A More Robust Authentication Scheme for Roaming Service in Global Mobility Networks Using ECC

Dianli Guo and Fengtong Wen

(Corresponding author: Fengtong Wen)

School of Mathematical Sciences, University of Jinan
No. 106, Jiwei Road, Shizhong District, Jinan 250022, China
(Email: wftwq@163.com)

(Received Aug. 13, 2013; revised and accepted Jan. 14 & Mar. 4, 2015)

Abstract

In 2012, Chuang et al. proposed a smart card based anonymous user authentication scheme for roaming service in global mobility networks. In this paper, however, we analyze Chuang et al.'s scheme and show that their scheme is in fact insecure to against server masquerading attack, off-line dictionary attack and user impersonation attack. Moreover, their scheme cannot achieve the claimed user anonymity once the smart card is compromised. Then, we propose a new robust authentication scheme for the roaming service in global mobility networks using elliptic curve cryptosystem to eliminate these weaknesses. Compared with the existing schemes, our proposed scheme can provide stronger security than previous schemes.

Keywords: Anonymity, authentication, roaming service

1 Introduction

Global mobility networks (GLOMONET) provide the global roaming service that permits mobile users to use the services provided by the home agent in a foreign agent. However, with the rapid development of such environment, many security problems are brought into attention due to the dynamic nature and vulnerable-to-attack structure.

As user privacy becomes a notable security issue in GLOMONET, it is desirable to protect the privacy of mobile users in remote user authentication process [17]. In order to achieve this goal, several authentication schemes [2,3,6,8–10,12–14,16,18,19] with user anonymity have been proposed for roaming service in GLOMONET. Nevertheless, most of the existing schemes were broken shortly after they were proposed.

In 2012, Chuang et al. [4] pointed out some previous authentication schemes for roaming service in GLOMONET could not achieve user anonymity. In order to remedy this flaw, Chuang et al. proposed a new authentication scheme with user anonymity for roaming service in GLOMONET.

In this paper, we analyze Chuang et al.'s scheme and show that their anonymous user authentication scheme is vulnerable to server masquerading attack, off-line dictionary attack, user impersonation attack, besides, it also cannot preserve user anonymity under the non-tamper resistance assumption of smart cards. Furthermore, we propose a more robust authentication scheme for roaming service in global mobility networks using elliptic curve cryptosystem, which can successfully prevent different kinds of network attacks.

This paper is organized as follows. In Section 2, we briefly review Chuang et al.'s scheme. We show its weaknesses in Section 3. Then, we propose a new robust authentication scheme in Section 4. In Section 5, we analyze the security of our proposal. In Section 6, we compare the performance of our new protocol with the previous schemes. Section 7 concludes the paper.

2 Review of Chuang et al.'s Scheme

Chuang et al.'s anonymous authentication scheme comprises three phases, namely registration phase, mutual authentication and key agreement phase and password changing phase. Each foreign agent F shares a secret key K_{FH} with the home agent H. The abbreviations and notations used in their scheme are listed in Table 1.

2.1 Registration Phase

Step 1. M freely chooses ID_M and PW_M, then sends them to H through a secure channel.

Table 1: Notations

M	A mobile user
H	The home agent of M
F	The foreign agent
ID_A	The identity of the participant A
PW_M	The password of M
K_{FH}	The pre-shared secret key between F and H
Pub_H	The home agent H's public key
Pri_H	The matching private key of Pub_H hold by H
x	The secret key of H
$h(\cdot)$	A one-way hash function
$\oplus$	Exclusive-OR operation
$\|$	String concatenation operation
E_k	An encryption function with key the k
D_k	A decryption function with key the k
Adv	The adversary

Step 2. H computes $R = h(ID_M\|x) \oplus PW_M$ and $k = h(PW_M)$. After that, H stores $\{ID_M, R, k, Pub_H, h(\cdot), E(\cdot)\}$ into the smart card and submits it to M.

