical messages. However, the security of traditional digital signatures and MACs depend on some unproven assumptions concerning the computational complexity of some algorithms and the selection of hash functions. With the development of quantum computing technology, the security of these unproven mathematical assumptions and hash functions is facing a great challenge [4, 5].

Compared with the traditional digital signatures and MACs, quantum authentication protocols [6, 7], whose security are based on fundamental properties of quantum mechanics instead of on unproven mathematical assumptions, seem more secure and attractive. Now, the quantum authentication has become an important research subject in quantum cryptography [8].

In the past few years, many quantum authentication protocols have been proposed to authenticate quantum messages [7, 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 only quantum authentication protocol of classical message was proposed by Curty *et al* [6]. In Curty *et al*'s protocol, the message sender and receiver shared a maximally entangled two-qubit $|\psi>_{AB}=(|01>_{AB}-|10>_{AB})/\sqrt{2}$ as their authentication key, and the message sender used the shared authentication key and the operation $E_{A\varepsilon}=|0><0|_A\otimes I_\varepsilon+|1><1|_A\otimes U_\varepsilon$ to encrypt the entangled two-qubit

ISSN: 2233-7857 IJFGCN

$|\varphi_i>$ or $|\varphi_j>$, where $<\varphi_i|\varphi_j>=\delta_{ij}$, and sent the encrypted particles to the receiver. The receiver authenticated one bit of classical message by decrypting and decoding the encrypted particles.

In this paper, a new quantum authentication protocol of classical messages is proposed. Compared with Curty *et al*'s protocol, in our protocol, the maximally entangled two-qubit $|\psi>_{AB}$ is not directly used as the authentication key. In fact, the message sender and receiver share a bit string as their authentication key. Only when the classical message is authenticated will the authentication key be encoded into a sequence of two-qubit maximally entangled states. So, the authentication key can be easily kept offline. To authenticate one bit of classical message, two non-entangled qubits ($|b>$, $|c>$) instead of a maximally entangled state are transmitted. Because the transmitted quantum qubits are nonorthogonal, they are indistinguishable. This makes that the disturbance on the quantum channel can be detected with a certain probability. Our protocol is secure against various kinds of attacks such as the no-message attack and message attacks.

The paper is organized as follows. In Section 2, we propose our new quantum authentication protocol of classical messages. In Section 3, we analyze the security of the proposed protocol against various attacks. In Section 4, we discuss the selection of unitary operations. In Section 5, we conclude.

2. New Construction of Quantum Authentication of Classical Messages

Assume Alice and Bob share a bit string $s=s_1s_2\ldots s_i\ldots$, which can be distributed by executing the quantum key distribution protocol in [8]. The bit string s is used as the authentication key offline. Now, 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. When the classical message is authenticated, Alice encodes the key string s into a sequence of two-qubit maximally entangled states $|s_1>$, $|s_2>\ldots$ where

$$|s_i>\in\left\{|\phi^+>=(|00>_{AB}+|11>_{AB})/\sqrt{2},|\phi^->=(|00>_{AB}-|11>_{AB})/\sqrt{2}\right\}.$$

Here, if $s_i=0$, $|s_i>=|\phi^+>$. Otherwise, $|s_i>=|\phi^->$. This sequence of two-qubit maximally entangled states can be seen as the authentication key online. Only when a binary message m is authenticated, will the key string s be encoded into the authentication key online. On the other hand, in our protocol, all the encoding and decoding algorithms can be public.

Assume the classical message to be authenticated is a bit string $m=m_1m_2\ldots m_i\ldots$, where $m_i\in\{0, 1\}$. Then the key string s is encoded into a sequence of two-qubit maximally entangled states $|s_1>$, $|s_2>$, …, $|s_i>$,…, where $|s_i>\in\left\{|\phi^+>,|\phi^->\right\}$. Alice and Bob share the sequence $|s_1>$, $|s_2>$, …, $|s_i>$,…, as their authentication key online. For any maximally entangled state $|s_i>$, Alice and Bob own the first qubit and the second one, respectively. We call the state $|s_i>$ the current key of Alice and Bob. On the other hand, in our protocol, a publicly known unitary operation U_A, which must satisfy the requirements described in the Section 3, is used. For more details about U_A, please refer to the Section 3.

