International Journal of Innovative
Computing, Information and Control
Volume **8**, Number **9**, September **2012**

ICIC International ©2012 ISSN 1349-4198
pp. 6415–6427

EFFICIENT MUTUAL AUTHENTICATION AND KEY AGREEMENT WITH USER ANONYMITY FOR ROAMING SERVICES IN GLOBAL MOBILITY NETWORKS

Yun-Hsin Chuang[1], Yuh-Min Tseng[2] and Chin-Laung Lei[1,*]

[1]Department of Electrical Engineering
National Taiwan University
No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan
yun@fractal.ee.ntu.edu.tw
*Corresponding author: lei@cc.ee.ntu.edu.tw

[2]Department of Mathematics
National Changhua University of Education
No. 1, Jin-De Road, Changhua City 500, Taiwan
ymtseng@cc.ncue.edu.tw

Received May 2011; revised September 2011

Abstract. *Global mobility networks provide effective global roaming services for personal communication users. Through the universal roaming technology, legitimate mobile users can enjoy the ubiquitous services. Mutual authentication and key agreement between mobile users and roaming servers is the primary security issue of many commercial mobile networks. For personal privacy, it becomes an important issue to develop a mutual authentication and key agreement scheme with anonymity for roaming services in global mobility networks to protect user's identity. Recently, many schemes concerned with this issue have been proposed. However, most of those schemes have been demonstrated that may have several security weaknesses and do not achieve user anonymity. In this paper, we propose a novel and efficient mutual authentication and key agreement scheme with user anonymity for roaming services in the global mobility network. Under the random oracle model, we show that our scheme can withstand known attacks. We also demonstrate that the proposed scheme provides the secrecy of the session key, strong anonymity of user's identity, and mutual authentication.*

Keywords: Anonymity, Authentication, Roaming service, Key agreement, Mobility network

1. **Introduction.** For personal communication users, Global mobility networks (GLOMONET) [1] provide effective global roaming services. Legitimate mobile users can enjoy the ubiquitous services through the universal roaming technology. Mutual authentication between a legitimate mobile user and a service provider of the visited network in GLOMONET can avoid illegal access from malicious intruders. Several authentication schemes that are suitable for roaming environment [1,3,10,12,18] have been proposed.

For personal privacy, it becomes a new research issue to develop a mutual authentication and key agreement (MAKA) scheme with user anonymity for roaming services in GLOMONET to protect user's identity. Here, we classify the anonymity of the mobile user into weak anonymity and strong anonymity as follows.

- *Weak anonymity*: The anonymity of user's identity is preserved. No one except the user's home agent can get the user's real identity during roaming.

- *Strong anonymity*: In addition to weak anonymity, it also satisfies user un-tractability. Even if a user has roamed several times in GLOMONET, no one except the user's home agent can trace the relationship between these roaming activities.

Several MKAK scheme with user anonymity for GLOMONET or wireless environments have been proposed [5,13,19,20,22,23]. Zhu and Ma [23] proposed a user authentication scheme with user anonymity in 2004. However, Lee et al. [13] pointed out a security weakness on the Zhu-Ma scheme [23] and further proposed an improvement in 2006. In 2008, Wu et al. [20] pointed out that the Zhu-Ma scheme does not provide anonymity, demonstrated that the Lee-Hwang-Liao scheme [13] does not achieve anonymity and backward secrecy, and then proposed an improvement. Chang et al. [5] also showed that the Lee-Hwang-Liao scheme [13] cannot provide anonymity under the forgery attack, and further proposed a novel authentication scheme in 2009. In the same year, Youn et al. [22] showed that the Wu-Lee-Tsaur scheme [20] is unable to provide anonymous authentication. They also demonstrated that the Chang-Lee-Chiu scheme [5] cannot achieve anonymity and cannot withstand a known session key attack. In 2010, Xu et al. [21] proposed a MAKA scheme preserving user anonymity in mobile networks. However, they did not prove that their scheme achieves forward secrecy. Indeed, it is easy to find that their scheme does not achieve forward secrecy on foreign agent side. Once the secret key K_{FH} is compromised, the former session key will also be compromised.

All of these user authentication and key agreement schemes [5,13,20,23] with user anonymity try to provide weak anonymity. In these schemes with weak anonymity, a mobile user is given a pseudo number to replace her/his real identity, so the pseudo number can be traced because she/he used the identical pseudo number throughout all the roaming activities. Actually, these schemes [5,13,20,23] have been demonstrated that do not achieve the intended goal of weak anonymity.

To the best of our knowledge, there is no provably secure mutual authentication and key agreement (MAKA) scheme with user anonymity for roaming services in GLOMONET has been proposed so far. Thereupon, it inspires us to propose an effective and provably secure MAKA with user anonymity for roaming services in GLOMONET.

In this paper, we propose a novel and efficient MKAK scheme with strong anonymity for roaming services in GLOMONET, which is provably secure and achieves forward secrecy on both mobile user and foreign agent sides. In our scheme, a mobile user can freely change his/her password of the smartcard without the help of the home agent. Under the random oracle model, we prove that the proposed scheme can withstand known attacks. We demonstrate that the proposed scheme provides the secrecy of the session key, strong anonymity of user's identity, as well as mutual authentication. We also show that our scheme is well suitable for low power mobile devices, and manifest the advantages of our scheme as compared to the related schemes [5,13,20,23].

The remainder of this paper is organized as follows. We describe the roaming environment of GLOMONET, address the system scenario, and propose our scheme in Section 2. We construct the adversarial model and define the security of an ID-based MAKA scheme for roaming services system in Section 3, and analyze the security of the proposed scheme in the random oracle model [2] in Section 4. In Section 5, we show that our scheme is well suitable for low power mobile devices by referring to some implementation data [4,6,9,15], and also compare our scheme to related schemes [5,13,20,23] to show that only our scheme is provably secure. Finally, we draw our conclusions in Section 6.

2. The Proposed Scheme.

2.1. **System environment.** The system environment of our scheme is described as follows. There are three kinds of participants in the roaming environment of global mobility networks: home agent, mobile users, and foreign servers. Each mobile user has its own home agent, and the home agent is responsible for issuing a smart card to the mobile user. The mobile user will use the smart card to roam over foreign networks. Assume that there is a pre-shared secret key between the home agent and each of the foreign servers. The home agent and a foreign server can use their pre-shared secret key to confirm the integrity and the secrecy of the transmitted message. The home agent publishes its public key and keeps the matching private key secrecy.