2.2 Mutual Authentication and Key Agreement Phase

Step 1. M inserts the smart card into the device and inputs PW_M^*. Then the smart card calculates $k^* = h(PW_M^*)$ and checks whether $k^* \overset{?}{=} k$. If yes, it means M is the cardholder; otherwise, the smart card terminates the procedure. Afterwards, the smart card randomly selects $n_M, r_M \in Z_q^*$, and computes $AID_M = E_{Pub_H}(r_M\|ID_M)$. Finally, M sends $m_1 = \{ID_H, AID_M, n_M\}$ to F.

Step 2. On receiving m_1, F generates n_F, $r_F \in Z_q^*$ and computes $V_1 = E_{Pub_H}(r_F \|ID_H \|ID_F \| AID_M \|n_M \|n_F)$. Subsequently, F sends $m_2 = \{ID_H, ID_F, V_1\}$ to H.

Step 3. Upon receiving m_2, H can obtain $(r_F \|ID_H \|ID_F \|AID_M \|n_M \|n_F)$ by decrypting V_1 using the private key Pri_H. Subsequently, H can get $(r_M\|ID_M)$ from decrypting AID_M. Then, H verifies the validity of M. If M successfully passes the verification, H generates a random integer $n_H \in Z_q^*$ and calculates $C = h(ID_M\|x) \oplus r_M$, $y = h(C\|r_M) \oplus n_H \oplus h(K_{FH}\|r_F)$, $z = h(C\|n_M\|r_M) \oplus n_H$, $V_2 = h(K_{FH}\|n_M\|n_F\|r_F\|y\|z)$, $V_3 = h(C\|z)$, and then sends $m_3 = \{V_2, V_3, y, z\}$ to F.

Step 4. Upon receiving m_3, F verifies $V_2 \overset{?}{=} h(K_{FH} \|n_M \|n_F \|r_F \|y \|z)$. If this equation holds, F computes $TK = y \oplus h(K_{FH}\|r_F)$, and then sends $m_4 = \{V_3, z, n_F\}$ to M; otherwise, F terminates this session.

Step 5. After receiving m_4, M calculates $C = R \oplus PW_M^* \oplus r_M$ and checks whether $h(C\|z)$ is equal to the received V_3. If it is true, then M establishes trust with F. Otherwise, this session will be terminated.

After the mutual authentication phase successfully, M and F share the session key $SK = h(TK\|n_M\|n_F) = h(h(C\|r_M) \oplus z \oplus h(C\|n_M\|r_M)\|n_M\|n_F)$.

2.3 Password Changing Phase

When M wants to update PW_M, M inserts his/her smart card into a terminal and inputs the origin password PW_M to the smart card.

Step 1. The smart card computes $h(PW_M)$ and checks whether it is equal to the stored k. If yes, M inputs a new password PW_M^{new}; otherwise, the smart card rejects the password change request and terminates this procedure.

Step 3. The smart card computes $k^{new} = h(PW_M^{new})$, $R^{new} = R \oplus PW_M \oplus PW_M^{new}$ and replaces k, R by k^{new}, R^{new}, respectively.

3 Analysis of Chuang et al.'s Scheme

To analyze the security weaknesses of Chuang et al.'s scheme, we assume that an attacker Adv could obtain the secret values stored in the smart cards by monitoring the power consumption [7,11] and intercept messages transmitted in the insecure communication channel. Under this assumption, we demonstrate that Chuang et al.'s scheme fails to provide user anonymity and is susceptible to various attacks, such as server masquerading attack, off-line dictionary attack, user impersonation attack.

3.1 Server Masquerading Attack

Assume an adversary Adv has intercepted the message $m_3 = \{V_2, V_3, y, z\}$ transmitted from H to F. Then Adv generates a random number $\overline{n_F}$ and sends $\overline{m_4} = \{V_3, z, \overline{n_F}\}$ to M, where $\overline{n_F}$ is selected randomly by Adv. After receiving $\overline{m_4}$ from Adv, M computes $C = R \oplus PW_M^* \oplus r_M$ and $h(C\|z)$, it is obvious that $V_3 = h(C\|z)$. Thus, M will be fooled into believing the adversary as the legitimate foreign agent F.

