ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, *25-27 June*, *2017*, *pp. 961-967*
doi: 10.18178/wcse.2017.06.167

Lightweight Authenticated Key Agreement Scheme with Smart Cards for Wireless Mobile Networks

Cheng Guo [1] and Chin-Yu Sun [2 +]

[1] School of Software, Dalian University of Technology, Dalian, Liaoning, 116620 China
[2] Department of Computer Science, National Tsing-Hua University, Hsinchu, Taiwan, 30013, R.O.C.

Abstract. With the rapid development of Internet technology, wireless communication and mobile networks have made our lives more convenient. However, they have also brought a lot of security issues. Because attackers can intercept and eavesdrop on messages which are transmitted through in wireless networks, the privacy and security of wireless communication and mobile networks have become a concern. In this paper, a novel authentication and key agreement scheme for wireless mobile systems is proposed. Most authentication and key agreement protocols for wireless communication need to utilize symmetric/asymmetric encryptions or decryptions to protect their protocols. Compared with related works, our proposed scheme only uses hash functions and XOR operations. For this reason, our proposed scheme significantly improves efficiency. The security and performance analysis shows that our proposed scheme can also achieve acceptable security and functionality requirements.

Keywords: wireless communication, authentication, key agreement, lightweight, smart card.

1. Introduction

There are many wireless applications. Wireless network technology includes Bluetooth for personal areas, wireless LANs (WLANs) for local areas, Universal Mobile Telecommunication (UTM) for wide areas, and satellite networks for the global network. Because wireless signals exist in a public space, attackers can easily intercept or eavesdrop on messages in order to obtain privacy information. Therefore, many researchers have designed security protocols to resist attacks or overcome other protocols' weaknesses. In addition, due to the hardware device limits, they also develop high efficient systems to limit power consumption.

In 1981, Lamport [10] was the first to propose a user password authentication scheme, which used a secure hash function to produce a one-time password for verifying user identity. In 1994, Aziz and Diffie [1] designed a privacy authentication scheme for wireless networks which used a random nonce and a user's certificate to protect security. In 1997, Park [13] focused on mutual authentication and proposed a session key exchange protocol based on certificates for the wireless mobile system. In 2004, Zhu and Ma [18] proposed a new authentication scheme with anonymity for wireless networks using a smart card to increase the security of the protocol. In their scheme, mobile users only need to perform symmetric encryptions/ decryptions to reduce the computational cost. In 2006, Lee et al. [8] pointed out that Zhu-Ma's scheme cannot achieve perfect backward secrecy, mutual authentication and cannot protect against a forgery attack; thus, they proposed an improvement to overcome the weaknesses. In 2011, Xu et al. [17] found that Lee et al.'s scheme still had some security weaknesses (i.e., non-anonymity, unfair key agreement, and the inapplicable security design), so they proposed a new authentication scheme with anonymity for wireless networks. Due to new security requirements and new security problems, the security of wireless mobile networks has received increasing interest in recent years [2, 4, 5, 7, 9, 11, 15]. In this paper, we propose a

+ Corresponding author. Tel.: +886-7-3427581.
E-mail address: sun.chin.yu@gmail.com.

novel password-based authentication scheme with smart cards in wireless mobile networks, without asymmetric and symmetric encryption/decryption. It is more suitable for use in wireless network communication and mobile network transmission, because it uses only hash functions and XOR operations to exchange messages among the mobile user, the foreign agent, and the home agent. The proposed scheme can also resist many security attacks, like non-anonymity, stolen smart card attack, replay attack and man-in-the-middle attack. We also propose the login phase for verifying the user's identity and the update password phase for making our protocol user-friendly. The remainder of this paper is organized as follows. Our proposed scheme is shown in Section 2. We analyze our scheme regarding security in Section 3. In Section 4, we discuss our proposed scheme's performance and computation cost. Finally, we make some conclusions in Section 5.

