A Secure Dynamic Conference Scheme with Anonymity for Mobile Communications

Shin-Jia, Hwang and Ming-Jhang, Cai
Department of Computer Science and Information Engineering,
TamKang University, Tamsui, Taipei Hsien, 251, Taiwan, R.O.C.
E-mail: sjhwang@mail.tku.edu.tw, 696420677@s96.tku.edu.tw

Abstract*-To allow many users to hold a secure video teleconference in mobile communications, a conference key distribution scheme with dynamic participations is necessary. In the proposed dynamic conference key distribution schemes, the conference keys do not satisfy the forward or backward secrecy. So these proposed schemes are vulnerable by active colluding attacks. To remove this disadvantage, our new dynamic conference distribution scheme with forward and backward secrecy among different validity periods is proposed. Due to the consideration of limited computing ability and electronic power, the conference key renewal is performed periodically. Moreover, our scheme also satisfies anonymity to protect the conferees' privacy.*

Keywords: Conference key distribution, mobile communications, cryptography

1. Introduction

Over the past few years, the popularity of personal communication systems (PCS for short) is growing rapidly around the world. Plenty of applications and services for PCSs are brought up recently, such as mobile commerce applications and teleconference applications. In the wireless mobile network (WMN for short), wireless communications allow people to communicate quickly and conveniently at anytime and anywhere. So the wireless communication becomes one of the principal mediums for transmitting information.

However, wireless communications are vulnerable to interceptions. The interceptions may be fraudulent call attempts and intrusion, or eavesdropping by third parties. In general, there are three main threats in mobile communications [11, 12].

1) *Eavesdropping*: Eavesdroppers find out mobile users' identities or their conversation content by intercepting transmitting messages.
2) *Impersonation*: An attack disguises a legitimate mobile user on a mobile network. To the mobile communications, this attack is a possible threat because the cloning of smart cards holding mobile users' information is possible.
3) *Tracking*: An adversary traces an individual mobile user's location.

To guard against these three threats, four basic security objectives should be satisfied by the schemes for the mobile communications [4].

1) Privacy protection of conversation contents transmitted among the conferences.
2) Privacy protection of information about conferees' locations during the conference.
3) Fraud prevention by authenticating portable units.
4) Replaying-attack prevention.

A practical scheme for mobile communications should adopt operations with low-computational costs since portable units have to operate over long periods of time by using low-power batteries. Therefore the cryptographic functions with low-computational costs are suitable to design schemes for mobile communications. Symmetric cryptosystems meet the criteria that computational cost is low [6]. But symmetric cryptosystems needs the help of secure session key agreement protocols between the sender and receiver.

In recent years, many authentication schemes and key distribution protocols between two users for wireless networks have been proposed [5, 8, 9, 13]. But these schemes do not suit the conference distribution scheme among more than two users. Hwang and Yang [4] first proposed their conference key distribution schemes which enable two or more users to share a secure conference key in 1995. Hwang [3] modified the conference key distribution scheme to resolve the dynamical problem that a user is able to join or quit a teleconference already in progress in 1999. Ng [7] pointed out the weakness of Hwang's dynamic conference key distribution scheme, and gave some modification comments. In 2003, Hwang and Chang [2] proposed their efficient

dynamic conference key distribution scheme by utilizing the self-encryption cryptographic function. Hwang and Chang's scheme exploits only a symmetric key cryptosystem rather than the public key cryptosystem. Bao's analysis [1] shows that Hwang's [3] and Hwang and Chang's [2] schemes are insecure against actively colluding attacks and passive attacks. In 2007, Wang et al. presented a simple authentication and dynamic conference key distribution scheme [10] achieving conferees' anonymity. However, Wang et al.'s scheme is also insecure against the active colluding attack in [1].

A dynamic conference key distribution scheme with batch conference key renewal mechanism is proposed for mobile communications. Our scheme allows multi-user to hold a secure conference. The security of our scheme that not only satisfies the four basic security objectives, but also satisfies security objectives: Anonymity, and forward and backward secrecy among conference keys for different validity periods. Our scheme is also secure against the active colluding attack and passive attack [1]. In our batch conference key renewing scheme, users are allowed to join or quit a conference and the network center has the ability to securely renew the conference keys periodically.