3.2 Off-line Dictionary Attack

In case a legitimate mobile user M's smart card is somehow obtained (e.g., stolen or picked up) by Adv, and he/she can extract the stored secret value k [1,7,11,15]. Then Adv can acquire M's password PW_M by performing the following procedures:

Step 1. Guesses a candidate password PW_M^* from the password space $\mathcal{D}_{PW}$.

Step 2. Computes $k^* = h(PW_M^*)$ and verifies the correctness of PW_M^* by checking $k^* \overset{?}{=} k$.

Step 3. Repeats the Steps 1 and 2 by replacing another guessed password until the correct password is found.

Generally, due to the inherent limitation of human cognition, the identity is easy-to-remember and hence the identity space is very limited, and it follows that the above attack can be completed quite effectively. The running time of the above attack procedure is $\mathcal{O}(|\mathcal{D}_{PW}| * T_h)$, where T_h is the running time for Hash operation. And hence, their scheme cannot resist off-line dictionary attack.

3.3 Failure to Provide Users' Anonymity

In Chuang et al.'s scheme, the home agent H stored ID_M in M's smart card. Hence, Adv can get ID_M by monitoring the power assumption [1,7,11,15]. Although Chuang et al.'s scheme does not use ID_M as a parameter in the login request message, it is used to compute AID_M. Then, Adv can launch a series of attacks, such as user impersonation attack, to damage the security of this scheme [4].

3.4 User Impersonation Attack

As explained above, if Adv successfully obtains $M's$ smart card, he/she can get PW_M and ID_M corresponding to M. Then, Adv can impersonate M to make fool of both F and H as follows.

In the mutual authentication and key agreement phase, Adv generates two random number n'_M, $r'_M \in Z_q^*$ and computes $AID'_M = E_{Pub_H}(r'_M \| ID_M)$. Then he/she sends the forged login request message $m'_1 = \{ID_H, AID'_M, n'_M\}$ to F.

It is easy to see the forged login request is in the correct format. Upon receiving m'_1, H and F will execute the protocol normally and Adv will pass the verification successfully.

4 Our Proposed Scheme

In this section, we propose a new authentication scheme with user anonymity in global mobility networks using elliptic curve cryptography. Our scheme consists of four phases, which are the registration phase, mutual authentication and key agreement phase, password changing phase and revocation phase.

Before the system begins, H generates two distinct large primes p and q with $p = 2q + 1$ and chooses a generator P of order q on the elliptic curve $E_p(a, b)$. H computes the public key $Q = x \cdot P \ mod \ p$ with the master secret key x of H. Subsequently, H computes a secret key $K_{FH} = h(ID_F \| x)$ for each foreign agent F.

4.1 Registration Phase

Step 1. M freely chooses his/her identity ID_M and password PW_M. Then, M sends them to H via a secure communication channel.

Step 2. H calculates $A = h(ID_M \| x)$, $B = h(ID_M \| v)$ and $C = h(ID_M \times P + PW_M \times P)$, where v is a secret random number chosen by H for every mobile user.

Step 3. After that, H maintains a registration table in the format (B, A). H can retrieve A from the registration table by B in the revocation phase and in the mutual authentication and key agreement phase.

Step 4. H personalizes the smart card with $\{C,\ P,\ Q,\ E_p(a, b),\ q,\ p,\ h(\cdot)\}$ and issues it to M.

4.2 Mutual Authentication and Key Agreement Phase

Step 1. M inserts his/her smart card into a card reader and enters ID_M, PW_M. Then, the smart card verifies $C \overset{?}{=} h(ID_M \times P + PW_M \times P)$, if not, the login phase is terminated immediately; otherwise, the smart card generates a random number $\alpha \in [1, q-1]$ and computes $X = \alpha \times P$, $X_1 = \alpha \times Q$, $D = ID_M \oplus h(X + X_1)$. Finally, the smart card sends $m_1 = \{ID_H, X, D\}$ to F.

