International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.335-344
http://dx.doi.org/10.14257/ijsia.2013.7.6.34

Cryptanalysis and Improvements of an Anonymous Authentication Scheme for Roaming Service in Global Mobility Networks

Zuowen Tan[1,2]
1. *Jiangxi Advanced Research Center of E-commerce Engineering, School of Information Technology,Jiangxi University of Finance and Economics, Nanchang 330032, China*
2. *Key Laboratory of Mathematics and Interdisciplinary Sciences of Guangdong Higher Education Institutes, Guangzhou University, Guangzhou 510006, China*
tanzyw@163.com

Abstract

In wireless environments, the issue of mutual authentication and key agreement with user anonimity is challenging. Recently, Mun et al. proposed an efficient anonymous authentication scheme for roaming services in wireless enviroments. Unfortunately, Kim et al. pointed out that Mun et al.'s anonymous authentication scheme suffers from replay attacks and man-in-the-middle attacks. They propose an improved secure anonymous authentication scheme for roaming services. Kim et al. claimed that their protocol removed the weaknesses of the Mun et al.'s scheme. However, we show that Kim et al.'s scheme fails to achieve anonymity. In addition, Kim et al.'s scheme is vulnerable to replay attacks and impersonation attacks and is impractical in the real-life implementation. We then propose an enhanced privacy-preserving authentication scheme. We demonstrate that our scheme overcomes the aforementioned weaknesses.

Keywords: *Authentication, Wireless network, Password, Smart card, Anonymity*

1. Introduction

Authenticated key exchange enables two or more parties communicating over a public network to generate a high-entropy cryptographic key (also known as a session key) [1-3]. In recent years, wireless and mobile communication systems bring people more and more convenience [4]. Wireless network makes people use mobile devices to access all kinds of services anytime and anywhere. However, the movement and open access in ubiquitous mobile wireless environments have raised some security issues such as user's privacy. Authentication with anonymity is fundamental. Many authentication and key agreement protocols for wireless environments have been proposed [5-9]. In 2004, Zhu *et al.*, presented an anonymous wireless scheme based on the smart card [5]. However, Lee *et al.*, [10] pointed out that Zhu-Ma scheme cannot achieve perfect backward secrecy and mutual authentication and cannot resist against a forgery attack. Lee et al. proposed a new authentication and key agreement protocol for wireless environments to overcome the weaknesses of Zhu-Ma scheme. Chang *et al.*, [11], Wu *et al.*, [9] and Xu *et al.*, [6] showed that Lee *et al.*,'s scheme failed to provide user anonymity,respectively. To remedy the weakness, they proposed their improvement respectively. Unfortunately, He *et al.*, [7] showed that Wu et al.'s scheme is vulnerable to several weaknesses such as failing to provide user anonymity. But their improved scheme is shown by Li *et al.*, in [8] that it lacks user friendliness and fairness in key agreement and suffers from attacks against user anonymity.

ISSN: 1738-9976 IJSIA

Mun *et al.*, [12] also showed that Wu *et al.*,'s scheme [9] disclosed legitimate user's password and failed to achieve perfect forward secrecy and anonymity. Mun *et al.*, [12] proposed an improved version on it. However, Kim *et al.*, [13] found that Mun et al.'s scheme is vulnerable to replay attacks and man-in-the-middle attacks. In order to overcome the security weaknesses, Kim et al. proposed a new anonymous authentication scheme. In this paper, we demonstrated that Kim-Kwak's protocol is susceptible to tractability of the user, impersonation attack and replay attack.

The rest of this paper is organized as follows. Section 2 reviews Kim-Kwak's protocol. Section 3 points out its security weaknesses. The improved scheme and its analysis are presented in Sections 4 and 5, respectively. Finally, we conclude in Section 6.

2. Review of Kim-Kwak's Scheme

In this section, we will briefly review of Kim-Kwak's scheme [13]. Figure 1 illustrates the basic system architecture of mutual authentication and key agreement in wireless and mobile communication systems.

Kim-Kwak's scheme consists of three phases: a registration phase, an authentication and key establishment phase, and an update session key phase. The notations used in the Kim-Kwak's scheme are listed in Table 1. The statement $\{A \rightarrow B: \{M\}\}$ denotes that A sends message M to B.

