Peer-to-Peer Netw. Appl. (2018) 11:63–73
DOI 10.1007/s12083-016-0499-3

An efficient and secure three-factor based authenticated key exchange scheme using elliptic curve cryptosystems

Lidong Han[1] · Xiao Tan[1] · Shengbao Wang[1] · Xikun Liang[1]

Received: 23 February 2016 / Accepted: 31 July 2016 / Published online: 5 September 2016

Abstract Recently, many authentication schemes have been provided which are based on biometrics with password and smart cards. The three-factor schemes can provide high security for remote authentication between a user and a server. In 2015, Lu et al. proposed a three-factor authentication scheme based on elliptic curve cryptography. However, we show that Lu et al's scheme leaks user's identity and is vulnerable to impersonation attacks. To enhance the scheme's security, we propose a new efficient three-factor authentication scheme. Furthermore, we give a formal security proof under BAN logic and random orale model. From comparative results of some recent ones, our scheme is efficient and secure for practical applications.

Keywords Authentication · Three factor · Elliptic curve cryptography · Biometric

✉ Shengbao Wang
shengbaowang@hznu.edu.cn

Lidong Han
ldhan@hznu.edu.cn

Xiao Tan
xiaotan.cs@gmail.com

Xikun Liang
schenken@163.com

[1] Institute of Information Science and Engineering, Hangzhou Normal University, Zhejiang, China

1 Introduction

With the rapid development of internet, authentication schemes are used to establish a secure communication over any insecure channel. After executing the authenticated protocol, the remote legal user can login and authenticate from a server, and access to special services. The server must reject the unauthorized or malicious entity who wants to use resources and services offered by the server. Researchers have studied two-factor authentication schemes based on password and a memory device. A user who has a smart card and a correct password can login and authenticate the special system. The user and the server agree on the same session key which is only known for both parties and is used to encrypt the message transmitted over a insecure internet.

Furthermore, many researchers consider biometrics as another factor to improve the security of authentication schemes, and the biometric contains face, fingerprint and iris and so on. The authentication schemes which are based on password, biometric and memory devices are generally called three-factor based schemes. Up to now, there are many various authentication schemes proposed to utilize in different applications. However, people also have presented many attacks against password based authentication schemes, such as password guessing attack, replay attack, impersonation attack, denial of service attack, etc. The legal user does not want to leak his/her identity to other parties except the server. Usually, the user's password is very short in order to remember easily. Hence, the secure scheme must resist password guessing attack. Moreover, the legal party can not impersonate as any entity to deceive a server or as a server to cheat a legal user. In a word, a secure and efficient authentication scheme must protect the user's privacy and reject a malicious adversary to access the services.

In 1981, Lamport [17] proposed the first password authentication scheme with one-way hash function. Password based protocols may suffer from password leakage attacks, insider attacks and server-spoofing attacks and require verification table to improve the security. Chang et al. [3, 4] presented a user authentication based on two factor password and smart card. Since then, many authors proposed different two-factor authentication schemes for various applications [9, 11, 13, 16, 26–28]. In 2004, Das et al. [9] proposed an dynamic ID-based authentication scheme with user anonymity. But Das et al.'s scheme is susceptible to impersonation attack by Ku and Chen [16] and insider attack and server spoofing attack by [27]. Wang et al. [26] proposed an improved authentication scheme. Khan et al. showed their scheme cannot protect user's anonymity in [13]. Wu et al. [28] proposed an efficient authentication scheme using smart card with pre-computation. However, He et al. [11] found that Wu et al.'s scheme is not secure against impersonation attacks and insider attacks.

All above mentioned authentication schemes are based on two factors password and smart cards. Lately, researchers focused on three factor based authentication and key agreement schemes by employing biometrics [1, 6, 14, 18, 25, 29, 30]. In 2013, Yeh et al. [30] showed that Fan et al.'s scheme is insecure against insider attack and presented an improved biometric based authentication scheme using elliptic curve cryptosystem (ECC). Wu et al. [29] gave a new smart card authentication protocol for telecare medicine information systems (TMIS) and claimed it's secure against offline password guessing attack, and impersonation attack and replay attack. Siddiqui et al. in [25] pointed out Wu et al.'s scheme is vulnerable to the mentioned attacks. Chen et al. [6] presented a new three factor authentication protocol based mobile devices. However, Chen et al.'s scheme was insecure against replay attack, forgery attack and can't provide user anonymity. Khan et al. [14] proposed an improved scheme based on Chen et al's scheme. In 2014, Arshad et al. [1] gave a new three factor based authentication scheme. Recently, Lu et al. [18] pointed out the security flaws of of Arshad et al.'s scheme, and proposed an biometric-based authentication schemes using elliptic curve cryptosystems.