2. Proposed Scheme

In this section, we propose an authentication scheme with smart cards for roaming service in wireless communication. Our scheme is divided into three phases: 1) registration phase, 2) login and authentication phase, and 3) update password phase. In the registration phase, a new mobile user (*MU*) who wants to roam the wireless network must first register with the home agent (*HA*). Then, *HA* will give him some secret parameters which are stored in the smart card, and *MU* can use his own smart card to login the home agent by foreign agent's (*FA*) help. In the authentication phase, *HA* can verify whether *MU* is authorized, and a session key can be created between *MU* and *FA.* In the update password phase, the user can update her/his password for user-friendly. Registration phase

2.1. Registration phase

A new mobile user has to execute the registration phase when she/he wants to roam the wireless network through a foreign agent and the home agent. In this phase, the home agent and the user use some secret parameters to coordinate a smart card. The details are described as following steps, and all parameters are transferred in the secure channel in this phase. ***Step1.*** *MU* selects a random number b and computes with her/his password PW_{MU}, such as $A = h(PW_{MU}||b)$. ***Step2.*** *MU* sends A and his identity ID_{MU} to *HA*. ***Step3.*** Then *HA* generates two random numbers x and y and computes as follows: $Z = h(ID_{MU}||h_k(x))$, $B = h(ID_{HA}||h_{\mathrm{k}}(x)) \oplus h(ID_{HA}||h_{\mathrm{k}}(y)) \oplus \mathrm{Z} \oplus \mathrm{A}$, $C = h(ID_{HA}||h_k(x)) \oplus Z$, $D = h(ID_{HA}||h_k(y)) \oplus Z$, and $Q = A \oplus Z$. ***Step4.*** *HA* stores $Q, B, C, D, h(.), x$ and y into the smart card and sends it to *MU*. ***Step5.*** *MU* stores his own secret random number b into the smart card. Here, $h_k(.)$ means that a keyed one-way hash function using the key k [3].

2.2. Login and authentication phase

After *MU* registers as a legal user to the *HA*, she or he can get a smart card for logging in. *MU* needs to key his/her PW_{MU} to proof he or she is the smart card owner. Then, it starts to run authentication phase, achieves mutual authentication, and establishes the session key between *FA* and *HA*. In this phase, we assume that $h_k(ID_{FA}||w)$ and w are already shared between *FA* and *HA*. ***Step1.*** First, *MU* enters his/her password and computes with b, such as $A = h(PW_{MU}||b)$, and then uses A to compute with Q, such as $Z = A \oplus Q$. The smart card checks whether $Z \oplus C \oplus D \oplus A$ equals to B or not, to verify the smart card owner. ***Step2.*** Then, *MU* generates a random number N_1 , and computes $E = N_1 \oplus C \oplus Z$ and $F = h(E||C \oplus Z)$. ***Step3.*** *MU* sends E, F, x and y to *FA*. ***Step4.*** After *FA* receives E, F, x and y from *FA*, *FA* generates a random number N_2, and computes $G = N_2 \oplus h_k(ID_{FA}||w)$ and $H = F \oplus h(G||h_k(ID_{FA}||w))$. ***Step5.*** *FA* sends E, G, H, w, x and y to *HA*. ***Step6.*** When *HA* receives those parameters, *HA* starts to compute whether $h(E||h(ID_{HA}||h_k(x)) \oplus h(G||h_k(ID_{FA}||w)? = H$ is equal or not, to verify receive message, then *HA* uses the received x, w and the key k to compute $h_k(ID_{FA}||w)$ to obtain N_1 by computing $E \oplus h(ID_{HA}||h_k(x))$, and obtains N_2 by computing $G \oplus h_k(ID_{FA}||w)$. And *HA* also computes $I = N_1 \oplus h_k(ID_{FA}||w)$, $K = N_2 \oplus h(ID_{HA}||h_k(y))$ and $L = h(h(N_1 \oplus N_2) \oplus h(I||K))$. ***Step7.*** *HA* sends I, K and L to *FA*. ***Step8.*** After *FA* receives I, K and L, *FA* gets N_1 by computing $I \oplus h_k(ID_{FA}||w)$. Then, *FA* uses N_1 to compute $h\big(h(N_1 \oplus N_2) \oplus h(I||K)\big)$ is equal to L or not. If so, then *FA* verifies *HA*, if it is not equal, the procedure is determined. The session key is created by computing $h(N_1 \oplus N_2) \oplus h(I||K)$. ***Step9.*** *FA* sends I, K and L to *MU*. ***Step10.*** When *MU* receives I, K and L, *MU* computes $K \oplus h(ID_{HA}||h_k(y))$ to

obtain N_2. Then, MU determines whether $h\big(h(N_1 \oplus N_2) \oplus h(I||K)\big)$ is equal to L, in order to verify the received I, K, and L and then computes $h(N_1 \oplus N_2) \oplus h(I||K)$ as the session key between FA and MU.

