Transactions Papers

An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks

Chin-Chen Chang, *Fellow, IEEE*, and Hao-Chuan Tsai

***Abstract*—Increasing numbers of mobile users are being allowed to use wireless networks, and universal access is being promoted. In the absent of a single, trusted authentication server, it is a great challenge to ensure the inter-domain security, which makes it feasible for users to migrate into foreign domains. Thus, an authentication mechanism is needed between mobile users and foreign servers, and an authenticated key also is highly desirable to support secure communications in wireless networks. In addition, maintaining the anonymity of users is an important security requirement, such as the information about customers's behaviors. Recent research has focused on these issues and has provided definitions and some constructions. Importantly, Tang and Wu proposed an efficient mobile authentication scheme, which they called ''Efficient Mobilization Authentication Scheme" (EMAS), which enjoys both computational efficiency and communication efficiency that exceed the efficiencies of other recent mobile authentication schemes. Unfortunately, we found out that Tang and Wu's scheme does not meet the basic security requirements. Therefore, to develop a more acceptable mobile authentication scheme, we propose a self-verified mobile authentication scheme that has a novel architecture. To provide the better computation efficiency and storage efficiency, our scheme does not require of long-term secret keys on the servers.**

***Index Terms*—Self-verified, mobile authentication, anonymous, key agreement, scalable, wireless networks.**

I. INTRODUCTION

USER mobility is highly desirable feature in the development of computer networks and telecommunication systems, especially in wireless networks. In one scenario, mobile users who initially subscribed to their home networks can travel to other networks with different operations and access services. This cellular network [1], [16] allows mobile users the advantage of accessing services without geographical limitations. To provide such service, a visited network must authenticate mobile users who originally subscribed to their own home networks. However, authentication in this type of network is a great challenge, since there is no trusted authentication server available to both the mobile users and the visited foreign server they may visit. In addition, it is essential for mobile users to authenticate the visited foreign server they visit. Previously proposed schemes [9], [13], [20] support the authentication of mobile users by a foreign server, but they do not support the authentication of the foreign server by the mobile users. As a result of this incomplete property, a potential problem exists. Let us consider the following scenario, *i.e.*, different foreign servers may provide services for different charge. Mobile users should be allowed to choose a specific foreign server to obtain the services they need. Hence, from a practical perspective, mutual authentication is important and should be provided to both mobile users and the visited foreign servers. Generally, two mechanisms are used to meet the security requirements for mobile authentication. The first mechanism consists of the use of symmetric key based schemes [19], [21], such as Kerberos [17]. Although these schemes are efficient and achieve mutual authentication of mobile users and the networks they visit, they are vulnerable to denial-of-service attacks and deposit attacks [22]. Hence, this mechanism does not provide the best authentication strategy for wireless networks. The second for mobile authentication in wireless networks [4], [8], [11], [14], [19] that is widely is the application of public-key cryptosystems [18]. The primary advantage of using public-key cryptosystems for mobile authentication is that the public-key cryptosystems have more robust security properties in communications than those of a single symmetric key.

In addition to the mutual authentication, it is also highly desirable to provide mobile users anonymity with respect to the adversaries as well as the foreign server. Unless the identity information is imperative in some emergency situations or special applications, the foreign server is only allowed to ensure the legitimate, rather than the real, identity of mobile users. This is because any illegal, undetected access to mobile users's location can be a critical violation of users's personal privacy. Hence, the anonymity of identity is a required

Manuscript received January 11, 2009; revised November 16, 2009; accepted May 5, 2010. The associate editor coordinating the review of this paper and approving it for publication was D. Zeghlache.

C.-C. Chang is with the Department of Computer Science and Information Engineering, Feng Chia University, Taichung, Taiwan, R.O.C, 40726 (e-mail: ccc@cs.ccu.edu.tw).

H.-C. Tsai is with the Department of the Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan, R.O.C, 6210.

Digital Object Identifier 10.1109/TWC.2010.092410.090022

property that must be incorporated in the design of a secure roaming scheme. Many studies have been proposed in the past decade [3], [8], [11], [14], [22], [23] to achieve these security requirements. Recently, Tang and Wu [20] proposed an efficient mobile authentication scheme, named EMAS, based on an elliptic curve discrete logarithm problem [12]. In EMAS, mobile users pre-share a secret with their home server via a trust delegation. The visited foreign server can verify the validity of mobile users based on a public certificate published by the home server, and, then, the visited foreign server can grant the communication key to mobile users. Compared with similar, existing schemes [14], [23], EMAS only requires two messages on a mobile user, or three messages in 3GPP Authentication and Key Agreement (AKA) [2]. This can provide mobile users and their home server synchronization in advance. Therefore, Tang and Wu claimed that their scheme can achieve both computational efficiency and communication efficiency. Unfortunately, according to our observation, some weaknesses, such as the scalability is not evident and personal privacy is still not protected in Tang and Wu's scheme.

To eliminate these weaknesses, we propose a new version with novel architectures. Our contribution in this paper includes a novel self-verified mobile authentication scheme, which provides both computational efficiency and communication efficiency. The security of the proposed mobile authentication scheme is based on elliptic curve cryptography. Although it involves more complicated operations than those of the bare symmetric key based schemes, the proposed scheme is still suitable for the implementation, since in actuality, fast scalar point multiplication algorithms [7], [10] exist in the elliptic curve cryptography. Hence, such complicated computations can be easily supported by the use of extra hardware equipment for wire-line communication servers. More importantly, compared with the previous public-key cryptosystems, the merit of elliptic curve cryptography arises from the fact that a strong level of security can be achieved with considerably shorter key length than in methods that are based on the difficulties of solving large integer factorizations or discrete logarithms over integers, such as RSA [18] or ElGlmal algorithms [5]. The proposed scheme has the following attractive characteristics:

(1). A mobile user and the communication entities can be authentic, that is, the mutual authentication can be achieved for a mobile user, a visited foreign server and the mobile user's home server.

(2). A session key assisted by the home server is available only to mobile communication users and the visited foreign servers, and such a session key would not be revealed to either the uninvolved servers or others.

