Published in IET Information Security
Received on 24th August 2009
Revised on 22nd February 2010
doi: 10.1049/iet-ifs.2009.0154

ISSN 1751-8709

Anonymous roaming in universal mobile telecommunication system mobile networks

M. Fatemi S. Salimi A. Salahi

Iran Telecommunication Research Centre, Tehran, Iran
E-mail: ssomayehs@yahoo.com

Abstract: A secure roaming protocol for mobile networks is proposed. Roaming has been analysed in some schemes from the security point of view; however, there are vulnerabilities in most of them and so the claimed security level is not achieved. The scheme offered by Wan *et al.* recently is based on hierarchical identity-based encryption, in which the roaming user and the foreign network mutually authenticate each other without the help of the home network. Although the idea behind this proposal is interesting, it contradicts technical considerations such as routing and billing. The proposed protocol makes use of similar functions used in Wan *et al.*'s scheme but contributes a distinguished structure that overcomes the previous shortcomings and achieves a higher possible level of security in mobile roaming as well as enhancing the security of the key issuing procedure.

1 Introduction

Owing to the tremendous development in wireless technology, user mobility has become an important network feature. Subscribers of a specific service network may wish to go outside the pre-scheduled coverage zone, which necessitates the indirect connection for accessing the services via foreign networks (FNs) (referred as roaming). There are three parties involved in a roaming scenario: a roaming user *U*, the user's home network (HN) and a visited FN, which has a roaming agreement with the user's HN. The user needs to be identified as an authorised subscriber of his HN in order to obtain the services from the FN. This will be achieved through a registration and authentication procedure between the user and the foreign server, which possibly will require the cooperation of the user's HN.

As a result of the open access nature of the radio interface in wireless transmission, more security measures should be provided in wireless networks compared to the wired networks. One of the prominent security issues in such networks is user's privacy. To preserve this feature, not only should user's identity be protected (anonymity requirement), but also his location and the relation between his activities should be kept secret (untraceability requirement). The violation of each of the mentioned requisites can seriously endanger the user's privacy. This problem is even more serious in a roaming scenario since a new entity, which is called FN, participates in all activities. So, the user's privacy should strongly be considered during the registration and authentication procedure in a roaming scenario.

Samfat *et al.* [1] have proposed a comprehensive classification for different levels of privacy protection according to the knowledge of different entities about the user's identification information. The classifications are as follows:

- C_1: Each user is anonymous to eavesdroppers and his activities are unlinkable to them.
- C_2: In addition to C_1, each user is anonymous to the foreign servers and his activities are unlinkable to them.
- C_3: In addition to C_2, the relationship between the user and servers (the home server and the foreign servers) is anonymous for eavesdroppers.
- C_4: In addition to C_3, the home server of the user is anonymous to the foreign servers.

- C_5: In addition to C_4, each user is anonymous and his activities are unlinkable to his home server.

It is mentioned in [1] that the levels C_4 and C_5 may be contradictory with other (unrelated to security) system requirements such as routing and billing. By introducing new techniques like onion routing [2], however, it has become realisable that the location information of participating users be even protected against their HNs without impeding the calls to be routed towards the users. In these techniques, each user submits a temporary number to the network. The network uses this number whenever it wants to page that user [3]. The solutions like this are mostly aimed at providing communication anonymity by means of anonymous routing algorithms in the context of mobile *ad hoc* networks. For example, the users need onion proxies that know the network topology [4].

The scenario that we consider in this paper is more compatible with the existing mobile network infrastructures in which the user needs to be reachable at any moment by a single identification (phone number). This necessitates that the home server be always aware of the mobile user's location in order to route the incoming calls towards the user. Moreover, the foreign server should know the identity of the home server for billing purposes. Therefore, it seems that the admissible level of privacy protection in this scenario is C_3 (note that we are not considering applications like e-cash, Internet surfing and e-mail checking in mobile networks).

The universal mobile telecommunication system (UMTS), the third generation of mobile technology, provides a limited C_1 class of privacy protection. In UMTS, similar to global system for mobile communication (the predecessor of UMTS), the roaming user sends his international mobile subscriber identity (IMSI) in clear during the first registration and receives a series of aliases known as temporary mobile subscriber identity (TMSI) for subsequent sessions. By using a different TMSI in each session, anonymity requirement is fulfilled to some extent; however, an adversary who continuously eavesdrops the radio interface can identify the user's IMSI and track his location.

A lot of schemes address the privacy of users in mobile networks [5–8]; however, they are mainly concentrated on the case where the user is in his home domain and so anonymity against the foreign servers is not investigated. As a result, they cannot be implemented in the roaming scenario. There are a number of other schemes which are claimed to achieve C_2 class of anonymity for roaming in UMTS [9–12], but some of them do not provide the security level they claim. For example, the scheme in [9] is vulnerable to deposit-case attack [13]. In the schemes proposed in [10, 12], there is some information leakage about the roaming user's identity from the parameters presented to the visited FNs. Hence, these schemes only provide C_1 class of privacy. It seems that the only secure protocol which meets the C_2 level of anonymity is presented in [11]; however, this protocol does not provide some security features such as key verification. The protocol in [11] is based on public key cryptosystem. Although mobile phones in the market today are powerful enough to run public key cryptography computations at reasonable speeds, it still involves the difficulties of a public key infrastructure (PKI).

Wan *et al.* [14] have recently proposed a privacy-preserving roaming protocol based on hierarchical identity-based encryption (IBE) [15] for mobile networks. This protocol is claimed to attain a new class of privacy protection, which is defined as follows:

- C_5^-: In addition to C_3, each user is anonymous and his activities are unlinkable to his home server, while foreign servers are allowed to know the identity of the home server.

As mentioned earlier, this security level necessitates a new infrastructure to make it possible for the HN to route the incoming calls towards the user, but no compensating infrastructure is taken into account in [14]. In the standard UMTS, the HN should be aware of the location of its users in order to route the incoming calls towards them. So, location privacy to the home server seems meaningless. Moreover, the FN should be able to prove the HN that it is serving one of the HN's users and asks for its payment. Besides the mentioned network issues, there is an anonymous key issuing protocol in [14] which sometimes fails the claimed level of security. In [14], every authorised user needs a pseudonym and a corresponding key to take part in a roaming scenario. However, it is assumed that a number of these requisite pairs (pseudonyms and temporary keys) are given to the users each time they participate in a key issuing protocol with their home server. In the case that a roaming user resides out of his HN domain for a long time, he would run out of pseudonyms and keys. This necessitates establishment of a connection between the user and its home server in order to receive a new set of the required roaming pairs. Since this connection should be held via the FNs, some information about the identity of the user and his home server reveals to the FNs which even contradicts the C_2 security requirements.