In order to deal with the revoke problem and avoid crimes, the home agent can know the real identity of a mobile user during his/her roaming phase. Since the home agent is the company that sales the communication service to the mobile user and charges the bill, the home agent should keep the records of the mobile user's accounts. Hence, the home agent can verify the validity of the mobile user by using its database after getting the real identity of a mobile user.

The mobile user uses the home agent's public key to encrypt user's identity. Since the home agent has the matching private secret key, only the home agent can obtain the real identity of the mobile user. In this case, other outsiders (including the visited foreign server) cannot know the identity of the mobile user and so that it can achieve the anonymity of the mobile user's identity. The public-key encryption or decryption can adopt some secure cryptosystems such as RSA [14], ElGamal [7], ECC [11], and pairing-based cryptography [8,16,17].

In the following, let us see the system scenario. When a mobile user wants to roam over a foreign network, the foreign server will send the request message to the corresponding home agent and the home agent can recover the mobile user's identity by using the received message and verify the validity of the mobile user. The home agent then computes the related information to let the foreign server and the mobile user can authenticate each other and establish a session key.

The notations used in the proposed scheme are defined as follows.

- M: a mobile user.
- H: the home agent of the mobile user M.
- F: the foreign agent (service provider) of a foreign network.
- ID_A: the identity of the participant A.
- PW_M: the password of the mobile user M.
- K_{FH}: the pre-shared secret key between F and H.
- Pub_H: the home agent H's public key.
- Pri_H: the matching private key of Pub_H hold by H.
- x: the home agent H's secret key.
- $h()$: a one way hash function.
- $E_k()$: an encryption function with the key k.
- $D_k()$: a decryption function with the key k.
- $\oplus$: the exclusive-or operation.
- $||$: the concatenation operation.

2.2. **Concrete scheme.** The proposed scheme consists of two phases: the registration phase and the mutual authentication and key agreement phase. Note that the identity ID_H of the home agent H and the identity ID_F of the foreign server F are public. Three phases of the proposed scheme are given as follows:

[***Registration Phase***] When a mobile user wants to register at the home agent H, the user has to submit a request to the home agent, and then the home agent will issue a smartcard with the related messages to the user. Note that the home agent does not need to keep the registration information. The detail of the registration phase is depicted in Figure 1 and presented as follows.

1. The mobile user M submits ID_M and PW_M to the home agent H via a secure channel.
2. The home agent H computes $R = h\ (ID_M||x) \oplus PW_M$ and $k = h\ (PW_M)$. The home agent H stores (ID_M, R, k, Pub_H, $h()$, $E()$) into the smart card, and then sends it to the mobile user M through a secure channel.

[***Mutual Authentication and Key Agreement Phase***] When a mobile user M with a smartcard wants to roam over a foreign agent F, the mobile user M can authenticate with F mutually and establish a session key with F. The details of the mutual authentication and key agreement phase are depicted in Figure 2 and presented as follows.

1. M submits the password PW_M^* to the smart card. The smart card checks if $h(PW_M^*) = k$. If yes, it randomly chooses n_M, $r_M \in Z_q^*$, and computes $AID_M = E_{Pub_H}(r_M||ID_M)$. M then sends $m_1 = \{$Login message, ID_H, AID_M, $n_M\}$ to F.
2. Upon receiving m_1, F generates n_F, $r_F \in Z_q^*$ and computes $V_1 = E_{Pub_H}(r_F||ID_H||ID_F||AID_M||n_M||n_F)$, and then sends $m_2 = \{$Authentication request, ID_H, ID_F, $V_1\}$ to H.
3. Upon receiving m_2, H generates a random integer $n_H \in Z_q^*$. H gets $(r_F||ID_H||ID_F||AID_M||n_M||n_F)$ by decrypting V_1 with the key Pri_H, and gets $(r_M||ID_M)$ by decrypting AID_M with the key Pri_H. H then verifies the validity of the mobile user M. H computes $C = h(ID_M||x) \oplus r_M$, $y = h(C||r_M) \oplus n_H \oplus h(K_{FH}||r_F)$, $z = h(C||n_M||r_M) \oplus n_H$, $V_2 = h(K_{FH}||n_M||n_F||r_F||y||z)$, $V_3 = h(C||z)$, and then sends $m_3 = \{V_2, V_3, y, z\}$ to F.

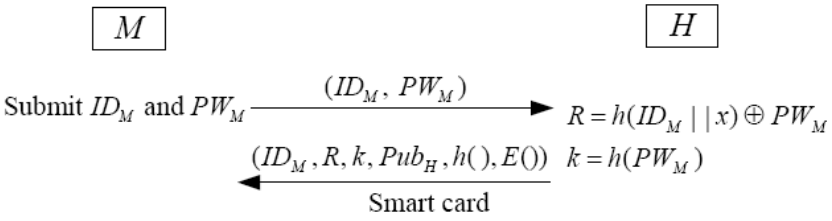

FIGURE 1. The registration phase

4. Upon receiving m_3, F checks whether V_2 is equal to $h(K_{FH}||n_M||n_F||r_F||y||z)$ or not. F computes $TK = y \oplus h(K_{FH}||r_F)$, and then sends $m_4 = \{V_3, z, n_F\}$ to M.
5. Upon receiving m_4, M computes $C = (R \oplus PW_M^*) \oplus r_M$ by using its smartcard and checks whether V_3 is equal to $h(C||z)$ or not. M computes $n_H = z \oplus h(C||n_M||r_M)$ and $TK = h(C||r_M) \oplus n_H$. If M is not the real owner of the smartcard, M does not have the real PW_M to get $h(ID_M||x) = (R \oplus PW_M)$.

Note that this phase will be aborted if any check in the above steps is invalid. After this phase is completed successfully, M and F can compute a session key $SK = h(TK||n_M||n_F)$.

