An Efficient and Secure Smart Card Based Authentication Scheme

Chien-Ming Chen[1], Bin Xiang[2], King-Hang Wang[3], Yong Zhang[4], Tsu-Yang Wu[1,5,6]

[1] College of Computer Science and Engineering, Shandong University of Science and Technology, China
[2] Harbin Institute of Technology (Shenzhen), China
[3] Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong
[4] Shenzhen University, China
[5] Fujian Provincial Key Laboratory of Big Data Mining and Applications, Fujian University of Technology, China
[6] National Demonstration Center for Experimental Electronic Information and Electrical Technology Education, Fujian University of Technology, China
chienming.taiwan@gmail.com, xiangbin.hit@qq.com, kevinw@cse.ust.hk, yzhang@szu.edu.cn, wutsuyang@gmail.com

Abstract

Remote user authentication schemes are helpful to provide authenticity between users and a remote server in network-based services. In order to meet the security requirements, many related schemes have been proposed. Recently, Moon et al. proposed a smart card based three-factor authentication scheme and claimed that the scheme prevented various attacks. However, just in the same year, Li et al. suggested a new insider attack scenario and pointed out that Moon et al.'s scheme suffers from a user anonymity violation attack, a user impersonation attack, and a server masquerade attack under this scenario. In this study, it is demonstrated that without the new attack scenario, Moon et al.'s scheme is still insecure against a traceability attack, an offline identity-guessing attack, an impersonation attack, and a man-in-the-middle attack. Based on Moon et al.'s scheme, a new three-factor authenticated key agreement scheme is proposed. The proposed scheme is validated by widely accepted BAN logic. In addition, the proposed scheme can satisfy various types of functional features and prevent various security attacks.

Keywords: Authentication key agreement, Biometric, Elliptic-curve cryptosystem, Smart card, BAN logic

1 Introduction

The advances in the field of computer networks and communications have led to enormous increase in applications based on the Internet of Things (IoT), including transportation, healthcare, online banking, and smart homes. However, the data transmitted between the users and these applications take place over unsecure channels. Thus, it is essential to use authenticated key agreement mechanism to protect the user privacy and data security. Based on the factors used in the authentication method, these schemes can be divided into one-factor, two-factor, and three-factor authentication schemes. The one-factor authentication scheme is only based on the password, and the first one [1] was proposed by Lamport in 1981. Since then, a series of one-factor authentication schemes were proposed [2-6]. However, the drawbacks of a password such as weak password and password-guessing attack make these schemes vulnerable. To increase the security, a smart card is added to design schemes. These password and smart card based authorization schemes [7-15] are known as two-factor authentication schemes. Unfortunately, in the past few years, some researches have demonstrated that the password and smart card based authentication methods are still vulnerable when the smart card is stolen and the secret data stored in the smart card are disclosed to the attacker [16-18]. To solve this problem, biometric characteristics such as fingerprint, iris, and palm print are used as a third factor to design a stronger scheme [19-31].

Recently, Liu et al. [29] proposed an efficient and secure smart card based three-factor authentication scheme for single-server environment; they claimed to have the capacity to prevent various security attacks. However, Moon et al. [31] pointed out several weaknesses of Liu et al.'s scheme such as no support for user anonymity, no support for perfect forward secrecy, cannot prevent outsider attack, and offline pass-word-guessing attack. Then, they proposed an improved scheme based on Liu et al.'s scheme. Unfortunately, later in the same year, Li et al. suggested a new insider attack scenario and pointed out that Moon et al.'s scheme suffers from a user anonymity violation attack, a user impersonation attack,

*Corresponding Author: Tsu-Yang Wu; E-mail: wutsuyang@gmail.com
DOI: 10.3966/160792642019072004011

and a server masquerade attack under this scenario [32]. In this study, we demonstrate that without the new insider attack scenario, Moon et al.'s scheme is still insecure against a traceability attack, an offline identity-guessing attack, an impersonation attack, and a man-in-the-middle attack. To solve these weaknesses, based on the Moon et al.'s scheme, a new three-factor authenticated key agreement scheme is proposed. The proposed scheme is then validated by widely accepted BAN logic. Through the performance analysis, we show that the proposed scheme is more secure with similar efficiency.

2 Preliminaries

In this section, the basic information about elliptic-curve cryptosystem [33-35], fuzzy-extractor [36], and model of attacker [31, 37-40] is described.

2.1 Elliptic-curve Cryptosystem

An elliptic curve denoted by E can be defined in the form of $E_p(a,b): y^2 = x^3 + ax + b (\text{mod } P)$ over a finite field F_p, where $a, b \in F_p$ and $4a^2 + 27b^2 \neq 0$. Given a point $P \in E_p$ and an integer $t \in F_p$, the point multiplication $tP = \underbrace{P + P + P + \ldots + P}_{t}$.

Elliptic-Curve Discrete Logarithm Problem (ECDLP): With two points $P, tP \in E_p$, it is computational impossible to obtain the value of t, where $t \in F_p$.

Elliptic-Curve Computational Diffie–Hellman Problem (ECCDHP): Using three points $P, tP, sP \in E_p$, it is difficult to compute $tsP \in E_p$, where $t, s \in F_p$.

2.2 Fuzzy Extractor

Biometrics information such as fingerprint and iris cannot be directly used in cryptographic algorithms without using a fuzzy extractor. The fuzzy extractor contains two algorithms, *Gen* and *Rep*.

$Gen(BIO_i) = (R_i, P_i)$. *Gen* is a probabilistic algorithm; it extracts the secret key data R_i and public reproduction parameter P_i from the given biometric input BIO_i.

$Rep(BIO_i', P_i) = R_i$. *Rep* is a deterministic algorithm; it reproduces the secret key data R_i from any biometric information BIO_i' close to BIO_i using the public reproduction parameter P_i.

2.3 Model of Attacker

Here, the attacker model under the three-factor authentication scheme is shown. An attacker A has the following capabilities:

- A has full control of a public channel, but not the secure channel, *i.e.*, the attacker can obtain all the transmitted data from a public channel.
- A can alter, delete, or replay the data captured from a public channel.
- A can read or extract the secret data from the stolen smart card issued to the user

3 Review of Moon et al.'s Scheme

In this section, Moon et al.'s scheme is briefly reviewed [31]. The scheme consists of the following four phases: (1) registration phase, (2) login phase, (3) authentication phase, and (4) password-change phase. The notations used in this paper are shown in Table 1.