According to the above discussions, the most perfect and practical scheme that is proposed so far, achieves the C_2 class of anonymity and the possible C_3 class is not provided in UMTS yet. In this paper, we propose a roaming protocol with enhanced security for mobile networks. Our proposed protocol, like Wan *et al.*'s, benefits from the hierarchical identity-based cryptosystem and related functions. Indeed, in our protocol, it is assumed that the hierarchical identity-based cryptosystem is implemented in the system for the purpose of encryption and authentication. In spite of similarity in the case of functions, the structure of our protocol differs from Wan

IET Inf. Secur., 2010, Vol. 4, Iss. 2, pp. 93–103
doi: 10.1049/iet-ifs.2009.0154

et al.'s to much extent. Owing to this variation, our protocol achieves the acceptable C_3 level of privacy. This alteration is mainly concentrated on the structure of users' temporary keys. The temporary keys are generated for the users in order that they could prove their obligation to their home servers. Our scheme is designed in such a way that the users are able to calculate their temporary keys themselves instead of the home servers, that is, while both the HN and the FN should participate in the key issuing procedure, only the user has the ability to compute his next temporary key. Also, the foreign server needs the cooperation of the home server to authenticate the roaming user. However, the foreign server obtains no information about the user's identity or permanent key during this collaboration. Likewise, the home server does not gain any information about the user's pseudonym or the corresponding key used for authentication between the user and the foreign server. These added security features guarantee the acceptable C_3 level of privacy in our protocol. We compare the security features of our roaming protocol with those of previous ones and show that our protocol has reached the C_3 security level with one additional local signalling compared to the best previous result [11] which achieves C_2.

The remainder of this paper is organised as follows. In Section 2, the concepts of identity-based and hierarchical IBE are described and the functions e and h are introduced which play major roles in our protocol. In Section 3, Wan *et al.*'s roaming protocol is reviewed and its drawbacks are described in details. Our enhanced roaming protocol is presented in Section 4. In Section 5, the security features of the proposed protocol are evaluated. The protocol is compared with the previous works in Section 6. A brief comparison between the new roaming protocol and the one in [11] is also presented in this section. Finally, Section 7 concludes the paper.

2 Preliminary

In this section, we briefly introduce the concept of IBE as well as hierarchical IBE (HIBE) schemes. In 1984, Shamir [16] asked for an identity-based cryptosystem; however, the first well-designed IBE was not released until 2001 [17]. Recall that an IBE is a public key cryptosystem in which the public key takes any arbitrary string like a name or an e-mail address and the private key generator (PKG) could produce a private key corresponding to each string. Hence, one can encrypt a message by a public key even if the public key's owner has not yet set-up his private key. An IBE scheme has a number of inherent advantages over the public key cryptosystems such as easier revocation of public keys and delegation of decryption keys [17]. In addition, there is no need to store the public keys in a database (PKI) in IBE systems.

An IBE scheme consists of four randomised algorithms: set-up, extraction, encryption and decryption. Before explaining these algorithms, it is necessary to introduce the concept of a bilinear map between two groups which is used in IBE scheme and will be employed frequently in our protocol.

Let G_1 be an additive group and G_2 be a multiplicative group, both of order q for some large prime q (e.g. 160 bits). We say that a map $e: G_1 \times G_1 \rightarrow G_2$ is an admissible bilinear map if:

1. $e(aP, bQ) = e(P, Q)^{ab}$ for all $a, b \in Z_q$ and $P, Q \in G_1$ (bilinear condition).

2. The map does not send all elements of $G_1 \times G_1$ to the identity element of G_2 (non-degeneracy condition).

3. There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$ (computability condition).

An example of groups G_1 and G_2 and a bilinear map between them can be found in [17]. In that example, G_1 is a subgroup of the additive group of points of an elliptic curve E/F_p and G_2 is a subgroup of the multiplicative group of a finite field $F_{p^2}^*$.

The existence of an admissible bilinear map $e: G_1 \times G_1 \rightarrow G_2$ leads to the following results in groups G_1 and G_2 [17].

- The decision Diffie–Hellman problem in G_1 is easy, that is, it is easy to distinguish between the distributions $\langle P, aP, bP, abP\rangle$ and $\langle P, aP, bP, cP\rangle$ where a, b and c are random in Z_q^* and P is random in G_1^* but the computational Diffie–Hellman (CDH) problem in G_1 can be still hard (it is hard to find abP given random $\langle P, aP, bP\rangle$).

- The bilinear Diffie–Hellman (BDH) problem in $\langle G_1, G_2, e\rangle$ is not harder than the CDH in G_1 or G_2, but the converse is still an open problem. The BDH problem in $\langle G_1, G_2, e\rangle$ is as follows: given $\langle P, aP, bP, cP\rangle$ for some a, b, c in Z_q^* compute $W = e(P, P)^{abc} \in G_2$.

For further study on the relationship between the mentioned problems, refer to [18].

Remark 1: Consider the isomorphism induced from G_1 to G_2 by the bilinear map e. More specifically, for a point $Q \in G_1^*$ define the isomorphism f_Q: $G_1 \rightarrow G_2$ by $f_Q(P) = e(P, Q)$. As mentioned in [17], an efficient algorithm for inverting f_Q for some Q results in an efficient algorithm for solving CDH problem in G_2. Consequently, the isomorphism f_Q is believed to be a one-way function whenever CDH is believed to be hard in G_2 as is the case in all of the examples in [17]. Therefore throughout this paper the bilinear map e is considered as a one-way function (P cannot be inferred from $e(P,Q)$ and Q).

Let n be the length of the message to be encrypted. The IBE scheme is as follows:

Set-up: Pick a random generator $P \in G_1$ and a random secret $s \in Z_q^*$. Choose cryptographic hash functions H_1: $\{0, 1\}^* \rightarrow G_1^*$, H_2: $G_2 \rightarrow \{0, 1\}^n$, H_3: $\{0, 1\}^n \times \{0, 1\}^n \rightarrow Z_q^*$ and H_4: $\{0, 1\}^n \rightarrow \{0, 1\}^n$. In this system, the public parameters are $\{G_1, G_2, e, P, sP, H_1, H_2, H_3, H_4\}$ and the master key is s.

Extraction: Each user's identity-based private key should be computed as $k_U = sH_1(U)$, where $U \in \{0, 1\}^*$ is the user's identity.

