ISSN 1392 – 124X INFORMATION TECHNOLOGY AND CONTROL, 2012, Vol. 41, No. 1

A MORE SECURE AND EFFICIENT AUTHENTICATION SCHEME WITH ROAMING SERVICE AND USER ANONYMITY FOR MOBILE COMMUNICATIONS

Chun-Ta Li

Tainan University of Technology, Department of Information Management
529 Zhongzheng Road, Tainan City 71002, Taiwan, R.O.C.
e-mail: th0040@mail.tut.edu.tw

crossref http://dx.doi.org/10.5755/j01.itc.41.1.1024

Abstract. In terms of convenience requirements, mobile communications have become one of the most important roaming services for wireless environments. Especially, how to prevent unauthorized users from illegitimate accesses in mobile communication systems has become an important issue. Password authentication with smart card is one of the mechanisms that were widely used to authenticate the validity of participants between a roaming user, the foreign agent and the home agent of a roaming user. In 2011, Yoon et al. proposed a user friendly authentication scheme with user anonymity for wireless communications and claimed that their scheme is secure and efficient using for battery-powered mobile devices in mobile communication systems. However, we observe that Yoon et al.'s scheme is vulnerable to insider attack, unfairness in session key computation, unable to provide user anonymity and is not easily reparable. In this paper, we offer a more secure and efficient authentication scheme to remedy its security weaknesses and provide reliable roaming accesses in mobile communication environments.

Keywords: Mobile communication systems; Network security; Password user authentication; Roaming service; Smart card; User anonymity; Wireless communication.

1. Introduction

Nowadays, wireless communication systems and mobile computing environments have become more and more popular in multifarious aspects, from the personal to the home, offices, commerce, industry, military, community, public places and so on. Through seamless roaming technology, a roaming user can obtain desired services from the home agent by using his/her mobile devices within a range of wireless networks at anytime and anyplace. When a mobile user roams to a foreign network, it becomes necessary to provide secure communications and perform authentication with a foreign agent under the assistance of his/her home agent [1, 6–8, 10–14, 16–18].

In order to ensure communication security and user privacy, many authentication scheme with roaming service and user anonymity for mobile communication environments have been proposed [3, 5, 8, 9, 11, 16, 17]. In 2004, Zhu and Ma [19] proposed a smart card based password authentication scheme with anonymity for roaming services. However, in 2006, Lee et al. showed that Zhu and Ma's scheme cannot resist forge attack and achieve mutual authentication [7]. Lee et al. further proposed an improved scheme to overcome the weaknesses of [19]. Unfortunately, in 2008, Wu et al. [16] pointed out security vulnerabilities of [7] and proposed their enhanced version of Lee et al.'s scheme. Later, Lee et al. [8] and He et al. [5] showed that [16] also failed to achieve user anonymity.

Recently, Yoon et al. propose a user friendly and anonymity authentication scheme using passwords and smart cards for wireless communications [17]. As mentioned in [17], the following criteria are important for providing efficiency and security to suitable battery-powered mobile devices. Major design goals include:

(1) User friendly A mobile user can freely choose and change his/her passwords and does not need to maintain the password verification table.

(2) User anonymity: A mobile user's real identity and location cannot be traced by a foreign agent or any adversary.

(3) Mutual authentication A roaming user and the foreign agent can authenticate each other under the assistance of roaming user's home agent.

(4) Key agreement: A roaming user and the foreign agent can securely agree on a common session key to protect their future communications. Moreover, the knowledge of previous session keys does not help an adversary to derive a new session key.

(5) Secure roaming Roaming phase is more secure compared with the related schemes. Major security goals include: forgery attacks resistance, known-key attacks resistance, insider attacks resistance, guessing attacks resistance, replay attacks resistance and so on.

In this paper, we show that Yoon-Yoo-Ha's scheme has three disadvantages as follows.

(1) It cannot protect against an insider attack.

(2) Unfairness in session key computation.

(3) Attacks against the user anonymity.

We will point out these three disadvantages more clearly in Section 3. In order to overcome the above three disadvantages, we would like to propose a more secure scheme that also achieves user anonymity and resistance to security attacks. Furthermore, our scheme is more efficient regarding performance by using lightweight Elliptic Curve Diffie-Hellman (ECDH) computation compared with Yoon et al.'s scheme which uses heavyweight asymmetric cryptosystem with certificates.