(3). Unlike similar previous scheme, the computational load of mobile users is reducing by diverting the most complicated operations to either the home server or the visited foreign server, avoiding the imposition of a heavy burden on the mobile users.

(4). The risk of compromising the secret information stored on the home server is reduced; Avoiding the need for the home server to maintain these stored secrets makes the home server scaleable when it must manage a large number of mobile users.

(5). The privacy of mobile users' information is provided, and, compared with the previous schemes, computational efficiency and communication round efficiencies can be ensured for both communication entities.

The rest of this paper is organized as follows. In Section II, we briefly introduce the background and related works. In Section III, we propose the enhanced scheme with a novel architecture. Next, the security properties and the performance issues are given in Section IV and Section V, respectively. Finally, our conclusions are presented in Section VI.

II. Security and Weaknesses of the Efficient Mobile Authentication

Traditional wireless mobile application of AAA provides authentication, authorization, and accounting services to mobile users. However, the wireless application is unable to support mutual authentication and key establishment for mobile users. To provide better security, Lee and Yeh [14] proposed an improved authentication protocol in terms of data security, user privacy, and computational load. Unfortunately, Lee and Yeh's protocol is susceptible to a false base-station attack [20]. Independently, Jiang *et al.* [11] proposed a version that was simpler and more robust than similar protocols that had been developed previously. However, for the mobile users, their protocol still has a heavy computational load and is inefficient in the storage rate. Compared with the traditional, public-key cryptosystems, elliptic curve cryptography (ECC) provides a good solution in terms of key size, computational efficiency, and communication efficiency. Hence, Tang and Wu [20] recently proposed an efficient mobile authentication scheme based on ECC, named EMAS, which involves three main protocols, i.e., trust delegation initialization, efficient mobile authentication, and home server off-line authentication. We now describe the weaknesses that exist in Tang and Wu's scheme.

A. Scalability is Deficient

In communication networks, scalability is a desirable property of systems, which indicates the ability of the systems to either process increasing workloads in a graceful manner or to be readily enlarged. In the trusted delegation initialization of Tang and Wu's scheme, each mobile user is associated with a secret delegation key σ which is shared with his home server. The main use of these secret delegation keys is to achieve mutual authentication between mobile users and a home server. It is trivial for a mobile user to protect his delegation key. However, the number of shared delegation keys that a home server must protect in directly related to the number of communicating mobile users. For example, if a million mobile users register with a specific home server, the home server must securely maintain these secret delegation keys. This is a significant challenge for home servers since they may also be the targets of attacks by adversaries. Hence, according to our observation, the scalability of Tang and Wu's scheme is deficient.

B. Confidentiality of a Session Key is Improper

Entity authentication and key establishment mechanisms are usually integrated as a single protocol. This is because an authentication protocol only provides authenticity between the intended parties, and, after the protocol has been completed, the intended communicating parties should establish a secret session key to protect the messages to be exchanged later. In addition, Mitchell *et al.* [15] pointed out that, as the security consideration, the established session key should not be controlled or chosen solely by any single one of the two communicating parties for the security requirement. Without this property, one party may be induced to force the use of an old key. However, in Tang and Wu's scheme, the session key ck is generated by the mobile user rather than through negotiation with a foreign server. In particular, for personal privacy, the home server should be not allowed to obtain the session key. Unfortunately, the session key, which is generated by the mobile user, will be encrypted by the secret delegation key , and then be transmitted to the home server. It is trivial to observe that the home server can also obtain the session key which should be known only by the mobile user and the foreign server. Hence, Tang and Wu's scheme does not provide a good key establishment property.

III. The Proposed Mobile Authentication Scheme

We first consider the various communications models in which the proposed scheme will primarily be used. Let π be a system security parameter. The entire system can be categorized into two entities, $i.e.$, the mobile user entity set $U(\pi)$=$\{U_1$,U_2,$\cdots$,$U_{Q_1(\pi)}\}$ and server network entity set $S(\pi)$=$\{S_1$,S_2,$\cdots$,$S_{Q_2(\pi)}\}$ with large capacities and powerful computational operations, where Q_1 and Q_2 are two polynomials and each element in the sets is the corresponding identities. Different from the previous schemes, in our scheme, we assume that the elements of the server entity are associated only with a public key pair of an asymmetric encryption scheme or a signature scheme. Each mobile user, called U_a $\in U(\pi)$, belongs to a specific server $S_h \in S(\pi)$ meaning that S_h is said to be the home server of U_a if $f(U_a) = S_h$ for a computable function $f(\cdot)$ and S_v is a foreign server of U_a for all v different from h. To provide anonymity of mobile users, note that only the home server has the privilege of accessing the real identity of mobile users, and, compared with the mobile user entity, elements in the server network entity are much less than those in the mobile user entity. Hence, we assume that S_h and S_v share a long-term secret key K_{hv} under restricted protection for all $h, v \in Q_2(\pi)$, and $h \neq v$. In addition, we define and extend the trust models which are generalizations of Tang and Wu [20]. No mutual trust relationship is established between any two end entities; this means that the mobile users cannot trust the visiting foreign servers without verifying and vice versa. Likewise, no trust relationship exists between the foreign servers and the home servers. In the proposed scheme, it is reasonable to assume that the home server is trustworthy because we must register it to obtain the server. Hence, the mobile users can only trust the home servers even though no direction communications is available between them resorting with proper authentication. And in this paper, we assume that each mobile user can obtain all the servers' identities.

We now propose a novel mobile authentication scheme to construct the authentication between mobile users and visited foreign servers. The proposed scheme is composed of two phases, $i.e.$, the self-verified trust delegation and self-verified mobile authentication phases. Before demonstrating the proposed scheme, the security parameters must be initialized by the system as follows. First, the system chooses a finite field F_p over a large odd prime number p, and then, defines an elliptic curve equation $E_p(a, b)$:y^2=$x^3 + ax + b \bmod p$ with the prime order q over F_p, for the chosen $a, b \in F_p$ which satisfy the equation $4a^3 + 27b^2 \neq 0$ [7]. Finally, the system chooses a base point G with the prime order q over $E_p(a, b)$ and publishes $E_p(a, b)$ and G.

