12-2013

A secure and effective anonymous user authentication scheme for roaming service in global mobility networks

Fengtong WEN

Willy SUSILO

Guomin YANG
Singapore Management University, gmyang@smu.edu.sg

Wireless Pers Commun (2013) 73:993–1004
DOI 10.1007/s11277-013-1243-4

A Secure and Effective Anonymous User Authentication Scheme for Roaming Service in Global Mobility Networks

Fengtong Wen · Willy Susilo · Guomin Yang

Published online: 7 June 2013

Abstract In global mobility networks, anonymous user authentication is an essential task for enabling roaming service. In a recent paper, Jiang et al. proposed a smart card based anonymous user authentication scheme for roaming service in global mobility networks. This scheme can protect user privacy and is believed to have many abilities to resist a range of network attacks, even if the secret information stored in the smart card is compromised. In this paper, we analyze the security of Jiang et al.'s scheme, and show that the scheme is in fact insecure against the stolen-verifier attack and replay attack. Then, we also propose a new smart card based anonymous user authentication scheme for roaming service. Compared with the existing schemes, our protocol uses a different user authentication mechanism, which does not require the home agent to share a static secret key with the foreign agent, and hence, it is more practical and realistic. We show that our proposed scheme can provide stronger security than previous protocols.

Keywords Roaming · Authentication · Cryptanalysis · Security · Smart card

1 Introduction

Nowadays, with the fast development of mobile technologies, Global Mobility Networks (GLOMONETs) have become widely available and interconnected. To provide global roaming service for a mobile user, remote authentication is an essential requirement. A typical remote authentication scenario involves three parties, namely a Mobile User (MU), a Foreign Agent FA) and a Home Agent HA). When a mobile user MU roams into a foreign network,

F. Wen (✉)
School of Mathematical Sciences, University of Jinan, Jinan 250022, China
e-mail: wftwq@163.com

F. Wen · W. Susilo · G. Yang
School of Computer Science and Software Engineering,
University of Wollongong, Wollongong, NSW 2522, Australia

the foreign agent FA authenticates the roaming user with the help of the user's home agent HA [1,11,12].

During the roaming process in GLOMONET, the mobile user MU is very much concerned about its privacy protection. The user's identity should be protected and his/her location and activities should be kept unlinkable. It is desirable to keep mobile users' identities anonymous in the remote user authentication process. In recent years, many anonymous authentication scheme (e.g. [2,6–8,13–15,19,21,24]) have been proposed for roaming services in GLOMONET. However, most of the existing protocols were broken shortly after they were proposed.

Mutual Authentication is a very important security feature. It requires that the client and server prove their respective identities to each other before performing any application functions. Recently, many research work (e.g. [4,8,20,24,22,23]) have been done in the design and analysis of mutual authentication protocols. However, some of them have been proved to be insecure against known attacks.

In 2012, Jiang et al. [10] pointed out the security flaws in some previous smart card based anonymous user authentication protocols. In order to remedy those weaknesses, Jiang et al. proposed an authentication scheme based on quadratic residue assumption, which is very efficient. Hence, Jiang et al.'s scheme seems to be a very good candidate authentication protocol for adoption in practice. Therefore, it is very interesting to analyze this scheme in detail to ensure that the security claims that are provided by the authors hold. It is unfortunate that we found some serious flaws in their scheme. In particular, the scheme is insecure due to two important issues namely the stolen-verifier attack and it cannot resist against replay attacks.

Our Contributions. The contributions of this paper are twofold. First, we show there exist several serious security flaws in Jiang et al.'s anonymous user authentication scheme, which are described as follows: 1) It is vulnerable to stolen-verifier attack. An attacker who has stolen the verifier table can obtain the session key SK and can impersonate the FA to fool the MU. 2) It also cannot resist replay attacks. Although the attacker cannot get the MU's session key shared with the FA, he/she can impersonate the MU to login the FA. 3) It is vulnerable to denial of service attack.

Second, we propose a new smart card based anonymous user authentication protocol for roaming service in global mobility networks. Our protocol makes use of a user authentication mechanism which is different from the previous approaches and can successfully prevent different kinds of network attacks.

Organization of the Paper. The rest of this paper is organized as follows. In the next section, we provide some mathematical preliminaries, which will be used throughout the paper. In Sect. 3, we briefly review Jiang et al.'s scheme. Subsequently, we show its weaknesses in Sect. 4. Then, we proceed with proposing our scheme in Sect. 5, together with analyzing its security in Sect. 6. In Sect. 7, we compare the performance of our new protocol with the previous schemes. Section 8 concludes the paper.

