INFORMATICA, 2013, Vol. 24, No. 1, 59–70

Efficient Mobile Conference Scheme for Wireless Communication

Der-Chyuan LOU[1], Kuo-Ching LIU[2], Hui-Feng HUANG[3] *

[1]*Department of Computer Science and Information Engineering, Chang Gung University Kweishan, Taoyuan 33302, Taiwan*

[2]*Department of Medical Laboratory Science and Biotechnology, China Medical University Taichung 404, Taiwan*

[3]*Department of Computer Science and Information Engineering, National Taichung University of Science and Technology Taichung 404, Taiwan*

e-mail: dclouprof@gmail.com, kchliu@mail.cmu.edu.tw, phoenix@nutc.edu.tw

Received: August 2011; accepted: June 2012

Abstract. Technological advances have allowed all conferees to hold a mobile conference via wireless communication. When designing a conference scheme for mobile communications it should be taken into account that the mobile users are typically using portable devices with limited computing capability. Moreover, wireless communications are more susceptible to eavesdropping and unauthorized access than conversations via wires. Based on elliptic curve cryptography, this article proposes a secure mobile conference scheme which allows a participant to join or quit a teleconference dynamically. Without any interactive protocol among participants are required to construct the common key. This can save on communication overhead.

Keywords: conference key, mobile communication, elliptic curve cryptography, 3GPP2.

1. Introduction

Today, people have many opportunities to obtain services or resources from application servers by using their mobile devices through the wireless network. Based upon the current situation, the further widespread development of wireless mobile communication will depend on the accessibility of secure networking. A conference key scheme enables a group of people to establish a common secret key to hold a secure conference. The rapid growth of technological advances has allowed all conferees to hold a mobile conference at anytime and anywhere via wireless communications. The conference key is a common secret key with which one can encrypt and decrypt messages to communicate with others in the group. The first type of conference key protocol allows a chairman to select a conference key and distribute it to all participants (Berkovits, 1991; Beller *et al.*, 1993; Chang *et al.*, 1992; Hwang and Yang, 1995; Hwang, 1999; Tseng and Jan, 1999; Yi *et al.*, 2003). The second type of conference key protocol allows all participants to compute a common

*Corresponding author.

key together without a chairman (Ingemarsson *et al.*, 1982; Steer *et al.*, 1990; Tzeng, 2002). A mobile teleconference is a synchronous collaboration session in which conferees at remote locations cooperate in an interactive procedure, such as a scientific discussion, a board meeting, or even a virtual classroom. On the other hand, compare to the transmission via hard wires, wireless communications transmit conversations via radio which are more susceptible to eavesdropping and unauthorized access. The traditional conference key scheme isn't suitable for wireless mobile participants (Berkovits, 1991; Chang *et al.*, 1992; Ingemarsson *et al.*, 1982; Tseng and Jan, 1999; Tzeng, 2002). Because a mobile user's portable devices are usually low powered, low cost, and limited to computing capability, it is crucial to ensure confidentiality and authenticity in mobile teleconferences. However, many conference schemes designed for wireless communication systems have been shown to be insecure (Ng, 2001; Wan *et al.*, 2006; Yi *et al.*, 2003).

For the limited computing capability in a mobile user's portable device, based on the RSA cryptography and congruence mechanism, Hwang and Yang (1995) proposed the conference key established scheme for mobile communications. But they fail to consider the situation that a participant may attend a conference for only a period of time. If a participant resigns or leaves the conference and he premeditatedly eavesdropped on data transmissions, he could then also decrypt the data. Thus, all messages are likely to be compromised during the span of the system. Later, Hwang improved Hwang and Yang's scheme to allow a participant to join afterward or quit a conference early, and meanwhile keep other participants' secret information unchanged (Hwang, 1999). However, Ng points out some extra modular multiplications and divisions that show Hwang's scheme to be slower for a mobile user (Ng, 2001). Recently, based on the modular square root (MSR) principle, a new conference scheme for mobile communications was proposed by Yi *et al.* (2003). Their scheme allows a participant to join or quit a conference dynamically. Both of Hwang's and Yi *et al.*'s conference key schemes need the conference bridge (trusted center) to distribute the common conference key and several interactive communications are required to generate the common conference key between conference bridge and each conferee (Hwang, 1999; Yi *et al.*, 2003). As a result, however, this creates further communication burden and inconvenience for the conference bridge and each conferee. Moreover, Ng (2001) showed that Hwang's scheme is insecure against eavesdropping and impersonation attacks; and Wan *et al.* (2006) points out that Yi *et al.*'s scheme is insecure against the replay attack.

