Journal of Information Hiding and Multimedia Signal Processing ©2009 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **2**, March **2015**

An Improved Anonymous Authentication Scheme for Roaming Services

Zuowen Tan[1,2]

[1]High Level Engineering Research Center of Electronic-Commerce,
Jiangxi Provincial Colleges and Universities,School of Information Technology
Jiangxi University of Finance and Economics
Nanchang 330032,China
tanzyw@163.com
[2]Department of Information Technology,Uppsala University
SE-751 05, Uppsala, Sweden

Received July, 2013; revised December, 2014

Abstract. *In wireless network and mobile network, a two-factor authentication scheme for roaming services enables a mobile user to achieve mutual authentication and key agreement with the foreign agent. In this paper, we review Kim et al.'s anonymous authentication scheme in global mobility networks. Analysis shows that Kim et al.'s scheme fails to achieve anonymity and two-factor authentication. In addition, Kim et al.'s scheme is vulnerable to impersonation attacks. It is also inconvenient for a mobile user since the mobile user cannot update password freely. We then propose a secure anonymous authentication scheme. Our proposed scheme satisfies six properties of secure authentication schemes for roaming services.*
Keywords: Authentication, Roaming service, Anonymity, Smart card

1. **Introduction.** In global mobility network, mobile users access roaming services from the home agent and foreign agents. In general, there are three parties involved in a roaming service: a mobile user MU, a foreign agent FA and the home agent HA. In order to prevent unauthorized access to the network, it is necessary to achieve mutual authentication and session key establishment between MU and FA by assistance of the HA [1, 2]. Two-factor authentication is one of the most efficient methods which have been applied in global mobility network. In 2004, Zhu and Ma proposed the first anonymous smart card based authentication scheme for roaming services [3]. However, their scheme [3] was subsequently found that it cannot achieve perfect backward secrecy and mutual authentication [4]. Lee et al. proposed an improvement on it [4]. Later, Wu et al. [5], Chang et al. [6]and Xu et al. [7] independently found that neither Zhu et al.'s nor Lee et al.'s schemes can provide user anonymity. Wu et al.'s or Chang et al.'s improved schemes still cannot achieve anonymity [8, 9, 10, 11]. In 2012, Mun et al. [11] showed that Wu et al.'s scheme does not offer perfect forward secrecy. Xie et al. [12] also proposed an authentication scheme for roaming services. However, He et al. [13] demonstrated that Xie et al.'s scheme suffers from impersonation attacks and it does not achieve mutual authentication between MU and the FA.

Recently, Kim and Kawk [14] found that the schemes in [4, 5] are vulnerable to replay attack and disclosure of password. Those schemes cannot achieve anonymity and perfect forward secrecy [14]. In addition, Kim and Kawk [14] demonstrated that Mun et al.'s

enhanced scheme [11] is vulnerable to replay attacks and man-in-the-middle attacks. They proposed an improved anonymous authentication scheme to overcome these weaknesses.

Based on [12, 14], we highlight that an anonymous two-factor authentication scheme in global mobility networks should satisfy the following requirements: R1. Anonymity: Any adversary can neither obtain the identity of user nor link different accesses to a same mobile user; R2. User friendliness: A mobile user is allowed to select and change his password freely; R3. Security: The scheme can resist various attacks such as replay attacks, the password guessing attacks, the stolen-verifier attacks, impersonation attacks, etc. It also achieves two-factor authentication, i.e. even if the smart card or password (not both) is disclosed, the scheme still can prevent the adversary from guessing the password or masquerading as the user; R4. Mutual authentication: The scheme can provide mutual authentication between FA and MU, FA and HA, MU and HA; R5. Perfect forward secrecy: Even if long secret keys are compromised, the previous session keys should not be revealed; R6. Efficiency: The scheme, especially for mobile user, should avoid using the cryptographic operations of high cost, for example, asymmetric key encryption or signature. In this paper, we show that Kim-Kwak's scheme is vulnerable according to these requirements. The remainder of this paper is organized as follows. In Section 2, we review Kim-Kwak's protocol. In Section 3, we examine its vulnerabilities. We will propose an anonymous authentication scheme and give its analysis in Sections 4 and 5, respectively. Finally, Section 6 concludes.