Our authentication protocol includes two steps as follows.

Step 1. When Alice wants to send Bob a bit message $m_i\in\{0, 1\}$, she first prepares two qubits $|a>$ and $|b>$, which are chosen from Table 1, according to the message m_i and her current key $|s_i>$. For example, suppose $m_i=0$ and $s_i=1$. Then, according to Table 1, $|a>=|b>=|\psi^+>$. Here, $|\psi^+>=(|0>+|1>)/\sqrt{2}$, $|\psi^->=(|0>-|1>)/\sqrt{2}$.

Table 1. The Values of |*a*> and |*b*>

s_i \ m_i	0	**1**
0	|*a*>=|*b*>=|0>	|*a*>=|*b*>=|1>
1	|*a*>=|*b*>=$\|\psi^+>$	|*a*>=|*b*>=$\|\psi^->$

Then, according to her part of $|s_i>$, she performs the following encrypting operation

$$E_A = |0><0|_A \otimes I + |1><1|_A \otimes U_A, \quad (1)$$

on the qubit |*a*>. Assume the encrypted particle of |*a*> is |*c*>. The state of |*c*> is

$$\rho_c = \frac{1}{2}\left(\rho_b + U_A \rho_b U_A^+\right), \quad (2)$$

where $\rho_b = |b><b|$. Then Alice sends the two qubits (|*b*>, |*c*>) to Bob.

Step 2. Once Bob receives the two qubits (|*b*>, |*c*>), he first checks his current key bit s_i. According to Table 1, if s_i=0 (s_i=1), Bob knows that |*b*> must belong to the set {|0>, |1>} ({$|\psi^+>$, $|\psi^->$}), so he makes an orthogonal measurement on |*b*> by using the orthogonal bases {|0>, |1>} ({$|\psi^+>$, $|\psi^->$}). If the result of the corresponding measurement is |0> ($|\psi^+>$), he can decode the binary message "0" from the result, or he can decode the binary message "1". Next, Bob decrypts |*c*> by performing the operation

$$D_B = |0><0|_B \otimes I + |1><1|_B \otimes U_A^+ \quad (3)$$

on his parts of $|s_i>$ and |*c*>. Then, Bob checks the current key bits s_i and chooses correct orthogonal bases from Table 2. After that, Bob performs an orthogonal measurement on the decrypted |*c*> by using the orthogonal bases. If the result of such a measurement is the same as the result of the measurement on |*b*>, Bob will accept the received binary message, or Bob will reject it.

Table 2. Orthogonal Bases for the Measurement on the Decrypted |*c*>

s_i	0	1
Orthogonal bases	{|0>, |1>}	{$|\psi^+>$, $|\psi^->$}

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

3. Security Analysis

In this section, we analyze the security of our protocol under forgery attacks. For the forgery attacks, we mainly consider two kinds of attacks: no-message attack and message attacks.

3.1. No-message Attack

The no-message attack is that, before Alice's sending any quantum message to Bob, Eve attempts to prepare two quantum states (|*b*>, |*c*>) so as to they can be accepted by Bob. Assume Eve prepares two normalized pure quantum states (|*b*>, |*c*>), and sends them to Bob. Her goal is to make the pair (|*b*>, |*c*>) pass the verification of Bob, then Bob will believe that the messages come from Alice. When Bob receives the two qubits, he cannot know that they come from a forger, so he executes the step 2 of the protocol and decodes

the binary message, which is only one bit. Before performing the measurement on the second qubit, the state of decrypted $|c\rangle$ is

$$\rho' = \left(|c\rangle\langle c| + U_A^+ |c\rangle\langle c| U_A \right)/2. \quad (4)$$