In the following, we describe the self-verified trust delegation and self-verified mobile authentication phases, respectively.

A. Self-verified Trust Delegation phase

For a mobile user U_a, initially, the home network S_h performs the following steps only once: S_h chooses a private key $x_{S_h}$$\in$$Z_q^*$ and computes the public key $Y_{S_h} = x_{S_h} * G$. To provide anonymity and reversibility for mobile users, S_h generates the unique master secret δ_{U_a} by calculating the equation $h(x_{S_h}, S_h)$=$h(U_a, S_h)$$\cdot$$\delta_{U_a}$ mod q, where $h(\cdot)$:$\{0, 1\}^*$$\rightarrow$$\{0, 1\}^l$ denotes a strong cryptographic, collision-free, hash function and behaves like random oracles [3]. To generate the authentication token, S_h calculates γ_{U_a}=$\delta_{U_a} * G$=(x_{U_a}, y_{U_a}), and $c = x_{U_a}$ mod q. Also, S_h calculates the self-verified, signature-like equations as follows: $e_{U_a} = h(c, U_a)$ and $s_{U_a} = \delta_{U_a} - x_{U_a} * G$ mod q. After that, S_h computes $h(\delta_{U_a} \| S_h)$ as the master delegation key and securely delivers the computed result along with (e_{U_a}, s_{U_a}) to the mobile user U_a for future authentication. Eventually,S_h destroys all of the secret information except for S_h's private key x_{S_h}. This means the private key x_{S_h} must be strictly protected. After receiving these messages, the mobile user U_a computes γ'_{U_a}=$s_{U_a} * G + Y_{S_h} * e_{U_a}$=$(x'_{U_a}, y'_{U_a})$, and $c' = x'_{U_a}$ mod q in order to ensure the integrity of the delegation key. In addition, he or she also computes $e'_{U_a} = h(c', U_a)$ and, if the computed result is equal to the received e_{U_a}, U_a accepts the master delegation key $h(\delta_{U_a} \| S_h)$.

It is worth noting that, if the secrets are generated by the home network S_h for which the public key is Y_{S_h}, U_a can verify the secrets successfully since $\gamma'_{U_a} = s_{U_a} * G + Y_{S_h} * e_{U_a} = s_{U_a} * G + x_{S_h} * G * e_{U_a} = (s_{U_a} + x_{S_h} * e_{U_a}) * G = \delta_{U_a} - x_{S_h} * e_{U_a} + x_{S_h} * e_{U_a} = \delta_{U_a} * G = \gamma_{U_a}$. To decrease the probability that $(e_{U_a}$, $s_{U_a})$ are replaced or compromised by an adversary, U_a also encrypts $[e_{U_a}, s_{U_a}]_{Y_{S_h}}$ by using the public key Y_{S_h} and stores them for future authentication. This additional procedure does not increase the heavy burden of U_a in terms of storage efficiency and computational overhead because U_a needs to encrypt them only one time rather than encrypts them for each session, and stores $[e_{U_a}, s_{U_a}]_{Y_{S_h}}$ instead of $(e_{U_a}$, $s_{U_a})$.

B. Self-verified Mobile Authentication Phase

Initially, the user U_a chooses an element $k_1$$\in_R$$Z_q^*$ and computes κ=$k_1 * G$. Next, U_a uses the master secret delegation key $h(\delta_{U_a} \| S_h)$ to generate a certificate $E_{h(\delta_{U_a} \| S_h)}[U_a, S_v, \kappa, ts]$, where $E_X[m]$ denotes that the message m is encrypted using key X and ts is the current timestamp, respectively. And then, U_a sends the items $\{[e_{U_a}, s_{U_a}]_{Y_{S_h}}, E_{h(\delta_{U_a}\|S_h)}[U_a, S_v, \kappa, ts], h(\kappa, ts)\}$ along with the identity of S_h to the visited foreign server $S_v \in S(\pi)$ for $S_v \neq S_h$. After receiving the messages from U_a, S_v generates an element $k_2 \in_R Z_q^*$ and computes $\lambda = k_2 * G$. In addition, according to the received identity of S_h, S_v applies the long-term secret key K_{hv} with S_h to encrypt a certificate $E_{K_{hv}}(h(\kappa, ts)\|\lambda)$ and retransmits the item $E_{h(\delta_{U_a}\|S_h)}[U_a, S_v, \kappa, ts]$ and $[e_{U_a}, s_{U_a}]_{Y_{S_h}}$ to the corresponding home network S_h. To authenticate both the mobile user and the foreign server, in this stage, S_h initially decrypts $[e_{U_a}, s_{U_a}]_{Y_{S_h}}$ and then uses the decrypted (e_{U_a}, s_{U_a}) and the private key x_{S_h} to compute $\delta'_{U_a} = s_{U_a} + x_{S_h} * e_{U_a} \bmod q$, and to recover the master delegation key $h(\delta'_{U_a}\|S_h)$. Next, S_h decrypts the item $E_{h(\delta_{U_a}\|S_h)}[U_a, S_v, \kappa, ts]$ to retrieve all encrypted items by U_a. Also, S_h computes $\gamma'_{U_a} = \delta'_{U_a} * G = (x'_{U_a}, y'_{U_a})$ and $c' = x'_{U_a} \bmod q$. Then, S_h utilizes the computed c' and the retrieved identity U_a to calculate $h(c', U_a)$. If the computed result is equal to the received e_{U_a}, and the retrieved timestamp ts is under the reasonable threshold, S_h successfully authenticates the mobile user U_a. In addition to this, S_h uses the previous decrypted message, which provides the identity of the visited foreign server S_v, to retrieve the pre-shared secret key K_{hv}, and to decrypt the message $E_{K_{hv}}(h(\kappa, ts)\|\lambda)$. Finally, S_h computes $h(\kappa, ts)$ and compares the computed result with the first item of the decrypted message. If it holds, S_h successfully authenticates the visited foreign server S_v. Before returning the messages to S_v, S_h generates a small positive element N to compute an ephemeral master key $EMK = h^N(h(\delta_{U_a}\|S_h)\|S_v\|ts)$, which can also be seen as the temporary identity of U_a, between the mobile user U_a and the visited foreign server S_v. Eventually, S_h sends the encrypted results $E_{h(\delta\|S_h)}(\kappa, \lambda, N)$, $E_{K_{hv}}(EMK, \kappa, \lambda, ts)$ to S_v. S_v decrypts $E_{K_{hv}}(EMK, \kappa, \lambda, ts)$ to retrieve the second item of the decrypted message and to compute $h(\kappa, ts)$. If the computed result equals $h(\kappa, ts)$ that was previously received from U_a, S_v successfully authenticates both U_a and S_h, and retransmits $E_{h(\delta\|S_h)}(\kappa, \lambda, N)$ to U_a. It is worth noting that the session key can be established as the form $sk = h(k_2 * \kappa, S_v, ts) = h(k_1 * k_2 * G, S_v, ts)$. After receiving messages from S_v, U_a uses the master delegation key to decrypt it to check whether the decrypted $\kappa' = k_1 * G$ equals the initially generated result. If U_a verifies this procedure successfully, U_a authenticates S_v and establishes the session key $sk = h(k_1 * \lambda, S_v, ts) = h(k_1 * k_2 * G, S_v, ts)$ for protecting later communications with S_v. The flowchart of self-verified mobile authentication phase can be summarized in Fig. 1.

