Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080641

A Novel Authentication Scheme with Anonymity for Wireless Communications

Liaojun Pang[1,2,*], *Huixian Li*[3], *Xia Zhou*[2] *and Yumin Wang*[1]

[1] State Key Laboratory of Integrated Services Networks, Xidian University, Xian 710071, China
[2] School of Life Science and Technology, Xidian University, Xian 710071, China
[3] School of Computer Science and Engineering, Northwestern Polytechnical University, Xian, 710072, China

Received: 11 Nov. 2013, Revised: 9 Feb. 2014, Accepted: 10 Feb. 2014
Published online: 1 Nov. 2014

Abstract: Aiming at the anonymity problem existing in Zhu *et al*.'s and Lee *et al*.'s schemes, Wu *et al*. proposed an improved scheme. But, Wu *et al*.'s scheme is also proven unable to provide anonymity. Especially, Zeng *et al*. declared that due to an inherent design flaw in Zhu *et al*.'s scheme, Zhu *et al*.'s scheme and its successors are unlikely to provide anonymity. However, in fact, we can use a simple but effective method to solve this anonymity problem. In this paper, based on Wu *et al*.'s scheme, we propose a novel authentication scheme with anonymity for wireless communications. Our method is also suitable for Zhu *et al*.'s and Lee *et al*.'s schemes. Analyses show that the proposed scheme can solve this anonymity problem and is almost as efficient as the exiting one in performance.

Keywords: wireless communication, anonymity, authentication

1 Introduction

Wireless network technology has undergone rapid development in recent years, and with wireless communications, small mobile devices within range of a wireless network can transfer data at any place and any time. In a mobile communication system such as GLOMONET (Global mobility network), through universal roaming technology, mobile users are able to access the network services provided by the home agent in a foreign network. This does facilitate the mobile users, but it also has brought forth the network security issue because wireless communication is broadcast in nature and anyone within range of a wireless device can easily intercept the packets sent out without being perceived [1]. How to authenticate mobile users is an important security issue. It is a big challenge for us to solve this security issue because there are a few things to consider in designing security protocols, such as the low computational power of mobile devices and the low bandwidth and the high channel error rate of wireless networks. Therefore, the security protocols should be designed to minimize the message size, the number of messages exchanged and the computation complexity [2].

Several authentication schemes [2,3,4] have been proposed in recent years for the mobile wireless networks. They can deal with users' roaming among areas administered by different network operators and be implemented by users' devices with limited computing resources. Zhu *et al*. [2] proposed an authentication scheme with anonymity to provide an anonymous authentication service for wireless communications, and Lee *et al*. [3] found some security issues in Zhu *et al*.'s scheme and proposed an improved scheme. Later, Wu *et al*. [4] pointed out that both of these two authentication schemes fail to provide anonymity due to the off-line guessing attack and thus proposed a new scheme. Soon after that, Zeng *et al*. [5], Lee *et al*. [6] and Youn *et al*. [7] pointed out that Wu *et al*.'s scheme still fails to provide anonymity, independently and respectively, but none of them has given an effective solution. Especially, Zeng *et al*. declared that due to an inherent design flaw in Zhu *et al*.'s scheme, Zhu *et al*.'s scheme and its successors are unlikely to provide anonymity. So, researchers tend to use more complex cryptographic methods to achieve the anonymity of mobile users, such as schemes [8,9], which are much less efficient than schemes [2,3,4] and increase the computing overheads of mobile devices largely, and no researchers have tried to solve the anonymity problem existing in these

* Corresponding author e-mail: ljpang@mail.xidian.edu.cn, liaojun.pang@wayne.edu

structure-like schemes in recent three years and it seems to be believed that no solution can be found. However, we find that there does exist such a solution, and it is hasty for Zeng *et al*. to declare their conclusion.

In this paper, we will give a simple but effective method to solve the anonymity problem and take Wu *et al*.'s scheme as an example to introduce our method. A novel authentication scheme is proposed based on Wu *et al*.'s scheme. Our method can also be used in Zhu *et al*.'s and Lee *et al*.'s schemes to solve the same anonymity problem.