Encryption: To encrypt $M \in \{0, 1\}^n$ using the public key U, choose a random $\sigma \in \{0, 1\}^n$ and set $r = H_3(\sigma, M)$. The ciphertext will be $\langle C = rP, \ \sigma \oplus H_2 \ (g_U^r), \ M \oplus H_4(\sigma)\rangle$, where $g_U = e(H_1(U), sP) \in G_2$.

Decryption: Let $C = \langle X, Y, Z\rangle$ be a ciphertext encrypted with U. If $X \notin G_1^*$, reject the ciphertext. Otherwise, compute $Y \oplus H_2(e(k_U, X)) = \sigma$ and $Z \oplus H_4(\sigma) = M$. If $X = H_3(\sigma, M)P$, report M as the decryption of C.

The above IBE scheme is resistant to the chosen ciphertext attack, assuming the hardness of the BDH problem [17]. Similar to public key cryptosystems, a hierarchy of PKGs is desirable in an IBE system to reduce the workload on master servers. A two-level HIBE (2-HIBE) is presented in [15]. There are three entities involved in a 2-HIBE scheme: a root PKG which possesses a master key s, domain PKGs which gain their domain keys from the root PKG and users with private keys generated by their domain PKGs. The 2-HIBE scheme benefits from a linear one-way function h: $G_1 \times Z_q^* \rightarrow G_1$ with the following properties:

1. For all $P \in G_1$, $a, x \in Z_q^*$, $h(aP, x) = ah(P, x)$.

2. Given $x, x_i \in Z_q^*$, $P \in G_1$ and $\langle x_i, h(aP, x_i)\rangle$ for $i = 1, \ldots, n$, $h(aP, x)$ could not be computed with any probabilistic polynomial-time algorithm.

Remark 2: The function h defined above is a one-way function with respect to its first argument, that is, P cannot be inferred from $h(P, x)$ and x.

The 2-HIBE system is defined as follows:

Set-up: Pick a random generator $P \in G_1$ and a random secret $s \in Z_q^*$. Choose cryptographic hash functions: H_1: $\{0, 1\}^* \rightarrow G_1$, H_2: $\{0, 1\}^* \rightarrow Z_q^*$ and H_3: $G_2 \rightarrow \{0, 1\}^n$. The public parameters are $\{G_1, G_2, e, P, sP, H_1, H_2, H_3\}$ and the master key is s.

KeyGen1: The key for domain S is $k_S = sH_1(S) \in G_1$.

KeyGen2: The key for user U in domain S is $k_U = h(k_S, H_2(S\|U)) \in G_1$.

Encryption: To encrypt $M \in \{0, 1\}^n$ with use of the public key $\langle S, U\rangle$, choose a random $r \in Z_q^*$. The ciphertext will be $C = \langle rP, \ M \oplus H_3(g)\rangle$, where $g = e(h(H_1(S), H_2(S\|U)), sP)^r$.

Decryption: Let $C = \langle rP, X\rangle$ be a ciphertext encrypted with $\langle S, U\rangle$. Compute $M = X \oplus H_3(e(k_U, rP))$ as the decryption of C.

3 Review of Wan *et al.*'s roaming protocol

In this section, we will review the roaming protocol proposed by Wan *et al.* [14] and discuss its defects. The protocol utilises a 2-HIBE scheme for both authentication/key agreement and encryption. A master secret s is generated by a trusted root server and the public key consists of $\{G_1, G_2, e, P, sP, H_1, H_2, H_3\}$ (H_1, H_2 and H_3 are the hash functions introduced in the definition of the 2-HIBE scheme and P is a random generator of G_1). Also, the root server generates a domain key $k_S = sH_1(S)$ for a server with the identity S.

When a user registers at his home domain HS with his real identity U, he receives a private key $K = h(k_{HS}, H_2(HS\|U))$ from the HS. Afterwards, whenever the home server receives a number of aliases $Nym_1, \ldots, Nym_n$ from the user U during a key issuing procedure, it computes the corresponding keys $k_i = h(k_{HS}, H_2(HS\|Nym_i))$ and sends them back to the user. The roaming protocol is depicted in Fig. 1.

As shown in Fig. 1, the roaming protocol consists of four message transmissions at the end of which, the foreign server and the roaming user authenticate each other and agree on the session keys sk_s and sk_u, respectively, such that $sk_u = sk_s$. H_4 is a hash function which maps $\{0, 1\}^*$ to $\{0, 1\}^l$ for some security parameter l and $E_S(X)$ denotes the ID-based encryption of message X with the public key S. As illustrated in the figure, in this protocol only the roaming user and the FN server are involved, without assistance of the user's HN.

The user U needs an unused pseudonym Nym_i and the corresponding private key k_i each time he participates in a roaming protocol within a FN's zone. Hence, when he uses up his private keys, he should resubmit new pseudonyms to his home server in order to obtain new private keys. This will be done through a private ID-based key issuing procedure as follows (the steps are exactly quoted from [14]):

1. The user U chooses a random number N_u and a number of pseudonyms Nym_i, $i = 1, \ldots, n$ and encrypts them using the home server's public key. He computes a signature using his ID-based key and sends U, N_u, E_{HS} $(Nym_1, \ldots, Nym_n, N_u)$, Sig_U $(U, N_u, Nym_1, \ldots, Nym_n)$ to the home server.

2. The home server decrypts the ciphertext to obtain Nym_i and N_u, and verifies the signature. If the signature is valid, the home server computes $k_i = h(k_{HS}, H_2(HS\|Nym_i))$ and