2. **Review of Kim-Kwak's scheme.** In this section, we will briefly review Kim-Kwak's authentication scheme for roaming services [14]. Their scheme consists of three phases: registration phase, authentication and key establishment phase, and update session key phase. The notations used in the Kim-Kwak's scheme are listed in Table 1.

Table 1. Notations

Notations	*Descriptions*	*Notations*	*Descriptions*
MU	Mobile User	$h()$	A secure one-way hash function
FA	Foreign Agent	N_X	Random nonce chosen by an entity X
HA	Home Agent	y	Secret number of MU generated by HA
ID_X	Identity of entity X	E_K	Symmetric Encryption using key K
x	Master secret key of HA	D_K	Symmetric Decryption using key K
PW_{MU}	Password of MU	f_K	MAC generation function by using the key K
$\oplus$	Exclusive-or operation	K_{XY}	Session key between entity X and Y
$\|$	String concatenation	$A \rightarrow B : \{m\}$	m is transmitted from A to B

2.1. **Registration phase.** Assume that the channel between MU and HA is secure during the registration phase. When a user MU wants to register with a home agent HA, MU and HA perform the following steps.

Step 1. MU$\rightarrow$ HA: $\{ID_{MU}, N_{MU}\}$.

MU selects an identity ID_{MU} and a random nonce N_{MU}, then sends them to HA.

Step 2. HA→ MU: {Smart card [ID_{MU}, ID_{HA}, A, K, N_{MU}, $h()$]}.

After receiving registration request, HA selects a random nonce N_{HA} and computes

$$A = h(x\|y) \oplus h(x\|ID_{MU}), B = h(h(x\|ID_{MU})\|h(x\|y)), \tag{1}$$

$$PW_{MU} = h(B\|N_{HA}), K = h(x||ID_{MU}) \oplus h(PW_{MU}\|N_{MU}). \tag{2}$$

HA stores {ID_{MU}, ID_{HA}, A, K, N_{MU}, $h()$} on a smart card and delivers it to MU.

2.2. **Authentication and key establishment phase.** The MU, HA and FA cooperatively execute the following steps.

Step 1. MU→ FA: {ID_{HA}, A, c_1, c_2, aP, N_{MU}}.

MU generates a nonce N'_{MU}, a random number a and computes

$$c_1 = K \oplus h(PW_{MU}\|N'_{MU}), c_2 = h(aP||h(PW_{MU}\|N'_{MU})\|h(PW_{MU}\|N_{MU})). \tag{3}$$

Next, the user forwards ID_{HA}, A, c_1, c_2, aP and N_{MU} to FA.

Step 2. FA→ HA: {ID_{FA}, A, c_1, c_2, aP, bP, N_{MU}}.

FA stores the ID_{HA} and aP from MU. And FA selects a random number b and computes bP. Then FA sends ID_{FA}, A, c_1, c_2, aP, bP and N_{MU} to HA.

Step 3. HA→ FA: {ID_{HA}, ID_{FA}, c_3, aP, bP }.

After receiving the message from FA, HA computes

$$h(x\|ID_{MU}) = A \oplus h(x\|y), B' = h(h(x\|ID_{MU})\|h(x\|y)), \tag{4}$$

$$PW_{MU} = h(B'\|N_{HA}), K = h(x\|ID_{MU}) \oplus h(PW_{MU}\|N_{MU}), \tag{5}$$

$$h(PW_{MU}\|N'_{MU}) = K \oplus c_1, \bar{c}_2 = h(aP\|h(PW_{MU}\|N'_{MU})\|h(PW_{MU}\|N_{MU})). \tag{6}$$

HA authenticates MU by checking if $\bar{c}_2 = c_2$. If the equation holds, HA then computes $c_3 = h(ID_{FA}\|aP\|bP\|K\|h(PW_{MU}\|)\|h(PW_{MU}\|N_{MU}))$, and delivers ID_{HA}, ID_{FA}, c_3, aP, and bP to FA.

Step 4. FA→ MU : {ID_{HA}, ID_{FA}, c_3, aP, bP}.