The next section gives the description of our scheme which includes the conference initialization scheme and batch conference key renewing scheme. In Section 3, the security analysis of our scheme is given. Then, in the same section, the comparison between Wang et al.'s and our schemes is given. Finally, the last section is our conclusions.

2. Our Scheme

Our scheme is consists of three phases: Setup phase, conference initialization phase, and conferee dynamic phase. In our scheme, there are two kinds of basic members: A trusted network center (NC for short) and users. The NC is a trusted central authority that is responsible for key generation and key distribution. Each legal user has to share a long-term private key with NC in advance. In the following, three phases are described, respectively.

Setup Phase

NC announces two public one-way hash functions $H_k()$ and $H()$ for all users, where k is the secret used for the $H_k()$. NC has to publish or adopt symmetric encryption function $E_k()$ and symmetric decryption functions $D_k()$, where k is the symmetric secret key. Each user U_i has a unique identity ID_i, and shares a unique secret key K_i with NC in advance. The notations used in our scheme are summarized in the following.

Notations

ID_i: The identity of user U_i.
ID_{NC} : The identity of the network center NC.
ID_{CK} : The identity of conference key CK.
t_i : The timestamp chosen by user U_i.
T : The timestamp chosen by network center.
K_i: The long-term private key share by U_i and NC.
k_i : The session key share by U_i and NC.
C-list : The list containing legal conferees.
lcm : Least common multiple
$E_k()$: Symmetric encryption function with the secret key k.
$D_k()$: Symmetric decryption function with the secret key k.
$H_k()$: A one-way hash function with the secret key k.
$H()$: A one-way hash function.

Some assumptions are used in our scheme. These assumptions are stated below. In our scheme, a secure session key agreement protocol with mutual authentication is assumed to exist between a user U_i and NC to generate a session key k_i. Due to the security consideration, assume that each user has to perform the secure session key agreement protocol with mutual authentication before applying the NC's services. The communication between NC and users are assumed to be busy.

Conference Initialization Phase

Without loss of generality, suppose that one user U_1 wants to construct a conference key with the other m-1 conferees, U_2, U_3, …, and U_m. First of all, U_1 has to share a session key k_1 with NC by running the secure session key agreement protocol, and mutually authenticates one another at the same time. After NC knows the identity of U_1, the conference initialization scheme is used to construct the conference key for the m users.

Conference Initialization Scheme

Step 1: U_1 generates a timestamp t_1, and computes $C_1 = E_{k1}(t_1, ID_i)$.
Step 2: U_1 sends C_1 to NC.
Step 3: NC decrypts C_1, and checks the freshness of the timestamp t_1 and format of the identity ID_i. If the timestamp t_1 is not fresh or the format of the decrypted identity ID_i is illegal, then stop.