IET Inf. Secur., 2010, Vol. 4, Iss. 2, pp. 93–103
doi: 10.1049/iet-ifs.2009.0154

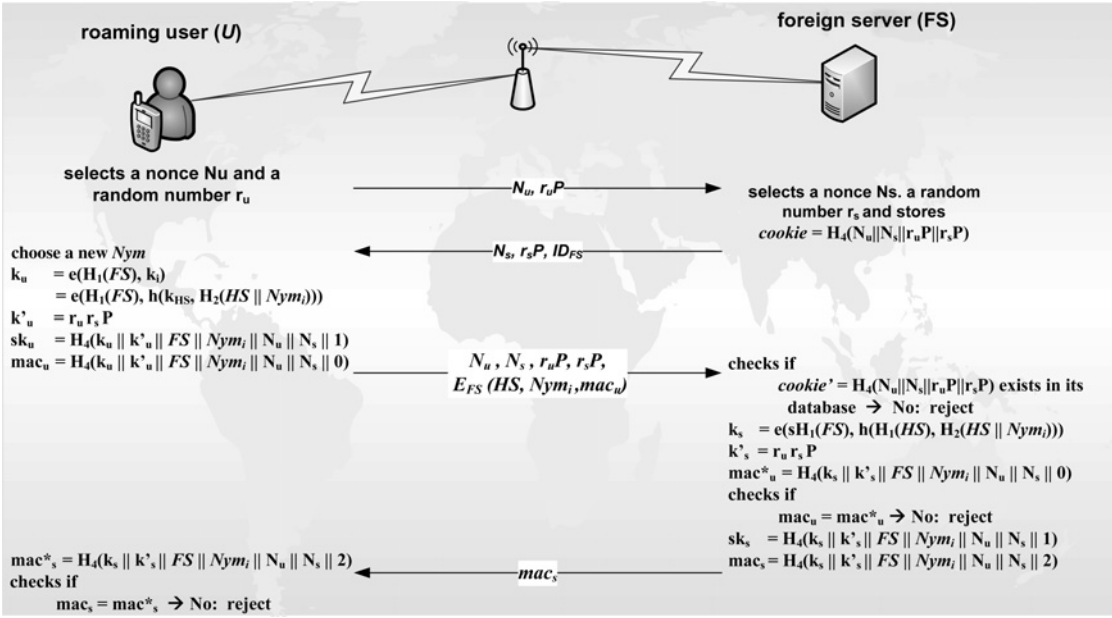

Figure 1 *Wan et al.'s roaming protocol*

sends $E_U(k_1, \ldots, k_n, N_u, N_s)$ and $\mathrm{Sig}_{HS}(k_1, \ldots, k_n, N_u, N_s)$ back to the user.

3. The user decrypts the ciphertext to obtain k_i, N_u and N_s. He also verifies the signature in the message and accepts k_i if the signature is valid.

The problem of Wan *et al.*'s roaming protocol becomes evident when the user participates in the key issuing procedure while connecting to the HN via a foreign server. Since all the messages are sent from the foreign server, the home server becomes aware of the user's location which contradicts the claimed privacy level (C_{5-}). Besides, the user sends his real identity in clear which contravenes even the C_1 requirements. Even if we accept that the user encrypts his message with the foreign server's public key before sending, at least the FN is aware of user's identity which contradicts the C_2 requirements. Note that we cannot assume that the anonymous key issuing protocol is just supposed to be used during the registration phase. With such an assumption, the user would just receive a limited number of pseudonyms and the corresponding keys, which constrains the user to restricted times of roaming.

The fundamental drawback of the mentioned protocol is its inappropriate level of security due to the protection of the user's location from his home server. Since the foreign and the home servers do not communicate during the authentication process, the location of the user remains unknown for the home server. Therefore the home server could not divert the calls towards the roaming user. In addition, since the foreign server could not prove the provided services to a visitor user, it could not charge its home server.

4 Anonymous roaming protocol

In this section, we present an enhanced roaming protocol which achieves C_3 level of security in mobile networks. Our protocol uses similar functions to Wan *et al.*'s (including hashes H_1, H_2, H_3, H_4 and the functions e and h) while eliminates its stated drawbacks and improves the key issuing procedure. The security of the protocol will be discussed in the next section.

4.1 Protocol

Again, we assume that a 2-HIBE is implemented in the system and the servers have received their private keys $\{sH_1(S_i)\}$. Also, we suppose that the user U obtains his private key $K_U = h(k_{HS}, H_2(HS\|U))$ during the registration at his home server. However, the structure of temporary keys has changed significantly and the key k corresponding to a pseudonym Nym is found through $k = e(h(h(H_1(HS), H_2(HS\|Nym)), H_2(HS)), sH_1(HS))$. This key will be computed by the user during the roaming protocol and will be used for the authentication and key agreement purposes when he enters another FN domain. In other words, when a user enters a FN domain, he fetches the pre-processed and unused pair of an alias and the corresponding temporary key from his memory. He introduces himself by this alias to the foreign server. Since the user could not generate a valid temporary key (related to an alias) without the home server's assistance, the temporary key can be interpreted as a warrant to verify user's subscription to his home server. Also, this key will be used in the session key generation. The session key will be subsequently employed to protect the connection between the user and the foreign server. Since the user needs a new pair of a pseudonym and the corresponding key for the next protocol execution, the key issuing takes place during

doi: 10.1049/iet-ifs.2009.0154

the authentication and key agreement protocol. That is the user chooses an arbitrary alias and drives some pseudorandom values from this selected alias. Then he sends these values to the foreign server and asks the foreign server and the home server to collaborate with him on the key generation. The protocol is designed such that the servers do not gain any information about the alias or the corresponding key. Finally, the user verifies the computed temporary key with the aid of his private key K_U.

As shown in Fig. 2, since we are considering the C_3 level of privacy, we involve the home server in our roaming protocol.

The protocol is as follows:

- When the foreign server detects a new user in his domain, it generates a nonce N_s and a random number r_s (both from Z_q^*) and computes r_sP. Then it stores the values N_s and r_sP in his database and sends the first message including his identity $\mathrm{ID_{FS}}$, N_s and r_sP to the user.

- Similarly, the user U generates a nonce N_u and a random number r_u and computes $k'_u = r_ur_sP$. Then he fetches the only unused pair of (Nym, k) from his memory and computes the session key to be shared with the foreign server as sk_u and a verifier mac_u according to relations (1) and (2)

$$\mathrm{sk}_u = H_4(k\|k'_u\|\mathrm{FS}\|\mathrm{Nym}\|N_u\|N_s\|1) \quad (1)$$

$$\mathrm{mac}_u = H_4(k\|k'_u\|\mathrm{FS}\|\mathrm{Nym}\|N_u\|N_s\|0) \quad (2)$$

After that, he selects an arbitrary $\mathrm{Nym_{next}}$ to be used in the next execution of the roaming protocol (either in the current FS or another FS). In order to compute the corresponding key k_{next} with the help of FS and HS, the user selects a random number $a^* \in Z_q^*$ and computes the following values

$$x_1^* = h(h(a^*H_1(\mathrm{HS}), H_2(\mathrm{HS}\|\mathrm{Nym_{next}})), H_2(\mathrm{HS})) \quad (3)$$

$$x_2^* = h(h(a^*H_1(\mathrm{HS}), H_2(\mathrm{HS}\|U)), H_2(\mathrm{HS})) \quad (4)$$

Also, he chooses random numbers b, a_1, $a_2 \in Z_q^*$ and computes $a_1x_1^*$, $a_2x_2^*$ and $E_{\mathrm{HS}}(b, U, E(K_U, U), \mathrm{ID_{FS}})$, where $E(K_U, U)$ is the symmetric encryption of U with the key K_U. Next, he sends the values $E_{\mathrm{FS}}(\mathrm{Nym}, \mathrm{ID_{HS}})$, N_u, r_uP, N_s, r_sP, mac_u, x_1^*, $a_1x_1^* + a_2x_2^*$ and $E_{\mathrm{HS}}(b, U, E(K_U, U), \mathrm{ID_{FS}})$ to the foreign server.