FA checks ID_{HA}, ID_{FA} and aP. Then FA sends ID_{HA}, ID_{FA}, c_3, aP, and bP to MU.

Step 5. MU→ FA: {S_{MF}}.

MU checks ID_{HA} and aP. Next MU computes

$$\bar{c}_3 = h(ID_{FA}\|aP\|bP\|K\|h(PW_{MU}\|N'_{MU})\|h(PW_{MU}||N_{MU}))$$

and verifies if $\bar{c}_3 = c_3$. After MU authenticates FA and HA, MU calculates the key $K_{MF} = h(abP)$ and generates $S_{MF} = f_{K_{MF}}(ID_{FA}\|aP\|bP)$. MU issues S_{MF} to FA.

Step 6. FA computes $K_{MF} = h(abP)$ and $S'_{MF} = f_{K_{MF}}(ID_{FA}\|aP\|bP)$. FA then checks whether $S'_{MF} = S_{MF}$. If they are equal, FA authenticates MU. Otherwise, the procedure is terminated.

2.3. **Update session key phase.** The phase is divided into three steps.

Step 1. MU→ FA: {b_iP}.

MU selects a random $b_i(i = 1,2,\cdots,n)$, computes b_iP, and sends b_iP to FA.

Step 2. FA→ MU: {a_iP, S_{MF_i}}.

FA selects a random number $a_i(i = 1,2,\cdots,n)$ and computes $K_{MF_i} = h(a_ib_iP)$, $S_{MF_i} = f_{k_{MF_i}}(a_ib_iP||a_{i-1}b_{i-1}P)$.FA then sends a_iP and S_{MF_i} to MU.

Step 3. MU computes a session key $K_{MF_i} = h(a_ib_iP)$ and $S'_{MF_i} = f_{k_{MF_i}}(a_ib_iP\|a_{i-1}b_{i-1}P)$. MU then checks whether $S'_{MF_i} = S_{MF_i}$.

3. **Vulnerabilities of Kim-Kwak's scheme.** In the section, we demonstrate that Kim-Kwak's scheme suffers from a few vulnerabilities.

3.1. **It cannot preserve user anonymity.** To protect user privacy, the authentication scheme needs to preserve user anonymity. Suppose that a passive attacker has intercepted the communication channel between MUs and FAs. Each time a mobile user MU roams into foreign network and logins to a FA, MU will send a login message $\{ID_{HA}, A, c_1, c_2, aP, N_{MU}\}$ to FA. Of MU's login message, three components ID_{HA}, A, and N_{MU} are unchanged during any login to any foreign agent. ID_{HA} represents the home agent of the user, while the others are also contained in the smart card. The elements A and N_{MU} are exclusive for the user MU. Therefore, a passive attacker could easily trace the user by comparing $\{ID_{HA}, A, N_{MU}\}$ in one login with those ones in other logins. Although a user's identity is not revealed, user anonymity is not well protected.

3.2. **It cannot provide user friendliness.** In global mobility networks, MU uses a mobile device to obtain roaming services from different foreign agents or the home agent. The way of authentication by identity and password is one of the most commonly used methods of authentication. Password is often of low entropy and easy to remember such a password. However, in Kim-Kwak's scheme, the password is not chosen by the user. On the contrary, the home agent computes a user's password by (2). In essence, the password is a hash value. Generally speaking, it is difficult for a user to remember. On the other hand, if a user wants to update password, the user must register with the home agent by selecting a new identity or a random nonce. It is inconvenient since the user always wants to update password after a certain period in order to ensure the security.

3.3. **It suffers from security flaw.** Firstly, from (6), we can infer that y is the same for mobile users. In order to compute PW_{MU}, with $h(x\|ID_{MU})$ from (2) or (5), HA must know the corresponding N_{HA}. Therefore, HA needs to maintain a database which is used for storing the pairs $(h(x\|ID_{MU}), N_{HA})$. It will lead to the protocol susceptible to the stolen-verifier attacks. When a user changes password, HA must update the database. It is also very inconvenient for both the users and the HA.