Table 1. Notations used in this paper

Term	Description
U_i	i^{th} user
ID_i, PW_i	identity and password of user i
S	server
x	secret key stored in S
P	base point of elliptic curve E
P_{pub}	public key of S ($P_{pub} = xP$)
T_i	timestamp of user i
T_i'	time of receiving login request message
T_s	timestamp of S
T_s'	time of receiving mutual authentication message
R_i, P_i	U_i's secret data and reproduce parameter
$h(\cdot)$	one-way collision-resistant hash function
$\oplus$	exclusive or operation
$\|\|$	concatenation operation

3.1 Registration Phase

At the beginning of Moon et al.'s scheme, the server S selects its secret key x and the base point P of elliptic curve E. Then, user U_i registers to the server as follows:

Step 1. U_i imprints his/her personal biometric information BIO_i and extracts (R_i, P_i) from $Gen(BIO_i) = (R_i, P_i)$. Next, U_i selects identity ID_i and password PW_i and computes $RPW_i = h(PW_i \| R_i)$. Finally, U_i sends the registration message $\{ID_i, RPW_i\}$ to server S over a secure channel.

Step 2. On receiving the message form U_i, S will first check whether the ID_i is valid and then computes $A_i = h(ID_i \| x)$, $B_i = h(A_i) \oplus RPW_i$, $C_i = h(ID_i \| RPW_i)$ and $D_i = x \oplus A_i \oplus h(x)$.

Step 3. S stores the data $\{B_i, C_i, D_i, h(\cdot), P\}$ into a smart card and sends it to U_i over a secure channel.
Step 4. On receiving the smart card form S, U_i stores P_i in it.

3.2 Login Phase

When a registered user U_i wants to login to the server S, the following steps should be performed:
Step 1. U_i inserts his/her smart card and enters identity ID_i and password PW_i, and imprints the biometric information BIO_i^* at the sensor. The sensor then recovers R_i from $\mathrm{Re}p(BIO_i^*, P_i) = R_i$.
Step 2. The smart card computes $RPW_i = h(PW_i \| R_i)$, $C_i' = h(ID_i \| RPW_i)$ and checks whether $C_i' = C_i$. If the two values are equal, *Step 3* is continued. Otherwise, the session is terminated.
Step 3. The smart card selects two random numbers α and n_i, and computes $h(A_i) = B_i \oplus RPW_i$, $AID_i = ID_i \oplus h(A_i)$, $E_i = \alpha P$, and $F_i = h(ID_i \| h(A_i) \| E_i \| T_i)$. Next, the message $\{AID_i, D_i, E_i, F_i, T_i\}$ is sent to S.

3.3 Authentication Phase

Upon completing this phase, user U_i and server S authenticate each other and establish a session key. The steps of this authentication phase are as follows:
Step 1. S checks whether $T_i - T_i' < \Delta T$ holds. If holds, then S continues to execute *Step 2*. Otherwise, the login request is rejected.
Step 2. S computes $A_i' = D_i \oplus x \oplus h(x)$, $ID_i' = AID_i \oplus h(A_i')$, and $F_i' = h(ID_i' \| h(A_i') \| E_i \| T_i)$. Next, it is checked whether $F_i' = F_i$.. If they are equal, then the user is authenticated, and the login request is accepted. Otherwise, the server rejects the login request.
Step 3. S selects a random number β and computes $F_i = \beta P$, $G_i = h(ID_i' \| h(A_i') \| F_i \| T_s)$ and sends the message $\{F_i, G_i, T_s\}$ to U_i.
Step 4. On receiving the message from S, U_i checks whether $T_i - T_i' < \Delta T$ holds. If holds, then U_i executes *Step 5*. Otherwise, the session is terminated.
Step 5. U_i computes $G_i' = h(ID_i \| h(A_i) \| F_i \| T_s)$ and checks whether $G_i' = G_i$. If they are equal, then S is authenticated. Otherwise, the session is terminated.
Step 6. Finally, U_i and S construct a shared session key $SK = \alpha\beta P$.

3.4 Password-change Phase

During the password-change phase, user U_i updates the password without the help of server as follows:
Step 1. U_i enters identity ID_i and password PW_i and imprints the biometric information BIO_i^* at the sensor. The smart card then authenticates whether the user is legal or not. If yes, then *Step 2* is executed. Otherwise, the session is terminated.
Step 2. U_i inputs the new password PW_i^{new}, and the smart card further computes $RPW_i^{new} = h(PW_i^{new} \| R_i)$, $B_i^{new} = B_i \oplus RPW_i \oplus PW_i^{new}$, and the parameter $C_i^{new} = C_i \oplus RPW_i \oplus PW_i^{new}$.
Step 3. The smart card uses RPW_i^{new} and C_i^{new} to replace the old RPW_i and C_i, respectively.

3.5 Li et al.'s New Insider Attack Scenario and Attacks

In Li et al.'s paper [36], they pointed out that Moon et al.'s scheme suffers from a user anonymity violation attack, and then they suggested a new insider attack. In the new insider attack, they assume that an attacker A has obtianed users' ID in the registration server. With the users' ID, A can further launch a user impersonation attack and a server masquerade attack.

4 Weaknesses of Moon et al.'s Scheme

In this section, our findings are described: The scheme of Moon et al. [31] suffers from a traceability attack, an offline identity-guessing attack, an impersonation attack, and a man-in-the-middle attack. In our attacks, the assumption mentioned in Li et al.'s paper [36] is not necessary. That it, an attacker A does not need to obtain users' ID in our attacks. It means that attacks proposed in this paper are more reasonable.

4.1 Traceability Attack

The main mechanism of traceability attack is that the attacker can trace a certain user with the message captured from a public channel. When designing anonymous authentication schemes, we should ensure that no attacks could be able to perform this attack. In Moon et al.'s scheme, the attacker A obtains the login message $\{AID_i, D_i, E_i, F_i, T_i\}$. As the values of AID_i and D_i are static and specific in different conversations, A can easily link these conversations and trace the user. Therefore, Moon et al.'s scheme suffers from traceability attack.

4.2 Offline Identity Guessing Attack

Assume that an attacker A has obtained the login message $\{AID_i, D_i, E_i, F_i, T_i\}$ from the public channel, then A can perform an offline identity-guessing attack as follows:
Step 1. Extract AID_i, E_i, F_i, and T_i from the login message.

Step 2. A guesses a possible identity ID_i' of user U_i and computes $h'(A_i)=AID_i \oplus ID_i'$, $F_i'=h(ID_i' \| h'(A_i) \| E_i \| T_i)$.
Step 3. A checks whether $F_i'=F_i$. If the two values are equal, then the ID_i' is returned. Otherwise, *Step 2* is repeated.