The remainder of the paper is organized as follows. Section 2 reviews the scheme [17], whose weaknesses are shown in Section 3. We then propose a new authentication scheme with roaming service and user anonymity in Section 4, whose security and performance are analyzed in Section 5. Section 6 concludes the paper.

2. A Review of Yoon et al.'s authentication scheme

In this section, we review Yoon et al.'s ECC-based authentication scheme [17]. Their scheme consists of three phases, namely: registration, authentication and roaming phase. For convenience of description, we will list the common notations used throughout this paper in Table 1.

2.1. Registration Phase

In this phase, all the communications between the mobile user MU and the home agent HA are through a secure channel.

(1) $MU \longrightarrow HA$**:** $ID_{MU}, PW_{MU} \oplus rn$
When a new MU wants to register at HA, he/she chooses his/her identity ID_{MU}, password PW_{MU} and a random number rn and sends ID_{MU} and $PW_{MU} \oplus rn$ to HA.

(2) $HA \longrightarrow MU$**:** $SMART\ CARD$
On receiving the registration request from MU, HA computes an authentication key $z = H(ID_{HA}||N||e)$ and $r = z \oplus PW_{MU} \oplus rn$ and issues a smart card to MU, where the smart card contains ID_{HA}, e, r and a strong one-way hash function $H(\cdot)$. In addition, the random number e is different for every mobile user and it is not stored in HA.

(3) MU enters rn into his/her smart card and MU's smart card contains ID_{HA}, e, r, rn and $H(\cdot)$.

2.2. Authentication Phase

When a mobile user MU roams a new foreign network and accesses the foreign agent FA, MU and FA are able to authenticate each other through MU's home agent HA. Figure 1 shows the authentication phase of Yoon et al.'s scheme. The following steps are performed during the authentication phase.

(1) $MU \longrightarrow FA$**:** c_1, e, ID_{HA}, T_{MU}
MU enters ID_{MU} and PW_{MU} to the card reader, then the reader extracts the authentication key z by computing $r \oplus PW_{MU} \oplus rn$. MU computes a temporary key $L = H(z||T_{MU})$, a message authentication code $MAC = H(ID_{MU}||x_0||x||T_{MU}||L)$ and $c_1 = (ID_{MU}||x_0||x||MAC)_L$ and sends an authentication request message c_1, e, ID_{HA} and T_{MU} to FA, where two random numbers x_0 and x are generated by MU and T_{MU} is MU's current timestamp to prevent replay attack.

(2) $FA \longrightarrow HA$**:** $c_1, e, T_{MU}, Cert_{FA}, Sig_{FA}, T_{FA}$

On receiving the authentication request from MU, FA checks the validity of timestamp T_{MU}. If it is valid, FA computes its signature $Sig_{FA} = S_{S_{FA}}(H(c_1||e||T_{MU}||T_{FA}))$ and sends the message $c_1, e, T_{MU}, Cert_{FA}, Sig_{FA}$, T_{FA} to HA, where T_{FA} is FA's current timestamp, S_{FA} is FA's private key and $Cert_{FA}$ is FA's certificate defined in X.509.

(3) $HA \longrightarrow FA$**:** $c_2, Cert_{HA}, Sig_{HA}, T_{HA}$
On receiving the message from FA, HA checks the validity of certificate $Cert_{FA}$ and timestamp T_{FA}. If they are valid, HA computes the authentication key $z = H(ID_{HA}||N||e)$ by using its identity ID_{HA}, secret key N and the received random number e. Then, HA computes $L = H(z||T_{MU})$ and decrypts $c_1 = (ID_{MU}||x_0||x||MAC)_L$ by using L. HA checks if the computed $H(ID_{MU}||x_0||x||T_{MU}||L)$ is the same as the received MAC or not. If it holds, HA computes $c_2 = E_{P_{FA}}(H(L)||x_0||x)$ and its signature $Sig_{HA} = S_{S_{HA}}(H(c_2||T_{HA}))$ and sends $c_2, Cert_{HA}, Sig_{HA}, T_{HA}$ to FA, where