Secondly, Kim-Kwak's scheme may not resist against offline dictionary attacks. Assume that an adversary has gained temporary access to the smart card of MU and then obtained the value K and N_{MU} stored in the card. By comparison with N_{MU}, the adversary can judge whether the message intercepted from the channel between a user and a foreign agent is involved with the user whose card contains K. Thus, (6) can be used to compute correctly $h(PW_{MU}\|N'_{MU})$. With knowledge of $\{N_{MU}, aP, c_2\}$, the adversary can mount an offline dictionary attack by guessing a password and then verifying whether (3) holds.

3.4. **It cannot provide mutual authentication between FA and HA..** Specifically, FA is not authenticated by HA during the authentication and key establishment phase. Therefore, after an attacker has intercepted the message $\{ID_{HA}, A, c_1, c_2, aP, N_{MU}\}$ transferred to FA, the attacker can impersonate FA as follows. The attacker first selects a random number b and computes bP. Then the attacker sends ID_{FA}, A, c_1, c_2, aP, bP and N_{MU} to HA. Clearly, the identity of MU will be validated by HA. HA will send $\{ID_{HA}, ID_{FA}, c_3, aP, bP\}$ to FA (here, the attacker) who transfers it to MU as in the real protocol. During the process, the only thing the attacker has done is to select b. The result is that the attacker will be authenticated as FA by MU. What is worse, one session key has been established between the attacker (regarded as FA by MU) and MU. Kim-Kwak's scheme suffers from impersonation attacks and man-in-middle attacks.

4. **The proposed scheme.** In the section, we propose a new anonymous authentication scheme in global mobility networks. The home agent HA generates the system parameters. Let P be a generator of an elliptic curve group G of prime order q. HA holds one

master key x and shares a key y with FA (different shared keys for different FAs). Let $H() : \{\}^* \to G$ and $h() : \{\}^* \to Z_q^*$ be two cryptographic hash functions. Other notations adopted in the proposed scheme are the same as those in Kim-Kwak's scheme. The proposed scheme is further subdivided into four phases: registration phase, authentication and key establishment phase, update session key phase and password change phase. The fourth phase is not necessarily required for each run of the protocol. Only when the mobile user MU wants to update password, the fourth phase is required.

4.1. **Registration phase.**

Step 1. MU→ HA: $\{ID_{MU}, d\}$.

The user MU selects an identity ID_{MU}, a password PW_{MU} and a random number N. Then MU computes $d = h(ID_{MU}\|PW_{MU}) \oplus N$ and sends ID_{MU} and d to HA.

Step 2. HA→ MU: smart card.

HA computes $c = h(ID_{HA}\|ID_{MU}||x) \oplus d$, $A = xH(ID_{MU}\|ID_{HA})$ and stores $\{c, A, P, q, h(),H()\}$ on a smart card. Then HA issues the card to MU through a secure channel.

Step 3. MU→ Smart card: $\{d_1, d_2\}$.

MU computes

$$D = A \oplus H(ID_{MU} \oplus PW_{MU}), d_1 = c \oplus N, d_2 = h(PW_{MU}\|ID_{MU}\|d_1\|D). \tag{7}$$

Then MU replaces $\{c, A\}$ with $\{d_1,d_2, D\}$ in the smart card.

4.2. **Authentication and key establishment phase.**

Step 1. MU→ Smart card: $\{ID_{MU}, PW_{MU}\}$.

MU inputs ID_{MU} and PW_{MU}. Then the smart card computes

$$d_2^{'} = h(PW_{MU}\|ID_{MU}\|d_1\|D)$$

and checks whether $d_2^{'} = d_2$.

Step 2. MU→ FA: $\{ID_{HA}, B, B_1, e\}$.

MU chooses a random $a \in Z_q^*$, a random nonce N_{MU} and computes

$$d^{'} = d_1 \oplus h(ID_{MU}\|PW_{MU}), B = aP, \tag{8}$$

$$B_1 = aH(ID_{MU}\|ID_{HA}), B_2 = a(D \oplus H(ID_{MU} \oplus PW_{MU})), \tag{9}$$

$$e = E_{B_2}(ID_{MU}\|ID_{FA}\|ID_{HA}\|N_{MU}\|h(d^{'}\|N_{MU}\|B\|B_1)). \tag{10}$$

Next, the user forwards ID_{HA}, B, B_1 and e to FA.