Recently, some researchers proposed other different three-factor authentication schemes [7, 19, 23, 24] for other application scenarios such as session initial protocol and cloud computing.

In this paper, we demonstrate that Lu et al.'s scheme fails to protect patient's anonymity. Additionally, we show that a legal user can impersonate any user of the system to communicate with the server, and disguise as a legitimate server to deceive a user. Furthermore, we put forward an improved biometric based authentication scheme to deal with the weakness of Lu et al.'s scheme. Our proposed scheme is robustly proven secure by Burrows-Abadi-Needham (BAN) logic and random oracle model of cryptography. Compared to some previous authentication schemes, the new scheme employs low computational cost in login and authentication phases.

The remainder of this paper is organized as follows: In first section, we introduce some notations and definitions used in this paper. Section 2 will review the biometric - based authentication scheme by Lu et al. Section 3 analyzes the security problems of Lu et al.'s protocol. We present a new biometric-based authentication scheme based on ECC in Section 4. Section 5 will prove the robust correctness and security of our scheme by BAN logic and ransom model method, respectively. And Section 6 give a comparison of our scheme and some previous authentication schemes in the aspect of security and efficiency. Finally, we give a conclusion in the last section.

1.1 Notations

In this section we will give some notations and definitions used throughout this paper, and introduce some cryptographic tools such as bio-hashing.

Table 1 lists the notations that will be appeared in this paper.

In Table 1, one-way hash function $h(\cdot)$ maps an arbitrary long string of to a string with fixed length which is denoted as hashed value. It can be represented as $h : \{0,1\}^* \rightarrow \{0,1\}^n$. Such hash function is easy to compute the output value with each input, but is hard to find the preimage given the hashed value.

When we compute hash function and $\oplus$ operation with the elliptic curve point $P = (x, y)$, we represent the point P as a value $x||y$.

Table 1 Notations

Symbol	Description
U	the user/patient
S	The telecare server
PW, ID, B	Password, Identity, Biometric of user
x	Private key of server
$h(\cdot)$	Cryptographic One-way hash function
$H(\cdot)$	Biometric Hash function
SK	Session key between U and S
$\|\|$	String concatenation operation
$\oplus$	Exclusive-or operation
$E_x(\cdot)$	Symmetric encryption with x
$D_x(\cdot)$	Symmetric decryption with x

1.2 Bio-hashing

Recently, people add the biometrics in authentication schemes to prove the user be genuine. However, imprint biometric characteristics such as fingerprint and face may not be exactly same at each time. Therefore, high false rejection of valid users often occurs in the verification of biometric schemes. In order to resolve this problem, Jin et al. [12] proposed a two-factor authenticator on iterated inner products between tokenised pseudo-random number and the user specific fingerprint features, which produces a set of user specific compact code that coined as Bio-Hashing. Bio-Hashing maps user's biometric onto specific random vectors in order to generate a code (called biocode), and then it discretizes the projection coefficients into zero and one. More details refer to the references [5, 20].

2 Review of Lu et al.'s scheme

In this section we review Lu et al.'s three-factor authentication scheme based on elliptic curve cryptography [18], which is based on Arshad et al.'s scheme [1]. It consists of four phases: registration, login, authentication, password change. We will introduce these phases briefly in the following.

2.1 Registration phase

When a user U_i want to registers to the server S, S issues the personalized smart card via the following steps:

- The user U_i inputs his biometric B_i, selects an identity ID_i, a password PW_i. The he computes $MP_i = PW \oplus H(B_i)$, and submits $\{ID_i, MP_i\}$ to the server S through a secure channel.
- S computes $AID_i = ID_i \oplus h(x)$ and $V_i = h(ID_i||MP_i)$, where x is S 's secret key. S issues a smart cardSC_i containing $\{AID_i, V_i, h(\cdot), H(\cdot)\}$ to the user U_i.