As a special scenario, consider the authentication phase when mobile user U_a is still located in the visited foreign server S_v for successive sessions. It is inefficient for S_v to authenticate U_a and to establish session keys resorting to the home server S_h. To deal with this scenario, we propose an additional one-time authentication phase. The primary feature of this phase is that the mobile user U_a is allowed to frequently renew session keys with the visited foreign server S_v. The advantage of renewing the session key is that, the mobile user can reduce the risk of a compromised session key for communicating with the visited foreign server. Assume that U_a has completed the self-verified mobile authentication process and has obtained the enough information to compute the ephemeral master key. After being authenticated by S_v, for the first time, U_a needs to communicate with S_v for the i^{th} session. He initially generates an element $k_{U_i} \in_R Z_q^*$ and then uses the portion of previous session key to compute $h(k_{U_{i-1}} * k_{S_{i-1}} * G) \oplus h^{N-i-2}(h(\delta_{U_a}\|S_h)\|S_v\|ts)$ and $k_i * G, h(k_i * G, h^{N-i}(\delta_{U_a}\|S_h)\|S_v\|ts))$. Next, U_a sends these computed results to S_v. And then, S_v uses $h(k_{U_{i-1}} * k_{S_{i-1}} * G)$ to retrieve $h^{N-i-2}(\delta_{U_a}\|S_h)\|S_v\|ts)$ and to compute $h^2(h^{N-i-2}(\delta_{U_a}\|S_h)\|S_v\|ts))$. If the computed result equals the ephemeral master key $h^{N-i-2}(\delta_{U_a}\|S_h)\|S_v\|ts)$, S_v successfully authenticates U_a. In addition, to ensuring the integrity of $k_{U_i} * G$, S_v uses the ephemeral master key to compute $h(k_i * G, h^{N-i}(\delta_{U_a}\|S_h)\|S_v\|ts))$ which is used for comparison with the received item. If it holds, S_v generates an element $k_{S_i} \in_R Z_q^*$ and computes $k_{S_i} * G, h^{N-i-1}(h(\delta_{U_a}\|S_h)\|S_v\|ts) \oplus h(k_{U_i} * k_{S_i} * G)$. Finally, S_v sends these computed results to U_a. And then, U_a can use the master delegation key to compute $h^{N-i-1}(h(\delta_{U_a}\|S_h)\|S_v\|ts)$ and to verify the integrity of the transcript $k_{S_i} * G$. If the verification succeeds, U_a successfully authenticates S_v. Note that the session key will be established in the form of $h(k_{U_i} * k_{S_i} * G, k_{U_i} * G, k_{S_i} * G, ts)$. for both communicating parties, and, no encryption or decryption operations are involved in this session key renewal phase. It is worth noting that after successfully establishing the session key, S_v will replace the ephemeral master key $h^{N-i}(h(\delta_{U_a}\|S_h)\|S_v\|ts)$ with $h^{N-i-1}(h(\delta_{U_a}\|S_h)\|S_v\|ts)$ for further authentication. The flowchart of one-time mobile authentication phase can be summarized in Fig. 2.

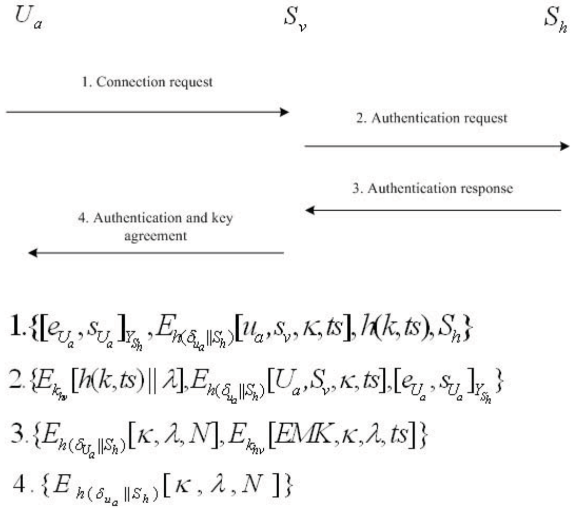

U_a
S_v
S_h
1. Connection request
2. Authentication request
3. Authentication response
4. Authentication and key agreement
$1.\{[e_{U_a}, s_{U_a}]_{Y_{S_h}}, E_{h(\delta_{u_a}\|S_h)}[u_a, s_v, \kappa, ts], h(k, ts), S_h\}$
$2.\{E_{k_{hv}}[h(k, ts)\| \lambda], E_{h(\delta_{u_a}\|S_h)}[U_a, S_v, \kappa, ts], [e_{U_a}, s_{U_a}]_{Y_{S_h}}\}$
$3.\{E_{h(\delta_{U_a}\|S_h)}[\kappa, \lambda, N], E_{k_{hv}}[EMK, \kappa, \lambda, ts]\}$
$4.\{E_{h(\delta_{u_a}\|S_h)}[\kappa, \lambda, N]\}$

Fig. 1. Self-verified mobile authentication process.

