International Journal of Multimedia and Ubiquitous Engineering
Vol.10, No.8 (2015), pp.199-206
http://dx.doi.org/10.14257/ijmue.2015.10.8.20

Quantum Authentication of Classical Messages without Entangled State as Authentication Key

Xiangjun Xin[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*
E-mail: xin_xiang_jun@126.com, fagenli@uestc.edu.cn

Abstract

Classical messages can be authenticated by traditional authentication protocols based on hash functions. The security of these protocols depends on long authentication keys, the selection of appropriate hash functions and some assumptions concerning the computational complexity of some algorithms. In this paper, by encoding the classical binary messages and binary keys as nonorthogonal quantum messages and nonorthogonal sets of states, respectively, and using quantum encrypting scheme, a new quantum authentication protocol is proposed. In our protocol, instead of entangled quantum states, the traditional binary bits, which can be easily saved, are encoded as quantum keys. Because the quantum messages are nonorthogonal, any forgery or measurement on the quantum messages will be detected with a certain probability. Our protocol allows the authentication of binary classical messages in a secure manner.

Keywords: *Quantum authentication; Qubit; Unitary operation; Security*

1. Introduction

With the computer science and network technology development quickly, secure communication becomes more and more important. One important topic is how to authentication the transmitted messages during the message communication.

To authenticate a message, one can use digital signature schemes or message authentication codes (MAC) [1]. The security of traditional digital signatures is based on unproven assumptions concerning the computational complexity of some algorithms, for example, factoring assumption and discrete logarithm problem. However, the development of quantum information and quantum computation makes these unproven assumptions become weaker and weaker [2, 3]. MACs can also be used to authenticate messages. To generate a MAC for a message, the corresponding tag (as a function of the message and a secret key previously shared) should be appended to the message so as to be used to verify the validity of the message. Then, it requires that an authentication key as long as the message should be distributed to the message sender and the corresponding receiver. But, for the traditional cryptography based on unproven assumptions of mathematical problems, it is hard to construct a key distribution protocol such that it can provide prefect secrecy for the shared keys.

At the same time, many researches focus on how to guarantee the information security with the equipment of quantum cryptography [4-7]. The information security provided by quantum cryptography (QC) is based on fundamental properties of quantum mechanics, instead of on unproven assumptions concerning the computational complexity of some algorithms. Compared with the traditional cryptography based on mathematics, QC can be used not only in key distribution protocols [8-9], but also in message authentication

ISSN: 1975-0080 IJMUE

protocols [10-11]. Now, quantum authentication protocols can be classified into two types: protocols of classical messages [10] and ones of quantum messages [11].

In this paper, we mainly discuss the quantum authentication protocols of classical messages. In 2001, the first quantum authentication protocol of classical messages was proposed by Curty and Santo [10]. In their protocol, a qubit is used as the authentication key to authenticate one bit classical message. The message sender and corresponding receiver have to share and save a two-qubit maximally entangled state before authenticating one-bit classical message. Therefore, the quantum storage should be used. In this paper, by encoding the classical messages and keys as nonorthogonal qubits and different unitary quantum operations, respectively, and using quantum encrypting scheme, a new quantum authentication protocol is proposed. In our protocol, the partners don't need to save any entangled state as the authentication key, but encode the binary key bits as unitary operations, which can be seemed as part of the authenticating key. Because the quantum messages are nonorthogonal, any forgery or measurement on the quantum messages will be detected with a certain probability. This protocol allows the authentication of binary classical messages in a secure manner.

