User-Anonymous and Short-Term Conference Key Distribution System via Link-Layer Routing in Mobile Communications

Ting-Yi Chang

Graduate Institute of e-Learning,
National Changhua University of Education,
No.1, Jin-De Road, Changhua City, Taiwan, R.O.C.
E-mail: tychang@cc.ncue.edu.tw

Min-Shiang Hwang*

Department of Management Information Systems,
National Chung Hsing University,
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
E-mail: mshwang@nchu.edu.tw
*Corresponding author

Abstract: There are occasions when some people carry their portable devices to a hotel room or office to hold a short-term conference over wireless networks. This paper designs a user-anonymous and short-term conference key distribution system to ensure secure communications over an open channel and to protect the identities of the users. Further, linker-layer routing between the mobile hosts makes it possible for mobile hosts to directly communicate with one another. Under the random oracle model and the elliptic curve version of the computational Diffie-Hellman assumption, the proposed system is demonstrated to be provably secure against active adversaries. Compared to previously proposed systems, the proposed system is efficient in terms of communication and computational complexity, and is suitable for low-power mobile devices.

Keywords: Conference key distribution system; computational Diffie-Hellman problems; elliptic curve discrete logarithm problem; mobile IP; one-way hash function.

Reference to this paper should be made as follows: Chang, T. Y. and Hwang, M. S. (xxxx) 'User-Anonymous and Short-Term Conference Key Distribution System via Link-Layer Routing in Mobile Communication', *Int. J. Mobile Communications*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: T. Y. Chang received his M.S. from the Graduate Institute of Computer Science and Information Engineering at Chaoyang University of Technology, and his Ph.D in the Department of Computer Science at National Chiao Tung University, Taiwan. Currently, he is an Associate Professor with the Graduate Institute of e-Learning, National Changhua University, Taiwan. His

current research interests include e-Learning, information security, cryptography, and mobile communications.

M. S. Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published over 100 articles on the above research fields in international journals.

1 Introduction

Wireless communication has become more and more convenient and popular in recent years. Convenient connection of portable devices to the Internet and communication with people all over the world is possible using mobile network layer protocols (Juang and Wu, 2009; Kim *et al.*, 2004; Massoud and Gupta, 2003; Mylonakis, 2004; Tan *et al.*, 2003). Unlike a traditional wired network, a wireless network can be easily accessed, and it is more difficult to tell which host is communicating with others in a wireless network than in a wired network. Cyber attackers have found wireless networks relatively easy to break into, and even use wireless technology to break into wired networks. Liu *et al.*'s study (2010) explored some factors affecting individuals' use of mobile security management systems. A robust mobile securities management system is necessary. Unfortunately, some problematic situations have not been properly considered in the mobile IP (Ioannidis *et al.*, 1991; Teraoka *et al.*, 1991) system. For example, there are times when some people carry their portable devices to a hotel room or office to hold a short-term conference. In this case, communicating directly among meeting attendees without network administration or additional infrastructure is necessary, and yet mobile IP does not provide services such as direct traffic links between/among end systems. In the existing mobile IP system, when the mobile hosts are located in the same range under a foreign agent, the datagram still has to travel through the foreign agent, which acts as an intermediary for the mobile hosts. On the other hand, the mobile hosts cannot share a common conference key to hold a secure conference for exchanging some confidential messages (Hwang and Yang, 1995).

Binkley and Trost (2001) proposed ad hoc routing at the link layer for mobile systems. This system utilizes an ad hoc protocol specified in the RFC 2501 to provide direct communication between mobile hosts. Mobile hosts broadcast *beacon* messages that include the IPs and *Machine Address Code* (MAC) addresses to provide direct communication through MAC addresses. In their system, the property of the ad hoc protocol is used to solve the problem of the mobile hosts being located in the same range under a foreign agent. All mobile hosts capture the existing shared context by choosing a fresh password and sharing it by symmetric keys among those presently in the room. However, it is an impracticable application, because setting the password is a problem in the first place.

Two well-known conference key establishment systems are: *Conference Key Distribution System* (CKDS) (Tseng and Jan, 1999; Wu, 1997; Yang *et al.*, 2003a) and *Conference Key Agreement System* (CKAS) (Ateniese *et al.*, 2000; Boyd and Nieto, 2003; Bresson *et al.*, 2001, 2002; Katz and Yung, 2002; Tseng, 2007). The CKDSs have a chairperson who is responsible for generating and securely distributing the conference key to all legal attending participants. The CKASs involve all participants cooperatively establishing a conference key without a chairperson. In this paper, we propose a user-anonymous and short-term CKDS for mobile IP to solve the problems in Binkley-Trost's scheme. The proposed CKDS allows some mobile hosts to quickly establish a secure conference environment. The security is based on the random oracle model and the elliptic curve version of the *Computational Diffie-Hellman* (CDH) assumption. To satisfy the low power of mobile devices, compared to previously proposed systems, the proposed CKDS is efficient in terms of communication and computational complexity.

The rest of our paper is organized as follows. Section 2 briefly looks at mobile IP registration and routing. Background issues and problems yet to be solved are presented and discussed, and some weaknesses of Binkley-Torst's scheme are shown. Section 3 shows how to use our proposed CKDS for solving the problems in mobile IP and Binkley-Torst's scheme. Section 4 analyzes and demonstrates the security of the proposed CKDS. Section 5 compares the performance between the proposed CKDS and the previously proposed CKDSs. Finally, conclusions, limitations and directions for future research of our study are given in Section 6.