Step 2. Upon receiving m_1, F generates a random integer number $\beta \in [1, q-1]$ and calculates $Y = \beta \times P$, $Y_1 = \beta \times Q$, $E = K_{FH} \times P + Y_1$. Then, F transmits the message $m_2 = \{ID_H, ID_F, X, D, Y, E\}$ to H.

Step 3. On receiving m_2, H computes $X_1 = x \times X$, $ID_M = D \oplus h(X + X_1)$, $B = h(ID_M \| v)$, and $A^* = h(ID_M \| x)$. Then, H retrieves A from the registration table by B and checks $A^* \overset{?}{=} A$. If B does not exist in the verifier table or $A^* \neq A$, H terminates this session. If three continuous requests from M fail in a short interval, H will ignore M's following request within a guard interval. If the all conditions hold, H verifies the legitimacy of M successfully. Afterwards, H computes $Y_1 = x \times Y$, $E^* = h(ID_F \| x) \times P + Y_1$ and verifies E^* with the received E. If they are equal, the authenticity of F is ensured; otherwise, H rejects this request. After the verification of M and F, H computes $I = ID_M \times P + X_1$, $J = h(h(ID_F \| x) \times P - Y_1) \oplus h(X_1)$ and $K = h(ID_F \| x) \times Y_1$. Finally, H sends the message $m_3 = \{I, J, K\}$ to F.

Step 4. After receiving m_3 from H, F firstly calculates $K_{FH} \times Y_1$ and verifies it with the received K. If it is valid, F computes $h(X_1) = J \oplus h(K_{FH} \times P - Y_1)$, $TK = h(X_1) \times \beta \times X$ and $sk = h(h(X_1) \times P - \beta \times X)$ and transmits the message $m_4 = \{I, Y, TK\}$ to M.

Step 5. Upon receiving m_4, M computes $I^* = ID_M \times P + X_1$ and $TK^* = h(X_1) \times \alpha \times Y$. Then M checks $I^* \overset{?}{=} I$ and $TK^* \overset{?}{=} TK$, respectively. If the two equations hold, M successfully authenticates H and F, then sends $m_5 = h(h(h(X_1) \times P - \alpha \times Y)\|0)$ to F. If any of these two equations is false, the authentication fails.

Step 6. After receiving m_5, F computes $m_5^* = h(sk\|0)$ and checks $m_5^* \overset{?}{=} m_5$. If they are equal, F ensures the legitimate of M; otherwise, terminates the session.

After mutual authentication, M and F compute and share the session key $SK = h(sk\|1) = h(h(h(X_1) \times P - \alpha \times \beta \times P)\|1)$ for future secure communication.

4.3 Password Changing Phase

When the user M wants to update his/her password offline, he/she inserts the smart card into a terminal and enters his/her identity ID_M and old password PW_M to the smart card.

Step 1. The smart card checks $C \overset{?}{=} h(ID_M \times P + PW_M \times P)$. If yes, M inputs a new password PW_M^{new}; otherwise, the smart card rejects the password change request and terminates this procedure.

Step 3. The smart card computes $C^{new} = h(ID_M \times P + PW_M^{new} \times P)$ and stores C^{new} into its memory to replace C.

4.4 Revocation Phase

In case of lost or stolen smart cards, M could request H to revoke his/her smart card. In our scheme, M should transmit ID_M to H via a secure communication channel, then H computes $h(ID_M\|v)$, and checks whether it exists in the registration table. If yes, H retrieves A from the registration table by B and checks whether $h(ID_M\|x)$ is equal to A. Supposing that these two conditions hold, H removes the entry (B, A) from the registration table. If M wants to re-register in H, he/she just needs to re-register in H through performing the registration phase again.

5 Secure Analysis of Our Scheme

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

We assume that the following problems are difficult to solve in polynomial time, in other words, there are no efficient polynomial-time algorithm to solve the following problems.

1) ECDLP [5]: Given two points $P,\ Q \in E_p(a,b)$, the elliptic curve discrete logarithm problem(ECDLP) is to find an integer $s \in Z_p^*$ such that $Q = s \cdot P$.