2 Mathematical Preliminaries

In this section, we discuss three computational problem: Quadratic residue problem, discrete logarithm problem and computational Diffie-Hellman problem, which will be used throughout the paper.

Table 1 Notations

MU	The mobile user
ID_{MU}	Identity of MU
PW_{MU}	Password of MU
HA	Home agent of MU
ID_{HA}	Identity of HA
FA	Foreign agent of MU roamed
ID_{FA}	Identity of FA
x	Master secret key stored in HA
ctr_{MU}	A counter of MU
SK	Session key shared between A and B
$H(\cdot)$	A secure collision-free one-way hash function
$A \oplus B$	XOR operation of A and B
$A \| B$	Data A concatenates with data B

2.1 Quadratic Residue Problem

Assume that $n = pq$, where p and q are two large primes. If $y = x^2 \ mod\ n$ has a solution, i.e., there exists a square root for y, then y is called a quadratic residue $mod\ n$. The set of all quadratic residue numbers in $[1, n-1]$ is denoted by QR_n. Then the quadratic residue problem states that, for $y \in QR_n$, it is hard to find x without the knowledge of p and q due to the difficulty of factoring n [17].

2.2 Discrete Logarithm Problem

Let G be a finite group, $g \in G$ with order n, $y \in G_g$. The problem is to find the smallest integer $x \in \{1, \ldots, n-1\}$ such that $g^x = y\,(mod\, n)$. It is easy to compute the discrete exponentiation $y = g^x\ (mod\, n)$ given g, x, n, but it is computationally infeasible to determine x given y, g, n, when n is large.

2.3 Computational Diffie-Hellman Problem

Consider a cyclic group G with order q. The CDH problem states that, given g, g^x, g^y for a generator g and random number $x, y \in \{1, 2, \ldots, q-1\}$, it is computationally intractable to compute the value g^{xy}.

The notations that will be used throughout this paper are listed in Table 1.

3 Review of Jiang et al.'s Scheme

Jiang et al.'s smart card based anonymous authentication scheme comprises three phases, namely the registration phase, the login and authentication phase and the password update phase. Each foreign agent shares a unique long-term K_{FH} with HA.

3.1 Registration Phase

Step 1. The MU sends his/her ID_{MU} to HA via a secure communication channel. HA computes $K_{MU} = h(ID_{MU} \| x)$ using the secret random number x.

Step 2. HA personalizes the smart card with $H(\cdot)$, K_{MU}, n and issues it to MU.
Step 3. After receiving the smart card, the MU computes $K^*_{MU} = K_{MU} \oplus h(ID_{MU} \| PW_{MU})$ and replaces K_{MU} with K^*_{MU}. Finally, the smart card contains $H(\cdot)$, K^*_{MU}, n

3.2 Login and Authentication Phase

Step 1. MU inserts his/her smart card into the device and enters his/her identity ID_{MU} and password PW_{MU}. The smart card computes $K_{MU} = K^*_{MU} \oplus h(ID_{MU} \| PW_{MU})$. Then the smart card generates a random number n_{MU} and computes $V_1 = (ID_{MU} \| K_{MU} \| n_{MU} \| ID_{FA})^2 \ mod \ n$. Finally, MU sends a login message $M_1 = (V_1, ID_{HA})$ to FA.
Step 2. Upon receiving M_1, FA generates a random number n_{FA} and computes $V_2 = h(M_1 \| n_{FA} \| K_{FH})$. Subsequently, FA sends the message $M_2 = (M_1, ID_{FA}, n_{FA}, V_2)$ to HA.
Step 3. After receiving M_2, HA checks whether ID_{FA} is the identity of an ally. If it is true, HA compares V_2 with $V_2^* = h(M_1 \| n_{FA} \| K_{FH})$. If $V_2 \neq V_2^*$, HA terminates the protocol. Otherwise, HA solves V_1 by using the Chinese Remainder Theorem with p and q to get $ID_{MU}, K_{MU}, n_{MU}, ID_{FA}$. Then, HA computes $h(ID_{MU} \| x)$ and compares it with the received K_{MU}. If they are equal, the authenticity of MU is ensured. Also, HA believes FA is the target foreign agent of MU. After that, HA computes $SK = h(h(ID_{MU} \| x) \| ID_{FA} \| n_{MU} \| n_{FA})$, $V_3 = SK \oplus h(K_{FH} \| n_{FA})$ and $V_4 = h(V_3 \| K_{FH})$, where SK is the session key between FA and MU. Finally, HA sends $M_3 = (V_3, V_4)$ to FA.
Step 4. After receiving the message M_3, FA computes $V_4^* = h(V_3 \| K_{FH})$ and checks whether $V_4^* = V_4$. If it is valid, FA computes $SK = V_3 \oplus h(K_{FH} \| n_{FA})$ and $V_5 = h(SK \| n_{FA})$, and sends $M_4 = (n_{FA}, V_5)$ to MU.
Step 5. Upon receiving M_4, MU computes $SK^* = h(h(ID_{MU} \| x) \| ID_{FA} \| n_{MU} \| n_{FA})$. Then MU computes $V_5^* = h(SK^* \| n_{FA})$ and checks whether it is equal to V_5. If it is true, then MU establishes trust with FA; otherwise, the authentication fails.