Step 3. FA→ HA: $\{ID_{FA}, B, B_1, C, e_1\}$.

FA stores ID_{HA} and B. And FA generates a random nonce N_{FA}, selects a random number b and computes

$$C = bP, e_1 = E_y(ID_{FA}\|ID_{HA}\|e||N_{FA}\|h(B\|B_1\|C\|(ID_{FA} \oplus N_{FA}))). \tag{11}$$

Then FA sends ID_{FA}, B, B_1, C and e_1 to to HA.

Step 4. HA→ FA: $\{ID_{HA}, z\}$.

HA uses ID_{FA} to search for the shared key. Then HA decrypts e_1 with the key y and parses the plain text into five parts ($ID^{'}$, $ID^{''}$, $e^{'}$,$N^{'}$,$h^{'}$). HA checks if

$$ID^{'} = ID_{FA}, ID^{''} = ID_{HA}, h^{'} = h(B\|B_1\|C\|(ID_{FA} \oplus N^{'})). \tag{12}$$

Next HA decrypts $e^{'}$ with xB_1, and parses the plain text into five parts (ID, *, *,$N^{''}$,$h^{''}$). HA further checks ID_{FA} and ID_{HA} and verifies if

$$h^{''} = h(h(ID_{HA}\|ID\|x)\|N^{''}\|B\|B_1). \tag{13}$$

After HA authenticates FA and MU, HA computes

$$z_1 = h(ID_{FA}\|ID_{HA}\|ID\|N^{''}\|B\|C), \tag{14}$$

$$z_2 = h(ID_{FA}\|ID_{HA}\|N^{'}\|z_1), \tag{15}$$

$$z = E_y(z_1||z_2\|B\|C\|N^{'}\|N^{''}). \tag{16}$$

and sends $\{ID_{HA}, z\}$ to FA.

Step 5. FA→ MU: $\{ID_{FA}, ID_{HA}, B, C, e_2, e_3\}$.

FA decrypts z and checks if $z_2 = h(ID_{FA}\|ID_{HA}\|N_{FA}\|z_1)$. FA computes $e_2 = E_{bB}(N_{FA})$, $e_3 = h(z_1||N^{''})$, and sends ID_{FA}, ID_{HA}, B, C, e_2 and e_3 to MU.

Step 6. MU→ FA: $\{S_{MF}\}$.

MU checks ID_{FA}, ID_{HA} and B. Next MU computes $N^{'} = D_{aC}(e_2)$ and verifies if

$$e_3 = h(h(ID_{FA}\|ID_{HA}\|ID_{MU}\|N^{'}\|B\|C)\|N_{MU}). \tag{17}$$

After MU authenticates FA and HA, MU calculates the key $K_{MF} = h(aC)$ and generates a MAC value $S_{MF} = f_{K_{MF}}(ID_{FA}\|B\|C\|N^{'}\|N_{MU})$. Next, MU issues S_{MF} to FA.

Step 7. FA computes $K_{MF} = h(bB)$ and $S^{'}_{MF} = f_{K_{MF}}(ID_{FA}\|B\|C\|N_{FA}\|N^{''})$. If $S^{'}_{MF} = S_{MF}$, FA authenticates the user.

4.3. **Update session key phase.** The phase is the same as in Kim-Kwak's scheme.

4.4. **Password change phase.**

Step 1. MU→ Smart card: $\{ID_{MU}, PW_{MU}\}$.

Before MU changes password, MU inputs ID_{MU} and the old password PW_{MU}. If they are valid, MU is allowed to submit a new password PW_{new}. The smart card computes

$$D_{new} = D \oplus H(ID_{MU} \oplus PW_{MU}) \oplus H(ID_{MU} \oplus PW_{new}),$$
$$d_{new1} = d_1 \oplus h(ID_{MU}\|PW_{MU}) \oplus h(ID_{MU}\|PW_{new}),$$
$$d_{new2} = h(PW_{new}\|ID_{MU}\|d_{new1}||D_{new}).$$

Step 2. The smart card replaces $\{d_1, d_2\ , D\}$ with $\{d_{new1}, d_{new2}, D_{new}\}$.