Table 1. Notations used throughout this paper

MU	The mobile user
HA	The home agent of MU
FA	The foreign agent of the network
ID_{MU}	The identity of MU
PW_{MU}	The password of MU
N	A strong secret key of HA
T_A	The current timestamp generated by an entity A
$Cert_A$	The certificate of an entity A
$(X)_K$	Encryption of a message X using a symmetric key K based on AES [2]
(P_A, S_A)	The asymmetric public key and private key pair of an entity A based on ECC [4]
$E_{P_A}(X)$	Encryption of a message X using a public key of an entity A
$S_{S_A}(X)$	Signature on a message X using a private key of an entity A
$\oplus$	The bitwise exclusive-or operation
$H(\cdot)$	A collision free one-way hash function such as SHA-256 [15]
$\|\|$	String concatenation

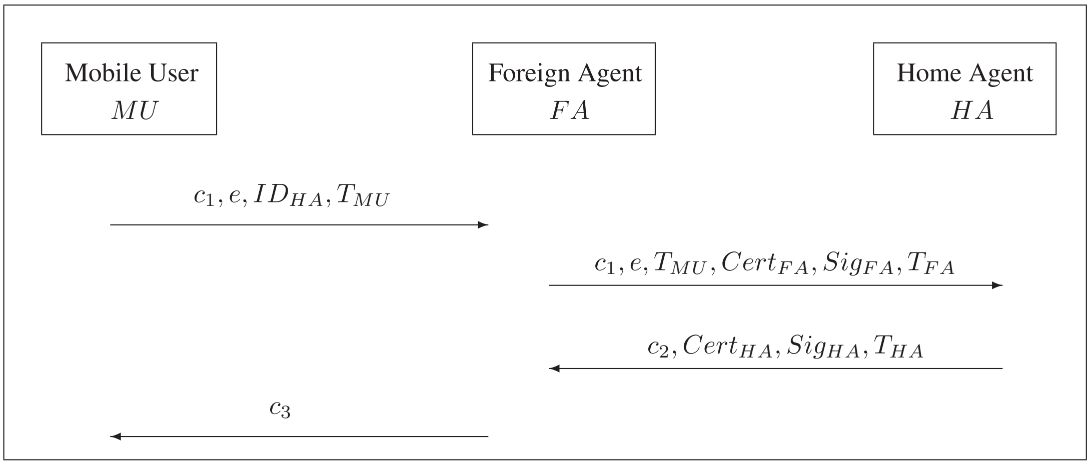

Figure 1. Authentication phase of Yoon et al.'s scheme

T_{HA} is HA's current timestamp, S_{HA} is HA's private key and $Cert_{HA}$ is HA's certificate defined in X.509.

(4) $FA \longrightarrow MU$**:** c_3
On receiving the message from HA, FA checks the validity of certificate $Cert_{HA}$ and timestamp T_{HA}. If they are valid, FA decrypts c_2 by using its private key and reveals $H(L)||x_0||x$. FA then computes a session key $sk = H(H(L)||x_0||x)$ and transmits $c_3 = (TCert_{MU}||H(x_0||x))_{sk}$ to MU, where $TCert_{MU}$ is a temporary certificate of MU.

(5) On receiving the message from FA, MU computes a session key $sk = H(H(L)||x_0||x)$ and decrypts c_3 by using sk to reveal $TCert_{MU}$ and $H(x_0||x)$. MU then checks if the computed $H(x_0||x)$ is the same as the revealed $H(x_0||x)$ or not. If it holds, MU authenticates FA and confirms that it is communicating with a legal FA.

2.3. Roaming Phase

When MU visits FA at the ith session, MU sends the following message to FA.

(1) $MU \longrightarrow FA$**:** c, mac
MU computes the ith session key $sk_i = H(H(L)||x||x_{i-1})$, a messages authentication value $mac = H(x_i||TCert_{MU}||Other\ Information||sk_i)$ and $c = (x_i||TCert_{MU}||Other\ Information)_{sk_i}$ and sends c and mac to FA for updating x_{i-1} with x_i in the next communication with FA, where x_i is a random number for next communication and $Other\ Information$ contains the

new call arrival rate, user mobility pattern, the cell/WLAN capacity and so on.