Because the attacker A can successfully guess the identity of user U_i, Moon et al.'s scheme cannot prevent offline identity attack.

4.3 User Impersonation Attack

From the above analysis, an attacker A can obtain the values of ID_i and $h(A_i)$ by launching an offline identity guessing attack. Then, it is demonstrated that Moon et al.'s scheme suffers from a user impersonation attack. This attack can be performed as follows:
Step 1. Extract D_i from the old login message and obtain the values of ID_i and $h(A_i)$ by launching an offline identity-guessing attack.
Step 2. A then constructs the login message by computing $AID_i^* = ID_i \oplus h(A_i)$, $E_i^* = \alpha' P$, and $F_i^* = h(ID_i \| h(A_i) \| E_i^* \| T_i^*)$, where α' is a random number selected by adversary and T_i^* is the current timestamp. Next, the login message $\{AID_i^*, D_i^*, E_i^*, F_i^*, T_i^*\}$ is sent to S.
Step 3. On receiving the login message, S verifies the timestamp T_i^* and F_i^*. Undoubtedly, they will pass the verification. S then computes $F_i = \beta P$, $G_i = h(ID_i' \| h(A_i') \| F_i \| T_s)$ and sends $\{F_i, G_i, T_s\}$ to A.
Step 4. On receiving the message $\{F_i, G_i, T_s\}$ from S, A can construct the session key $SK = \alpha' \beta P$.

In this case, an attacker A can be authenticated by the server as a legal user, and a shared session key SK can be established with the server. Therefore, Moon et al.'s scheme cannot prevent user impersonation attack.

4.4 Server Spoofing Attack

Attacker A can perform a server spoofing attack as follows:
Step 1. Extract D_i from the old login message and obtain the values of ID_i and $h(A_i)$ by launching an offline identity-guessing attack.
Step 2. A intercepts the login message from U_i to S and forges the return values $F_i^* = \beta' P$ and $G_i^* = h(ID_i \| h(A_i) \| F_i^* \| T_s^*)$, where β' is a random number and T_s^* is the current stamp. Next, A sends the forged authentication message $\{F_i^*, G_i^*, T_s^*\}$ to U_i.
Step 3. U_i checks the values of T_s^* and G_i^*. As the parameters ID_i and $h(A_i)$ are the actual values of U_i, they will pass the verification. Finally, U_i computes the time session key $SK = \alpha \beta' P$.

In this case, an attacker A can be authenticated by the user as a legal server, and a shared session key SK is established. Therefore, Moon et al.'s scheme cannot prevent server spoofing attack.

4.5 Man-in-the-middle Attack

Since an attacker A can masquerade any of the two communication entities (the user or the remote server) and send messages to the other one without being detected. Therefore, Moon et al.'s scheme suffers from a man-in-the-middle attack.

5 Proposed Scheme

In this section, a new authentication scheme is proposed to offer enhanced security by resolving the vulnerabilities of Moon et al.'s scheme. The proposed scheme also consists of four phases: (1) registration phase, (2) login phase, (3) authentication phase, and (4) password-change phase.

5.1 Registration Phase

At the beginning of the proposed scheme, the server S selects a secure one-way hash function $h(\cdot)$, the base point P of elliptic curve E, the master key x, and computes the public key $P_{pub} = xP$. Then, user U_i can be registered in the server as a legal user. All the steps performed between the user and server take place over a secure channel. The details of this phase are described as follows and shown in Figure 1.
Step 1. U_i imprints the personal biometric information BIO_i and extracts (R_i, P_i) from $Gen(BIO_i) = (R_i, P_i)$. Then, U_i selects identity ID_i and password PW_i and computes $RPW_i = h(PW_i \| R_i)$. Next, U_i sends the registration message $\{ID_i, RPW_i\}$ to S.
Step 2. On receiving the registration message, S computes $A_i = h(ID_i \| x)$, $B_i = A_i \oplus RPW_i$, and $C_i = h(ID_i \| RPW_i)$. S then stores the data $\{B_i, C_i, P_{pub}, h(\cdot), P\}$ into a new smart card and sends the card to U_i.
Step 3. When U_i receives the smart card from S, P_i is stored in it. Finally, the smart card contains $\{B_i, C_i, P_{pub}, h(\cdot), P, P_i\}$.

5.2 Login Phase

In the login phase, user U_i performs the following steps as shown in Figure 2.