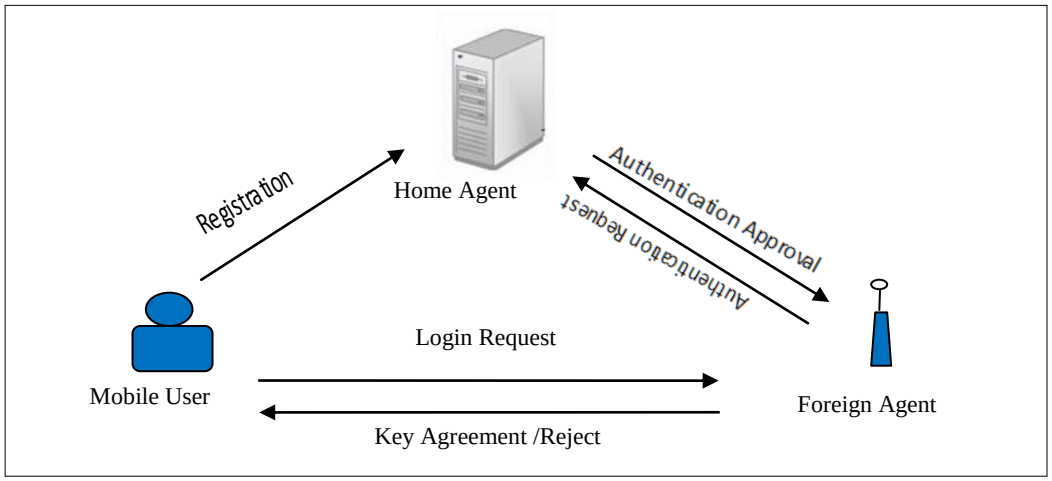


Figure 1. System Architecture

Table 1. Notations

Notations	Descriptions	Notations	Descriptions
MU	Mobile User	$h(.)$	A secure one-way hash function
FA	Foreign Agent	N/N'	Random nonce
HA	Home Agent	y	Random nonce generated by each mobile user
ID_X	Identity of an entity X	SE_K	Dymmetric Encryption using key K
x	Secret key of home agent	SD_K	Symmetric Decryption using key K
PW	Password of MU	E_K	Asymmetric Encryption using key K
$\oplus$	Exclusive- or operation	D_K	Symmetric Decryption using key K
$\|\|$	String concatenation	f_K	MAC generation function by using the key K

2.1. Registration Phase

When a new *MU* wants to register with the Home Agent *HA*, he/she performs the following steps through a secure channel:

Step 1. *MU*→*HA*: $\{ID_{MU}, h(ID_{MU}||PW), h(PW||N)\}$.

MU chooses a random *N* and password *PW*, then computes $h(ID_{MU}||PW)$, $h(PW||N)$. Next, *MU* sends them with ID_{MU} to *HA*.

Step 2. *HA*→*MU*: Smart card.

HA stores $h(IDMU||PW)$ and $h(PW||N)$ in its database after the received $h(IDMU||PW)$ is identified. *HA* computes $V=h(h(ID_{MU}||PW)||h(PW||N))$, $K=h(x||ID_{MU}) \oplus h(PW||N)$ and $B=h(x) \oplus h(y)$. *HA* then issues a smart card containing $\{ID_{MU}, ID_{HA}, B, K, V, y, h()\}$ to *MU*.

Step 3. *MU* puts *N* into the smart card.

2.2. Authentication and Key Establishment Phase

Step 1. *MU* inserts his/her smart card into the device and inputs identity *IDMU* and password *PW*. Next, the card generates a random nonce *N*' and computes

$$h(x) = B \oplus h(y), c_1 = K \oplus h(PW||N),\ c_2 = h(x) \oplus h(IDMU\ ||PW),$$

$$c_3 = h(x||ID_{MU}) \oplus V, c_4 = K \oplus h(PW||N'),\ c_5 = h(h(PW||N')||\ h(PW||N)).$$

Step 2. *MU*→*FA*: $\{ID_{HA}, c_2, c_3, c_4, c_5\}$.

Step 3. *FA*→*HA*: $\{ID_{FA}, c_2, c_3, c_4, c_5\}$.

Then *FA* stores the received ID_{HA} from *MU* for further communication.