(2) On receiving the message from MU, FA decrypts c with its computed ith session key sk_i and checks the validity of $TCert_{MU}$ and mac. If they are valid, FA updates x_{i-1} with x_i for next communication with MU.

3. Weaknesses of Yoon et al.'s authentication scheme

In this section, we demonstrate that Yoon et al.'s authentication scheme exposes the mobile user and remote agent to the risk of insider attack and is failing to achieve user anonymity. We explain as follows:

3.1. Insider Attack

If the privileged insider of the home agent has the knowledge of mobile user MU's authentication key $z = H(ID_{HA}||N||e)$, he/she may try to damage the communication privacy between MU and FA. Assuming an attacker MA obtained MU's authentication key z, MA can eavesdrop MU's authentication request message c_1, e, ID_{HA}, T_{MU} and decrypt c_1 to reveal $ID_{MU}||x_0||x||MAC$ by computing $L' = H(z||T_{MU})$. Thus, MA can easily derive the common session key $sk' = H(H(L')||x||x_0)$ to damage the communication privacy between MU and FA. Finally, the attacker, the mobile user and the foreign agent compute the same session key $sk = sk'$ and the attacker can employ sk' to launch a malevolent communication later.

3.2. Unfairness in Session Key Computation

Given two entities MU and FA, the computed session key sk must contain some contribution from each involved entity and no-one can control the session key from the connection single-handed. Unfortunately, we observe that Yoon et al.'s scheme is unfair for computing a session key and it can unilaterally be determined by MU. In Step **(1)** of the authentication phase, MU can always choose x and x_0 and compute L, where L is computed by MU alone and x and x_0 are two random numbers generated by MU alone, such that in Step **(4)** of the authentication phase, the session key computed by FA according to $sk = H(H(L)||x||x_0)$ is always MU's pre-determined x, x_0 and L. Therefore, sk does not contain any contribution from FA and Yoon et al.'s scheme cannot achieve fairness of the session key computation.

3.3. Attacks Against User's Anonymity

Yoon et al. claimed that the user anonymity is guaranteed by encrypting MU's identity ID_MU into c_1 with key L and FA or any attacker cannot know the real identification ID_{MU} of MU without having the encryption key $L = H(z||T_{MU})$. However, we found that user anonymity of Yoon et al.'s scheme still cannot be protected from an eavesdropping attack in authentication phase. Consider that a mobile user MU roams into the foreign network and sends the login request c_1, e, ID_{HA}, T_{MU} to FA to access service, the contents of e and ID_{HA} are for the mobile user MU's exclusive use and these two values always unchanging in Step **(1)** of the authentication phase. As a result, even though MU's identity ID_{MU} is still protected by using symmetric encryption technique, an attacker can easily trace down the relation between MU and HA by comparing (e, ID_{HA}) with all of the eavesdropped messages in wireless networks. Let us consider the following scenario.

Suppose there is an authentication request message transmitted between some mobile user MU and foreign agent FA containing (e, ID_{HA}). This means that these two entities are involved in an authentication phase and the attacker can discover the relation of a connection between MU, FA and HA. In this way, the attacker can discover other complete connection information between involved entities from MU to FA.

4. The Proposed Scheme

To remedy the weaknesses mentioned in Section 3, we propose a more secure and efficient authentication scheme based on elliptic curve discrete logarithm problem. Our scheme consists of four phases, namely: initialization, registration, authentication and roaming phase. The detail phases of our proposed scheme are shown in the following.

4.1. Initialization Phase

Before the system begins, the home agent HA selects two large prime numbers p and n and an elliptic curve equation E_p over a finite field $p : y^2 = x^3 + ax + b \bmod p$, where $p > 2^{160}$, $n > 2^{160}$, a and b are two integer elements and $4a^3 + 27b^2 \bmod p \neq 0$. HA also chooses an elliptic curve equation E and a base point P with the order n over E. In addition, HA selects its secret key N and computes $P_{HA} = NP$. Finally, HA keeps N in private, publishes $(E_p, E, n, P, P_{HA}, H(\cdot))$ and agrees a pre-shared symmetric key SK_{HF} between HA and FA.