2 Literature Review

In this section, we introduce the registration and the routing of mobile IP, respectively. There are some security issues that need to be overcome when mobile hosts move to the same visited network. Mobile IP (Ioannidis *et al.*, 1991; Teraoka *et al.*, 1991) is a modification from IP allowing hosts to continue to receive the datagram no matter where they happen to be attached to the Internet. A *Home Agent* (HA) is a host or router on a mobile host's home network. When a *Mobile Host* (MH) moves away from its home network, the HA is responsible for tunneling the datagram to the MH and a *Care-of-Address* (CoA) associates the mobile node with its home address by providing information on the MH's current point of attachment to the Internet or an organization's network. A *Foreign Agent* (FA) is a router on an MH's visited network providing routing services to the mobile node while registered.

When an MH moves away from its home network, it obtains a CoA on the visited network by soliciting or listening for FA advertisements or contacting the *Dynamic Host Configuration Protocol* (DHCP) specified in the RFC 1541. Here, the mutual authentication between the MH and the FA should be achieved. Molva *et al.* (Molva *et al.*, 1994; Samfat *et al.*, 1995) proposed a Kerberos-like scheme for this mutual authentication. Then, the MH registers the CoA with its

HA through FA. When the HA receives a *registration request* from an FA, the HA maintains the current CoA for the MH. In the registration period, the HA and MH can pre-share a secret key to be used for authenticating each other when the MH moves away from its home network. The authentication between HA and FA can be realized using an AAA (*Authentication*, *Authorization*, and *Accounting*) server (Kang and Park, 2006; Yang *et al.*, 2003b), simultaneously providing authentication, authorization, and accounting among agents. Long *et al.* (Long *et al.*, 2004) pointed out the crash of the home AAA server or any failure of the network along the path from the visited network to the home network will prohibit the roaming user from being authenticated. They proposed a public key certification to implement the above situation by modifying the SSL protocol. Later, Chang *et al.* (Chang *et al.*, 2006) showed the privacy of the roaming user and the round efficiency in Long *et al.*'s scheme are at risk and proposed an improved version conserving the advantages of Long *et al.*'s scheme.

Many public key systems have been used for mobile authentication. Unfortunately, the computational complexity of public key systems makes them inefficient and thus unsuitable for low-power mobile devices. Tang and Wu (2008) used an elliptic curve system based trust delegation mechanism to generate a delegation pass code for MH authentication. Since a less time-consuming elliptic curve is used, their system was more efficient than other systems.

The triangle routing problem delays the delivery of the datagrams and unnecessarily burdens networks and routers. Suppose any *Correspond Node* (CN) sends the datagrams to the MH and the datagrams sent to the MH's home address are intercepted by its HA, tunneled by its HA to the CoA, received at the endpoint (either at HA or the MH itself), and finally delivered to the MH. In the reverse direction, the datagrams sent by the MH are generally delivered to their destination using standard IP routing mechanisms, not necessarily passing through the HA. Datagrams going to the MH must travel through the HA when the MH is away from home, and this asymmetric routing is termed *triangle routing*.

For route optimization (Perkins and Johnson, 2000), the MH sends a *Binding Update* to inform the HA or CN of its current location when it is not on its home network. The mapping of the home address to the CoA is stored in the *Binding Cache* entry, which sets up the routing logic on the HA and CN to deliver traffic targeted for the MH's home address toward the MH's CoA. The traffic-flow service allows the MH to maintain communications using its home address while changing the network access location identified by the CoA. The *Binding Acknowledgment* is sent by the HA or CN to confirm the reception of the *Binding Update*. Both messages are protected by the IPSec protocol, specified in the companion RFC 3776. Unfortunately, there are still some problems with mobile IP. The problems and weaknesses of the solution proposed by Binkley and Torst are presented as follows.

Adjacent Mobile Hosts. In practical applications, when two MHs move to the same visited network and they would like to communicate with each other. The datagram must pass through the FA twice, even if the HA has sent out a *binding* message. Such a mechanism is not efficient because it wastes network resources. There are times when some people bring their notebook computers to a hotel room or office to have a conference. The MHs should be able to communicate with each other without network administration or any additional infrastructure. For example, MH_1 and MH_2 have moved into the range of FA. Since MH_1 and MH_2 share the same link, they should be able to communicate directly. However, for either the normal IP or the mobile IP, the same problem occurs in that there is a need for a router for this communication to be possible. In mobile IP, MHs must use an FA.

In a normal IP environment, the traditional IP subnet and *Address Resolution Protocol* (ARP) specified in the RFC 826 may be used to solve the problem. A subnet mask is used to determine whether the destination host is on a directly connected link. If on a direct connection, the sender will use an ARP table to match the MAC address and then directly send the packet out using the MAC address. However, it is easy to fake IP-to-MAC address bindings using ARP (Bellovin, 1989). In the mobile IP environment, the host can be quite mobile. MH_1 and MH_2 have no knowledge of who the neighbor is (that is sharing the same link). According to mobile IP routing, assume MH_1 sends the datagrams to MH_2. The datagrams sent to HH_1's home address are intercepted by its HA_1, tunneled by its HA_1 to the CoA, received at the FA, and finally delivered to MH_2. For the same reason, MH_2 also sends the datagrams through FA.

Moreover, in the wireless or mobile environment, access is quite easy. Any attacker may send an ARP packet containing its own MAC address and the victim's IP address to usurp the IP-to-MAC address binding of the victim in another part of the ARP cache. This enables the attacker to receive packets intended for the victim.