- Upon receiving the above values, the foreign server checks if N_s and r_sP exist in its database and aborts the connection if it does not find such values. Otherwise, it decrypts $E_{\mathrm{FS}}(\mathrm{Nym}, \mathrm{ID_{HS}})$ with its private key $sH_1(\mathrm{FS})$ and obtains the Nym and $\mathrm{ID_{HS}}$. Then, it generates a random number $c \in Z_q^*$ and computes z

$$z = h(h(cH_1(\mathrm{HS}), H_2(\mathrm{HS}\|\mathrm{Nym})), H_2(\mathrm{HS})) \quad (5)$$

- Subsequently, the FS sends z and $E_{\mathrm{HS}}(b, U, E(K_U, U), \mathrm{ID_{FS}})$ to the HS.

- The home server decrypts the message $E_{\mathrm{HS}}(b, U, E(K_U, U), \mathrm{ID_{FS}})$ with its private key $sH_1(\mathrm{HS})$ and checks whether it has received the messages from the server with the identity $\mathrm{ID_{FS}}$ or not. Then it authenticates the user U by verifying the correctness of $E(K_U,U)$. The home server terminates the connection if any of these verifications fails. Otherwise, it computes the following values and sends them back to the FS.

$$y = e(z, sH_1(\mathrm{HS})) \quad (6)$$

$$sH_1(\mathrm{HS}) - bH_1(\mathrm{HS}) = (s - b)H_1(\mathrm{HS}) \quad (7)$$

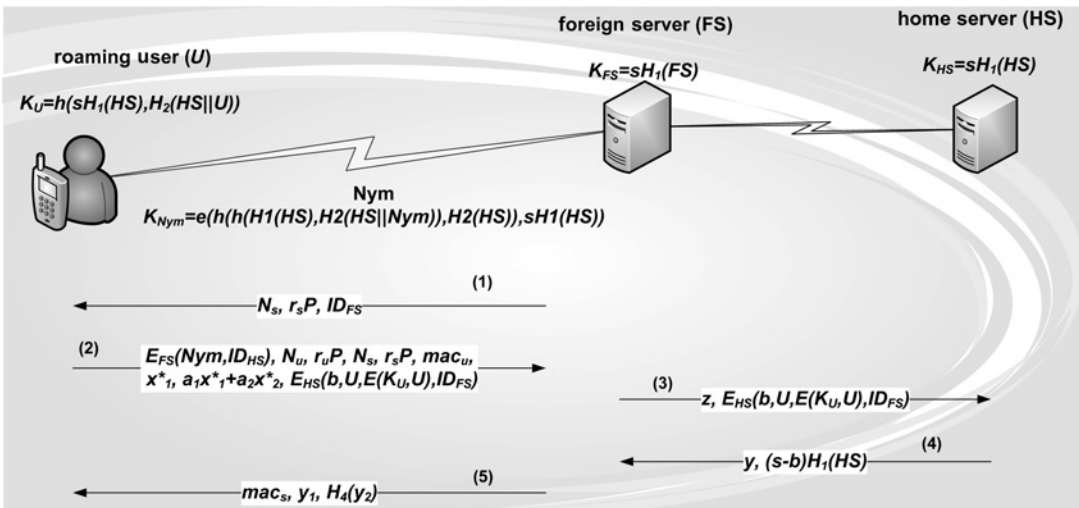

Figure 2 *Signalling in the anonymous roaming protocol*

IET Inf. Secur., 2010, Vol. 4, Iss. 2, pp. 93–103
doi: 10.1049/iet-ifs.2009.0154

- The FS computes $k_s' = r_s r_u P$ and the values

$$k^* = y^{c^{-1}} \tag{8}$$

$$\text{mac}_u^* = H_4(k^* \| k_s' \| \text{FS} \| \text{Nym} \| N_u \| N_s \| 0) \tag{9}$$

The FS rejects the connection if the equality $\text{mac}_u = \text{mac}_u^*$ does not hold. Otherwise, it accepts k^* as the user's key corresponding to Nym and authenticates the user. The computed k^* together with the message $E_{\text{HS}}(b, U, E(K_{\text{U}}, U\|b), \text{ID}_{\text{FS}})$ are credentials by which the foreign server will be able to request the user's home server for service charge. Indeed, these values become a proof for payment request. In the next step, the foreign server computes the session key sk_s and the authenticator mac_s according to relations (10) and (11)

$$\text{sk}_s = H_4(k^* \| k_s' \| \text{FS} \| \text{Nym} \| N_u \| N_s \| 1) \tag{10}$$

$$\text{mac}_s = H_4(k^* \| k_s' \| \text{FS} \| \text{Nym} \| N_u \| N_s \| 2) \tag{11}$$

Moreover, the foreign server calculates y_1 and y_2 to make the computation of k_{next} feasible for the user.

$$y_1 = e(x_1^*, (s-b)H_1(\text{HS})) \tag{12}$$

$$y_2 = e(a_1 x_1^* + a_2 x_2^*, (s-b)H_1(\text{HS})) \tag{13}$$

Finally, it returns mac_s, y_1 and $H_4(y_2)$ to the user.

- When the user receives the messages from the foreign server, he computes

$$\text{mac}_s^* = H_4(k^* \| k_u' \| \text{FS} \| \text{Nym} \| N_u \| N_s \| 2) \tag{14}$$

and checks the equality $\text{mac}_s = \text{mac}_s^*$. If it does not hold, the user aborts the connection. Otherwise, he authenticates the foreign server and computes the following values

$$y_1^* = y_1 \cdot e(x_1^*, bH_1(\text{HS})) \tag{15}$$

$$k_{\text{next}} = (y_1^*)^{a^* 1} \tag{16}$$

$$y_2^* = (y_1)^{a_1}[e(h(a^* K_{\text{U}}, H_2(\text{HS})), H_1(\text{HS}))e(x_2^*, -bH_1(\text{HS}))]^{a_2} \tag{17}$$

Afterwards, the user considers whether $H_4(y_2) = H_4(y_2^*)$ or not. If the equation holds, he accepts k_{next} as the key corresponding to Nym_{next}. If not, he rejects the connection.