4.2. Registration Phase

(1) $MU \longrightarrow HA$**:** $ID_{MU}, H(PW_{MU} \oplus rn)$
When a new MU wants to register at HA, he/she chooses his/her identity ID_{MU}, password PW_{MU} and a random number rn and

sends ID_{MU} and $H(PW_{MU} \oplus rn)$ to HA for registration.

(2) $HA \longrightarrow MU$**:** $SMART\ CARD$
On receiving the registration request from MU, HA computes an authentication key $z = H(ID_{MU}||N) \oplus H(PW_{MU} \oplus rn)$ and issues a smart card to MU, where the smart card contains ID_{HA}, E_p, E, n, P, P_{HA}, z and a strong one-way hash function $H(\cdot)$.

(3) MU enters rn into his/her smart card and MU's smart card contains ID_{HA}, E_p, E, n, P, P_{HA}, z, rn and $H(\cdot)$.

4.3. Authentication Phase

Figure 2 shows the authentication phase of our proposed scheme. The detailed steps are described as follows.

(1) $MU \longrightarrow FA$**:** $X, IND, c_1, ID_{HA}, T_{MU}$
When MU visits a new foreign network, MU inserts smart card into card reader and enters ID_{MU} and PW_{MU}. Then smart card chooses a random number x and computes $X = xP$, $X_1 = xP_{HA}$, $Z = z \oplus H(PW_{MU} \oplus rn)$, $IND = ID_{MU} \oplus H(X_1||T_{MU})$ and $c_1 = H(X_1||Z)$, where T_{MU} is MU's current timestamp and both parameters X and X_1 can be precomputed off-line. MU sends an authentication request message $(X, IND, c_1, ID_{HA}, T_{MU})$ to FA.

(2) $FA \longrightarrow HA$**:** $X, IND, c_1, Y, T_{MU}, T_{FA}, MAC_{FA}$

On receiving the authentication request from MU, FA checks the validity of timestamp T_{MU}. If it is valid, FA chooses a random number y and computes $Y = yP$ and $MAC_{FA} = H(X||IND||c_1||Y||T_{MU}||T_{FA}||SK_{HF})$. FA then sends the message $(X, IND, c_1, Y, T_{MU}, T_{FA}, MAC_{FA})$ to HA, where T_{FA} is FA's current timestamp and the parameter Y can be precomputed off-line.

(3) $HA \longrightarrow FA$**:** MAC_{HA}, c_2', T_{HA}
On receiving the message from FA, HA checks the validity of timestamp T_{FA}. If it holds, HA checks if the computed value $H(X||IND||c_1||Y||T_{MU}||T_{FA}||SK_{HF})$ is the same as the received MAC_{FA} or not. If it holds, HA computes $X_1' = XN$, $ID_{MU}' = IND \oplus H(X_1'||T_{MU})$ and $c_1' = H(X_1'||H(ID_{MU}'||N))$ and checks if the computed identity ID_{MU}' is a legal user and whether the equation $c_1' = c_1$ holds. If they are valid, HA computes $MAC_{HA} = H(X||Y||ID_{FA}||ID_{HA}||T_{HA}||SK_{HF})$ and $c_2 = H(X_1'||H(ID_{MU}'||N)||X||Y||ID_{FA}||ID_{HA})$ and sends the response message $(MAC_{HA}, c_2' = c_2 \oplus H(T_{HA}||SK_{HF}), T_{HA})$ to FA, where T_{HA} is HA's current timestamp.

(4) $FA \longrightarrow MU$**:** Y, c_2, c_3
On receiving the message from HA, FA checks the validity of timestamp T_{HA} and whether the equation $H(X||Y||ID_{FA}||ID_{HA}||T_{HA}||SK_{HF}) = MAC_{HA}$ holds. If they are valid, FA believes that HA is a valid home agent and MU is an authenticated user. FA then computes $c_2 = c_2' \oplus H(T_{HA}||SK_{HF})$ and a session key $sk = yX = xyP$ and transmits $(Y, c_2, c_3 = (TCert_{MU})_{sk})$ to MU, where $TCert_{MU}$ is a temporary certificate of MU.