Then, according to the step 2 of the protocol, Bob checks his key bits s_i, and makes two corresponding orthogonal measurements. Then we can obtain the probability P_f that Eve deceives Bob, where

$$P_f \le \max\left\{ tr[G_0\rho_b],\ tr[G_1\rho_b], tr[G_2\rho_b],\ tr[G_3\rho_b] \right\}/2, \quad (5)$$

$$\rho_b = |b\rangle\langle b|,$$
$$G_0 = |1\rangle\langle 1| + |\psi^-\rangle\langle\psi^-|,$$
$$G_1 = |1\rangle\langle 1| + |\psi^+\rangle\langle\psi^+|,$$
$$G_2 = |0\rangle\langle 0| + |\psi^-\rangle\langle\psi^-|,$$
$$G_3 = |0\rangle\langle 0| + |\psi^+\rangle\langle\psi^+|.$$

Because ρ' is a positive semidefinite matrix with trace one, we have $tr\left(|0\rangle\langle 0|\,\rho'\right) \le 1$ and $tr\left(|\psi^+\rangle\langle\psi^+|\,\rho'\right) \le 1$. On the other hand, G_0, G_1, G_2 and G_3 are four positive semidefinite matrices with trace two. So, any eigenvalue of the four matrices is in the interval [0, 2]. Because $|G_k| \neq 0$ for any $k \in \{0, 1, 2, 3\}$, any eigenvalue of the four matrices should not be 0 or 2. Therefore, $P_f < 1$. In fact, we can compute that P_f is less than the maximum of the eigenvalues of G_0, G_1, G_2 and G_3. That is, $P_f < 0.854$. Let λ be a security parameter. This means that the successful probability of forging a classical message with λ bits is less than $(P_f)^\lambda$. For example, the successful probability of forging a classical message with 128 bits is less than $(0.854)^{128}$, which can be ignored.

Now, we analyze the security of our protocol in a more complex case. That is, Eve could have prepared two general mixed states ($\rho_b = \sum_{i=0}^{1} p_i |b_i\rangle\langle b_i|$, $\rho_c = \sum_{i=0}^{1} q_i |c_i\rangle\langle c_i|$) with $\sum_{i=0}^{1} p_i = 1$ and $\sum_{i=0}^{1} q_i = 1$. In this case, similarly, we can get the same P_f as equation (5). Then, then we can also obtain $P_f < 0.854$.

From the discussion above, it is known that the successful probability P_f of forging one bit message under no-message attack is strictly less than one. Then, the successful probability of forging a classical message with λ bits is less than $(P_f)^\lambda$, where λ is a security parameter.

3.2. Message Attacks

There are two kinds of message attacks, TPCP map and measurement attack.

In the first kind of attack called TPCP map, 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 ($|b\rangle$, $|c\rangle$) into ($|b'\rangle$, $|c'\rangle$) so that the tampered pair can pass the verification of Bob. Then, based on the knowledge of all the public aspects of the quantum authentication, Eve determines two unitary quantum operations and applies them to the two particles sent by 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 particles 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 Bob two quantum particles ($|b\rangle$, $|c\rangle$), which are chosen from Table 1 and Table 2, respectively, according the key bit s_i shared by Alice and Bob. The goal of Eve is to convert ($|b\rangle$, $|c\rangle$) into ($|b'\rangle$, $|c'\rangle$) by performing some unitary operations so that $\langle b'|b\rangle=0$ and $|c'\rangle$ can pass the verification of Bob. If Eve can achieve her aim, she will send the tampered states ($|b'\rangle$, $|c'\rangle$) to Bob. In this case, Bob will extract a tampered binary message $k\in\{0, 1\}$ from the received particles, instead of the valid binary message $j\in\{0, 1\}$ ($j\neq k$). In fact, in order to achieve this goal, Eve can construct and perform a unitary operation U_E on $|b\rangle$ and its corresponding state will be converted into $|b'\rangle$, which satisfies $\langle b'|b\rangle=0$. The operation should satisfy the following condition:

$$\langle 0|U_E|0\rangle=\langle 1|U_E|1\rangle=\langle \psi^+|U_E|\psi^+\rangle=\langle \psi^-|U_E|\psi^-\rangle=0. \tag{6}$$