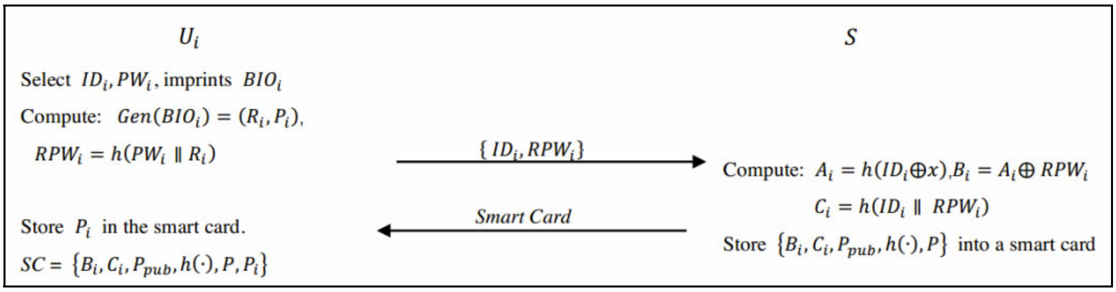

Figure 1. Registration phase of proposed scheme

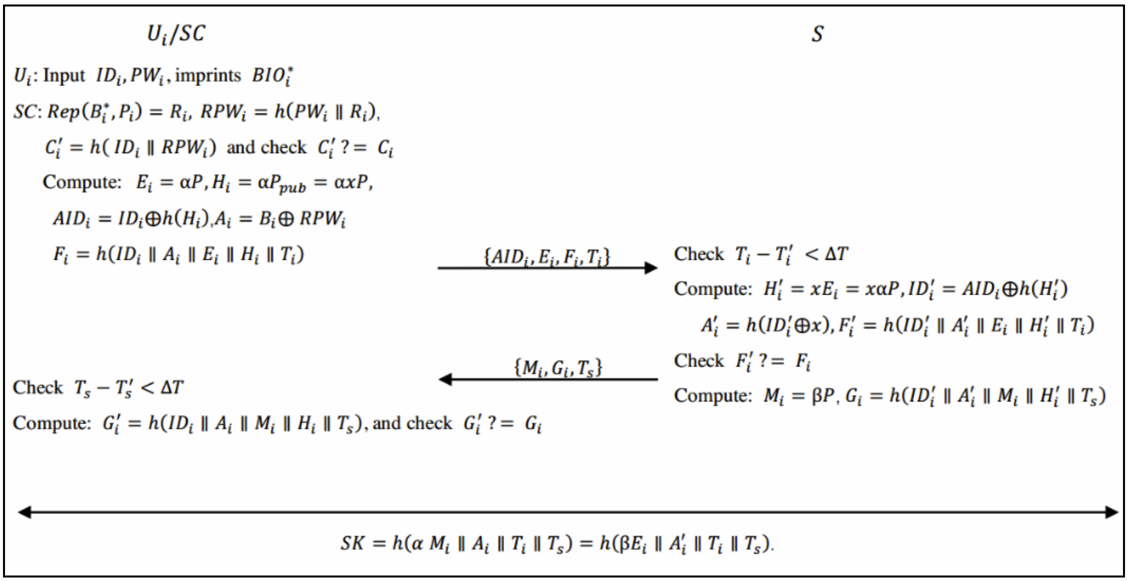

Figure 2. Login and authentication phase of the proposed scheme

Step 1. U_i inserts the smart card and enters identity ID_i and password PW_i and then imprints the biometric information BIO_i^* at the sensor. The sensor recovers R_i from $\mathrm{Re}\,p(BIO_i^*, P_i) = R_i$.

Step 2. The smart card computes $RPW_i = h(P_i \parallel R_i)$ and $C_i' = h(ID_i \parallel RPW_i)$. Next, the smart card checks whether $C_i' = C_i$. . If they are equal, the smart card believes that the user is legal and continues to *Step 3*. Otherwise, the login phase is terminated.

Step 3. The smart card selects a random number α, and then it computes $E_i = \alpha P, H_i = \alpha P_{pub}, \alpha xP$, $AID_i = ID_i \oplus h(H_i)$, $A_i = B_i \oplus RPW_i$, and $F_i = h(ID_i \parallel A_i \parallel E_i \parallel H_i \parallel T_i)$, where T_i is the current timestamp. Next, the smart card sends the login message $\{AID_i, D_i, E_i, F_i, T_i\}$ to server *S*.

5.3 Authentication Phase

When server *S* receives the login message from user U_i, it performs the following steps to achieve mutual authentication and key agreement. The details are shown in Figure 2.

Step 1. *S* checks whether $T_i - T_i' < \Delta T$ holds, where T_i' is the time when the login message arrives. If it holds, then the server continues to execute *Step 2*. Otherwise, the login request is rejected.

Step 2. *S* computes $H_i' = xE_i = x\alpha P, ID_i' = AID_i \oplus h(H_i')$, $A_i' = h(ID_i' \oplus x)$, $F_i' = h(ID_i' \parallel A_i' \parallel E_i \parallel H_i' \parallel T_i)$ and checks whether $F_i' = F_i$. If they are equal, then U_i is authenticated, and the login request is accepted. Otherwise, *S* rejects the login request.

Step 3. *S* selects a random number β and then computes $M_i = \beta P$, $G_i = h(ID_i' \parallel A_i' \parallel M_i \parallel H_i' \parallel T_s)$, where T_s is the timestamp of *S*. Then, the message $\{M_i, B_i, T_s\}$ is sent to U_i.

Step 4. On receiving message $\{M_i, B_i, T_s\}$ from *S*, U_i checks whether $T_i - T_i' < \Delta T$ holds, where T_s' is the time of receiving the mutual authentication message. If it holds, then U_i continues to execute *Step 5*. Otherwise, the session is terminated.

Step 5. U_i computes $G_i' = h(ID_i \parallel A_i \parallel M_i \parallel H_i \parallel T_s)$. and checks whether $G_i' = G_i$. If they are equal, then *S* is authenticated. Otherwise, the session is terminated.

Step 6. Finally, U_i and S construct a shared session key $SK = h(\alpha M_i \| A_i \| T_i \| T_s) = h(\beta E_i \| A_i' \| T_i \| T_s)$.

5.4 Password-change Phase

In the password-change phase, user U_i updates the password without the help of server as follows:

Step 1. U_i inserts the smart card and enters identity ID_i and password PW_i and then imprints the biometric information BIO_i^* at the sensor. The sensor recovers R_i from $Rep(BIO_i^*, P) = R_i$.

Step 2. The smart card computes $RPW_i = h(PW_i \| R_i)$ and $C_i' = h(ID_i \| RPW_i)$. Next, it is checked whether $C_i' = C_i$. If the two values are equal, the smart card continues to *Step 3*. Otherwise, the request is terminated.

Step 3. U_i inputs new password PW_i^{new}, and the smart card further computes $RPW_i^{new} = h(PW_i^{new} \| R_i)$, $B_i^{new} = B_i \oplus RPW_i \oplus RPW_i^{new}$, and $C_i^{new} = h(ID_i \| RPW_i)$.

Step 4. The smart card uses B_i^{new} and C_i^{new} to replace the old B_i and C_i in the memory, respectively.

6 Security Analysis of Proposed Scheme

In this section, the correctness of proposed scheme was analyzed by BAN logic, and the other security features under the attacker model mentioned in section 2 are discussed.

6.1 Mutual Authentication Proof Using BAN Logic

In this subsection, the well-known BAN logic was used to prove the mutual authentication and key agreement scheme. The notations used in BAN logic are shown below.

- $P \mid\equiv X$: P believes the statement X
- $P \triangleleft X$: P once received an information including X
- $P \mid\sim X$: P once said X
- $P \mid\Rightarrow X$: P controls X
- $\#X$: Statement X is fresh
- $P \xleftrightarrow{K} X$: K is the shared information between P and X
- $\{X\}_K$: X is encrypted by key K
- $\langle X \rangle_K$: X is combined with key K
- $(X)_K$: X is hashed with key K

The main rules proposed in BAN logic are defined as follows:

Rule 1. $\dfrac{P \mid\equiv X \xleftrightarrow{K} Q,\ P \triangleleft \{X\}_K}{P \mid\equiv Q \mid\sim X}$

Rule 2. $\dfrac{P \mid\equiv \#(X),\ P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \equiv X}$

Rule 3. $\dfrac{P \mid\equiv Q \mid\Rightarrow X,\ P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$

Rule 4. $\dfrac{P \mid\equiv (X)}{P \mid\equiv (X, Y)}$

Rule 5. $\dfrac{P \mid\equiv (X, Y)}{P \mid\equiv (X)}$

The proposed mutual authentication has the following goals:

Goal 1: $A \mid\equiv A \xleftrightarrow{SK} S$

Goal 2: $S \mid\equiv A \xleftrightarrow{SK} S$

Goal 3: $A \mid\equiv S \mid\equiv A \xleftrightarrow{SK} S$

Goal 4: $S \mid\equiv A \mid\equiv A \xleftrightarrow{SK} S$

First, the message exchange in the proposed scheme is determined.