[***Password Changing Phase***] In our scheme, a mobile user can freely change his password of the smartcard without the help of the home agent. When a mobile user M with a smartcard wants to change the password of the smartcard, M makes a request to the smartcard, and then inputs the origin password PW_M to the smartcard. If $h(PW_M) = k$,

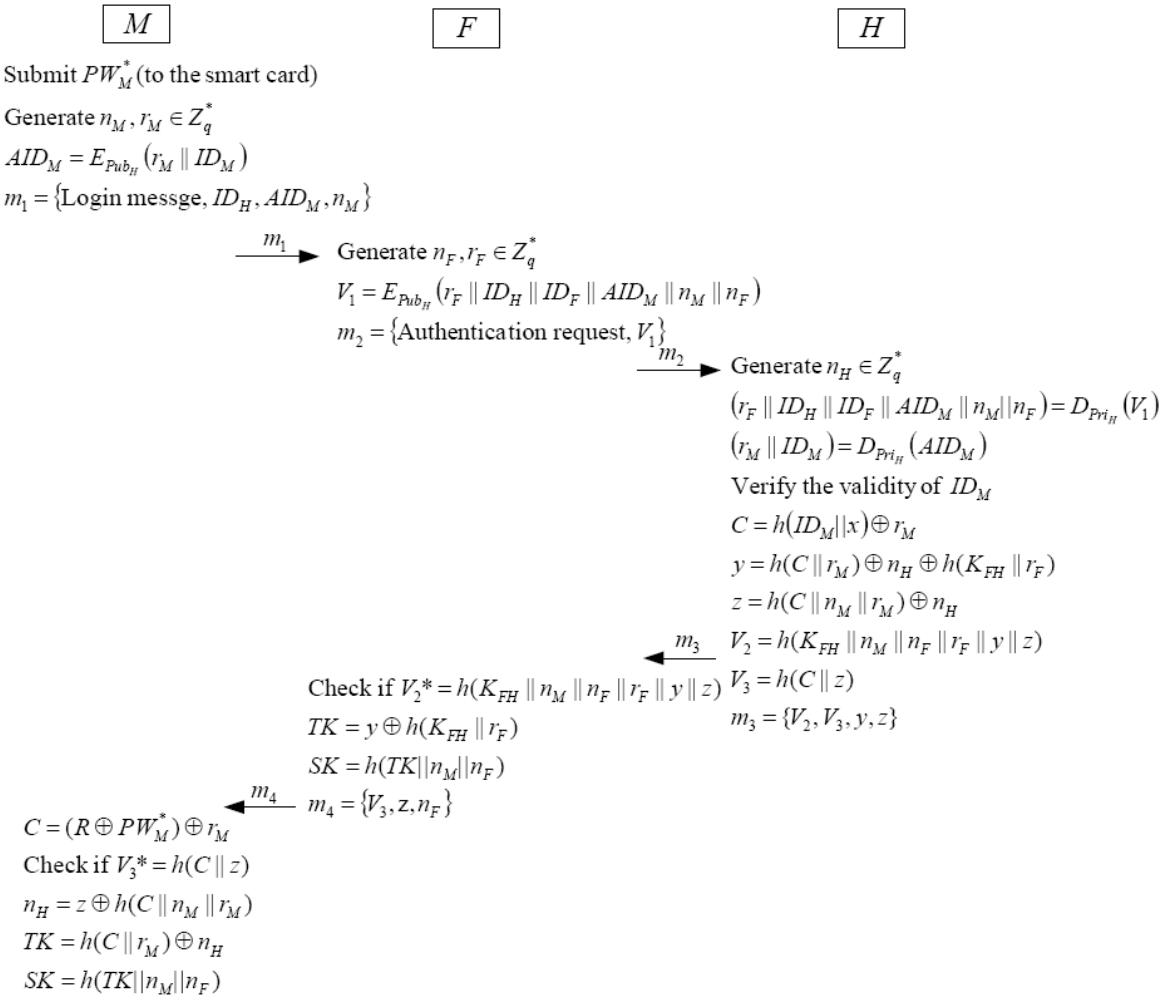

FIGURE 2. The mutual authentication and key agreement phase

then the smartcard lets M input a new password PW'_M. The smartcard then replaces R by $(R \oplus PW_M \oplus PW'_M)$, and replaces k by $h(PW'_M)$.

3. **Security Model.** In this section, we construct a security model of an ID-based MAKA with user anonymity for roaming services system.

3.1. **Adversarial model.** In this subsection, we define the adversarial model of an ID-based MAKA scheme for roaming services system. Assume that the multi-server environment contains three kinds of participants, a mobile user's home agent H, n users $\mathcal{M} = \{M_i | \text{ for } i = 1, \ldots, n\}$ and m foreign agents $\mathcal{F} = \{F_j | \text{ for } j = 1, \ldots, m\}$. Each user M_i and each agent F_j have unique identities ID_{M_i} and ID_{F_j}, respectively. In this model, we allow each user M_i to execute the scheme repeatedly with each agent F_j. *Instances* of M_i (resp. F_j) model distinct executions of the scheme. We denote sth instance of M_i (resp. F_j, H), called an oracle, by $\Pi^s_{M_i}$ (resp. $\Pi^s_{F_j}$, Π^s_H) for an integer $s \in N$. The public parameters and identities $\mathcal{ID} = \{ID_{M_i}, ID_{F_j} | \text{ for } M_i \in \mathcal{M}, F_j \in \mathcal{F}\}$ are known by each participant (including the home agent H, users and agents) and adversaries.

Adversarial model. The model is used to formalize the adversary's capabilities. We allow that a probabilistic polynomial time (PPT) adversary $\mathcal{A}$ can potentially control all communications in the network via accessing to a set of oracles as defined below. We consider the following types of queries for ID-based MAKA scheme. Let $\alpha \in \{\mathcal{M}, \mathcal{F}, ID_H\}$.