IV. Security Analysis and Discussions

Before demonstrating the security analysis, we first depict the security basis on which the security of proposed scheme relies.

DEFINITION 1. Elliptic Curve Discrete Logarithm Assumption: Let E be an elliptic curve over a finite field F_p with a prime order q, where the operation is denoted multiplicatively.

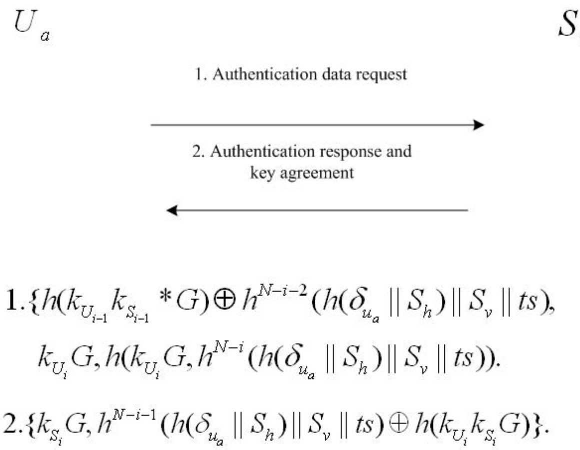

U_a
S_v
1. Authentication data request
2. Authentication response and key agreement
$1.\{h(k_{U_{i-1}}k_{S_{i-1}} * G) \oplus h^{N-i-2}(h(\delta_{u_a} \| S_h) \| S_v \| ts),$
$k_{U_i}G, h(k_{U_i}G, h^{N-i}(h(\delta_{u_a} \| S_h) \| S_v \| ts)).$
$2.\{k_{S_i}G, h^{N-i-1}(h(\delta_{u_a} \| S_h) \| S_v \| ts) \oplus h(k_{U_i}k_{S_i}G)\}.$

Fig. 2. One-time mobile authentication process.

Suppose that G is a base point over $E(F_p)$, and that a (t, ϵ)–ECDL attacker in $E(F_p)$ is a probabilistic Turing machine Δ running in time t such that $Succ_G^{ecdl}(\Delta)$=Pr[$\Delta(aG, bG) = abG$]$\geq$ ϵ, where the probability is taken over the random values a and b. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is (t, ϵ)–intractable if there exists no (t, ϵ)–attacker in $E(F_p)$. The Elliptic Curve Discrete Logarithm Assumption is the case for all polynomial t and any non-negligible ϵ.

Theorem 1. Let us consider the proposed self-verified mobile authentication scheme, in which the encryption key size N is equipped with a uniform distribution. Let A be an adversary against the Authenticated Key Exchange (AKE) security of the proposed scheme within a time bound t, with less than q_s interactions with the communication entities, also asking q_h hash-queries, and q_E encryption/decryption queries. Then

$$Adv_P^S(A) \leq \frac{2q_E^2+q_s^2}{2(q-1)} + \frac{q_s^2}{2^l} + \frac{q_E+q_s}{q-1} + \frac{q_s}{2N} + (q_h+q_E)Succ_G^{ecdl}(t'),$$

where $t' \leq t + (q_s + q_E)\tau_G$ and τ_G denotes the computational time for a multiplication in G with order q.

A. More Discussions

1) Identity Anonymity and Untraceability Analysis: As explained above, the real identity of the mobile user U_a, is encrypted by the master delegation key. Since only the home server S_h can derive the master delegation key, it is implied that no one except S_h can obtain the real identity. In addition, an illegitimate tracker cannot trace the location of a targeted mobile user. The property of this untraceability can be ensured by the above mentioned reason. When a mobile user moves to different visited foreign networks, the foreign server authenticates a mobile user by using the ephemeral master key EMK=$h^N(h(\delta_{U_a} \| S_h) \| S_v \| ts)$, which is computed by the home server. This ephemeral master key, which can be seen as the temporary identity of a mobile user, is different in each foreign server and is dynamically updated so that there is no direction relationship among these ephemeral master keys. Hence, it is infeasible for an illegitimate tracker to trace the location of a mobile user in different roaming domains.

2) Prevention of Impersonation Attacks: Without loss of generality, three impersonation attack scenarios can be considered in the proposed scheme, i.e., an adversary impersonates the home server, a visited foreign server, and a mobile user. Herein, we explain that these attacks cannot be performed successfully in the proposed scheme as follows. (1). If an adversary wants to impersonate the home server to cheat a foreign server, he must produce the responding confirmation $E_{K_{hv}}(\kappa, \lambda, ts)$ which implies that an adversary processes the long-term secret key K_{hv}. In addition, to be verified by a foreign server, an adversary still must compute the master delegation key $h(\delta_{U_a} \| S_h)$ to derive the legitimate ephemeral master key. Hence, an adversary cannot impersonate the home server. (2). An adversary, which is an uninvolved malicious foreign server, cannot impersonate the home server to cheat a mobile user. Since the master delegation key is only derived by the home server, it is computationally infeasible to calculate the legitimate ephemeral key $h^N(h(\delta_{U_a} \| S_h) \| S_v \| ts)$ that contains $h(\delta_{U_a} \| S_h)$, which was generated by the real home server. (3). Since the real identity is unknown to an adversary, he can forge a fake identity ID_f to impersonate a mobile user. However, he still must compromise $h(\delta_{U_a} \| S_h)$ from the transmitted items $[e_{U_a}, s_{U_a}]_{Y_{S_h}}$ which is equivalent to solve an instance of the elliptic curve discrete logarithm problem.

