A Secure and Efficient Mutual Authentication and Key Agreement Protocol with Smart Cards for Wireless Communications

Cheng Guo[1,2], Chin-Chen Chang[3,4], and Shih-Chang Chang[5]
(Corresponding author: Chin-Chen Chang)
School of Software Technology, Dalian University of Technology, China[1]
Key Laboratory for Ubiquitous Network and Service Software of Liaoning Province, China[2]
Department of Information Engineering and Computer Science, Feng Chia University, Taiwan[3]
Department of Computer Science and Information Engineering, Asia University, Taiwan[4]
(E-mail: alan3c@gmail.com)
Department of Computer Science and Information Engineering, National Chung Cheng University, Taiwan[5]
(Received Oct. 10, 2016; revised and accepted Feb. 20, 2017)

Abstract

Mobile user authentication and key agreement for wireless networks is an important security priority. In recent years, several user authentication and key agreement protocols with smart cards for wireless communications have been proposed. In 2011, Xu et al. proposed an efficient mutual authentication and key agreement protocol with an anonymity property. Although the protocol of Xu *et al.* has many benefits, we find that it still suffers from several weaknesses which have been previously overlooked. In this paper, we propose a secure and efficient mutual authentication and key agreement protocol. Confidentiality of the session key and updating of the password efficiently are presented as the main contributions of this paper. Finally, evaluations of our proposed protocol show that our protocol can withstand various known types of attacks, and also satisfies essential functionality requirements. Additionally, efficiency analyses show that our protocol is simple and cost-efficient.

Keywords: Authentication; Key Agreement; Smart Cards; Wireless Communications

1 Introduction

With the rapid development of wireless communications technologies, devices, such as the mobile phone, the PDA (personal digital assistant), and the iPad, have become more and more popular. Mobile users can roam into a foreign network and transmit messages or data to foreign agents, or access some services provided by a foreign agent by using their mobile devices. Obliviously, before establishing communication between a mobile user and a foreign agent, the foreign agent and the user need to carry out mutual authentication and establish a session key. Confidentiality and authentication are two fundamental security goals for wireless communications. Up to now, many authentication and key agreement schemes for wireless environments have been proposed in the literature [3, 7, 8, 16, 19, 23]. Due to the limited power consumption, bandwidth, and storage resources of mobile devices, the authentication and key agreement protocol must take computation efficiency and communication cost on mobile users into consideration. Currently, smart card based user authentication schemes [2, 4, 6, 10, 13, 14, 17, 20, 21] have been widely developed and applied due to their low computational cost, convenient portability, and cryptographic properties. Therefore, in recent years, research [1, 3, 9, 10, 18, 19, 22] on authentication and key agreement based on smart cards for wireless communications has become more and more popular in the world.

In 1998, Miller *et al.* [12] first proposed an authentication and key agreement protocol based on elliptic curve cryptograph (ECC). Their scheme is suitable for running in wireless mobile devices due to its low computational cost. In 2004, Zhu and Ma [23] proposed an authentication protocol with anonymity for wireless communications using smart cards. Later, Lee *et al.* [7] pointed out that Zhu and Ma's protocol has several security weaknesses, and then they improved it. However, recently, Xu *et al.* [19] showed that Lee *et al.*'s protocol [7] is vulnerable to several weaknesses, and then proposed a mutual authentication and key agreement protocol preserving user anonymity in mobile networks. They claimed that their protocol was immune to various known types of attacks and achieved identity anonymity, key agreement fairness, and user friendliness. However, in this paper, we will show that Xu *et al.*'s protocol has three weaknesses as follows:

1) It cannot protect against an insider attack;

2) Session-key problem;

3) Inefficiency of the password-changing operation;

We will detail these weaknesses later.

To the best of our knowledge, in the most existing authentication and key agreement protocols for wireless communications, the home agent was able to compute the session key between the mobile user and the foreign agent. There are potential risks for some confidential communications.

In order to remedy these weaknesses, we propose an enhanced authentication and key agreement protocol with smart cards for wireless communications. Analysis shows that the proposed protocol is effective in protection from the above weaknesses. Furthermore, our protocol is immune to various known types of attacks. Compared with the previous schemes [3, 7, 19], our protocol not only satisfies more security and functionality requirements, but also provides an acceptable computational cost. As mentioned in the literature [3, 5, 9, 15, 18, 19] and the above description, the following requirements are important for a strong user mutual authentication and key agreement protocols using passwords and smart cards for wireless communications:

1) Mutual authentication;

2) Update password freely and efficiently;

3) Fairness in key agreement;

4) No registration/password table;

5) Low communication cost and computational complexity;

6) Protection of user anonymity;

7) Withstanding the insider attack;

8) Withstanding the replay attack;

9) Withstanding the offline dictionary attack without the smart card;

10) Withstanding the offline dictionary attack with the smart card;

11) Confidentiality of the session key.