Step 4. After receiving the message from *FA*, *HA* computes $h(IDMU\ ||PW)^* = h(x) \oplus c_2$ and searches its database for $h(PW||N)$ corresponding to $h(IDMU\ ||PW)^*$. Then *HA* computes

$$V' = h(h(ID_{MU}||PW)||\ h(PW||N)),\ h(x||ID_{MU}) = c_3 \oplus V',$$

$$K = h(x||ID_{MU}) \oplus h(PW||N), h(PW||N') = K \oplus c_4,\ c_5' = h(h(PW||N')||\ h(PW||N)).$$

HA checks if $c_5' = c_5$. If they are equal, *HA* authenticates *MU*. *HA* then selects a random number *a* and computes *aP*. Next, *HA* computes

$$c_6 = h(K||h(PW||N')||\ h(PW||N)), c_7 = h(IDFA\ ||h(PW||N')||\ h(PW||N)),\ c_8 = E_V(aP||\ c_7).$$

Step 5. *HA*→ *FA*: { ID_{HA}, ID_{FA}, c_6, c_8, *aP* }.

Step 6. *FA* →*MU*: { ID_{HA}, ID_{FA}, c_6, c_8, *aP* }.

FA checks the format of ID_{HA} and ID_{FA} and stores *aP* before *FA* transfers the message to *MU*.

Step **7.** *MU* checks the format of ID_{HA} and computes $c_6' = h(K||h(PW||N')||\ h(PW||N))$ then checks whether if $c_6' = c_6$. If they are equal, *MU* can authenticate *HA*. Next, *MU* decrypts $E_V(aP||c_7)$ and obtains c_7. *MU* computes $c_7' = h(IDFA||h(PW||N')||\ h(PW||N))$ and checks if $c_7' = c_7$. If they are equal, *MU* authenticates *FA*. *MU* then selects a random number *b* and computes *bP*, $K_{MF} = h(abP)$, and $S_{MF} = fK_{MF}(ID_{FA}\ ||bP)$.

Step 8. *MU*→*FA*: $\{bP, S_{MF}\}$.

Step 9. *FA* computes $K_{MF} = h(abP)$ and $S_{MF}' = fK_{MF}(ID_{FA} \| bP)$, and checks whether $S_{MF}' = S_{MF}$. If they are not equal, the procedure is terminated. Otherwise, *FA* authenticates *MU*.

2.3. Update Session Key Phase

Step 1. $MU \rightarrow FA$: $\{b_iP\}$.

MU selects a random number b_i (i=1,2,…,n) and computes b_iP. *MU* then sends b_iP and to *FA*.

Step 2. $FA \rightarrow MU$: $\{a_iP, S_{MFi}\}$.

FA selects a random number a_i(i=1,2,…,n) and computes

$$a_iP, K_{MFi} = h(a_ib_iP), S_{MFi} = fK_{MFi}(a_ib_i \| a_{i-1}b_{i-1}P).$$

FA then sends $\{a_iP, S_{MFi}\}$ to *MU*.

Step 3. *MU* computes a session key $K_{MFi} = h(a_ib_iP)$ and $S_{MFi}' = fK_{MFi}(a_ib_i \| a_{i-1}b_{i-1}P)$. *MU* then checks whether $S_{MFi}' = S_{MFi}$. If they are equal, *MU* and *FA* use the new session key K_{MFi}.

3. Security Analysis of Kim-Kwak's Scheme

Next, we demonstrate that Kim-Kwak's scheme suffers from several deficiencies.

3.1. Unfairness in Key Agreement

A key agreement protocol is called *fair* only when the agreed session key is determined by the cooperation of each involved entity. That is, no one can control the session key. We find that Kim-Kwak's scheme is not really a fair key agreement scheme. During the authentication and key establishment phase, *HA* selects a random number *a* and computes *aP* in **Step 4**, while *MU* selects a random number *b* and computes *bP* in **Step 7**. The session key is computed by the *FA* and *MU* according to $K_{MF}=h(abP)$. Obivously, *FA* has not taken participant in choosing the parameters related to the session key.