2.3. Update password phase

In a user-friendly system, it is essential for a user to change their password for security and make it easy to remember. In our scheme, we proposed the update password phase as a user-friendly authentication scheme. The details are described as follows: ***Step1.*** First, MU enters his/her PW_{MU}. ***Step2.*** Then, the smart card computes $A = h(PW_{MU}||b)$ and $Z = A \oplus Q$. ***Step3.*** The smart card determines whether $Z \oplus C \oplus D \oplus A \,?= B$, in order to verify the smart card owner. ***Step4.*** After verifying the smart card owner, MU can enter the new password PW_{MU_NEW}. ***Step5.*** Then, the smart card computes $A' = h(PW_{MU\_NEW}||b)$ and $B' = B \oplus A \oplus A'$. ***Step6.*** Finally, the new B' is used to replace the old B stored in the smart card.

3. Security Analysis

In this section, we use attack scenarios to show that our proposed scheme can resist potential attacks. Assume that there is an attacker, Eve, who has the ability to intercept and eavesdrop on the public message transmitted between the user, the foreign agent, and home agent. We show our security analyses in the following sections.

3.1. Our proposed scheme resists the smart card loss case

Here, we assume that, Eve, has the ability to extract the secret parameters Q, B, C, D, $h(.)$, x, y, and b, from the smart card and tries to use the secret parameters to pass the verification of the smart card or verification of the home agent. She may try to use those parameters to compute the following 11 equations:
1) $Q \oplus B = h(ID_{HA}||h_k(x)) \oplus h(ID_{HA}||h_k(y))$, 2) $Q \oplus C = A \oplus h(ID_{HA}||h_k(x))$
3) $Q \oplus D = A \oplus h(ID_{HA}||h_k(y))$, 4) $B \oplus C = h(ID_{HA}||h_k(y)) \oplus A$
5) $B \oplus D = h(ID_{HA}||h_k(x)) \oplus A$, 6) $C \oplus D = h(ID_{HA}||h_k(x)) \oplus h(ID_{HA}||h_k(x))$
7) $Q \oplus B \oplus C = h(ID_{HA}||h_k(y)) \oplus Z$, 8) $Q \oplus B \oplus D = h(ID_{HA}||h_k(x)) \oplus Z$
9) $Q \oplus C \oplus D = A \oplus h(ID_{HA}||h_k(x)) \oplus h(ID_{HA}||h_k(y)) \oplus Z$
10) $B \oplus C \oplus D = A \oplus Z$, and 11) $Q \oplus B \oplus C \oplus D = 0$

Apparently, Eve cannot obtain user privacy parameter $A = h(PW_{MU}||b)$ because she does not have the correct key k. Without the key k, Eve cannot compute the correct $h(ID_{HA}||h_k(x))$, $h(ID_{HA}||h_k(y))$ and $Z = h(ID_{MU}||h_k(x))$ by himself to extract parameter A from the above equations. In other words, even if the attacker holds all the parameters Q, B, C, D, $h(.)$, x, y, and b, she still cannot obtain any information. Accordingly, our proposed scheme can resist the smart card loss case.

3.2. Replay attack

Here, we assume that Eve tries to intercept the transmitted messages E, F, x and y in Step 3 of the authentication phase and resend it to the home agent in order to obtain the session key between the user and the foreign agent. When the home agent sends back the response messages I, K, and L to Eve, she cannot extract the random nonce N_2 created by the foreign agent, because Eve does not have the correct $h(ID_{HA}||h_k(y))$ to compute $K \oplus h(ID_{HA}||h_k(y))$ in order to extract the random nonce N_2. Even if Eve holds the messages E, F, x and y, she still cannot obtain the random nonce N_1, because she does not have the correct $C \oplus Z$ to extract N_1 from message E. Without the random nonces N_1 and N_2, Eve cannot create the session key between the user and the foreign agent. In other words, even if an attacker intercepts and resends any transmitted message in our scheme, she or he still cannot obtain the correct session key. In addition, there is shared key $h_k(\,ID_{FA}||w)$ and w between the foreign agent and the home agent. Assume that Eve intercepts the transmitted messages E, G, H, w, x, and y in Step 5 of authentication phase and resends it to the home agent. When the home agent sends back the response messages I, K, and L to Eve, she still cannot extract the random nonces N_1 and N_2, because she does not have the correct shared key. Thus, our proposed scheme can resist the replay attack.

