Wireless Pers Commun (2014) 74:229–243
DOI 10.1007/s11277-013-1282-x

Cryptanalysis and Improvement of an Anonymous Authentication Protocol for Wireless Access Networks

Debiao He · Yuanyuan Zhang · Jianhua Chen

Published online: 18 June 2013

Abstract Authentication protocols with anonymity attracted wide attention since they could protect users' privacy in wireless communications. Recently, Hsieh and Leu proposed an anonymous authentication protocol based on elliptic curve Diffie–Hellman problem for wireless access networks and claimed their protocol could provide anonymity. However, by proposing a concrete attack, we point out that their protocol cannot provide user anonymity. To overcome its weakness, we propose an improved protocol. We also provide an analysis of our proposed protocol to prove its superiority, even though its computational cost is slightly higher.

Keywords Wireless networks · Authentication · Anonymity · Elliptic curve Diffie–Hellman

1 Introduction

With the development of the mobile technology and communication technology, wireless networks have been widely used in our life. To provide secure roaming service for a user between the home network and a visited foreign network, authentication protocols for wireless access networks are required. In a roaming scenario, there are three parties, i.e. a mobile station (MS), a home agent (HA) and a foreign agent (FA). When a MS roams into a foreign network, the MS and the FA could authenticate each other under the help of HA. At the same time, the MS and the FA generate a session key for future communication.

D. He (✉) · Y. Zhang · J. Chen
School of Mathematics and Statistics,
Wuhan University, Wuhan, China
e-mail: hedebiao@163.com

D. He
State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China

Anonymity is an important property of roaming services. The disclosure of a user's identity may allow unauthorized entities to track his movement history and current location. Any unauthorized illegal access to information related to users' location without their permission can be a serious violation of privacy. To protect users' privacy, many authentication protocols [1–9] for wireless networks with anonymity have been proposed. However, the performance and security of those protocols are not satisfying. In 2004, Zhu and Ma [10] proposed an efficient authentication protocol based on the hash function and smart cards to preserve user anonymity. However, Lee et al. [11] found that Zhu and Ma's protocol cannot provide mutual authentication and is vulnerable to the forgery attack. Chen et al. [12] also pointed out that Zhu et al.'s protocol cannot provide anonymity. To enhance security, Yang et al. [13] proposed a new authentication protocol with anonymity for wireless networks using symmetric cryptosystems. Unfortunately, Chen et al. [12] found that Yang et al.'s protocol [13] cannot withstand the password guessing attacks. Chen et al. also proposed an improved protocol to overcome these weaknesses. However, Hsieh and Leu [14] pointed out that Chen et al.'s protocol is vulnerable to the denial of authentication attack. To improved security, they also proposed an improved protocol based on the elliptic curve Diffie-Hellman problem (ECDLP) [15]. They claimed that their protocol could withstand various attacks and could provide anonymity. However, we found that a malicious user in their protocol could easily obtain other users' identities. Their protocol cannot preserve user anonymity. This paper first demonstrates the weakness in their protocol and then proposed an improved protocol to overcome the above weakness.

The organization of the paper is sketched as follows. Section 2 gives a brief review the protocol of Hsieh and Leu. Section 3 discusses the cryptanalysis of Hsieh et al.'s protocol. Section 4 proposes an improved protocol. Sections 5 and 6 analyze the security and performance separately. At last, some conclusions are proposed in Sect. 7.

2 Review Hsieh and Leu's Protocol

For convenience, the notations used in this paper are described as follows.

- q : The field size (may be either an odd prime p or 2^m, where m is a prime);
- F_q : A finite field;
- $E(F_q)$: An elliptic curve define on the finite field F_q;
- G : A base (generating) point consisting of prime order on $E(F_q)$;
- n : The order of the point G;
- HA : A home agent;
- FA : A foreign agent;
- MS : A mobile station;
- ID_{HA} : The identity of HA;
- ID_{FA} : The identity of FA;
- ID_{MS} : The identity of MS;
- PW_{MS} : Then password of MS;
- k_{FH} : A secret key shared by the FA and the HA;
- x, y : The secret keys of HA;
- $(M)_k$: Ciphertext M encrypted with the symmetric key k;
- $h(\cdot)$: A secure hash function;

Hsieh and Leu's protocol consists of three phases: the registration phase, the ticket-issuing phase, and the ticket authentication phase. The detail is described as follows.

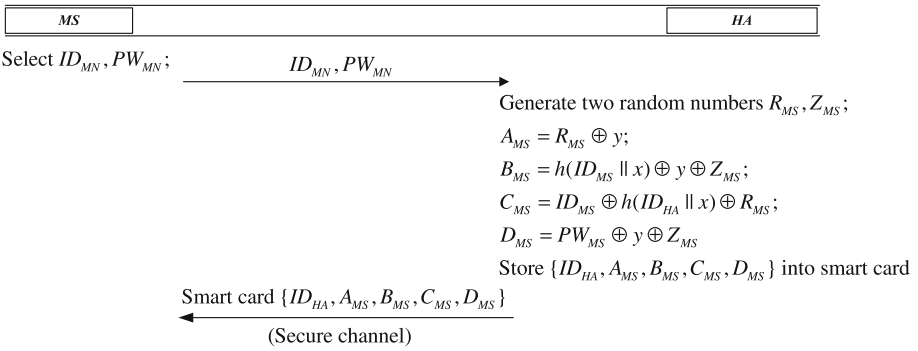


Fig. 1 The registration phase of Hsieh and Leu's protocol

2.1 Phase I: The Registration Phase

To be a legal user, as shown in Fig. 1, a mobile station MS will register in the home agent HA through the following steps.

(1) MS chooses his identity ID_{MS} and password PW_{MS} freely. Then, MS sends ID_{MS} and PW_{MS} to HA through a secure channel.
(2) Upon receiving ID_{MS} and PW_{MS}, HA generates two random number R_{MS} and Z_{MS}. HA computes $A_{MS} = R_{MS} \oplus y$, $B_{MS} = h(ID_{MS}, x) \oplus y \oplus Z_{MS}$, $C_{MS} = ID_{MS} \oplus h(ID_{HA}, x) \oplus R_{MS}$ and $D_{MS} = PW_{MS} \oplus y \oplus Z_{MS}$. At last, HA stores ID_{HA}, A_{MS}, B_{MS}, C_{MS} and D_{MS} into a smart card and issues it to MS.

2.2 Phase II: The Ticket-Issuing Phase

When the MS roams into a foreign network, as shown in Fig. 2, he will register in the FA through the following steps.