2) CDHP [5]: Given three points $P,\ s \cdot P,\ t \cdot P \in E_p(a,b)$, where $s,\ t \in Z_p^*$, the computation Diffie-Hellman problem(CDHP) is to find the point $(s \cdot t)P$ on $E_p(a,b)$.

Theorem 1. *Our scheme could provide mutual authentication.*

Proof. Mutual authentication means that these three communication parties involved in global mobility networks can authenticate each other before generating the common session key. In order to withstand user & server masquerading attack, it is necessary for a robust authentication scheme to satisfy this security feature. In our scheme, only the home agent H can generate I, J, K using its secret key x. Then the foreign agent F could check the validity of K to verify H. Afterwards, the mobile user M could check the validity I and TK to verify H and F, respectively. Further, our scheme allow them to agree on a session key which varies in each session run. Therefore, our scheme satisfies this feature. □

Theorem 2. *Our scheme could provide perfect forward security.*

Proof. The forward secrecy is defined as the assurance that any previous session keys cannot be compromised if the master secret key x of the home agent H is leaked. In our scheme, the session key $h(h(h(X_1) \times P - \alpha \times \beta \times P)\|1)$ is generated by two one-time random number $\{\alpha, \beta\}$ in each session. Moreover, even if the adversary eavesdrops the mutual authentication messages, he/she still cannot compute $\alpha \times \beta \times P$ from $\alpha \times P$ and $\beta \times P$ since the intractability of the Diffie-Hellman problem. Therefore, our scheme could provide perfect forward security. □

Theorem 3. *Our scheme could provide user anonymity and untraceability.*

Proof. In the proposed scheme, the information of ID_M is hidden in $D = ID_M \oplus h(X + X_1)$. If the adversary wants to retrieve the mobile user M's identity from D, he/she should compute $X_1 = \alpha \times x \times P$ from $\alpha \times P$ and $Q = x \times P$ to obtain the value $h(X + X_1)$, then he/she will face with the CDHP. Furthermore, $\{X, D\}$ varies in each session because they are generated by the random number α. It is difficult for the adversary to tell apart M from others in the communication channel. Hence, the proposed scheme satisfies user anonymity and untraceability. □

Theorem 4. *Our scheme could withstand user impersonation attack.*

Proof. In our scheme, if the adversary wants to forgery the legal mobile user M, he/she has to generate a valid message $m_1 = \{ID_H, X, D\}$, where $D = ID_M \oplus h(X + X_1)$, $X = \alpha \times P$. However, *Adv* cannot generate a valid D without the knowledge of ID_M. Therefore, our scheme could withstand user impersonation attack. □

Theorem 5. *Our scheme could withstand server masquerading attack.*

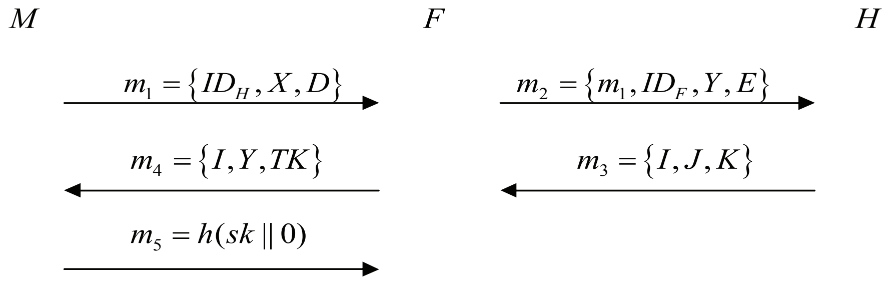

Figure 1: Message flows in authentication and key agreement phase

Table 2: Comparisons of the security properties

	Ours	He et al.'s [6]	Chuang et al.'s [4]
User anonymity	Yes	No	No
Prevention of user impersonation attack	Yes	No	No
Prevention of off-line dictionary attack	Yes	No	No
Prevention of server masquerading attack	Yes	No	No
Revocation of smart cards	Yes	No	No
Freely change password	Yes	No	Yes
Mutual authentication	Yes	No	No
Prevention of replay attack	Yes	No	No