Compared to RSA cryptography and modular square root (MSR) technique, elliptic curve cryptography (ECC) can provide the same level of security with smaller key sizes (Koblitz, 1987; Miller, 1986). It has been shown that 160-bit ECC provides comparable security to 1024-bit RSA cryptography and 224-bit ECC provides comparable security to 2048-bit RSA cryptography (Koblitz, 1987; Miller, 1986). Therefore, under the same security level, smaller key sizes of ECC could offer merits of faster computational efficiency, as well as memory, energy and bandwidth savings. Hence by using ECC instead of RSA and MSR it can achieve much more energy and bandwidth savings. Owing to the merits of ECC, recently, based on ECC, Sui *et al.* have included their key agreement protocol in the 3GPP2 specifications (3rd Generation Partnership Project 2; Sui *et al.*,

2005; 3GPP2 N.S001 vl.0; 3GPP2 C.S0016-B vl.0). However, Sui *et al.*'s scheme is not secure. Later, under ECC, Lu and Cao present an enhanced authenticated key agreement protocol for wireless mobile communication and also include their scheme in 3GPP2 specifications to improve Sui *et al.*'s scheme.

Because to the ECC can be applied to 3GPP2 mobile networks, this article uses 160-bit ECC as the cryptographic infrastructure to propose a novel mobile conference in which conference keys in a conference are different from each session. It means the common conference key is updated in each session. Our goal is to minimize the potential damages over a public network. Once the time period has elapsed, the participants in a conference cannot access any messages with previously used common keys. Therefore, if a user resigns or is deleted from a conference and eavesdropped on later messages, he/she could not then decrypt the message with former conference keys. The purpose is to protect future messages. In the proposed scheme, no conference bridge (or trusted center) and interactive protocol among participants is required to construct the common conference key for each session. This avoids communication overhead. In addition, the proposed method has the following three properties.

(1) The conference key computation and verification algorithm are quite simple and efficient.
(2) It can be easily implemented into a dynamic conference system for mobile communication because other participants' information items don't need to be immediately changed once a participant is added or deleted.
(3) Once a participant leaves the conference, he/she does not have the access to decrypt the data with his former conference keys.

Based upon the above properties, the proposed conference system is more flexible and practical. Moreover, the proposed method allows one to broadcast data so that only authorized participants with proper keys can decrypt the data to obtain useful information. Broadcasting data can save quite a lot of bandwidth over the point-to-point transmission. Hence, it is more suitable for contemporary computer environment. This article is organized as follows. In the next section, we present the necessary related works of the proposed scheme. In Section 3, we introduce the design principles of the conference scheme for mobile communications. The security and performance of the scheme is discussed in Section 4. Finally, some conclusions are given in Section 5.

2. Preliminaries

Prior to the propose of elliptic-curve scheme, this session first introduces the properties of elliptic curves (Koblitz, 1987; Kumanduri, 1998; Miller, 1986) that will allow us to discuss the security of the proposed scheme in Section 4.

An elliptic curve is generally given by

$$y^2 = x^3 + ax^2 + bx + c. \tag{1}$$

Let q be a prime number larger than 3. An elliptic curve modulo q, E_q is the set of solutions (x, y) satisfying

$$y^2 = x^3 + ax^2 + bx + c \pmod{q}. \tag{2}$$

Here we take x and y to be in a fixed complete residue system modulo q, so E_q is a finite set. The group law on an elliptic curve is defined when the discriminant is nonzero, where the discriminant of the curve in (2) is $\Delta = 27c^2 + 4a^3c + 4b^3 - a^2b^2 + 8abc \bmod q$. Again, the point at infinity is O. The rules for addition of points on E_q apply with the interpretation that the reciprocal is the inverse modulo q. When the inverse modulo q does not exist, then the corresponding line is "vertical" modulo q. Suppose that two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. The rules are as follows. If $x_1 = x_2 \bmod q$, then $P_1 + P_2 = O$. If $y_1 = 0 \bmod q$, then $P_1 = -P_1$ and $2P_1 = O$. In other cases, the sum $P_1 + P_2$ is obtained by computing $\lambda = \frac{x_1 - x_2}{y_1 - y_2} \bmod q$, if $P_1 \neq P_2$, or $\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1} \bmod q$, if $P_1 = P_2$, and then let $x_3 = \lambda^2 - a - x_1 - x_2 \bmod q$. Hence, $P_1 + P_2 = (x_3, y_3)$, where $y_3 = \lambda(x_1 - x_3) - y_1 \bmod q$. The addition rules are given below. For all $P, Q \in E_q$,