Table 1: Notation

Notation	Meaning
PW_A	The password of an entity A
ID_A	The identity of an entity A
T_A	The timestamp generated by an entity A
$Cert_A$	The certificate of an entity A
$(X)_K$	Encrypting a message X with a symmetric Key K
$E_A(X)$	Encrypting a message X with A's public key
$S_A(X)$	Signature on a message X with A's private key
h	A one-way hash function
$\|\|$	Concatenation operation
$\oplus$	Bitwise exclusive-or operation
$A \rightarrow B : M$	An entity A sends a message M to an entity B
MU	The mobile user
HA	The home agent
FA	The foreign agent

2 Review of Wu et al.'s scheme

Wu *et al*.'s scheme is similar to Zhu *et al*.'s and Lee *et al*.'s in structure. In Table 1, we list the notations and abbreviations used in their scheme. Their scheme can be divided into three phases: initial phase, first phase, and second phase. In the initial phase, a new mobile user (MU) registers with the home agent (HA) and HA delivers a password and a smart card for the MU through a secure channel. In the first phase, the foreign agent (FA) authenticates MU and establishes a session key. In the second phase, MU visits FA and FA serves for MU. The details of these three phases can be shown as follows.

A. Initial Phase

When a new MU wants to register with his/her HA, he/she sends his/her identity ID_{MU} to the HA. Upon receiving the registration information from MU, HA computes the MU's password PW_{MU} and a value r as follows:

$$PW_{MU} = h(N||ID_{MU}) \quad (1)$$

$$r = h(N||ID_{HA}) \oplus h(N||ID_{MU}) \oplus ID_{HA} \oplus ID_{MU} \quad (2)$$

where N is a secret value kept by HA. Then, HA sends PW_{MU} and a smart card containing ID_{HA}, r and a one-way hash function h to MU through a secure channel.

B. First Phase

In this phase, FA authenticates MU and issues a temporary certificate $TCert_{MU}$ to MU. The certificate will be used in the second phase when MU always communicates with this FA within this area. The steps of this phase can be shown as follows.

Step 1. $MU \rightarrow FA : n, C, ID_{HA}, T_{MU}$.

MU computes $n = r \oplus PW_{MU}$ and $C = (h(ID_{MU})||x_0||x)_L$, where $L = h(T_{MU} \oplus PW_{MU})$ is his/her temporary key, and x_0 and x are two secret random numbers. The timestamp T_{MU} is used to prevent from the replaying attack.

Step 2. $FA \rightarrow HA : b, n, C, T_{MU}, S_{FA}(h(b, n, C, T_{MU}, Cert_{FA})), Cert_{FA}, T_{FA}$.

Upon receiving messages from MU, FA firstly checks if the timestamp T_{MU} is valid. If it is valid, FA forwards the information received from MU with his/her certificate $Cert_{FA}$, a secret random number b and the corresponding signature $S_{FA}(h(b, n, C, T_{MU}, Cert_{FA}))$ to HA.

Step 3. $HA \rightarrow FA : c, W, S_{HA}(h(b, c, W, Cert_{HA}))), Cert_{HA}, T_{HA}$.

Upon receiving messages from FA, HA firstly checks if FA's certificate $Cert_{FA}$ and the timestamp T_{FA} are valid. If both of them are valid, HA can obtain the real identity of MU by computing $n \oplus h(N||ID_{HA}) \oplus ID_{HA} = ID_{MU}$. Then, compute $L = h(T_{MU} \oplus h(N||ID_{MU}))$ and use it as the decryption key to decrypt C to obtain $h(ID_{MU})$, x_0 and x. HA locally computes $h(ID_{MU})$ and compares it with the one obtained by decryption. If they are equal in value, the MU is a legal user. Next, HA generates a random number c and computes $W = E_{FA}(h(h(N||ID_{MU}))||x_0||x)$ and its signature $S_{HA}(h(b, c, W, Cert_{HA})))$. At last, send these messages with its certificate $Cert_{HA}$ and a timestamp T_{HA} to FA.

Step 4. $FA \rightarrow MU : (TCert_{MU}||h(x_0||x))_k$.

Upon receiving messages from HA, FA firstly checks if HA's certificate $Cert_{HA}$ and the timestamp T_{HA} are valid. If both of them are valid, decrypt W with its private key to obtain $h(h(N||ID_{MU}))$, x_0 and x. Then, the session key between FA and MU is accordingly derived as $k = h(h(h(N||ID_{MU}))||x||x_0) = h(h(PW_{MU})||x||x_0)$. Next, FA issues to MU the temporary certificate $TCert_{MU}$, and computes $(TCert_{MU}||h(x_0||x))_k$ and sends it to MU.