Then, we have

$$U_E=\begin{pmatrix} 0 & z \\ -z & 0 \end{pmatrix}, \tag{7}$$

where z is a complex number with $|z|=1$. So, Eve is able to find a unitary operation which can convert the first qubit into $|b'\rangle$ so that $\langle b'|b\rangle=0$. Now, we assume that Eve performs a unitary operation U_c on $|c\rangle$, and sends the result ($|b'\rangle$, $|c'\rangle$) to Bob. Before Bob performs the step 2, the state of $|c'\rangle$ should be

$$\rho_{c'}=\frac{1}{2}\left(U_c\rho_b U_c^+ + U_c U_A \rho_b U_A^+ U_c^+\right), \tag{8}$$

where $\rho_b=|b\rangle\langle b|$. After Bob's decrypting operation, $|c'\rangle$ is converted into $|c''\rangle$ so that its density operator

$$\rho_{c''}=\frac{1}{2}\left(U_c\rho_b U_c^+ + U_A^+ U_c U_A \rho_b U_A^+ U_c^+ U_A\right). \tag{9}$$

The state $|c''\rangle$ can pass the verification of Bob with probability 1 if and only if the following condition (10) holds:

$$\begin{cases} \langle 0|U_c|0\rangle=\langle 1|U_c|1\rangle=\langle 0|U_A^+U_cU_A|0\rangle=\langle 1|U_A^+U_cU_A|1\rangle=\langle \psi^+|U_c|\psi^+\rangle=0 \\ \langle \psi^-|U_c|\psi^-\rangle=\langle \psi^+|U_A^+U_cU_A|\psi^+\rangle=\langle \psi^-|U_A^+U_cU_A|\psi^-\rangle=0 \end{cases} \tag{10}$$

From the condition (10), we obtain $U_c=\begin{pmatrix} 0 & x \\ -x & 0 \end{pmatrix}=U_A\begin{pmatrix} 0 & y \\ -y & 0 \end{pmatrix}U_A^+$, where x and y are two complex numbers with the $|x|=|y|=1$. Let $U_A=\begin{pmatrix} g_1 & g_2 \\ g_3 & g_4 \end{pmatrix}$. Then the following condition (11) should be satisfied:

$$-\frac{g_2}{g_3}=-\frac{g_3}{g_2}=\frac{g_1}{g_4}=\frac{g_4}{g_1}, \text{ or } \begin{cases} g_1=g_4=0 \\ g_2^2=g_3^2\neq 0 \end{cases}, \text{ or } \begin{cases} g_2=g_3=0 \\ g_1^2=g_4^2\neq 0 \end{cases} \tag{11}$$

Therefore, to make the successful probability of converting ($|b\rangle$, $|c\rangle$) into ($|b'\rangle$, $|c'\rangle$) less than one, Alice and Bob should choose U_A so that the condition (11) is not satisfied. In this case, the probability of successful tampering one bit message will be strictly less than one, independently of Eve's TPCP map.

3.2.2. Measurement

For the measurement attack, Eve attempts to obtain the authentication key by performing some measurements on the quantum particles sent from Alice. In this kind of

attack, instead of performing predetermined quantum operations on the particles sent by Alice, Eve makes measurements on ($|b\rangle$, $|c\rangle$) and attempts to get some information about the authentication key. According to Table 1, if Eve were able to distinguish the states $\{|0\rangle, |1\rangle, |\psi^+\rangle, |\psi^-\rangle\}$, she could get the information about the current key bit s_i. However, $\langle k|\psi^+\rangle \neq 0$ and $\langle k|\psi^-\rangle \neq 0$ for all $k \in \{0, 1\}$, so the states $\{|0\rangle, |1\rangle, |\psi^+\rangle, \psi^-\rangle\}$ are indistinguishable, then Eve can not obtain the information of the current key bit s_i.