(1) $-O = O$.
(2) $O + P = P$ and $P + O = P$.
(3) If $P = (x, y) \neq O$, then $-P = (x, -y)$. (Note that P and $-P$ are the only points on E_q with the same x-coordinate.)
(4) If $Q = -P$, then $P + O = O$.
(5) For any positive integer k and a point $P \in E_q$, the scalar multiplications kP is $kP = P + P + \cdots + P$, where P is added to itself k times.
(6) If the number of elements on E_q is n, then for every point P on E_q, it has $nP = O \bmod q$.

In the elliptic curve cryptosystems, the elliptic curve discrete logarithm problem in E_q is the following: Given $P \in E_q$ with order n (that is $nP = O$) and Q is a point in the cyclic group $G = \langle P \rangle$, it is intractable to find r such that $Q = rP$.

3. The Proposed Scheme

Let the set $U = \{U_1, U_2, \ldots, U_m\}$ be the initial participant set. One participant is the chairman who initiates the conference. That is, anyone can be a chairman for each session time. The idea being that the chairman is to distribute the secret session key to each participant from each session. During a conference, each session key is randomly selected by a chairman, and it is different for each session conference. Without a trusted center to distribute the session key, the chairman U_i broadcasts some messages so that other legal participants of U can evaluate and prove the validity of the session key without any interactive communication for each session. Now, we are going to propose a novel conference scheme for mobile communication. The procedure of the proposed scheme contains two phases: initial computation phase and conference session key computation and verification phase. We state the details of these phases as follows:

Initial computation phase

Based on elliptic curve cryptography (ECC), the system or certificate authority (CA) chooses a large prime number q ($q \approx 2^160$) and an elliptic curve E_q (the elliptic curve E is over the finite field F_p); a cyclic group $G = \langle P \rangle$ of points over the elliptic curve E_q, where P is the generator of the cyclic group and has an order n of at least 160 bits. It provides $nP = O$ and the point at infinity is O. Then, the system publishes the elliptic E_q, P, n, and a one-way secure hash function $h(\ )$.

Let $U = \{U_1, U_2, \ldots, U_m\}$ be the set consisting of m participants in the conference. Each U_i in U, selects a long-term secret key $k_i \in Z_q$ and computes the corresponding public key (point) $Q_i = k_i P \in G$ over the elliptic curve E_q. Moreover, one is only allowed to delete or add the participant set at the beginning of period (session) conference.

Conference key computation and verification phase

Suppose that user U_i initiates the conference. Then, the chairman U_i chooses a random number K as a conference key and encrypts it with U_j's public key Q_j ($j = 1, 2, \ldots, m,\ j \neq i$) in this session, respectively. The detail of this procedure is described as follows.

1. U_i selects a random number r and computes $R = rP = (R_x, R_y)$ and $A_j = rQ_j = rK_jP = (A_jx, A_jy)$ for $j = 1, 2, \ldots, m,\ j \neq i$ over the elliptic curve E_q, where A_jx and A_jy are the x-component and y-component of point A_j, respectively. Similarly, R_x and R_y are the x-component and y-component of point R, respectively. Next, according to the concept of Schnorr's digital signature (Schnorr, 1990), U_i computes $s = r + k_i(K \| R_x \| R_y)$ and $z_j = (K \oplus A_jx \oplus A_jy)$ ($j = 1, 2, \ldots, m,\ j \neq i$) ; it also broadcasts $(R, s, z_1, z_2, \ldots, z_j, \ldots, z_m)$ to each U_j ($j = 1, 2, \ldots, m,\ j \neq i$), where is $Vert$ the concatenation of operations.
2. From the broadcasting information $(R, s, z_1, z_2, \ldots, z_j, \ldots, z_m)$, each participant U_j of U retrieves R, s, z_j, and uses his/her secret key k_j to compute $A_j = k_jR = k_j(rP) = rQ_j = (A_jx, A_jy)$ over the elliptic curve E_q; and recovers the conference session key $K = (z_j \oplus A_jx \oplus A_jy)$. To ensure the validity of session key $K = (z_j \oplus A_jx \oplus A_jy)$, with U_i's public key Q_i and the point R, U_j checks the following equation:

$$sP = R + h\big(K \| R_x \| R_y\big)Q_i. \tag{3}$$

If (3) holds, then K is an accurate conference key distributed from user U_i in this session.

According to the Diffie–Hellman algorithm over elliptic curve (Diffie and Hellman, 1976), for each U_j ($j \neq i$) in U, it provides that $A_j = rQ_j = r(k_jP) = k_j(rP) = k_jR = (A_jx, A_jy)$ over E_q. Hence, any participant U_j of U can accurately derive the common session key $K = (z_j \oplus A_jx \oplus A_jy)$ by means of z_j. The above procedure is briefly illustrated in Fig. 1.

We show the correctness of (1) over the elliptic curve E_q as follows. In the proposed scheme, it has $s = r + k_ih(K \| R_x \| R_y)$, then $sP = rP = k_ih(K \| R_x \| R_y)P = R + h(K \| R_x \| R_y)Q_i$ over the elliptic curve E_q. Therefore, it provides that $sP = R + h(K \| R_x \| R_y)Q_i$.

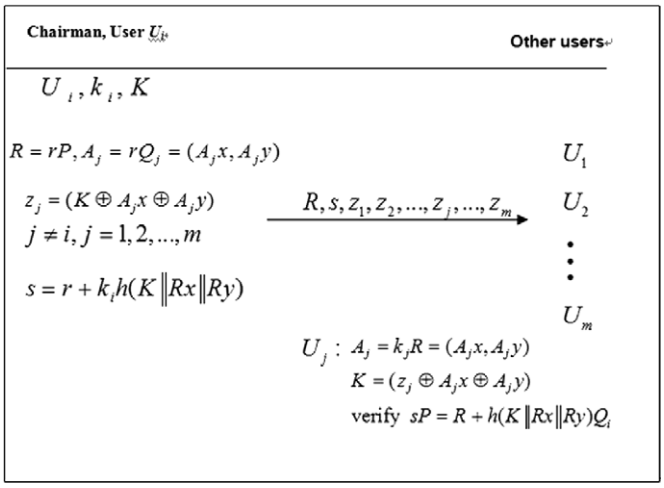

Fig. 1. The proposed scheme.

Therefore, the proposed scheme can provide the non-interactive communication for the common conference key during each session. It could reduce a lot of communication costs for each participant to obtain the common conference key. For the security of the proposed scheme, the random number r and the session key K cannot be reused.

Furthermore, the proposed scheme can easily be implemented in a dynamic conference distribution scheme because all information items from other participants need not be immediately refreshed once the conference adds or deletes a participant. We define the addition and deletion of participants as follows.

Adding a participant. Suppose that a new person U_{m+1} joins the existing participant set $U = \{U_1, U_2, \ldots, U_m\}$ at some period. In the same way, the system (or CA) would first broadcasts the new participant U_{m+1} to the users of $\{U_1, U_2, \ldots, U_m\}$. U_{m+1} also selects a long-term secret key k_{m+1} in Z_q and computes the corresponding public key $Q_{m+1} = k_{m+1}P$ over E_q. Then, all the other participants' information in the system stays the same. Hence, according to the above conference key computation and verification phase, each U_j of $U' = \{U_1, U_2, \ldots, U_m, U_{m+1}\}$ can recover and verify the validity of new common conference key for the future.

Deleting a participant. It is a straight forward process, to delete person U_j in the existing participant set $U = \{U_1, U_2, \ldots, U_n\}$ from some period. At the beginning of period, the system claims that U_j is deleted from a conference and then discards the publication information Q_j. Also, other participants' information in this system is not updated. From the above conference key computation and verification phase, chairman U_i broadcasts new information R, s, and z_a $(a = 1, 2, \ldots, m,\ a \neq j)$ to other participants so that any participant U_a $(a \neq j)$ of U can recover and verify the validity of new common conference key for future session. In other words, none of the chairmen in the new set $U' = \{U_1, U_2, \ldots, U_{j-1}, U_{j+1}, \ldots, U_m\}$ need to compute z_j for U_j from future session.

