Wireless Pers Commun (2017) 97:2665–2682
DOI 10.1007/s11277-017-4629-x

An Anonymous Authentication Scheme with the Enhanced Security for Wireless Communications

Rui Chen[1] · **Dezhong Peng**[1]

Published online: 6 July 2017
© Springer Science+Business Media, LLC 2017

Abstract In wireless communication system, a good protocol should satisfy many requirements: user identity authentication, privacy protection, computational efficiency and resist some known attacks. Thus design a highly secure anonymous authentication protocols for wireless networks is a challenging task. Over recent years, many researchers have proposed their own solutions to address this issue. In 2014, Niu et al. analyzed Yoon et al.'s authentication scheme, then put forward a smart card based authentication scheme with anonymity for wireless networks. They claimed their scheme achieves many security requirements and resists some known threats. Nevertheless, after detailed analysis, we prove that the scheme of Niu et al. is prone to some malicious attacks such as replay attacks and DoS attacks. Moreover, the scheme does not work when large amount of mobile users access a foreign agent simultaneously. To overcome these drawbacks, we present a new secure authentication scheme with user anonymity by improving Niu et al.'s scheme. The proposed protocol not only satisfies many security properties, such as strong anonymity, mutual authentication and periodically update session key, but also resists well-known threats. Furthermore, the security and performance analyses indicates that the new scheme is well suitable for wireless communications when it is compared with previous protocols.

Keywords Authentication · Security · Anonymity · Wireless communications · Elliptic curve cryptosystem

✉ Rui Chen
crs1934@hotmail.com

Dezhong Peng
pengdz@scu.edu.cn

[1] College of Computer Science, Sichuan University, Chengdu 610068, China

1 Introduction

With the advancement and rapid growth of the information and communication technologies, it has brought us not only advantages of life, but also risks and challenges. In wireless communications system, the mobile users(*MU*) can obtain the service supplied by its home agent (*HA*) whenever they roam to a foreign agent(*FA*). To achieve identity authentication, *FA* needs assistance of the *MU*'s *HA* [1–18] . Generally, a secure user authentication scheme for wireless communications should meet a series of requirements [4], such as user anonymity, low communication cost and computational complexity, single registration, updating session key periodically, etc.

In order to achieve secure and effective mutual authentication and privacy protection in wireless communications, a lot of anonymous authentication protocols have been published [1–8, 13–20]. Zhu and Ma [5] proposed the first authentication scheme for wireless environments in 2004. Later, Lee et al. [6] pointed that Zhu-Ma's scheme had many shortcomings, such as cannot provide strong backward secrecy and authenticate each other, and then, they put forward an authentication scheme which fixed these security drawbacks. Subsequently, in 2008, Chang et al. [2] and Wu et al. [7] indicated that Lee et al.'s scheme cannot achieve user anonymity, and an adversary can join the same *HA* to get other users' identities. They put forward an improvement scheme to remedy this weakness. But their scheme also cannot protect user's privacy and vulnerable to other several weakness (i.e., replay attack and impersonation attack) [3, 12].

In 2012, Li and Lee [8] found that He et al.'s scheme [3] has three drawbacks: lacks of user friendliness; fails to achieve user anonymity; and unfairness in key agreement. Meanwhile, Xiong et al. [21] also showed that the scheme in [12] has some flaws. Additionally, they put forward their own improvement schemes respectively. Unfortunately, in 2013, Das [4] proved the scheme of Li and Lee [8] has some security issues in login, authentication and password change phases. Further, Das et al. proposed a novel scheme to withstand the weaknesses of Li and Lee's scheme. But in 2014, Wen et al. [14] and Hu et al. [13] discovered that Das et al.'s scheme is still vulnerable to impersonation attack and offline password guessing attack respectively, then they presented the enhanced schemes to overcome the flaws.

In 2015, Farash et al. [15] presented a lightweight authentication scheme with anonymity, which is improved on Shin et al's scheme [16] and Wen et al.'s scheme [17]. But Chung et al. [18] found their scheme cannot provide user anonymity, authentication and password replacement. At the same year, Djellali et al. [19] put forward an authentication scheme based on Markov chain and claimed their scheme provides both user anonymity and mutual authentication. Later on, Kang et al. [22] analyzed the security of Djellali et al. 's scheme, and exhibited that their protocol cannot prevent insider attack, offline-password guessing attack, impersonation attack and replay attack. In 2016, Jiang et al. [20] proposed a three-factor authentication protocol for e-health clouds. But then Irshad and Chaudhry [23] found that Jiang et al.'s scheme is subject to denial of service(DoS) attack.

Recently, Niu and Li [9] analysed the authentication protocol of Yoon et al. [10] and indicated that Yoon et al.'s scheme is not secure due to some security defects, such as unfair in key agreement and unable to protect user anonymity. Then they put forward an novel user authentication scheme for wireless environments on account of elliptic curve cryptosystem (ECC) [24], they claimed that the improved scheme had several excellent features, including achieving user anonymity, providing mutual authentication, security of session key exchanging and the ability to resist some known attacks like offline password-

guessing attack, forgery attack and so on. However, we found Niu et al.'s scheme also had some significant security vulnerabilities and cannot prevent some known attacks.

The contributions of this paper are three points. Firstly, through careful analysis, we show that Niu et al.'s protocol is still insecure because of the following four security weaknesses in it:

(1) Niu et al.'s scheme unable to provide secure authentication at login phase.
(2) Niu et al.'s scheme unable to resist replay attack. A hostile *FA* can impersonate *MU* by forwarding the *MU*'s login request to another foreign agent.
(3) Niu et al.'s scheme unable to work when large number of *MU* s visit a *FA* simultaneously. The *FA* will not be able to distinguish the *MU*s when lots of *MU*s visit a *FA* simultaneously.
(4) Niu et al.'s scheme unable to resist the potential DoS attack. If an attacker stolen the smart card or device, the DoS attack can be easily launched by generating a lot of redundant messages to *FA* and *HA*.

Secondly, we present an enhanced secure and effective authentication protocol with anonymity for wireless communications to address the above problems. Considering the limited power and resources of mobile users, our scheme makes use of some low-cost functions(i.e. ECC, hash, XOR), hence it has high computational efficiency compared with previous schemes. The proposed scheme not only enjoys many merits from Niu et al.'s scheme like user anonymity, resistance of some known attacks, no verification table, timestamp verification and so on, but also improve it in security and DoS resistance. In other words, the proposed scheme protects the user's privacy and provides mutual authentication, perfect forward secrecy and counters against off-line password guessing, impersonation, replay, and other known attacks.

Thirdly, we put forward a new method to effectively prevent DoS attack. Because the three-party roaming protocols demand the *FA* forward all login messages to *HA* unconditionally, the adversary can easily launch DoS attack on *HA* and *FA*. In this paper, an efficient way to address this issue was offered and its feasibility was approved. Additionally, further analysis also indicates that our protocol can successfully resist various well-known attacks and really applicable to mobile environment.

The structure of the rest of the paper is as follows. Section 2 provides a simply review and analysis of Niu et al.'s scheme. In Sect. 3, we describe the details of our improved scheme, which is then analyzed in Sect. 4. Next, we compare the performance and functionality of the new scheme with previous works in Sect. 5. Finally, we draw some conclusion in Sect. 6.