The paper is organized as follows. In the second Section, we propose a new quantum authentication protocol of classical messages. In the third Section, we analyze the security of the proposed protocol against various attacks such as the no-message attack and message attack. 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 to transmit quantum messages. So, it is necessary to encode the classical bits into a quantum messages. On the other hand, to verify the quantum messages sent from Alice and decode the corresponding classical bits, a quantum decoding algorithm should be performed by Bob. All the encoding and decoding algorithms can be public. In our protocol, the bits of the classical message and the tag are encoded as nonorthogonal qubits, and the verification of the tag of the message is performed by making the measurements using different orthogonal sets of quantum states. This makes that a forgery or a tamped quantum message can be detected with certain probability. Assume that the classical message to be authenticated is a bit string $m=m_1m_2\ldots m_i\ldots$, where $m_i\in\{0, 1\}$. As for the secret authentication key, we will assume that Alice and Bob share a secret binary string $s_1s_2\ldots,s_i,\ldots$, where $s_i\in\{0, 1\}$ and $i=0, 1, \ldots$, and this string is used as the authentication key, which can be shared by Alice and Bob by executing the quantum key distribution protocol in [4]. In our protocol, we call the key bits m_i and m_{i+1} are current key bit and next key bit, respectively. On the other hand, in our protocol, the message sender Alice and receiver Bob will choose two publicly known unitary quantum operations, U_0 and U_1, which must satisfy the requirements described in the Section 3(For more detail, please refer to the Section 3). Our authentication procedure goes as follows.

Step 1. When Alice wants to send Bob a bit message $m_i\in\{0, 1\}$, she prepares two quantum states ($|a\rangle$, $|c\rangle$) according to her current key bit s_i and the next key bit s_{i+1} , where $|a\rangle$ and $|c\rangle$ are chosen from Table 1 and Table 2 as follows, respectively：

Table 1. The Value of $|a\rangle$

s_i \ m_i	0	**1**
0	$\|a\rangle=\|\varphi_0\rangle=\|0\rangle$	$\|\boldsymbol{a}\rangle=\|\boldsymbol{\varphi_1}\rangle=\|\mathbf{1}\rangle$

1	$\boldsymbol{a}\rangle=\|\boldsymbol{\psi_0}\rangle=\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	$\boldsymbol{a}\rangle=\|\boldsymbol{\psi_1}\rangle=\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$

Table 2. The Value of $|c\rangle$

s_{i+1}	$\|\boldsymbol{c}\rangle$
0	$U_0\|a\rangle$
1	$U_1\|a\rangle$

For example, if m_i=0, s_i=1 and s_{i+1}=0, then the authenticated message m_i and the corresponding tag are encoded as $|a\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $|c\rangle=\frac{1}{\sqrt{2}}U_0(|0\rangle+|1\rangle)$, respectively. After finishing the encoding process, Alice sends the two qubits ($|a\rangle$, $|c\rangle$) to Bob.

Step 2. Once Bob receives the two qubits, he first checks his current key bit s_i. According to Table1, if s_i=0(s_i=1), Bob knows that the first qubit must belong to the set $\{|\varphi_0\rangle, |\varphi_1\rangle\}(\{|\psi_0\rangle, |\psi_1\rangle\})$. So he makes an orthogonal measurement on the first qubit $|a\rangle$ by using the orthogonal set $\{|\varphi_0\rangle, |\varphi_1\rangle\}(\{|\psi_0\rangle, |\psi_1\rangle\})$. If the result of the corresponding measurement is $|\varphi_0\rangle$ ($|\psi_0\rangle$), he can decode the binary message "0" from the result, or he can decode the binary message "1". Next, according to the next key bits s_{i+1}, Bob verifies the validity of the corresponding tag $|c\rangle$ of $|a\rangle$. To do this, Bob performs an orthogonal measurement on the second qubit received by using the orthogonal set chosen from the following Table 3:

Table 3. The Orthogonal Sets for the Measurement of the Second Qubit

s_{i+1} \ s_i	0	**1**
0	$\{U_0\|\varphi_0\rangle, U_0\|\varphi_1\rangle\}$	$\boldsymbol{\{U_0\|\psi_0\rangle, U_0\|\psi_1\rangle\}}$
1	$\boldsymbol{\{U_1\|\varphi_0\rangle, U_1\|\varphi_1\rangle\}}$	$\boldsymbol{\{U_1\|\psi_0\rangle, U_1\|\psi_1\rangle\}}$

That is, if the binary message decoded from the first qubit received is $k\in\{0, 1\}$, s_i=0(s_i=1) and $s_{i+1}=j\in\{0, 1\}$, then the result of the measurement on the second qubit should be $U_j|\varphi_k\rangle$($U_j|\psi_k\rangle$). In this case, Bob will accept the message sent from Alice, or Bob will reject received particles.