The reminder of this paper is organized as follows. In next section, we briefly review Xu *et al.*'s scheme, whose weaknesses are pinpointed in Section 3. Section 4 describes a new secure and efficient mutual authentication and key agreement protocol that gives a remedy for Xu *et al.*'s scheme. Section 5 analyzes the security of our protocol and presents functionality considerations and computational cost among our protocol and the related protocols. Finally, we give a conclusion in Section 6.

2 Review of Xu *et al.*'s Scheme

In this section, we review Xu *et al.*'s [19] mutual authentication and key agreement protocol in mobile networks, which claims to be immune to various known types of attacks. Basically, Xu *et al.*'s scheme contains three phases: out-of-band registration, mutual authentication between MN and FA, and session key renewal. Table 1 lists the notations used in Xu *et al.*'s scheme.

Table 1: The notations used in Xu *et al.*'s scheme

Notations	Descriptions
MN	A mobile user
HA	Home agent of a mobile user
FA	Foreign agent of the network visited by the user
PW_X	The password of a mobile user X
ID_X	The identity of an entity X
$h(.)$	A one-way hash function
T_X	Time stamp by an entity X
$\|\|$	String concatenation operation
$\oplus$	The bitwise XOR operation
$E_{K(.)}$	Symmetric encryption of a message using key K

2.1 Out-of-band Registration Phase

Xu *et al.*'s scheme is initialized by the HA with choosing the public parameters (p, q, g), where g is a generator in a multiplicative group of order q, $p = 2q + 1$ is the modulus for the group, and both p and q are public large prime numbers. The HA selects a private key b and computes its public key $B = g^b \bmod p$. When a mobile user MN wants to register with his HA, he chooses his identity ID_{MN} and password PW_{MN}, and then submits them to the HA. Then HA computes $u = E_N(h(PW_{MN})||ID_{MN})$ with its server secret key N, and securely issues a smart card to the MN, which contains p, g, B, u, and $h(.)$.

2.2 Mutual Authentication Phase

As a precondition, HA needs to pre-share a distinct symmetric key k_{FH} with each FA. When a user MN visits a new foreign network, the following steps are performed:

Step 1. MN enters his identity ID_{MN} and his password PW_{MN} to the smart card. Then the device selects two secret random numbers a and r_{MN}, computes $A = g^a \bmod p$, $D = h(B^a \bmod p)$, $C = h(PW_{MN}) \oplus D$, $R = E_C(r_{MN}||ID_{MN})$, and $U = E_D(T_{MN}||u)$, where T_{MN} is a time stamp. Finally, the device sends the authentication message $(ID_{HA}, T_{MN}, A, R, U)$ to FA.

Step 2. On receiving the authentication message, FA first checks whether T_{MN} is valid. If so, FA chooses

a random number r_{FA}, generates its timestamp T_{FA}, computes $Q = E_{k_{FH}}(T_{MN}||r_{FA}||T_{FA}||U||R)$, and sends the message (A, Q) to HA.

Step 3. On receiving the message (A, Q), HA decrypts Q with k_{FH}, and obtains the message $T_{MN}||r_{FA}||T_{FA}||U||R$. HA first checks whether T_{FA} is valid. If so, HA computes $D = h(A^b \bmod p)$ for decrypting U, so as to recover $T_{MN}||u$. Then HA checks whether the T_{MN} equals the previous one from Q. If the timestamp is valid, HA decrypts u with his secret key N to recover $h(PW_{MN})||ID_{MN}$, and computes $C = h(PW_{MN}) \oplus D$ so as to recover $r_{MN}||ID_{MN}$. If ID_{MN} from R equals the previous one from u, MN is authenticated. Finally, HA computes $K = E_{k_{FH}}(r_{FA}||r_{MN})$ and $S = E_D(r_{MN}||r_{FA}||ID_{FA})$, and sends the message (K, S) to FA.

Step 4. FA decrypts K to obtain $r_{FA}||r_{MN}$. If the recovered r_{FA} equals the previous one, the FA believes that MN is an authorized user, and forwards S to MN.

Step 5. MN decrypts S to recover $r_{MN}||r_{FA}||ID_{FA}$. If r_{MN} and ID_{FA} are verified, MN believes FA is authenticated. Then, both MN and FA can compute the session key $k = r_{MN} \oplus r_{FA}$.