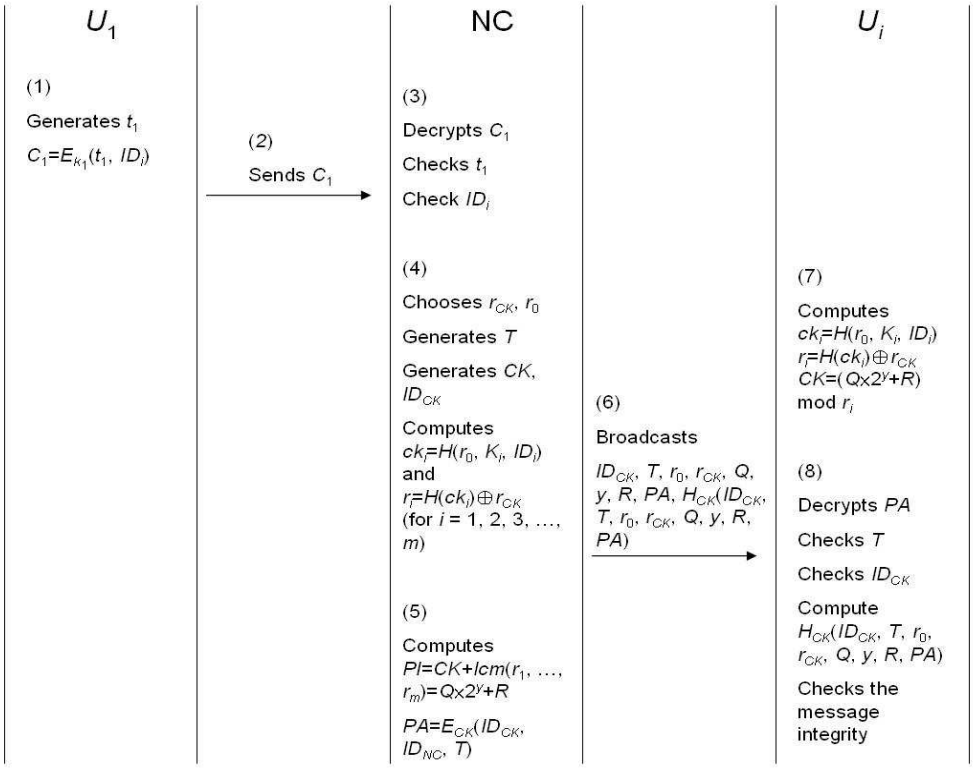

Fig. 1: Conference Initialization Scheme

Step 4: NC chooses two random numbers r_{CK}, and r_0, and generates a timestamp T, and a new conference key CK with the corresponding unique conference key identity ID_{CK}. Then NC computes $ck_i= H(r_0, K_i, ID_i)$ and $r_i= H(ck_i)\oplus r_{CK}$ for i= 1, 2, 3, …, and m.

Step 5: NC computes the public information $PI= CK+ lcm(r_1, r_2, …, r_m)$, finds Q, y, and R such that $PI= Q\times 2^y+R$, and $PA= E_{CK}(ID_{CK}, ID_{NC}, T)$, where y is a predetermined bit-length parameter for the decomposition of PI. NC keeps the secret record $\{ID_{CK}, CK, r_0, r_{CK}, C\text{-}list\}$. Here *C-list* is the list containing legal conferees. The initial value of *C-list* is $\{ID_1, ID_2, …, ID_m\}$.

Step 6: NC broadcasts ID_{CK}, T, r_0, r_{CK}, Q, y, R, PA, and $H_{CK}(ID_{CK}, T, r_0, r_{CK}, Q, y, R, PA)$ after waiting for a time period whose length is random determined by NC.

Step 7: Each user U_i computes $ck_i= H(r_0, K_i, ID_i)$, $r_i= H(ck_i)\oplus r_{CK}$, and $CK= (Q\times 2^y+R) \bmod r_i = PI \bmod r_i = (CK+lcm(r_1, r_2, …, r_m)) \bmod r_i$.

Step 8: Each user U_i decrypts PA to obtain ID_{CK}, ID_{NC}, and T. Then each user checks the freshness of timestamp T. If the timestamp T is validity, U_i checks whether or not the decrypted ID_{CK} and the received ID_{CK} are equal. If they are equal, the user U_i is the conferee; otherwise, the user U_i is not. Finally, each user U_i checks the message integrity by recomputed the hash value of $H_{CK}(ID_{CK}, T, r_0, r_{CK}, Q, y, R, PA)$. If the recomputed hash value is equal to the received $H_{CK}(ID_{CK}, T, r_0, r_{CK}, Q, y, R, PA)$, the user U_i enters the conference with the initial conference key CK; otherwise stop.

Figure 1 illustrates the conference initialization scheme.

Conferee Dynamic Phase

To the same conference, some conferees may leaves while some other users want to join the conference. To deal with the leave or join of the same conference, NC has to renew the conference key each time for the forward and backward secrecy of the conference keys. However, this