For example, suppose m_i=0, s_i=1 and s_{i+1}=0. The qubits sent by Alice must be ($|\psi_0\rangle$, $U_0|\psi_0\rangle$). Then, according to Table 1 and Table 3, Bob will makes two orthogonal measurements on the two qubits by using the orthogonal sets $\{|\psi_0\rangle, |\psi_1\rangle\}$ and $\{U_0|\psi_0\rangle, U_0|\psi_1\rangle\}$, respectively. Then, the results of the measurement will be ($|\psi_0\rangle$, $U_0|\psi_0\rangle$). Therefore, Bob can decode the pair ($|\psi_0\rangle$, $U_0|\psi_0\rangle$) and get the binary message "0" sent from Alice. The result of the measurement on the second qubit shows that the message received is valid. If the results of the measurement are not ($|\psi_0\rangle$, $U_0|\psi_0\rangle$), Bob will reject the received message.

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 our protocol, the first qubit $|a\rangle$ uniquely determines the classical bit sent from the message sender. The message receiver extracts the classical bit from the first qubit by performing a corresponding orthogonal measurement. On the other hand, the second qubit $|c\rangle$ is used as a tag for the first qubit. Since Bob knows the correct orthogonal bases of the

measurement, the tag will pass the verification in case of no forgery or tampering takes place. That is, if a forgery or a tampered message 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, and then 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 two quantum states ($|a\rangle$, $|c\rangle$) that pass the decoding algorithm. For the message attack, we assume that Eve can access the quantum messages transmitted in the quantum channel, and she try to manipulate the quantum messages sent 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.

To make our protocol be secure under all attacks discussed above, we will give the conditions that must be satisfied for the unitary operations U_0 and U_1 chosen by Alice and Bob.

3.1. No-Message Attack

Assume Eve prepares two normalized pure quantum states ($|a\rangle$, $|c\rangle$), and sends them to Bob. Her goal is to make the pair ($|a\rangle$, $|c\rangle$) pass the verification of Bob. 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 tries to decode the binary message. Then, according to the step 2 of the protocol, Bob checks his key bits s_i and s_{i+1}, and makes two corresponding orthogonal measurements on the received states. Then we can obtain the probability P_f that Eve deceives Bob

$$\begin{aligned}
P_f = {} & \frac{1}{4}\langle a|\varphi_0\rangle\langle\varphi_0|a\rangle\langle c|U_0|\varphi_0\rangle\langle\varphi_0|U_0^+|c\rangle + \\
& \frac{1}{4}\langle a|\varphi_0\rangle\langle\varphi_0|a\rangle\langle c|U_1|\varphi_0\rangle\langle\varphi_0|U_1^+|c\rangle + \\
& \frac{1}{4}\langle a|\varphi_1\rangle\langle\varphi_1|a\rangle\langle c|U_0|\varphi_1\rangle\langle\varphi_1|U_0^+|c\rangle + \\
& \frac{1}{4}\langle a|\varphi_1\rangle\langle\varphi_1|a\rangle\langle c|U_1|\varphi_1\rangle\langle\varphi_1|U_1^+|c\rangle + \\
& \frac{1}{4}\langle a|\psi_0\rangle\langle\psi_0|a\rangle\langle c|U_0|\psi_0\rangle\langle\psi_0|U_0^+|c\rangle + \\
& \frac{1}{4}\langle a|\psi_0\rangle\langle\psi_0|a\rangle\langle c|U_1|\psi_0\rangle\langle\psi_0|U_1^+|c\rangle + \\
& \frac{1}{4}\langle a|\psi_1\rangle\langle\psi_1|a\rangle\langle c|U_0|\psi_1\rangle\langle\psi_1|U_0^+|c\rangle + \\
& \frac{1}{4}\langle a|\psi_1\rangle\langle\psi_1|a\rangle\langle c|U_1|\psi_1\rangle\langle\psi_1|U_1^+|c\rangle \\
= {} & \frac{1}{2}tr\left(|\varphi_1\rangle\langle\varphi_1|\rho_a\right) + \frac{1}{4}tr\left(G_0\rho_c\right)tr\left[\left(|\varphi_0\rangle\langle\varphi_0| - |\varphi_1\rangle\langle\varphi_1|\right)\rho_a\right] + \\
& \frac{1}{2}tr\left(|\psi_1\rangle\langle\psi_1|\rho_a\right) + \frac{1}{4}tr\left(G_1\rho_c\right)tr\left[\left(|\psi_0\rangle\langle\psi_0| - |\psi_1\rangle\langle\psi_1|\right)\rho_a\right]
\end{aligned} \tag{2}$$