(1) MS inputs PW_{MS} into his smart card. The smart card computes $y \oplus Z_{MS} = D_{MS} \oplus PW_{MS}$ and $h(ID_{MS}, x) = B_{MS} \oplus y \oplus Z_{MS}$. The smart cards generates two random number a and N_{MS}, computes $Q_{MS} = aG$, $E_{MS} = R_{MS} \oplus y \oplus N_{MS}$, $F_{MS} = h(ID_{MS}, x) \oplus Q_{MS}$ and $CID_{MS} = ID_{MS} \oplus h(ID_{HA}, x) \oplus R_{MS} \oplus N_{MS}$. At last, MS sends the message $M_1 = \{ID_{HA}, E_{MS}, F_{MS}, CID_{MS}\}$ to the FA.
(2) Upon receiving M_1, FA generates a random number b, computes $Q_{FA} = bG$. Then, FA sends $M_2 = \{ID_{FA}, E_{MS}, F_{MS}, CID_{MS}, (ID_{FA}, Q_{FA}, T_{FA})_{k_{FH}}\}$ to HA, where T_{FA} is the current timestamp.
(3) Upon receiving M_2, HA computes $R_{MS} \oplus N_{MS} = E_{MS} \oplus y$, $ID_{MS} = CID_{MS} \oplus h(ID_{HA}, x) \oplus R_{MS} \oplus N_{MS}$ and $Q_{MS} = F_{MS} \oplus h(ID_{MS}, x)$. HA obtains $(ID_{FA}, Q_{FA}, T_{FA})$ by decrypting $(ID_{FA}, Q_{FA}, T_{FA})_{k_{FH}}$. Then, HA checks the freshness of T_{FA}. If T_{FA} is not fresh, HA stops the session; otherwise, HA generates a random number c, computes $G_{MS} = h(h(ID_{MS}, x), Q_{MS}) \oplus cQ_{FA}$, $H_{MS} = h(h(ID_{MS}, x), Q_{MS}, cQ_{FA})$ and $I_{MS} = h(h(ID_{MS}, x), Q_{MS} + 1, cQ_{FA} + 1)$. At last, HA sends $M_3 = \{G_{MS}, H_{MS}, (T_{HA}, cQ_{MS}, I_{MS})_{k_{FH}}\}$ to FA, where T_{HA} is the current timestamp.
(4) Upon receiving M_3, FA gets $(T_{HA}, cQ_{MS}, I_{MS})$ by decrypting $(T_{HA}, cQ_{MS}, I_{MS})_{k_{FH}}$. FA checks the freshness of T_{HA}. If it is not fresh, FA stops the session; otherwise, FA generates a unique ticket identifier T_{ID} and a expired time T_{exp}, and computes $SK_1 = bcQ_{MS} = abcG$. At last, FA sends $M_4 = \{G_{MS}, H_{MS}, (T_{ID}, T_{exp})_{SK_1}\}$ to MS.

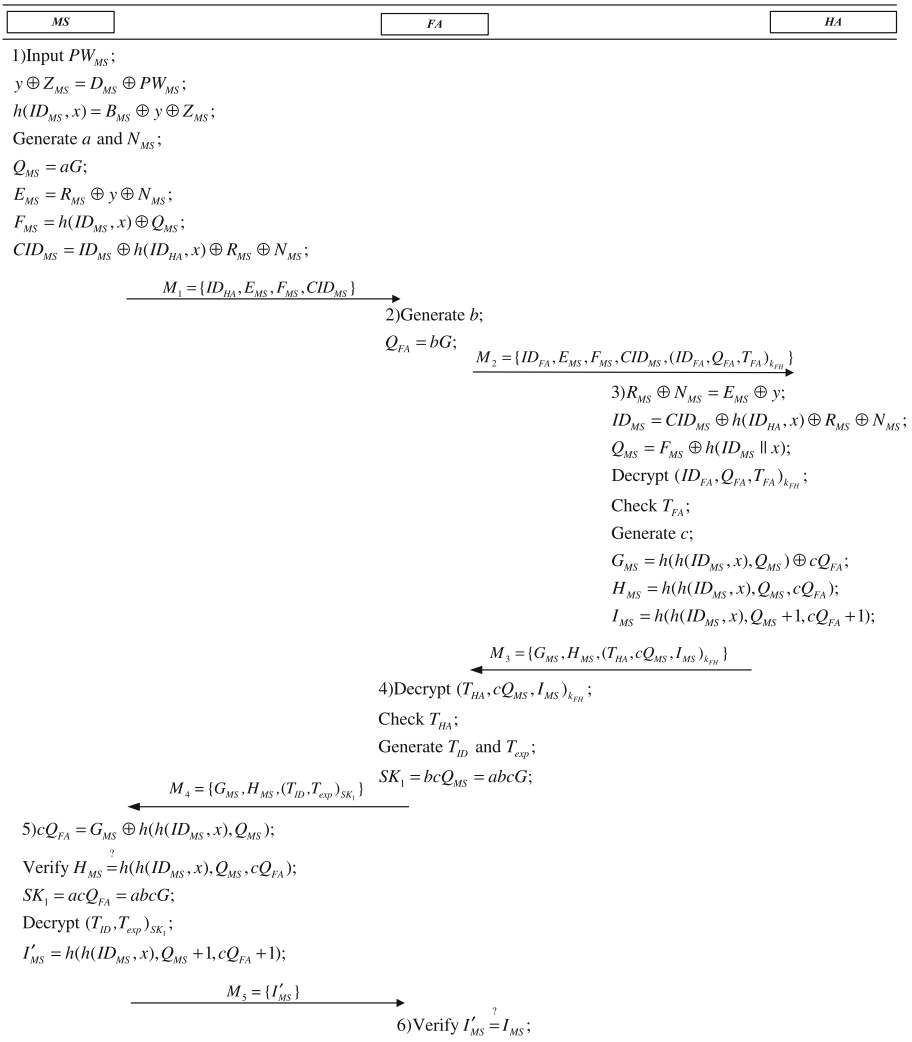


Fig. 2 The ticket-issuing phase of Hsieh and Leu's protocol

(5) Upon receiving M_4, MS computes $cQ_{FA} = G_{MS} \oplus h(h(ID_{MS}, x), Q_{MS})$ and checks whether H_{MS} and $h(h(ID_{MS}||x)||Q_{MS}||cQ_{FA})$ are equal. If they are not equal, MS stops the session; otherwise, MS computes $SK_1 = acQ_{FA} = abcG$ and gets T_{ID}, T_{exp} by decrypting $(T_{ID}, T_{exp})_{SK_1}$ using SK_1. At last, MS computes $I'_{MS} = h(h(ID_{MS}, x), Q_{MS} + 1, cQ_{FA} + 1)$ and sends $M_5 = \{I'_{MS}\}$ to FA.
(6) Upon receiving M_5, FA checks whether I'_{MS} and I_{MS} are equal. If they are not equal, FA stops the session. Otherwise, the user is authenticated.