If all the verifications pass successfully, at the end of the protocol, the user authenticates the foreign server as a legal server authorised by the root server and computes a key for his next alias. Besides, the foreign server authenticates the user as a certified user of the home server and informs the home server about presence of one of its users in its domain. Nym is the name by which the foreign server identifies the user (i.e. an identity for the user in the foreign server's domain) and $\text{sk}_u = \text{sk}_s$ is the key that the user and the home server have agreed upon to be used for security purposes.

4.2 Proofs

Now we consider the equations employed in the protocol and present proofs for the less obvious ones. The following theorems and their corresponding proofs are valid with the assumption of correctness of the values computed by different entities.

Theorem 1: The key k^* computed by the foreign server through (9) is equivalent to the user's key k.

Proof:

$$\begin{aligned}
k_{\text{next}} &= (y_1^*)^{(a^*)^{-1}} = [y_1 e(x_1^*, bH_1, (\text{HS}))]^{(a^*)^{-1}} \\
&= [e(x_1^*, (s-b)H_1(\text{HS}))]e(x_1^*, bH_1(\text{HS}))]^{(a^*)^{-1}} \\
&= [e(x_1^*, sH_1(\text{HS}))]^{(a^*)^{-1}} = e((a^*)^{-1}x_1^*, sH_1(\text{HS})) \\
&= e((a^*)^{-1}h(h(a^*H_1(\text{HS}), H_2(\text{HS}\|\text{Nym}_{\text{next}})), \\
&\quad H_2(\text{HS})), sH_1(\text{HS})) \\
&= e(h(h((a^*)^{-1}a^*H_1(\text{HS}), H_2(\text{HS}\|\text{Nym}_{\text{next}})), \\
&\quad H_2(\text{HS})), sH_1(\text{HS})) \\
&= e(h(h(H_1(\text{HS}), H_2(\text{HS}\|\text{Nym}_{\text{next}})), H_2(\text{HS})), sH_1(\text{HS}))
\end{aligned}$$

□

Theorem 2: The key k_{next} calculated by the user through (16) is the key corresponding to Nym_{next}.

Proof:

$$\begin{aligned}
k_{\text{next}} &= (y_1^*)^{(a^*)^{-1}} = [y_1 e(x_1^*, bH_1, (\text{HS}))]^{(a^*)^{-1}} \\
&= [e(x_1^*, (s-b)H_1(\text{HS}))]e(x_1^*, bH_1(\text{HS}))]^{(a^*)^{-1}} \\
&= [e(x_1^*, sH_1(\text{HS}))]^{(a^*)^{-1}} = e((a^*)^{-1}x_1^*, sH_1(\text{HS})) \\
&= e((a^*)^{-1}h(h(a^*H_1(\text{HS}), H_2(\text{HS}\|\text{Nym}_{\text{next}})), \\
&\quad H_2(\text{HS})), sH_1(\text{HS})) \\
&= e(h(h((a^*)^{-1}a^*H_1(\text{HS}), H_2(\text{HS}\|\text{Nym}_{\text{next}})), \\
&\quad H_2(\text{HS})), sH_1(\text{HS})) \\
&= e(h(h(H_1(\text{HS}), H_2(\text{HS}\|\text{Nym}_{\text{next}})), \\
&\quad H_2(\text{HS})), sH_1(\text{HS}))
\end{aligned}$$

□

Theorem 3: The value y_2^* in (17) is equivalent to the y_2 computed in (13).

doi: 10.1049/iet-ifs.2009.0154

Proof:

$$
\begin{aligned}
y_2^* &= (y_1)^{a_1}[e(h(a^*K_U, H_2(\mathrm{HS})), H_1(\mathrm{HS}))e(x_2^*, \\
&\quad -bH_1(\mathrm{HS}))]^{a_2} \\
&= [e(x_1^*, (s-b)H_1(\mathrm{HS}))]^{a_1}[e(h(a^*h(sH_1(\mathrm{HS}), \\
&\quad H_2(\mathrm{HS}\|U)), H_2(\mathrm{HS})), H_1(\mathrm{HS}))e(x_2^*, -bH_1(\mathrm{HS}))]^{a_2} \\
&= e(a_1x_1^*, (s-b)H_1(\mathrm{HS}))[e(h(h(a^*H_1(\mathrm{HS}), H_2(\mathrm{HS}\|U)), \\
&\quad H_2(\mathrm{HS})), sH_1(\mathrm{HS}))e(x_2^*, -bH_1(\mathrm{HS}))]^{a_2} \\
&= e(a_1x_1^*, (s-b)H_1(\mathrm{HS}))[e(x_2^*, sH_1(\mathrm{HS}))e(x_2^*, \\
&\quad -bH_1(\mathrm{HS}))]^{a_2} \\
&= e(a_1x_1^*, (s-b)H_1(\mathrm{HS}))[e(x_2^*, (s-b)H_1(\mathrm{HS}))]^{a_2} \\
&= e(a_1x_1^*, (s-b)H_1(\mathrm{HS}))e(a_2x_2^*, (s-b)H_1(\mathrm{HS})) \\
&= e(a_1x_1^* + a_2x_2^*, (s-b)H_1(\mathrm{HS})) = y_2
\end{aligned}
$$

□

5 Protocol evaluation and security analysis

In this section, we evaluate the proposed roaming protocol in view points of security goals and security levels enumerated in previous sections. For this purpose, it is necessary to investigate the structure of temporary keys and the variables used in the protocol at the first instance.

5.1 Evaluating the structure of temporary keys and other variables in the protocol

In the proposed protocol, the user chooses an arbitrary string as his next alias and attempts to calculate the corresponding key. This is carried out with the help of both the current visited foreign server and the home server during the authentication and key agreement procedure. To assure the untraceability and privacy of the user, no information should be disclosed about $\mathrm{Nym}_{\mathrm{next}}$ and k_{next} to neither the servers nor the eavesdroppers during the key issuing procedure. The suggested structure for users' keys is chosen based on the following requirements:

- A user should not be able to compute a temporary key corresponding to a pseudonym without the help of his home server; however, there is no need to inform the home server of the pseudonym to obtain the related key.

- The user should be able to verify the resultant key by the help of his permanent private key. Indeed, the user could use his private key K_U to produce a similar structure to the temporary keys related to his permanent identity U and exploit the result as a reference in the key verification.