3.3 Password Change Phase

When MU wants to renew a password, MU inserts his/her smart card into the terminal and enters his/her identity ID^*_{MU}, the old password PW_{MU}, and the new password PW^{**}_{MU}. Then the smart card retrieves $K_{MU} = K^*_{MU} \oplus h(ID_{MU} \| PW_{MU})$ and computes $K^{**}_{MU} = K_{MU} \oplus h(ID^*_{MU} \| PW^{**}_{MU})$. Finally, the smart card stores K^{**}_{MU} in place of K^*_{MU}

4 Security Analysis of Jiang et al.'s Scheme

4.1 Security Against Stolen-Verifier Attacks

In Jiang et al.'s scheme, it is assumed that each foreign agent shares a unique long-term key K_{FH} with HA which should be stored in the verifier table of HA's database. In case the verifier table in the HA's database is leaked out or stolen by an attacker, the attacker can compute SK corresponding to any user MU and can also proceed spoofing attack. This is illustrated as follows.

4.1.1 Computing SK

Step 1. Eavesdrops a login request message $M_2 = (M_1, ID_{FA}, n_{FA}, V_2)$ and the corresponding message $M_3 = (V_3, V_4)$.
Step 2. Computes $h(K_{FH} \| n_{FA})$ using the stolen long-term key K_{FH} and n_{FA}.
Step 3. Computes $SK = V_3 \oplus h(K_{FH} \| n_{FA})$.

It can be seen that Jiang et al.'s protocol does not achieve perfect forward secrecy if the attacker obtains the FA's long-term key K_{FH} shared with HA.

4.1.2 Spoofing Attack

Step 1. Intercepts a login request message $M_2 = (M_1, ID_{FA}, n_{FA}, V_2)$ and chooses a random number n'_{FA}, and then computes $V'_2 = h(M_1 \| n'_{FA} \| K_{FH})$ using the stolen long-term key K_{FH} and n'_{FA}. Sends $M'_2 = (M_1, ID_{FA}, n'_{FA}, V'_2)$ to the HA.
Step 2. The HA authenticates the MU and FA following the step 3 of Jiang et al.'s scheme and sends message $M'_3 = (V'_3, V'_4)$ to the attacker, where $V'_3 = SK' \oplus h(K_{FH} \| n'_{FA})$, $V'_4 = h(V'_3 \| K_{FH})$, $SK' = h(h(ID_{MU} \| x) \| ID_{FA} \| n_{MU} \| n'_{FA})$.
Step 3. After receiving the message $M'_3 = (V'_3, V'_4)$, the attacker computes $SK' = V'_3 \oplus h(K_{FH} \| n'_{FA})$, $V'_5 = h(SK' \| n'_{FA})$ and sends $M'_4 = (n'_{FA}, V'_5)$ to the MU.
Step 4. The MU computes $SK^* = h(h(ID_{MU} \| x) \| ID_{FA} \| n_{MU} \| n'_{FA})$, $V^*_5 = h(SK^* \| n'_{FA})$ and conforms $V^*_5 = V'_5$. The MU believes that the attacker is the FA.

Hence, it is clear that the attacker can impersonate the FA whenver he/she likes.

4.2 Security Against Replay Attacks

In Jiang et al.'s scheme, during the login and authentication phase, the MU sends the login message $M_1 = (V_1, ID_{HA})$ to FA via a public channel, where $V_1 = (ID_{MU} \| K_{MU} \| n_{MU} \| ID_{FA})^2 \bmod n$. Suppose an attacker intercepts this message and sends another message $M'_1 = M_1$ in the next time to FA. Then after receiving this message during Login and authentication phase, the FA generates a random number n'_{FA} and computes $V'_2 = h(M'_1 \| n'_{FA} \| K_{FH})$. Subsequently, FA sends the message $M'_2 = (M'_1, ID_{FA}, n'_{FA}, V'_2)$ to HA. After receiving M'_2, then HA also processes this message and ensures that the attacker is a legal user. Although the attacker can not obtain the session key SK, he/she can impersonate the MU to login to the FA. As a result, Jiang et al.'s scheme fails to protect a strong replay attack using the random number.