$m_1 \cdot A \rightarrow S : \{AID_i, E_i, T_i\}$; ; this message can be idealized to $\langle AID_i, \alpha P_i, T_i \rangle_{A \xleftrightarrow{Hi} S}$.

$m_1 \cdot S \rightarrow A : \{M_i, T_s\}$; this message can be idealized to $\langle \beta P_i, T_s \rangle_{A \xleftrightarrow{H'i} S}$.

The following assumptions are true in the proposed scheme.

$B_1 \cdot A \mid\equiv \#(T_s)$

$B_2 \cdot S \mid\equiv \#(T_i)$

$B_3 \cdot A \mid\equiv A \xleftrightarrow{H_i'} S$

$B_4 \cdot S \mid\equiv A \xleftrightarrow{H_i} S$

$B_5 \cdot A \mid\equiv S \mid\Rightarrow A \xleftrightarrow{SK} S$

$B_6 \cdot S \mid\equiv A \mid\Rightarrow A \xleftrightarrow{SK} S$

Then, the mutual authentication of proposed scheme is given.

Based on m_1, $S_1 : S \triangleleft \langle AID_i, \alpha P, T_i \rangle_{A \xleftrightarrow{H_i} S}$.

Based on S_1, B_4, *Rule* 1, $S_2 : S \mid\equiv A \mid\sim \langle AID_i, \alpha P, T_i, A \xleftrightarrow{SK} S \rangle$

Based on m_2, $S_3 : A \triangleleft \langle \beta P, T_s \rangle_{A \xleftrightarrow{H_i'} S}$.

Based on S_3, B_3, *Rule* 1, $S_4 : A \mid\equiv S \mid\sim \langle \beta P, T_s, A \xleftrightarrow{SK} S \rangle$

Based on S_2, B_1, and *Rules* 2 and 4, $S_5 : S \mid\equiv A \mid\equiv \langle AID_i, \alpha P, T_i, A \xleftrightarrow{SK} S \rangle$.

Based on S_5, *Rule* 5, $S_6 : S \mid\equiv A \mid\equiv A \xleftrightarrow{SK} S$ (*Goal* 4).

Based on S_6, B_6, and *Rule* 3, $S_7 : S \mid\equiv A \xleftrightarrow{SK} S$ (*Goal* 2).

Based on S_4, B_2, *Rules* 2 and 4, $S_8 : A \mid\equiv A \mid\equiv \langle \beta P, T_s, A \xleftrightarrow{SK} S \rangle$.

Based on S_8, *Rule* 5, $S_9 : A \mid\equiv S \mid\equiv A \xleftrightarrow{SK} S$ (*Goal* 3).

Based on S_9, B_5, *Rule* 3, $S_{10}: A \mid\equiv A \xleftrightarrow{SK} S$ (*Goal* 1)

6.2 Further Security Discussion

Further, the proposed scheme can satisfy various types of functional features and prevent various attacks.

6.2.1 User Untraceability

Assume that an attacker A can obtain the login message $\{AID_i, E_i, F_i, T_i\}$ of U_i. However, the parameters AID_i, E_i, F are protected by a random number α, which is different in each conversation. Therefore, A cannot trace user U_i by the transmitted messages, and the proposed scheme provides user untraceability.

6.2.2 User Anonymity

An authentication scheme can provide user anonymity if there is no attacker with the ability to compromise the user's identity. In the proposed scheme, an attacker A cannot obtain the user's real identity by launching any active or passive attack in every phase. Considering the registration, login, and authentication phases, the identity of U_i is protected by a secure one-way hash function; therefore, A cannot obtain it. As no message is transmitted in the password-change phase, A cannot obtain the identity of U_i.

Furthermore, A cannot launch a guessing attack to obtain the identity of U_i because without the server's secret key x, A cannot compute the parameter $H_i = H_i' = xE_i$ and hence cannot use $F_i = h(ID_i \| A_i \| E_{ii} \| H_i \| T_i)$ or $G_i = h(ID_i' \| A_i' \| M_i \| H_i' \| T_s)$ or $AID_i = ID_i \oplus h(H_i)$ to verify the correctness of guessed identity ID_i^*.

In a word, in the proposed scheme, nobody can know the actual identity of U_i besides U_i and server S.

6.2.3 User Impersonation Attack

In this attack, an attacker A may attempt to masquerade as a legal user to login into the server. Suppose that A has already obtained all the messages $\{AID_i, E_i, F_i, T_i, M_i, G_i, T_s\}$ transmitted in the channel and the secret data $\{B_i, C_i, P_{pub}, h(\cdot), P, P_i\}$ stored in the smart card. However, without the identity of U_i and server's master key x, A cannot construct the parameter $A_i = h(ID_i \oplus x)$ which is required in the parameter $F_i = h(ID_i \| A_i \| E_i \| T_i)$. Therefore, the login request message $\{AID_i, E_i, F_i, T_i\}$ cannot be constructed. Thus, the proposed scheme can prevent user impersonation attack.

6.2.4 Server Spoofing Attack

In this attack, an attacker A may attempt to masquerade as a legal user to login into the server. Suppose that A has already obtained all the messages $\{AID_i, E_i, F_i, T_i, M_i, G_i, T_s\}$ transmitted in the channel and the secret data $\{B_i, C_i, P_{pub}, h(\cdot), P, P_i\}$ stored in the smart card. However, without the identity of U_i and server's master key x, A cannot construct the parameter $A_i = h(ID_i \oplus x)$ that is required in the parameter $F_i = h(ID_i \| A_i \| E_i \| H_i \| T_i)$. Therefore, the login request message $\{AID_i, E_i, F_i, T_i\}$ cannot be constructed. Thus, the proposed scheme can prevent user impersonation attack.

6.2.5 Man-in-the-middle Attack

Because an attacker A can neither masquerade as a legitimate user nor as a legal server in the login and authentication phases, there is no way to establish two session keys with the user and remote server. Thus, the proposed scheme can prevent man-in-the-middle attack.