3.3. Man-in-the-middle attack

Here, we assume that Eve intercepts and modifies the messages between the user and the foreign agent in Steps 3 and 5 of the login and authentication phase. We divide these steps into two separate cases for analysis. ***Case 1*:** Assume that Eve intercepts the messages E, F, x and y in Step3 of the login and authentication phase, where $E = N_1 \oplus h(ID_{HA}||h_k(x))$ and $F = h(E||h(ID_{HA}||h_k(x)))$. She may try to modify them and send the fake messages E′, F′, x' and y' to the home agent for verification. However, she will not success, because she does not have the secret key k to generate the correct parameter $h_k(x')$ and E'. When the home agent computes and verifies $h(E'||h(ID_{HA}||h_k(x')) \oplus h(G'||h_k(ID_{FA}||w))$, it will not equal H′, so the home agent can terminate the procedure immediately. Assume that Eve somehow obtains the correct $h_k(x')$ to generate E'', F'', x'' and y'', where $E'' = N_1 \oplus h(ID_{HA}||h_k(x'))$ and $F'' = h(E''||h(ID_{HA}||h_k(x')))$. The home agent sends the response messages I'', $K''$and L'' back to the original user MU, where $I'' = N_1 \oplus h_k(ID_{FA}||w')$, $K'' = N_2{}' \oplus h(ID_{HA}||h_k(y'))$ and $L'' = h\big(h(N_1{}' \oplus N_2{}') \oplus h(I'||K')\big)$. When MU finds that $h(ID_{HA}||h_k(y'))$ is not equal to $h(ID_{HA}||h_k(y))$, MU will terminate the procedure immediately. ***Case 2*:** Now, assume that Eve changes his target to Step 5 of the login and authentication phase and intercepts messages E, G, H, w, x. Unfortunately, she cannot generate the correct messages without the key k by himself. In other words, Eve cannot use the fake w'', x'' and y'' to compute $E''' = N_1 \oplus h(ID_{HA}||h_k(x''))$, $G'' = N_2 \oplus h_k(ID_{FA}||w'')$. For this reason, when the home agent checks $h(ID_{HA}||h_k(x''))$ and $h_k(ID_{FA}||w'')$, she will find that $h_k(x'')$ and $h_k(ID_{FA}||w'')$ do not hold, and then terminate the procedure. Thus, the proposed scheme can resist the man-in-the-middle attack.

3.4. Impersonation attack

Regarding the impersonation attack, Eve may impersonate MU, FA, and HA. The details of each case are described below. ***Case 1*:** (Impersonate MU) Assume that Eve wants to impersonate a legal user MU. First, she steals MU's smart card first, and then enters the correct password. However, even if Eve knows all of the parameters stored in the smart card, she still cannot extract the correct password or any personal information (see Section 3.1). Hence, the attacker cannot impersonate the legal user in this way. If Eve wants to skip the login, she may try to intercept messages E, F, x, and y from the legal user MU and compute the fake message E''''. Eve will still fail: she cannot use x''' to generate the $h_k(x''')$, because she does not have the correct key k. When the home agent finds that $h_k(x''')$ is not correct, the home agent terminates this process immediately. In short, without this key k in our scheme, Eve can do nothing. ***Case 2*:** (Impersonate FA) In our proposed scheme, there are several FAs in the wireless network environment. Each FA has his number w; HA uses his key k to compute $h_k(ID_{FA}||w)$ and shares it with FA. Assume that Eve wants to impersonate one FA. When she receives the messages E, F, x, and y from the user MU, she may try to create one random nonce $N_2{}''$ and random number w''', but she cannot compute the correct $h_k(ID_{FA}||w''')$ without HA's key k. Therefore, Eve cannot pass the verification when HA checks $h_k(ID_{FA}||w''')$. When the home agent finds out that it is not correct, it terminates the process. ***Case 3*:** (Impersonate HA) Assume that Eve wants to impersonate HA. Upon receiving the messages $E, G, H, w, x,$ and $y,$ she cannot extract N_1 and N_2 without the key k, even if she creates the fake messages I''', K'''*and* L''' and sends them back to the foreign agent and the user. Without the correct $h_k(ID_{FA}||w)$ and $h(ID_{HA}||h_k(y))$, both the foreign agent and the user cannot extract N_1 and N_2 to create the session key. For this reason, our proposed scheme can resist the impersonation attack.

