International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.285-292
http://dx.doi.org/10.14257/ijsia.2015.9.7.25

Quantum Authentication Protocol for Classical Messages Based on Bell states and Hash Function

Xiangjun Xin[1], Xiaolin Hua[1], Jianpo Song[2] and Fagen Li[3]

[1]*School of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou 450002, China*
[2]*Department of Computer Science, Xuchang Technology and Economy school, Changge 461500, China*
[3]*School of Computer Science and Engineering,University of Electronic Science and Technology of China, Chengdu 611731, China*
xin_xiang_jun@126.com

Abstract

Quantum authentication protocols can be used to authenticate both quantum messages and classical messages. In this paper, a new quantum authentication protocol of classical messages is proposed. In our protocol, a sequence of Bell states is shared by the message sender and the corresponding receiver. This sequence is used as the authentication key. Four different unitary operations U_0, U_1, U_2 and U_3 are used to encode a classical message m *and its hash value h(m) into a sequence of Bell states. To authenticate the classical message, the message receiver extracts m and h(m) from the qubits owned by himself/herself, and verifies whether h(m) matches m. The adversary's disturbance to the quantum channel can be detected by checking whether h(m) matches m. The transmitted message has the properties of both secrecy and authentication. Our quantum authentication protocol is secure against message attack and no-message attack.*

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

1. Introduction

Message authentication protocols can be used to authenticate the sources, integrity and unforgeability of the transmitted messages. In the classical message authentication protocols based on mathematical complexity assumptions, digital signature schemes [1, 2] and message authentication codes (MACs) are usually used [3]. However, with the development of quantum computing technology, the security of the classical message authentication protocols based on the unproven mathematical assumptions are faced with a great challenge.

Quantum cryptosystems [4, 5] take advantage of Heisenberg's uncertainty principle, according to which measuring a quantum system in general disturbs it and yields incomplete information about its state before the measurement. This makes that the eavesdropper who tries to eavesdrop the information in the quantum channel can be detected. This advantage makes that quantum cryptography can be used to distribute secret key so that the key has the property of perfect secrecy. Now, although quantum cryptography is best known for its applications in key distribution protocols [6, 7], quantum techniques can also assist in the achievement of quantum authentication protocols [8, 9, 10-12]. In this paper, we mainly focus on the study of quantum authentication protocols.

In the quantum authentication protocols, the authenticated messages are encrypted by using quantum encrypting algorithm, so these protocols have the properties of both secrecy and authentication for the transmitted messages. To our knowledge, most of the

ISSN: 1738-9976 IJSIA

quantum authentication protocols so far were used to authenticate quantum messages. However, in the communication world, classical messages are widely used. So, it is necessary to study the quantum authentication of classical messages. The quantum authentication protocols of classical messages can be more secure than the classical authentication protocols, because the security of the former is based on fundamental properties of quantum mechanics instead of on unproven mathematical assumptions.

The early quantum authentication protocols of classical messages were proposed by Curty et al. [8, 9]. In these protocols, the message sender and corresponding receiver shared two-qubit maximally entangled states as their authentication key. To authenticate one bit of classical message, the message sender sent the entangled qubits to the message receiver.

In this paper, a new quantum authentication protocol of classical messages is proposed. Our protocol is different from the early ones. That is, in our protocol, the hash function is introduced to reduce the successful probability of various kinds of known attacks such as no-message attack and message attack. In our protocol, the message sender and message receiver share a sequence of Bell states as their authentication key. To send a classical message, the message sender performs some unitary operations on his/her own particles and sends the results to the message receiver. One transmitted particle can carry two bits of classical messages. The message receiver decodes the classical message and its corresponding hash value from the received sequence of particles. By checking the hash value of the decoded classical message, the message receiver can verify the validity of the transmitted classical message. Any forgery or measurement on the transmitted particles will be detected by the valid message receiver.

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.