Weaknesses in Binkley-Trost's Scheme. To overcome the above problem, Binkley and Trost (2001) used an ad hoc protocol. In an ad hoc network, there is no fixed mobile switching center or base station. MHs within each other's radio range communicate directly, while those that are far apart rely on other hosts as routers to relay messages. In practice, the ad hoc network provides point-to-point communication. In mobile IP, each agent broadcasts an ICMP router discovery *advertisement* message specified in the RFC 1256 to inform nearby MHs that are in the home network or some visited network. In the ad hoc protocol, MHs broadcast *beacon* messages (Binkley and Trost, 2001) which augment the ICMP Router Discovery packet with the MAC and IP addresses.

For example, when MH_3 has moved into the range of MH_1 and MH_2, it can transmit a *beacon* message including its IP and MAC addresses. When MH_1 and MH_2 receive the *beacon* message, they verify the authenticity. If the *beacon* message is authentic, they add MH_3's IP and MAC addresses to their tables of known bindings. Therefore, MH_1 and MH_2 have knowledge of MH_3's IP and MAC addresses to use IP-to-MAC mapping to send packets to MH_3 directly. In this scheme, the agents and MHs broadcast *beacon* messages at a fixed rate. Agents broadcast *advertisement* messages once per second and MHs separately broadcast *beacon* messages once every ten seconds. MHs also transmit a *beacon* message to FA right before sending a *registration request*. This is assured when FA relays a *registration reply* using the IP-to-MAC mapping directly.

From the viewpoint of security, all the MHs share a symmetric key for *beacon* message authentication. When they meet face-to-face, one person can write a password on a blackboard for every one to install on their MHs during the meeting. Then the password is a seed to generate the symmetric key. By the end of the meeting, they can break the acceptance of *beacon* message authentication. If this password is a sufficiently long and random string, it can be used directly to set up a secure conference. In practice, finding a complicated password is difficult. It is much more user-friendly to set natural language phrases as passwords so people can recognize them easily. However, natural language phrases are weak keys for symmetric cryptosystems because they are drawn from a rather limited set of possibilities. The adversary can mount dictionary attacks or guessing attacks, recording the encrypted traffic and then attempting trial decryption with candidate passwords until he/she finds the correct one.

As we all know, anonymous communication has an important place in our political and social discourse. In their scheme, there does not seem to be sufficient privacy for the attending participants in the conference. Every participant must meet face-to-face to obtain the password written on a blackboard. It may lead to a participant being influenced by the other participants.

3 The Proposed Scheme

In this section, a user-anonymous and short-term designed CKDS is used for repairing the weaknesses in Binkley-Trost's scheme. Initially, the system chooses a public one-way hash function $H : \{0,1\}^* \rightarrow \{0,1\}^l$, an elliptic curve E defined over a finite field $\mathbb{F}_q$ and a base point $G \in E(\mathbb{F}_q)$ of prime order p, where q is typically a prime power (Koblitz *et al.*, 2000).

In the registration period, MH_i chooses a secret key $x_{\mathsf{MH}_i} \in_R \mathbb{Z}_p^*$, the corresponding public key $Y_{\mathsf{MH}_i} = x_{\mathsf{MH}_i} \cdot G$, and identity id_{MH_i}. Then MH_i registers Y_{MH_i}, id_{MH_i} and MAC address MAC_i with HA. Finally, HA delivers a symmetric key k_i to MH_i over a secure channel. FA also has the secret key x_{FA}, the corresponding public key $Y_{\mathsf{FA}} = x_{\mathsf{FA}} \cdot G$, and the identity id_{FA}. The following system parameters and notations are summarized and used throughout the paper.

$H : \{0,1\}^* \rightarrow \{0,1\}^l$	a public one-way hash function.
E	an elliptic curve defined over a finite field $\mathbb{F}_q$.
q	a prime power.
G	a base point over $E(\mathbb{F}_q)$ of prime order p.
$x_{\mathsf{MH}_i/\mathsf{FA}}$	a secret key over $\mathbb{Z}_p^*$ of $\mathsf{MH}_i/\mathsf{FA}$.
$Y_{\mathsf{MH}_i/\mathsf{FA}}$	a public key of $\mathsf{MH}_i/\mathsf{FA}$, where $Y_{\mathsf{MH}_i/\mathsf{FA}} = x_{\mathsf{MH}_i/\mathsf{FA}} \cdot G$.
$id_{\mathsf{MH}_i/\mathsf{FA}}$	an identity of $\mathsf{MH}_i/\mathsf{FA}$.
k_i	a symmetric key shared between MH_i and its HA.
$list_{\mathsf{IP-MAC}}$	a list records IP-to-MAC of MH_i.
$E_k(m)$	expresses the ciphertext of a data item m encrypted with a symmetric key k.
$D_k(m)$	expresses the plaintext of a data item m decrypted with a symmetric key k.
T	a timestamp.

The public system parameters and each public key information are recorded by a public directory. In the following subsections, we will separately show how an MH_i registers with FA and how the conference can be held in the same FA.

3.1 Mobile Host Registers with Foreign Agent

Figure 1 shows the procedure when MH_i moves to a visited network and registers its location with its HA. The following steps are performed.

Step R1. By receiving the FA *Advertisement* message, MH_i recognizes it is in a visited network or the home network.

Step R2. MH_i sends the *Registration Request* message with an attending conference request within it.