According to the specifications of the bilinear map e and the linear one-way function h and with the aid of random values, no information leaks about $\mathrm{Nym}_{\mathrm{next}}$ from the variables sent by the user. These variables include x_1^* and $a_1x_1^* + a_2x_2^*$. Moreover, the variables $y = e(z, sH_1(\mathrm{HS}))$ and $(s-b)H_1(\mathrm{HS})$ reveal no information about the home server's key to the foreign server. Also, the user could not obtain any information about the home server's key $sH_1(\mathrm{HS})$ by accessing the values $y_1 = e(x_1^*, (s-b)H_1(\mathrm{HS}))$, $y_2 = e(a_1x_1^* + a_2x_2^*, (s-b)H_1(\mathrm{HS}))$, k and K_U. Hence, he would not be able to calculate the related key to an alias without the assistance of the home and foreign servers.

5.2 Verification of the computed key corresponding to the next pseudonym

To assure about the correctness of the calculated k_{next}, the user computes an auxiliary variable x_2^* and sends $a_1x_1^* + a_2x_2^*$ to the foreign server. Then he computes $e(x_2^*, sH_1(\mathrm{HS})) = e(h(K_U, H_2(\mathrm{HS})), H_1(\mathrm{HS}))^{a^*}$ and uses it as a reference to decide whether y_1^* in (15) is equal to $e(x_1^*, sH_1(\mathrm{HS}))$ or not. The correct y_1^* results in a reliable k_{next}. The verification process is carried out corresponding to (15)–(17).

5.3 Mutual authentication between the user and the visited foreign server

The user and the foreign server mutually authenticate each other through mac_s and mac_u, respectively. Since the foreign server receives an encrypted pseudonym Nym, it is able to compute mac_s only if it knows the private key $sH_1(\mathrm{FS})$. Also, calculation of mac_u by the user means that he knows the key k corresponding to Nym, which subsequently denotes that the user is an authorised subscriber of his home server.

5.4 Mutual authentication between the user and his home server

The roaming user has to be ensured that the home server is informed about his location for routing purposes. It realises when the user verifies mac_s since the foreign server needs the help of the home server in order to compute k which is used in calculation of mac_s. Furthermore, the home server authenticates the user through the message $E_{\mathrm{HS}}(b, U, E(K_U, U), \mathrm{ID}_{\mathrm{FS}})$.

5.5 Anonymity of the user

The user makes use of pseudonyms to be identified by the foreign servers and no one except the home server gets aware of the user's real identity. Moreover, each pseudonym is used only once and the user chooses a different alias for the next identification. This approach makes the user untraceable.

5.6 Security against the deposit-case attack

In the deposit-case attack scenario, a malicious server M attempts to change the messages from the roaming user to the foreign server such that the foreign server believes that M is the user's home server and sends the signalling

IET Inf. Secur., 2010, Vol. 4, Iss. 2, pp. 93–103
doi: 10.1049/iet-ifs.2009.0154

towards M, without being detected by the user nor the real home server. In our protocol, if a malicious server M changes the message $E_{FS}(\text{Nym}, \text{ID}_{HS})$ in order to replace ID_{HS} with ID_M, the foreign server obtains a false Nym which could be detected via mac_u.

5.7 Perfect forward secrecy

Our proposed roaming protocol makes use of elliptic curve-based Diffie–Hellman key exchange protocol to establish a session key between the user and the foreign server. Therefore it has perfect forward secrecy. That is, even if an adversary has compromised all the long-term keys of all the participants, he could not obtain past session keys. With the use of Macs, our protocol defends against the man-in-the-middle attack.

According to the above considerations, our roaming protocol achieves the C_3 level of security. Also, the foreign server could prove the presence of the home server's subscriber in its domain on the strength of the message $E_{HS}(b, U, E(K_U, U), \text{ID}_{FS})$ and so charges the related home server.

6 Comparison between the proposed protocol and the previous works

Before we present a comparison between the new roaming protocol and all the previous works, we briefly introduce the protocol in [11] and compare it with the one introduced in this paper. The reason behind the selection of [11] is that this is the only previous roaming protocol which achieves C_2.

The protocol in [11] is shown in Fig. 3. Here, $E_S(\cdot)$ denotes the public key cryptography with the public key of S. $\text{mac}_{K_U}(\cdot)$ and $\text{Sig}_S(\cdot)$ show the mac produced with K_U and the signature produced by S, respectively. s is the session ID and g is a generator of a multiplicative group of order q in which the CDH is assumed to be hard. x and y are random elements in Z_q^* chosen by the roaming user and the foreign server, respectively.

In the protocol in [11], the roaming user employs an alias to introduce himself to the foreign server. He sends the identity of HS together with a nonce for FS. He also sends the message c_1 to be delivered to HS. Upon the receipt of this message, FS produces a nonce and sends c_1 and N_s to the HS. The HS decrypts c_1 and obtains the permanent key K_U. It checks if the key exists in its database and then checks the validity of $\text{mac}_{K_U}(m_1, \text{count}_U, \text{ID}_{HS})$. HS also checks if it has received the message from a server with the identity specified in m_1. If all the verifications hold, it sends m_2, $\text{SIG}_{HS}(m_2, N_s, \text{ID}_{FS})$ back to FS. The FS now obtains the temporary identity (alias) of the roaming user.

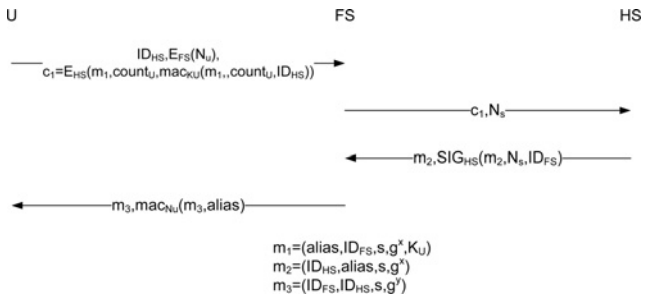

Figure 3 *Roaming protocol in [11]*

Table 1 Comparison of implementation and security features between our proposed roaming protocol and the previous ones

	GK [9]	ZM [12]	YWD [11]	JLSS [10]	WKP [14]	Our protocol
Cryptosystem	public key	public key	public key	symmetric key	ID-based	ID-based
Security level	C_1	C_1	C_2	C_1	unacceptable C_{5-} in standard UMTS	C_3
Communication cost	3L + 2I	2L + 2I	2L + 2I	4L + 2I[a]	4L[b]	3L + 2I
Key verification	–	–	–	–	no	yes
Alias concealment from the HS	yes	no alias	no	no	no	yes
U/HS authentication	mutual	mutual	mutual	mutual	no	mutual
U/FS authentication	mutual	mutual	mutual	mutual	mutual	mutual
Forward secrecy	yes	no	yes	no	yes	yes

L: local communication, I: inter-domain communication
[a]2L + 2I communications are needed for authentication and two extra local communications are needed for key agreement
[b]2L + 2I extra communications are needed during the key issuing procedure

It verifies the correctness of the signature and then produces a random number $y \in Z_q^*$, calculates the session key $(g^x)^y$ and sends the message $m_3 \mathrm{mac}_{N_U}(m_3, \text{alias})$ to the user. Upon receipt of this message, the user checks if mac is produced properly and then computes the session key as $(g^x)^y$.