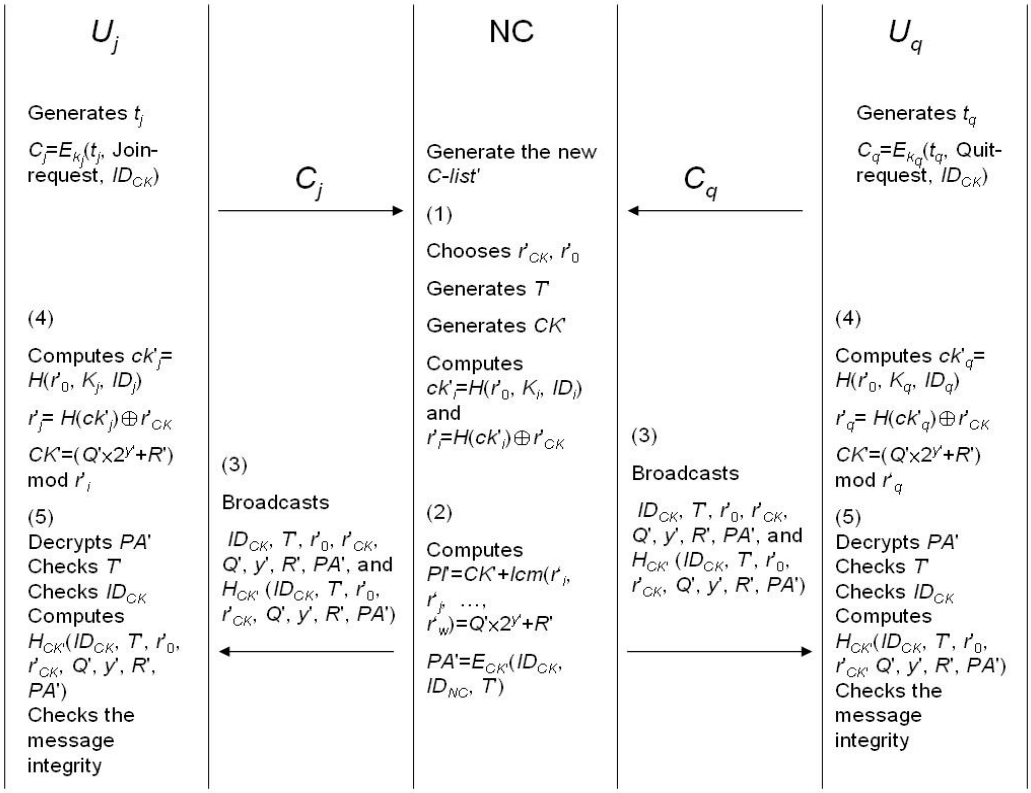

Fig. 2: Batch Conference Key Renewing Scheme

load to renew the conference key for each leave or joint is heavy. Under the efficiency consideration, NC may renew the conference keys periodically to reduce the renew load in our scheme. But the forward and backward secrecy of the conference keys become partial. Therefore a batch key renewal scheme is described.

Before the renew point of the conference key, each conferee who wants to leave the conference with ID_{CK} sends the quit-request while each user who wants to join the conference with ID_{CK} sends the joint-request. After collecting these joint-requests and quit-request, NC broadcasts the renew message to renew the conference key and the conferee list at the renew point.

The batch conference key renewing scheme is described by the joining procedure, quitting procedure, and the renewing scheme.

Joining procedure: Suppose that a user U_j wants to join the conference with the identity ID_{CK}. The user U_j first shares a session key k_j with NC by using the secure session key agreement protocol with mutual authentication. Then U_j generates a timestamp t_j, and computes $C_j= E_{kj}(t_j$, Join-request, $ID_{CK})$. Afterward, U_j sends C_j to network center NC.

Quitting procedure: Suppose that a conferee U_q wants to leave the conference with ID_{CK}. The conferee U_q first generates a timestamp t_q and shares a session key k_q with NC. Then U_q computes $C_q= E_{kq}(t_q$, Quit-request, $ID_{CK})$, and sends C_q to NC.

Renewing Scheme

NC generates the new conferee list *C-list'* for the conference with identity ID_{CK}. At the renewing point, NC renews the conference key by the following steps.

Step 1: NC chooses two random numbers r'_{CK} and r'_0, and generates a timestamp T' and a new conference key CK'. Then NC computes $ck'_i= H(r'_0, K_i, ID_i)$ and $r'_i = H(ck'_i)\oplus r'_{CK}$ for all legal conferee U_i belonging to *C-List'*.

Step 2: NC computes the public information $PI' = CK' + lcm(r'_i, r'_j,\ldots, r'_w) =Q'\times 2^{y'}+ R'$ and $PA'= E_{CK'}(ID_{CK}, ID_{NC}, T')$, where r'_i is the computed value for the conferee U_i in *C-list'* . NC keeps the new record $\{ID_{CK}$,

CK', r'_0, r'_{CK}, $C\text{-}list'$}.

Step 3: NC broadcasts ID_{CK}, T', r'_0, r'_{CK}, Q', y', R', PA', and $H_{CK'}(ID_{CK}, T', r'_0, r'_{CK}, Q', y', R', PA')$.