2.3 Phase III: The Ticket Authentication Phase

After obtaining an anonymous ticket by decrypting $(T_{ID}, T_{exp})_{SK_{FA}}$, MS could login in FA through the ticket. Since a new session key will be compromised in the next session, each

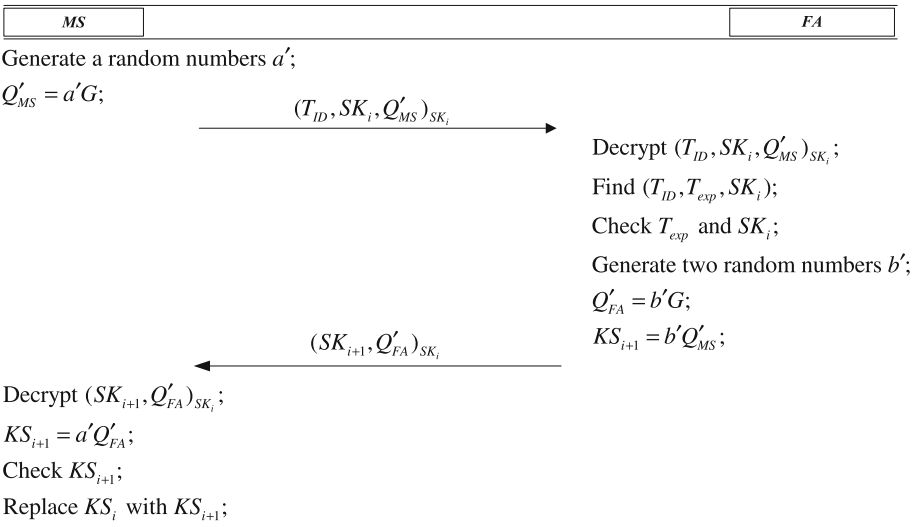


Fig. 3 The ticket authentication phase of Hsieh and Leu's protocol

anonymous ticket should be authenticated by FA when MS wants to carry out a secure and anonymous session. Figure 3 shows the ticket authentication phase in the ith session which is described as follows.

(1) MS generates a new random number a', computes $Q'_{MS} = a'G$ and sends $(T_{ID}, SK_i, Q'_{MS})_{SK_i}$ to FA.
(2) After receiving $(T_{ID}, SK_i, Q'_{MS})_{SK_i}$, FA decrypts it and deceives (T_{ID}, SK_i, Q'_{MS}). Then, FA uses T_{ID} to find the corresponding ticket entry (T_{ID}, T_{exp}, SK_i) in the ticket table. If T_{exp} is expired FA stops the session. Otherwise, FA checks whether SK_i in the ticket table and the decrypted one are equal. If they are not equal, FA stops the session. Otherwise, FA chooses a new random number b' and computes $Q'_{FA} = b'G$, $KS_{i+1} = b'Q'_{MS}$. Then, the FA sends the message $(SK_{i+1}, Q'_{FA})_{SK_i}$ to the MS.
(3) Upon receiving $(SK_{i+1}, Q'_{FA})_{SK_i}$, MS decrypts it and deceives (SK_{i+1}, Q'_{FA}). Then, MS computes $KS_{i+1} = a'Q'_{FA}$ and checks whether KS_{i+1} and the decrypted one are equal. If they are not equal, MS stops the session. Otherwise, MS replaces KS_i with KS_{i+1}.

3 Analysis of Hsieh and Leu's Protocol

Hsieh and Leu [14] claimed that their protocol could provide anonymity. However, in this section, we shall disprove their claim by giving a concrete attack. Let MS_A be a malicious mobile station. Then, he could get a legal smart card by registering in HA. Since the openness of the wireless networks, we could assume that MS_A has total control over the communication channel, which means that he can insert, delete, or alter any messages in the channel. MS_A could extract another mobile station MS's identity through the following two phases.

- *The first phase*

(1) MS_A inputs his password into his smart and generates a login message $M_1 = \{ID_{HA}, E_{MS_A}, F_{MS_A}, CID_{MS_A}\}$ through the steps in the ticket-issuing phase, where

$Q_{MS_A} = a_{MS_A}G$, $E_{MS_A} = R_{MS_A} \oplus y \oplus N_{MS_A}$, $F_{MS_A} = h(ID_{MS_A}, x) \oplus Q_{MS_A}$, $CID_{MS_A} = ID_{MS_A} \oplus h(ID_{HA}, x) \oplus R_{MS_A} \oplus N_{MS_A}$ and a_{MS_A} is a random number generate by MS_A.

(2) MS_A intercepts the message $M_1 = \{ID_{HA}, E_{MS_A}, F_{MS_A}, CID_{MS_A}\}$ and computes $h(ID_{HA}||x) \oplus y = ID_{MS_A} \oplus CID_{MS_A} \oplus E_{MS_A}$.

- *The second phase*

(1) When another mobile station MS of HA wants to register in FA, he will send a login message $M_1 = \{ID_{HA}, E_{MS}, F_{MS}, CID_{MS}\}$ through the steps in the ticket-issuing phase, where $Q_{MS} = a_{MS}G$, $E_{MS} = R_{MS} \oplus y \oplus N_{MS}$, $F_{MS} = h(ID_{MS}, x) \oplus Q_{MS}$, $CID_{MS} = ID_{MS} \oplus h(ID_{HA}, x) \oplus R_{MS} \oplus N_{MS}$ and a_{MS} is a random number generate by MS.

(2) MS_A intercepts the message $M_1 = \{ID_{HA}, E_{MS}, F_{MS}, CID_{MS}\}$ and computes $ID_{MS} = CID_{MS} \oplus E_{MS} \oplus h(ID_{HA}, x) \oplus y$.

Since $E_{MS} = R_{MS} \oplus y \oplus N_{MS}$ and $CID_{MS} = ID_{MS} \oplus h(ID_{HA}, x) \oplus R_{MS} \oplus N_{MS}$, then we have

$$\begin{aligned} &CID_{MS} \oplus E_{MS} \oplus (h(ID_{HA}, x) \oplus y) \\ &= (ID_{MS} \oplus h(ID_{HA}, x) \oplus R_{MS} \oplus N_{MS}) \oplus (R_{MS} \oplus y \oplus N_{MS}) \oplus (h(ID_{HA}, x) \oplus y) \\ &= ID_{MS} \oplus h(ID_{HA}, x) \oplus h(ID_{HA}, x) \oplus y \oplus y \oplus R_{MS} \oplus R_{MS} \oplus N_{MS} \oplus N_{MS} \\ &= ID_{MS} \end{aligned}$$

We can conclude that MS_A could get the identity of a legal mobile station MS. Therefore, Hsieh and Leu's protocol cannot provide anonymity.

4 Our Improved Protocol

Similar to Hsieh and Leu's protocol, our protocol also consists of three phases: the registration phase, the ticket-issuing phase, and the ticket authentication phase. The detail is described as follows.