3.2. Flaws in Design

Firstly, the registration message $\{h(ID_{MU}||PW), h(PW||N)\}$ of each user is kept in the *HA*, which makes the protocol susceptible to the stolen-verifier-attacks. Next, when the user's password is expired or leaked and the user *MU* would like to update his/her password, the *MU* must ask the *HA* to update the database. Because $\{h(ID_{MU}||PW), h(PW||N)\}$ must be kept in the database of *HA*. It is very inconvienent for both the *MU* and the *HA*.

Secondly, during the authentication and key establishment phase, the two random numbers *a* and *b* are chosen by *HA* and *MU*, respectively. Thus, *FA* does not know *a*. Upon the assumption of CDH, it is infeasible for *FA* to compute *abP* without knowledge of *a* or *b* from *aP* and *bP*. Therefore, *FA* cannot calculate the session key $K_{MF} = h(abP)$. This is a serious flaw of design.

3.3. Replay Attack

Kim *et al.*, claimed that their scheme could resist against replay attack. However, we found that an attacker could mount replay attack. Suppose that an attacker has eavesdropped the message $\{ID_{HA}, c_2, c_3, c_4, c_5\}$ transmitted from *MU* to *FA* during the authentication and key

establishment phase. The attacker can impersonate *MU* to participant in the authentication and key establishment phase as follows:

Step 1. When the attacker accesses an *FA*, the attacker sends $\{ID_{HA}, c_2, c_3, c_4, c_5\}$ to *FA*. After receiving this message, *FA* transfers $\{ID_{FA}, c_2, c_3, c_4, c_5\}$ to *HA* as in the real protocol.

Step 2. *HA* computes and checks whether $c_5' = c_5$. In essence, the above equation holds. Next, *HA* selects a random number *a* and computes aP, c_6, c_7, c_8. Finally, *HA* sends $\{ ID_{HA}, ID_{FA}, c_6, c_8, aP \}$ to *FA* who next tranfers it to *MU*.

Step 3. The attacker selects a random number *b* and computes bP, $K_{MF} = h(abP)$, and $S_{MF} = fK_{MF}(ID_{FA} || bP)$.

3.4. Impersonation Attack

Any attacker can impersonate *MU* to update session keys (even if the attacker has not mounted the above replay attacks). The *update session key* phase in Kim-Kwak's scheme, has no mutual authentication mechanism. Only the user can authenticate *FA*. Thus the attacker can select freely a random number b_i (i=1,2,…,n) and compute b_iP. The attacker then sends b_iP to *FA*. Therefore the attacker computes a session key $K_{MFi} = h(a_ib_iP)$ using the received a_iP from *FA*.

Similarly, Kim et al.'s scheme [12] suffers from such impersonation attacks in the *update session key* phase.

3.5. Attacks Against The User's Anonymity

In wireless environments, an attacker can intercept the communication channel between *MU* and *FA*. Consider that *MU* roams into a foreign network and sends the login message $\{ID_{HA}, c_2, c_3, c_4, c_5\}$ to *FA*. Since $c_2 = h(x) \oplus h(IDMU || PW)$ and $c_3 = h(x||ID_{MU}) \oplus V$, the message $\{ID_{HA}, c_2, c_3\}$ is for the user *MU*'s exclusive use and is unchanged for any access to any foreign agent. The attacker could easily trace the user by checking if $\{ID_{HA}, c_2, c_3\}$ is the same. Thus, user anonymity is not well protected even though the user's identity is not revealed.

4. The proposed Scheme

The notations of the proposed scheme are the same as those in Kim-Kwak's scheme. *HA* chooses the public parameters: a finite field F_q over a large prime q and an elliptic curve group with an order n point P over the curve. *HA* selects x in F_q as the master key and computes the public key $P_{HA}=xP$. *FA* selects y in F_q as the private key and computes the public key $P_{FA}=yP$.

4.1. Registration Phase

Step R1. $MU \rightarrow HA$: $\{ID_{MU}, h(h(ID_{MU} \oplus N) \oplus PW)\}$.

MU chooses a random N and password PW, then computes $h(h(ID_{MU} \oplus N) \oplus PW)$.

Step R2. *HA* chooses a random Z and computes $V = h(x||ID_{HA}||ID_{MU}) \oplus h(h(ID_{MU} \oplus N) \oplus PW)$, $R = h(x||ID_{HA}) \oplus SE_x(ID_{MU}||Z)$. *HA* then issues a smart card containing $\{V, R, h()\}$ to *MU*.