5. **Analysis.** The proposed scheme can provide fairness of key establishment since B and C, which determines the session key, are selected by MU and FA, respectively. Both MU and FA can compute aC or bB, and further share a session key. No one except them could work it out. In the following, we show that the proposed authentication scheme satisfies the requirements mentioned in Section 1. Correctness of the proposed scheme is obvious.

5.1. **Security requirement analysis.**

5.1.1. *Anonymity.* During the second phase, MU transmits $\{ID_{HA}, B, B_1, e, S_{MF}\}$ to FA. $B = aP$, $B_1 = aH(ID_{MU}\|ID_{HA})$, e is the cipher text of B, B_1 and ID_{MU}, while S_{MF} is MAC value about messages $\{ID_{FA}\|B\|C\|N^{'}\|N_{MU}\}$. For the user MU, these messages except ID_{HA} change with each run of the protocol. Therefore, any adversary cannot link different runs of the protocol to a same mobile user.

Next, the identity of the mobile user MU appears in the messages transmitted among MU, FA and HA in two forms. One is contained in the cipher text e as a part of plain text. Since the key $B_2 = xB_1$, without knowledge of x, any adversary cannot compute B_2 to recover the identity ID_{MU}. The other is in the hash value B_1, z_1 as part of preimage. From (13), z_1 is part of plain text of z. Because FA has the shared key y, FA can decrypt z. However, due to the one-wayness of hash function, any one including FA cannot obtain the identity ID_{MU} from B_1 or z_1. Therefore, the scheme can preserve the user anonymity.

5.1.2. *User friendliness.* The fourth phase of the proposed scheme ensures that a mobile user can change password freely without the participation of the HA.

5.1.3. *Security.* First, we show that the proposed scheme achieves two-factor authentication. Assume that an adversary obtains the smart card and extracts the information $\{d_1,d_2,D\}$ stored in the card. If the adversary has no password or identity, the adversary cannot still compute $d^{'}$ or B_2 since $d^{'} = d_1 \oplus h(ID_{MU}\|PW_{MU})$, $B_2 = a(D \oplus H(ID_{MU} \oplus PW_{MU}))$. Since $d^{'}$ is used to verify the identity, and B_2 is a Diffie-Hellman key shared with HA, the adversary cannot impersonate the use MU. In addition, HA authenticates FA and MU by checking (12). Becauseof in the equation (10), $h(d^{'}\|N_{MU}\|B\|B_1)$ only appears in form of cipher text and, and the equation does not contain the information of password, the proposed scheme can also resist against the undetectable on-line/off-line password guessing attack. On the other hand, assume that an adversary obtains the password. Since the identity is well protected (see anonymity analysis), any adversary could not compute the verification message $d^{'}$ or the key B_2. That is, the adversary cannot work out a correct e.

Secondly, we demonstrate that the proposed scheme can resist the password guessing attacks, the replay attacks, the stolen-verifier attacks, impersonation attacks, etc. As shown above, the proposed scheme can resist password guessing attacks. Next, in the proposed scheme, the freshness of the messages transmitted and the shared session key is provided by two random nonces N_{MU},N_{FA} and two elements B, C. So message replayed can easily be identified by FA, HA and MU. Moreover, the adversary could not compute session key from B and C. In addition, from Section 4, we know that the proposed scheme does not need to maintain a verification table or password table at the home agent. Therefore, nobody can obtain any verifiable information about the mobile user from HA. The proposed scheme can resist against the stolen verifier attacks. Finally, mutual authentication implies that the proposed scheme can also resist against the impersonation attacks and man-in-the-middle attacks (see the mutual authentication analysis below).

5.1.4. *Mutual authentication.*

Mutual authentication between MU and HA: MU authenticates HA by verifying whether (17) holds. There are two important messages N_{MU} and ID_{MU} in the equation. Before MU transmits them to FA who further transfers them to HA, N_{MU} and ID_{MU} have been encrypted with B_2. However, (B_1, $xH(ID_{MU}\|ID_{HA})$, B_2) is a Diffie-Hellman tuple. Therefore, after B_1 is generated by MU, only one with x can compute B_2. Thus MU can authenticate HA through Eq (17). Similarly, HA believes that the user must have an identity ID_{MU} and know $xH(ID_{MU}\|ID_{HA})$, and $h(ID_{HA}\|ID_{MU}\|x)$.