At the end of this protocol, the user and the home server have mutually authenticated each other. Similarly, the user and the foreign server have authenticated each other and agreed upon a session key. However, an eavesdropper can easily obtain the identity of the user's home server. Also, there is no way for the user and FS to assure that they have obtained the correct session key. As a consequence, the protocol in [11] provides the security level C_2 with the cost of four communications, but it does not satisfy the key verification characteristic. On the other hand, our proposed protocol achieves the security level C_3 with one additional local communication, while assures the key verification property. In addition, the aliases in [11] are known for the home server and it can easily track the user in FN domains, while they are kept secret towards the home server in our protocol.

A comparison between the security features of our roaming protocol and the previous proposed protocols is given in Table 1. It can be seen that compared to the best previously proposed protocol in UMTS at [11], our protocol achieves a higher security level with only one additional local communication as well as the superiority that our protocol uses an ID-based cryptosystem instead of the public key one. The protocol in [14] is also shorter than our protocol; however, it provides an unacceptable level of security and even sometimes violates the C_2.

7 Conclusion

In this paper, we presented a secure roaming protocol, which achieves C_3 level of anonymity in mobile networks according to the classification based on Samfat *et al.*'s work. The proposed roaming protocol makes use of hierarchical identity-based cryptosystems instead of public key cryptosystems, and so there is no need to a PKI. Likewise, it benefits from two maps introduced by the IBE and HIBE systems in the key issuing procedure. With an appropriate usage of these maps properties, we could involve the visited foreign server, the home server and the user in the next key generation procedure, while the user is the only entity who gets aware of the generated key. This feature improves the privacy (including un-traceability) of the user. The key issuing is a mandatory procedure and happens during the authentication and key agreement protocol. Also, the capability of verifying the generated key by the user is added to the protocol. We compared our proposed roaming protocol with the previous works and demonstrated that it has provided a significantly higher level of privacy for the roaming user.

8 References

[1] SAMFAT D., MOVLA R., ASOKAN N.: 'Untraceability in mobile networks'. ACM Mobicom'95, 1995, pp. 26–36

[2] REED M., SYVERSON P., GOLDSCHLAG D.: 'Anonymous connections and onion routing', *IEEE J. Select. Areas Commun.*, 1998, **16**, (4), pp. 482–494

[3] REED M., SYVERSON P., GOLDSCHLAG D.: 'Protocols using anonymous connections: mobile applications'. 5th Int. Workshop Proc. Security Protocols, 1998 (*LNCS*, **1361**), pp. 13–23

[4] ARDAGNA C.A., JAJODIA S., SAMARATI P., STAVROU A.: 'Privacy preservation over untrusted mobile networks'. Privacy in location-based applications: research issues and emerging trends book contents, 2009 (*LNCS*), Vol. 5599, pp. 84–105

[5] BARBEAU M., ROBERT J.M.: 'Perfect identity concealment in UMTS over radio access links'. IEEE Int. Conf. Wireless and Mobile Computing, Networking and Communications (WiMob'05), August 2005, pp. 72–77

[6] JUANG W.S., WU J.L.: 'Efficient 3GPP authentication and key agreement with robust user privacy protection'. Proc. IEEE Wireless Communications and Networking Conf. WCNC'07, 2007, pp. 2720–2725

[7] KIM W.H., YOON E.J., YOO K.Y.: 'A new authentication protocol providing user anonymity in open network'. WINE'05, 2005 (*LNCS*, **3828**), pp. 414–423

[8] SATTARZADEH B., ASADPOUR M., JALILI R.: 'Improved user identity confidentiality for UMTS mobile networks'. Proc. Fourth European Conf. on Universal Multiservice Networks, 2007, pp. 401–409

[9] GO J., KIM K.: 'Wireless authentication protocol preserving user anonymity'. Symp. Cryptography and Information Security (SCIS 2001), 2001, pp. 159–164

[10] JIANG Y., LIN C., SHEN S., SHI M.: 'Mutual authentication and key exchange protocols for roaming services in wireless mobile networks', *IEEE Trans. Wirel. Commun.*, 2006, **5**, (9), pp. 2569–2577

[11] YANG G., WONG D.S., DENG X.: 'Efficient anonymous roaming and its security analysis'. ACNS'05, 2005 (*LNCS*, **3531**), pp. 334–349

[12] ZHU J., MA J.: 'A new authentication scheme with anonymity for wireless environments', *IEEE Trans. Consum. Electron.*, 2004, **50**, (1), pp. 231–235

[13] YANG G., WONG D.S., DENG X.: 'Deposit-case attack against secure roaming'. Tenth Australasian Conf. Information

IET Inf. Secur., 2010, Vol. 4, Iss. 2, pp. 93–103
doi: 10.1049/iet-ifs.2009.0154

Security and Privacy (ACISP 2005), 2005 (*LNCS*, **3574**), pp. 417–428

[14] WAN Z., REN K., PRENEEL B.: 'A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks'. First ACM Conf. on Wireless Network Security (WiSec'08), 2008

[15] HORWITZ J., LYNN B.: 'Toward hierarchical identity-based encryption'. Proc. EUROCRYPT'02, 2002 (*LNCS*, **2332**), pp. 466–481

[16] SHAMIR A.: 'Identity-based cryptosystems and signature schemes'. Advances in Cryptology: Crypto'84, 1985 (*LNCS*, **196**), pp. 47–53

[17] BONEH D., FRANKLIN M.: 'Identity-based encryption from the weil pairing'. Advances in Cryptology: Crypto'01, 2001 (*LNCS*, **2139**), pp. 213–229

[18] JOUX A.: 'The weil and tate pairings as building blocks for public key cryptosystems'. Proc. Fifth Algorithmic Number Theory Symp.'02, 2002 (*LNCS*, **2369**), pp. 20–32