4.3 Security Against Denial of Service Attack

In their scheme, there is no verification of old password before the new password update. If an attacker manages to gain temporary access to MU's smart card, he/she can launch a kind of denial of service attack as follows:

(1) Inserts MU's smart card into a card reader and initiates a password change request.
(2) Submits two random strings R_1, R_2 as MU's old password and new password.
(3) The smart card computes $K^{**}_{MU} = h(ID_{MU} \| x) \oplus h(ID_{MU} \| PW_{MU}) \oplus h(ID_{MU} \| R_1) \oplus h(ID_{MU} \| R_2)$ and update the K^*_{MU} with K^{**}_{MU}.

Once the value of K^*_{MU} is updated, the MU cannot login successfully even if he/she gets his/her smart card back because $K^{**}_{MU} \oplus h(ID_{MU} \| PW_{MU}) \neq h(ID_{MU} \| x)$, and since then MU's login request will be denied by HA during the login and authentication phase.

5 The Proposed Scheme

In this section, we propose a new authentication scheme with privacy preservation in Global mobility networks. Notably, the new scheme makes use of a counter-based authentication mechanism to resist against replay attack. In order to resist against stolen-verifier attacks, we replace the static long-term key K_{FH} with a dynamic Diffie-Hellman key. The new scheme can also resist against a range of attacks such as offline password guessing attacks and denial of service attack, even if the smart card is stolen.

Before the system begins, HA generates two secret large primes p, q and computes the number $n = pq$. The home agent HA chooses a multiplication group G and an element $g \in G$ with order q', where p' and q' are public large primes and $p' = 2q' + 1$ is the modulus for the group G (p', q' is different from p, q). The HA selects a private key $S_{HA} = a\ (< q')$ and computes the public key $P_{HA} = g^a\ mod\ p'$. Similarly, the foreign agent FA selects a private key $S_{FA} = b\ (< q')$ and computes the public key $P_{FA} = g^b\ mod\ p'$. The new protocol has three phases: registration, login and authentication, and password change.

5.1 Registration Phase

Step 1. The MU chooses his/her own identity ID_{MU} and password PW_{MU}, and generates a large random number d. He/she then computes the hash value $f = H(ID_{MU} \| PW_{MU} \| d)$, and sends the registration message ID_{MU}, f to the HA via a secure channel.
Step 2. HA computes $K^*_{MU} = h(ID_{MU} \| x) \oplus f$ using the secret random number x. HA then initiates a counter $ctr_{MU} = 0$ for MU and creates a record (ID_{MU}, ctr_{MU}) in its database. HA then personalizes the smart card with $h(\cdot)$, K^*_{MU}, ctr_{MU}, n and issues it to MU.
Step 3. After receiving the smart card, the MU computes $f^* = h(ID_{MU} \oplus PW_{MU} \oplus d)$ and stores f^* in the smart card. Finally, the smart card contains $h(\cdot)$, K^*_{MU}, f^*, n, d, ctr_{MU}.

5.2 Login and Authentication Phase

Step 1. $MU \rightarrow FA : M_1$. MU inserts his/her smart card into the device and enters his/her identity ID_{MU} and password PW'_{MU}. The smart card computes $f' = h(ID_{MU} \oplus PW'_{MU} \oplus d)$ and verifies whether $f^* = f'$ or not. If $f^* \neq f'$, the login phase terminates immediately. Otherwise, the smart card computes $K_{MU} = K^*_{MU} \oplus h(ID_{MU} \| PW_{MU} \| d)$. Then MU generates a random number n_{MU} and computes $ctr_{MU} = ctr_{MU} + 1$, $V_1 = (ID_{MU} \| K_{MU} \| n_{MU} \| ctr_{MU} \| ID_{FA})^2\ mod\ n$. Finally, MU sends a login message $M_1 = (V_1, ctr_{MU}, ID_{HA})$ to FA.
Step 2. $FA \rightarrow HA : M_2$. FA computes $K = P^b_{HA}\ mod\ p' = g^{ab}\ mod\ p'$, $V_2 = h(V_1 \| ctr_{MU} \| K)$. Subsequently, FA sends the message $M_2 = (M_1, ID_{FA}, V_2)$ to HA.
Step 3. $HA \rightarrow FA : M_3$. HA checks whether ID_{FA} is the identity of an ally. If it is true, HA compares $K = P^a_{FA}\ mod\ p' = g^{ab}\ mod\ p'$ and $V^*_2 = h(V_1 \| ctr_{MU} \| K)$. If $V_2 \neq V^*_2$, HA terminates the protocol. Otherwise, HA solves V_1 by using the Chinese Remainder Theorem with p and q to get $ID_{MU}, K_{MU}, n_{MU}, ctr_{MU}, ID_{FA}$. Then, the HA verifies the retrieved ctr_{MU} with the stored ctr'_{MU} corresponding to ID_{MU}. If $ctr_{MU} > ctr'_{MU}$, then the HA replaces ctr'_{MU} with new counter ctr_{MU} in its database and proceeds the next step. Otherwise, the HA rejects this message and considers it as a replay message. After that, HA computes $h(ID_{MU} \| x)$ and compares it with the received K_{MU}. If they are