Where $\rho_a = |a\rangle\langle a|$ and $\rho_c = |c\rangle\langle c|$, and

$$G_0 = U_0|\varphi_0\rangle\langle\varphi_0|U_0^+ + U_1|\varphi_0\rangle\langle\varphi_0|U_1^+,$$

$$G_1 = U_0 \mid \psi_0 >< \psi_0 \mid U_0^+ + U_1 \mid \psi_0 >< \psi_0 \mid U_1^+$$

Are two positive semidefinite matrixes with trace two. So, the eigenvalues of G_0 and G_1 are in the set [0, 2], from which we can get

$$P_f \le \frac{1}{2}\max\left\{tr\left(\mid \varphi_0 >< \varphi_0 \mid \rho_a\right), tr\left(\mid \varphi_1 >< \varphi_1 \mid \rho_a\right)\right\} + \frac{1}{2}\max\left\{tr\left(\mid \psi_0 >< \psi_0 \mid \rho_a\right), tr\left(\mid \psi_1 >< \psi_1 \mid \rho_a\right)\right\} .$$

$$\le 1$$

Therefore, to make P_f <1, any eigenvalue of G_0 and G_1 should not be 0 or 2. This implies that the condition

$$\left|G_0\right| \neq 0 \text{ or } \left|G_1\right| \neq 0, \tag{3}$$

should be satisfied.

Now, we analyze the security of our protocol in a more complex case. That is, Eve could have prepared two general mixed states ($\rho_a = \sum_{i=0}^{1} p_i \mid a_i >< a_i \mid$, $\rho_c = \sum_{i=0}^{1} q_i \mid c_i >< c_i \mid$), with $\sum_{i=0}^{1} p_i = 1$ and $\sum_{i=0}^{1} q_i = 1$, instead of the pure quantum states (|*a*>, |*c*>). In this case, similarly, we can get the same P_f as Eq. (2). Then, if the unitary operations U_0 and U_1 satisfies the condition (3), we can also obtain P_f<1.

From the discussion above, it is known that Alice and Bob can choose appropriate U_0 and U_1 satisfying condition (3) so that the successful probability of forgery under no-message attack is strictly less than one.

3.2. Message Attack

There are two kinds of message attacks. 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 (|*a*>, |*c*>) into (|*a'*>, |*c'*>) so that the new pair can pass the verification of Bob. Then, based on the knowledge of all the public aspects of the quantum authentication scheme used, 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 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 two quantum particles (|*a*>, |*c*>), which are chosen from the Table1 and Table 2, respectively, according the key bits s_i and s_{i+1} shared by Alice and Bob. The goal of Eve is to convert (|*a*>, |*c*>) into (|*a'*>, |*c'*>) by perform some unitary operations such that <*a'*|*a*>=0 and the second qubit |*c'*> can pass the verification of Bob in step 2 of the protocol. If Eve can achieve her aim, she will send the tampered states (|*a'*>, |*c'*>) to Bob. In this case, Bob will extract a tampered binary message $k \in \{0, 1\}$ from the received particles, instead of extracting the valid binary message $j \in \{0, 1\}$ ($j \neq k$), which is the original message sent by Alice. In fact, in order to achieve this goal, Eve can perform the unitary operation $U_a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ on the first particle and its corresponding state will be converted into |*a'*>, which satisfies <*a'*|*a*>=0. For the second

particle, Eve performs an arbitrary TPCP map M , denoted by the unitary operation U_E. Then the state of the second particle is converted into $|c'\rangle=U_E|c\rangle$. The state $|c'\rangle$ can pass the verification of Bob with probability 1 if and only if it satisfies the following condition:

$$\begin{cases} <\varphi_n | U_l^+ U_E U_l | \varphi_n >= 0 \\ <\psi_n | U_l^+ U_E U_l | \psi_n >= 0 \end{cases} \quad \text{for all } n,\ l = 0,1 \tag{4}$$