2 Review and Analysis of the Niu et al.'s Scheme

2.1 Review of the Scheme of Niu et al.

We first simply review Niu et al.'s scheme [9] before giving a description of its drawbacks. Table 1 lists some symbols used throughout in Niu et al.'s scheme. Their protocol have following entities: a mobile user *MU*, a home agent *HA* of *MU* and a visited foreign agent *FA*. The operation process of the scheme include three different phases: the registration phase, the authentication phase, and the session key update phase.

Table 1 Notations used in this paper

Notation	Description
MU	Mobile user
HA	Home agent of MU
FA	Foreign agent of the network
PW_A	Password of A
ID_A	Identity of A
T_A	Timestamp generated by A
T_{auth}	The average time of the authentication and establishment phase
$Cert_A$	Certificate of A
$(M)_K$	Message M encrypted by symmetric key K
p, n	Two large prime numbers
F_P	A finite field
$E_P(a,b)$	An elliptic curve defined on finite field F_P
P	A point on elliptic curve $E_P(a,b)$ with order n
(P_A, S_A)	(Public key, private key) pair of A based on ECC
$E_{P_A}(M)$	Message M encrypted by public key P_A
$S_{S_A}(M)$	Message M signed by private key S_A
$h()$	One-way hash function
$f()$	A number generation function
$\oplus$	XOR operation
$\|$	Concatenation

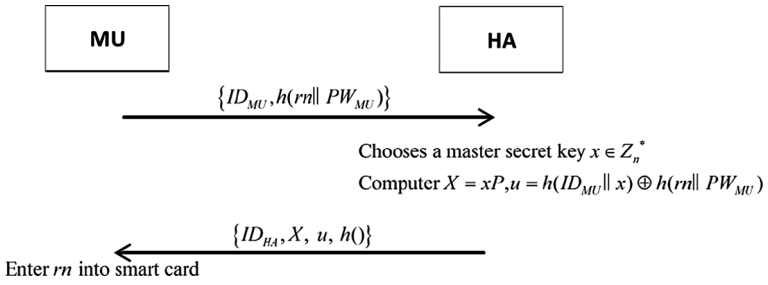

Fig. 1 Registration phase of Niu's scheme

2.1.1 Registration Phase

When visiting a foreign agent FA, the MU requires registration to his/her home agent HA before obtaining the service provided by FA, the handshake is described in Fig. 1. The registration process of Niu et al.'s protocol is as follows:

Step R1 MU randomly chooses an identity ID_{MU}, password PW_{MU} and a number r_n. Next the MU sends the message $\{ID_{MU}, h(r_n \| PW_{MU})\}$ to HA via a secure channel.

Step R2 When receiving $\{ID_{MU}, h(r_n \parallel PW_{MU})\}$ from MU, the HA generates a strong secret key x and caculates $X = xp, u = h(ID_{MU} \parallel x) \oplus h(r_n \parallel PW_{MU})$.

Step R3 HA delivers a smart card, which includes $\{ID_{HA}, X, u, h()\}$, to MU through a secure channel.

Step R4 MU puts the received smart card into mobile device and enters r_n into it.

2.1.2 Authentication and Establishment of Session Key Phase

When a mobile user MU roams to a foreign agent(FA), the MU needs to be authenticated by FA with the help of its HA as well as verifies the validity of FA. The detail process of this phase in Niu et al.'s scheme is shown in Fig. 2.

Step L1 The MU enters the ID_{MU} and PW_{MU} into its mobile device.

Step L2 The smart card in the mobile device randomly generates a number $a \in Z_n^*$ and calculates $A = aP, D = aX = axP, SID = ID_{MU} \oplus h(D \parallel T_{MU}), E = u \oplus h(r_n \parallel PW_{MU}), C_1 = h(E \parallel D)$.

Step L3 The MU generates a timestamp T_{MU} and submits the login request message $\{A, SID, C_1, T_{MU}, ID_{HA}\}$ to FA.

Step L4 When FA receives the login request from MU, it validates the message first. If the timestamp T_{MU} is in the allowable range, FA saves the received information and produces a timestamp T_{FA} and a random number $b \in Z_n^*$. Then, FA calculates $B = bP$ and the signature $Sig_{FA} = S_{S_{FA}}(h(A \parallel SID \parallel C_1 \parallel T_{MU} \parallel B \parallel T_{FA}))$ using its private key S_{FA}.

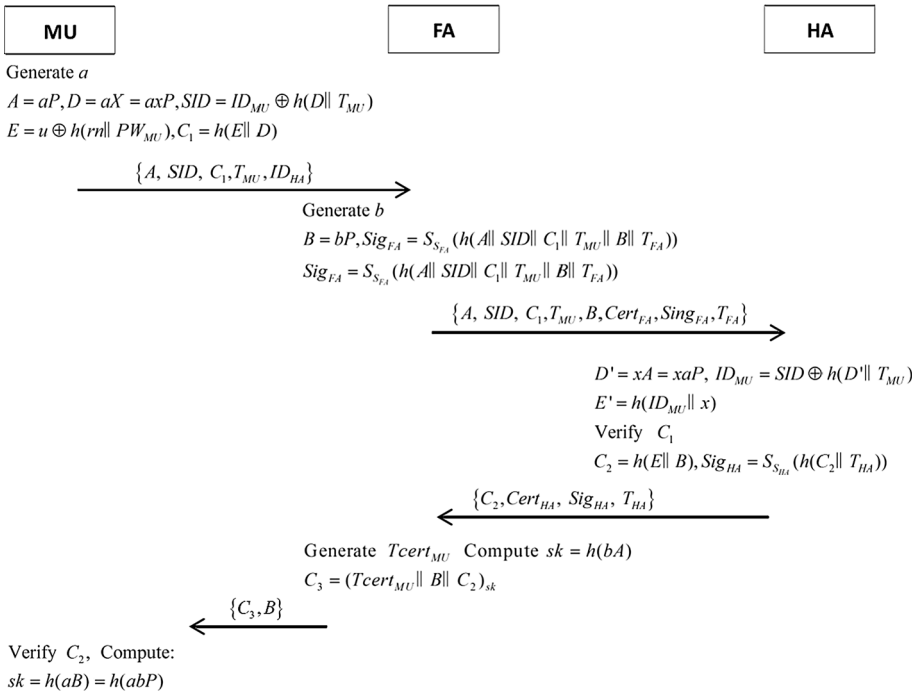

Fig. 2 Authentication and establishment of session key phase of Niu et al.'s scheme

Step L5 *FA* submits $\{A, SID, C_1, T_{MU}, B, Cert_{FA}, Sig_{FA}, T_{FA}\}$ to *HA*, where $Cert_{FA}$ is *FA*'s certificate.