2.3 Session Key Renewal Phase

In this phase, the session key can be updated by MN and FA from k_i for the current ith session to $k_{i+1} = h(k_i||r_{MN})$ for the next session.

3 Weaknesses of Xu *et al.*'s Scheme

The authors of [19] proposed a mutual authentication and key agreement protocol featuring user identity anonymity. They claimed that their protocol was resilient to various attacks, cost-efficient for a mobile user, and achieved key agreement fairness. However, in this section, we present that Xu *et al.*'s scheme still has a number of serious deficiencies. The detailed description of three weaknesses is as follows.

3.1 Insider Attack

Insider attack means that if an insider of HA has obtained a mobile user MN's password, there may be an unauthorized and illegitimate access to any foreign agent. In the registration phase of Xu *et al.*'s protocol, MN sent his identity ID_{MN} and password PW_{MN} to the home agent HA, that is, PW_{MN} was revealed to HA. It will give an inside attacker an opportunity to impersonate other users. With a strong authentication protocol in wireless networks, there should be no way to directly obtain the users' passwords.

3.2 Session-key Problem

In Xu *et al.*'s protocol, the session key can be computed as $k = r_{MN} \oplus r_{FA}$ by MN and FA, respectively. However, the mutual authentication between MN and FA must resort to the assistance of the corresponding HA. However, in the mutual authentication phase of Xu *et al.*'s protocol, HA can recover the r_{MN} and r_{FA} from the authentication request. Therefore, HA also has a capability to compute the session key $k = r_{MN} \oplus r_{FA}$. It is well known that this session key is used to encrypt all messages in the communication session between MN and FA. We can see that the protocol of Xu *et al.* merely provided the session key agreement. However, they cannot guarantee the confidentiality of the session key. As to many applications, there are potential risks. That is, the design in Xu *et al.*'s protocol is actually insecure and infeasible.

3.3 Inefficiency of Password-changing Operation

In a strong user authentication and key agreement protocol, user should have a capability to update his password. In Xu *et al.*'s protocol, we can see that HA computes $u = E_N(h(PW_{MN})||ID_{MN})$ with its server secret key N, and stores u into the smart card. It means that the smart card needs to replace the old parameter u with the new parameter $u*$. Since the password PW_{MN} is encrypted by HA using his secret key N, MN has to resubmit his new PW^*_{MN} to HA, and HA replaces the original u in MN's smart card with $u* = E_N(h(PW^*_{MN})||ID_{MN})$. MN has to communicate with HA through the smart card and the wireless network. This makes the password-changing operation inefficient.

4 The Proposed Protocol

To overcome the above-mentioned weaknesses, in this section, we propose a secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications, which consists of parameter-generation phase, registration phase, authentication phase, key agreement phase, and password-change phase.

4.1 Parameter-generation Phase

Compared with public key cryptosystems such as RSA and ElGamal, ECC provides a better efficiency because it is believed that the same level of security can be achieved with a smaller key size. Therefore, ECC-based authentication and key agreement protocols are more suitable for smart cards and mobile devices which usually have energy constraints and significant bandwidth.

For ease of presentation, we employ some abbreviations and notations provided in Xu *et al.*'s protocol, summarized in Table 1. In the proposed protocol, the elliptic curve equation is defined as $E_P : y^2 = x^3 + ax + b(\bmod p)$

over a prime finite field Z_p, where $a, b \in Z_p$, and $4a^3 + 27b^2 (\mathrm{mod} p) \neq 0$.

Our protocol is initialized by the HA by choosing the public parameters (E_P, G), where G is a generator point of E_P. The HA selects his private key $SK_{HA} = c$ and computes his public key $PK_{HA} = c \times G(\mathrm{mod} p)$. Also, the FA selects his private key $SK_{FA} = d$ and computes his public key $PK_{FA} = d \times G(\mathrm{mod} p)$.

4.2 Registration Phase

The registration phase is similar to that of Xu *et al.*'s protocol. When a mobile user MN wants to register and become a new legal user, MN submits his identity ID_{MN} to HA over a secure channel. As is shown in Figure 1, the following steps are performed by the HA in this phase.

Step 1. HA computes $u = E_{K_S}(ID_{MN}||K_S) \oplus h(pw)$, where K_S is the HA's secret key, and pw is the initial password selected by HA.

Step 2. HA computes $IM = E_{K_S}(ID_{MN}||r)$, where r is a random number to provide the identity protection.