It is obvious that the proposed scheme can easily add/delete a participant to/from the existing set U.

4. Analysis of the Security and Performance

The security of our proposed method is founded in the difficulty of solving the discrete logarithm problem in E_q, a secure one-way hash function, and the Schnorr's (1990) digital signature. We will review some security terms needed for security analysis (Diffie and Hellman, 1976; Koblitz, 1987; Miller, 1986).

DEFINITION 1. A secure hash function, $h(\ )$:, $x \rightarrow y$, is one-way, if given x, it is easy to compute $h(x) = y$; however, given y, it is hard to compute $h^{-1}(y) = x$.

DEFINITION 2. The elliptic curve discrete logarithm problem (ECDLP) in E_q is as follows: Given $P \in E_q$ with order n (that is $nP = O$) and Q is a point in the cyclic group $G = \langle P \rangle$, it is intractable to find r such that $Q = rP$.

DEFINITION 3. The elliptic curve computational Diffie–Hellman problem (ECDHP) is as follows: Given t_1P and t_2P over elliptic curve E_q, it is hard to compute t_1t_2P for any positive integers t_1 and t_2.

Next, we will discuss the security and performance of our scheme as follows.

4.1. *Security Analysis*

The security of the proposed scheme can be shown as follows:

(1) Security of the participant's secret and the conference key

The security of our proposed method is founded in the difficulty of the elliptic curve discrete logarithm and a one-way hash function. Based on elliptic curve discrete logarithms problem (ECDLP), it is very difficult to obtain any participant's secret key k_i from the corresponding public key $Q_i = k_iP$ over the elliptic curve. Thus, each participant's private key k_i can be kept secret and reused during the span of the system.

By according to the Schnorr's (1990) digital signature, with the secret key k_i, only the participant (chairman) U_i can provide the valid signature $s = r + k_ih(K\|R_x\|R_y)$ resulting that $sP = R + h(K\|R_x\|R_y)Q_i$ holds over the elliptic curve, where $R = rP$. It is under the same the security level of Schnorr's digital signature. Hence, from the broadcasting information $(R, s, z_1, z_2, \ldots, z_j, \ldots, z_m)$, any participant U_j $(j \neq i)$ can retrieve (R, s, z_j) with his/her secret key k_j to compute $A_j = k_jR = rQ_j = (A_jx, A_jy)$ and the common conference key $K = (z_j \oplus A_jx \oplus A_jy)$. Therefore, without knowing r $(R = rP)$ or U_j's secret key k_j, it is very hard for the attacker to derive the common conference key K from the broadcasted data R, Q_j, and z_j. The security is based on the elliptic curve computational Diffie–Hellman problem (ECDHP): For Given $R = rP$ and

$Q_j = k_j P$ over elliptic curve E_q, it is hard to compute $A_j = k_j R = rQ_j = rk_j P$ for any positive integer r and k_j.

(2) The impersonation attack

By applying the concept of Schnorr's signature scheme (Schnorr, 1990), without U_i's private key k_i, anyone cannot forge the signature (R, s) for the conference key K, where $s = r + k_i h(K \| R_x \| R_y)$ and r is a secret random number. Hence, from the broadcasting information $(R, s, z_1, z_2, \ldots, z_j, \ldots, z_m)$, any participant U_j can retrieve (R, s, z_j) and use his/her secret key k_j to compute $A_j = k_j R = rQ_j = (A_j x, A_j y)$ and the common conference key $K = (z_j \oplus A_j x \oplus A_j y)$.

To ensure K is an accurate conference key distributed from user (chairman) U_i in this session, with chairman U_i's public key Q_i and the point R, through signature verification each U_j $(j \neq i)$ checks the equation $sP = R + h(K \| R_x \| R_y) Q_i = sP - R$ holds. Moreover, given s, R, and Q_i, it provides that $h(K \| R_x \| R_y) Q_i = sP - R$. Without the secret key of the chairman, the adversary cannot easily to forge the valid information R, S, and K. The security is based on the Schnorr's signature method. Therefore, the attacker cannot easily masquerade as a legal user to cheat other participants.