- **Extract** (ID): Give the adversary $\mathcal{A}$ the long-term secret key of ID which is chosen by $\mathcal{A}$, where $ID \notin \mathcal{ID}$.
- **Execute** (M_i, F_j): Give the adversary $\mathcal{A}$ the complete transcripts of an honest execution between M_i, F_j and H. This query models the passive attack.
- **Send** (Π^s_α, m): $\mathcal{A}$ sends a message m to instance Π^s_α. When Π^s_α receives m, Π^s_α responds to $\mathcal{A}$ according to the ID-based MAKA scheme. This query models the active attack.
- **Reveal** (Π^s_α): Give $\mathcal{A}$ the session key for the instance Π^s_α. This query models the known session key attack.
- **Corrupt** (ID_α): Give $\mathcal{A}$ the long-term secret key held by ID_α. This query models the forward secrecy.
- **Test** (Π^s_α): This query is used to define the advantage of $\mathcal{A}$. When $\mathcal{A}$ asks this query to an instance Π^s_α for $\alpha \in \{\mathcal{M}, \mathcal{F}\}$, the oracle chooses a random bit $b \in \{0,1\}$. The oracle returns the session key if $b = 1$; or returns a random value if $b = 0$. $\mathcal{A}$ is allowed to make a single Test query at any time during the game.

In the model, we consider two types of adversaries. A *passive adversary* is allowed to issue the **Execute**, **Reveal**, **Corrupt**, and **Test** queries; an *active adversary* is additionally allowed to issue the **Send** and **Extract** queries.

3.2. **Definitions of security.** To demonstrate the security of the ID-based MAKA scheme for roaming services system, we give definitions of security in this subsection.

Definition 3.1. *Π^s_α and Π^t_β, where $\alpha \in \mathcal{M}$ and $\beta \in \mathcal{F}$, are said to be **partners** if they authenticate mutually and establish a session key.*

Definition 3.2. *An oracle Π^s_α with its partner Π^t_β is said **fresh** (or holds a fresh key SK) if the follows two conditions hold:*

(1) Π^s_α accepted a session key $SK \neq NULL$ with Π^t_β and neither Π^s_α nor Π^t_β has been asked for the Reveal query.
(2) There is no Corrupt query has been asked before the query Send (Π^s_α, m) or Send (Π^t_β, m) has been asked.

Definition 3.3. *An ID-based MAKA scheme for multi-server environment offers existential unforgeability and maintains session key secrecy against adaptive chosen ID attacks if no probabilistic polynomial-time adversary $\mathcal{A}$ has a non-negligible advantage in the following game played between an adversary $\mathcal{A}$ and infinite set of oracles Π^s_α for $ID_\alpha \in \mathcal{ID}$ and $s \in N$.*

(1) A long-term key is assigned to each user and server through the initialization phase related to the security parameter.
(2) The adversary $\mathcal{A}$ may ask several queries and get back the results from the corresponding oracles.
(3) There is no Reveal (Π^s_α) query or Corrupt (ID_α) query have been asked before the Test (Π^s_α) query has been asked.
(4) The adversary $\mathcal{A}$ may ask other queries during asking the Test (Π^s_α) query where Π^s_α is fresh. $\mathcal{A}$ outputs its guess b' for the bit b which is chosen in the Test (Π^s_α) query eventually and the game is terminated.

The advantage of the adversary $\mathcal{A}$ is measured by the ability of distinguishing a session key from a random value. We define *Succ* to be the event that $\mathcal{A}$ correctly guesses the bit b, which is chosen in the Test query. The advantage of the adversary $\mathcal{A}$ in the attacked scheme P is defined as $Adv_{\mathcal{A},P}(k) = |2 \cdot \Pr[Succ] - 1|$.

4. **Security Analysis.** In this section, we discuss the security analysis of the proposed scheme in the random oracle model [2]. The random oracle model is usually adopted to demonstrate the security of the key establishment scheme or the signature scheme. The random oracle model assumes that the hash function is actually a true random function and it produces a random value for each new query.

In the random oracle model, the security of the proposed scheme is based on the assumptions specified below.

Assumption 1: Public-key cryptosystem. There exists a public-key cryptosystem that can provide secure public-key encryption/decryption. The public-key encryption/decryption can adopt some secure cryptosystems such as RSA [14], ElGamal [7], ECC [11], and pairing-based cryptography [8,16,17]. In the public-key cryptosystem, a message can be encrypted using the public key of the dedicated receiver while it can be decrypted using the matching private key.

Assumption 2: Hash function. There exists a secure one-way hash function H: $X = \{0,1\}^* \to Y = Z_p^*$, which satisfies the following requirements:

(i) Given any $y \in Y$, it is hard to find $x \in X$ such that $H(x) = y$.

(ii) Given any $x \in X$, it is hard to find $x' \in X$ such that $x' \neq X$ and $H(x') = H(x)$.

(iii) It is hard to find x, $x' \in X$ such that $x' \neq x$ and $H(x') = H(x)$.

For convenience, we denote the maximum advantages of the adversary with the running time T by the following notations.

- $Adv_{Asym.}^{Break}(T)$: breaking public-key cryptosystem to get the plaintext.
- $Adv_{MN}^{Forge}(T)$: impersonating a mobile user.
- $Adv_{FA}^{Forge}(T)$: impersonating a foreign agent.
- $Adv_{HA}^{Forge}(T)$: impersonating the home agent.
- $Adv_{\mathcal{A}}(T)$: attacking the proposed scheme.

Lemma 4.1. *The proposed scheme resists forging mobile user attack, and achieves user's anonymity.*

Proof: Since h is one-way non-collusion function and x is the private key of the home agent HA, an adversary $\mathcal{A}$ cannot find x to create a new certificate $h(ID||x)$ for a new ID. Thus, the proposed scheme resists forging mobile user attack.

Since the identity ID_M is only appear in the value which is encrypted by the public-key cryptosystem and only the home agent has the matching private secret key to decrypt it, no one can get ID_M except the home agent. Thus, the proposed scheme achieves user's anonymity.

Lemma 4.2. *Assume that the hash function h is a random oracle. Suppose that there exists a forger $\mathcal{A}$, who impersonates the foreign agent with running time T in the proposed scheme. Then $Adv_{FA}^{Forge}(T) \leq \frac{1}{2} Adv_{Asym.}^{Break}(T)$.*

Proof: Suppose that $\mathcal{A}$ can impersonate an agent $F(ID_F)$ when a mobile user $M(ID_M)$ logins. To compute $SK{=}h(TK||n_m||n_F)$ to pass the verification, $\mathcal{A}$ has to ask the h hash query oracle for $(TK||n_m||n_F)$, and hence $\mathcal{A}$ needs to compute TK first.