4.1 Phase I: The Registration Phase

To be a legal user, as shown in Fig. 4, a mobile station MS will register in the home agent HA through the following steps.

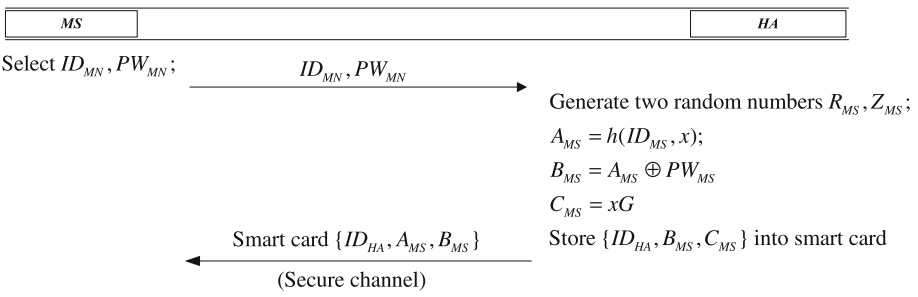


Fig. 4 The registration phase of our protocol

(1) MS chooses his identity ID_{MS} and password PW_{MS} freely. Then, MS sends ID_{MS} and PW_{MS} to HA through a secure channel.
(2) Upon receiving ID_{MS} and PW_{MS}, HA computes $A_{MS} = h(ID_{MS}, x)$ $B_{MS} = A_{MS} \oplus PW_{MS}$ and $C_{MS} = xG$. At last, HA stores ID_{HA}, A_{MS} and C_{MS} into a smart card and issues it to MS.

4.2 Phase II: The Ticket-Issuing Phase

When the MS roams into a foreign network, as shown in Fig. 5, he will register in the FA through the following steps.