Step L6 Once the message is received by *HA*, the *HA* first validate the certificate $Cert_{FA}$ and the timestamp T_{FA}. If they are valid, *HA* can perform authentication to *FA* through the signature Sig_{FA} using *FA*'s public key P_{FA}. Next, *HA* computes $D' = xA = xaP, ID'_{MU} = SID \oplus h(D' \parallel T_{MU})$ and gets *MU*'s real identity, and checks if the ID'_{MU} is valid. If it is, *HA* calculates $E' = h(ID'_{MU} \parallel x), C'_1 = h(E' \parallel D')$, and compares C'_1 with C_1. If the two values are the same, *HA* considers *MU* as legal user, then *HA* gets current timestamp T_{HA} and computes $C_2 = h(E' \parallel B), Sig_{HA} = S_{S_{HA}}(h(C_2 \parallel T_{HA}))$, and then *HA* sends the message $\{C_2, Cert_{HA}, Sig_{HA}, T_{HA}\}$ to *FA*.

Step L7 When *FA* receives the information from *HA*, it verifies the certificate $Cert_{HA}$, timestamp T_{HA} and Sig_{HA}. If both of them are valid, *FA* puts the timestamp and others information into a temporary certificate $Tcert_{MU}$. Then, *FA* calculates $sk = h(bA) = h(abP)$ as the session key and $C_3 = (Tcert_{MU} \parallel B \parallel C_2)_{sk}$. After that, *FA* sends $\{C_3, B\}$ to *MU*.

Step L8 When the message from *FA* is received, the *MU* decrypts C_3 using computed session key $sk = h(aB) = h(abP)$ and obtains $Tcert_{MU}, B$ and C'_2, then *MU* computes $C_2 = h(E \parallel B)$ and compares C_2 with C'_2, if the two values are equal, *MU* can confirm that *FA* is authenticated by *HA*, so *MU* and *FA* can safely communicate with each other through the session key *sk*.

2.1.3 Update Session Key Phase

If a *MU* always stay in a same *FA*, the session key between the *MU* and the *FA* need to be regularly update for reasons of safety. Their *i*th session key $sk_i (i = 2, \ldots, n)$ can be updated as follows. We demonstrate this phase in Fig. 3.

Step U1 *MU* randomly selects a number $a_i \in Z_n^*$ and computes $A_i = a_i P (i = 2, \ldots, n)$. Next, *MU* sends A_i to *FA*.

Step U2 *FA* also randomly chooses a number $b_i \in Z_n^*$ and computes $B_i = b_i P (i = 2, \ldots, n)$. Then, *FA* calculates $sk_i = h(b_i A_i) = h(a_i b_i P)$ and $V_i = h(a_i b_i P \parallel a_{i-1} b_{i-1} P)$ which sk_i is a new session key. After that, *FA* submits $\{B_i , V_i\}$ to *MU*.

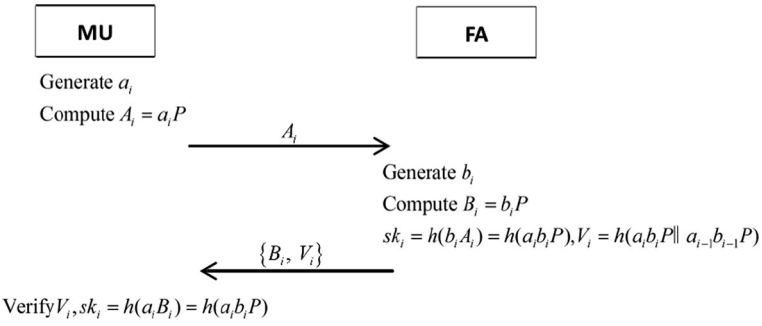

Fig. 3 Update session key phase of Niu's scheme

Step U3 After receiving message $\{B_i, V_i\}$ from FA, the MU computes $V_i' = h(a_i B_i \parallel a_{i-1} B_{i-1}) = h(a_i b_i P \parallel a_{i-1} b_{i-1} P)$ and checks if V_i' and V_i are the same. If so, MU computes the new session key $sk_i = h(a_i B_i) = h(a_i b_i P)$ by using the received B_i and replaces old session key sk_{i-1} with new session key sk_i.

2.2 Weaknesses in the Scheme of Niu et al.

Although Niu et al. presented an improved protocol of Yoon et al.'s scheme, we show that there are still some shortcomings and deficiencie in their scheme. The detail is as follows:

2.2.1 Niu et al.'s Scheme Unable to Achieve Secure Authentication at Login Phase

In Niu et al.'s scheme, the MU needs to input its identity and password into the mobile device for access services when he/her first visits a foreign network. However, we notice that both the inputed identity and password are not to be checked by smart card in the mobile device. That means even if the MU careless inputs wrong login information, their scheme still carry on the login and authentication process. Eventually, the HA will verify that the MU is illegal and terminates the authentication phase in step L6. The step L2 to L6 are unnecessarily operations and result in extra communication and computational costs.

One possible solution to the problem is that the MU's entered information (i.e. ID_{MU} and PW_{MU}) should be verified in the early stages of the login phase. Then it can avoid the additional computational and communication overhead in the login phase. Finally, because of this information verfication problem, Niu et al.'s scheme unable to achieve secure authentication at login phase.

2.2.2 Niu et al.'s Scheme Unable to Resist Replay Attack

Suppose a mobile user MU_i visits a new foreign agent FA_j and sends a login message to it, a hostile FA_j can impersonate this mobile user through replaying its login information to access the services from other foreign network like FA_{j+1}.

The detailed steps for the above problem is discussed below. Suppose a MU_i submits login request message $\{A, SID, C_1, T_{MU}, ID_{HA}\}$ to FA_j. After receiving the information, the FA_j impersonates MU_i to forward MU_i's login request to another foreign agent FA_{j+1}. Since the login request does not include the sender's information, the FA_{j+1} would consider that this is a message from a mobile user rather than a foreign network. The message will always be maliciously used by FA_j in its lifetime of the timestamp T_{MU}, then FA_j and FA_{j+1} send the same message to HA respectively in the same time threshold. Next, FA_j generates two session keys for MU_i and FA_{j+1} which the values of the two session keys are the same and equal $sk = h(abP)$. In update session key phase, FA_j can also computes the same session key k_i as MU_i's session key at ith session. Finally, Niu et al.'s scheme unable to resist replay attack even if they have adopted the timestamp.

Note the FA_{j+1} will find that it is under the relay attack only the information transportation time exceeds the preset lifetime. But choosing a proper timestamp's lifetime is a difficult work in some real environments, so we should take this security issue into account.

Table 2 Performance comparisons

	MU	*FA*	*HA*
Our scheme	4H+1S+2EC	2H+1S+3A+2EC	3H+4A+1EC
Niu and Li [9]	4H+1S+3EC	2H+1S+2A+2EC	4H+2A+1EC
Zhao et al. [11]	7H+1S+3EC	2H+3S+2A+3EC	6H+2S+2A+3EC
He et al. [3]	8H+3S	2H+2S+2A	4H+2S+3A
Farash et al. [15]	5H	1H+2S	5H+2S

H hash operation, *S* symmetric encryption/decryption, *A* asymmetric encryption/decryption, *EC* ECC multiplication operation

2.2.3 Niu et al.'s Scheme Unable to Complete Login and Authentication Phase When Large Number of MUs Visit a FA Simultaneously

In Niu et al.'s scheme, suppose that in a short time interval, there are large number of mobile users from a same home agent, say HA_i, roam to a foreign agent, say FA_j, and send login request messages to FA_j for accessing service at the same time. The FA_j passes all access request messages to their home agent, HA_i, and then HA_i verify these messages and generates the reply message $\{C_2, Cert_{HA}, Sig_{HA}, T_{HA}\}$ for every login request message. Next, the HA_i sends these reply messages to FA_j in a short time interval. Note that every reply message $\{C_2, Cert_{HA}, Sig_{HA}, T_{HA}\}$ does not contain any information about *MU*, that result in the FA_j cannot establish the one to one correspondence relation between reply messages and *MU*s when receiving so many reply messages from HA_i. Finally, the Niu et al.'s scheme cannot work in this circumstance.