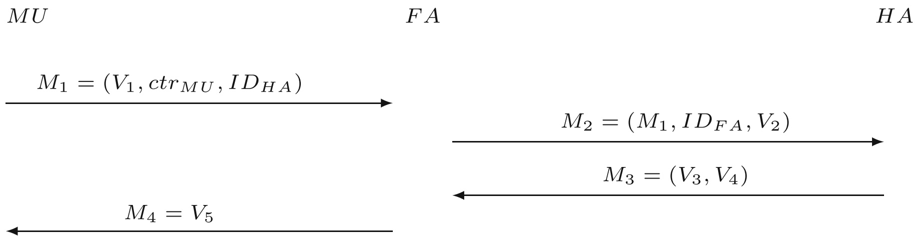


Fig. 1 Message flows in login and authentication phase

equal, the authenticity of MU is ensured. Also, HA believes FA is the target foreign agent of MU. HA computes $SK = h(h(ID_{MU}\|x)\|ID_{FA}\|n_{MU}\|ctr_{MU})$, $V_3 = SK \oplus h(K)$ and $V_4 = h(V_3\|K)$, where SK is the session key between FA and MU. Finally, HA sends $M_3 = (V_3, V_4)$ to FA.

Step 4. $FA \rightarrow MU : M_4$. FA computes $V_4^* = h(V_3\|K)$ and checks whether $V_4^* = V_4$. If it is valid, FA computes $SK = V_3 \oplus h(K)$ and $V_5 = h(SK\|P_{FA})$, and sends $M_4 = V_5$ to MU.

Step 5. Upon receiving M_4, MU computes $SK^* = h(h(ID_{MU}\|x)\|ID_{FA}\|n_{MU}\|ctr_{MU})$. Then MU computes $V_5^* = h(SK^*\|P_{FA})$ and checks $V_5^*? = V_5$. If it equals, then MU establishes trust with FA; otherwise, the authentication fails.

5.3 Password Change Phase

When MU wants to renew a password, MU inserts his/her smart card into the terminal and enters his/her identity ID_{MU}, the old password PW_{MU}^{old} and computes $f' = h(ID_{MU} \oplus PW_{MU}^{old} \oplus d)$, and then verifies whether $f^* = f'$ or not. If $f^* \neq f'$, the login phase terminates immediately. Otherwise, MU enters the new password PW_{MU}^{new}. Then, the smart card retrieves $K_{MU} = K_{MU}^* \oplus h(ID_{MU}\|PW_{MU}^{old}\|d)$ and computes $K_{MU}^{**} = K_{MU} \oplus h(ID_{MU}\| PW_{MU}^{new}\|d)$. Finally, the smart card stores K_{MU}^{**} in place of K_{MU}^*.

6 Security Analysis of the Proposed Scheme

In this section, we analyze the security of the proposed scheme and show that it can resist against different types of attacks and also it provides user anonymity.

6.1 User Anonymity

It is very important and necessary for a secure authentication protocol to provide user anonymity [3,5]. From Fig. 1, we can see that the communication transcript reveals no information about the identity ID_{MU} of the user. In fact, ID_{MU} is concealed in V_1, only the person who knows the value of p, q can solve the quadratic residue problem to obtain ID_{MU}. In our scheme, the secret value p, q is stored by HA. Therefore, the attacker including the FA cannot identify the MU from the login message.