2. New Construction of Quantum Authentication of Classical Messages

In our protocol, four Bell states as follows

$$|\psi^- >= \frac{1}{\sqrt{2}}(|01> - |10>),$$

$$|\psi^+ >= \frac{1}{\sqrt{2}}(|01> + |10>),$$

$$|\phi^- >= \frac{1}{\sqrt{2}}(|00> - |11>),$$

$$|\phi^+ >= \frac{1}{\sqrt{2}}(|00> + |11>),$$

are used. Let $H:\{0, 1\}^* \rightarrow \{0, 1\}^n$ be a secure public cryptographic hash function, where n is a positive number. On the other hand, in our protocol, four unitary operations

$$U_0 = I = |0><0| + |1><1|,$$

$$U_1 = \sigma_z = |0><0| - |1><1|,$$

$$U_2 = \sigma_x = |1><0| + |0><1|,$$

$$U_3 = i\sigma_y = |0><1| - |1><0|.$$

are used.

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 message into a sequence of particles. On the other hand, to verify the quantum messages sent from Alice and decode the corresponding classical message, a quantum

decoding algorithm should be performed by Bob. All the encoding and decoding algorithms can be public. In our protocol, four different unitary operations, U_0, U_1, U_2 and U_3, are performed on the qubits owned by Alice so as to encode the classical message into a sequence of Bell states.

Assume the message to be authenticated is a bit string $m=m_1m_2\ldots m_i\ldots m_t$, where m_i is a two-bit message. This is, $m_i \in \{00, 01, 10, 11\}$ for $i=1, 2, \ldots, t$. We will assume that Alice and Bob share a sequence of two-qubit maximally entangled states $|s_1>, |s_2>, \ldots, |s_i>, \ldots, |s_{t+n}>$ as their authentication keys, where

$$|s_i>=|\psi^->=\frac{1}{\sqrt{2}}\left(|01>_{AB}-|10>_{AB}\right).$$

Both Alice and Bob own one qubit of the state $|s_i>$. For each $|s_i>$, Alice owns the first qubit, while Bob owns the second one. In detail, the shared sequence of particles $|s_1>, |s_2>, \ldots, |s_i>, \ldots, |s_{t+n}>$ is denoted by $\{(P_{A,1}, P_{B,1}), (P_{A,2}, P_{B,2}), \ldots, (P_{A,t}, P_{B,t}), (P_{A,t+1}, P_{B,t+1}), \ldots,(P_{A,t+n}, P_{B,t+n})\}$, where the sequence of particles $\{P_{A,1}, P_{A,2}, \ldots,P_{A,t}, P_{A,t+1}, \ldots,P_{A,t+n}\}$ is owned by Alice, while the sequence of particles $\{P_{B,1}, P_{B,2}, \ldots,P_{B,t}, P_{B,t+1}, \ldots,P_{B,t+n}\}$ by Bob. By performing the four unitary operations $\{U_0, U_1, U_2, U_3\}$ on the first qubit of $|s_i>$, Alice can transform the state $|s_i>$ into $|\psi^->, |\psi^+>, -|\phi^->, -|\phi^+>$, respectively. In fact, we have

$$U_0 \otimes I\,|\psi^->=|\psi^->,$$
$$U_1 \otimes I\,|\psi^->=|\psi^+>,$$
$$U_2 \otimes I\,|\psi^->=-|\phi^->,$$
$$U_3 \otimes I\,|\psi^->=-|\phi^+>.$$

Alice and Bob agree on that the four Bell states $|\psi^->, |\psi^+>, |\phi^->, |\phi^+>$ (or the four unitary operations U_0, U_1, U_2 and U_3) correspond to four two-bit messages 00, 01, 10, 11, respectively. Before sending the classical message $m=m_1m_2\ldots m_t\ldots m_t$ to Bob, Alice computes the hash value $h(m)=m_{t+1}m_{t+2}\ldots m_{t+n}$, after which she performs the corresponding unitary operations on the first particle $P_{A,i}$ ($i=1, 2,\ldots, t+n$) according to m_i ($i=1, 2,\ldots, t+n$) and sends the results $P'_{A,i}$ ($i=1, 2,\ldots, t+n$) to Bob. For example, if m=1011…00…01 and $h(m)$=0110(*i.e.*, n=4), then $m||h(m)$= 1011…00…010110, where the symbol "||" denotes connection. Alice will perform the unitary operations U_2, U_3, …, U_0, …,U_1, U_1, U_2 on the particles $\{P_{A,1}, P_{A,2}, \ldots,P_{A,t}, P_{A,t+1}, P_{A,t+2}\}$, respectively, and sends the results to Bob. Then, Bob will own the sequence of Bell states $\{-|\phi^->, -|\phi^+>,\ldots, |\psi^->,\ldots,|\psi^+>, |\psi^+>,-|\phi^->\}$ for the message $m\,||h(m)$.