Since $TK = y \oplus h(K_{FH}||r_F) = h(C||r_M) \oplus h(C||n_M||r_M) \oplus z$, $\mathcal{A}$ has to ask $\mathcal{B}$ the h hash query oracle for $(K_{FH}||r_F)$ or $h(C||r_M)$ or $h(C||n_M||r_M)$. Then we can construct an attacker $\mathcal{B}$ to break the public-key cryptosystem. Suppose that there is a secure public-key cryptosystem oracle Φ. When $\mathcal{B}$ gives (encrypt, a) to Φ, Φ outputs $E_{k_{pub}}(r||a)$ to $\mathcal{B}$, where r and the private key k_{pri} is not given to $\mathcal{B}$. When $\mathcal{B}$ gives (decrypt, b) to Φ, for which b was not be outputted by Φ, Φ then outputs $D_{k_{pri}}(a)$ to $\mathcal{B}$. $\mathcal{B}$'s goal is computing r.

$\mathcal{B}$ runs $\mathcal{A}$ as a subroutine and simulates its attack environment. $\mathcal{B}$ sets Z_q^*, public-key encryption/decryption functions E/D, a one-way non-collision hash function h, and x in Z_q^* as the secret key of the home agent. $\mathcal{B}$ sets Pub_H and Pri_H as home agent's public key and private key, respectively. $\mathcal{B}$ gives the public parameters $\langle q, h, Pub_H, E, D\rangle$ to $\mathcal{A}$. $\mathcal{B}$ permeates the problem into the queries, which are asked by $\mathcal{A}$.

Without loss of generality, assume that $\mathcal{A}$ does not ask queries on the same message more than once, and the hash query is asked before the Send and Corrupt (or Extract) queries. $\mathcal{B}$ maintains list L_h to ensure identical responding and avoid collision of the queries. $\mathcal{B}$ simulates the oracle queries of $\mathcal{A}$ as follows:

***h*-query.** When $\mathcal{A}$ makes an h-query for m, $\mathcal{B}$ returns a random number q_m and adds (m,q_m) to L_h if $(m, q_m) \notin L_h$.

Send-query. For convenience, we classify the send query into three types as follows.

- Send $(\prod_{M_i}^s$, start):
  - If $M_i \in \mathcal{ID}$, then $\mathcal{B}$ asks Φ for (encrypt, ID) to get $E_{k_{pub}}(r||ID)$, and returns it to $\mathcal{A}$.
  - If $M_i \notin \mathcal{ID}$, then $\mathcal{B}$ chooses a random number r_α inZ_q^*, and then computes and returns $AID_\alpha = E_{PubH}(r_\alpha||ID_\alpha)$ to $\mathcal{A}$.
- Send$_{FH}(\prod_{Fj}^s$, $(ID_H$, AID_M, $n_M))$: $\mathcal{B}$ chooses a random number n_{Fj}, r_{Fj} in Z_q^*, and asks Φ for (encrypt, $ID_H||ID_{Fj}||AID_M||n_M||n_{Fj}$) to get V_1. $\mathcal{B}$ then returns V_1 to $\mathcal{A}$.
- Send $(\prod_H^s$, $V_1)$: $\mathcal{B}$ computes D_{PriH} (V_F) to get $(ID_H||ID_\alpha||AID_M||n_M||n_\alpha||r_\alpha)$, and computes D_{PriH} (AID_M) to get $(r_M||ID_M)$. $\mathcal{B}$ sets $V_2 = a_1$, $V_3 = a_2$, $y = a_3 \oplus r_M$, $z = a_4 \oplus n_H$. $\mathcal{B}$ then returns $\{V_2, V_3, y, z\}$ to $\mathcal{A}$.

Execute-query. When $\mathcal{A}$ asks an Execute (M_i, F_j) query, then $\mathcal{B}$ returns the transcript $\langle AID_{Mi}, n_{Mi}, n_{Fj}, V_1, V_2, V_3, y, z\rangle$ by using the above simulation of Send queries.

Extract-query.

- When $\mathcal{A}$ asks an Extract query for $(ID_\alpha$, $PW_\alpha)$ for a mobile user, where $ID_\alpha \notin \mathcal{M}$, $\mathcal{B}$ randomly chooses $q_\alpha \in Z_q^*$, adds $\langle(ID_\alpha||x), q_\alpha\rangle$ to L_h. $\mathcal{B}$ then computes and returns $R_\alpha = q_\alpha \oplus PW_\alpha$ to $\mathcal{A}$.
- When $\mathcal{A}$ asks an Extract query for $(ID_\alpha$, $PW_\alpha)$ for a foreign agent, where $ID_\alpha \notin \mathcal{F}$, $\mathcal{B}$ randomly chooses $K_{\alpha H}$ in Z_q^*, stores $K_{\alpha H}$ in the password list, and returns $K_{\alpha H}$ to $\mathcal{A}$.

Corrupt-query.

- When $\mathcal{A}$ asks a Corrupt query for ID_α for a mobile user, where $ID_\alpha \in \mathcal{M}$, $\mathcal{B}$ finds $\langle ID_\alpha, q_\alpha\rangle$ in L_h. Then $\mathcal{B}$ returns $R_\alpha = q_\alpha \oplus PW_\alpha$ to $\mathcal{A}$.
- When $\mathcal{A}$ asks a Corrupt query for ID_α for a foreign agent, where $ID_\alpha \in \mathcal{F}$, $\mathcal{B}$ finds $K_{\alpha H}$ in the password list, and returns $K_{\alpha H}$ to $\mathcal{A}$.

Reveal-query. When $\mathcal{A}$ makes a Reveal query, $\mathcal{B}$ returns a random number, since the session key is a random number generated in the h-query. Note that $\mathcal{B}$ returns the same random number in each identical Reveal-query.

Test-query. When $\mathcal{A}$ makes a Test query, if the query is not asked in the lth session, $\mathcal{B}$ aborts it. Otherwise, $\mathcal{B}$ randomly chooses a bit b, $\mathcal{B}$ returns the session key if $b = 1$, else returns a random number.

Since $TK = y \oplus h(K_{FH}||r_F) = h(C||r) \oplus h(C||n_M||r) \oplus z$, $\mathcal{A}$ has to ask $\mathcal{B}$ the h hash query oracle for $(K_{FH}||r)$ or $h(C_s||r)$ or $h(C_s||n_M||r)$. Thus $\mathcal{B}$ can get r to break the public-key cryptosystem.