Afterward, MU can compute the session key $k = h(h(PW_{MU})||x||x_0)$ and then decrypt $(TCert_{MU}||h(x_0||x))_k$ to obtain the temporary certificate $TCert_{MU}$ and $h(x_0||x)$. HA locally computes $h(x_0||x)$ and compares it with the one obtained by decryption. If they are equal in value, the authentication succeeds and $TCert_{MU}$ can be accepted.

C. Second Phase

In this phase, MU visits FA at the ith session when he/she is still within this FA. In this case, MU sends the following message to FA.

$MU \rightarrow FA : TCert_{MU}, (x_i||TCert_{MU}||OtherInformation)_{ki}$

MU encrypts $(x_i||TCert_{MU}||OtherInformation)_{ki}$

with the session key k_i of the ith session, where k_i can be derived from the unexpired previous secret knowledge x_{i-1} and a fixed secret x as $k_i = h(h(h(N||ID_{MU}))||x||x_{i-1}) = h(h(PW_{MU})||x||x_{i-1}), i = 1,2,...,n$.

Upon receiving messages from MU, FA firstly checks if MU's certificate $TCert_{HA}$ is valid. If it is valid, FA decrypts $(x_i||TCert_{MU}||OtherInformation)_{ki}$ with k_i. Then, verify the integrity of the message by comparing the two $TCert_{MU}$. If it holds, save x_i for the next communication.

3 Weakness of Wu et al.'s scheme

Wu *et al*. solved the security issue that they have found in Lee *et al*.'s and Zhu *et al*.'s schemes and proposed an improved scheme. But, Zeng *et al*. [5], Lee *et al*. [6] and Youn *et al*. [7] pointed out that Wu *et al*.'s scheme still fails to provide anonymity, independently and respectively: an attacker MN, who has registered as a user of HA, can obtain the identities of other mobile users as long as they registered with the same HA. The detailed attack processes can be shown in Fig. 1. Without losing generality, we assume that MU is a mobile user who has registered with the same HA as MN, and then explain how MN disclose the real identity of MU as follows:

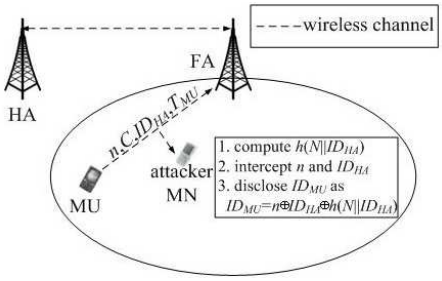

Fig. 1: Attack processes on Wu *et al*.'s scheme.

Because MN is a legal user who has registered with an HA, he/she can derive PW_{MN}, ID_{HA}, r and h from the HA (see Sec. 2-A), where

$$PW_{MN} = h(N||ID_{MN})$$

and

$$r = h(N||ID_{HA}) \oplus h(N||ID_{MN}) \oplus ID_{HA} \oplus ID_{MN}.$$

Then, MN can obtain $h(N||ID_{HA})$ by computing

$$\begin{aligned} & r \oplus PW_{MN} \oplus ID_{HA} \oplus ID_{MN} \\ &= h(N||ID_{HA}) \oplus h(N||ID_{MN}) \oplus ID_{HA} \oplus ID_{MN} \\ &\quad \oplus h(N||ID_{MN}) \oplus ID_{HA} \oplus ID_{MN} \\ &= h(N||ID_{HA}). \end{aligned}$$

When another mobile user MU, who has registered with the same HA, is running the first phase with some FA, MN can easily intercept ID_{HA} and $n = r \oplus PW_{MU} = h(N||ID_{HA}) \oplus ID_{HA} \oplus ID_{MU}$ from the messages of Step 1 because of the broadcast nature of wireless communications [1,2]. Then, MN can obtain the real identity of this MU by computing

$$\begin{aligned} & n \oplus ID_{HA} \oplus h(N||ID_{HA}) \\ &= h(N||ID_{HA}) \oplus ID_{HA} \oplus ID_{MU} \oplus ID_{HA} \oplus h(N||ID_{HA}) \\ &= ID_{MU}. \end{aligned}$$

Through analyses above, we can see that Wu *et al*.'s scheme does fail to achieve the anonymity of mobile users, and that any legal user can recover the real identities of other mobile users who have registered with the same HA. In addition, since Zhu *et al*.'s and Lee *et al*.'s schemes have the same initial phase as Wu *et al*.'s, and in Step 1 of the first phase, the same messages n and ID_{HA} are required to be sent from MU to FA, these two schemes also suffer from the attack mentioned above.