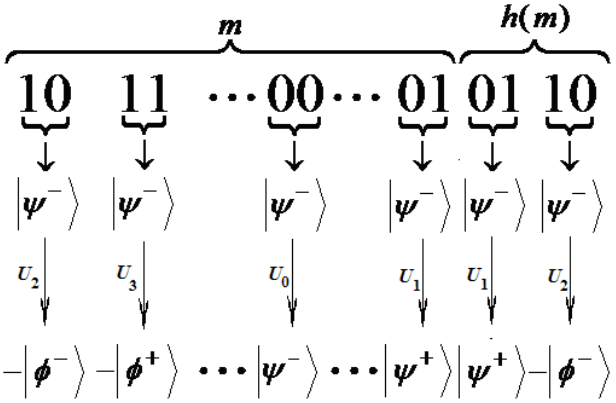

Figure 1. An Example of Alice's Encoding Process

Once receiving the particles $\{P'_{A,1}, P'_{A,2}, \ldots, P'_{A,t}, P'_{A,t+1}, \ldots, P'_{A,t+n}\}$ from Alice, Bob makes the Bell-basis measurements on the sequence of pairs $\{(P'_{A,1}, P_{B,1}), (P'_{A,2}, P_{B,2}), \ldots, (P'_{A,t}, P_{B,t}), (P'_{A,t+1}, P_{B,t+1}), \ldots, (P'_{A,t+n}, P_{B,t+n})\}$. Then, Bob can decode the classical message m and its hash value h from the results of the measurements on $\{(P'_{A,1}, P_{B,1}), (P'_{A,2}, P_{B,2}), \ldots, (P'_{A,t}, P_{B,t}), (P'_{A,t+1}, P_{B,t+1}), \ldots, (P'_{A,t+n}, P_{B,t+n})\}$. If $h=h(m)$, Bob accepts the message m, or he will reject it. For example, if the results of the measurements are

$$\underbrace{|\phi^-\rangle, |\phi^+\rangle, \ldots, |\psi^-\rangle, \ldots, |\psi^+\rangle}_{t \text{ Bell states for message } m}, \quad \underbrace{|\psi^+\rangle, |\phi^-\rangle}_{\text{two Bell states for hash value } h(m)},$$

Bob can get the classical message m=1011…00…01 and the hash value 0110. To authenticate the validity of m, Bob verifies whether $h(m)$= 0110. If $h(m)$= 0110, Bob will accept the message m, or he will reject it.