Mutual authentication between FA and HA: After HA received $\{ID_{FA},B,B_1,C,e_1\}$, HA searches for the key y on the basis of ID_{FA}. Then HA checks whether (11) holds. A random nonce N_{FA} besides $\{ID_{FA},B,B_1,C\}$ is involved with Eq (7). Since N_{FA} is encrypted using the key y, which is shared only by HA and FA, HA thinks that all the messages $\{ID_{FA},B,B_1,C\}$ are valid and they come from FA. In the other direction, FA authenticates HA by verifying $z_2 = h(ID_{FA}\|ID_{HA}\|N_{FA}\|z_1)$. The equation contains z_2, N_{FA} and z_1. Only their cipher text z but the plain text is transmitted over the channel. If (16) holds, FA believes that z is generated by the entity who has the key y. The nonce N_{FA} is only contained in the cipher text e_1. It indicates that z is generated by HA.

Mutual authentication between MU and FA: The way in which MU authenticates HA can also be used to authenticate FA by MU. Since (17) contains ID_{MU} and N_{MU}, if it holds, MU believes that the sender of $\{ID_{FA},ID_{HA}, B, C, e_2, e_3\}$ has been authenticated by HA. Moreover, the nonce N_{MU} is specially selected to establish a session key with FA. Conversely, FA confirms that the sender of $\{ID_{HA}, B, B_1, e\}$ is proved to be a registered

user of the HA. Later, FA checks whether $S'_{MF} = f_{K_{MF}}(ID_{FA}\|B\|C\|N_{FA}\|N'')$. If it holds, FA believes that the sender knows a. Thus, FA authenticates MU.

5.1.5. *Perfect forward secrecy.* Assume that the master secret keys x and the shared key y are disclosed and the adversary has intercepted all the messages transmitted among the user MU, the foreign agent FA, and the home agent HA. The adversary attempts to learn a used session key. With x, the adversary can know the identity of a mobile user who has access to FA. However, it is still infeasible to work out aC or bB from $\{B,C\}$ since the adversary will be confronted with an instance (B,C,aC) or (B,C,bB) of computational Diffie-Hellman problems. Therefore, the adversary cannot compute the session keys. The analysis also applies to the update session key phase. On the assumption of computational Diffie-Hellman, the proposed scheme can provide perfect forward secrecy. According the requirements mentioned in Section 1, we compare the proposed scheme with the previous anonymous authentication schemes for roaming services [3, 4, 5, 11, 14]. The comparison results are listed below in Table 2.

Table 2. Comparison in term of the requirements

	Proposed scheme	[3]	[4]	[5]	[11]	[14]
R1	Yes	No	No	No	Yes	No
R2	Yes	No	No	No	No	No
R3	Yes	Yes	No	No	No	No
R4	Yes	No	No	No	Yes	No
R5	Yes	No	No	No	Yes	Yes

Table 3. Comparison in term of computation cost

	Kim-Kwak's scheme			Li et al.'s Scheme			The proposed Scheme		
	MU	FA	HA	MU	FA	HA	MU	FA	HA
Random number generation	2	1	0	1	1	1	1	1	0
Module exponentiation	0	0	0	4	5	3	0	0	0
MAC generation (with key)	1	1	0	0	0	0	1	1	0
Point multiplication	2	2	0	0	0	0	4	2	1
Hash (mapping into a field)	8	1	7	3	2	5	6	4	5
Hash (mapping into an element)	0	0	0	0	0	0	2	0	0
Symmetric encryption/decryption	0	0	0	4	4	5	2	3	3
Signature generation/verification	0	0	0	0	2	2	0	0	0