Moreover, based on the secure hash function $h(\ )$, it is difficult for the adversary to find the conference key K causing that $h(K \| R_x \| R_y) Q_i = sP - R$. The probability of obtaining the exactly $h(K \| R_x \| R_y) Q_i = sP - R$ is equivalent to performing an exhaustive search on K. Therefore, without knowing r $(R = rP)$ or U_i's secret key k_j, it is very hard for the attacker to derive the common conference key K from the broadcasted data z_j.

Hence, the attacker cannot easily masquerade as a legal user to cheat other participants or obtain the secret information of the conference. The proposed scheme can withstand a impersonation attack.

On the other hand, with the conference key K and the broadcasted data $z_j = (K \oplus A_j x \oplus A_j y)$, the other legal user U_a $(a \neq j)$ can obtain the point $A_j = (A_j x, A_j y) = rk_j P$. However, based on ECDLP, it is very difficult for the legal user U_a $(a \neq j)$ to derive any participant U_j's secret key k_j or the random number r from the point A_j over the elliptic curve.

(3) Replay attack

In addition, the random number r and the session key K are used one time. Therefore, the participant is able to detect whether these messages are valid or not. In this way, a replaying attack can be prevented.

(4) Forward and backward secrecy

Now, if participant U_j leaves the participant set $U = \{U_1, U_2, \ldots, U_m\}$ at some time, then according to the deletion protocol, the chairman don't need to compute the new information z_j for U_j in the future session. In this situation, even if U_j tried to eavesdrop on data transmission, he/she could not decrypt any data with his/her former conference keys for the future. Hence, the proposed conference scheme is secure even if a participant is deleted from the existing participant set. Moreover, since the conference secret keys are randomly picked by the chairman in each session, it is almost impossible for the attacker

to generate other session keys. Even if one secret conference key K is compromised at some session, it is very difficult for the attacker to derive any session key for the past and future. Thus, the proposed scheme can achieve the forward and backward secrecy.

4.2. *Performances*

Based on the RSA cryptography and modular square root (MSR) techniques, Hwang (1999) and Yi *et al.* (2003) proposed conference schemes for mobile communications, respectively. Both of Hwang's and Yi *et al.*'s conference schemes need the conference bridge (trusted center) to distribute the common conference key and several interactive communications are required to generate the common conference key between the conference bridge and each conferee. Therefore, as a result, this causes further communication burden and inconvenience. Moreover, the security of the MSR technique is based on the difficulty of extracting modular square roots of a quadratic residue modulo N (where and are large distinct primes) when and are unknown (Yi *et al.*, 2003). It is computationally infeasible to factor N when and are large enough (typically their length are 512–1024 bits). Obviously, the security of the MSR is similar to that of the RSA cryptography. However, both of Hwang's and Yi *et al.*'s schemes have been shown to be insecure (Wan *et al.*, 2006).

Based on elliptic curve cryptography (ECC), this paper proposes a secure and efficient conference scheme for mobile communications. In the proposed method, the most expensive operation is the point multiplication of the form kP for $k \in z_n^*$ and P is a cyclic group of points over an elliptic curve (Koblitz, 1987; Miller, 1986). Typically, under modulus N, the computation time for a modular exponentiation operation is about $O(|N|)$ modular multiplications, where $|N|$ denotes the bit length of $|N|$. With modulus N, the time for performing one point multiplication over an elliptic curve is approximate to a modular exponentiation computation (Koblitz, 1987; Miller, 1986). Compared to RSA and MSR, ECC can achieve the same level of security with smaller key sizes (Koblitz, 1987; Miller, 1986). Practically speaking, it has been shown that 160-bit ECC provides comparable security to 1024-bit RSA cryptography and 224-bit ECC provides comparable security to 2048-bit RSA cryptography. Therefore, under the same security level, smaller key sizes of ECC could enable faster computational efficiency, as well as memory, energy and bandwidth savings. Due to the merits of ECC, the proposed conference scheme uses 160-bit ECC as the underlying cryptographic infrastructure. Moreover, the proposed scheme does not require the conference bridge (trusted center) to distribute the conference key without any interactive protocols among participants to construct the common conference key for each session. With our method, one can broadcast data so that only authorized participants with proper keys can decrypt the data to obtain useful information. Broadcasting data can save quite a lot of bandwidth over the point-to-point transmission. Hence, it is more suitable for modern computer environment.