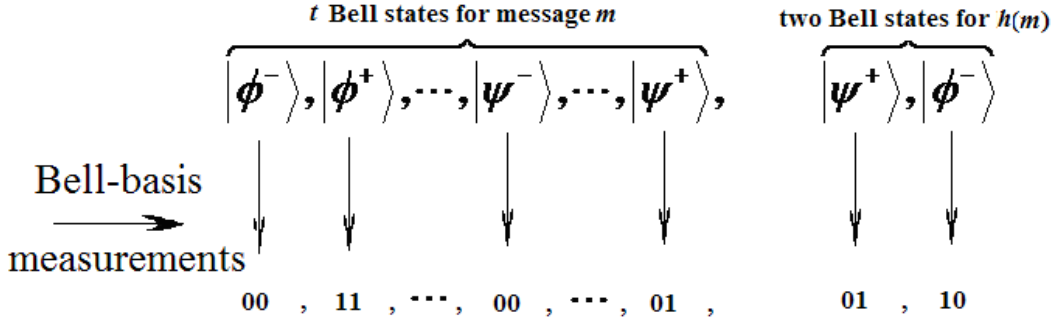

Figure 2. An Example of Bob's Decoding Process

3. Security Analysis

From our protocol, it is found that the each qubit sent from Alice carries two bits of binary message. Bob extracts the classical message m and its corresponding hash value from the results of quantum measurements by performing Bell-basis measurements. Because Alice and Bob share the sequence of Bell states, $\{(P_{A,1}, P_{B,1}), (P_{A,2}, P_{B,2}), \ldots, (P_{A,t}, P_{B,t}), (P_{A,t+1}, P_{B,t+1}), \ldots, (P_{A,t+n}, P_{B,t+n})\}$, the message m and its hash value $h(m)$ can always be decoded and verified. The message m will pass the verification in case that no forgery or tampering with the sent message occurs. That is, if a forgery or tampered message can pass the verification of Bob, our protocol would fail.

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

The no-message attack is that, before Alice's sending any message to Bob, Eve attempts to prepare a sequence of qubits that passes the decoding algorithm.

For the message attacks, we assume that Eve can access the qubits transmitted in the quantum channel, and she tries to manipulate the quantum message sent from Alice and produces a forged message. In this kind of attack, Eve also attempts to obtain the authentication key by performing some measurements on the quantum message sent from Alice.

3.1. No-message Attack

Assume Eve prepares a sequence of pure qubits $\{|a_1\rangle, |a_2\rangle, \ldots, |a_t\rangle, |a_{t+1}\rangle, \ldots, |a_{t+n}\rangle\}$ and sends it to Bob. Her goal is to make the sequence pass the verification of Bob so as to make Bob believe that the classical message carried by this sequence comes from Alice. When Bob receives this sequence, he cannot know that it comes from a forger, so he performs the Bell-basis measurements on the qubits owned by himself.

For example, assume $|a_1\rangle=e|0\rangle+f|1\rangle$, which comes from Eve. When Bob receives $|a_1\rangle$, the global state of $(P_{A,1}, |a_1\rangle, P_{B,1})$ is

$$|v>=\frac{1}{2}\begin{bmatrix}(e|0>-f|1>)|\psi^+>+(e|0>+f|1>)|\psi^->+\\(f|0>-e|1>)|\phi^+>-(f|0>+e|1>)|\phi^+>\end{bmatrix}.$$

When Bob performs the Bell-basis measurement on the particles $|a_1>$ and $P_{B,1}$, he will get the results $|\psi^+>$, $|\psi^->$, $|\phi^+>$, $|\phi^->$ with the probability 1/4 , respectively. That is, when Bob receives the forged sequence $\{|a_1>, |a_2>, \ldots, |a_t>, |a_{t+1}>, \ldots, |a_{t+n}>\}$, he will perform the Bell-basis measurements on the sequence $\{(|a_1>, P_{B,1}), (|a_2>, P_{B,2}), \ldots, (|a_{t+n}>, P_{B,t+n})\}$, and get a random sequence of Bell states $\{|r_1>, |r_2>, \ldots, |r_t>, |r_{t+1}>, \ldots, |r_{t+n}>\}$, where $|r_i>$ is one of the four Bell bases. This means that the classical message m' extracted from $\{|r_1>, |r_2>, \ldots, |r_t>\}$ and the hash value h' extracted from $\{|r_{t+1}>, \ldots, |r_{t+n}>\}$ satisfy the verification equation $h'=h(m')$ with probability $1/2^n$. Then, the successful probability of forgery under no-message attack of Bob is as little as $1/2^n$.

3.2. Message Attacks

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. Note that for each Bell state, Eve can only have the access to the particle transmitted from Alice. Although Eve does not know what classical message is transmitted, she attempts to convert the authentic message into another one so as to pass the verification of Bob. So, for our protocol, Eve performs a unitary operation on the particles from Alice and sends the results to Bob. Eve tries to convert each Bell state into another one so that the tampered Bell state 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 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 the authentication key by performing some measurements on the transmitted message in the quantum channel. This kind of attack is more dangerous. If Eve can extract the information of authentication key from the results of the measurements, she may arbitrarily prepare the forged messages, which can pass the verification of Bob.