Step R3. *MU* puts N into the smart card.

4.2. Login Phase

Step L1. *MU* inserts the smart card into the card reader and keys ID_{MU} and PW. Then the smart card computes $C=V \oplus h(h(ID_{MU} \oplus N) \oplus PW)$. The card randomly chooses $a \in F_q$, N_1 and computes $A=aP$, $e_1 = E_{P_{HA}}(R||C||ID_{FA}||A||T_{MU}||ID_{HA}||N_1)$ where T_{MU} is the time stamp.

Step L2. $MU \rightarrow FA$: $\{ID_{HA}, A, e_1\}$.

4.3. Authentication Phase

Step A1. $FA \rightarrow HA$: $\{ID_{FA}, e_2\}$.

FA chooses a random number $b \in F_q$ and computes $B=bP$, $F=yP_{HA}$,$e_2= SE_F(B||T_{FA}||e_1)$.

Step A2. *HA* computes $F=xP_{FA}$ and decrypts e_2. *HA* first checks if T_{FA} is valid. Next, *HA* decrypts e_1 and obtains $R||C||ID_{FA}||A||T_{MU}||ID_{HA}||N_1$. *HA* checks if T_{MU} is valid and the extracted ID_{FA} and ID_{HA} equals to the received ID_{FA} and its identitiy, respectively. If they are right, *HA* computes $SD_x(R \oplus h(x||ID_{HA}))$ and gets $ID_{MU}||Z$. Finally, *HA* checks if $h(x||ID_{HA}||ID_{MU})=C$.

Step A3. $HA \rightarrow FA$: $\{ID_{HA}, e_4\}$.

HA computes $L=xA \oplus C$ and $e_3=SE_L(A||ID_{HA}||B||N_1)$. Then *HA* encrypts $e_3||ID_{HA}||T_{HA}||(A \oplus B)$ with F and generates e_4.

Step A4. $FA \rightarrow MU$: $\{e_3\}$.

FA decrpts e_4 with the shared F and checkes if T_{HA} is valid and the extracted ID_{HA}, $A \oplus B$ equals to the received ID_{HA}, $A \oplus B$. *FA* sends e_3 to *MU* and computes the session key $K = h(bA)$.

Step A5. *MU* (in fact, the smart card) computes $L=aP_{HA} \oplus V \oplus h(h(ID_{MU} \oplus N) \oplus PW)$ and decrpts e_3 with L. *MU* parses the plaintext into $A||ID_{HA}||B||N_1$. Then, *MU* checks if $\{A,ID_{HA},N_1\}$ is right. If it is right, *MU* computes the session key $K = h(aB)$.

4.4. Password Change Phase

Step P1. If *MU* wants to change password, *MU* inserts his smart card into the card reader and keys ID_{MU} and PW. Afterwards, the smart card asks the user if *MU* changes the password. If *MU* resubmits a new password PW_{new} and a new random N_{new}, the smart card computes

$$V_{\text{new}} = V \oplus h(h(ID_{MU} \oplus N) \oplus PW) \oplus h(h(ID_{MU} \oplus N_{\text{new}}) \oplus PW_{\text{new}}).$$

Step P2. The smart card replaces $\{V, N\}$ with $\{V_{\text{new}}, N_{\text{new}}\}$.

5. Analysis

In this section, we analyze the security propertities and performance of the proposed privacy-preserving authentication and key agreement protocol.

5.1. Security Analysis

Prevent password guessing attacks: Of all the message $\{ID_{HA}, A, e_1\}$ transmitted over the public channel between *MU* and *FA*, only e_1 contains *C* which derives from $V \oplus h(h(ID_{MU} \oplus N) \oplus PW)$, and *A* is not related to password. Since *C* is encrypted with the public key of *HA*, only *HA* can recover it. Thus the undetectable on-line password guessing attack will not work. In essence, *HA* cannot obtain *PW* even in registration phase since *MU* sends $h(h(ID_{MU} \oplus N) \oplus PW)$ but *PW* to *HA*. Moreover, the off-line password guessing attacks will also fail in our proposed scheme. As shown in the registration phase, the password is protected in the smart card as $h(x||ID_{HA}||ID_{MU}) \oplus h(h(ID_{MU} \oplus N) \oplus PW)$. Therefore, without key *x* or ID_i, any adversary is unable to obtain a verification function about the password from the stolen card or the message transmitted over the public channel. The proposed scheme can resist password guessing attacks.