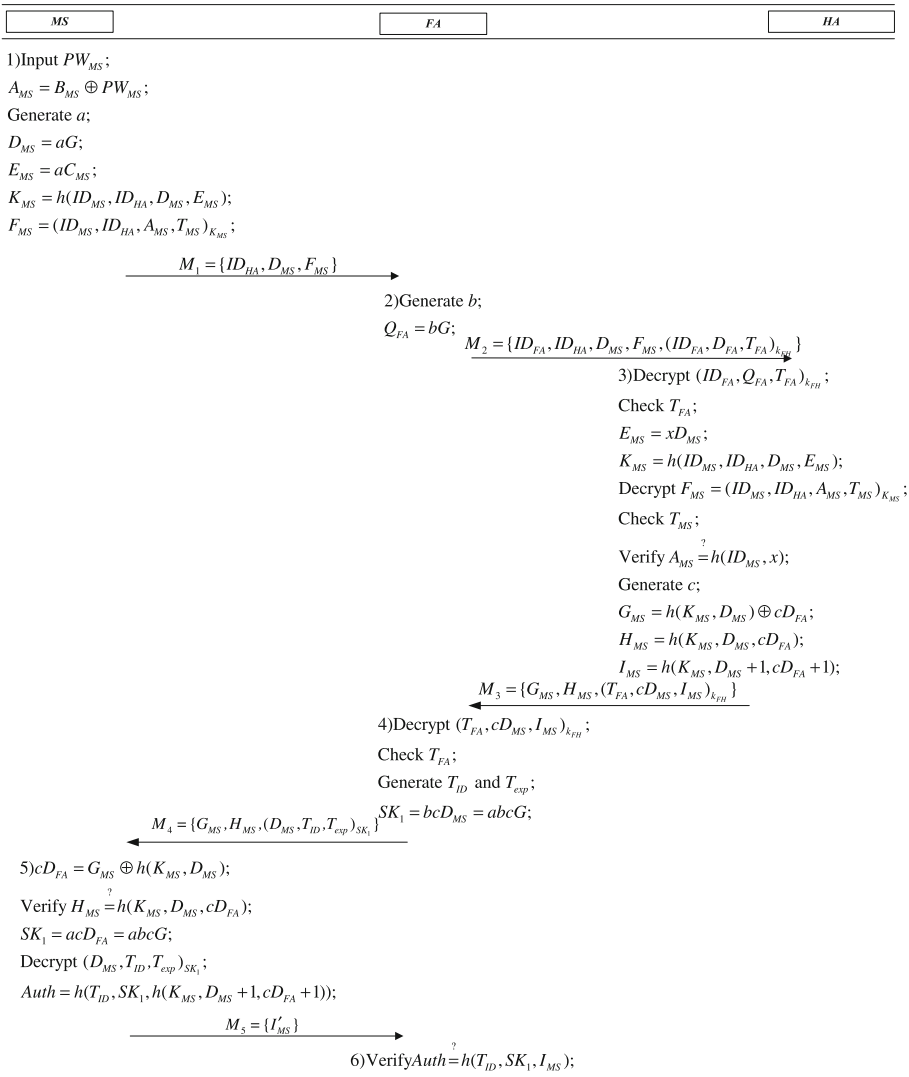


Fig. 5 The ticket-issuing phase of our protocol

(1) MS inputs PW_{MS} into his smart card. The smart card computes $A_{MS} = B_{MS} \oplus PW_{MS}$. The smart cards generates a random number a and computes $D_{MS} = aG$, $E_{MS} = aC_{MS}$, $K_{MS} = h(ID_{MS}, ID_{HA}, D_{MS}, E_{MS})$ and $F_{MS} = (ID_{MS}, ID_{HA}, A_{MS}, T_{MS})_{K_{MS}}$, where T_{MS} is the current timestamp. MS sends the message $M_1 = \{ID_{HA}, D_{MS}, F_{MS}\}$ to the FA.
(2) Upon receiving M_1, FA generates a random number b, computes $D_{FA} = bG$. Then, FA sends $M_2 = \{ID_{FA}, ID_{HA}, D_{MS}, F_{MS}, (ID_{FA}, D_{FA}, T_{FA})_{k_{FH}}\}$ to HA, where T_{FA} is the current timestamp.
(3) Upon receiving M_2, HA obtains $(ID_{FA}, Q_{FA}, T_{FA})$ by decrypting $(ID_{FA}, Q_{FA}, T_{FA})_{k_{FH}}$. Then, HA checks the freshness of T_{FA}. If T_{FA} is not fresh, HA stops the session; otherwise HA computes $E_{MS} = xD_{MS}$, $K_{MS} = h(ID_{MS}, ID_{HA}, D_{MS}, E_{MS})$ and decrypts F_{MS} to get $(ID_{MS}, ID_{HA}, A_{MS}, T_{MS})$. Then, HA checks the freshness of T_{MS}. If T_{MS} is not fresh, HA stops the session; otherwise, HA checks whether A_{MS} and $h(ID_{MS}, x)$ are equal. If they are not equal, HA stops the session; otherwise, HA generates a random number c, computes $G_{MS} = h(K_{MS}, D_{MS}) \oplus cD_{FA}$, $H_{MS} = h(K_{MS}, D_{MS}, cD_{FA})$ and $I_{MS} = h(K_{MS}||D_{MS} + 1||cD_{FA} + 1)$. At last, HA sends $M_3 = \{G_{MS}, H_{MS}, (T_{FA}, cD_{MS}, I_{MS})_{k_{FH}}\}$ to FA.
(4) Upon receiving M_3, FA gets $(T_{FA}, cQ_{MS}, I_{MS})$ by decrypting $(T_{FA}, cD_{MS}, I_{MS})_{k_{FH}}$. FA checks whether T_{HA} is the one he has sent. If it is not that one, FA stops the session; otherwise, FA generates a unique ticket identifier T_{ID} and an expired time T_{exp}, and computes $SK_1 = bcQ_{MS} = abcG$. At last, FA sends $M_4 = \{G_{MS}, H_{MS}, (D_{MS}, T_{ID}, T_{exp})_{SK_1}\}$ to MS.
(5) Upon receiving M_4, MS computes $cD_{FA} = G_{MS} \oplus h(K_{MS}, D_{MS})$ and checks whether H_{MS} and $h(K_{MS}, D_{MS}, cD_{FA})$ are equal. If they are not equal, MS stops the session; otherwise, MS computes $SK_1 = acD_{FA} = abcG$ and gets $(D_{MS}, T_{ID}, T_{exp})$ by decrypting $(D_{MS}, T_{ID}, T_{exp})_{SK_1}$ using SK_1. At last, MS computes $Auth = h(T_{ID}, SK_1, h(K_{MS}, D_{MS} + 1, cD_{FA} + 1))$ and sends $M_5 = \{Auth\}$ to FA.
(6) Upon receiving M_5, FA checks whether $Auth$ and $h(T_{ID}, SK_1, I_{MS})$ are equal. If they are not equal, FA stops the session. Otherwise, the user is authenticated.

4.3 Phase III: the Ticket Authentication Phase

The phase of our protocol is the same as that of Hsieh and Leu's protocol. To save space, we will not repeat the description.

5 Security Analysis

5.1 Authentication Proof Based on BAN-Logic

The BAN logic [16] is a well known formal model. It has been widely used to analyze the security of authentication and key distribution protocols. We will demonstrate the validity of our protocol through the BAN logic. For convenience, the notations used in BAN logic analysis are described as follows.

- $P| \equiv X$: The principal P believes a statement X, or P is entitled to believe X.
- $\#(X)$: The formula X is fresh.
- $P \Rightarrow X$: The principal P has jurisdiction over the statement X.
- $P \triangleleft X$: The principal P sees the statement X.
- $P| \sim X$: The principal P once said the statement X.

- (X, Y) : The formula X or Y is one part of the formula (X, Y).
- $< X >_Y$: The formula X combined with the formula Y.
- $\{X\}_Y$: The formula X is encrypted under the key K.
- $(X)_Y$: The formula X is hash with the key K.
- $P \overset{K}{\longleftrightarrow} Q$: The principals P and Q use the shared key K to communicate. The key K will never be discovered by any principal except P and Q.
- sk : The session key used in the current session.

We also define some main logical postulates of BAN logic as follows, since they will be used in our proof.

- The message-meaning rule: $\frac{P|\equiv P \overset{K}{\leftrightarrow} Q, P \lhd \{X\}_K}{P|\equiv Q|\sim X}$.
- The freshness-conjuncatenation rule: $\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$.
- The nonce-verification rule: $\frac{P|\equiv \#(X), P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$.
- The jurisdiction rule: $\frac{P|\equiv Q \Rightarrow X, P|\equiv Q|\equiv X}{P|\equiv X}$.

According to the analytic procedures of BAN logic, the proposed protocol will satisfy the following goals:

Goal 1. $MS| \equiv (MS \overset{SK_1}{\longleftrightarrow} FA)$;
Goal 2. $MS| \equiv FA| \equiv (MS \overset{SK_1}{\longleftrightarrow} FA)$;
Goal 3. $FA| \equiv (MS \overset{SK_1}{\longleftrightarrow} FA)$;
Goal 4. $FA| \equiv FA| \equiv (MS \overset{SK_1}{\longleftrightarrow} FA)$;
Goal 5. $MS| \equiv (MS \overset{T_{ID}}{\longleftrightarrow} FA)$;
Goal 6. $MS| \equiv FA| \equiv (MS \overset{T_{ID}}{\longleftrightarrow} FA)$;
Goal 7. $FA| \equiv (MS \overset{T_{ID}}{\longleftrightarrow} FA)$;
Goal 8. $FA| \equiv MS| \equiv (MS \overset{T_{ID}}{\longleftrightarrow} FA)$;

First, we transform our proposed protocol to the idealized form as follows:

$Msg\ 1.\quad MS \rightarrow HA: \quad \{(ID_{MS}, ID_{HA}, T_{MS}, Q_{MS})_{A_{MS}}\}_{K_{MS}}$
$Msg\ 2.\quad FA \rightarrow HA: \quad \{ID_{FA}, D_{FA}, T_{FA}\}_{k_{FH}}$
$Msg\ 3.\quad HA \rightarrow MS: \quad (D_{MS}, MS \overset{cD_{FA}}{\longleftrightarrow} FA)_{K_{MS}}$
$Msg\ 4.\quad HA \rightarrow FA: \quad \{T_{FA}, MS \overset{cD_{MS}}{\longleftrightarrow} FA, I_{MS}\}_{k_{FH}}$
$Msg\ 5.\quad FA \rightarrow MS: \quad \{D_{MS}, MS \overset{T_{ID}}{\longleftrightarrow} FA, MS \overset{SK_1}{\longleftrightarrow} FA\}_{SK_1}$
$Msg\ 6.\quad MS \rightarrow FA: \quad (T_{ID}, MS \overset{T_{ID}}{\longleftrightarrow} FA, MS \overset{SK_1}{\longleftrightarrow} FA)_{SK_1}$

Second, we make the following assumptions about the initial state of the protocol to analyze the proposed protocol:

A_1: $MS| \equiv \#(T_{MS})$;
A_2: $MS| \equiv \#(D_{MS})$;
A_3: $FA| \equiv \#(T_{FA})$;
A_4: $FA| \equiv \#(T_{ID})$;
A_5: $HA| \equiv \#(T_{MS})$;
A_6: $HA| \equiv \#(T_{FA})$;
A_7: $MS| \equiv (MS \overset{A_{MS}}{\longleftrightarrow} HA)$;