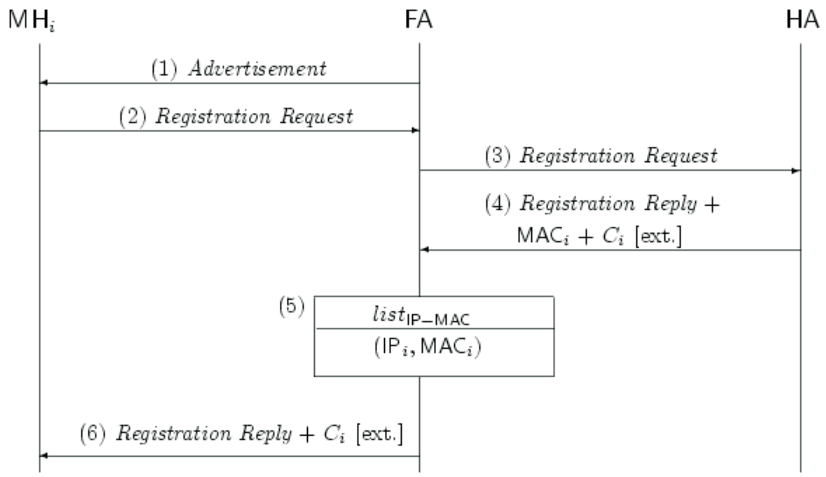
Step R3. FA relays the *Registration Request* message to HA. So HA can create or modify a *mobility binding* for MH_i.

Step R4. HA returns a *Registration Reply* message to FA after authenticating MH_i. If MH_i is a legal user, the *Registration Request* message will include MH_i's MAC_i and $C_i = E_{k_i}(Y_{\mathsf{FA}} \| id_{\mathsf{FA}} \| id_{\mathsf{MH}_i} \| T)$. The secure relationship between HA and FA can be achieved by the AAA server (See (Kang and Park, 2006; Yang *et al.*, 2003b) for more detailed descriptions).

Step R5. By receiving HA's notification, FA obtains MH_i's MAC_i from HA. Then, FA records MH_i's IP address IP_i and MAC_i in $list_{\mathsf{IP-MAC}}$.

Step R6. Because FA knows MH_i's MAC address, FA relays the *Registration Reply* message and C_i through MAC_i, which informs MH_i of the status of its request and indicates the lifetime granted by HA. Then, MH_i uses k_i to obtain Y_{FA}, id_{FA}, and id_{MH_i} by decrypting as $D_{k_i}(C_i)$. Then, MH_i checks whether the expiration time of T and the format of id_{MH_i} are correct. If correct, C_i is sent by HA.

Figure 1 MH_i registering with FA



Following procedure, FA can obtain the MAC address of the legal mobile host, and the mobile host can obtain the public key and identity of the legal FA using HA's authentication.

3.2 A Conference Key Distribution System

Without loss of generality, assume n mobile hosts MH_1, MH_2, $\cdots$, MH_n have registered with FA and are to attend a short-term conference. The CKDS is comprised of two stages: *Conference Key Distribution and* $list_{\mathsf{IP-MAC}}$ *Encryption Stage*, *Conference Key Recovery and* $list_{\mathsf{IP-MAC}}$ *Decryption Stage*. Details of these stages will be stated in the following.

Conference Key Distribution and $list_{\mathsf{IP-MAC}}$ ***Encryption Stage***
FA plays the role of the chairperson and performs the following steps for distributing a short-term conference key ck with l-bit and $list_{\mathsf{IP-MAC}}$ to a set of attending mobile hosts in a conference $Group = \{\mathsf{MH}_1, \mathsf{MH}_2, \ldots, \mathsf{MH}_n\}$, where l can be set as the same length of $list_{\mathsf{IP-MAC}}$.

Step d1. Compute the common session key $k_{\mathsf{FA-MH}_i} = x_{\mathsf{FA}} \cdot Y_{\mathsf{MH}_i}$ shared with $\mathsf{MH}_i \in Group$ and the hash value $h_i = H(k_{\mathsf{FA-MH}_i} \| id_{\mathsf{FA}} \| id_{\mathsf{MH}_i} \| T)$, where T is a timestamp.

Step d2. Choose a conference key ck at random and compute $\alpha_i = h_i \oplus ck$ for $1 \leq i \leq n$, where $\oplus$ is the bit-wise exclusive-or operation. Encrypt the $list_{\mathsf{IP-MAC}}$ as $C_{\mathsf{IP-MAC}} = E_{ck}(list_{\mathsf{IP-MAC}}) = ck \oplus list_{\mathsf{IP-MAC}}$. Since ck is random for each session, the symmetric key encryption is replaced by the one-time pad cipher.

Step d3. Compute the check value $V = H(ck \| C_{\mathsf{IP-MAC}} \| T)$.

Step d4. Broadcast the message $\{T \| C_{\mathsf{IP-MAC}} \| V \| \alpha_i\}$ for $1 \leq i \leq n$.

Conference Key Recovery and $list_{\mathsf{IP-MAC}}$ ***Decryption Stage***
Each $\mathsf{MH}_i \in Group$ in the conference counts on the message $\{T \| C_{\mathsf{IP-MAC}} \| V \| \alpha_i\}$ for $1 \leq i \leq n$, to recover the conference key ck and $list_{\mathsf{IP-MAC}}$ by performing the following steps.

Step r1. Check the validity of the timestamp T. If it is invalid, stop recovering the conference key.

Step r2. Compute the common session key $k_{\mathsf{MH}_i\mathsf{-FA}} = x_i \cdot Y_{\mathsf{FA}}$ shared with FA and the hash value $h_i = H(k_{\mathsf{MH}_i\mathsf{-FA}} \| id_{\mathsf{FA}} \| id_{\mathsf{MH}_i} \| T)$.

Step r3. Use the values h_i and α_i to obtain $ck = \alpha_i \oplus h_i$.

Step r4. Check the validity of ck and the ciphertext $C_{\mathsf{IP-MAC}}$ by verifying $H(ck \| C_{\mathsf{IP-MAC}} \| T) = V$.

Step r5. Obtain $list_{\mathsf{IP-MAC}}$ by decrypting $D_{ck}(C_{\mathsf{IP-MAC}}) = C_{\mathsf{IP-MAC}} \oplus ck$.