(5) On receiving the message from FA, MU checks whether the equation $H(X_1||Z||X||Y||ID_{FA}||ID_{HA}) = c_2$ holds. If it holds, MU believes that it is communicating with a legal FA. Finally, MU computes a session key $sk' = xY = xyP = sk$ and decrypts c_3 by using sk' to obtain $TCert_{MU}$.

4.4. Roaming Phase

When MU visits FA at the ith session, MU sends the following message to FA.

(1) $MU \longrightarrow FA$**:** m_i, mac
MU computes $m_i = (sk_{i+1}||TCert_{MU}||Other\ Information)_{sk_i}$ and a messages authentication value $mac = H(sk_{i+1}||TCert_{MU}||Other\ Information)$ and sends m_i and mac to FA for updating sk_i with sk_{i+1} in the next communication with FA, where sk_{i+1} is a session key for next communication and $Other\ Information$ contains the new call arrival rate, user mobility pattern, the cell/WLAN capacity and so on.

(2) On receiving the message from MU, FA decrypts m_i with its computed ith session key sk_i and checks the validity of $TCert_{MU}$ and mac. If they are valid, FA updates sk_i with sk_{i+1} for next communication with MU.

5. Security and Performance Analyses

This section shows the performance comparisons of our scheme and Yoon et al.'s scheme in case of the authentication phase and demonstrates that the propose scheme can prevent weaknesses in Yoon et al.'s scheme. To prove the security of our scheme, we present two important mathematical problems on elliptic curves.

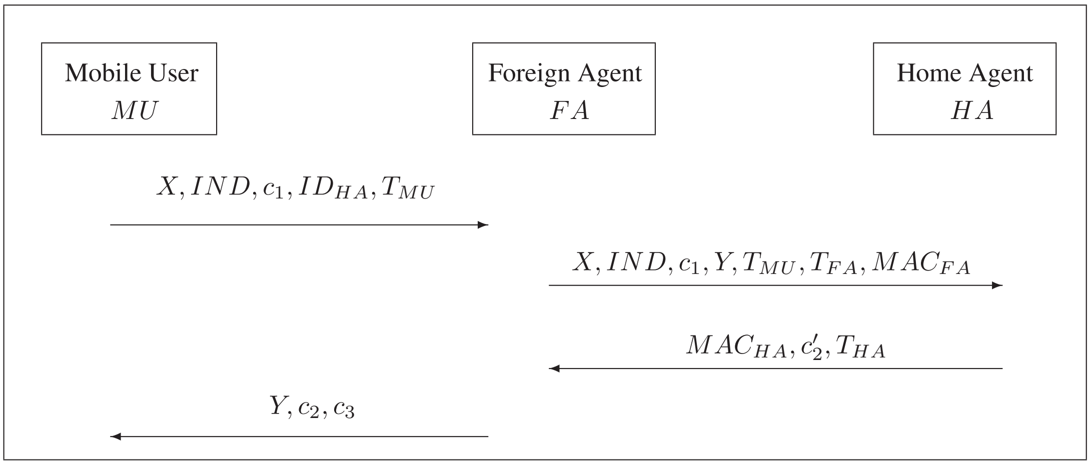

Figure 2. Authentication phase of our proposed scheme

Elliptic Curve Discrete Logarithm Problem:
Given $P, aP \in G$, it is hard to find a.

Elliptic Curve Computational Diffie-Hellman Problem:

Given $P, aP, bP \in G$, it is hard to compute $abP \in G$.

5.1. Insider Attack Resistance

Assume that a privileged insider MA has the knowledge of a legitimate user's (MU) authentication key $z = H(\ ID_{MU}||N) \oplus H(PW_{MU} \oplus rn)$ and tries to login for obtaining a roaming service. However, MA cannot pass the verification of $Z = z \oplus H(PW_{MU} \oplus rn)$ because MA does not know MU's password PW_{MU} and random number rn which MU stores in the smart card after MU has received and verified his/her smart card. Thus, our scheme prevents insider attack.