6.2 Security Against Replay Attacks [18]

In our scheme, we used the counter based authentication mechanism to prevent replay attacks. If the adversary replays the previous login message, then HA will detect the attack when examining the counter ctr_{MU} of the user MU. The concrete step is as follows: During the login and authentication phase, when the HA receives a message $M_2' = (M_1', ID_{FA}, V_2')$, it verifies the retrieved the counter ctr_{MU}' with the stored counter ctr_{MU} according to the ID_{MU}. If the message $M_2' = (M_1', ID_{FA}, V_2')$ is a replay message, then the HA will find that $ctr_{MU}' \geq ctr_{MU}$. The HA simply rejects this message. Hence, our scheme prevents the replay attacks through the use of counter.

6.3 Security Against Impersonation Attacks [16]

We consider three types of impersonation attacks, namely MU impersonation attack, FA impersonation attack, and HA impersonation attack.

$MU Impersonation$. In order to impersonate the MU, the adversary must obtain the value of ID_{MU}, K_{MU}. We then consider two situations: (1) the adversary compromises the user identity and password but the smart card is secure; and (2) the adversary compromises the smart card but the user identity and password are secure.

In the first case, it is obvious that adversary is unable to obtain the value of K_{MU} since the smart card is secure. Notice that K_{MU} is concealed in $K_{MU}^* = K_{MU} \oplus H(ID_{MU} \| PW_{MU} \| d)$ in the smart card. Since the smart card is secure, the adversary is unable to obtain (K_{MU}^*, d) or K_{MU}.

In the second case, when the smart card is stolen and compromised, the adversary can learn the values of $(h(\cdot), K_{MU}^*, f^*, n, d, ctr_{MU})$ in the smart card. However, this time the adversary knows neither ID_{MU} nor PW_{MU}, and again he/she cannot computes the value of K_{MU}. We must also consider offline password guessing attacks in this case, that is the adversary uses a brute force search to find out the correct password. Let the adversary select randomly an identity candidate ID_{MU}' and a password candidate PW_{MU}'. Then the adversary can compute $f' = H(ID_{MU}' \oplus PW_{MU}' \oplus d)$ and then compare f' with f^*. If they are equal, the adversary may think that PW_{MU}' and ID_{MU}' as the correct password and real identity of the MU. In fact, the message pair (ID_{MU}', PW_{MU}') which satisfy the above equality is not unique. Even if this attack can be carried out in the offline manner by repeatedly trying the next identity candidate and password candidate, it is still a difficult problem for the adversary to obtain the real ID_{MU}, PW_{MU} of the MU.

FA/HA *Impersonation.* Since FA and HA use Diffie-Hellman keys to authenticate each other, the adversary is unable to impersonate either of them due to the intractability of the Diffie-Hellman problem. Also, the attacker cannot impersonates FA to fool MU. Since he/she does not posses the secret x and ID_{MU}, n_{MU}, the attacker cannot compute $V_5 = h(SK \| P_{FA}) = h(h(h(ID_{MU} \| x) \| ID_{FA} \| n_{MU} \| ctr_{MU}) \| P_{FA})$. On the other hand, it is impossible for him/her to obtain the session key SK by computing $SK = V_3 \oplus h(K)$ due to the difficulty of solving Diffie-Hellman problem and form the $V_5 = h(SK \| P_{FA})$ to the MU.

6.4 Secure Key Establishment and Forward Secrecy [9]

At the end of the protocol, the MU, FA and HA will establish a common session key $SK = h(h(ID_{MU} \| x) \| ID_{FA} \| n_{MU} \| ctr_{MU})$. Since the attacker does not know the value of x, he/she cannot compute the SK directly. Even if the previous session keys are disclosed, the attacker cannot obtain any future session key due to the security of one-way hash function.

Our proposed protocol also achieves perfect forward secrecy. Since the value of n_{MU} is freshly generated in each session, all the past session keys will remain secure even if the long-term secret key x is compromised at a later stage.

Table 2 Security and usability comparison

Feature	He et al. [8]	Jiang [10]	Ours
Correct password update	No	No	Yes
Stolen verifier-table resistance	No	No	Yes
User anonymity	No	Yes	Yes
Mutual authentication	No	Yes	Yes
Strong replay resistance	No	No	Yes
Key agreement	No	Yes	Yes
Password protection	No	Yes	Yes
Two-factor security	No	Yes	Yes
Denial of service resistance	No	No	Yes

6.5 Protection Against Attacks in Section 4

In this section, we show how our new scheme overcomes the security weaknesses presented in Sect. 4.