3.2.1. TPCP Map: Consider that Alice sends to Bob a sequence of quantum particles $\{P'_{A,1}, P'_{A,2}, \ldots, P'_{A,t}, P'_{A,t+1}, \ldots, P'_{A,t+n}\}$. Assume the sequence $\{(P'_{A,1}, P_{B,1}), (P'_{A,2}, P_{B,2}), \ldots, (P'_{A,t}, P_{B,t}), (P'_{A,t+1}, P_{B,t+1}), \ldots, (P'_{A,t+n-1}, P_{B,t+n-1}), (P'_{A,t+n}, P_{B,t+n})\}$ is a sequence of Bell states (say, $|\psi^+>, |\phi^->, \ldots, |\phi^+>, |\phi^+>, \ldots, |\psi^->, -|\phi^->$). The goal of Eve is to convert this sequence into another one (say, $|\phi^+>, -|\psi^->, \ldots, |\psi^+>, |\psi^+>, \ldots, -|\phi^->, |\psi^->$) by performing some unitary operation U_E (say, U_2) on all the particles from Alice, so that the disturbed sequence can pass the verification of Bob. Note that this change will make that the classical message m' and the hash value h' extracted from the disturbed sequence do not satisfy the verification equation $h'=h(m')$. Therefore, the sequence disturbed by Eve can not pass the verification of Bob, and the attack of TPCP map will be detected by Bob, so our protocol 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 message sent by Alice, Eve makes measurements on the sequence of particles $\{P'_{A,1}, P'_{A,2}, \ldots, P'_{A,t}, P'_{A,t+1}, \ldots, P'_{A,t+n}\}$, which is generated by encoding the classical message m and its hash value $h(m)$ with Alice's sequence $\{P_{A,1}, P_{A,2}, \ldots, P_{A,t}, P_{A,t+1}, \ldots, P_{A,t+n}\}$ and the four unitary operations U_0, U_1, U_2, U_3. The goal of Eve is to obtain the sequence $\{P_{A,1}, P_{A,2}, \ldots, P_{A,t}, P_{A,t+1}, \ldots, P_{A,t+n}\}$ from $\{P'_{A,1}, P'_{A,2}, \ldots, P'_{A,t}, P'_{A,t+1}, \ldots, P'_{A,t+n}\}$. If Eve knows which unitary operation is performed on $P_{A,i}(i=1,2,\ldots,t+n)$, she can perform the same unitary operation on $P'_{A,t}$ and get the original particle $P_{A,i}$.

Note that any pair in the sequence {($P'_{A,1}$, $P_{B,1}$), ($P'_{A,2}$, $P_{B,2}$), …, ($P'_{A,t}$, $P_{B,t}$)} and {($P'_{A,t+1}$, $P_{B,t+1}$), …, ($P'_{A,t+n}$, $P_{B,t+n}$)} is one of the four Bell states, where the particles $P_{B,1}$, $P_{B,2}$, …, $P_{B,t}$, $P_{B,t+1}$, …, $P_{B,t+n}$ are owned by Bob. Eve can get $P'_{A,i}$, but she cannot get the particle $P_{B,\ i}$, for i=0, 1, …, $t+n$. This means that Eve can only perform some measurements on $P'_{A\ ,i}$. The state of any $P'_{A\ ,i}$ is $(|0><0|+|1><1|)/2$. That is, the state of the first qubit of each pair ($P'_{A\ ,t}$, $P_{B,i}$) (i=1, …, $t+n$) is always the same. Then, from any $P'_{A\ ,i}$, Eve can get no information about the unitary operation on $P_{A,i}$ performed by Alice. Then Eve cannot get the original particle $P_{A,\ i}$ from $P'_{A\ ,i}$.