If the advantage Adv_{Server}^{Forge} of $\mathcal{A}$ correctly guess b in the Test query is ε, then $\mathcal{A}$ issues a query for $(K_{FH}||r)$ or $h(C_s||r)$ or $h(C_s||n_M||r)$ with advantage 2ε. Thus, the secret value r appears in the list L_h with probability at least 2ε. Therefore, $\mathcal{B}$ breaks the public-key

cryptosystem with probability at least 2ε as required, we have $2\varepsilon \leq Adv^{Break}_{Asym.}(T)$. In this case, we have $Adv^{Forge}_{Server} = \varepsilon \leq \frac{1}{2} Adv^{Break}_{Asym.}(T)$.

Lemma 4.3. *Assume that the hash function h is a random oracle. Suppose that there exists a forger $\mathcal{A}$, who breaks the forward secrecy on either mobile user or foreign agent sides. Then $Adv^{Break}_{Forward} \leq \frac{1}{2} Adv^{Break}_{Asym.}(T)$.*

Proof: Suppose that an adversary $\mathcal{A}$, who can break the forward secrecy of the proposed scheme. To compute $SK = h(TK||n_m||n_F)$ to guess b', $\mathcal{A}$ has to ask the h hash query oracle for $(TK||n_m||n_F)$, and hence $\mathcal{A}$ needs to compute TK first. Since $TK = y \oplus h(K_{FH}||r_F) = h(C||r_M) \oplus h(C||n_M||r_M) \oplus z$, $\mathcal{A}$ has to ask $\mathcal{B}$ the h hash query oracle for $(K_{FH}||r_F)$ or $h(C||r_M)$ or $h(C||n_M||r_M)$. Then we can construct an attacker $\mathcal{B}$ to break the public-key cryptosystem.

Suppose that $\mathcal{A}$ asks the corrupt query to the Challenger for a mobile user M and a foreign agent F. Then the Challenger gives $\mathcal{A}$ the long term secret key $h(ID_M||x)$ and K_{FH} of M and F, respectively. Suppose that there is a secure public-key cryptosystem oracle Φ. When $\mathcal{B}$ gives (encrypt, a) to Φ, Φ outputs $E_{k_{pub}}(r||a)$ to $\mathcal{B}$, where r and the private key k_{pri} is not given to $\mathcal{B}$. When $\mathcal{B}$ gives (decrypt, b) to Φ, for which b was not be outputted by Φ, Φ then outputs $D_{k_{pri}}(a)$ to $\mathcal{B}$. $\mathcal{B}$'s goal is computing r. Let $\mathcal{A}$ ask the h, Send, Execute, Extract query, Corrupt, Reveal, and Test queries, which are specified in the proof of Lemma 4.2.

$\mathcal{B}$ runs $\mathcal{A}$ as a subroutine and simulates its attack environment. $\mathcal{B}$ sets Z^*_q, public-key encryption/decryption functions E/D, a one-way non-collision hash function h, and x in Z^*_q as the secret key of the home agent. $\mathcal{B}$ sets Pub_H and Pri_H as home agent's public key and private key, respectively. $\mathcal{B}$ gives the public parameters $\langle q, h, Pub_H, E, D\rangle$ to $\mathcal{A}$. $\mathcal{B}$ permeates the problem into the queries, which are asked by $\mathcal{A}$.

Since $TK = y \oplus h(K_{FH}||r_F) = h(C||r) \oplus h(C||n_M||r) \oplus z$, $\mathcal{A}$ has to ask $\mathcal{B}$ the h hash query oracle for $(K_{FH}||r)$ or $h(C_s||r)$ or $h(C_s||n_M||r)$. Thus $\mathcal{B}$ can get r to break the public-key cryptosystem.

If the advantage Adv^{Forge}_{Server} of $\mathcal{A}$ correctly guess b in the Test query is ε, then $\mathcal{A}$ issues a query for $(K_{FH}||r)$ or $h(C_s||r)$ or $h(C_s||n_M||r)$ with advantage 2ε. Thus, the secret value r appears in the list L_h with probability at least 2ε. Therefore, $\mathcal{B}$ breaks the public-key cryptosystem with probability at least 2ε as required, we have $2\varepsilon \leq Adv^{Break}_{Asym.}(T)$. In this case, we have $Adv^{Break}_{Forward} = \varepsilon \leq \frac{1}{2} Adv^{Break}_{Asym.}(T)$.

Theorem 4.1. *The proposed scheme is a secure scheme that resists user and server-impersonating attacks, provides full forward secrecy, and achieves user's anonymity under the hardness of the public-key cryptosystem and hash function assumptions.*

Proof: By Lemma 4.1, the proposed scheme resists forging mobile user attack, and achieves user's anonymity. By Lemma 4.2, the proposed scheme resists forging server attack. By Lemma 4.3, the proposed scheme provides full forward secrecy. Thus, the proposed scheme is a secure scheme that resists user and server-impersonating attacks, provides full forward secrecy, and achieves user's anonymity under the hardness of the public-key cryptosystem and hash function assumptions.

5. Performance Analysis and Comparisons.

In this section, we compare our scheme with the recently proposed schemes with user anonymity [5,13,20,23] to manifest the advantages of our scheme. We also demonstrate that our scheme is well suitable for low power mobile devices.

The public-key encryption/decryption can adopt some secure cryptosystems such as RSA, ElGamal, ECC, and pairing-based cryptography. The symmetric encryption/decryption operation used in the recently proposed schemes [5,13,20,23] can use some known symmetric cryptosystems such as Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES). For convenience to analyze the performance, assume that the RSA cryptosystem is the asymmetric (public-key) encryption/decryption operation in our scheme and the AES cryptosystem is the symmetric encryption/decryption operation in the recently proposed schemes [13,20,23].