2.2.4 Niu et al.'s Scheme Unable to Prevent the Potential DoS Attack

When a *MU* wants to get the service of a *FA*, the *MU* should submits the login request message $\{A, SID, C_1, T_{MU}, ID_{HA}\}$ to *FA* first. Because the timestamp T_{MU} and the number a are constantly changing, the information $\{A, SID, C_1, T_{MU}\}$ are also different in every login request message. Then the *FA* does not verify the login message and directly forward it to *HA*. So if the smart card gets viruses or malicious using by attacker, it can launch DoS attack by generating large number of illegal login request messages to *FA* and *HA*. That will rapidly run out of the resources of *FA* and *HA* and force them to stop providing services to legitimate *MU*s.

3 Our Proposed Scheme

In this section, we propose an improvement user authentication scheme for roaming environment on account of the security of elliptic curve cryptosystem(ECC). The proposed scheme fixes the vulnerabilities and security weaknesses pointed out in Niu et al.'s scheme while remaining its advantages. The new scheme has four phases: the initialization phase, the registration phase, the authentication and session key establishment phase, and the update session key phase. Table 1 lists the notations and corresponding description used in our scheme.

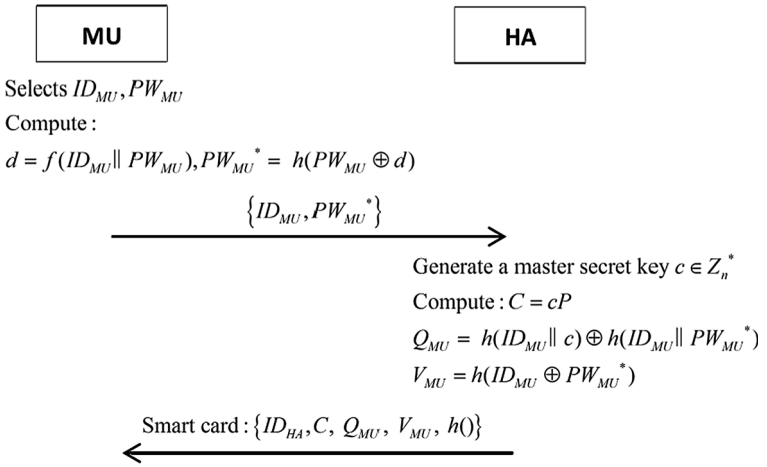

Fig. 4 Registration phase of our scheme

3.1 Preliminaries

In this section, we will review some basic knowledge of elliptic curve cryptosystem(ECC). More details of ECC refer to [24].

3.1.1 Elliptic Curve Cryptosystem

Comparing with other non-ECC cryptography, ECC requires a smaller key size and less time to achieve equivalent security. The equation $E_P(a,b) : y^2 \equiv x^3 + ax + b (\text{mod } p)$ over the prime finite field F_p^* is defined to be elliptic curve equation, where p is a big prime number, $a, b \in F_p^*$ and $4a^3 + 27b^2 \neq 0 \ (\text{mod } p)$. All the points $(x, y) \in F_p^* \times F_p^*$ satisfying the equation $E_P(a,b)$ make up an elliptic curve. The point multiplications kP over $E_P(a,b)$ is defined as $k \cdot P = P + P + \ldots + P(k \text{ times})$, where $k \in F_p^*, P \in E_P(a,b)$.

3.1.2 Related Cryptographic Assumptions

We suppose that the following difficult problems cannot be solved in polynomial time.

(1) *elliptic curve discrete logarithm problem(ECDLP)*: Given two points $P, Q \in E_P(a,b)$,it is hard to search an integer $k \in F_p^*$ such that $Q = k \cdot P$

(2) *elliptic curve computational Diffie-Hellman problem(ECDHP)*: Given three points $P, kP, mP \in F_p^*$, it is hard to calculate kmP over $E_P(a,b)$

3.2 Initialisation Phase

The process of initialization phase is the following: First, *HA* randomly selects an elliptic curve equation $E_P(a,b)$ and a base point P with the order n over $E_P(a,b)$, and releases the information $\{E_P(a,b), n, P\}$ as its public parameters. Then the *HA* and the *FA* generates their public and private key pair respectively. Suppose that the private key of *HA* and *FA*