6.2.6 Outsider Attack

In this attack, the attacker has registered with server S, not the user of the system. In this situation, A can obtain the smart card from the server with the data $\{B_\alpha, C_\alpha, P_{pub}, h(\cdot), P\}$. To obtain the server's secret key x, it must be extracted from point $P_{pub} = xP$. This is computationally impossible due to the hardness of **ECDLP**. Thus, the proposed method can prevent outsider attack.

6.2.7 Stolen Smart Card Attack

Suppose that an attacker A obtains the secret data $\{B_i, C_i, P_{pub}, h(\cdot), P, P_i\}$ stored in the smart card and captures all the transmitted messages $\{AID_i, E_i, F_i, T_i, M_i, G_i, T_s\}$ from a public channel. To establish an authorized conversation with server S, $F_i = h(ID_i \| A_i \| E_i \| H_i \| T_i)$ must be constructed in the login phase. This is impossible as $A_i = B \oplus RPW_i = h(ID_i \oplus x)$ cannot be forged in the absence of RPW_i or the user's identity ID_i and server's master key x. Thus, the proposed method can prevent stolen smart card attack.

6.2.8 Session Key Security

In the proposed scheme, only user U_i and server S can calculate the shared session key $SK =$

$h(\alpha M_i \| A_i \| T_i \| T_s) = h(\beta E_i \| A_i' \| T_i \| T_s)$ as the random numbers α and β are different in every conversation. During each conversation, with the captured information $\{AID_i, E_i, F_i, T_i, M_i, G_i, T_s\}$, A cannot calculate $\alpha\beta P$ using the values E_i and M_i due to the hardness of **ECCDHP**. Besides, the server's secret key *x* is unknown to *A*, which is needed when computing H_i. Therefore, *A* cannot calculate *SK*. Thus, the proposed scheme provides session key security.

6.2.9 Session Key Security

Known-key security means that when the authentication and key agreement scheme is executed, the user and server generate a unique session key. In other words, although the session key generated between the user and server is compromised, no impact is made on another session key. In the proposed scheme, suppose A knows $SK = h(\alpha M_i \| A_i \| T_i \| T_s) = h(\beta E_i \| A_i' \| T_i \| T_s)$, the random numbers α and β, and the server's secret key *x*, it is impossible for *A* to construct another key $SK^* = h(\alpha^* M_i \| A_i \| T_i \| T_s) = h(\beta^* E_i \| A_i' \| T_i \| T_s)$ because α^*, β^* are different and cannot be extracted from $E_i = \alpha^* P$ and $M_i = \beta^* P$. Thus, the proposed scheme provides known-key security.

6.2.10 Perfect Forward Secrecy

Perfect forward secrecy means that with the secret keys of U_i and server *S*, an attacker still cannot obtain the previous session keys. In the proposed scheme, the long-term secret key of U_i is PW_i and data $\{B_i, C_i, P_{pub}, h(\cdot), P, P_i\}$ stored in the smart card, and that of server S is the secret key *x*. Then, when A attempts to compute $SK = h(\alpha M_i \| A_i \| T_i \| T_s) = h(\beta E_i \| A_i' \| T_i \| T_s)$, A faces the hardness of **ECCDHP**. Therefore, the proposed scheme provides perfect forward secrecy.

6.2.11 Li et al.'s New Insider Attack

Li et al. proposed a new insider attack in their paper. That is, an attacker *A* steals the users' *ID* from a registration server and then use these stolen data and transmitted messages in the public channel to impersonate a legal user. However, in our scheme, the registration server does not store users' *ID* in the database. It means that *A* cannot obtain any useful information from the server. Therefore, the proposed scheme resists Li et al.'s new insider attack.

7 Performance Analysis

In this section, the security features and communication cost are compared among the proposed scheme and other schemes [14-15, 26-31].

Form Table 2, we can conclude that only the proposed protocol can fit all secure requirements such as user impersonation attack, server spoofing attack, man-in-the-middle attack, replay attack, and stolen smart card attack. Besides, the proposed protocol can provide session key security, known-key security, perfect forward secrecy and freely selected and exchanged password.

The Table 3 shows that the proposed scheme performs one more hash operation and two further scale multiplication functions than Moon et al.'s scheme to achieve authentication and key agreement; however, the proposed scheme performs better in terms of the ability to prevent different kinds of attacks.

Table 2. Comparison of security features (Y: Satisfy N: Not satisfy)

	[14]	[15]	[28]	[30]	[26]	[27]	[29]	[31]	Proposed
F1	Y	Y	Y	Y	N	N	N	N	Y
F2	Y	Y	Y	Y	N	N	N	N	Y
F3	Y	Y	Y	Y	N	N	N	N	Y
F4	Y	Y	Y	Y	Y	Y	N	Y	Y
F5	Y	Y	Y	Y	Y	Y	Y	Y	Y
F6	Y	Y	Y	Y	Y	Y	Y	Y	Y
F7	Y	Y	Y	Y	Y	Y	Y	Y	Y
F8	N	Y	Y	N	N	Y	N	Y	Y
F9	Y	N	Y	Y	Y	Y	Y	Y	Y

F1: Withstanding user impersonation attack, F2: withstanding server spoofing attack,
F3: withstanding man-in-the-middle attack, F4: withstanding replay attack, F5: withstanding stolen smart card attack, F6: satisfying session key security, F7: satisfying known-key security, F8: providing perfect forward secrecy, F9: freely selected and exchanged password

Table 3. Comparison of cost among the proposed scheme and other schemes

	C1	C2	C3	C4	C5	C6	Total
[14]	1H	2H+3S	3H+3S	4H+6S+1M	1H+5S	1H+5S	12H+22S+1M
[15]	-	2H+1S	4H+2M	4H+1S+2M	2H	-	12H+2S+4M
[28]	1H	2H+3S	8H+4S	10H+10S+1M	1H+6S	1H+9S	23H+32S+1M
[30]	-	2H+1S	3H+1S	3H+1S+1E	-	-	8H+2S+2E
[26]	-	1H+1S	2H+2M+4E	1H+1M+4E	3H+2M+2E	3H+2M+3E	10H+14E+7M
[27]	-	2H+2S	4H+1M+4E	3H+3E	3H+2M+4E	-	12H+3M+13E
[29]	1H	3H	6H	6H	4H	-	20H
[31]	1H+1F	4H	3H+1F+2P	4H+2P	3H+1F	-	15H+3F+4P
The proposed	1H+1F	2H	4H+1F+3P	5H+3P	4H+1F	-	16H+3F+6P

C1: Computational cost of user in registration phase, C2: computational cost of server in registration phase, C3: computational cost of user in login and authentication phases, C4: computational cost of server in login and authentication phases, C5: computational cost of user in password-change phase C6: Computational cost of the server in password-change phase,
H: hashing operation, E: modulus exponential operation, S: symmetric encryption/decryption operation M: Multiplication/ division operation,
P: scalar multiplication, F: fuzzy extraction, Null: cannot provide this functionality.