Note that finding this anonymity problem is not our contribution, and this problem is perceived by [5,6,7], independently and respectively. Our contribution is to give a solution to it, and propose an improved scheme based on Wu *et al*.'s scheme.

4 The proposed scheme

In Wu *et al*.'s scheme, it is easy for all MUs, who have registered with some HA, to obtain the same value $h(N||ID_{HA})$ according to (1) and (2), which enables an attacker, who has registered with some HA, to easily disclose the real identities of other mobile users who have registered with the same HA (see Sec. 3). Therefore, to avoid the anonymity problem, the value $h(N||ID_{HA})$ should be modified in a way to make it changeable for different mobile users. The proposed scheme is shown as follows.

A. Initial Phase

This phase is similar to the one in Wu *et al*.'s scheme except for the computation of the value r. When a new MU wants to register with his/her HA, he/she sends his/her identity ID_{MU} to the HA. Upon receiving the registration information from MU, HA computes the MU's password PW_{MU} and a value r as follows:

$$PW_{MU} = h(N||ID_{MU}) \tag{3}$$

$$r = h(N||ID_{HA}||h(PW_{MU})) \oplus PW_{MU} \oplus ID_{HA} \oplus ID_{MU} \tag{4}$$

where N is a secret value kept by HA. Then, HA sends PW_{MU} and a smart card containing ID_{HA}, r and h to MU through a secure channel.

B. First Phase

The steps of this phase can be shown as follows.

Step 1. $MU \rightarrow FA : n, V, C, ID_{HA}, T_{MU}$.

MU computes $n = r \oplus PW_{MU}$, $V = h(PW_{MU})$ and $C = (x_0||x)L$, where $L = h(T_{MU} \oplus PW_{MU})$ is his/her temporary key, x_0 and x are two secret random numbers, and T_{MU} is the timestamp.

Step 2. $FA \rightarrow HA : b, n, V, C, T_{MU}, S_{FA}(h(b, n, V, C, T_{MU}, Cert_{FA})), Cert_{FA}, T_{FA}$.

Upon receiving messages from MU, FA firstly checks if the timestamp T_{MU} is valid. If it is valid, FA forwards the information received from MU with his/her certificate $Cert_{FA}$, a secret random number b and the corresponding signature $S_{FA}(h(b, n, V, C, T_{MU}, Cert_{FA}))$ to HA.

Step 3. $HA \rightarrow FA : c, W, S_{HA}(h(b, c, W, Cert_{HA}))), Cert_{HA}, T_{HA}$.

Upon receiving messages from FA, HA firstly checks if FA's certificate $Cert_{FA}$ and the timestamp T_{FA} are valid. If both of them are valid, HA can obtain the real identity of MU by computing $h(N||ID_{HA}||V) \oplus ID_{HA} \oplus n = ID_{MU}$. HA locally computes $PW_{MU} = h(N||ID_{MU})$ and $V = h(PW_{MU})$, and compares the computed V with the one received from FA. If they are equal in value, MU is a legal user. Then, compute $L = h(T_{MU} \oplus PW_{MU})$ where PW_{MU} is computed locally and then use it as the decryption key to decrypt C to obtain x_0 and x. Next, HA generates a random number c and computes $W = E_{FA}(x_0||x)$ and its signature $S_{HA}(h(b, c, W, Cert_{HA})))$. At last, send these messages with its certificate $Cert_{HA}$ and a timestamp T_{HA} to FA.

Step 4. $FA \rightarrow MU : (TCert_{MU}||h(x_0||x))_k$.

Upon receiving messages from HA, FA firstly checks if HA's certificate $Cert_{HA}$ and the timestamp T_{HA} are valid. If both of them are valid, FA decrypts W with its private key to obtain x_0 and x. Then, the session key between FA and MU is accordingly derived as $k = h(V||x||x_0) = h(h(PW_{MU})||x||x_0)$. Next, FA issues to MU the temporary certificate $TCert_{MU}$, and computes $(TCert_{MU}||h(x_0||x))_k$ and sends it to MU.

Afterward, MU can compute the session key $k = h(V||x||x_0)$ and then decrypt $(TCert_{MU}||h(x_0||x))_k$ to obtain the temporary certificate $TCert_{MU}$ and $h(x_0||x)$. The value $h(x_0||x)$ can be used to check the validity of the received messages.

C. Second Phase

This phase is similar to the old one except for the computation of the session key k_i. When MU visits FA at the ith session when he/she is still within this FA, he/she sends the following message to FA.