5.2. Fairness in Session Key Computation

As shown in the authentication phase, MU randomly selects his/her contribution $X = xP$ and sends a login request to FA. On receiving the login request message from MU, FA chooses its contribution $Y = yP$ and sends a message to HA. On receiving the message from FA, HA must make sure that MU is a legal user and FA is a legal foreign agent. If so, HA sends two confirm messages to FA and MU. FA and MU got message of MAC_{HA} and c_2, respectively. Finally, the session key $sk' = xY = xyP = sk$ contains equal contributions from MU and FA, and thus is a fair key agreement scheme.

5.3. Provision of User Anonymity

An anonymity feature of users is that foreign agents or any adversary cannot find out anything about a mobile user from a message which is transferred with or without the identity, except home agent can verify it. In the proposed scheme, the encrypted value $IND = ID_{MU} \oplus H(X_1||T_{MU})$ is used instead of ID_{MU} to guarantee the user anonymity. Since ID_{MU} is never transmitted as plaintext over wireless communications, so except the home agent of MU, foreign agents or anyone else cannot find the real identity ID_{MU} of MU without knowing the encrypted key $H(X_1||T_{MU})$.

Furthermore, because x was randomly chosen and integrated into login request message (X, IND, c_1), there is no relationship between the previous x and the current x of an MU. Therefore, FA or anyone else cannot trace an MU and the feature of user anonymity is fully protected in our proposed scheme.

5.4. Performance Analyses and Functionality Comparisons

For performance analysis, we compare the computational primitives involved in authentication phase of our scheme and Yoon et al.'s, and tabulate the results in Table 2. The heavyweight computations are executing asymmetric encryption/decryption, signature generation/verification, and multiplication operation of point. Our scheme needs only two more multiplication operations of point, two less hash operations and two less symmetric computations than Yoon et al.'s scheme. Moreover, the proposed scheme does not require any asymmetric computations to prevent insider attacks and provide user anonymity. Therefore,

Table 2. Performance comparisons in authentication phase

Primitives	Entities	Our scheme	Yoon et al.'s scheme [17]
Multiplication operation of point	MU	1 + 2 Pre	N/A
	FA	1 + 1 Pre	N/A
	HA	1	N/A
Hash operation $H(.)$	MU	4	5
	FA	3	4
	HA	6	6
Symmetric encryption	MU	N/A	1
	FA	1	1
	HA	N/A	N/A
Symmetric decryption	MU	1	1
	FA	N/A	N/A
	HA	N/A	1
Signature generation	MU	N/A	N/A
	FA	N/A	1
	HA	N/A	1
Signature verification	MU	N/A	N/A
	FA	N/A	1
	HA	N/A	1
Asymmetric encryption	MU	N/A	N/A
	FA	N/A	N/A
	HA	N/A	1
Asymmetric decryption	MU	N/A	N/A
	FA	N/A	1
	HA	N/A	N/A

Note: "Pre" denotes pre-computed operation; "N/A" denotes not used by the scheme.

Table 3. Functionality comparisons between Wu et al.'s scheme, Yoon et al.'s scheme and the proposed scheme

Properties	Wu et al.'s scheme [16]	Yoon et al.'s scheme [17]	Proposed scheme
User anonymity	No	No	Yes
No verification table	Yes	Yes	Yes
User friendly	No	Yes	Yes
Mutual authentication	Yes	Yes	Yes
Forgery attacks resistance	No	Yes	Yes
Insider attacks resistance	No	No	Yes
Fairness in session key computation	No	No	Yes

our scheme can be performed more efficiently than Yoon et al.'s scheme.

Table 3 shows the functionality comparison between the proposed scheme and others [16, 17]. Wu et al.'s and Yoon et al.'s schemes do not provide user anonymity, insecure to insider attacks and are unfairness in session key establishment. Moreover, Wu et al.'s scheme lacks forgery attacks resistance and user friendliness due to the fact that the password is not chosen by the user freely. However, as shown in Table 3, the proposed scheme not only provides user anonymity and some functionality requirements but also resists all security attacks. From the above descriptions, it demonstrates that our scheme has many excellent features and is more efficient than other related schemes.