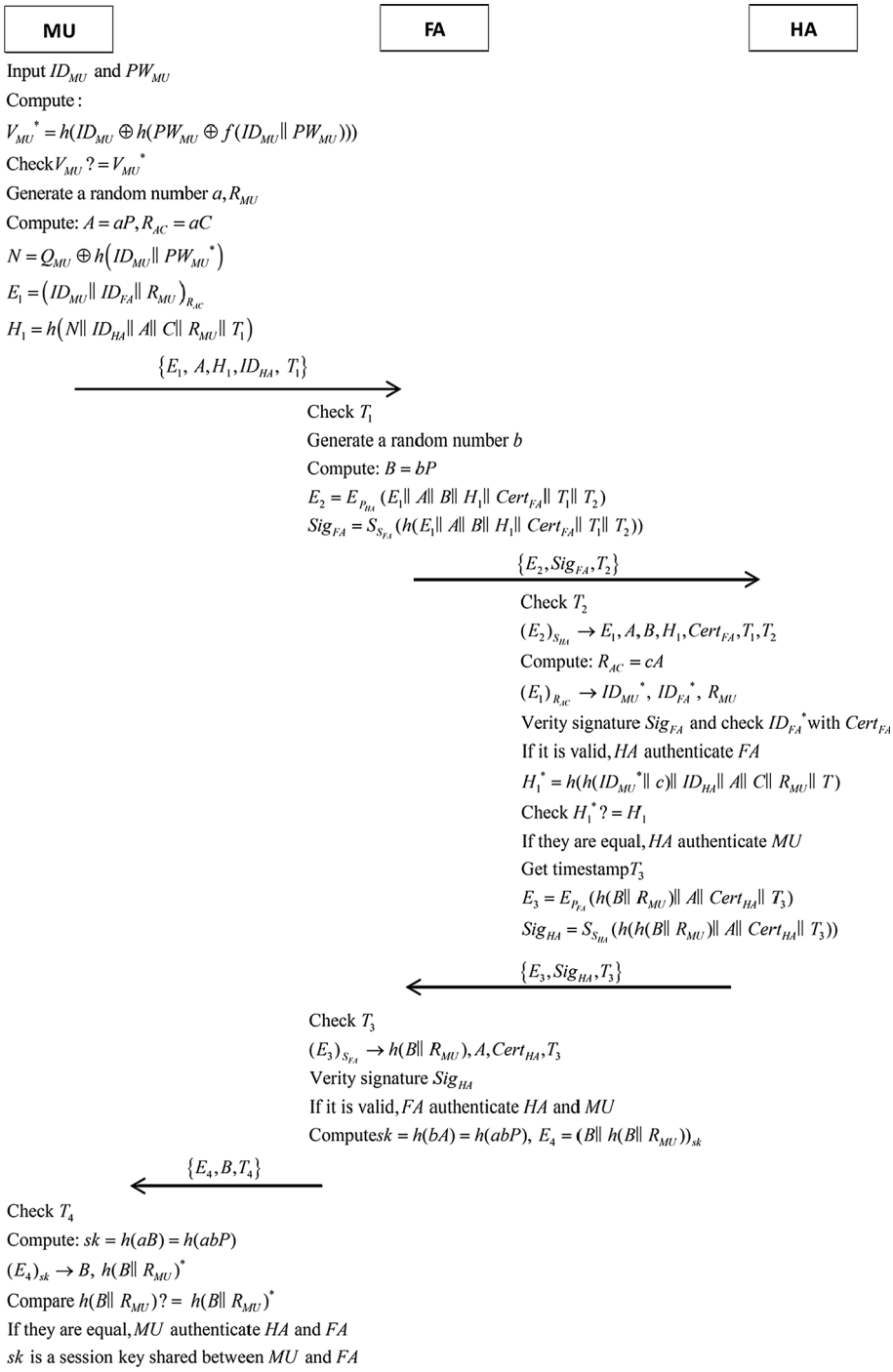

Fig. 5 Authentication and establishment of session key phase of our scheme

are $S_{HA} \in Z_n^*$ and $S_{FA} \in Z_n^*$, and the corresponding public key are $P_{HA} = S_{HA}P$ and $P_{FA} = S_{FA}P$. Afterwards, each *HA* and *FA* should publish its certificate $Cert_{HA}$ and $Cert_{FA}$. These published certificates must pass the authentication by a trusted Certificate Authority(CA).

3.3 Registration Phase

When a roaming mobile user *MU* wants to gain the services of a foreign network, the *MU* needs to register to his/her home agent *HA* first.

The registration process between *MU* and *HA* is depicted in Fig. 4.

Step R1 The *MU* generates a identity ID_{MU} and a corresponding password PW_{MU}, and computes a temporary value $d = f(ID_{MU} \| PW_{MU})$ where $f()$ is a number generating algorithm based on hardware encryption module. Then *MU* computes a hash value $PW_{MU}^* = h(PW_{MU} \| d)$ and transmits the message $\{ID_{MU}, PW_{MU}^*\}$ to its *HA* through a secure channel.

Step R2 Upon receipt of the above information $\{ID_{MU}, PW_{MU}^*\}$, *HA* firstly determines whether the identity ID_{MU} is exist in its user table. If the identity already exists, the *HA* notifies *MU* to send a new registration information with a new identity. Otherwise, the *HA* chooses a number $c \in Z_n^*$ as master secret key, and computes $C = cP, Q_{MU} = h(ID_{MU} \| c) \oplus h(ID_{MU} \| PW_{MU}^*), V_{MU} = h(ID_{MU} \oplus PW_{MU}^*)$. Then *HA* puts the message of $\{ID_{HA}, C, Q_{MU}, V_{MU}, h()\}$ into a smart card and distributes it to *MU* over a secure channel.

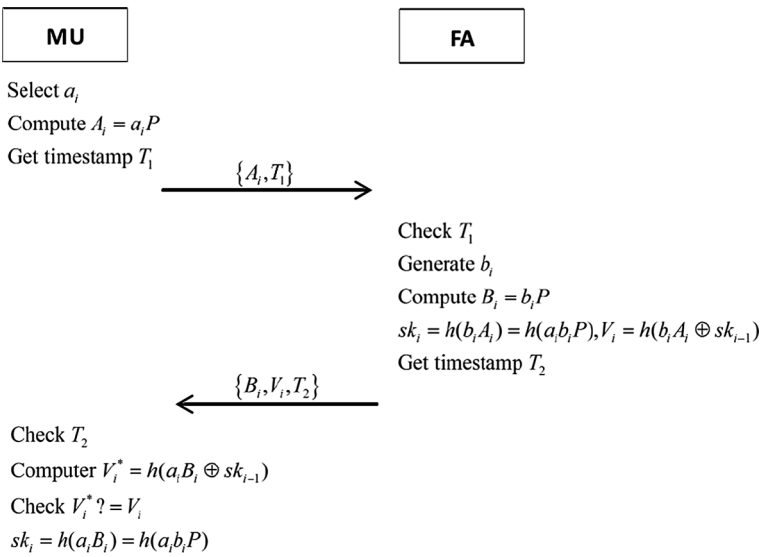

Fig. 6 Update session key phase of our scheme

3.4 Authentication and Establishment of Session Key Phase

When a MU visits a new foreign network FA, they need to mutual authentication before establish communication links. The following steps are performed during authentication and establishment of session key phase. Figure 5 illustrates this process in detail.

Step L1 MU enters the login information into the mobile device. Then the smart card in the mobile device generates the temporary value $d = f(ID_{MU} \| PW_{MU})$ and $V^*_{MU} = h(ID_{MU} \oplus h(PW_{MU} \| d))$, and compares the values of V^*_{MU} and V_{MU}. If the two values are equal, it means MU is a legitimate user. Otherwise the login process is going to be aborted immediately by smart card. Then the smart card randomly chooses a number $a \in Z^*_n$ and $R_{MU} \in Z^*_n$, for the sake of resist DoS attack, the a and R_{MU} will remain in the memories of mobile device for a short time(suppose that the average time of the authentication and establishment phase is T_{auth}, we choose the threshold time is $1.5T_{auth}$ by considering of transmission latency). Then the smart card caculates $A = aP, R_{AC} = aC, N = Q_{MU} \oplus h(ID_{MU} \| PW^*_{MU}), E_1 = (ID_{MU} \| ID_{FA} \| R_{MU})_{R_{AC}}, H_1 = h(N \| ID_{HA} \| A \| C \| R_{MU} \| T_1)$, where T_1 is the current timestamp. Then MU sends $\{E_1, A, H_1, ID_{HA}, T_1\}$ to FA.

Step L2 Upon receiving the login request message $\{E_1, A, H_1, ID_{HA}, T_1\}$ at time T_2, FA checks whether the time span between T_1 and T_2 is in a preset time threshold ΔT. (i.e., check if $T_2 - T_1 \leq \Delta T$). If not, FA terminates the phase. Otherwise the FA checks the message to prevent DoS attack, if the number of login requests from a same MU exceeds the threshold level in a preset time interval, the FA can judge it suffers from the DoS attack and terminates the login phase, and notifies MU's home agent. Otherwise, FA randomly selects a number $b \in Z^*_n$, and caculates $B = bP, E_2 = E_{P_{HA}}(E_1 \| A \| B \| H_1 \| Cert_{FA} \| T_1 \| T_2), Sig_{FA} = S_{S_{FA}}(h(E_1 \| A \| B \| H_1 \| Cert_{FA} \| T_2))$. Here P_{HA} is the HA's public key, S_{FA} is the FA's private key, $Cert_{FA}$ is the FA's certificate. Then FA submits $\{E_2, Sig_{FA}, T_2\}$ to HA.