Proof. In our scheme, if Adv wants to impersonate H or F to fool the mobile user M, he/she has to generate a valid reply message $m_4 = \{I, Y, TK\}$, where $I = ID_M \times P + X_1$, $TK = h(X_1) \times \beta \times X$ and $Y = \beta \times P$. However, the adversary cannot generate I and TK without the knowledge of x. So, our scheme could withstand server masquerading attack. □

Theorem 6. *Our scheme could withstand stolen smart card attack.*

Proof. If M's smart card is lost and obtained by Adv, he/she can extract the stored data $\{C,\ P,\ Q,\ E_p(a,b),\ q,\ p,\ h(\cdot)\}$ in the smart card through the differential power analysis [1, 7, 11, 15] and intercept the message $m_1 = \{ID_H,\ X,\ D\}$, $m_2 = \{ID_H,\ ID_F,\ X,\ D,\ Y,\ E\}$, $m_3 = \{I, J, K\}$, $m_4 = \{I, Y, TK\}$. If Adv wants to obtain ID_M from these messages, he/she has to compute $X_1 = \alpha \times x \times P$ from $\alpha \times P$ and $Q = x \times P$. Adv will face with the CDHP.

We should consider the off-line password guessing attack in this case, that is, the adversary uses a brute force search to find out the correct password from the value C. In our proposed anonymous authentication scheme, the user identity is protected against outsiders what can help to withstand the password guessing attack. Since there can be a huge number of users in the mobile system, it is infeasible for an adversary to do an exhaustive search for all the possible $(ID, Password)$ pairs. Therefore, our scheme can withstand stolen smart card attack. □

Theorem 7. *Our scheme could withstand replay attacks.*

Proof. In our scheme, Adv may intercept the message $m_1 = \{ID_H, X, D\}$ and replay it to the foreign agent F. However, the adversary cannot generate valid m_5 without knowing x and α. Then, F can find the attack by checking the valid of m_5. Moreover, Adv also cannot generate valid SK without knowing the value β to construct a communication channel with F. Therefore, our scheme could withstand replay attack. □

6 Comparisons

In this section, we compare security properties of the proposed authentication scheme with other related schemes, including the schemes of He et al. [6] and Chuang et al. [4]. 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. We define the following notations are used in Table 3: t_h: the time complexity of the hash computation; t_{sym}: the time complexity of the symmetric encryption/decryption; t_{asym}: the time complexity of encryption/decryption or signature using asymmetric cryptosystem.

According to Table 2, we can conclude that He et al.'s scheme does not satisfy any of the criterion listed in Table 2. Chuang et al.'s scheme satisfies only one criteria listed in Table 2. While, our proposed scheme can achieve all the criterion listed in Table 2. Particularly, our proposed scheme does not require H to store some secret information that is shared with F in its 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 [4, 6] in case of the mutual authentication phase. From Table 3, it is easy to see that our scheme is more efficient than other schemes. Our scheme requires three extra transmitted messages as compared with Chuang et al.'s scheme and five extra transmitted messages as compared with He et al.'s scheme. However, our proposed scheme does not proceed encryption/decryption using asymmetric cryptosystem, moreover, our scheme achieves stronger security than the previous solutions as shown in Table 2.

Table 3: Efficiency comparison

	Chuang et al. [4]	He et al. [6]	Ours
C1	$2t_h + t_{asym}$	$10t_h + 2t_{sym}$	$5t_h$
C2	$2t_h + t_{asym}$	$4t_h$	$7t_h$
C3	$6t_h + 2t_{asym}$	$4t_h + 2t_{sym} + 4t_{asym}$	$7t_h$
C4	1	1	3/2
C5	1	1	1
C6	6	5	7
C7	7	6	9

C1: Computation cost of the M
C2: Computation cost of the F
C3: Computation cost of the H
C4: Communication rounds between the M and F
C5: Communication rounds between the F and H
C6: Total messages transmitted between M and F
C7: Total messages transmitted between F and H

7 Conclusions

In this paper, we analyze several security flaws in Chuang et al.'s authentication scheme with user anonymity for roaming service in global mobility networks. Further, we propose a new authentication scheme for roaming service in GLOMONET to overcome these shortcomings. In addition, the security analysis and performance comparisons demonstrate our proposal is more secure and suitable to the practical application environment.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments. This work is supported by Natural Science Foundation of Shandong Province(NO.ZR2013FM009).