3.5. Perfect forward secrecy

In the login and authentication phase of our proposed scheme, the session key $SK = h(N_1 \oplus N_2) \oplus h(I||K)$ contains the random nonces N_1 and N_2 and two parameters $I = N_1 \oplus h(ID_{FA}||y)$ and $K = N_2 \oplus h(ID_{HA}||y)$; I and K also contain the random nonces N_1 and N_2. Furthermore, in every new round, because MU and FA change the new random nonce, the session key can also be changed. If Eve somehow obtains the session key, he only can use it in this round. In short, she cannot decrypt the previously transmitted message or the subsequent transmitted message by using this session key.

4. Discussions

In this section, we analyze the performance and computational cost of our proposed scheme. We believe that our proposed scheme achieves mutual authentication, is user-friendly and provides anonymity. We analyze the computational cost of our proposed scheme compared with related works. It is well known that in wireless communication networks and mobile networks system, hardware devices (i.e., wireless sensors and global mobile phones) cannot support heavy computation. The details of the performance and computational cost are in the following sections.

4.1. Mutual authentication

In the login and authentication phase of our proposed scheme, when the user MU needs to connect to HA, MU will first send $E = N_1 \oplus C \oplus Z$, $F = h(E||C \oplus Z)$, x and y to FA. Then, FA will use the received parameters to compute $G = N_2 \oplus h_k(ID_{FA}||w)$. $H = F \oplus h(G||h_k(ID_{FA}||w))$, where H includes E, F and G, so when HA verifies H, it also verifies whether E, F and G are correct or not. After that, HA sends $I = N_1 \oplus h(ID_{FA}||y)$, $K = N_2 \oplus h(ID_{HA}||y)$ and $L = h\big(h(N_1 \oplus N_2) \oplus h(I||K)\big)$ to FA and MU, FA computes $I \oplus h(ID_{FA}||y)$ to extract N_1, then FA will use N_1, N_2, I and K to verify L. MU also computes $K \oplus h(ID_{HA}||y)$ to extract N_2 and then verifies L to make sure that the message is correct or not. Therefore, the user, the foreign agent, and the home agent can verify each other. Thus, our proposed scheme can achieve mutual Authentication.

4.2. User-friendly

The update password phase ensures that our proposed scheme is user-friendly. Users can change their password to update it, or make it easy to remember by executing the update password phase in our scheme.

4.3. Anonymity

In Step 3 of the login and authentication phase of our proposed scheme, MU sends E, F, x, and y to FA, where $E = N_1 \oplus C \oplus Z = N_1 \oplus h(ID_{HA}||h_k(x))$ and $F = h(E||C \oplus Z) = h(E||h(ID_{HA}||h_k(x)))$. Obviously, there is no user identity or information in those transmitted messages. Therefore, even if the attacker somehow gets all of the parameters from the smart card, the attacker cannot perform any attacks with those secret parameters (see Section 3.1).

4.4. Computational cost

We compare the computational cost with other related schemes [6, 8, 12, 16, 18]. Computational cost is an important issue in wireless communication networks and global mobility networks, because the hardware devices limit and heavy computation can exhaust sensor or battery resources. Our proposed scheme is based on the one-hash function, the keyed one-way hash function, and the XOR operations, as shown in Table I (H: One-way hash function, X: XOR operation, Ecc: Elliptic curve addition, Asy: Asymmetric cryptosystem, Sy: Symmetric cryptosystem, Sign: Signature).

TABLE 1: Comparison of computational costs

Primitives	Entities	Ours	[6]	[12]	[18]	[8]	[16]
H	MU	12	10	5	2	4	3
	FA	8	4	4	2	4	5
	HA	24	4	5	5	5	4
X	MU	17	0	2	3	3	1
	FA	7	0	2	1	1	0
	HA	13	0	3	3	3	3
Sy	MU	0	2	1	2	2	1
	FA	0	1	1	1	2	0
	HA	0	2	0	1	1	2
Asy	MU	0	0	0	0	0	0
	FA	0	1	0	2	2	3
	HA	0	1	0	3	2	0
E	MU	0	2	0	0	0	0
	FA	0	2	0	0	0	0
	HA	0	0	0	0	0	0
Sign	MU	0	0	0	0	0	0
	FA	0	2	0	0	0	0
	HA	0	2	0	0	0	0