Where

$$|\varphi_0\rangle=|0\rangle,\ |\varphi_1\rangle=|1\rangle,\ |\psi_0\rangle=\frac{1}{\sqrt{2}}(|0>+|1>),\ |\psi_1\rangle=\frac{1}{\sqrt{2}}(|0>-|1>).$$

From condition (4), we can obtain

$$U_E = U_0 \begin{pmatrix} 0 & x \\ -x & 0 \end{pmatrix} U_0^+ = U_1 \begin{pmatrix} 0 & y \\ -y & 0 \end{pmatrix} U_1^+,$$

Where x and y are two complex numbers with the absolute value 1. This implies

$$U \begin{pmatrix} 0 & x \\ -x & 0 \end{pmatrix} = \begin{pmatrix} 0 & y \\ -y & 0 \end{pmatrix} U . \tag{5}$$

Where $U = U_1^+ U_0$ is a unitary matrix. Let $U = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}$. From condition (5), we can get that the condition (6) as follow should be satisfied:

$$-\frac{t_2}{t_3} = -\frac{t_3}{t_2} = \frac{t_1}{t_4} = \frac{t_4}{t_1}, \text{ or } \begin{cases} t_1 = t_4 = 0 \\ t_2^2 = t_3^2 \neq 0 \end{cases}, \text{ or } \begin{cases} t_2 = t_3 = 0 \\ t_1^2 = t_4^2 \neq 0 \end{cases} \tag{6}$$

Therefore, to make the successful probability of converting ($|a\rangle$, $|c\rangle$) into ($|a'\rangle$, $|c'\rangle$) less than one, Alice and Bob can select the elements of U_0 and U_1 such that the condition (6) is not satisfied. That is, if Alice and Bob choose U_0 and U_1 such that that requirement (6) is not satisfied, then the probability of successful tampering will be strictly less than one, independently of Eve's TPCP map.

3.2.2. Measurement

In this kind of attack, instead of performing a predetermined quantum operation on the message sent by Alice, Eve makes measurements on ($|a\rangle$, $|c\rangle$) and attempts to get some information about the authentication key. According to Table 1, if Eve were able to distinguish the states $\{|\varphi_0\rangle, |\varphi_1\rangle, |\psi_0\rangle, |\psi_1\rangle\}$, she could get some information about the current key bit s_i. However, $\langle\psi_i|\varphi_j\rangle\neq 0$, so the states $\{|\varphi_0\rangle, |\varphi_1\rangle, |\psi_0\rangle, |\psi_1\rangle\}$ are indistinguishable. Then, Eve can not obtain the information of the current key bit s_i shared by Alice and Bob. According to Table 2, if Eve were able to distinguish the quantum states

$$\{U_0|\varphi_0\rangle, U_0|\varphi_1\rangle, U_0|\psi_0\rangle, U_0|\psi_1\rangle, U_1|\varphi_0\rangle, U_1|\varphi_1\rangle, U_1|\psi_0\rangle, U_1|\psi_1\rangle\},$$

She could get the information about the next key bit s_{i+1}. In order to avoid this attack, Alice and Bob must choose U_0 and U_1 such that the set of states

$$\{U_0|\varphi_0\rangle, U_0|\varphi_1\rangle, U_0|\psi_0\rangle, U_0|\psi_1\rangle, U_1|\varphi_0\rangle, U_1|\varphi_1\rangle, U_1|\psi_0\rangle, U_1|\psi_1\rangle\}$$

Is not orthogonal. This requirement can be rewritten as

$$< a | U_1^+ U_0 | a >\neq 0 \tag{7}$$

For, at least, one $|a\rangle\in\{|\varphi_0\rangle, |\varphi_1\rangle, |\psi_0\rangle, |\psi_1\rangle\}$. Therefore, to make the probability of Eve succeeding in getting key bit s_i or s_{i+1} less than one, Alice and Bob can choose U_0 and U_1 such that the condition (7) is satisfied.