Step 4: Each user U_L in $C\text{-}list'$ computes $ck'_L = H(r'_0, K_L, ID_L)$, $r'_L = H(ck'_L) \oplus r'_{CK}$, and $CK' = (Q' \times 2^{y'} + R') \bmod r'_L = PI' \bmod r'_L = (CK' + lcm(r'_i, r'_j, \ldots, r'_w)) \bmod r'_L$.

Step 5: Each user U_L in $C\text{-}list'$ decrypts PA' to obtain ID_{CK}, ID_{NC}, and T'. Then each user U_L in $C\text{-}list'$ checks the freshness of timestamp T'. If T' is fresh, U_i checks whether or not the decrypted ID_{CK} is the same as the received ID_{CK}. If they are the same, the user U_L is confirmed that he/she is the conferee; otherwise, U_L is not. Finally, each user U_L checks the message integrity by recomputed the hash value of $H_{CK'}(ID_{CK}, T', r'_0, r'_{CK}, Q', y', R', PA')$. If the recomputed hash value is equal to the received $H_{CK'}(ID_{CK}, T', r'_0, r'_{CK}, Q', y', R', PA')$, U_L enters the conference with the renewed conference key CK'; otherwise he/she stops.

The batch conference key renewing scheme is illustrated by Fig. 2

3. Security Analysis and Discussions

The security analysis of our scheme is first given. Our scheme that not only satisfies the four basic security objectives, but also satisfies security objectives which includes anonymity, partial forward secrecy, and partial backward secrecy.

Table 1: Security Comparison between Wang et al.'s and Our Schemes

Security Property	Wang et al's[10]	Our Scheme
Privacy of conversation	YES	YES
Privacy of locations	YES	YES
Prevention of fraud	YES	YES
Prevention of replaying attacks	YES	YES
Anonymity	YES	YES
Forward security	NO	YES
Backward security	YES	YES
Key renewal ability	YES	YES
Integrity	YES	YES
Secure dynamic ability	NO	YES

The security of K_i's is first considered. In our scheme, only the $ck_i = H(r_0, K_i, ID_i)$ is computed by using K_i. However, K_i is protected by the one-way hash functions, so $ck_i = H(r_0, K_i, ID_i)$ does not release the value of K_i. Therefore, the security of K_i's is guaranteed by the one-way hash function in our scheme.

Consider the security of the conference key. The security of the CK in its period of validity is discussed first. Only the public information $PI = CK + lcm(r_1, r_2, \ldots, r_m)$ contains of the value of CK. To obtain CK from PI, the secret value r_i must be used. Since $r_i = H(ck_i) \oplus r_{CK} = H(H(r_0, K_i, ID_i)) \oplus r_{CK}$, r_i is computed only by the user who holds the long-term private key K_i. Since K_i is secure, r_i and CK is secure in CK's validity period. Moreover, only the legal conferees can obtain the conference key CK, our scheme satisfies the 3rd property.

The security analysis of our dynamic conference keys in different validity periods for the same conference is considered below. The conference keys in different validity periods are chosen randomly and independently, so one conference key releases no information about the other conference keys. To obtain the conference keys, attackers may use one secret value r_i's to obtain the other r_j's, where $j \neq i$. Since $r_i = H(ck_i) \oplus r_{CK} = H(H(r_0, K_i, ID_i)) \oplus r_{CK}$, the randomness of r_i is determined by the randomness of H, r_{CK}, and r_0. Since a secure one-way hash function can be used as a pseudo random number generator, assume the randomness of H is almost the same as a secure pseudo random generator. Because r_{CK}, and r_0 are chosen randomly, the value of r_i is also random and independent of the other r_j's, where $j \neq i$. Similarly, the value of r_i is also random and independent of the other r'_j's. No one can use some known value of r_i to derive the values of r_j's or r'_j's. Since the secret values of r_j's are renew for different validity periods, the PI release no information about another PI'. Therefore, the conference keys in our scheme satisfy the forward and backward security among different validity periods.

The conversation privacy is protected in our scheme. The conversation content is protected by a symmetric cryptosystem in our scheme. The conference keys are secure according to the above analysis. Therefore, the privacy of conversation content is provided by the secure symmetric cryptosystem.

To resist replaying attacks, timestamps are used in the communication among NC and users. The received message is accepted only when the attached timestamp is fresh. Thus, our scheme is secure against the replaying attack.