4. Discussion

In Section 3, we analyze all kinds of attacks, which must be considered, and present the requirements for the unitary operation U_A avoiding the success of the attacks. We have shown that, in order to avoid the message attacks, Alice and Bob should agree to choose U_A so that the condition (11) is not satisfied. In fact, the unitary operation U_A can be easily selected. For example, we can choose

$$U_A = \begin{pmatrix} \frac{i}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}i}{2} & -\frac{1}{2} \end{pmatrix} \tag{12}$$

so that the condition (11) is not satisfied. But, how to find the optimum U_A, so that the successful probability of all attacks for the protocol is as little as possible, is still an open problem.

5. Conclusions

In this paper, a new quantum authentication protocol of classical messages is proposed. In our protocol, a bit string is used as the authentication key, which can be easily kept offline. Only when a classical message is authenticated will the authentication key be encoded into a sequence of two-qubit maximally entangled states. To authenticate a bit message, two qubits are transmitted, and a quantum encrypting scheme is used, too. Because the transmitted qubits are nonorthogonal, they are indistinguishable. This can guarantee any forgery or invalid measurement of the transmitted particles will be detected with a certain probability. Our protocol can be proved to be secure against various attacks such as no-message attack and message attacks.

Acknowledgments

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

References

[1] D. Boneh and X. Boyen, “Short Signatures without Random Oracle”, EUROCRYPT 2004, Interlaken, Switzerland, LNCS 3027, **(2004)**, pp. 56-73.
[2] C. J. Cha and J. H. Cheon, “An Identity-based Signature from Gap Diffie-Hellman Groups”, PKC 2003, Miami, FL, USA, LNCS 2567 **(2003)**, pp.18-30.
[3] M. Bellare, R. Canetti, H. Krawczyk, “Keying Hash Functions for Message Authentication”, Advances in Cryptology — CRYPTO ’96 , Santa Barbara, California, USA, LNCS 1109 **(1996)**, pp. 1-15.
[4] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithm and Factoring”, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Santa Fe, New Mexico, USA, **(1994)**, pp. 124-134.
[5] L. K. Grover, “Quantum Mechanics Helps in Searching for a Needle in a Haystack”, Physical Review Letters, vol. 79, no. 2, **(1997)**, pp. 325-328.

[6] M. Curty and D. J. Santos, "Quantum Authentication of Classical Messages", Physical Review A, vol. 64, no. 6, **(2001)**, 062309.
[7] M. Curty, D. J. Santos and E. Pérez, "Qubit Authentication", Physical Review A, vol. 66, no.7, **(2002)**, 022301.
[8] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computer, System and Signal Processing, Bangalore, India, (**1984)**, pp. 175-179.
[9] T. Yan and F. L. Yan, "Quantum Key Distribution Using Four-level Particles", Chinese Science Bulletin, vol. 56, no. 1, **(2011)**, pp. 24-28.
[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] W. M. Shi, Y. H. Zhou, Y. G. Yang, "Quantum Deniable Authentication Protocol", Quantum Information Processing, vol. 13, no. 7, **(2014)**, pp. 1501-1510.
[12] 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.

Authors

Xiangjun Xin, he received his Ph.D. degree in Cryptography from Xidian University in 2007. He is now an associate professor in the School of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou, China. His recent research interests include cryptography and network security.

Fagen Li, he received his Ph.D. degree in Cryptography from Xidian University, Xi'an, P. R. China in 2007. He is now an associate professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China. His recent research interests include cryptography and network security.