Following the above procedure, the MHs attending the conference in the same range of FA can recover the authenticated $list_{\mathsf{IP-MAC}}$. They can directly communicate with each other by mapping this list and using the common conference key ck. Even if two mobile hosts are not within each other's direct reach, they can still communicate with each other through FA.

4 Security Analysis

In this section, we discuss the security of the proposed CKDS. In the system, any adversary intending to reveal a secret key $x_{\mathsf{MH}_i/\mathsf{FA}}$ from its corresponding public key $Y_{\mathsf{MH}_i/\mathsf{FA}}$ will have to face the *Elliptic Curve Discrete Logarithm Problem* (ECDLP). The system has a public directory recording the public system parameters and all the public key information. Each user in the system can access this information through the public directory. On the other hand, besides the above assumptions, the authentication between HA and FA is based on the same assumptions found in (Kang and Park, 2006; Yang *et al.*, 2003b).

The proposed CKDS is secure against a malicious adversary to reveal CK or forge V. Here, we adopt the elliptic curve version of the CDH assumption to prove the proposed CKDS is secure against the adversary. The following lists the security definition.

CDH problem: *There are several domain parameters that is a prime power q such that an elliptic curve E over a finite field $\mathbb{F}(q)$, and a base point G with prime order p. For given $Y_1 = x_1 \cdot G$ and $Y_2 = x_2 \cdot G$ to compute $x_1 \cdot x_2 \cdot G$, where x_1 and x_2 are randomly chosen from $\mathbb{Z}_p^*$, is computationally hard. There is no efficient algorithm $\mathcal{A}$ that satisfying*

$$\Pr[\mathcal{A}(x_1 \cdot G, x_2 \cdot G) = x_1 \cdot x_2 \cdot G] < \frac{1}{P(|q|)},$$

for any polynomial P, where the probability is over the random choice of x_1 and x_2. We say the elliptic curve version of the CDH problem is hard if there is no such polynomial-time algorithm $\mathcal{A}$.

In Step d4, the broadcast messages are $\{T\|C_{\mathsf{IP-MAC}}\|V\|\alpha_i\}$ for $1 \le i \le n$. Clearly, anyone can obtain ck by computing $ck = \alpha_i \oplus h_i$ if he or she knows h_i. In the following, we will prove for giving Y_{FA} and Y_{MH_i} to compute $x_{\mathsf{FA}} \cdot x_{\mathsf{MH}_i} \cdot G$ for $1 \le i \le n$, are computationally hard, where x_{FA} and x_{MH_i} are the random value over $\mathbb{Z}_p^*$. By the probability argument, since for any $V_0 \in \{0,1\}^l$, we have $\Pr[V = V_0] = \frac{1}{2^l}$. For any fixed V_0, the random variable is fixed. Therefore, we only consider the probability distribution for

$$\Pr[\mathcal{A}(x_1 \cdot G, x_2 \cdot G) = x_1 \cdot x_2 \cdot G | V = V_0] < \frac{1}{P(|q|)}.$$

Theorem 4.1: *Under the random oracle model, if the elliptic curve version of the CDH problem is hard, any malicious adversary cannot obtain the conference key ck.*

Proof. Proof by contradiction: assume that algorithm $\mathcal{A}'$ can output the conference key ck with the inputs $Y_{\mathsf{FA}}, Y_{\mathsf{MH}_i}$, and $\{T\|C_{\mathsf{IP-MAC}}\|V\|\alpha_i\}$ in a polynomial-time. We can construct algorithm $\mathcal{A}$ to compute $x_1 \cdot x_2 \cdot G$ by giving Y_1 and Y_2 in a polynomial-time, where $Y_1 = x_1 \cdot G$, $Y_2 = x_2 \cdot G$, and $x_1, x_2 \in_R \mathbb{Z}_p^*$. First, the points Y_1 and Y_2 are the inputs of algorithm $\mathcal{A}$. Then, the algorithm $\mathcal{A}$ sets the following points.

$$Y_{\mathsf{FA}} = Y_1$$
$$Y_{\mathsf{MH}_i} = Y_2,$$

and randomly chooses $\alpha_i \in_R \{0,1\}^l$. Once the algorithm $\mathcal{A}'$ outputs ck, the algorithm $\mathcal{A}$ computes $h_i = \alpha_i \oplus ck$. In the random oracle model, $\mathcal{A}$ will maintain a list $list_H$ for the oracle H, which is initially set to empty. At any time, $\mathcal{A}'$ can query the random oracle. When $\mathcal{A}'$ issues a query to H, $\mathcal{A}$ will return the same output for identical inputs in hash queries by checking the list $list_H$ before creating a new output. Under the random oracle assumption (Bellare and Rogaway, 1993), $\mathcal{A}'$ must ask a value $k_{\mathsf{FA-MH}_i}||id_{\mathsf{FA}}||T$ of hash queries to H, thus $\mathcal{A}'$ can use h_i to find the corresponding $k_{\mathsf{FA-MH}_i} = x_1 \cdot x_2 \cdot G$ in $list_H$. In other words, $\mathcal{A}'$ has the probability $\Pr[\mathcal{A}(x_1 \cdot G, x_2 \cdot G) = x_1 \cdot x_2 \cdot G | V = V_0] = 1$, which is a contradiction for Assumption 1. On the other hand, since the check value V is composed by ck, if any adversary has the ability to forge V, we can also construct an algorithm in a polynomial-time to find the corresponding hash query in the random oracle, and then output ck.

Theorem 4.2: *Under the elliptic curve version of the CDH assumption, if a one-time pad cipher is theoretically unbreakable, any malicious adversary cannot obtain the* $list_{\mathsf{IP-MAC}}$.