Shcneier [14] showed that one RSA encryption/decryption is equal to 100 DES encryptions/decryptions and one DES encryption/decryption is equal to 5/3 modular exponentiations. Moreover, in [8], one modular exponentiation is similar to performing eight multiplications and 48 additions over an elliptic curve. In here, RSA is an asymmetric encryption/decryption, and DES is a symmetric encryption/decryption. In our proposed scheme, we use the keyed one-way hash function that Bellare et al. demonstrated [3]. Bellare et al. designed a one-way cryptographic hash function with a key, which means that the key is input as part of the data hashed by the function (i.e., hashing data x using key k is performed by applying the hash function h to concatenation of k and x, such as $h(k||x)$). This is the same as in our proposed scheme's notation $h_k(x)$, where a keyed one-way hash function's computation cost is equal to a one-way hash function.

5. Conclusions

We propose a novel authentication scheme used in wireless communications networks. It can resist most famous attacks, including the replay attack, man-in-the-middle attack, and impersonation attack, and can achieve perfect forward secrecy. Even if an attacker can obtain all parameters in the smart card, she/he still cannot use them to modify our proposed scheme. The scheme is user-friendly, achieves mutual authentication, and anonymity as well as low computational cost. Moreover, it does not use any asymmetric or symmetric encryptions/decryptions. Therefore, our proposed scheme is more efficient for use in wireless networks systems and achieves high security.

6. References

[1] A. Aziz and W. Diffie. Privacy and authentication for wireless local area networks. *IEEE Pers. Commun.* 1994, 1(1): 25-31.

[2] L. Buttyan, C. Gbaguidi, S. Staamann, U. Wilhelm. Extensions to an authentication technique proposed for the globe mobility network. *IEEE Trans. Commun*. 2000, 48(3): 373-376.

[3] M. Bellare, R. Canetti, H. Krawczyk. Keying hash functions for message authentication. *Proc. of Cryptology – Crypto, Lecture Notes in Computer Science*. 1996, pp.1-15.

[4] J. Cao, M. Ma, M. Cao. An enhanced authentication scheme in GLOMONETs. *Proc. of 4th IEEE International Conference on Broadband Network and Multimedia Technology*. 2011, pp.579-585.

[5] D. He and S. Chan. A secure and lightweight user authentication scheme with anonymity for the global mobility network. *Proc. of 13th International Conference on Network-Based Information Systems*. 2010, pp.305-312.

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

[7] K. F. Hwang and C. C. Chang. A self-encryption mechanism for authentication of roaming and teleconference services. *IEEE Trans. Wirel. Commun*. 2003, 2(2): 400-407.

[8] C. C. Lee, M. S. Hwang, I. E. Liao. Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Trans. Ind. Electron*. 2006, 53(5): 1683-1687.

[9] C. Y. Lee, C. C. Chang, C. H. Lin. User authentication with anonymity for global mobility networks. *Proc. of 2nd International Conference on Mobile Applications and Systems*. 2005, pp.1-5.

[10] L. Lamport. Password authentication with insecure communication. *Commun. ACM*. 1981, 24(11): 770-772.

[11] C. T. Li and C. C. Lee. A novel user authentication and privacy preserving scheme with smartcards for wireless communications. *Math. Comput. Modelling*. 2012, 55(1-2): 35-44.

[12] H. Mun, K. Han, Y. S. Lee, Y. Y. Chan, H. H. Choi. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Math. Comput. Modelling*. 2012, 55(1-2): 214-222.

[13] C. S. Park. On certificate-based security protocols for wireless mobile communication systems. *IEEE Netw*. 1997, 11(5): 50-55.

[14] B. Schneier. *Applied cryptography, protocols, algorithms, and source code in C*. John Wiley and Sons Inc., 2nd Edition, 1996.

[15] T. Zhou and J. Xu. Provable secure authentication protocol with anonymity for roaming service in global mobility

networks. *Comp. Netw*. 2011, 55(1): 205-213.

[16] C. C. Wu, W. B. Le, W. J. Tsaur. A secure authentication scheme with anonymity for wireless communication, *IEEE Commun. Lett*. 2008, 12(10): 722-723.

[17] J. Xu and D. Feng. Security flaws in authentication protocols with anonymity for wireless environments. *Electronics and Telecommunications Research Institute*. 2009, 31(4): 460-462.

[18] J. Zhu and J. Ma. A new authentication scheme with anonymity for wireless evironments. *IEEE Trans. Consum. Electron*. 2004, 50(1): 231-235.