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

Chun-Ta Li
Taiwan 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 → HA: ID\(_{MU}\), PW\(_{MU}\) ⊕ 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\(_{MU}\) ⊕ rn to HA.

(2) HA → MU: SMART CARD

On receiving the registration request from MU, HA computes an authentication key z = H(ID\(_{HA}\)\(|N\)\(|e\)) and r = z ⊕ PW\(_{MU}\) ⊕ 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(·). 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(·).

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 → 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 ⊕ PW\(_{MU}\) ⊕ rn. MU computes a temporary key L = H(z\(|ID\(_{MU}\)|rn), 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 → 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\(_{FA}\)(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 → 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\(|ID\(_{MU}\)|rn) 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\(_{FA}\)(H(L)|x\(_0\)|x) and its signature Sig\(_{HA}\) = S\(_{HA}\)(H(c\(_2\)|T\(_{HA}\))) and sends c\(_2\), Cert\(_{HA}\), Sig\(_{HA}\), T\(_{HA}\) to FA, where
A More Secure and Efficient Authentication Scheme with Roaming Service and User Anonymity for Mobile Communications

Table 1. Notations used throughout this paper

<table>
<thead>
<tr>
<th>Notations</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MU</td>
<td>The mobile user</td>
</tr>
<tr>
<td>HA</td>
<td>The home agent of MU</td>
</tr>
<tr>
<td>FA</td>
<td>The foreign agent of the network</td>
</tr>
<tr>
<td>IDMU</td>
<td>The identity of MU</td>
</tr>
<tr>
<td>PW</td>
<td>The password of MU</td>
</tr>
<tr>
<td>N</td>
<td>A strong secret key of HA</td>
</tr>
<tr>
<td>TA</td>
<td>The current timestamp generated by an entity</td>
</tr>
<tr>
<td>CertA</td>
<td>The certificate of an entity</td>
</tr>
<tr>
<td>(X)K</td>
<td>Encryption of a message X using a symmetric key K based on AES [2]</td>
</tr>
<tr>
<td>(PA, SA)</td>
<td>The asymmetric public key and private key pair of an entity A based on ECC [4]</td>
</tr>
<tr>
<td>EP A(X)</td>
<td>Encryption of a message X using a public key of an entity A</td>
</tr>
<tr>
<td>SS A(X)</td>
<td>Signature on a message X using a private key of an entity A</td>
</tr>
<tr>
<td>⊕</td>
<td>The bitwise exclusive-or operation</td>
</tr>
<tr>
<td>H(·)</td>
<td>A collision free one-way hash function such as SHA-256 [15]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Mobile User

<table>
<thead>
<tr>
<th>MU</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDHA, T</td>
</tr>
<tr>
<td>c1, e</td>
</tr>
</tbody>
</table>

Foreign Agent

<table>
<thead>
<tr>
<th>FA</th>
</tr>
</thead>
<tbody>
<tr>
<td>CertFA, SigFA, TA</td>
</tr>
<tr>
<td>c2</td>
</tr>
<tr>
<td>c3</td>
</tr>
</tbody>
</table>

Home Agent

<table>
<thead>
<tr>
<th>HA</th>
</tr>
</thead>
<tbody>
<tr>
<td>CertHA, SigHA, T</td>
</tr>
</tbody>
</table>

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

THA is HA’s current timestamp, SHA is HA’s private key and CertHA is HA’s certificate defined in X.509.

(4) FA → MU; c3
On receiving the message from HA, FA checks the validity of certificate CertHA and timestamp THA. If they are valid, FA decrypts c2 by using its private key and reveals H(L||x0||x). FA then computes a session key sk = H(H(L)||x0||x) and transmits c3 = (TCPertMU||H(x0||x))sk to MU, where TCPertMU is a temporary certificate of MU.

(5) On receiving the message from FA, MU computes a session key sk = H(H(L)||x0||x) and decrypts c3 by using sk to reveal TCPertMU and H(x0||x). MU then checks if the computed H(x0||x) is the same as the revealed H(x0||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 → FA; c, mac
MU computes the ith session key ski = H(H(L)||x ||x−1||x−2||...||x0) as the messages authentication value mac = H(xi||TCPertMU||Other Information||ski) and c = (xi||TCPertMU||Other Information)ski, and sends c and mac to FA for updating x−1 with xi in the next communication with FA, where xi 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 $i$th 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 unchanged 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 and HA by comparing $(e, ID_{HA})$. 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 $p : y^2 = x^3 + ax + b \ (mod \ p)$, where $p > 2^{160}$, $n > 2^{160}$, $a$ and $b$ are two integer elements and $4a^3 + 27b^2 \ (mod \ p) \neq 0$. 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) $MU \rightarrow HA, ID_{MU}, H(PW_{MU} \oplus rn)$

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
A More Secure and Efficient Authentication Scheme with Roaming Service and User Anonymity for Mobile Communications

follows.

proposed scheme. The detailed steps are described as

4.3. Authentication Phase

Figure 2 shows the authentication phase of our

smart card contains

rent timestamp and the parameter

and whether the equation

c

HA

is a legal user

present two important mathematical problems on el-

of our scheme and Yoon et al.’s scheme in case of

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.
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 \( MU \)’s 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 multiplications 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

<table>
<thead>
<tr>
<th>Primitives</th>
<th>Entities</th>
<th>Our scheme</th>
<th>Yoon et al.’s scheme [17]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiplication operation of point</td>
<td>MU</td>
<td>1 + 2 Pre</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>FA</td>
<td>1 + 1 Pre</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>HA</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td>Hash operation ( H(.) )</td>
<td>MU</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>FA</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>HA</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Symmetric encryption</td>
<td>MU</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FA</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HA</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Symmetric decryption</td>
<td>MU</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>FA</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>HA</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td>Signature generation</td>
<td>MU</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>FA</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HA</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td>Signature verification</td>
<td>MU</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>FA</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HA</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td>Asymmetric encryption</td>
<td>MU</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>FA</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>HA</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td>Asymmetric decryption</td>
<td>MU</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>FA</td>
<td>N/A</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>HA</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User anonymity</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>No verification table</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User friendly</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mutual authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Forgergy attacks resistance</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Insider attacks resistance</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Fairness in session key computation</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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 computation. 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 mo-
bile 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


Received August 2011.