By using our way, one requires only the computation of point multiplication expressions kP and kQ_j over elliptic curve. In the proposed scheme, the chairman needs $(m+1)$ point multiplications over elliptic curve. For efficiency's sake, one (any chairman) can use

some storage to store secure (secret) pre-computation such as $\{r_1P, r_2P, \ldots, r_dP\}$ and $\{r_1Q_j, r_2Q_j, \ldots, r_dQ_j\}$ in his/her lookup table, where $j = 1, 2, \ldots, m$. Everyone can construct his lookup table and keep it secretly and update it whenever he/she wants. As these xP and xQ_j are needed for computations, one (chairman) can be immediately retrieved from the lookup table so that the computation is performed faster. For example, given $x = r_1+2r_3$, the chairman U_i wants to obtain xP and xQ_j, then he/she can retrieve these values $\{r_1P, r_3P\}$ and $\{r_1Q_j, r_3Q_j\}$ for $j = 1, 2, \ldots, m$ from his/her lookup table resulting the value $xP = r_1P + r_3P + r_3P$ and $xQ_j = r_1Q_j + r_3Q_j + r_3Q_j$ are computed. In this situation, the chairman U_i requires only $2m$ point additions for the proposed scheme.

On the other hand, from the broadcasting data, it is only required three point multiplications for any participant U_j in set the U to derive and verify the accurate conference key distributed from the chairman U_i. Therefore, it can save on communication and computation overhead. It is better suited for resource constrained devices. In addition, since all public items of other participants in a conference need not be immediately refreshed once a participant is added or deleted, the proposed scheme can be easily implemented in a dynamic conference scheme.

5. Conclusions

For the limited computing capability in a mobile user's portable device, based on elliptic curve cryptography (ECC), this paper presents a secure and efficient conference scheme for mobile communication. In the proposed scheme, no conference bridge (or trusted center) is required, each legal participant can initiate the conference and distribute the common conference key without any interactive communication; thus, it can save on communication overhead In addition, the proposed scheme has the following properties.

(1) The Conference key computation and verification algorithm are quite simple and efficient.
(2) It can be easily implemented into a dynamic conference system for mobile communication because other participants' information pieces in the system don't need to be immediately updated once a participant is added or deleted.
(3) Once a participant leaves the conference, he/she could not decrypt the data with his/her former conference keys for future periods.

Acknowledgment. The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation. This research was partially supported by the National Science Council, Taiwan, under contract No. NSC-99-2221-E-025-003.

References

Berkovits (1991). How to broadcast a secret. In: *Proceedings Advances in Cryptology-Eurocrypt'91*, pp. 535–541.

Beller, M.J., Chang, L.F., Yacobi, Y. (1993). Privacy and authentication on a portable communication system. *IEEE Journal on Selected Areas Communication*, 11, 821–829.

Chang, C.C., Wu, T.C., Chen, C.P. (1992). The design of a conference key distribution system. In: *Proceedings Advances in Cryptology (Auscrypt'92)*, pp. 459–466.

Diffie, W., Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory (IT-22)*, 644–654.

Hwang, M.S. (1999). Dynamic participation in a secure conference scheme for mobile communications. *IEEE Transactions on Vehicular Technology Technology*, 48, 1469–1474.

Hwang, M.S., Yang, W.P. (1995). Conference key distribution schemes for secure digital mobile communications. *IEEE Journal on Selected Areas in Communications*, 13(2), 416–420.

Ingemarsson, I., Tang, D.T., Wong, C.K. (1982). A conference key distribution system. *IEEE Transactions on Information Theory*, 28(5), 714–720.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48, 203–209.

Kumanduri, R. (1998). *Number Theory with Computer Applications*. Prentice Hall, Upper Saddle River, No. 07458, pp. 479–508.

Lu, R., Cao, Z. (2006). Off-line password guessing attack on an efficient key agreement protocol for secure authentication. *International Journal of Network Security*, 3(1), 35–38.

Miller, V. (1986). Uses of elliptic curves in cryptography. In: *Advances in Cryptology (Crypto'85), Lecture Notes in Computer Science*, Vol. 218. Springer, Berlin, pp. 417–426.