In the following, we review some implementation data. Scott et al. [15] describe the implementation of exponential operation in 0.07 seconds on the Philips HiPerSmart with a maximum clock speed of 36 MHz and an instantiation of the MIPS-32 based SmartMIPS architecture. Ghoreishi and Pourmina [9] showed that the processor could perform 1024-bit RSA operation in 14.586 ms and 49.467 ms at 54.6 MHz and 16.1 MHz on Xilinx VirtexII and XC4000 series FPGA (Field Programmable Gate Array), respectively. Duh et al. [6] implemented AES on a sensor node based on MOTE-KIT 5040 (8-bit Atmel ATmega128L 8 MHz). Their implementation can encrypt and decrypt a 128-bit block of plaintext in 0.857 ms and 1.328 ms, respectively. In [4], the execution time of a hash function is 0.065 ms, in which the implementation is performed on the MSP430 family with a frequency of 8 MHz. The execution time of the related operations is summarized in Table 1.

Table 1. Execution times (in milliseconds) of the related operations

Operations	Exponential operation	*AES*-128 encryption	*AES*-128 decryption	*RSA*-1024	*Hash*
Execution Time	0.07 s	0.857 ms	1.328 ms	14.586 ms	0.065 ms
Platform	MIPS-32 based SmartMIPS (36 MHz) [15]	MOTE-KIT 5040 (8-bit Atmel ATmega128L 8 MHz) [6]		54.6 MHz Xilinx VirtexII series FPGA [9]	8 MHz MSP430 family [4]

For convenience to evaluate the computational cost, some notations are defined as follows. Note that the exclusive-OR operation is ignored here since its computational cost is very light.

- T_{exp}: The time of executing a exponential operation, that would be $H()$ in our scheme.
- T_{Sym}: The time of executing a symmetric encryption/decryption. We adopt AES here.
- T_{Asym}: The time of executing a encryption/decryption operation or a signature operation by using the asymmetric cryptosystem, that would be $E()$ or $D()$ in our scheme. We introduce RSA [14] here.
- T_{Hash}: The time of executing a one way hash function, that would be $H()$ in our scheme.

Considering the Mutual Authentication and Key Agreement Phase in Section 2, the mobile user M uses the home agent H's public key Pub_H to encrypt the nonce r_M and M's identity ID_M in the first step, and M operates three hash functions in Step 5, and M has to compute $SK = h(TK||n_M||n_F)$. The computation cost of the mobile user is $(1T_{Asym} + 4T_{Hash})$, and the estimated execution time of the mobile user is 14.846 ms. The foreign server F uses the shared key Pub_H to encrypt $(r_F||ID_H||ID_F||AID_M||n_M||n_F)$ in Step 2. F requires two hash functions in Step 4, respectively. F then has to compute $SK = h(TK||n_M||n_F)$, hence F requires one symmetric encryption and five hash functions

totally. The computation cost of the foreign server is ($1T_{Asym}$+$3T_{Hash}$), and the estimated execution time is 14.781 ms. The home agent H uses the shared key K_{FH} to decrypt V_1 to get ($ID_H||r_F||ID_F||n_F||AID_M||n_M$) in Step 3. In order to get M's real identity and (r_M, AID_M) from the foreign agent F, the home agent H uses its matching private key Pri_H to decrypt the messages. H requires two asymmetric decryptions and six hash functions in Step 3, hence the estimated execution time of the home agent is 29.562 ms.

Table 2 presents the comparisons between the recently proposed schemes with user anonymity [5,13,20,23] and our scheme in terms of security property, anonymity, round number, computational costs, and the estimated execution time of three participants (including mobile user, foreign server and home agent). A communication round is viewed as a participant sending a piece of information to the other participant.

TABLE 2. Comparisons of the recently proposed schemes and our scheme

Property \ Scheme	Zhu-Ma 2004 [23]	Lee-Hwang-Liao 2006 [13]	Wu-Lee-Tsaur 2008 [20]	Chang-Lee-Chiu 2009 [5]	Xu-Zhu-Feng 2010 [21]	Ours
Security property (or known attacks)	No backward secrecy [13] No mutual authentication [13] User forgery [13]	No backward secrecy [20] User forgery [5]	Session key stealing [9]	Session key stealing [22]	Partial forward secrecy	Full forward secrecy Provably secure
Anonymity	No [20]	No [5,20]	No [22]	No [22]	Claimed Non-proved	Strong (Proved)
Round number	4	4	4	8	4	5
Computational cost of the mobile user	$2T_{Sym} + 2T_{Hash}$	$2T_{Sym} + 4T_{Hash}$	$2T_{Sym} + 4T_{Hash}$	$7T_{Hash}$	$T_{exp} + 3T_{Sym}$ $+2T_{Hash}$	$1T_{Asym} + 4T_{Hash}$
Estimated execution time of the mobile user	1.844 ms	1.974 ms	1.974 ms	0.455 ms	73.172 ms	14.846 ms
Computational cost of the foreign server	$1T_{Sym} + 2T_{Asym}$ $+2T_{Hash}$	$1T_{Sym} + 2T_{Asym}$ $+3T_{Hash}$	$1T_{Sym} + 2T_{Asym}$ $+3T_{Hash}$	$3T_{Hash}$	$2T_{sym}$	$1T_{Asym} + 3T_{Hash}$
Estimated execution time of the foreign server	30.63 ms	30.695 ms	30.695 ms	0.195 ms	2.185 ms	14.781 ms
Computational cost of the home agent	$1T_{Sym} + 1T_{Asym}$ $+5T_{Hash}$	$1T_{Sym} + 2T_{Asym}$ $+5T_{Hash}$	$1T_{Sym} + 2T_{Asym}$ $+6T_{Hash}$	$8T_{Hash}$	$T_{exp} + 6T_{Sym}$ $+2T_{Hash}$	$2T_{Asym} + 6T_{Hash}$
Estimated execution time of the home agent	15.239 ms	30.825 ms	30.89 ms	0.52 ms	77.156 ms	29.562 ms

As shown in Table 2, it is obvious that only our scheme is provably secure, and the other schemes [5,13,20,23] suffer from several security attacks, which were presented in Section 1. Our scheme achieves forward secrecy on both mobile user and foreign sides. Actually, the recently proposed schemes with user anonymity [5,13,20,23] cannot achieve user anonymity. In Section 3, we have formally proven that that the proposed scheme provides the secrecy of the session key, strong anonymity of user's identity, as well as mutual authentication.