Step 3. HA issues the password pw and the smart card to MN over a secure channel, where the smart card contains $\{u, IM, h(.), PK_{HA}\}$.

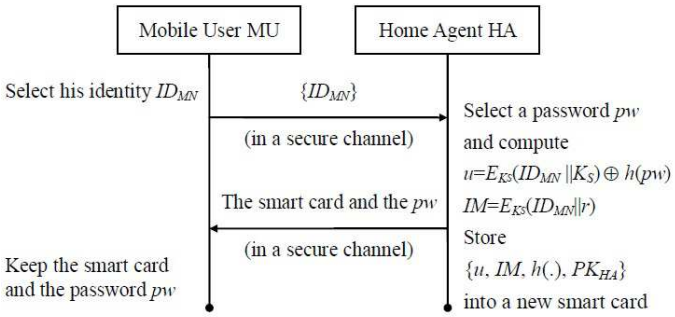

Figure 1: The registration phase of the proposed protocol

4.3 Authentication Phase

In this phase, the mobile user MN and a foreign agent FA can authenticate each other and share a session key K for the subsequent secret communication. When a mobile user MN roams into a new foreign network and wants to access service, the following steps are performed.

Step 1. MN enters his identity ID_{MN} and his password pw to the smart card. Then the smart card chooses two random numbers e and r_{MN}, and computes $A = e \times G(\mathrm{mod} p)$ and $U = E_D(T_{MN}||u)$, where T_{MN} is a current time stamp and $D = e \times PK_{HA} = e \times c \times G$. Subsequently, the smart card computes $N = h(pw) \oplus D$ as a secret key, and computes $R = E_N(r_{MN}||ID_{MN})$.

Step 2. The smart card sends an authentication request message $\{R, ID_{HA}, IM, U, A, T_{MN}\}$ to FA.

Step 3. After receiving the authentication request from MN, FA first check whether the time stamp T_{MN} is valid. If it is valid, FA selects a random number r_{FA} and computes $V = E_M(T_{MN}||r_{FA}||T_{FA}||U||IM||R)$, where $M = d \times PK_{HA} = d \times c \times G$, and T_{FA} is a time stamp. Then, FA sends the message $\{A, V, PK_{FA}\}$ to HA.

Step 4. After receiving the message $\{A, V, PK_{FA}\}$, HA first computes $M = c \times PK_{FA} = c \times d \times G$, and decrypts V by using M. HA then verifies whether T_{FA} is valid. If so, HA decrypts IM by using his secret key K_S to recover ID_{MN}, and computes $E_{K_S}(ID_{MN}||K_S)$. Then, HA computes $D = c \times A = c \times e \times G$ for decrypting U aiming at recovering T_{MN} and u. HA checks whether the decrypted T_{MN} is the same as the T_{MN} decrypted from V. If they are valid, HA can obtain $h'(pw)$ by computing $E_{K_S}(ID_{MN}||K_S) \oplus u$.

Step 5. HA can compute $N' = h'(pw) \oplus D$. If MN submitted a correct password in Step 1, we can believe $N = N'$. And, HA can decrypt R for recovering r_{MN} and ID_{MN}. Then HA checks whether ID_{MN} from R equals the previous one from u. If so, MN is authenticated.

4.4 Key Agreement Phase

In this phase, FA and HA can be authenticated, and a secure session key between MN and FA can be established. The steps of this phase are shown as follows.

Step 1. HA computes $K = E_{cPK_{FA}}(r_{MN}||r_{FA})$ and $S = E_{cA}(r_{MN}||r_{FA}||ID_{FA}||PK_{FA})$, and sends the message (K, S) to FA.

Step 2. After receiving the message, FA decrypts K with $d \times PK_{HA}$ to recover r_{MN} and r_{FA}. If the recovered r_{FA} and the original one are identical, FA believes that the mobile user MN is a valid user. Then FA forwards S to MN.

Step 3. Upon receiving the message S from FA, MN first decrypts S with $e \times PK_{HA}$, where $e \times PK_{HA} = c \times A$, for recovering $\{r_{MN}, r_{FA}, ID_{FA}, PK_{FA}\}$. If the r_{MN} and the ID_{FA} are both verified, MN believes that FA is authenticated. Finally, both MN and FA can compute the agreed session key $SK = E_{d \times A}(r_{MN} \oplus r_{FA}) = E_{e \times PK_{FA}}(r_{MN} \oplus r_{FA})$.

The above two phases are outlined in Figure 2.

4.5 Password-change Phase

When a mobile user MN wants to renew a password, MN can insert his smart card into the card reader and performs the following steps.