Ng, S.L. (2001). Comments on dynamic participation in a secure conference scheme for mobile communications. *IEEE Transaction on Vehicular Technology*, 50, 334–335.

Steer, D., Strawczynski, L., Diffie, W., Wiener, M. (1990). A secure audio teleconference system. In: *Proceedings Advances in Cryptology (Crypto'88)*, pp. 520–528.

Schnorr, C.P. (1990). Efficient identification and signatures for smart cards. *Lecture Notes in Computer Science*, Vol. 435, *Advances in Cryptology (Crypto'89)*. Springer, Berlin, pp. 339–351.

Sui, A., Hui, L., Yiu, S., Chow, K., Tsang, W., Chong, C., Pun, K., Chan, H. (2005). An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication. *IEEE Wireless and Communications and Networking Conference (WCNC 2005)*, pp. 2088–2093.

Tseng, Y.M., Jan, J.K. (1999). Anonymous conference key distribution systems based on the discrete logarithm problem. *Computer Communications*, 22, 749–754.

Tzeng, W.G. (2002). A secure fault-tolerant conference-key agreement protocol. *IEEE Transactions on Computers*, 51(4), 373–379.

Wan, Z., Bao, F., Deng, R.H., Ananda, L. (2006). Security analysis on a conference scheme for mobile communications. *IEEE Transactions on Wireless Communication*, 5(6), 1238–1240.

Yi, X., Siew, C.K., Tan, C.H. (2003). A secure and efficient conference scheme for mobile communications. *IEEE Transaction on Vehicular Technology*, 52(4), 784–793.

3GPP2 N.S001 vl.0, OTASP and OTAPA. Available at : `http://www.3gpp2.org`. Jan. 1999.

3GPP2 C.S0016-B vl.0, Over-the-Air Service Provisioning of mobile stations in spread spectrum standards. Available at: `http//www.3gpp2.org`. Oct. 2002.

D.-C. Lou was born in Chiayi, Taiwan, Republic of China, on March 18, 1961. He received the BS degree from Chung Cheng Institute of Technology (CCIT), National Defense University, Taiwan, R.O.C., in 1987 and the MS degree from National Sun Yat-Sen University, Taiwan, R.O.C., in 1991, both in electrical engineering. He received the PhD degree in 1997 from the Department of Computer Science and Information Engineering at National Chung Cheng University, Taiwan, R.O.C. He was an assistant, lecturer, associate professor, and professor with the Department of Electrical Engineering at CCIT, from 1987 to 2009. He had served as director of Computer Center of CCIT from 2004 to 2006. Currently, he is a professor with the Department of Computer Science and Information Engineering, Chang Gung University. His research interests include multimedia security, steganography, cryptography, computer arithmetic, and distributed system.

K.-C. Liu received the MSc degree in microbiology from National Taiwan University, Taiwan and PhD degree from the Graduate Institute of Biotechnology in National Chung Hsing University, Taiwan, respectively. Currently, he is an assistant professor at the Department of Medical Laboratory Science and Biotechnology in China Medical University. His research interests focus on the areas of biotechnology and healthcare.

H.-F. Huang received her PhD degree in computer science and information engineering from National Chung Cheng University. Her first degree is bachelor of mathematics from Fu Jen Catholic University and master of mathematics from National Taiwan University. Currently, she is a professor at the Department of Computer Science and Information Engineering in National Taichung University of Science and Technology. Her research interests focus on the areas of cryptography and information security, network security, algorithm, and electronic commerce etc.

Efektyvi belaidžio ryšio mobiliųjų konferencijų schema

Der-Chyuan LOU, Kuo-Ching LIU, Hui-Feng HUANG

Technologiniai pasiekimai leidžia visiems konferencijos dalyviams dalyvauti belaidžio ryšio mobiliojoje konferencijoje. Projektuojant belaidžio ryšio mobiliųjų konferencijų schemą, būtina atsižvelgti į tai, jog dalyviai paprastai naudoja ribotų skaičiavimo galimybių nešiojamuosius įrenginius. Straipsnyje pasiūlyta mobiliojo slapto ryšio schema grįsta elipsinių kreivių kriptografija, kuri įgalina dalyvį prie konferencijos prisijungti arba atsijungti dinamiškai. Nereikalingas joks interaktyvus vartotojų bendrojo rakto suformavimo protokolas.