A_8: $MS| \equiv (MS \overset{K_{MS}}{\longleftrightarrow} HA)$;
A_9: $HA| \equiv (MS \overset{A_{MS}}{\longleftrightarrow} HA)$;
A_{10}: $HA| \equiv (MS \overset{K_{MS}}{\longleftrightarrow} HA)$;
A_{11}: $FA| \equiv (FA \overset{k_{FH}}{\longleftrightarrow} HA)$;
A_{12}: $HA| \equiv (FA \overset{k_{FH}}{\longleftrightarrow} HA)$;
A_{13}: $MS| \equiv HA| \Rightarrow (MS \overset{cD_{FA}}{\longleftrightarrow} FA)$.
A_{14}: $FA| \equiv HA| \Rightarrow (MS \overset{cD_{FA}}{\longleftrightarrow} FA)$.
A_{15}: $MS| \equiv FA \Rightarrow (MS \overset{T_{ID}}{\longleftrightarrow} FA)$;
A_{16}: $MS| \equiv FA \Rightarrow (MS \overset{SK_1}{\longleftrightarrow} FA)$;
A_{17}: $FA| \equiv MS \Rightarrow (MS \overset{T_{ID}}{\longleftrightarrow} FA)$;
A_{18}: $FA| \equiv MS \Rightarrow (MS \overset{SK_1}{\longleftrightarrow} FA)$;

Third, we analyze the idealized form of the proposed protocol based on the BAN logic rules and the assumptions. The main proofs are stated as follows:

According to the message $Msg1$, we could get
S_1: $HA \triangleleft \{(ID_{MS}, ID_{HA}, T_{MS}, Q_{MS})_{A_{MS}}\}_{K_{MS}}$.
According to the assumption A_9, we apply the message-meaning rule to get
S_2: $HA| \equiv MS| \sim (ID_{MS}, ID_{HA}, T_{MS}, Q_{MS})_{A_{MS}}$.
According to the assumption A_{10}, we apply the message-meaning rule to get
S_3: $HA| \equiv MS| \sim (ID_{MS}, ID_{HA}, T_{MS}, Q_{MS})$.
According to the assumption A_5, we apply the freshness-conjuncatenation rule to get
S_4: $HA| \equiv MS| \equiv (ID_{MS}, ID_{HA}, T_{MS}, Q_{MS})$.
According to the message Msg 2, we could get
S_5: $HA \triangleleft \{ID_{FA}, D_{FA}, T_{FA}\}_{k_{FH}}$.
According to the assumption A_{11}, we apply the message-meaning rule to get
S_6: $HA| \equiv FA| \sim (ID_{FA}, D_{FA}, T_{FA})$.
According to the assumption A_3, we apply the freshness-conjuncatenation rule to get
S_7: $HA| \equiv FA| \equiv (ID_{FA}, D_{FA}, T_{FA})$.
According to the message Msg 3, we could get
S_8: $MS \triangleleft (D_{MS}, FA \overset{cD_{FA}}{\longleftrightarrow} HA)_{K_{MS}}$.
According to the assumption A_8, we apply the message-meaning rule to get
S_9: $MS| \equiv HA| \sim (D_{MS}, FA \overset{cD_{FA}}{\longleftrightarrow} HA)$.
According to the assumption A_2, we apply the freshness-conjuncatenation rule to get
S_{10}: $MS| \equiv HA| \equiv (D_{MS}, MS \overset{cD_{FA}}{\longleftrightarrow} FA)$.
According to S_{10}, we apply the BAN logic rule to break conjunctions to produce
S_{11}: $MS| \equiv HA| \equiv (MS \overset{cD_{FA}}{\longleftrightarrow} FA)$.
According to assumption A_{13}, we apply the jurisdiction rule to get
S_{12}: $MS| \equiv (MS \overset{cD_{FA}}{\longleftrightarrow} FA)$.
According to $SK_1 = a(cD_{FA}) = abcG$, we could get
S_{13}: $MS| \equiv (MS \overset{SK_1}{\longleftrightarrow} FA)$. **(Goal 1)**
According to the message Msg 4., we could get
S_{14}: $FA \triangleleft \{T_{FA}, MS \overset{cD_{MS}}{\longleftrightarrow} FA, I_{MS}\}_{k_{FH}}$.
According to the assumption A_{12}, we apply the message-meaning rule to get
S_{15}: $FA| \equiv HA| \sim (T_{FA}, MS \overset{cD_{MS}}{\longleftrightarrow} FA, I_{MS})$.

According to the assumption A_3, we apply the freshness-conjuncatenation rule to get

S_{16}: $FA| \equiv HA| \equiv (T_{FA}, MS \overset{cD_{MS}}{\longleftrightarrow} FA, I_{MS})$.

According to S_{16}, we apply the BAN logic rule to break conjunctions to produce

S_{17}: $FA| \equiv HA| \equiv (MS \overset{cD_{MS}}{\longleftrightarrow} FA)$.

According to assumption A_{14}, we apply the jurisdiction rule to get

S_{18}: $FA| \equiv (MS \overset{cD_{FA}}{\longleftrightarrow} FA)$.

According to $SK_1 = b(aD_{MS}) = abcG$, we could get

S_{19}: $FA| \equiv (MS \overset{SK_1}{\longleftrightarrow} FA)$. **(Goal 3)**

According to the message Msg 5, we could get

S_{20}: $MS \triangleleft \{D_{MS}, MS \overset{T_{ID}}{\longleftrightarrow} FA, MS \overset{SK_1}{\longleftrightarrow} FA\}_{SK_1}$.

According S_{20}, we apply the message-meaning rule to get

S_{21}: $MS| \equiv FA| \sim (D_{MS}, MS \overset{T_{ID}}{\longleftrightarrow} FA, MS \overset{SK_1}{\longleftrightarrow} FA)$.

According to the assumption A_2, we apply the freshness-conjuncatenation rule to get

S_{22}: $MS| \equiv FA| \equiv (D_{MS}, MS \overset{T_{ID}}{\longleftrightarrow} FA, MS \overset{SK_1}{\longleftrightarrow} FA)$.

According to S_{22}, we apply the BAN logic rule to break conjunctions to produce

S_{23}: $MS| \equiv FA| \equiv (MS \overset{SK_1}{\longleftrightarrow} FA)$. **(Goal 2)**

S_{24}: $MS| \equiv FA| \equiv (MS \overset{T_{ID}}{\longleftrightarrow} FA)$. **(Goal 6)**

According to S_{24} and the assumption A_{15}, we apply the jurisdiction rule to get

S_{25}: $MS| \equiv (MS \overset{T_{ID}}{\longleftrightarrow} FA)$. **(Goal 5)**

According to the message Msg 6, we could get

S_{26}: $MS \triangleleft (T_{ID}, MS \overset{T_{ID}}{\longleftrightarrow} FA, MS \overset{SK_1}{\longleftrightarrow} FA)_{SK_1}$.