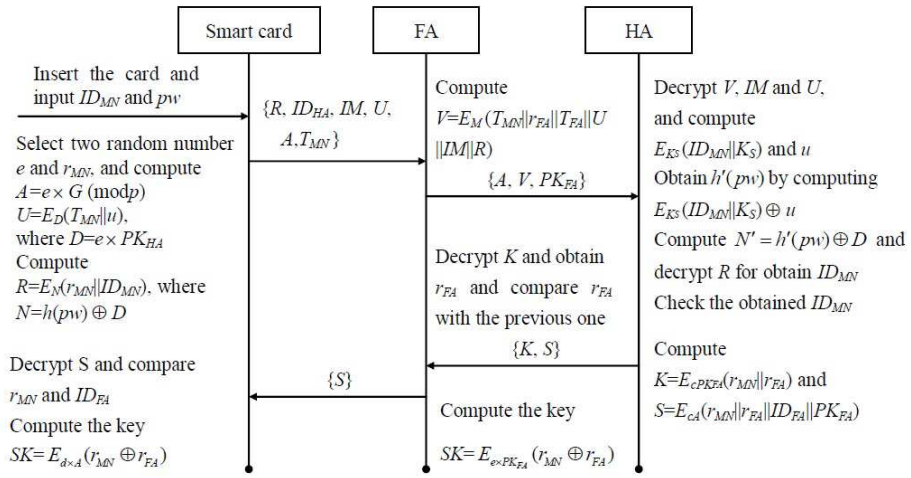

Figure 2: The authentication and key agreement phase of the proposed protocol

Step 1. Firstly, MN keys in the old password, and requests to renew password pw. Next, MN enters the new password pw^*.

Step 2. The smart card computes $u* = u \oplus h(pw) \oplus h(pw*)$, and replaces u with $u*$.

5 Evaluations of the Proposed Protocol

In this section, we will give an analysis for our protocol in terms of security, functionality, and efficiency.

5.1 Security Analysis

In this subsection, security analysis of our protocol will be discussed. At the end of this subsection, the comparisons of the related works are given in Table 2.

1) User anonymity

Anonymity is becoming a major concern in many security requirements. The aim of user anonymity in wireless networks is to make sure that the real identity of a mobile user is protected from anyone besides his home agent.

During the registration phase, HA computes u by encrypting $ID_{MN}||K_S$ with his secret key K_S and computes $IM = E_{K_S}(ID_{MN}||r)$, where r is a random number to provide the identity protection. Even though the smart card containing u and IM is lost and the attackers obtain $\{u, IM\}$ from the smart card, they can not retrieve any information about the user's real identity since the identity information is encrypted by using HA's secret key K_S. In the authentication phase, the smart card sends an authentication request $\{R, ID_{HA}, IM, U, A, T_{MN}\}$ to FA. Since R and U are encrypted by using the corresponding session key D between MN and HA and N, where $N = h(pw) \oplus D$, respectively, HA cannot retrieve the real identity of the user according to these authentication messages.

2) Withstanding the insider attack

The insider attack in the authentication for wireless networks is that the mobile user's password is submitted to the home agent in the registration phase, and an inside attacker can steal his password and impersonate this user. In our proposed protocol, in the registration phase, the initial password is provided by the home agent. And the home agent issues a smart card containing this password and other security parameters to the mobile user. And then, the user has a capability to change the password freely and securely. As described in Section 4.5, the update-password operation does not require the assistance of the home agent. Therefore, an inside attacker cannot obtain any information about the user's password from the home agent.

3) Withstanding the replay attack

The replay attack is that the login messages are maliciously or fraudulently repeated or delayed between the user and the server. In the authentication phase, the authentication request message contains the timestamp T_{MN} and T_{FA} . If the adversaries delay the request message or resend these messages, we can check whether the current time is valid according to the timestamp.

4) Withstanding the offline dictionary attack without the smart card

The offline dictionary attack without the smart card is that attackers attempt to guess the user's password or the user's identity via the intercepted message between the mobile user and the foreign agent or between the foreign agent and the home agent. In the proposed protocol, we can see that the authentication request message $R = E_N(r_{MN}||ID_{MN})$,

Table 2: Security comparisons between the related protocols and the proposed protocol

	Our protocol	**He *et al.*'s protocol [3]**	**Xu et la.'s protocol [19]**	**Lee *et al.*'s protocol [7]**
S1	YES	NO	YES	NO
S2	YES	YES	NO	NO
S3	YES	YES	YES	YES
S4	YES	YES	YES	YES
S5	YES	YES	YES	YES
S6	YES	NO	NO	NO