8 Conclusion

In this study, we analyzed a smart card based three-factor authentication scheme proposed by Moon et al. claimed to have the ability to prevent various attacks. However, the scheme was found to be susceptible to traceability attack, offline identity-guessing attack, impersonation attack, and man-in-the-middle attack even without the new attack scenario as suggested by Li et al. To solve the security weaknesses in Moon et al.'s scheme, a new three-factor remote user authentication key agreement scheme was designed. The proposed scheme can prevent various attacks; the proposed scheme was validated using the well-known BAN logic.

Acknowledgements

The work of Yong Zhang was supported in part by the Science & Technology Plan Projects of Shenzhen (JCYJ20170302145623566). The work of Tsu-Yang Wu was supported in part by the Natural Science Foundation of Fujian Province under Grant no. 2018J01636 and the Science and Technology Development Center, Ministry of Education, China under Grant no. 2017A13025.

References

[1] L. Lamport, Password Authentication with Insecure Communication, *Communications of the ACM*, Vol. 24, No. 11, pp. 770-772, November, 1981.

[2] S. M. Bellovin, M. Merritt, Augmented Encrypted Key Exchange: A Password-based Protocol Secure against Dictionary Attacks and Password File Compromise, *Proceedings of the 1st ACM Conference on Computer and Communications Security*, Fairfax, Virginia, 1993, pp. 244-250.

[3] W.-S. Juang, S.-T. Chen, H.-T. Liaw, Robust and Efficient Password-authenticated Key Agreement Using Smart Cards, *IEEE Transactionson Industrial Electronics*, Vol. 55, No. 6, pp. 2551-2556, June, 2008.

[4] C.-M. Chen, Y. Huang, E. K. Wang, T.-Y. Wu, Improvement of a Mutual Authentication Protocol with Anonymity for Roaming Service in Wireless Communications, *Data Science and Pattern Recognition*, Vol. 2, No. 1, pp. 15-24, 2018.

[5] J. Nam, K.-K R. Choo, S. Han, J. Paik, D. Won, Two-round Password-only Authenticated Key Exchange in the Three-party Setting, *Symmetry*, Vol. 7, No. 1, pp. 105-124, January, 2015.

[6] N. Anwar, I. Riadi, A. Luthfi, Forensic SIM Card Cloning Using Authentication Algorithm, *International Journal of Electronics and Information Engineering*, Vol. 4, No. 2, pp. 71-81, June, 2016.

[7] C.-C. Chang, C.-S. Laih, Remote Password Authentication with Smart Cards, *IEE Proceedings E-Computers and Digital Techniques*, Vol. 139, No. 4, pp. 372, July, 1992.

[8] D. Mishra, A. Chaturvedi, S. Mukhopadhyay, Design of a Lightweight Two-Factor Authentication Scheme with Smart Card Revocation, *Journal of Information Security and Applications*, Vol. 23, pp. 44-53, August, 2015.

[9] A. G. Reddy, A. K. Das, E.-J. Yoon, K.-Y. Yoo, A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography, *IEEE Access*, Vol. 4, pp. 4394-4407, July, 2016.

[10] A. G. Reddy, E.-J. Yoon, A. K. Das, K.-Y. Yoo, Lightweight Authentication with Key-Agreement Protocol for Mobile Network Environment Using Smart Cards, *IET Information Security*, Vol. 10, No. 5, pp. 272-282, September, 2016.

[11] S. Kumari, X. Li, A. K. Das, H. Arshad, M. K. Khan, A User Friendly Mutual Authentication and Key Agreement Scheme for Wireless Sensor Networks Using Chaotic Maps, *Future Generation Computer Systems*, Vol. 63, pp. 56-75, October, 2016.

[12] M. Karuppiah, S. Kumari, A. K. Das, X. Li, F. Wu, S. Basu, A Secure Lightweight Authentication Scheme with User

Anonymity for Roaming Service in Ubiquitous Networks, *Security and Communication Networks*, Vol. 9, No. 17, pp. 4192-4209, August, 2016.

[13] S. A. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, M. K. Khan, An Enhanced Privacy Preserving Remote User Authentication Scheme with Provable Security, *Security and Communication Networks*, Vol. 8, No. 18, pp. 3782-3795, June, 2015.

[14] C.-M. Chen, C.-T. Li, S. Liu, T.-Y. Wu, J.-S. Pan, A Provable Secure Private Data Delegation Scheme for Mountaineering Events in Emergency System, *IEEE Access*, pp. 3410-3422, February, 2017.

[15] H.-M. Sun, B.-Z. He, C.-M. Chen, T.-Y. Wu, C.-H. Lin, H. Wang, A Provable Authenticated Group Key Agreement Protocol for Mobile Environment, *Information Sciences*, Vol. 321, November, 2015.

[16] K.-H. Wang, C.-M. Chen, W. Fang, T.-Y. Wu, A Secure Authentication Scheme for Internet of Things, *Pervasive and Mobile Computing*, Vol. 42, pp. 15-26, Dec. 2017.

[17] C.-G. Ma, D. Wang, S.-D. Zhao, Security Flaws in Two Improved Remote User Authentication Schemes Using Smart Cards, *International Journal of Communication Systems*, Vol. 27, No.10, pp. 2215-2227, October, 2014.

[18] T. S. Messerges, E. A. Dabbish, R. H. Sloan, Examining Smart-card Security under the Threat of Power Analysis Attacks, *IEEE transactions on computers*, Vol. 51, No. 5, pp. 541-552, August, 2002.

[19] E.-J. Yoon, K.-Y. Yoo, Robust Biometrics-based Multi-Server Authentication with Key Agreement Scheme for Smart Cards on Elliptic Curve Cryptosystem, *The Journal of Supercomputing*, Vol. 63, No.1, pp. 235-255, January, 2013.

[20] D. He, Security Flaws in a Biometrics-based Multi-server Authentication with Key Agreement Scheme, *IACR Cryptology ePrint Archive*, 2011, pp. 365.