According S_{26}, we apply the message-meaning rule to get

S_{27}: $MS| \equiv FA| \sim (T_{ID}, MS \overset{T_{ID}}{\longleftrightarrow} FA, MS \overset{SK_1}{\longleftrightarrow} FA)$.

According to the assumption A_{17}, we apply the freshness-conjuncatenation rule to get

S_{28}: $MS| \equiv FA| \equiv (T_{ID}, MS \overset{T_{ID}}{\longleftrightarrow} FA, MS \overset{SK_1}{\longleftrightarrow} FA)$.

According to S_{26}, we apply the BAN logic rule to break conjunctions to produce

S_{29}: $FA| \equiv MS| \equiv (MS \overset{SK_1}{\longleftrightarrow} FA)$. **(Goal 4)**

S_{30}: $FA| \equiv MS| \equiv (MS \overset{T_{ID}}{\longleftrightarrow} FA)$. **(Goal 8)**

According to S_{30} and the assumption A_{18}, we apply the jurisdiction rule to get

S_{31}: $FA| \equiv (MS \overset{T_{ID}}{\longleftrightarrow} FA)$. **(Goal 7)**

According to **(Goal 1)**, **(Goal 2)**, **(Goal 3)**, **(Goal 4)**, **(Goal 5)**, **(Goal 6)**, **(Goal 7)** and **(Goal 8)**, we know that both of MS and FA believe that the session key SK_1 and a unique ticket identifier T_{ID} is shared between MS and FA.

5.2 Discussions on the Possible Attacks

In this sub section, we will show our protocol could provide the user anonymity and withstand some attacks [17–19].

Anonymity: In our protocol, MS's identity ID_{MS} is included in the message $F_{MS} = (ID_{MS}, ID_{HA}, A_{MS}, T_{MS})_{K_{MS}}$. The adversary A has to compute get $K_{MS} = h(ID_{MS}, ID_{HA}, D_{MS}, E_{MS})$ if he wants to get the identity ID_{MS}. A has to compute $E_{MS} = aC_{MS} = axG$ from $C_{MS} = xG$ and $D_{MS} = aG$. Therefore, A will face with the computational Diffie–Hellman problem and our protocol could provide anonymity.

Impersonation attack: Suppose an adversary A wants to impersonate MS to login in HA. He could generate a random number a and computes $D_{MS} = aG$, $E_{MS} = aC_{MS}$ and $K_{MS} = h(ID_{MS}, ID_{HA}, D_{MS}, E_{MS})$. However, he cannot generate a legal $F_{MS} = (ID_{MS}, ID_{HA}, A_{MS}, T_{MS})_{K_{MS}}$ to pass HA's verification since he cannot compute $A_{MS} = h(ID_{MS}, x)$ without the knowledge of x. Therefore, our protocol could withstand the impersonation attack.

Stolen-verifier attack: In our protocol, HA keeps no verifier table at all. So, the adversary cannot steal or modify any verification information of MS. Therefore, our protocol could withstand the stolen-verifier attack.

Smart card stolen attack: In our protocol, the adversary A may get MS's smart card and extract the registration information $\{ID_{HA}, B_{MS}, C_{MS}\}$ through the side channel attack [20,21], where $A_{MS} = h(ID_{MS}, x)$ and $B_{MS} = A_{MS} \oplus PW_{MS}$. A may also get the message $M_1 = \{ID_{HA}, D_{MS}, F_{MS}\}$ related with the password, where $D_{MS} = aG$, $E_{MS} = aC_{MS}$, $K_{MS} = h(ID_{MS}, ID_{HA}, D_{MS}, E_{MS})$ and $F_{MS} = (ID_{MS}, ID_{HA}, A_{MS}, T_{MS})_{K_{MS}}$. He could guess a password PW'_{MS} and computes $A'_{MS} = B_{MS} \oplus PW'_{MS}$. To verify the correctness of PW'_{MS}, A has to compute $K_{MS} = h(ID_{MS}, ID_{HA}, D_{MS}, E_{MS})$. Then, he has to compute $E_{MS} = aC_{MS} = axG$ from $C_{MS} = xG$ and $D_{MS} = aG$. Therefore, he has to solve the computational Diffie–Hellman problem and our protocol could withstand the smart card stolen attack.

Replay attack: In our protocol, the adversary A may intercept the authentication message $\{ID_{FA}, ID_{HA}, D_{MS}, F_{MS}, (ID_{FA}, D_{FA}, T_{FA})_{k_{FH}}\}$ transmitted between FA and HA, where $F_{MS} = (ID_{MS}, ID_{HA}, A_{MS}, T_{MS})_{K_{MS}}$. HA could find the attack by checking the freshness of T_{MS} and T_{FA} if A replay the message to it. Therefore, our protocol could withstand the replay attack.

Denial of authentication attack: In step 4 of the ticket-issuing phase, the unique ticket identifiers T_{ID} and T_{exp} are encrypted by a session key SK_1. Even if a malicious attacker intercepts $(D_{MS}, T_{ID}, T_{exp})_{SK_1}$, he cannot falsify the unique ticket without decrypting $(D_{MS}, T_{ID}, T_{exp})_{SK_1}$. Therefore, our protocol could withstand a denial of authentication attack successfully.

6 Performance Analysis

In this section, we will compare our protocol with Hsieh and Leu's protocol of [14]. For convenience, some notations are defined as follows.

- T_{hash} : The time for executing the hash function;
- T_{sym} : The time for executing the symmetric key cryptography;
- T_{XOR} : The time for executing the XOR operation;
- T_{EC-mul} : The time for executing the elliptic curve point multiplication.

Table 1 shows performance comparisons between our protocol and Hsieh and Leu's protocol [14]. The total computational cost of ticket-issuing phase in their protocol is $6T_{EC-mul} + 8T_{hash} + 6T_{sym} + 11T_{XOR}$. The total computational cost of ticket-issuing phase in our protocol is $7T_{EC-mul} + 13T_{hash} + 7T_{sym} + 3T_{XOR}$. To be more precise, the computational time of a one-way hashing operation, a symmetric encryption/decryption operation and an elliptic curve point multiplication operation is 0.0005, 0.0087 and 0.063075 s separately [14,22]. Moreover, the computational cost of XOR operation could be ignored when compared with other operations. The total computational time of ticket-issuing phase in their protocol and our protocol is 0.43465 and 0.508925 s separately. However, their pro-