5.2. **Performance analysis.** Of the related schemes [3, 4, 5, 11, 14, 15], Li et al.'s scheme [15] achieves all the security requirements R1-R5. Compared with them, the proposed scheme does not only obtain the same security level as Li et al.'s scheme (see Section 5.1), but it has as high efficiency as the schemes [3, 4, 5, 11, 14]. Since it uses symmetric crypto-system and Elliptic curve group instead of a public key crypto-system with certificate, the communication overhead and computation cost are reduced greatly. Especially, the mobile user does not need to do asymmetric key encryption or signature. Table 3 shows the comparison with Li et al.'s scheme [15] in term of computation cost during the authentication and key establishment phase. Here we neglect the XOR operation. We also list the comparison result with Kim-Kwak's scheme. As shown above in Table 3, the mobile user is not required to execute any module exponentiation in the proposed

scheme. The mapping-into-an element hash operation costs a little much. However, in the proposed scheme, the smart card can pre-compute them. Moreover, the proposed scheme overcomes the weaknesses of Kim-Kwak's scheme.

6. **Conclusion.** In this paper, we discussed Kim-Kwak's scheme and showed that there exist a few security flaws in the scheme. In order to remove these weaknesses, we proposed a new authentication scheme. We demonstrate that our scheme can provide anonymity, user friendliness, security, mutual authentication, and perfect forward secrecy. Compared with the previous anonymous authentication schemes for roaming services, the proposed scheme has more security properties and it also holds high performance.

Acknowledgment. This work is partially supported by the National Natural Science Foundation of China under Grant Nos.61163053,61462033, Natural Science Foundation of Jiangxi Province (20142BAB207015). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] C. Guo, C. C. Chang, and C. Y. Sun, Chaotic maps-based mutual authentication and key agreement using smart cards for wireless communications, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 2, pp. 99-109, 2013.

[2] H. F. Zhu, T. H. Liu, D. Zhu, and H. Y. Li, Robust and simple n-party entangled authentication cloud storage protocol based on secret sharing scheme, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 2, pp. 110-118, 2013.

[3] J. Zhu and J. Ma, A new authentication scheme with anonymity for wireless environments, *IEEE Trans. on Consumer Electronics*, vol. 51, no. 1, pp. 230-234, 2004.

[4] C. C. Lee, M. S. Hwang, and D. H. Liao, Security enhanced on a new authentication scheme with anonymity for wireless environments, *IEEE Trans. on Industrial Electronics*, vol. 53, no. 5, pp. 1683-1686, 2006.

[5] 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.

[6] C. C. Chang, C. Y. Lee, and Y. C. Chiu, Enhanced authentication scheme with anonymity for roaming service in global networks, *Computer Communications*, vol. 34, no. 4, pp. 611-618, 2009.

[7] 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.

[8] P. Zeng, Z. Cao, K. R. Choo, and S. Wang, On the anonymity of some authentication schemes for wireless communications, *IEEE Communications Letters*, vol. 13, no. 3, pp. 170-171, 2009.

[9] T. Y. Youn, Y. H. Park, and M. J. Li, Weaknesses in an anonymous authentication scheme for roaming service in global mobility networks, *IEEE Communication Letters*, vol. 13, no. 7, pp. 1118-1123, 2009.

[10] D. He, M. Ma, Y. Zhang, C. Chen, and J. J. Bu, A strong user authentication scheme with smart cards for wireless communications, *Computer Communications*, vol. 34, no. 3, pp. 367-374, 2011.

[11] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, Enhanced secure anonymous authentication scheme for roaming service in global mobility networks, *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp.214-222, 2012.

[12] Q. Xie, B. Hu, X. Tan, M. Bao, and X. Yu, Robust anonymous two-factor authentication scheme for roaming service in global mobility network, *Wireless Personal Communications*, vol. 74, no. 2, pp. 601-614, 2014.

[13] D. He, N. Kumar, M. K. Khan, and J. Lee, Anonymous two-factor authentication for consumer roaming service in global mobility networks, *IEEE Trans. on Consumer Electronics*, vol. 59, no. 4, pp. 811-817, 2013.

[14] J. S. Kim and J. Kwak, Secure and efficient anonymous authentication scheme in global mobility networks, *Journal of Applied Mathematics*, vol. 2013, Article ID 302582, 12 pages, http://dx.doi.org/10.1155/2013/302582.

[15] C. T. Li and C. C. Lee, A novel user authentication and privacy preserving scheme with smart card for wireless communications, *Mathematical and Computer Modelling*, vol. 55, no. 1-2, pp.35-44, 2012.