Proof. Assume the symmetric key encryption $C_{\mathsf{IP-MAC}} = E_{ck}(list_{\mathsf{IP-MAC}})$ is replaced by the one-time pad cipher. The ciphertext $C_{\mathsf{IP-MAC}}$ is computed as

$$C_{\mathsf{IP-MAC}} = ck \oplus list_{\mathsf{IP-MAC}}$$

To obtain $list_{\mathsf{IP-MAC}}$ from $C_{\mathsf{IP-MAC}}$ without knowing ck, the probability is $\frac{1}{2^l}$. Theorem 4.1 has proven any malicious adversary cannot obtain the conference key ck under the elliptic curve version of the CDH assumption. The one-time pad can be shown to be theoretically unbreakable if a ciphertext is encrypted using a random key (Mao, 2004). Since the conference key is randomly chosen by FA for each session, it satisfies the requirements of a one-time pad cipher. If the length of $list_{\mathsf{IP-MAC}}$ is larger than l bits, then ck is treated as a seed and a pseudorandom bit generator is utilized to generate an enough length for $list_{\mathsf{IP-MAC}}$. The security of the pseudorandom bit generators relies on the presumed intractability of the underlying number-theoretic problem.

Theorem 4.3: *Under the random oracle model, if the elliptic curve of the CDH assumption is hard, any malicious adversary cannot find out who attends the conference.*

Proof. Any legal participant MH_j can obtain h_i by computing $h_i = ck \oplus \alpha_i$ for $\forall i \neq j$. Under the random orale model, the one-way hash function H is a true random function, that is, $H(k_{\mathsf{MH}_i-\mathsf{FA}} \| id_{\mathsf{FA}} \| id_{\mathsf{MH}_i} \| T)$ is an independent random variable from $k_{\mathsf{MH}_i-\mathsf{FA}} \| id_{\mathsf{FA}} \| id_{\mathsf{MH}_i} \| T$. Therefore, no one can discover who attends the conference.

5 Performance Analysis and Comparisons

In this section, we compare the computational complexity and the number of messages broadcasted for recovering a session key, and the number of messages that should pass through FA to pass our CKDS with those of Wu's CKDS, Tseng-Jan's CKDS, and Yang *et al.*'s CKDS. To analyze the computational complexity, the following notations are defined.

T_H	the time for computing the adopted one-way hash function H.
T_{EXP}	the time for computing modular exponentiation.
T_{MUL}	the time for computing modular multiplication.
T_{INV}	the time for computing for modular inverse.
T_{EC_MUL}	the time for computing the multiplication of a number and a point on the elliptic curve.
T_{XOR}	the time for computing the bit-wise exclusive-or operation.
T_L	the time for constructing a 2-degree polynomial L using the Lagrange interpolation formula.
$T_{L(x)}$	the time for computing $L(x)$ given the value x.
n	the number of mobile hosts in the conference.

Both Yang *et al.*'s CKDS and our CKDS adopts the elliptic curve cryptographic. The elliptic curve discrete logarithm problem with order 160-bit prime offers approximately the same level of security as the discrete logarithm problem with a 1024-bit modulus prime (Katz and Yung, 2002). Computing the multiplication of a number and a point on the elliptic curve and a modular exponentiation requires an average of 29 1024-bits and 240 1024-bits modular multiplications, respectively. Further, in our CKDS, FA uses ck as the symmetric key to encrypt $list_{\mathsf{IP-MAC}}$. All mobile hosts in the conference can use $list_{\mathsf{IP-MAC}}$ to broadcast messages directly thought MAC addresses rather than through FA to pass the messages. The following comparisons between Wu's CKDS, Tseng-Jan's CKDS, and Yang *et al.*'s CKDS without the above improvement and our CKDS are assumed in the same circumstance of mobile IP.

In the *Conference Key Distribution and* $list_{\mathsf{IP-MAC}}$ *Encryption Stage* of our CKDS, in Step d1, FA computes the common session key $k_{\mathsf{FA-MH}_i}$ shared with each MH_i and the hash value h_i for $1 \leq i \leq n$, requiring $n \times T_{EC\_MUL} + n \times T_H$. Then, Step d2 requires $(n+1) \times T_{XOR}$ for computing α_i for $1 \leq i \leq n$ and encrypt $list_{\mathsf{IP-MAC}}$. Here, the symmetric encryption uses the one-time pad cipher. Next, in Step d3, FA computes the check value V, requiring T_H. Total computational complexity in this stage is required $n \times T_{EC\_MUL} + (n+1) \times T_{XOR} + (n+1) \times T_H$.

After receiving the broadcast message $\{T \| C_{\mathsf{IP-MAC}} \| V \| \alpha_i\}$ broadcast by FA, each MH_i enters the *Conference Key Recovery and* $list_{\mathsf{IP-MAC}}$ *Decryption Stage*. He or she verifies T in Step r1, and computes the common session key $k_{\mathsf{MH}_i-\mathsf{FA}}$ shared with FA and the hash value h_i, requiring $T_{EC\_MUL} + T_H$. Then, in Step r3, each participant recover ck requires T_{XOR}. In Step r4, each participant checks the validity of ck, requiring T_H. Finally, Step r5 requires T_{XOR} to recover $list_{\mathsf{IP-MAC}}$. The total computational complexity in this stage is $T_{EC\_MUL} + 2 \times T_H + 2 \times T_{XOR}$.