S1: User anonymity; S2: Withstanding the insider attack; S3: Withstanding the replay attack; S4: Withstanding the offline dictionary attack without the smart card; S5: Withstanding the offline dictionary attack with the smart card; S6: Confidentiality of the session key

$IM = E_{K_S}(ID_{MN}||r)$ and $U = E_D(T_{MN}||u)$. Since r_{MN} and r are random numbers, and $u = E_{K_S}(ID_{MN}||K_S) \oplus h(pw)$, even though the identity ID_{MN} and the password are weak, the attackers cannot guess the right password and the identity. In the next phase, FA sends the message $\{A, V, PK_{FA}\}$ to HA, where V contains a random number r_{FA}. So, the attackers cannot obtain any information about the user's identity and his password.

5) Withstanding the offline dictionary attack with the smart card

We assume that the attackers can obtain the information stored in the smart card through some ways. This attack is the same as the above attack except in this case. In our proposed protocol, the password pw is stored in the smart card as the form $u = E_{K_S}(ID_{MN}||K_S) \oplus h(pw)$. Since the attackers cannot obtain the home agent's secret key K_S, they cannot guess the right password.

6) Confidentiality of the session key

Key agreement protocol is to establish a secret session key between the mobile user MN and the foreign agent FA aim at encrypting further communications between the MN and the FA. Therefore, the session key should be shared only between the MN and the FA, and other entities cannot retrieve any information about the session key. However, in [3, 7, 19], the home agent also has a capability to calculate the session key. In the proposed protocol, the session key $SK = E_{d\times A}(r_{MN} \oplus r_{FA}) = E_{e\times PK_{FA}}(r_{MN} \oplus r_{FA})$, where the $r_{MN} \oplus r_{FA}$ is encrypted by using an agreed key. Though the home agent can obtain r_{MN} and r_{FA}, he can not compute the key $d\times e\times G = e\times d\times G$. So, HA cannot compute the session key SK.

5.2 Functionality Consideration

Now we move on the functionality consideration. Some comparisons with related works are presented. We examine our protocol as follows.

1) Mutual authentication

In the proposed protocol, the foreign agent and the mobile user can authenticate each other under the assistance of the home agent HA, and after a successful validation, a common session key can be established between the foreign agent and the mobile user.

To achieve the mutual authentication, HA stores $u = E_{K_S}(ID_{MN}||K_S) \oplus h(pw)$ and $IM = E_{K_S}(ID_{MN}||r)$ in MN's smart card at the registration phase. In Step 1 of the authentication phase, the smart card computes $R = E_N(r_{MN}||ID_{MN})$, where $N = h(pw) \oplus D$, and sends $\{R, IM, U\}$ to FA. FA utilizes a session key M between FA and HA to encrypt these authenticated request information $\{R, IM, U\}$ and sends these messages to HA. HA can recover $\{R, IM, U\}$ and retrieve ID_{MN} from IM by using his secret key K_S. Further, HA computes $E_{K_S}(ID_{MN}||K_S)$ and obtain $h'(pw)$ by computing $E_{K_S}(ID_{MN}||K_S) \oplus u$. Then, HA can compute $N' = h'(pw) \oplus D$, and retrieve ID_{MN} from R. We can see that if the mobile user does not submit the correct ID_{MN} and password, HA cannot decrypt R correctly, and the retrieved ID_{MN} cannot equal the previous one from IM. Finally, both MN and FA can compute the agreed session key $SK = E_{d\times A}(r_{MN} \oplus r_{FA}) = E_{e\times PK_{FA}}(r_{MN} \oplus r_{FA})$.

2) Update password freely and efficiently

In the proposed protocol, when the home agent HA issues a smart card to the mobile user MN, the MN can update his password freely. As described in Section 4.5, each mobile user can choose or update one of his favorite strings as his password, not decided by the home agent. And, the update-password operation can be performed without the assistance of the home agent. As to wireless networks, when a mobile user roams into a foreign network, the update-password operation of our proposed protocol is more suitable than Xu *et al.*'s protocol in terms of communication cost.