Resist against replay attack: For each run of the proposed scheme, several nonces $\{A,B,N_1\}$ and time stamps $\{T_{MU},T_{FA},T_{HA}\}$ are used to verify freshness of every message. Thus, an attacker cannot replay the message. Therefore, the proposed scheme can resist replay attacks.

Achieve anonymity: In Step L2 of our scheme, *FA* receives $\{ID_{HA}, A, e_1\}$. e_1 includes *R* and *C* which contains ID_M as $C=h(x||ID_{HA}||ID_{MU})$ and $R=h(x||ID_{HA}) \oplus SE_x(ID_{MU}||Z)$. Thus, *FA* has no way of knowing ID_{MU} without the private key *x* of *HA*. Moreover, since *A* and e_1 depend on two random numbers *a*, N_1 and the login time T_{MU}, the login message $\{ID_{HA}, A, e_1\}$ is different from each other. Thus, any attacker who controls the communication channel cannot still trace dowm the user by comparing *A* or e_1 in our proposed login scheme even if any attacker has intercepted all the transmitted message between *FA* and *MU*. Therefore, the user's anonymity is well protected.

Table 2. Comparison Regarding Security Properties

	Ours	[8]	[6]	[7]	[9]	[12]	[13]
Anonymity	Yes	Yes	Yes	No	No	Yes	No
Perfect forward security	Yes	Yes	Yes	No	No	Yes	Yes
Mutual authentication	Yes	Yes	Yes	No	No	No	No
Against replay attacks	Yes	Yes	Yes	Yes	No	No	No
Against impersonation attacks	Yes	Yes	Yes	No	No	No	No
Fairness in key agreement	Yes	Yes	No	No	No	Yes	No

Table 3. Comparison Regarding Performance

	Li et al.'s Scheme			Our Scheme		
	MU	*FA*	*HA*	*MU*	*FA*	*HA*
Random number generation	1	1	1	2	1	0
Module exponentiation	1+3 Pre	3+2 Pre	2+1 Pre	N/A	N/A	N/A
Point multiplication	N/A	N/A	N/A	2+1 Pre	2+1 Pre	1+1 Pre
Hash operations	3	2	5	3	1	1
Symmetric encryption/decryption	4	4	5	1	2	2
Asymmetric encryption/decryption	N/A	N/A	N/A	1	N/A	2
Signature generation/verification	N/A	2	2	N/A	N/A	N/A

Provide mutual authentication between MU and FA: *MU* authenticates *FA* by verifying {*A*, ID_{HA}, N_1} in Step A5. Although *FA* received e_1 which contains the nounce N_1 in Step L2, *FA* cannot still recover it from its ciphertext e_1 without knowledge of the secret key *x* of *HA*. Similarily, since the decryption key *L* is shared by *HA* and *MU*, *FA* cannot recover N_1 from e_3. Thus, *MU* authenticates the *HA*, further *FA*. Conversely, *FA* decrpts e_4 with the shared key *F* and checks if T_{HA} is valid and the extracted ID_{HA}, $A \oplus B$ equals to the received ID_{HA}, $A \oplus B$, respectively. Since *B* is transmitted over the open channel only in the ciphtertext form, thus when *FA* obtains $A \oplus B$ by decrpting e_4, *FA* authenticates the *HA*, further *MU*. The mechnism can aslo prevent it from man-in-the-middle attacks.

Provide perfect forward secrecy: If an adversary has *HA*'s master keys *x*, the adversary can recover {*A*, *B*}. However, it is infeasible to work out *aB* or *bA* from {*A*, *B*} on the assumption of computational Diffie-Hellman. Thus, the adversary cannot compute the session key by the formula $K = h(aB)$ or $h(bA)$.

Provide fairness in key agreement: The session key is determined by {*A*, *B*} which is chosen by *MU* and *FA*. So, *MU* and *FA* can share a session key. Even *HA* cannot work it out. It is important. But in Xu et al.'s schem [6], *HA* can obtain the session key of *MU* and *FA*.