Step L3 Upon receiving $\{E_2, Sig_{FA}, T_2\}$ from FA at time T_3, HA firstly checks the time difference among T_2 and T_3. Next, HA decrypts $(E_2)_{S_{HA}} =$

Table 3 Function comparisons

	Ours	Niu and Li [9]	Zhao et al. [11]	He et al. [3]	Farash et al. [15]
User's anonymity	Yes	Yes	Yes	Yes	No
Mutual authentication	Yes	No	Yes	Yes	No
Perfect forward secrecy	Yes	Yes	Yes	No	Yes
Location password verification	Yes	No	Yes	Yes	No
Resist off-line password guessing attack	Yes	Yes	Yes	No	No
Resist replay attack	Yes	No	No	Yes	No
Resist Denial of Service (DoS) attack	Yes	No	No	No	No
Resist authentication phase terminate	Yes	No	Yes	No	No

$(E_1, A, B, H_1, Cert_{FA}, T_1, T_2)$ using its private key and decrypts $(E_1)_{R_{AC}} = (ID^*_{MU}, ID^*_{FA}, R_{MU})$ using the computed $R_{AC} = cA$, then verifies the signature Sig_{FA} and checks if the ID^*_{FA} is a valid user using $Cert_{FA}$. If the two values are valid, *FA* is authenticated. After that, *HA* computes $H^*_1 = h(h(ID^*_{MU} \parallel c) \parallel ID_{HA} \parallel A \parallel C \parallel R_{MU} \parallel T_1)$. Then *HA* checks $H^*_1 ? = H_1$. If the result is equal, the *MU* is authenticated by *HA*. subsequently, *HA* caculates $E_3 = E_{P_{FA}}(h(B \parallel R_{MU}) \parallel A \parallel Cert_{HA} \parallel T_3), Sig_{HA} = S_{S_{HA}}(h(h(B \parallel R_{MU}) \parallel A \parallel Cert_{HA} \parallel T_3))$, where T_3 is the current timestamp. At last, *HA* sends $\{E_3, Sig_{HA}, T_3\}$ to *FA*.

Step L4 Upon receiving $\{E_3, Sig_{HA}, T_3\}$ from *HA*, *FA* verifies the freshness of T_3 first. Then *FA* decrypts $(E_3)_{S_{FA}} = (h(B \parallel R_{MU}), A, Cert_{HA}, T_3)$ and uses *HA*'s public key P_{HA} to verify the validity of the signature Sig_{HA}. If the result is valid, *HA* is authenticated which also means that *HA* claimed *MU* is a legitimate user. Next, *FA* generates a mutual and secret session key $sk = h(bA) = h(abP)$ with *MU* and $E_4 = (B \parallel h(B \parallel R_{MU}))_{sk}$, and sends $\{E_4, B, T_4\}$ to *MU* where T_4 is the current timestamp.

Step L5 Once the message $\{E_4, B, T_4\}$ is received by *MU*, he/she checks the freshness of T_4 first, then decrypts $(E_4)_{sk} = (B^*, h(B \parallel R_{MU})^*)$ using the computed session key $sk = h(aB) = h(abP)$. Then *MU* computes $h(B \parallel R_{MU})$ and checks whether $B^* ? = B$ and $h(B \parallel R_{MU})^* ? = h(B \parallel R_{MU})$. If both of them are equal, *FA* and *HA* are all authenticated by *MU*. Then *MU* confirms the shared session key is *sk* and can safely communicate with *FA*.

3.5 Update Session Key Phase

The shared session key between *MU* and *FA* must to be updated regularly for security reason if the *MU* stays in the *FA* all the time. *MU* and *FA* can use the following steps for updating their shared session key $sk_i (i = 2, \ldots, n)$ at the *i*th session. The details of update session key phase of our new scheme are shown in Fig. 6.

Step U1 *MU* randomly chooses $a_i \in Z^*_n$ and caculates $A_i = a_i P (i = 2, \ldots, n)$. Then, *MU* generates a timestamp T_1 and sends $\{A_i, T_1\}$ to *FA*.

Step U2 When receiving the information at time T_2, *FA* firstly checks the freshness of T_1. If it fails validation, *FA* stops the process immediately. Otherwise, *FA* generates a new random number $b_i \in Z^*_n$ and caculates $B_i = b_i P (i = 2, \ldots, n)$. Next, *FA* generates $sk_i = h(b_i A_i) = h(a_i b_i P)$ as new session key and $V_i = h(a_i b_i P \oplus a_{i-1} b_{i-1} P)$ and submits $\{B_i, V_i, T_2\}$ to *MU*.

Step U3 Upon receiving $\{B_i, V_i, T_2\}$ from *FA*, *MU* firstly checks the freshness of T_2. If the time difference is within the allowable range, *MU* computes $V^*_i = h(a_i B_i \oplus a_{i-1} B_{i-1}) = h(a_i b_i P \oplus a_{i-1} b_{i-1} P)$ and checks whether $V^*_i = V_i$. If so, *MU* generates a new session key $sk_i = h(a_i B_i) = h(a_i b_i P)$ and replaces the old session key sk_{i-1} with sk_i.

4 Security Analysis of the Proposed Scheme

In this section, we discuss some security characteristics and efficiency of our new user authentication scheme. We mainly divide it into seven aspects.

4.1 Ability to Provide User Anonymity

We can obtain the *MU*'s anonymity from using symmetric encryption technique and hash function in the new protocol. Suppose that the attacker steals the mobile device and has extracted the secrets $\{ID_{HA}, C, Q_{MU}, V_{MU}, h()\}$ by analyzing the communication messages or the energy consumption of the mobile device [25, 26], but without konwing the the secret key c and the algorithm $f()$, he/she cannot get the secret information such as *MU*'s real identity and *MU*'s password. Assume the attacker eavesdrops the messages transmitting among *MU*, *FA* and *HA*. Based on the ECDLP problem, the attacker cannot obtain the random a from A and thus cannot obtain ID_{MU}, R_{MU} from E_1. Meanwhile the attacker cannot to get the moving history and current position of *MU* because the random value a is adopted, which is constantly changing for each login. Furthermore, because the these random variables a, R_{MU} and T_1 are dynamically changed in different login request messages, the message $\{E_1, A, H_1, T_1\}$ is also different for each login.

In the login phase of our new scheme, the random number a, R_{MU} will not change in a preset time interval, that will not reduce *MU*'s anonymity because a legal *MU* does not send the login information frequently. A legal *MU* sends the login request message only once for getting services while an adversary sends large number of messages to *FA* in a short time interval for the purpose of DoS attack.

Hence, the proposed scheme can provide user's anonymity.

4.2 Ability to Mutual Authentication and Prevent Impersonation Attacks

The new scheme can realize mutual authentication among *MU*, *HA* and *FA* and prevent impersonation attacks. The details are as following:

(1) Mutual authentication between *MU* and *HA*
In the step L3 of authentication stage, *HA* can verify the identity of *MU* if ID^*_{MU} is exist and the values of the computed H^*_1 and the recevied H_1 are equal. On the other hand, because only the *HA* has authority to get R_{MU} and B at the same time, so *MU* can authenticate *HA* in step L5 by checking $h(B \parallel R_{MU})^{*}? = h(B \parallel R_{MU})$. So *MU* and *HA* can achieve mutual authentication.