(1) In our proposed scheme, there is no verifier table in HA's database to store the secret information of MU or FA. Thus, the attacker cannot launch stolen-verifier attacks.
(2) In order to prevent replay attack, we used the counter based authentication mechanism. HA can detect the attack by examining the counter ctr_{MU} of the user MU.
(3) In order to prevent denial of service attack, the smart card will verify whether the PW_{MU} entered by MU is correct or not in the login phase and password update phase.

7 Performance Comparison

We compare our new scheme with two recently proposed smart card based anonymous user authentication schemes due to He et al. [8] and Jiang et al. [10]. In Table 2, we provide the comparison based on the key security of these schemes, while we compare their efficiency in terms of computation and communication cost in Table 3. The following notation are used in Table 3. t_h: The time complexity of the hash computation; t_m: The time complexity of the modular squaring computation; t_{qr}: The time complexity of computing a square root modulo n; t_{me}: The time complexity of computing modular exponentiation; t_{sym}: The time complexity of symmetric encryption/decryption; t_{asym}: The time complexity of encryption/decryption or signature using asymmetric cryptosystem.

From Table 2, we can conclude that our proposed scheme provides better security and usability than the other two schemes.He et al.'s scheme in [8] does not satisfy any of the criterion listed in Table 2. Jiang et.al.'s scheme in [10] does not satisfy four of the nine criterion. Our scheme can achieve all the criterion listed in Table 2. In particular, one special feature of our scheme is that we do not require the HA to store some secret information that is shared with FA in his/her database, which enhances our scheme's security strength to resist against different attacks.

In Table 3, we summarize the efficiency comparison between our scheme and other schemes in [8,10] in case of the authentication phase. From the Table 3, it is easy to see that our scheme is more efficient than He et al.'s scheme in [8]. Our scheme requires two extra Modular Exponentiation for FA and HA as compared with Jiang et al.'s scheme. It is not a problem because the FA and the HA are powerful and have no resource constraints.

Table 3 Efficiency comparison

	Jiang et al. [10]	He et al. [8]	Ours
C1	$3t_h + t_m$	$10t_h + 2t_{sym}$	$3t_h + t_m$
C2	$4t_h$	$t_h + t_{asym}$	$3t_h + t_{me}$
C3	$5t_h + t_{qr}$	$4t_h + 2t_{sym} + 4t_{asym}$	$5t_h + t_{me} + t_{qr}$
C4	1	1	1
C5	1	1	1
C6	4	5	4
C7	6	6	5

C1: Computation cost of the MU
C2: Computation cost of the FA
C3: Computation cost of the HA
C4: Communication rounds between the MU and FA
C5: Communication rounds between the FA and HA
C6: Total messages transmitted between the MU and FA
C7: Total messages transmitted between the FA and HA

Moreover, we also save one hash operation for MU and reduce one transmitted message. On the other hand, our scheme achieves stronger security than the previous solutions, as is shown in Table 2.

8 Conclusion

In this paper, we discussed several security weaknesses in a recently proposed smart card based privacy preservation user authentication scheme by Jiang et al. We showed that this scheme is vulnerable to stolen-verifier attacks, replay attacks, denial of service attack. In order to withstand its security flaws, subsequntly we proposed a new smart card based user authentication scheme with user's anonymity for roaming service which can achieve stronger security. Our scheme does not require HA to store a verifier-table in its database and uses counter based authentication mechanism to prevent replay attacks.

References

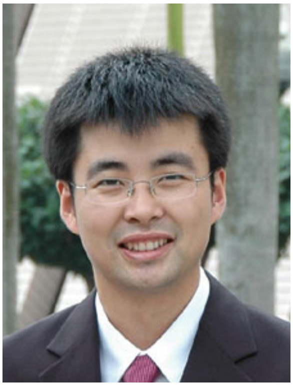
1. Chang, C., Lee, J., & Chang, Y. (2005). Efficient authentication protocols of GSM. *Computer Communications*, *28*(8), 921–928.
2. Chang, C., Lee, C., & Chiu, Y. (2009). Enhanced authentication scheme with anonymity for roaming service in global mobility networks. *Computer Communications*, *32*(4), 611–618.
3. Chaum, D. (1985). Security without identification: Trunsactions systems to make big brother obsolete. *Communications of the ACM*, *28*(10), 1030–1044.
4. Das, A. (2013). A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. *Networking Science*, *2*(1–2), 12–27.
5. ETSI TS 102 165–1 V4.1.1 Telecommunications and internet protocol harmonization over networks (TIPHON) release 4; protocol framework definition; methods and protocols for security; part 1: Threat analysis.
6. Fatemi, M., Salimi, S., & Salahi, A. (2010). Anonymous roaming in universal mobile telecommunication system mobile networks. *IET Information Security*, *4*(2), 93–103.
7. He, D., Ma, M., Zhang, Y., & Chen, C. (2010). A strong user authentication scheme with smart cards for wireless communications. *Computer Communications*, *34*(3), 367–374.