Table 1 Computational complexities of Wu's CKDS, Tseng-Jan's CKDS, Yang *et al.*'s CKDS and our CKDS

	Key distribution stage	Key recovery stage
Wu's CKDS	$n \times T_{EXP} + (n+1) \times T_H$ $T_{INV} + (n^3 + 3 \times n^2 - n)$ $\times T_{MUL}$	$T_{EXP} + 2 \times T_H + T_{INV} +$ $(3 \times n^2 - n) \times T_{MUL}$
Tseng-Jan's CKDS	$n \times T_{EXP} + (n+1) \times T_H$ $+(n \times (n-1)/2) \times T_{MUL}$	$T_{EXP} + 2 \times T_H + (n-1)$ $\times T_{MUL}$
Yang *et al.*'s CKDS	$n \times T_{EC\_MUL} + n \times T_{L(x)}$ $+(n+1) \times T_H$	$T_{EC\_MUL} + T_L + 2 \times T_H$
Our CKDS	$n \times T_{EC\_MUL} + (n+1) \times$ $T_{XOR} + (n+1) \times T_H$	$T_{EC\_MUL} + 2 \times T_H + 2 \times$ T_{XOR}

The computational complexities of Wu's CKDS, Tseng-Jan's CKDS, and Yang *et al.*'s CKDS have been shown in their paper, respectively. According to Table 1, both Yang *et al.*'s CKDS and our CKDS adopt the elliptic curve system, which are much more efficient than Wu's CKDS and Tseng-Jan's CKDS. Further, our CKDS is more efficient than Yang *et al.*'s CKDS, that is, T_{XOR} replaces T_L and $T_{L(x)}$ in our CKDS, and also encrypt/decrypt $list_{\mathsf{IP-MAC}}/C_{\mathsf{IP-MAC}}$.

Table 2 The number of broadcasting messages and the number of messages through FA in Wu's CKDS, Tseng-Jan's CKDS, Yang *et al.*'s CKDS *et al.* and our CKDS

	# of broadcasting messages	# of messages via FA
Wu's CKDS	$n+3$	$n \times m$
Tseng-Jan's CKDS	$n+3$	$n \times m$
Yang *et al.*'s CKDS	$n+3$	$n \times m$
Our CKDS	$n+3$	0

On the other hand, in our CDKS, the number of messages should be broadcast in the *Conference Key Distribution and* $list_{\mathsf{IP-MAC}}$ *Encryption Stage* is $n+3$, i.e., $\{T \| C_{\mathsf{IP-MAC}} \| V \| \alpha_i\}$. Though the number of messages is the same as that in Wu's CKDS, Tseng-Jan's CKDS, and Yang *et al.*'s CKDS, our CKDS also encrypts $list_{\mathsf{IP-MAC}}$ as $C_{\mathsf{IP-MAC}}$. In the following, the effects of FA without encrypting $list_{\mathsf{IP-MAC}}$ in Wu's CKDS, Tseng-Jan's CKDS, and Yang *et al.*'s CKDS will be shown. Assume MH_i wants to broadcast m confident messages to other mobile hosts in the conference. The corresponding ciphertexts should use FA to transfer. However, in our CKDS, since each MH_i has the $list_{\mathsf{IP-MAC}}$, the corresponding ciphertexts can be transferred by MAC addresses directly if they are within each other's direct reach. Table 2 shows the number of corresponding ciphertexts should be by FA in our CKDS is zero, but that in Wu's CKDS, Tseng-Jan's CKDS, and Yang *et al.*'s CKDS is $n \times m$.

6 Conclusions and Limitations

In the proposed CKDS scheme, which is more efficient than Wu's CKDS, Tseng-Jan's CKDS, and Yang *et al.*'s CKDS, so there is no need for FA to be a router to transmit datagrams between the MHs in a conference. To protect a participant from the influence of other participants, the identity of the participant in our scheme is hidden. Our scheme can successfully solve the problems in mobile IP and Binkley-Torst's scheme to allow some mobile hosts to quickly establish a secure conference environment by a linker-layer routing.

However, this study has some limitations. First, the crashing of FA will prohibit the MHs from setting up a secure conference environment since the FA plays the role of the chairperson for distributing a short-term conference key. Conference key agreement systems can be utilized in future study. That is, all participants cooperatively establish a conference key without a chairperson. The conference key is determined by all participants rather than individuals. Second, if a MH is not covered by the radio range of the FA, the MH has no ability to be authenticated by the FA and then attend the conference. Future study should combine mobile ad hoc networks (MANET) which is a self-configuring network of mobile devices connected by wireless links in the proposed scheme. In a MANET, each MH must forward traffic unrelated to its own use, and therefore be a router. A MH is not covered by the radio range of the FA can use other MHs which are in the FA's radio range to accomplish its authentication and then attend the conference.

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC98-2622-E-018-004-CC3. The authors would like to acknowledge the many helpful suggestions of anonymous reviewers.

References

Ateniese, G., Steiner, M. and Tsudik, G. (2000) 'New multiparty authentication servives and key agreement protocols', *IEEE J. Sel. Areas Commum*, Vol. 18, No. 4, pp. 628–639.

Bellare, M. and Rogaway, P. (1993) 'Random oracles are practical: a paradigm for designing efficient protocols', *Proceedings of the 1st annual Conference on Computer and Communications Security*, pp. 62–73.

Bellovin, S. M. (1989) 'Security problems in TCP/IP protocol suite', *ACM Computer Communications Review*, Vol. 19, No. 2, pp. 32–48.

Binkley, J. and Trost, W. (2001) 'Authenticated ad hoc routing at the link layer for mobile systems', *ACM-Baltzer Wireless Networks*, Vol. 7, No. 2, pp. 139–145.

Boyd, C. and Nieto, J. M. G. (2003) 'Round-optimal contributory conference key agreement', *Proceddinging of Public-Key Cryptography, Lecture Notes in Computer Science 2567*, pp. 161–174.