On the other hand, since the states $\{|\varphi_0\rangle, |\varphi_1\rangle, |\psi_0\rangle, |\psi_1\rangle\}$ are nonorthogonal, the first qubit is indistinguishable. Of course, When Bob verifies the second qubit by performing a correct measurement, if it can not pass the verification, we can infer that the first qubit

may have been tampered by Eve, or it is a forged qubit. If necessary, Alice and Bob can also publish the state of the first qubit $|a\rangle$ to detect the tampering or measurement performed by Eve.

4. Discussion

In Section 3, we analyze all kinds of attacks, which must be considered, and present the requirements for the unitary operations U_0 and U_1 avoiding the success of the attacks. We have shown that, in order to avoid the forgery attacks and measurement attack, Alice and Bob should agree to choose U_0 and U_1 such that the conditions (3, 7) are satisfied and the condition (6) is not satisfied. In fact, the unitary operations U_0 and U_1 can be easily selected to satisfy all the requirements. For example, we can choose

$$U_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad U_1 = \begin{pmatrix} \frac{i}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}i}{2} & -\frac{1}{2} \end{pmatrix}. \tag{8}$$

We can verify that all the requirements are satisfied by the matrixes selected in (8). But, how to find the optimum U_0 and U_1 such that all the successful probability of attack for the protocol is as little as possible is still an open problem.

5. Conclusions

In this paper, using a pair of qubits, a new quantum authentication protocol of classical messages is proposed. The first qubit is used to carry the classical message, and the second qubit can be seemed as a tag for the classical message. Both qubits are selected in different nonorthogonal sets of states, which make the transmitted quantum messages are indistinguishable. But, since the message receiver masters the correct authentication key, he can always perform the correct measurements on the received quantum messages and decode the corresponding binary messages from the received states. In Section 3, to make the successful probability of all attacks analyzed less than one, Alice and Bob can choose the unitary operations U_0 and U_1 satisfying the specified conditions. In practice, Alice and Bob need not save any quantum state as their authentication keys. When executing the protocol, they can encode the classical key as different orthogonal sets of states, but the states selected from the different orthogonal sets should be nonorthogonal. On the other hand, the classical binary messages can be encoded as nonorthogonal qubits selected from different orthogonal sets of states so that the transmitted quantum messages are indistinguishable. The nonorthogonal property between different states makes the proposed protocol be secure against the various attacks.

Acknowledgements

This work is supported by the Natural Science Foundation of China (Grant No. 61272525) and the Fundamental and Advanced Technology Research Project of Henan province (Principal Investigator: Xiangjun Xin).

.

References

[1] W. Diffie and M. Hellman, “New Direction in Cryptography,” IEEE Transactions on Information Theory, vol.22 no. 6, **(1976)**.
[2] 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, USA, **(1994)** November 20- 22.
[3] L. K. Grover, “Quantum Mechanics Helps in Searching for a Needle in a Haystack,” Phys. Rev. Lett., vol.79 no.2, **(1997)**.
[4] 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.
[5] W. M. Shi, "Quantum Deniable Authentication Protocol," Quantum Information Processing, vol. 13 no 7, **(2014)**.
[6] M. Li, "Public-key Encryption and Authentication of Quantum Information," Science China: Physics, Mechanics and Astronomy, vol. 55 no 9, **(2012)**.
[7] T. Hwang, Y. P. Luo, C. W. Yang and T. H. Lim, "Quantum Authencryption: One-step Authenticated Quantum Secure Direct Communications for Off-line Communicants," Quantum Information Processing, vol.13 no 4, **(2014)**.
[8] T. Yan and F. Yan, "Quantum Key Distribution Using Four-level Particles," Chinese Science Bulletin, vol.56 no 1, **(2011)**.
[9] A. El Allati, M. El Baz and Y.Hassouni, "Quantum Key Distribution via Tripartite Coherent States," Quantum Inf. Process, vol. 10 no 5, (**2011)**.
[10] M. Curty and D. J. Santos, "Quantum Authentication of Classical Messages," Phys. Rev. A, vol.64 no.6, **(2001)**.
[11] M. Curty, D. J. Santos and E. Pérez, "Qubit Authentication," Phys. Rev. A, vol.66 no. 2, **(2002)**.

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.