On the other hand, it should be noted that the pair ($P'_{A\ ,i}$, $P_{B,i}$) is one of the four Bell states. Therefore, the measurement on $P'_{A\ ,i}$ performed by Eve will lead to the corresponding change of particle $P_{B,i}$ due to the property of entanglement of Bell states. That is, the measurements on $P'_{A\ ,i}$ performed by Eve will randomly change the classical message m and its hash value $h(m)$ into new m' and h', respectively. This will lead to $h' \neq h(m')$. Then, the measurements performed by Eve will be detected by Bob.

Therefore, the measurements on the sequence {$P'_{A,1}$, $P'_{A,2}$, …,$P'_{A,t}$, $P'_{A,t+1}$, …,$P'_{A,t+n}$} can not help Eve obtain the particles {$P_{A,1}$, $P_{A,2}$, …, $P_{A,t}$, $P_{A,t+1}$, …, $P_{A,t+n}$ }. What is more, the measurements performed by Eve can be detected by Bob. Then, our protocol is secure against measurement attack. On the other hand, our authentication scheme also provides, in some sense, data encryption.

4. Conclusions

In this paper, a new quantum authentication protocol of classical messages is proposed. In this protocol, the message sender and receiver share a sequence of Bell states. The classical message and its corresponding hash value are encoded as a sequence of Bell states by performing four unitary operations. During the verification phase, the hash function is used to check the validity of decoded message from quantum particles. The forgery, tampering and measurement on the transmitted message can be detected by the message receiver. The transmitted message also has the properties of both secrecy and authentication.

Acknowledgements

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, **(2004)** May 2-6; Interlaken, Switzerland, LNCS 3027, pp. 56-73.
[2] C. J. Cha and J. H. Cheon, “An identity-based signature from gap Diffie-Hellman groups”, PKC 2003, **(2003)** January 6-8; Miami, FL, USA, LNCS 2567, pp.18-30.
[3] M. Bellare, R. Canetti, H. Krawczyk, “Keying hash functions for message authentication”, Advances in Cryptology — CRYPTO ’96, **(1996)** August 18–22; Santa Barbara, California, USA, LNCS 1109, pp.1-15.
[4] C. H. Bennett, G. Brassard, S. Breidbart, S. Wiesner, “Quantum cryptography, or unforgeable subway tokens”, Advances in Cryptology — CRYPTO ’82, **(1982)** August 23–25; Santa Barbara, California, USA, 1983, Plenum Press, pp.267-275.
[5] 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, **(1984)** December 10-12; Bangalore, India, pp.175-179.
[6] T. Yan and F. L. Yan, “Quantum key distribution using four-level particles”, Chinese Science Bulletin, vol.56, no.1, **(2011)**, pp.24-28.
[7] A. El Allati, M. El Baz, Y. Hassouni, “Quantum key distribution via tripartite coherent states”, Quantum Information Processing, vol.10, no.5, **(2011)**, pp.589–602.

[8] M. Curty and D. J. Santos, "Quantum authentication of classical messages", Physical Review A, vol.64, no.6, **(2001)**, 062309.
[9] Curty M., Santos D. J., and Pérez E., "Qubit authentication", Physical Review A, vol. 66, no.7, **(2002)**, 022301.
[10] W. M. Shi, Y. H. Zhou, Y. G. Yang, "Quantum deniable authentication protocol", Quantum Information Processing, vol.13, no.7, **(2014)**, pp.1501-1510.
[11] M. Li, "Public-key encryption and authentication of quantum information", Science China: Physics, Mechanics and Astronomy, vol.55, no.9, **(2012)**, pp.1618-1629.
[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. His recent research interests include cryptography and network security.

Xiaolin Hua, she is now a postgraduate in the School of Mathematics and Information Science, Zhengzhou University of Light Industry. Her recent research interests include cryptography and network security.

Jianpo Song, he is now a lecturer in the Department of Computer Science, Xuchang Technology and Economy school. His recent research interests include mathematics education and network security.

Fagen Li, he received his Ph.D. degree in Cryptography from Xidian University, Xi'an, and 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. His recent research interests include cryptography and network security.