(2) Mutual authentication between *FA* and *HA*
FA and *HA* can perform mutual authentication in step L3 and L4 of the authentication stage. *HA* can verify the identity of *FA* by checking whether *FA*'s signature Sig_{FA} is equal $S_{P_{FA}}(h(E_1 \parallel A \parallel B \parallel H_1 \parallel Cert_{FA} \parallel T_1 \parallel T_2))$ using *FA*'s public key P_{FA} and ID^*_{FA} is valid using *FA*'s certificate $Cert_{FA}$. *HA* also can be authenticated by *FA* if its signature Sig_{HA} is equal to $S_{P_{HA}}(h(h(B \parallel R_{MU}) \parallel A \parallel Cert_{HA} \parallel T_3))$.

(3) Mutual authentication between *MU* and *FA*
Because the *HA* has authenticated *MU*'s valid in step L3 before *HA* sends the reply message, the *FA* can simultaneously authenticate *HA* and *MU* with the message $\{E_3, Sig_{HA}, T_3\}$ from *HA* in step L4. *MU* also can authenticated *FA* by checking $h(B \parallel R_{MU})^{*}? = h(B \parallel R_{MU})$ which from *HA*.

4.3 Ability to Meets the Security Requirement for Perfect Forward Secrecy

The capability of forward secrecy means that even if an adversary breaks the whole passwords of the participants, he/her still cannot compromise the previous session keys.

The shared session key $sk = h(abP)$ in the new scheme is generated by two numbers a and b which belong to the MU and the FA respectively, and has nothing to do with the system master key c. The random number cannot be obtain from $A = aP, B = bP, R_{AC} = aC = cA$ based on the security of ECDLP and ECDHP problem. So even though the master key c is compromised or an adversary gets the whole passwords of the participants, the transmitted messages and the previous established session keys will not be leaked. Hence, our new scheme can achieve strong forward secrecy.

4.4 Ability to Resist Off-Line Password Guessing Attack with Smart Card Security Breach

In the new scheme, we assumed that the attacker has obtained the information $\{ID_{HA}, C, Q_{MU}, V_{MU}, h()\}$ from the stolen MU's smart card and has eavesdropped a previous transmitted messages $\{E_1, A, H_1, ID_{HA}, T_1, E_2, Sig_{FA}, T_2, E_3, Sig_{HA}, T_3, E_4, B, T_4\}$. Note that the password of MU only appear in Q_{MU}, V_{MU} and H_1, which Q_{MU}, V_{MU} is stored in smart card. Clearly if the values ID_{MU}, d and the master key c are unknown, the attacker cannot launch this type of attack.

4.5 Ability to Prevent Replay Attack

Our proposed scheme can protect foreign agent against the normal impersonal attack by replaying previously sent login request due to the the identity ID_{FA_j} was employed. As mentioned in the previous section, we suppose that a MU sends the message $\{E_1, A, H_1, ID_{HA}, T_1\}$ to a foreign agent, say FA_j. Upon receiving the message, FA_j impersonates the MU to forward its login request to another network, say FA_{j+1}. Then FA_{j+1} pass the received information to HA. To be more precise, FA_{j+1} submits message $\{E_2, Sig_{FA_{j+1}}, T_2\}$ to HA, where $E_2 = E_{P_{HA}}(E_1 \parallel A \parallel B \parallel H_1 \parallel Cert_{FA_{j+1}} \parallel T_1 \parallel T_2)$ and $E_1 = (ID_{MU} \parallel ID_{FA_j} \parallel R_{MU})_{R_{AC}}$. In the authentication phase of the new scheme, HA computes $R_{AC} = cA$ and decrypts E_1 to obtain ID_{FA_j}. HA can authenticate FA's valid by comparing ID_{FA_j} with the identity in the certificate $Cert_{FA_{j+1}}$. If the values of them are not the same, HA stops the authentication phase and sends a message "The user is illegal" to FA_{j+1}. After receiving the message "The user is illegal" from HA, FA_{j+1} will terminate the authentication processing with FA_j. Eventually, FA_j cannot impersonate other mobile user(e.g. MU) and establish a session with FA_{j+1}. Hence, our new scheme can effectively prevent the messages replay attacks described in Sect. 2.

4.6 Ability to Prevent Potential DoS Attack

With Denial-of-Service(DoS) attack [27], the adversaries send large amounts of bogus login message to network servers so as to rapidly consume the resources of FA and HA and render them unable to provide services to legitimate MUs. Most of the three-party roaming handover authentication [1–10] requires the FA to retransmit all the login request to HA unconditionally, then the attackers can easily start DoS attack on HA via FA. One way to

thwart the DoS attack is that the *FA* can verify the received login request message before forwarding it.

Our scheme proposes a method which can prevent the potential DoS attack. All the smart card distributed by network servers should preset a time threshold(e.g. $1.5T_{auth}$), and the random number a and R_{MU} will keep in the mobile device's memories within this period, that is the content $\{E_1, A, H_1, ID_{HA}\}$ of sending login request message will not change too. Suppose a mobile user, say MU_i, catches a virus or malicious use by an adversary, it flood a lot of illegal access request messages $\{E_1, A, H_1, ID_{HA}, T_1\}$ to a foreign agent, say FA_j. When receiving the message from MU_i, the FA_j firstly verifies these messages. If there are large number of messages contain the same $\{E_1, A, H_1, ID_{HA}\}$ in preset time threshold, FA_j can judge it is suffering from DoS attack. Subsequently, FA_j abandons all the messages from the MU_i and terminates the session with MU_i and sends a notify "MU_i has been compromised" to MU_i's home agent. Finally, our scheme can effectively prevent the potential DoS attack.

4.7 Ability to Avoid Authentication Phase Interrupt When Large Number of *MU*s Visit a *FA*

In the circumstances, we suppose that there are a lot of *MU*s from a same *HA* visit a *FA*, they send their login request messages to *FA* respectively for getting service, and the *FA* pass all the messages to *HA*, then the *HA* will reply to all the messages in a short time after verify those messages. Note that every reply message $\{E_3, Sig_{HA}, T_3\}$ from *HA* contains the information of *MU*, the *FA* could decrypt E_3 and get A, which is sent by *MU*. So the *FA* can map every message to every *MU* by A and b because of they are all random number derived from *MU* and *FA* respectively.

Hence, the proposed scheme can complete the login and authentication phase when massive user roam a same *FA* because the A and b were employed.

5 Performance Comparison and Functionality Analysis

In this section, we firstly compares the performance functionality of the new scheme with other related works. Table 2 shows the performance comparisons results. Some symbols used in Table 2 are as follows: H denotes the one-way hash function operation(i.e., SHA-1 [28]); S denotes the symmetric encryption/decryption operation(i.e., AES [29]); A denotes the encryption/decryption operation using a pair of asymmetric keys(i.e., RSA [30]); and EC means the ECC multiplication operation. Table 3 lists the functionality comparisons among the new scheme and other related works. As the Table 3 shows, our scheme possesses a lot of outstanding features and is more safe and more robust than others.