5.2. Performance Analysis

Of the schemes [6-9, 12, 13], Li *et al.*,'s scheme [8] achieves all the security requirements. For performance analysis, we compare the computation cost of our scheme and Li et al.'s scheme.

6. Conclusion

In this paper, we discussed Kim-Kwak's scheme and showed that their protocol is susceptible to tractability of the user, impersonation attack and replay attack. Moreover, it cannot provide fairness in key agreement. There is a serious flaw of design which will not make *FA* to obtain session key. We proposed an enhanced scheme which removes these security flaws. We also demonstrate that our scheme has more security properties and hold high performance compared with the previous scheme.

Acknowledgements

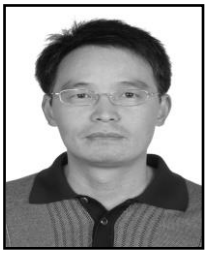
This work is supported by the National Natural Science Foundation of China under Grant No.61163053, Natural Science Foundation of Jiangxi Province (20122BAB201035),the Open Project Program of Key Laboratory of Mathematics and Interdisciplinary Sciences of Guangdong Higher Education Institutes, Guangzhou University (No. 2012-02-02-01) and Foundation of Jiangxi Educational Committee under Grant GJJ13301.

References

[1] M. Kim, J. Nam and D. Won, "An improved secure dynamic ID-based remote user authentication scheme with key agreement using symmetric cryptology," International Journal of Security and Its Applications, vol. 7, no. 3, **(2013)**, pp. 143-152.
[2] J. Nam, K.-K. Raymond Choo, J. Paik and D. Won, "Cryptanalysis of server-aided password-based authenticated key exchange protocols", International Journal of Security and Its Applications, vol. 7, no. 2, **(2013)**, pp. 47-58.
[3] Y. An and Y. Joo, "Security analysis and improvements of a password-based mutual authentication scheme with session key agreement", International Journal of Security and Its Applications, vol. 7, no. 1, **(2013)**, pp. 85-94.

[4] C.-T. Li, C.-Y. Weng, C.-C. Lee and C.-W. Lee, "Towards secure and dynamic password based user authentication scheme in hierarchical wireless sensor networks," International Journal of Security and Its Applications, vol. 7, no. 3, **(2013)**, pp. 249-258.
[5] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," IEEE Transactions on Consumer Electronics, vol. 51, no. 1, **(2004)**, pp. 230-234.
[6] 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, **(2012)**, pp. 319-325.
[7] D. He, M. Ma, Y. Zhang, C. Chen and J. J. Bu, "A strong user authentication scheme with smart cards for wireless communications", Computer Communications, vol. 33, **(2011)**, pp. 367-374.
[8] C. T. Li and C. C. Lee, "A novel user authentication and privacy preserving scheme with smart card for wireless communications", Mathematical and Computer Modelling, vol. 55, **(2012)**, pp. 35-44.
[9] C. C. Wu, W. B. Lee and W. J. Tsaur, "A secure authentication scheme with anonymity for wireless communications", IEEE Communication Letters, vol. 12, no. 10, **(2008)**, pp. 722-723.
[10] C. C. Lee, M. S. Hwang and D. H. Liao, "Security enhanced on a new authentication scheme with anonymity for wireless environments", IEEE Transactions on Industrial Electronics, vol. 53, no. 5, **(2006)**, pp. 1683-1686.
[11] C. C. Chang, C. Y. Lee and Y. C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global networks", Computer Communications, vol. 34, no. 4, **(2009)**, pp. 611.
[12] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun and H. H. Choi., "Enhanced secure anonymous authentication scheme for roaming service in global mobility networks", Mathematical and Computer Modelling, vol. 55, **(2012)**, pp. 214-222.
[13] J.-S. Kim and J. Kwak, "Improved secure anonymous authentication scheme for roaming service in global mobility networks", International Journal of Security and Its Applications, vol. 6, no. 3, **(2012)**, pp. 45-54.

Author



Zuowen Tan received his M.S. degree in Mathematics from Xiangtan University, China in 2002. He received his Ph.D. degree in Mathematics from Institute of Systems Science, Academy of Mathematics and System Science, CAS in 2005. Since 2011, he has been a professor at Department of Computer Science & Technology, School of Information Technology, Jiangxi University of Finance & Economics, China. His research interests include information security and cryptography.