Our scheme satisfies anonymity. In our scheme, the trusted NC knows the members of the conference while the other users cannot. NC broadcasts any public information for all legal users who may or may not conferees. Since the broadcasting information contains no information about conferees, the public information cannot be

used to find out the members of the conference.

There are three special cases in our scheme may release the initial conferees, the leaving conferees, and the joining conferees. To initial a conference, the initial conferee has to perform the session key agreement protocol with mutual authentication in advance. The session key agreement protocol with mutual authentication may release the identity of the initial conferee. Due to our assumption that each user has to perform the protocol before applying the NC's services, the adversary only doubt the initial conferee wants to initial a conference. After waiting a time period with a randomly chosen length, the initial conferee's identity is hidden among the other users who also perform the session key agreement protocol with NC. The initial conferee's identity is protected. Similarly, the identities of leaving and joining conferees are protected by the similar way. Therefore, our scheme satisfies anonymity property.

4. Conclusions

A dynamic conference key distribution scheme with batch conference key renewal mechanism is proposed for mobile communications. Our scheme satisfies not only the basic security objectives [4], but also anonymity, forward and backward secrecy among different validity periods. To deal with the dynamic participation, our batch conference key renewing scheme allows users (conferees) to join (leave) a conference with the help of NC. Since the NC periodically renews the conference key randomly and independently, our dynamic scheme satisfies the forward and backward secrecy among different validity periods. Due to the forward and backward secrecy, our scheme is secure against the active colluding attack and passive attack [1].

References

[1] F. Bao, "Analysis of a Secure Conference Scheme for Mobile Communication," *IEEE Transactions on Wireless Communications*, Vol. 5, No. 8, pp. 1984-1986, August 2006.

[2] K. F. Hwang and C. C. Chang, "A Self-encryption Mechanism for Authentication of Roaming and Teleconference Services," *IEEE Transactions on Wireless Communications*, Vol. 2, No. 2, pp. 400-407, March 2003.

[3] M. S. Hwang, "Dynamic Participation in a Secure Conference Scheme for Mobile Communications," *IEEE Transactions on Vehicular Technology*, Vol. 48, No. 5, pp. 1469-1474, September 1999.

[4] M. S. Hwang and W. P. Yang, "Conference Key Distribution Schemes for Secure Digital Mobile Communications," *IEEE Journal on Selected Areas in Communications*, Vol. 13, No.2, pp. 416-425, February 1995.

[5] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual Authentication and Key Exchange Protocols for Roaming Services in Wireless Mobile Networks," *IEEE Transactions on Wireless Communications*, Vol. 5, No. 9, pp. 2569-2577, September 2006.

[6] D. L. Mills, "Precision Synchronization of Computer Network Clocks," A*CM SIGCOMM Computer Communication Review*, Vol. 24, pp. 28-43, 1994.

[7] S. L. Ng, "Comments on Dynamic Participation in a Secure Conference Scheme for Mobile Communications," *IEEE Transactions on Vehicular Technology*, Vol. 50, pp. 334-335, January 2001.

[8] M. Shi, X. Shen, and J. W. Mark, "A Light Weight Authentication Scheme for Mobile Wireless Internet Applications," *Wireless Communications and Networking*, Vol. 3, pp. 2126-2131, March 2003.

[9] C. Tang and D. O. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks," *IEEE Transactions on Wireless Communication*, Vol. 7, No. 4, pp. 1408-1416, April 2008.

[10] J. Wang, N. Jiang, H. Li, X. Niu, and Y. Yang, "A Simple Authentication and Key Distribution Protocol in Wireless Mobile Networks," *Wireless Communications, Networking and Mobile Computing*, pp. 2282-2285, September 2007.

[11] X. Yi, C. K. Siew, and C. H. Tan, "A Secure and Efficient Conference Scheme for Mobile Communications," *IEEE Transactions on Vehicular Technology*, Vol. 52, No. 4, pp. 784-793, July 2003.

[12] X. Yi, C. K. Siew, C. H. Tan, and Y. Ye, "A Secure Conference Scheme for Mobile Communications," *IEEE Transactions on Wireless Communications*, Vol. 2, No. 6, pp. 1168-1177, November 2003.

[13] J. Zhu and J. Ma, "A New Authentication Scheme with Anonymity for Wireless Environments," *IEEE Transactions on Consumer Electronics*, Vol. 50, pp. 231-235, February 2004.