6. Conclusions

In this paper, we have analyzed Yoon et al.'s ECC-based authentication scheme for mobile communication systems. We have shown that their scheme is vulnerable to insider attack, unfairness in session key computation and is unable to provide user anonymity. To provide secure roaming service in mobile communication environments, we propose an improved scheme with user anonymity and demonstrate that our scheme is more secure and efficient, as compared with Yoon et al.'s authentication scheme. Therefore, it is practicable to use our scheme for seamless roaming over wireless communication networks.

Acknowledgment

The authors would like to express their appreciation to the anonymous referees for their valuable suggestions and comments. This research was partially supported by the National Science Council, Taiwan, R.O.C., under contracts no: NSC 100-2221-E-165-002.

References

[1] **R. Abdellatif, H.K. Aslan, S.H. Elramly**. "New real time multicast authentication protocol." *International Journal of Network Security*, 12(1), 2011, 13-20.

[2] National Institute of Standards and Technology, "US department of commerce, advanced encryption standard." *US Federal Information Processing Standard Publication*, 2001, 197.

[3] **C.C. Chang, C.Y. Lee, Y.C. Chiu**. "Enhanced authentication scheme with anonymity for roaming service in global mobility networks." *Computer Communications*, 32(4), 2009, 611-618.

[4] **D. Hankerson, A. Menezes, S. Vanstone**. "Guide to elliptic curve cryptography." *LNCS*, 2004, New York: Springer.

[5] **D. He, M. Ma, Y. Zhang, C. Chen, J. Bu**. "A strong user authentication scheme with smart cards for wireless communications." *Computer Communications*, 34(3), 2011, 367-374.

[6] **D. He, J. Chen, J. Hu**. "Weaknesses of a remote user password authentication scheme using smart card." *International Journal of Network Security*, 13(1), 2011, 58-60.

[7] **C.C. Lee, M.S. Hwang, I.E. Liao**. "Security enhancement on a new authentication scheme with anonymity for wireless environments." *IEEE Transactions on Industrial Electronics*, 53(5), 2006, 1683-1686.

[8] **J.S. Lee, J.H. Chang, D.H. Lee**. "Security flaw of authentication scheme with anonymity for wireless communications." *IEEE Communications Letters*, 13(5), 2009, 292-293.

[9] **C.T. Li**. "Secure smart card based password authentication scheme with user anonymity." *Information Technology and Control*, 40(2), 2011, 157-162.

[10] **C.T. Li, C.C. Lee, L.J. Wang, C.J. Liu**. "A secure billing service with two-factor user authentication in wireless sensor networks." *International Journal of Innovative Computing, Information and Control*, 7(8), 2011, 4821-4831.

[11] **C.T. Li, C.C. Lee**. "A novel user authentication and privacy preserving scheme with smart cards for wireless communications." *Mathematical and Computer Modelling*, 55(1-2), 2012, 35-44.

[12] **C.T. Li, M.S. Hwang**. "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks." *Information Sciences*, 181(23), 2011, 5333-5347.

[13] **C.T. Li, C.C. Yang, M.S. Hwang**. "A secure routing protocol with node selfishness resistance in MANETs." *International Journal of Mobile Communications*, 10(1), 2012, 103-118.

[14] **C.T. Li, C.C. Lee**. "A robust remote user authentication scheme using smart card." *Information Technology and Control*, 40(3), 2011, 236-245.

[15] National Institute of Standards and Technology, "US department of commerce, secure hash standard." *US Federal Information Processing Standard Publication*, 2002, 180-182.

[16] **C.C. Wu, W.B. Lee, W.J. Tsaur**. "A secure authentication scheme with anonymity for wireless communications." *IEEE Communications Letters*, 12(10), 2008, 722-723.

[17] **E.J. Yoon, K.Y. Yoo, K.S. Ha**. "A user friendly authentication scheme with anonymity for wireless communications." *Computers & Electrical Engineering*, 37(3), 2011, 356-364.

[18] **E.J. Yoon**. "An efficient and secure identity-based strong designated verifier signature scheme." *Information Technology and Control*, 40(4), 2011, 323-329.

[19] **J. Zhu, J. Ma**. "A new authentication scheme with anonymity for wireless environments." *IEEE Transactions on Consumer Electronics*, 51(1), 2004, 230-234.

Received August 2011.