References

[1] G T. Becker, *Intentional and Unintentional Side-channels in Embedded Systems*, University of Massachusetts Amherst, 2014.

[2] C. C. Chang and C. Y. Lee, "A smart card-based authentication scheme using user identify cryptography," *International Journal of Network Security*, vol. 15, no. 2, pp. 139–147, 2013.

[3] C. Chen, D. J. He, S. Chan, J. J. Bu, Y. Gao and R. Fan, "Lightweight and provably secure user authentication with anonymity for the global mobility network," *International Journal of Communication Systems*, vol. 24, no. 3, pp. 347–362, 2011.

[4] Y. H. Chuang, Y. M. Tseng and C. L. Lei, "Efficient mutual authentication and key agreement with user anonymity for roaming services in global mobility networks," *International Journal of Innovative Computing Information and Control*, vol. 8, no. 9, pp. 6415–6427, 2012.

[5] D. Hankerson, A. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer: Heidelberg, 2003.

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

[7] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," in *Proceedings of Advances in Cryptology*, pp. 388–397, Santa Barbara, CA, U.S.A., 1999.

[8] C. C. Lee, M. S. Hwang and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless communications," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1686, 2006.

[9] C. C. Lee, R. X. Chang and T. Williams, "On the anonymity of an enhanced authentication scheme for a roaming service in global mobility networks," *International Journal of Secure Digital Information Age*, 2010, (in press).

[10] 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, pp. 35–44, 2012.

[11] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 5, no.51, pp. 541–552, 2002.

[12] J. Niu and X. Li, "A novel user authentication scheme with anonymity for wireless communications," *Security and Communication Networks*, vol. 7, no. 10, pp. 1439–1640, 2014.

[13] R. Ramasamy and A. P. Muniyandi, "An efficient password authentication scheme for smart card," *International Journal of Network Security*, vol. 14, no. 3, pp. 180–186, 2012.

[14] S. K. Sood, "An improved and secure smart card based dynamic identity authentication protocol," *International Journal of Network Security*, vol. 14, no. 1, pp. 39–46, 2012.

[15] J. van Woudenberg, M. Witteman, and B. Bakker, "Improving differential power analysis by elastic alignment," in *Proceedings of the 11th International Conference on Topics in Cryptology (CT-RSA'11)*, pp. 104–119, 2011.

[16] F. T. Wen, W. Susilo, G. M. Yang, "A robust smart card-based anonymous user authentication protocol for wireless communications," *Security and Communication Networks*, vol. 7, no. 6, pp. 987–993, 2014.

[17] G. M. Yang, D. C. Wong, and X. T. Deng, "Anonymous and authenticated key exchange for roaming networks," *IEEE Transactions on Wireless Communication*, vol. 6, no. 9, pp. 3461–3472, 2007.

[18] P. Zeng, Z. Cao, K. K. R. Choo, and S. Wang, "On the anonymity of some authentication schemes for wireless communications," *IEEE Communications Letters*, vol. 13, no. 3, pp. 170–171, 2009.

[19] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environment," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 230–234, 2004.

Dianli Guo received his B.S.degree in applied mathematics from Heze University, China in June 2011. He is currently working towards his M.S degree in applied mathematics at Jinan University, China. His current research interest includes wireless network security and applied cryptography.

Fengtong Wen received his B.S degree in mathematics from Qufu normal university, China in June 1994. He received his M.S degree in fundamental mathematics from Qufu normal university, China in June 1997. He received his Ph.D degree in cryptography from Beijing University of Posts and Telecommunications, China in 2006. He is a professor at the School of mathematics, university of Jinan, China. His research interests include information security, cryptography and applied mathematics.