$MU \rightarrow FA : TCert_{MU}, (x_i||TCert_{MU}||OtherInformation)_{ki}$

MU encrypts $(x_i||TCert_{MU}||OtherInformation)_{ki}$ with the session key k_i of the ith session, where k_i can be derived from the unexpired previous secret knowledge x_{i-1} and a fixed secret x as $k_i = h(V||x||x_{i-1}) = h(h(PW_{MU})||x||x_{i-1}), i = 1, 2, ..., n$.

Upon receiving messages from MU, FA firstly checks if MU's certificate $TCert_{HA}$ is valid. If it is valid, FA decrypts $(x_i||TCert_{MU}||OtherInformation)_{ki}$ with k_i. Then, verify the integrity of the message by comparing the two $TCert_{MU}$. If it holds, save x_i for the next communication.

5 Analyses and discussions

A. Security Analysis

Though it is simple, our method can solve the anonymity problem mentioned above. Now, we shall describe how the proposed scheme prevents the above attacker from disclosing the identities of other mobile users.

This anonymity problem existing in the existing schemes [2,3,4] is due to the fact that each legal mobile user can obtain the same value $h(N||ID_{HA})$ with the information received from HA during the initial phase (see Sec. 3). However, in our scheme, we set $r = h(N||ID_{HA}||h(PW_{MU})) \oplus PW_{MU} \oplus ID_{HA} \oplus ID_{MU}$, that is to say, $h(N||ID_{HA})$ is replaced by $h(N||ID_{HA}||h(PW_{MU}))$ where PW_{MU} is MU's password and kept secret to others by MU. So, by the attack mentioned above, each legal mobile user can obtain only a person-specific value $h(N||ID_{HA}||h(PW_{MU}))$ that is different for different mobile users and is useless for legal mobile users in recovering the identities of other mobile users. Therefore, the attack mentioned above is prevented and the adversary mentioned in Sec. 3 is unable to perceive the identity of any mobile user. Although the value $V = h(PW_{MU})$ has to be transmitted in plaintext, PW_{MU} remains secure according to the security of the hash function.

Also, because our scheme is based on Wu *et al*.'s scheme and the computation of the session key between MU and FA is similar to that of Wu *et al*.'s scheme in security considerations, our scheme can achieve the backward secrecy like Wu *et al*.'s scheme. At the same time, this method can be used in Zhu *et al*.'s and Lee *et al*.'s schemes to solve their anonymity problem.

B. Performance Analysis

The advantage of these three structure-like schemes [2,3,4] lies in their high computation performance, which makes them practical especially for mobile devices with limited computing resources. Here, we shall briefly discuss the performance of the proposed scheme in terms of the message size, the number of messages exchanged and the computation complexity by comparing with Wu *et al*.'s scheme. In the initial phase, one more hash computation, $h(PW_{MU})$, is needed for HA, and the message size and the number of message sent from HA to MU is kept unchanged. In the first phase, MU is required to compute $V = h(PW_{MU})$ and the number of messages transmitted by MU is added by 1 because V should be transmitted to FA. But, in this case, the total message size transmitted by MU is kept unchanged because in our scheme the ciphertext of $h(ID_{MU})$ is not needed to be transmitted (see Step 1 of Sec. 5). By this means, we can conclude that the total message size between FA and HA is not raised. Table 2 and Table 3 show the comparison of

Table 2: COMPARISON OF THE MESSAGE SIZE

Schemes	$MU \oplus FA$	$FA \oplus HA$	$HA \oplus FA$	$FA \oplus MU$
Wu *et al*.'s[4]	$5l_0+1l_1$	$5l_0+2l_1+1l_2+1l_3$	$4l_0+1l_1+1l_2+1l_3$	$1l_0+1l_3$
Ours	$5l_0+1l_1$	$5l_0+2l_1+1l_2+1l_3$	$3l_0+1l_1+1l_2+1l_3$	$1l_0+1l_3$

l_1: the length of timestamps; l_2: the length of signatures; l_3: the length of certificates; l_0: the length of other data.

Table 3: COMPARISON OF THE COMPUTATION COMPLEXITY

Schemes	MU	FA	HA
Wu *et al*.'s[4]	$2E+5H+2\oplus$	$2S+1P+1E+3H$	$2S+1P+1E+8H+6\oplus$
Ours	$2E+4H+2\oplus$	$2S+1P+1E+3H$	$2S+1P+1E+8H+5\oplus$

S: signature or its verification; P: public-key encryption or decryption; E: symmetric encryption or decryption.

our scheme with Wu *et al*.'s scheme in terms of the message size and the computation complexity, respectively.