[21] H. Kim, W. Jeon, K. Lee, Y. Lee, D. Won, Cryptanalysis and Improvement of a Biometrics-Based Multi-Server Authentication with Key Agreement Scheme, *International Conference on Computational Science and Its Applications*, Springer, Berlin, Heidelberg, 2012, pp. 391- 406.

[22] M.-C. Chuang, M.-C. Chen, An Anonymous Multi-Server Authenticated Key Agreement Scheme Based on Trust Computing Using Smart Cards and Biometrics, *Expert Systems with Applications*, Vol. 41, No. 4, pp. 1411-1418, March, 2014.

[23] D. Mishra, A. K. Das, S. Mukhopadhyay, A Secure User Anonymity-preserving Biometric-based Multi-Server Authenticated Key Agreement Scheme Using Smart Cards, *Expert Systems with Applications*, Vol. 41, No. 18, pp. 8129-8143, December, 2014.

[24] H. Lin, F. Wen, C. Du, An Improved Anonymous Multi-Server Authenticated Key Agreement Scheme Using Smart Cards and Biometrics, *Wireless Personal Communications*, Vol. 84, No. 4, pp. 2351-2362, October, 2015.

[25] K.-H. Wang, C.-M. Chen, W. Fang, T.-Y. Wu, On the Security of a New Ultra-Lightweight Authentication Protocol in Iot Environment for RFID Tags, *Journal of Supercomputing*, Vol. 74, Issue 1, pp. 65-70, January, 2018.

[26] C.-M. Chen, K.-H. Wang, T.-Y. Wu, E. K. Wang, On the Security of a Three-party Authenticated Key Agreement Protocol Based on Chaotic Maps, *Data Science and Pattern Recognition*, Vol. 1, No. 2, pp. 1-10, December, 2017.

[27] X. Li, J. Niu, M. K. Khan, J. Liao, An Enhanced Smart Card Based Remote User Password Authentication Scheme, *Journal of Network and Computer Applications*, Vol. 36, No. 5, pp. 1365-1371, September, 2013.

[28] X. Li, W. Qiu, D. Zheng, K. Chen, J. Li, Anonymity Enhancement on Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards, *IEEE Transactions on Industrial Electronics*, Vol. 57, No. 2, pp. 793-800, August, 2009.

[29] Y.-J. Liu, C.-C. Chang, S.-C. Chang, An Efficient and Secure Smart Card Based Password Authentication Scheme, *International Journal of Network Security*, Vol. 19, No. 1, pp. 1-10, January, 2017.

[30] R. Song, Advanced Smart Card Based Password Authentication Protocol, *Computer Standards & Interfaces*, Vol. 32, No. 5-6, pp. 321-325, October, 2010.

[31] J. Moon, D. Lee, J. Jung, D. Won, Improvement of Efficient and Secure Smart Card Based Password Authentication Scheme, *International Journal of Network Security*, Vol. 19, No. 6, pp. 1053-1061, November, 2017.

[32] W. Li, Y. Shen, P. Wang, Breaking Three Remote User Uthentication Systems for Mobile Devices, *Journal of Signal Processing Systems*, Vol. 90, No. 8-9, pp. 1179-1190, September, 2018.

[33] N. Koblitz, Elliptic Curve Cryptosystems, *Mathematics of Computation*, Vol. 48, No. 177, pp. 203-209, Math, 1987.

[34] N. Koblitz, A. Menezes, S. Vanstone, The State of Elliptic Curve Cryptography, *Designs, Codes and Cryptography*, Vol. 19, No. 2-3, pp. 173-193, March, 2000.

[35] V. S. Miller, Use of Elliptic Curves in Cryptography, *Conference On the Theory and Application of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 1985, pp. 417-426.

[36] Y. Dodis, L. Reyzin, A. Smith, Fuzzy Extractors: How to Generate Strong Keys from Biometrics and other Noisy Data, *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 2004, pp. 523-540.

[37] S. Kumari, A. K. Das, X. Li, F. Wu, M. K. Khan, Q. Jiang, S. K. Hafizul, A Provably Secure Biometrics-based Authenticated Key Agreement Scheme for Multi-Server Environments, *Multimedia Tools and Applications*, Vol. 77, No. 2, pp. 2359-2389, January, 2018.

[38] P. Chandrakar, H. Om, An Efficient Two-Factor Remote User Authentication and Session Key Agreement Scheme Using Rabin Cryptosystem, *Arabian Journal for Science and Engineering*, Vol. 43, No. 2, pp. 661-673, February, 2018.

[39] H. Xiong, J. Sun,, Comments on Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing, *IEEE Transactions on Dependable and Secure Computing*, Vol. 14, No. 4, pp. 461-462, 2017.

[40] H. Xiong, J. Tao, C. Yuan, Enabling Telecare Medical

Information Systems with Strong Authentication and Anonymity, *IEEE Access*, Vol. 5, pp. 5648-5661, March, 2017.

Biographies

Chien-Ming Chen received his Ph.D. from the National Tsing Hua University, Taiwan. He is currently an associate professor of College of Computer Science and Engineering at Shandong University of Science and Technology, China. Dr. Chen serves as an executive editor of International Journal of Information Computer Security. He also serves as an associate editor of three international Journals: Journal of Information Hiding and Multimedia Signal Processing, Data Science and Recognition, Journal of Network Intelligence. His current research interests include network security, mobile internet, wireless sensor network and cryptography.

Bin Xiang is currently pursuing the M.S. degree in Harbin Institute of Technology Shenzhen Graduate School, China. His current research interests include security protocol and network security.

King-Hang Wang received his Ph.D. from the National Tsing Hua University and BEng from the Chinese University of Hong Kong. He worked in the Hong Kong Institute of Technology in 2010 as a lecturer. He joined the Hong Kong University of Science and Technology since 2015. His research focus is cryptography, mobile security, and provable authentication.

Yong Zhang was born in 1976. He received the B.S., M.S. and Ph.D. degrees in Communication Engineering from PLA Science and Technology University, Nanjing, China, in 1997, 2001 and 2004 respectively. He is currently working as a professor in Shenzhen University, China. His research interests include intelligence information processing, information security and cloud computing, etc.

Tsu-Yang Wu received the Ph.D. degree in Department of Mathematics, National Changhua University of Education, Taiwan in 2010. Currently, he is an associate professor in College of Computer Science and Engineering at Shandong University of Science and Technology, China. In the past, he is an assistant professor of Shenzhen Graduate School, Harbin Institute of Technology. He serves as executive editor in Journal of Network Intelligence and as associate editor in Data Science and Pattern Recognition. His research interests include cryptography and network security.