Bresson, E., Chevassut, O. and Pointcheval, D. (2001) 'Provably authenticated group Diffie-Hellman key exchange', *Proceeding of the 8th Annual ACM Conference on Computer and Communications Security*, pp. 255–264.

Bresson, E., Chevassut, O. and Pointcheval, D. (2002) 'Dynamic group Diffie-Hellman key exchange under standard assumptions', *Advances in Cryptology, Eurocrypt'02, Lecture Notes in Computer Science 2332*, pp. 275–286.

Chang, Y. F., Lee, J. S. and Chang, C. C. (2006) 'A secure and efficient authentication scheme for mobile users', *International Journal of Mobile Communications*, Vol. 4, No. 5, pp. 581–594.

Hwang, M. S. and Yang, W. P. (1995) 'Conference key distribution protocols for digital mobile communication systems', *IEEE Journal on Selected Areas in Communications*, Vol. 13, No. 2, pp. 416–420.

Ioannidis, J., Duchamp, D. and Maguire, G. Q. (1991) 'IP-based protocols for mobile internetworking', *ACM SIGCOMM Computer Communication Review*, Vol. 21, No. 4, pp. 235–245.

Juang, W. S. and Wu, J. L. (2009) 'Robust and efficient authenticated key agreement in mobile communications', *International Journal of Mobile Communications*, Vol. 7, No. 5, pp. 562–579.

Kang, H. S. and Park, C. S. (2006) 'A key management scheme for secure mobile IP registration based on AAA protocol', *IEICE Transactions on Fundamentals*, Vol. E89-A, No. 6, pp. 1842–1846.

Katz, J. and Yung, M. (2002) 'Scalable protocols for authenticated group key exchange', *Advances in Cryptology, Crypto'02. Lecture Notes in Computer Science 2729*, pp. 110–125.

Kim, J., Lee, I., Lee, Y., Choi, B., Hong, S. J., Tam, K., Naruse, K. and Maeda, Y. (2004) 'Exploring e-business implications of the mobile internet: a cross-national survey in Hong Kong, Japan and Korea', *International Journal of Mobile Communications*, Vol. 2, No. 1, pp. 1–21.

Koblitz, N., Menezes, A. and Vanstone, S. A. (2000) 'The state of elliptic curve cryptography', *Designs, Codes and Cryptography*, Vol. 9, No. 2/3, pp. 173–193.

Liu, Z., Min, Q. and Ji, S. (2010) 'An empirical study of mobile securities management systems adoption: a task - technology fit perspective', *International Journal of Mobile Communications*, Vol. 8, No. 2, pp. 230–243.

Long, M., Wu, C. H. and Irwin, J. D. (2004) 'Localised authentication for inter-network roaming across wireless LANs', *IEE Proceeding of Communications*, Vol. 151, No. 5, pp. 496–500.

Mao, W. (2004) *Modern Cryptography: Theory and Practice*, Prentice Hall.

Massoud, S. and Gupta, O. K. (2003) 'Consumer perception and attitude toward mobile communication', *International Journal of Mobile Communications*, Vol. 1, No. 4, pp. 390–408.

Molva, R., Samfat, D. and Tsudik, G. (1994) 'Authentication of mobile users', *IEEE Network, Special Issue on Mobile Communications*, Vol. 8, No. 2, pp. 26–34.

Mylonakis, J. (2004) 'Can mobile services facilitate commerce? findings from the Greek telecommunications market', *International Journal of Mobile Communications*, Vol. 2, No. 2, pp. 188–198.

Perkins, C. and Johnson, D. (2000) *Route optimization in mobile IP*, IETF Internet Draft.

Samfat, D., Molva, R. and Asokan, N. (1995) 'Untraceability in mobile networks', *Proceedings of International Conference on Mobile Computing and Networking*, pp. 26–36.

Tan, J., Wen, H. J. and Gyires, T. (2003) 'M-commerce security: the impact of Wireless Application Protocol (WAP) security services on e-business and e-health solutions', *International Journal of Mobile Communications*, Vol. 1, No. 4, pp. 409–424.

Tang, C. and Wu, D. O. (2008) 'An efficient mobile authentication for wireless networks', *IEEE Transactions on Wireless Communications*, Vol. 7, No. 4, pp. 1408–1416.

Teraoka, F., Yokore, Y. and Tokoro, M. (1991) 'A network architecture providing host migration transparency', *ACM SIGCOMM Computer Communication Review*, Vol. 21, No. 4, pp. 209–220.

Tseng, Y. M. (2007) 'A commuication-efficient and fault-tolerant conference-key agreement protocol with forward secrecy', *The Journal of Systems and Software*, Vol. 80, No. 7, pp. 1091–1101.

Tseng, Y. M. and Jan, J. K. (1999) 'Anonymous conference key distribution systems based on the discrete logarithm problem', *Computer Communications*, Vol. 22, No. 8, pp. 749–754.

Wu, T. C. (1997) 'Conference key distribution system with uesr anonymity based on algebraic approach', *IEE Proceedings - Computer Digital Technology*, Vol. 144, No. 2, pp. 145–148.

Yang, C. C., Chang, T. Y. and Hwang, M. S. (2003a) 'A new anonymous conference key distribution system based on the elliptic curve discrete logarithm problem', *Computer Standards & Interfaces*, Vol. 25, No. 2, pp. 141–145.

Yang, C. C., Hwang, M. S., Li, J. W. and Chang, T. Y. (2003b) 'A solution to mobile IP registration for AAA', *Proceeding of CIC 2002, Lecture Notes in Computer Science 2524*, pp. 329–337.