From Table 2 and Table 3, it is easy to see that our scheme is almost as efficient as Wu *et al*.'s scheme in performance, and it is also suitable for low-performance and cheap mobile devices with limited computing resources. The computing overhead of mobile devices is much less than that of schemes [8,9], which makes our scheme more attracting for practical applications.

6 Conclusion

Due to the low computational power of mobile devices and the low bandwidth and the high channel error rate of wireless networks, the traditional security protocols are useless for wireless networks and the protocol designer must try to minimize the message size, the number of messages exchanged and the computation complexity when designing a security protocol for wireless networks. Based on some simple operations, several anonymous authentication schemes have been proposed for the mobile wireless networks. Unfortunately, it has been proven that none of them can achieve the anonymity as they exclaimed. Especially, Zeng *et al*. declared that due to an inherent design flaw in these schemes, it is unlikely for any scheme based on the simple operations to provide anonymity, and more complex cryptographic methods should be used to achieve the anonymity of mobile users. However, we find that Zeng *et al*.'s conclusion is not true and there is still some simple method to solve the anonymity problem. So, in this paper, aiming at the anonymity problem existing in Wu *et al*.'s scheme, we propose an effective remedy and give an improved scheme based on Wu *et al*.'s. Analyses show that our scheme can achieve the anonymity and is as effective as Wu *et al*.'s scheme. Our method can also be applicable to other schemes such as Zhu *et al*.'s and Lee *et al*.'s because they have the similar structure. That is to say, Zeng *et al*.'s conclusion that the schemes structurally similar to Wu *et al*.'s are unlikely to provide anonymity is hasty, and the anonymity problem can be solved in a very simple way. Our scheme can be used in the mobile communication systems such as GLOMONET to achieve the security of communication and the anonymity of the user during roaming.

Acknowledgement

National Natural Science Foundation of China under grant numbers 61103178 and 60803151; Basic Science Research Fund in Xidian University under grant number K5051310006.

References

[1] L. J. Pang, H. X. Li, and Q. Q. Pei, IET Communications, **6**, 1126-1130 (2012).
[2] J. Zhu and J. Ma, IEEE Trans. Consumer Electron., **50**, 230-234 (2004).
[3] C. C. Lee, M. S. Hwang, and I. E. Liao, IEEE Trans. Industrial Electron., **53**, 1683-1687 (2006).
[4] C. C. Wu, W. B. Lee, and W. J. Tsaur, IEEE Commun. Lett., **12**, 722-723 (2008).
[5] P. Zeng, Z. F. Cao, K. R. Choo, and S. B. Wang, IEEE Commun. Lett., **13**, 170-171 (2009).
[6] J. S. Lee, J. H. Chang, and D. H. Lee, IEEE Commun. Lett., **13**, 292-293 (2008).
[7] T. Y. Youn, Y. H. Park, and J. Lim, IEEE Commun. Lett., **13**, 471-473 (2009).
[8] D. He, J. Bu, S. Chan, and C. Chen, IEEE Trans. Wireless Commun., **11**, 48-53 (2012).
[9] J. L. Tsai, N. W. Lo, and T.C Wu, IEEE Commun. Lett., **16**, 1100-1102 (2012).

Liaojun Pang received his Bachelor degree and Master degree in Computer Science and Technology from Xidian University of China, in 2000 and 2003, respectively. In 2006, he received the Ph.D degree in Cryptography from Xidian University of China. Now, he is a researcher with State Key Laboratory of Integrated Services Networks of Xidian University, and at the same time he is a professor with the School of Life Science and Technology of Xidian University. He was a visiting scholar at the Department of Computer Science at Wayne State University of USA from 2012 to 2013. His research interests include Internet security, cryptography, secure mobile agent system and e-commerce security technology. He became a Member (M) of IEEE in 2009.

Huixian Li received the Ph.D Degree in Cryptography from Dalian University of Technology. Now, she is an associate professor in the School of Computer Science and Engineering at the Northwestern Polytechnical University, and at the same time she is a visiting scholar at the Department of Computer Science at Wayne State University of USA. Her research interests include information security, cryptography, and security technologies for mobile health care systems.

Xia Zhou is a postgraduate student with School of Life Science and Technology, Xidian University of China. Her research interests include cryptography and information security.

Yumin Wang is a professor with the State Key Lab. of Integrated Service Networks, Xidian University of China. His research interests include cryptography, coding, and information theory. He is a Senior Member of IEEE.