3) Nonrepudiation: Nonrepudiation is a major requirement for a system with many principals and mobility support. In our proposed scheme, each mobile user U_a obtains a different pair certificate-like item (e_{U_a}, s_{U_a}) from the home server S_h in the self-verified trust delegation phase. The certificate-like item implies the authorization from S_h. According this authorization, the visited foreign server S_v transfers his trust in S_h to the requested anonymous U_a. Since only S_h has the ability to authenticate U_a on his behavior, if S_h authenticates U_a successfully, that means the unique certificate-like item (e_{U_a}, s_{U_a}) has been verified and the corresponding messages are encrypted by the master delegation key. U_a is unable to repudiate resource usage at a visited domain because the home server has generated the corresponding information to the mobile user U_a. Similarly, the mobile user has transmitted the verified token $h(\kappa, ts)$ and S_v also generates the corresponding message $E_{K_{hv}}(h(\kappa, ts) \| \lambda)$, if the authentication is verified successfully, the home server will generate the message related to the ephemeral master key to S_v. Since the mobile user will also compute the same ephemeral master key, S_v cannot wrongly claim resource usage by the mobile user. Thus, our proposed scheme can also provide the property of nonrepudiation.

4) Key Management: In the traditional public-key cryptosystem based schemes, the verification of the mobile users depends on the public key of the mobile users. Unfortunately, it is not easy to achieve this feature in practical when the mobile users are linear increasing in the system; the complexity of the public-key infrastructure (PKI) will be complicated. In our proposed scheme, the home server authorizes the mobile users according to the certificate-like item (e_{U_a}, s_{U_a}). The home server can recover the master delegation key from it with his protected private key. Hence, the home server does not need to manage a lot of public keys of the mobile users. Simultaneously, the number of servers is much less than that of mobile users, hence, the complexity of PKI can be reduced significantly. Thus, key management will become easier than those of schemes based on public-key cryptosystems.

V. Performance Analysis

The computation overhead and communication overhead for the mobile users, the visited foreign servers and the home servers are reasonable in the proposed scheme. Due to the limited wireless spectrum supported for communications between mobile users, limited power constrains, and the limited numbers of servers, it is especially important that the performance be given a high priority in performance for communication rounds between the mobile users and the foreign servers. As mentioned earlier, there are only two communication rounds between the mobile users and the foreign servers, and this is the minimum number of rounds required to achieve mutual authentication and authenticated key agreement.

Performance comparisons, based on the mobile authentication phase, for the proposed scheme and the related schemes are given in Table 1. Note that the notations M, V, and H denote mobile users, the visited foreign severs, and home servers, respectively. It can be concluded that the complexity of the proposed scheme is equal to or less than those proposed by Jiang *et al.* and Tang and Wu. In addition, the computation costs for mobile users are quite low. Since, point multiplications are relatively time consuming operations compared to the other processing operations in the proposed scheme, some operations can be pre-calculated to increase the efficiency, e.g., $k_1 * G, k_2 * G$. As a result of these improvements, the use of the proposed scheme would not be a heavy burden for the computation-constrained mobile users. It is remarkable that the home server must perform (1+N) hash operations. This is because that the home server must generate an ephemeral delegation keys to the visited foreign servers for the next successive sessions between mobile users and the foreign servers. If we only consider those successive sessions in which the home server is involved only once, the amortized cost of performance of hash operations by the home server is required only (1+1/N). Generally, for the mobile users, the elliptic curve can be easily embedded with application specific chipset (e.g., ARM SC200). For instance, the estimated time, which is based on a Pentium II 400MHz with constrained available memory, of scalar point multiplication on Koblitz curve 163-bit is approximately 1.95 milliseconds [6]. To measure the communication part, we can observe that only one reception and one transmission are demanded on the mobile users. Hence, the total transmitted messages of our proposed scheme is 160+163+128+160=611 bits ($\simeq$75 bytes), for the 160-bit hash function, the 128-bit symmetric encryption, and the 163-bit ECC And, in Tang and Wu's scheme, the message length of their scheme is roughly 100 bytes. Hence, compared with Tang and Wu's scheme, our proposed scheme is more suitable for the wireless environment.

In Table 2, we compare the security requirements of our proposed scheme and some related schemes. As Table 2 shows, on key establishment, only the scheme developed by Jiang *et al.* and ours provide session key establishment by acquiring the session key from the home server. This is an important feature for mobile authentication applications with the specific foreign servers. Concerning pre-shared secrets, the scheme developed by Jiang *et al.* does not have to store any pre-shared secret, the home server still must compute the warrants and maintain them for all mobile users. Also, their scheme requires mobile users to publish their public-key to a trusted third party which is more complicated and less efficient than the proposed scheme. Finally, concerning renewal session keys, in Tang and Wu's scheme, the session key ck, which can only be used within the valid time, is generated by the mobile user. If ck has not expired based the valid time, it is still used for the next session through the home server's off-line authentication phase. However, once the valid time has expired, a foreign server must authenticate mobile users by resorting to the home server once again. Compared with the other schemes, Tang and Wu's scheme does not fully support renewal session keys.

TABLE I
PERFORMANCE COMPARISONS

Performance Metrics		Jiang *et al.*	Tang-Wu	Our
Exponential operation	M	1+Pre	1+ck	1+2Pre
/Point multiplication.	V	1+Pre	3	1+1Pre
/Asym. decryption	H	3	1	2
Hash	M	1	1	1
	V	N/A	2	1
	H	1	1	1+N
Symmetric	M	2	2	2
encryption	V	2	2	2
/decryption	H	3	3	4
Anonymity		Yes	No	Yes
H knows the session key		No	Yes	No

TABLE II
COMPARISON AMONG RELATED SCHEMES

	3GPP	Jiang *et al.*	Tang-Wu	Our
Authenticate H	Yes	Yes	Yes	Yes
Key estabishment	E	EH	E	EH
User anonymity	Partially	Yes	No	Yes
Types	Symm.	Asymm.	Asymm.	Asymm.
Store preshare secrets	Yes	Partially	Yes	No
renewal session key	No	Yes	No	Yes
Mutual key agreement	No	Yes	No	Yes
Forward secrecy	N/A	Yes	No	Yes
Mutual Entity Authentication	No	Yes	Yes	Yes
Computational Loads on user part	Medium	Heavy	Low	Low
Tranmission round	5	4	4	4

VI. Conclusion

In this paper, we have demonstrated that Tang and Wu's scheme has still vulnerable to several weaknesses. To remedy these weaknesses, we have proposed an improved scheme with the novel and efficient architecture. We focus on preserving the secrecy of mobile users' identities for large scale wireless networks. The proposed scheme has several attractive characteristics as follows, $i.e.$, the mutual authentication can be achieved among mobile users, the visited foreign servers and the home servers; the home server does not have to store the long-term keys shared with mobile users which is scalable in wireless networks; the privacy of mobile users' information is maintained, and the established session key can only be shared by the communication parties, and, even the home server cannot obtain the established session key. We analyzed the security properties of the proposed scheme and compare them with those to other similar schemes. The result of the analysis indicated that, the proposed scheme is superior to other similar schemes with respect to security, and, in addition, it is well-suited for the low power devices used with wireless networks.