3) Fairness in key agreement

Table 3: Functionality comparisons between the related protocols and the proposed protocol

	Our protocol	**He *et al.*'s protocol [3]**	**Xu et la.'s protocol [19]**	**Lee *et al.*'sprotocol [7]**
F1	YES	YES	YES	YES
F2	YES	YES	YES	NO
F3	YES	YES	NO	NO
F4	YES	NO	YES	YES
F5	YES	YES	YES	YES
F1: Mutual authentication; F2: Update password freely; F3: Update password efficiently; F4: Fairness in key agreement; F5: No registration/password table				

Our proposed protocol ends up with MN and FA agreeing on a session key $SK = E_{d\times e\times G}(r_{MN} \oplus r_{FA})$, where r_{MN} and r_{FA} are random numbers selected by MN and FA, respectively, which has a similar structure with the session key of Xu *et al.*'s protocol. The difference is that $r_{MN} \oplus r_{FA}$ is encrypted by using an agree key $d \times A = e \times PK_{FA}$, where e is a secret value of MN, and d is a secret value of FA. Therefore, the session key SK contains equal contributions from both parties.

4) No registration/password table

In some password-based authentication protocols, the server has to store a password table or a registration table for verification. That is, HA has to maintain a secret and large table. And, it will give a chance for an inside attacker to access the password or the registration information. In the proposed protocol, HA does not need to keep a registration table or a password table. HA can compute the verification messages $u = E_{K_S}(ID_{MN}||K_S) \oplus h(pw)$ and $IM = E_{K_S}(ID_{MN}||r)$, and store u and IM into the smart card. In the authentication phase, FA and MN can authenticate each other under the assistance of HA.

Finally, we summarize the functionality of our protocol and make comparisons with that of related works [3, 7, 19] in Table 3.

5.3 Efficiency Analysis

In this subsection, we will evaluate the performance of our protocol and make comparisons with the related works. The heavy weight computation of the proposed protocol is to execute scalar multiplication on elliptic curve. The computational cost of elliptic curve point multiplication is much less than that of modular exponentiation, and 160-bit elliptic curve discrete logarithm problem and 1024-bit discrete logarithm problem have the same security level. Therefore, contrary to traditional public key cryptosystem-based authentication and key agreement protocol, our proposed protocol reduces the computation, communication, and storage space costs since ECC is used. In Table 4, we tabulate the computational costs of MN, FA, and HA for our proposed protocol and the related protocols [3, 7, 19].

6 Conclusions

Recently, Xu *et al.* proposed a mutual authentication and key agreement protocol preserving user anonymity in mobile networks. In this paper, we have shown the weaknesses of the protocol of Xu *et al.* and further proposed an improved protocol based on ECC. Furthermore, we propose a secure and efficient mutual authentication and key agreement protocol with smart cards for wireless communications. Security analyses show that our protocol is able to provide mutual authentication and key agreement with user anonymity and is effective in withstanding various attacks. Meanwhile, our protocol provides essential functionalities that satisfy the most important applications for mobile devices in wireless networks. Efficiency analyses also demonstrate that our protocol is more efficient than the previous ones.

Acknowledgments

This paper is supported by the National Science Foundation of China under grant No. 61401060, 61501080 and 61572095, and the Fundamental Research Funds for the Central Universities' under grant No. DUT16QY09.

References

[1] P. Y. Cui, "An improved ownership transfer and mutual authentication for lightweight RFID protocols," *International Journal of Network Security*, vol. 18, no. 6, pp. 1173-1179, 2016.

[2] C. Guo and C. C. Chang, "Chaotic maps-based password-authenticated key agreement using smart cards," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, pp. 1433–1440, 2013.

[3] D. J. He, M. D. Ma, Y. Zhang, C. Chen, and J. J. Bu, "A strong user authentication scheme with anonymity for wireless communications," *Computer Communications*, vol. 34, pp. 367–374, 2011.

Table 4: Performance comparisons between the related protocols and the proposed protocol

Primitives		**Our protocol**	**He *et al.*'s protocol [3]**	**Xu et la.'s protocol [19]**	**Lee *et al.*'s protocol [7]**
H	MN	1	10	1	2
	FA	N/A	5	N/A	N/A
	HA	1	5	N/A	3
E	MN	N/A	N/A	2	N/A
	FA	N/A	N/A	N/A	N/A
	HA	N/A	N/A	1	N/A
S	MN	4	2	3	2
	FA	3	1	2	1
	HA	7	2	6	1
M	MN	3	N/A	N/A	N/A
	FA	2	3	N/A	N/A
	HA	2	3	N/A	N/A
H: Hash operation; E: Modulus exponential operation; S: Symmetric encryption or decryption; M: Scalar multiplication on elliptic curve					

[4] M. S. Hwang, S. K. Chong, and T. Y. Chen, "DoS resistant ID-based password authentication scheme using smart cards," *Journal of Systems and Software*, vol. 83, pp. 163–172, 2010.

[5] M. H. Ibrahim, "Octopus: An edge-fog mutual authentication scheme," *International Journal of Network Security*, vol. 18, no. 6, pp. 1089-1101, 2016.