8. He, D., Chan, S., Chen, C., & Bu, J. (2011). Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks. *Wireless Personal Communications*, *61*, 465–476.
9. IEEE 1363–2000: IEEE Standard Specifications For Public Key Cryptography. Institute of Electrical and Electronics Engineers, 2000.
10. Jiang, Q., Ma, J., Li, G., & Yang, L. (2013). An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. *Wireless Personal Communications*, *68*, 1477–1491.
11. Lee, C., Hwang, M., & Liao, I. (2008). A new authentication protocol based on pointer forwarding for mobile communications. *Wireless Communication and Mobile Computing*, *8*(5), 661–672.
12. Lee, C., Hwang, M., & Yang, W. (2003). Extension of authentication protocol for GSM. *IEE Proceedings Communications*, *150*(2), 91–95.
13. Lee, C., Hwang, M., & Liao, I. (2006). Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Industrial Electronics*, *53*(5), 1683–1686.
14. Lee, T., Chang, C., & Hwang, T. (2005). Private authentication techniques for the global mobility network. *Wireless Personal Communications*, *35*(4), 329–336.
15. Lee, J., Chang, J., & Lee, D. (2009). Security flaw of authentication scheme with anonymity for wireless communications. *IEEE Communications Letters*, *13*(5), 292–293.
16. Menezes, A., Van Oorschot, P., & Vanstone, S. (1997). *Handbook of applied cryptography*. Boca Raton, FL: CRC.
17. Rosen, K. (1988). *Elementary number theory and its applications*. Reading, MA: Addison-Wesley.
18. Syverson, P. (1994), A taxonomy of replay attacks. In *Proceedings IEEE computer security foundations workshop VII*, pp. 131–136.
19. Wang, R., Juang, W., & Lei, C. (2009). A robust authentication scheme with user anonymity for wireless environments. *International Journal of Innovative Computing, Information and Control, 5*(4), 1069–1080. http://grouper.ieee.org/groups/1363/.
20. Wang, R., Juang, W., & Lei, C. (2011). Robust authentication and key agreement scheme preserving the privacy of secret key. *Computer Communications*, *34*(3), 274–280.
21. Wu, C., Lee, B., & Tsaur, W. (2008). A secure authentication scheme with anonymity for wireless communications. *IEEE Communications Letters*, *12*(10), 722–723.
22. Yang, G., Wong, D., Wang, H., & Deng, X. (2008). Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences*, *74*(7), 1160–1172.
23. Yang, G., Wong, D., & Deng, X. (2007). Anonymous and authenticated key exchange for roaming networks. *IEEE Transactions on Wireless Communications*, *6*(9), 1035–1042.
24. Zhu, J., & Ma, J. (2004). A new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Consumer Electronics*, *51*(1), 230–234.

Author Biographies

Fengtong Wen received his Ph.D. degree at Beijing University of Posts and Telecommunications in 2006. Now he is an Associate professor of University of Jinan. His main research topics are Cryptography and information security. He has published more than 30 research papers in the areas of applied cryptography and mathematics.

Willy Susilo obtained his Bachelor Degree in Computer Science from Universitas Surabaya, Indonesia with a "Summa Cum Laude" predicate. He received his Master and Doctor of Philosophy degrees from UOW in 1996 and 2001, resp. His main research interest include cryptography and computer security, in particular the design of signature schemes. He was promoted as a Professor in the School of CS and SE, UOW in 2009. Prior to his current prestigious ARC Future Fellow role, he was the Head of School of SCSSE, Deputy Director of ICT Research Institute and the Academic Program Director for UoW (Singapore). He has published more than 200 papers in journals and conference proceedings in cryptography and network security. He has served as the program committee member of several international conferences.



Guomin Yang received his Ph.D. degree from City University of Hong Kong in 2009. After his Ph.D., he joined the Temasek Laboratories at National University of Singapore as a research scientist. He is now a Lecturer in the School of Computer Science and Software Engineering at University of Wollongong. Dr Yang's has published more than 30 research papers in the areas of applied cryptography and network security. In 2007, he was awarded the (ISC)2 information security scholarship, one of eight recipients all over the world receiving the award.