Acknowledgement

We thank Prof. Djamal Zeghlache and the anonymous reviewers for their feedback and suggestions.

Appendix A
Proof of Theorem 1

Proof. A sequence of game reductions is involved in the proof. We define a sequence of game starting at the real game G_0.

Game G_0: This is the real attack game in the random oracle models. Several oracles are available to the adversary: a hash oracle, the encryption/decryption oracles E and D, and all mobile users and servers instances U^i and S^j. For any game G_n we define several events as in the following:

event S_n occurs if $b = b'$, where b is the binary bit involved in the Test-query, and b' is the output of the adversary;

event $Encrypt_n$ occurs if the adversary A submits a data which has encrypted using the key by himself;

By the definition, we have $Adv_P{}^{ake}(A)$=2Pr[S_0]-1. Furthermore, if the adversary has not stopped playing the game after q_s Send-queries of lasts for more than time t, we terminate the game and choose a random bit b' as the output, where q_s and t are predetermined upper bounds.

Game G_1: In this game, we simulate the hash oracle $h(\cdot)$:$\{0,1\}^*{\rightarrow}\{0,1\}^l$ and the encryption/decryption oracles by maintaining a hash list Λ_h and an encryption list Λ_E, respectively. Also, all instances can be simulated as the real players do, for Send, Execute, Reveal, and Test-queries.

From this simulation, we can easily see that this game is indistinguishable from the real attack unless the permutation property of E or D does not hold. As a result, according to the birthday paradox, the probability of collisions happened is at most q_E^2/2(q-1) since $|G|$=(q-1), where q_E is the size of Λ_E. In addition, the same reason applied to the output of hash function H is bounded by $q_h^2/2^{l+1}$. Consequently, we have

$$|\text{Pr}[S_1]\text{-Pr}[S_0]| \leq \tfrac{q_E^2}{2(q-1)} + \tfrac{q_h^2}{2^{l+1}}.$$

Game G_2: In this game, we modify the game that the home server processes the Send-query so that the adversary will be the only one to encrypt data. To make G_2 and G_1 are perfectly indistinguishable, we apply the following rule:

Rule $R1^{(2)}$: Choose either a random element κ^* and then compute $\kappa = D_{h(\delta_{U_a})\|S_h}(*,*,\kappa^*,*)$. Without loss of generality, we look for the record $D_{h(\delta_{U_a}\|S_h)}(*,*,\kappa^*,*)$ in the list Λ_E to define ϕ (we thus have $\kappa = \phi * G$) and finally compute the portion of the secret information of the session key $K_{sk} = \phi * \kappa^*$. When κ^* has not been previously obtained as the ciphertext returned by encryption-queries, G_2 and G_1 are indistinguishable. Since only the adversary may ask encryption queries, the home server is simulated using the decryption oracle. Thus, we obtain

$$|\text{Pr}[S_2]\text{-Pr}[S_1]| \leq \tfrac{q_s q_E}{q-1}.$$

Game G_3: In this game, we avoid collisions amongst the hash queries asked by the adversary to the ephemeral master key, amongst the shared key K_{hv}, and amongst the output of the Send-queries. Assume that no collision has been found by the adversary for the ephemeral master key $h^N(h(\delta\|S_h)\|S_v\|ts)$; no encrypted data corresponds to multiple identical plaintext. We apply the following rules:

Rule $h1^{(3)}$: Choose a random element $r \in\{0,1\}^l$. If this query is directly asked by the adversary and $(*,r)\in \Lambda_A$, where Λ_A denotes the queried list of adversaries, then we abort the game. However, this rule may still make the game abort with the probability bounded for $q_h^2/2^{l+1}$.

Rule $D1^{(3)}$: Choose a random element $\phi \in Z_q^*$ and compute $Z = \phi * G$. If $(*,Z,*,*,Z^*)\in \Lambda_E$, we abort the game; otherwise, we add the record $(\kappa, Z, \phi, D, Z^*)$ to Λ_E.

Then, for any pair (Z, Z^*), we can derive that the game to abort is bounded by the probability $q_E^2/2(q-1)$. It is worth noting that this may happen when processing Send-query, the game is also aborted with the probability $q_s^2/2(q-1)$ by the birthday paradox. The two games G_3 and G_2 are indistinguishable unless one of the above rules makes the game to abort, hence, we can obtain

$$|\text{Pr}[S_3]\text{-Pr}[S_2]| \leq \tfrac{q_s^2+q_E^2}{2(q-1)} + \tfrac{q_h^2}{2^{l+1}}.$$

Game G_4: We define game G_4 by aborting the executions wherein the adversary may have been lucky in guessing the master delegation key without asking the corresponding hash query. We use the following rule:

Rule $S1^{(4)}$: Check whether $H = H'$, where $H' = h(\delta_{U_a}\|S_h)$. If it does hold, check if $(\delta_{U_a}\|S_h, H \in \Lambda_A)$. If either of these two tests fail, then reject the master delegation key, terminate without accepting.