[6] W. S. Juang, S. T. Chen, and H. T. Liaw, "Robust and efficient password-authenticated key agreement using smart card," *IEEE Transactions on Industrial Electronics*, vol. 55, pp. 2551–2556, 2008.

[7] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronic*, vol. 53, pp. 1683–1686, 2006.

[8] C. T. Li and M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks," *Information Sciences*, vol. 181, pp. 5333–5347, 2011.

[9] C. T. Li and C. C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications," *Mathematical and Computer Modeling*, vol. 55, pp. 35–44, 2012.

[10] X. Li, J. W. Niu, M. K. Khan, and J. G. Liao, "An enhanced smart card based remote user password authentication scheme," *Journal of Network and Computer Applications*, vol. 36, pp. 1365–1371, 2013.

[11] Y. Ma, "NFC communications-based mutual authentication scheme for the internet of things," *International Journal of Network Security*, vol. 19, no. 4, pp. 631-638, 2017.

[12] V. S. Miller, "Use of elliptic curves in cryptography," in *Proceeding of the Advances in Cryptology (CRYPTO'85)*, pp. 417–426, 1985.

[13] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure user anonymity-preserving biometric- based multi-server authenticated key agreement scheme using smart cards," *Expert Systems with Applications*, vol. 41, pp. 8129–8143, 2014.

[14] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure and efficient ecc-based user anonymity-preserving session initiation authentication protocol using smart card," *Peer-to-Peer Networking and Applications*, vol. 9, pp. 171–192, 2016.

[15] M. Ramadan, F. Li, C. Xu, *et al.*, "User-to-user mutual authentication and key agreement scheme for LTE cellular system," *International Journal of Network Security*, vol. 18, no. 4, pp. 769-781, 2016.

[16] R. V. Sampangi and S. Sampalli, "Metamorphic framework for key management and authentication in resource-constrained wireless networks," *Information Sciences*, vol. 19, pp. 430–442, 2017.

[17] D. Z. Sun, J. P. Huai, J. Z. Sun, J. X. Li, J. W. Zhang, and Z. Y. Feng, "Improvements of juang *et al.*s password-authenticated key agreement scheme using smart cards," *IEEE Transactions on Industrial Electronics*, vol. 56, pp. 2284–2291, 2009.

[18] C. C. Wu, W. B. Lee, and W. J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," *IEEE Communications Letters*, vol. 12, pp. 722–723, 2008.

[19] 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, pp. 319–325, 2011.

[20] H. M. Yang, Y. X. Zhang, Y. Z. Zhou, and et al., "Provably secure three-party authenticated key agreement protocol using smart cards," *Computer Networks*, vol. 58, pp. 29–38, 2014.

[21] K. H. Yeh, C. Su, N. W. Lo, Y. Li, and Y. X. Hung, "Two robust remote user authentication protocols using smart cards," *Journal of Systems and Software*, vol. 83, pp. 2556–2565, 2010.

[22] E. J. Yoon, K. Y. Yoo, and K. S. Ha, "A user friendly authentication scheme with anonymity for wireless communications," *Computers and Electrical Engineering*, vol. 37, pp. 356–364, 2011.

[23] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Consumer Electronics*, vol. 51, pp. 230–234, 2004.

Biography

Cheng Guo received the B.S. degree in computer science from Xian University of Architecture and Technology in 2002. He received the M.S. degree in 2006 and his Ph.D in computer application and technology, in 2009, both from the Dalian University of Technology, Dalian, China. From July 2010 to July 2012, he was a post doc in the Department of Computer Science at the National Tsing Hua University, Hsinchu, Taiwan. Since 2013, he has been an associate professor in the School of Software Technology at the Dalian University of Technology. His current research interests include information security, cryptology and cloud security.

Shih-Chang Chang received his B.S. degree in 2005 and his M.S. degree in 2007, both in Department of Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan. He is currently pursuing his Ph.D. degree in Computer Science and Information Engineering from National Chung Cheng University, Chiayi, Taiwan. His current research interests include electronic commerce, information security, computer cryptography, and mobile communications.

Chin-Chen Chang received his B.S. degree in applied mathematics in 1977 and the M.S. degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. From 1983-1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the college of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From July 1998 to June 2000, he was the director of Advisory Office of the Ministry of Education of the R.O.C. From 2002 to 2005, he was a Chair Professor of National Chung Cheng University. Since February 2005, he has been a Chair Professor of Feng Chia University. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression and data structures. He is a fellow of the IEEE.