6 Conclusions

In wireless mobility networks, roaming user authentication is an important task, and a lot of solution schemes have been put forward to enhance the security and efficiency in authentication. In this paper, we analyse Niu et al.'s scheme in detail and found that although they claimed their protocol can protect the networks against some known attacks, their scheme still has several weaknesses. For the sake of improving its security in wireless communications networks, we present a novel roaming authentication scheme based on

ECC. Security analysis has indicated that our protocol is able to resist various known attacks like impersonation attack, replay attack and DoS attack. Meanwhile, the new protocol also support mutual authentication among all kinds of entities and provide user anonymity in mobile networks. The functionality comparisons and performance comparison also demonstrate that our new scheme is more suitable for wireless communications networks.

References

1. Hsiang, H.-C., & Shih, W.-K. (2009). Improvement of the secure dynamic id based remote user authentication scheme for multi-server environment. *Computer Standards & Interfaces*, *31*(6), 1118–1123.
2. Chang, C.-C., Lee, C.-Y., & Chiu, Y.-C. (2009). Enhanced authentication scheme with anonymity for roaming service in global mobility networks. *Computer Communications*, *32*(8), 611–618.
3. He, D., Mab, M., Zhang, Y., Chen, C., & Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications. *Computer Communications*, *34*(8), 367–374.
4. Das, A. K. (2013). A secure and effective user authentication and privacypreserving protocol with smart cards for wireless communications. *Networking Science*, *2*, 12–27.
5. Zhu, J., & Ma, J. (2004). A new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Consumer Electronics*, *51*(21), 230–234.
6. Lee, C. C., Hwang, M. S., & Liao, I. E. (2006). Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Industrial Electronics*, *53*(5), 1683–1687.
7. Wu, C.-C., Lee, W.-B., & Tsaur, W.-J. (2008). A secure authentication scheme with anonymity for wireless communications. *IEEE Communications Letters*, *12*(2), 722–723.
8. Li, C.-T., & Lee, C.-C. (2012). A novel user authentication and privacy preserving scheme with smart cards for wireless communications. *Elsevier*, *55*, 35–44.
9. Niu, J., & Li, X. (2014). A novel user authentication scheme with anonymity for wireless communications. *Security and Communication Networks*, *7*(7), 1467–1476.
10. Yoon, E.-J., Yoo, K.-Y., & Ha, K.-S. (2011). A user friendly authentication scheme with anonymity for wireless communications. *Computers and Electrical Engineering*, *37*, 356–364.
11. Zhao, D., Peng, H., Li, L., & Yang, Y. (2014). A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, *78*, 247–269. 7.
12. Kang, M., Rhee, H. S., & Choi, J. Y. (2011). Improved user authentication scheme with user anonymity for wireless communications. *Ieice Trans Fundamentals*, *94*(2), 860–864.
13. Hu, B., Xie, Q., Bao, M., & Dong, N. (2014). Improvement of user authentication protocol with anonymity for wireless communications. *Kuwait Journal of Science*, *41*(1), 155–169.
14. Wen, F., Susilo, W., & Yang, G. (2014). A robust smart cardbased anonymous user authentication protocol for wireless communications. *Security & Communication Networks*, *7*(6), 987–993.
15. Farash, M. S., Chaudhry, S. A., Heydari, M., Sadough, S. M. S., Kumari, S., & Khan, M. K. (2015). A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. *International Journal of Communication Systems*. doi:10.1002/dac.3019.
16. Shin, S., Yeh, H., & Kim, K. (2015). An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks. *Peer-to-Peer Networking and Applications*, *8*(4), 1–10.
17. Wen, F., Susilo, W., & Yang, G. (2013). A secure and effective anonymous user authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, *73*(3), 993–1004.
18. Chung, Y., Choi, S., Lee, Y., Park, N., & Won, D. (2016). An enhanced lightweight anonymous authentication scheme for a scalable localization roaming service in wireless sensor networks. *Sensors*, *16*(10), 1653.
19. Djellali, B., Belarbi, K., Chouarfia, A., & Lorenz, P. (2015). User authentication scheme preserving anonymity for ubiquitous devices. *Security & Communication Networks*, *8*(17), 3131–3141.
20. Jiang, Q., Khan, M. K., Lu, X., Ma, J., & He, D. (2016). A privacy preserving three-factor authentication protocol for e-health clouds. *Journal of Supercomputing*, *72*(10), 3826–3849.
21. Xiong, H., Wang, X., & Li, F. (2012). Security flaw of an improved user authentication scheme with user anonymity for wireless communications. *IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences*, *95-A*, 256–258.

22. Kang, D., Mun, J., Lee, D., & Won, D. (2015). Cryptanalysis of user authentication scheme preserving anonymity for ubiquitous devices. In: D. S. Park, H. C. Chao, Y. S. Jeong, & J. Park (Eds.), *Advances in Computer Science and Ubiquitous Computing*, Lecture Notes in Electrical Engineering. (Vol. 373, pp. 309–315)
23. Irshad, A., & Chaudhry, S. A. (2016). Comments on a privacy preserving three-factor authentication protocol for e-health clouds. *Journal of Supercomputing*, *4*(73), 1504–1508.
24. Hankerson, D., Menezes, A., & Vanstone, S. (2004). *Guide to elliptic curve cryptography*. Berlin: Springer.
25. Kocher, P., Jaffe, J., & Jun, B. (1999). Differential power analysis. In: M. Wiener (Ed.), *Advances in Cryptology (CRYPTO'99), Lecture Notes in Computer Science* (Vol. 166, pp. 388–397). Heidelberg: Springer.
26. Ts, M., Ea, D., & Rh, S. (2002). Examining smartcard security under the threat of power analysis attacks. *IEEE Transactions on Computers*, *51*(5), 541–552.
27. Needham, R. M. (1993). Denial of service. In *Proceedings of the 1st ACM conference on computer and communications security*, series CCS '93 (pp. 151–153). New York, NY, USA: ACM. http://doi.acm.org/10.1145/168588.168607
28. Eastlake 3rd, D., & Jones, P. (2001). US Secure Hash Algorithm 1 (SHA1), RFC 3174. doi:10.17487/RFC3174.
29. Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES-the advanced encryption standard*. Berlin: Springer.
30. Buchmann, J. (2004). *Introduction to cryptography* (2nd ed.). New York: Springer.

Rui Chen received the B.S. degree in computer science from Sichuan Normal University, Chengdu, P. R. China in 2004, and M.S. degree in computer software and theory from Sichuan Normal University in 2007, and currently studying for the Ph. D. degree in computer science from Sichuan University, Chengdu, P. R. China, in 2012. Now he is an lecturer of the College of Computer Science, Sichuan Normal University, Chengdu. His current interests include security protocols and mobile wireless network security, etc.

Dezhong Peng received the BS degree in applied mathematics, the MS and PhD degrees in computer software and theory from the University of Electronic Science and Technology of China, Chengdu, China, in 1998, 2001, and 2006, respectively. From 2001 to 2007, he was with the University of Electronic Science and Technology of China as an assistant lecturer and a lecturer. He was a Postdoctoral Research Fellow at the School of Engineering, Deakin University, Australia from 2007 to 2009. Currently, he is a Professor at the Machine Intelligence Laboratory, College of Computer Science, Sichuan University, Chengdu, China. His research interests include blind signal processing and neural networks. He is a member of the IEEE.