This rule provides that the accepted delegation master key comes from either the simulator, or the adversary that has correctly decrypted $D_{h(\delta_{U_a}\|S_h)}$(*,*,κ^*, $*$) into κ. Game G_4 and game G_3 are perfectly indistinguishable unless the home server rejects a valid message encrypted by $H = h(\delta_{U_a}\|S_h)$. Since κ does not appear in the previous session, the probability that the delegation key has been correctly guessed by the adversary without asking hash queries is bounded by

$$|\text{Pr}[S_4]\text{-Pr}[S_3]| \leq \text{Pr}[Encrypt_4],\ |\text{Pr}[Encrypt_4]| \leq \tfrac{q_s}{2N}.$$

Game G_5: In this game, we simulate the executions using the random self-reducibility of the elliptic curve discrete logarithm problem. Given a pair ECDLP instance (A, B), where $X = \alpha A, Y = \beta B$, and we wish to derive $Z = ECDLP(X, Y)$. By picking randomly in the Λ_A list, we can obtain the elliptic curve discrete logarithm secret value with the probability $(1/(q_s + q_E))$. This is a triple $(X, Y, ECDLP(X, Y))$. We therefore can find the values α and β such that $ECDLP(X, Y) = ECDLP(\alpha A, \beta B) = ECDLP(A, B)^{\alpha\beta}$. Thus, we have

$$|\text{Pr}[S_5]\text{-Pr}[S_4]| \leq (q_s + q_E) \cdot Succ_G^{ecdl}(t'),$$

where $t' \leq t + (q_s + q_E)\tau_G$. And this concludes the proof.

References

[1] 3GPP, "Wireless local area network (WLAN) interworking security," 3GPP TS 33.234, 2004.

[2] J. Arkko and H. Haverinen, "Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA)," RFC 4187, 2006.

[3] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. Computer Commun. Security*, 1993, pp. 62–73.

[4] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," *IEEE J. Sel. Areas Commun.*, vol. 11, no. 6, pp. 821–829, Aug. 1993.

[5] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[6] D. Hankerson, J. L. Hernandez, and A. Menzes, "Software implementation of elliptic curve cryptography over binary fields," in *Proc. CHES 2000*, *Lecture Notes Comput. Sci.* 1965, Springer-Verlag, pp. 1–24, 2000.

[7] D. Hankerson, A. Menzes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, 2nd edition. New York: Springer-Verlag, 2004.

[8] Q. He, D. Wu, and P. Khosla, "Quest for personal control over mobile location privacy," *IEEE Commun. Mag.*, vol. 42, no. 5, pp. 130–136, 2004.

[9] K. F. Hwang and C. C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," *IEEE Trans. Wireless Commun.*, vol. 2, no. 2, pp. 400–407, Mar. 2003.

[10] K. Jarrinen and J. Skytta, "On parallelization of high-speed processors for elliptic curve cryptography," *IEEE Trans. VLSI Syst.*, vol. 16, no. 9, pp. 1162–1175, Sep. 2008.

[11] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2569–2576, Sep. 2006.

[12] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Security*, vol. 1, no. 1, pp. 36–63, 2001.

[13] S. Kent and R. Atkinson, "Security architecture for the Internet protocol," RFC 2401, Nov. 1998.

[14] W. B. Lee and C. K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," *IEEE Trans. Wireless Commun.*, vol. 4, no. 1, pp. 57–64, 2005.

[15] C. Mitchell, M. Ward, and P. Wilson, "On key control in key agreement protocols," *Electron. Lett.*, vol. 34, pp. 980–981, 1998.

[16] R. Molva, D. Samfat, and G. Tsudik, "Authentication of mobile users," *IEEE Network*, vol. 8, no. 2, pp. 26–34, 1994.

[17] B. C. Neuman and T. Tso, "Kerberos: an authentication service for computer networks," *IEEE Commun. Mag.*, vol. 32, no. 9, pp. 33–38, 1994.

[18] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signature and public-key cryptosystem," *Commun. ACM*, vol. 21, pp. 120–126, Feb. 1978.

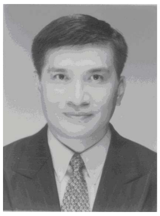
[19] D. Samfat, R. Molva, and N. Asokan, "Untraceability in mobile networks," in *Proc. Int. Conf. Mobile Computing Networking*, 1995, pp. 26–36.

[20] C. Tang and D. O. Wu, "An efficient mobile authentication scheme for wireless networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1408–1416, Apr. 2008.

[21] Z. J. Tzeng and W. G. Tzeng, "Authentication of mobile users in the third generation mobile system," *Wireless Personal Commun.*, vol. 16, no. 1, pp. 35–50, Jan. 2001.

[22] G. Yang, D. S. Wong, and X. Deng, "Anonymous and authenticated key exchange for roaming networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3461–3472, 2007.

[23] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 734–742, 2005.



Chin-Chen Chang received his BS degree in applied mathematics in 1977 and the MS degree in computer and decision sciences in 1979, both from National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. Since February 2005, Professor Chang has been a Chair Professor of Feng Chia University. In addition, he has served as a consultant to several research institutes and government departments. Professor Chang's specialties include, but are not limited to, data engineering, database systems, computer cryptography, and information security. A researcher of acclaimed and distinguished services and contributions to his country and advancing human knowledge in the field of information science, Professor Chang has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. And since his early years of career development, he consecutively won the Outstanding Youth Award of Taiwan, Outstanding Talent in Information Sciences of Taiwan, the AceR Dragon Award of the Ten Most Outstanding Talents, the Outstanding Scholar Award of Taiwan, Outstanding Engineering Professor Award of Taiwan, Chung-Shan Academic Publication Awards, Distinguished Research Awards of the National Science Council of Taiwan, the Outstanding Scholarly Contribution Award of the International Institute for Advanced Studies in Systems Research and Cybernetics, Top Fifteen Scholars in Systems and Software Engineering of the *Journal of Systems and Software*, and so on. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, and Research Fellow, by universities and research institutes. Professor Chang has also published more than one thousand papers in information sciences. In the meantime, he participates actively in international academic organizations and performs advisory work to government agencies and academic organizations.

Hao-Chuan Tsai received the BS degree in mathematics in 2002 from SooChow University, Taipei, Taiwan, and the MS degree in computer science and information engineering in 2004 from Fu Jen Catholic University, Taipei, Taiwan. He is currently pursuing his PhD degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan. His research interests include cryptography, image hiding, and information security.