According to Table 2, compare our scheme with Xu-Zhu-Feng scheme [21], the execution time of the mobile user in our scheme decrease **80%** from Xu-Zhu-Feng scheme. The computation cost of the foreign server and the home agent in our scheme are slightly higher than the Chang-Lee-Chiu scheme [5]. Even though our scheme increases extra computational cost than the recently proposed schemes with anonymity [5,13,20,23], the point is that our scheme provides complete security properties. The estimated execution

time of mobile user in our scheme is less than 15 ms on the low power mobile device. Conclusively, the proposed scheme is better than the other recently proposed schemes with anonymity [5,13,20,21,23] and much suitable for roaming services in GLOMONET.

6. **Discussion and Conclusions.** Although the proposed scheme is efficient and provably secure, there is still a deficiency of our proposed scheme. The deficiency of the proposed scheme is that servers have to communicate with the home agent during the mutual authentication phase. However, if servers need not communicate with the home agent during the mutual authentication phase, then the computational costs of users and servers would be raised for maintaining the security of the scheme. Thus, there is a trade-off between the computational costs and communicating cost.

In this paper, we have proposed a novel and efficient mutual authentication and key agreement scheme, which achieves full forward secrecy and strong anonymity, for roaming services in GLOMONET. Under the random oracle model, we have demonstrated that our scheme withstands forgery attacks, achieves the secrecy of the session key, strong anonymity of user's identity, and full forward secrecy. For performance analysis, we have demonstrated that the proposed scheme is well suitable for low power mobile devices in roaming services of GLOMONET.

Acknowledgement. We would like to thank the anonymous referees for their valuable comments and constructive suggestions. This research is partially supported by the "Advanced Metering Infrastructure (AMI) Enhancement Project" of the Institute for Information Industry which is subsidized by the Ministry of Economy Affairs Taiwan, and by the National Science Council, Taiwan, under Grants NSC 100-2218-E-002-010 and NSC 100-2218-E-002-008.

REFERENCES

[1] F. Akyildiz, X. Jiang and S. Mohanty, A survey of mobility management in next-generation all-IP-based wireless systems, *IEEE Wireless Communications*, vol.11, no.4, pp.16-28, 2004.

[2] M. Bellare and P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, *Proc. of the 1st Annual ACM Conference on Computer and Communications Security*, pp.62-73, 1993.

[3] L. Buttyan, C. Gbaguidi, S. Staamann and U. Wilhelm, Extensions to an authentication technique proposed for the global mobility network, *IEEE Transactions on Communications*, vol.48, no.3, pp.373-376, 2000.

[4] S. Cavalieri and G. Cutuli, Implementing encryption and authentication in KNX using Diffie-Hellman and AES algorithms, *Proc. of the 35th Annual Conference of IEEE on Industrial Electronics*, pp.2459-2464, 2009.

[5] C. C. Chang, C. Y. Lee and Y. C. Chiu, Enhanced authentication scheme with anonymity for roaming service in global mobility networks, *Computer Communications*, vol.32, pp.611-618, 2009.

[6] D. R. Duh, T. C. Lin, C. H. Tung and S. J. Chan, An implementation of AES algorithm with the multiple spaces random key pre-distribution scheme on MOTE-KIT 5040, *Proc. of IEEE International Conference of Sensor Networks, Ubiquitous, and Trustworthy Computing*, vol.2, pp.64-71, 2006.

[7] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, vol.31, no.4, pp.469-472, 1985.

[8] G. Frey, M. Müller and H.-G. Rück, The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, *IEEE Transactions on Information Theory*, vol.45, no.5, pp.1717-1719, 1999.

[9] S. S. Ghoreishi and M. A. Pourmina, High speed RSA implementation based on modified Booth's technique and montgomery's multiplication for FPGA platform, *Proc. of the 2nd International Conference on Advances in Circuits, Electronics and Micro-Electronics*, pp.86-93, 2009.

[10] K. F. Hwang and C. C. Chang, A self-encryption mechanism for authentication of roaming and teleconference services, *IEEE Transactions on Wireless Communications*, vol.2, no.2, pp.400-407, 2003.

[11] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, vol.48, pp.203-209, 1987.
[12] J.-S. Lee, Y.-F. Chang and C.-C. Chang, Secure authentication protocols for mobile commerce transactions, *International Journal of Innovative Computing, Information and Control*, vol.4, no.9, pp.2305-2314, 2008.
[13] C. C. Lee, M. S. Hwang and I. E. Liao, Security enhancement on a new authentication scheme with anonymity for wireless environments, *IEEE Transactions on Industrial Electronics*, vol.53, no.5, pp.1683-1687, 2006.
[14] R. Rivest, A. Shamir and L. Aldeman, A method for obtaining digital signatures and public-key cryptosystems, *ACM Communication*, vol.21, no.2, pp.120-126, 1978.
[15] M. Scott, N. Costigan and W. Abdulwahab, Implementing cryptographic pairings on smartcards, *Proc. of Cryptographic Hardware and Embedded Systems*, vol.4249, pp.134-147, 2006.
[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
[17] J. Tate, WC-groups over p-adic fields, in *Séminaire N. Bourbaki*, Secretariat math'ematique, Paris, 1957.
[18] Z. J. Tzeng and W. G. Tzeng, Authentication of mobile users in third generation mobile system, *Wireless Personal Communications*, vol.16, no.1, pp.35-50, 2001.
[19] R.-C. Wang, W.-S. Juang and C.-L. Lei, A robust authentication scheme with user anonymity for wireless environments, *International Journal of Innovative Computing, Information and Control*, vol.5, no.4, pp.1069-1080, 2009.
[20] C. C. Wu, W. B. Lee and W. J. Tsaur, A secure authentication scheme with anonymity for wireless communications, *IEEE Communication Letters*, vol.12, no.10, pp.722-723, 2008.
[21] J. Xu, W. T. Zhu and D. G. Feng, An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks, *Computer Communications*, vol.34, no.3, pp.319-325, 2011.
[22] T. Y. Youn, Y. H. Park and J. Lim, Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks, *IEEE Communication Letters*, vol.13, no.7, pp.471-473, 2009.
[23] J. Zhu and J. Ma, A new authentication scheme with anonymity for wireless environments, *IEEE Transactions on Consumer Electronics*, vol.50, no.1, pp.230-234, 2004.