Table 1 Performance comparisons

	Hsieh and Leu's protocol	Our protocol
Computational cost of ticket-issuing phase		
MS	$2T_{EC-mul} + 4T_{hash} + 1T_{sym} + 6T_{XOR} \approx 0.13685$	$3T_{EC-mul} + 4T_{hash} + 1T_{sym} + 2T_{XOR} \approx 0.19925$
FA	$2T_{EC-mul} + 3T_{sym} \approx 0.12765$	$2T_{EC-mul} + 3T_{sym} + 1T_{hash} \approx 0.13635$
HA	$2T_{EC-mul} + 4T_{hash} + 2T_{sym} + 5T_{XOR} \approx 0.14555$	$2T_{EC-mul} + 5T_{hash} + 3T_{sym} + 1T_{XOR} \approx 0.15475$
Total	$6T_{EC-mul} + 8T_{hash} + 6T_{sym} + 11T_{XOR} \approx 0.43465$	$7T_{EC-mul} + 13T_{hash} + 7T_{sym} + 3T_{XOR} \approx 0.508925$
Computational cost of ticket-authentication phase		
MS	$2T_{EC-mul} + 2T_{sym} \approx 0.12715$	$2T_{EC-mul} + 2T_{sym} \approx 0.12715$
FA	$2T_{EC-mul} + 2T_{sym} \approx 0.12715$	$2T_{EC-mul} + 2T_{sym} \approx 0.12715$
HA	–	–
Total	$4T_{EC-mul} + 4T_{sym} \approx 0.2543$	$4T_{EC-mul} + 4T_{sym} \approx 0.2543$

tocol cannot provide anonymity. It is well known that security is of top priority in wireless communications. Therefore, it is acceptable to enhance security at the cost of increasing computational time slightly.

7 Conclusion

Recently, Hsieh and Leu proposed an anonymous authentication protocol based on elliptic curve Diffie–Hellman problem for wireless access networks. They claimed that their protocol could provide anonymity and could withstand various attacks. However, after reviewing of their protocol and analyzing of its security, we demonstrate their protocol cannot provide anonymity. To overcome the weakness, we also proposed an improved protocol based on elliptic curve Diffie–Hellman problem for wireless access networks. Analysis shows our protocol could overcome the weakness in their protocol at increasing the computational cost slightly. Therefore, our protocol is more suitable for practical applications.

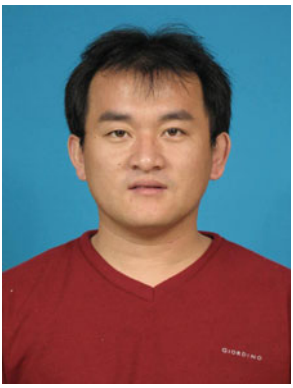
Acknowledgments The authors thank Prof. R. Prasad and the anonymous reviewers for their valuable comments. This research was supported by the Open Funds of State Key Laboratory of Information Security (No. 2013-3-3) and the Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20110141120003).

References

1. Juang, W., Lei, C., & Chang, C. (1999). Anonymous channel and authentication in wireless communications. *Computer Communications*, *22*, 1502–1511.
2. Rahman, M., & Imai, H. (2002). Security in wireless communication. *Wireless Personal Communications*, *22*(2), 213–228.
3. Harn, L., & Lin, H. (1993). Authentication in wireless communications. In *IEEE Global Telecommunications Conference (GLOBECOM '93)* (pp. 550–554).
4. Barbancho, A., & Peinado, A. (2003). Cryptanalysis of anonymous channel protocol for large-scale area in wireless communications. *Computer Networks*, *43*, 777–785.
5. Lee, C., Hwang, M., & Liao, I. (2006). Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Industrial Electronics*, *53*(5), 1683–1687.

6. Peinado, A. (2004). Privacy and authentication protocol providing anonymous channels in GSM. *Computer Communications*, *27*, 1709–1715.
7. Lin, W., & Jan, J. (2001). A wireless-based authentication and anonymous channels for large scale area. *In Proceedings of the IEEE symposium on computers and communications, 2001* (pp. 36–41).
8. Fathi, H., Shin, S., Kobara, K., & Imai, H. (2007) Protocols for authenticated anonymous communications. In *18th International symposium on personal, indoor and mobile radio, communications (PIMRC07)* (pp. 1–5).
9. He, D. (2012). Cryptanalysis of an authenticated key agreement protocol for wireless mobile communications. *ETRI Journal*, *34*(3), 482–484.
10. Zhu, J., & Ma, J. (2004). A new authentication scheme with anonymity for wireless environments. *IEEE Transactions on Consumer Electronics*, *50*(1), 231–235.
11. Lee, C., Chang, C., & Lin, C. (2005). User authentication with anonymity for global mobility networks. In *2th Asia pacific conference on mobile technology, applications and systems* (pp. 1–5).
12. Chen, Y., Chuang, S., Yeh, L., & Huang, J. (2011). A practical authentication protocol with anonymity for wireless access networks. *Wireless Communications and Mobile Computing*, *11*, 1366–1375.
13. Yang, C., Tang, Y., Wang, R., & Yang, H. (2005). A secure and efficient authentication protocol for anonymous channel in wireless communications. *Applied Mathematics and Computation*, *169*(2), 1431–1439.
14. Hsieh, W., & Leu, J. (2012). Anonymous authentication protocol based on elliptic curve Diffie–Hellman for wireless access networks. *Wireless Communications and Mobile Computing*, doi:10.1002/wcm.2252.
15. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, *48*, 203–209.
16. Burrows, M., Abadi, M., & Needham, R. (1990). A logic of authentication. *ACM Transaction on Computer System*, *8*(1), 18–36.
17. He, D., & Wu, S. (2012). Security flaws in a smart card based authentication scheme for multi-server environment. *Wireless Personal Communications*, doi:10.1007/s11277-012-0696-1.
18. Li, X., Xiong, Y., Ma, J., & Wang, W. (2012). An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. *Journal of Network and Computer Applications*, *35*(2), 763–769.
19. Wang, B., & Ma, M. (2012). A smart card based efficient and securedmulti-server authentication scheme. *Wireless Personal Communications*, doi:10.1007/s11277-011-0456-7.
20. Kocher, P., Jaffe, J., & Jun, J. (1999) Differential power analysis. In *Proceedings of advances in cryptology (CRYPTO 99)* (pp. 388–397).
21. Messerges, T., Dabbish, E., & Sloan, R. (2002). Examining smart- card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, *51*(5), 541–552.
22. Li, C., Hwang, M., & Chung, Y. (2008). A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Computer Communication*, *31*, 2803–2814.

Author Biographies



Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University in 2009. He is currently a lecturer of Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols.

Yuanyuan Zhang received the M.S. degree in applied mathematics from Wuhan University, Wuhan, China in 2012. She is currently pursuing the Ph.D. degree in applied mathematics from Wuhan University, Wuhan, China. Her research interests are in the areas of cryptography, information security and network security.

Jianhua Chen received the B.Sc. degrees in applied mathematics from Harbin Institute of Technology, Harbin, China, in 1983, and received the M.Sc and the Ph.D. degree in applied mathematics from Wuhan University, Wuhan, China, in 1989 and 1994, respectively. Currently, he is a professor of Wuhan University. His current research interests include number theory, information security and network security.