2.2 Login and authentication phase

- U_i first inserts smart card SC_i into a device reader, and enters his identity ID_i, password PW_i and imprints biometric B_i at the sensor. Then SC_i verifies whether $h(ID_i||PW_i \oplus H(B_i)) = V_i$. If correct, goto next step. Otherwise, reject the request.
- SC_i selects a random number d_u, and computes $K = h(ID_i||ID_i \oplus AID_i)$, $M_1 = K \oplus d_u P$ and $M_2 = h(ID_i||d_u P||T_1)$. The smartcard SC_i sends the message $\{ M_1, M_2, AID_i, T_1 \}$ to S.
- After receiving the request, S first checks whether $|T_c - T_1| < \Delta T$, where T_c is current time stamp. If true, S use his private key x to extract ID_i by computing $AID_i \oplus h(x)$. Then he computes $d_u P = h(ID_i||h(x)) \oplus M_1$ and verifies whether $M_2 = h(ID_i||d_u P||T_1)$. If it holds, S generates a random d_s, and computes $M_3 = K \oplus d_s P$, $SK = d_s(d_u P)$, $M_4 = h(K||d_u P||SK||T_2)$, where T_2 is the current time. Then, S submits $\{M_3, M_4, T_2\}$ to U_i.
- Upon receiving the message from S, SC_i checks T_2's validity. Then, U extracts $d_s P$ by computing $M_3 \oplus K$. The he calculates $SK = d_u(d_s P)$, $M_4' = h(K||d_u P||SK||T_2)$. It checks whether $M_4' = M_4$ holds. If correct, SC_i computes $M_5 = h(K||d_s P||SK||T_3)$ and then sends the response $\{M_5, T_3\}$.
- S checks T_3, and verifies $h(K||d_s P||SK||T_3) \stackrel{?}{=} M_5$. If both correct, S authenticates U_i and accepts SK as a session key.

2.3 Password change phase

If a user U_i wants to change his password, U_i inserts the smart card into card reader and keys in ID_i, PW_i and B_i. Then, SC_i checks $h(ID_i||PW_i \oplus H(B_i)) \stackrel{?}{=} V_i$. If holds, U_i inputs a new password PW_i^{new}, SC_i computes $V_i^{new} = h(ID_i||PW_i^{new} \oplus H(B_i))$ and then it replaces V_i by V_i^{new}.

3 Security weakness of Lu et al.'s scheme

This section shows that Lu et al.'s scheme fails to achieve the security goals they claimed. In attack model, we assume that an adversary could obtain the information which is stored into a user's smartcard by monitoring the power consumption as in [15, 21]. An adversary has the ability of controlling over the communication channel that he can extract and modify the transmitting message between U_i and S. In the following, we will discuss the security of Lu et al.'s scheme in detail.

3.1 User's identity leakage

In Lu et al.'s scheme, the user's identity is obscured by computing $AID_i = ID_i \oplus h_2(x)$, which is transmitted by public channel in login phase. For external adversary, it's very difficult to recover the patient's identity without knowledge of the secret value x. However, for a legal but malicious user U_j, he can retrieve $h(x)$ using his own identity ID_j and the value AID_j stored in smart card. Then, U_j can compute any other patient's identity by computing $ID = AID \oplus h(x)$, where AID is intercepted by U_j in ini-

tiating login phase. Therefore, Lu et al.'s scheme does not protect user anonymity since a user's identity is leaked to a malicious user.

3.2 Server impersonation attack

Lu et al. claimed their scheme could withstand various attacks. Now, we demonstrate a legitimate user U_j can impersonate as a legal sever. He perform the following steps to impersonate as a legal server.

- (1). U_j extracts the secret information $\{V_i, AID_i, h(\cdot), H(\cdot)\}$ stored into his smart card by executing the power attack. U_j retrieve $h(x)$ by computing $AID_i \oplus ID_i$ using his password PW.
- (2). When a user U_i performs the login and authentication process and sends $\{M_1, M_2, AID_i, T_1\}$ to S. U_j intercepts the login message.
- (3). U_j computes $AID_i \oplus h(x)$ using $h(x)$ to extract the identity of U_i. Then U_j chooses a random $d_s' \in Z_p^*$, and computes $M_3' = h(ID_i||h(x)) \oplus d_s'P$, $SK' = d_s'(d_uP)$, $M_4' = h(K|T_2||SK'||d_uP|)$, where T_2 is current time stamp. U_j returns the responding message $\{M_3', M_4', T_2\}$ to U_i
- (4). U_i verifies T_2 's freshness. Then He computes $K \oplus M_3' = d_s'P$, $SK = d_u(d_s'P)$, $M_4^* = h(K||d_uP||SK||T_2) \stackrel{?}{=} M_4'$. U_i accepts the session key SK and believes U_j as a legitimate sever.

Therefore, a legal patient can simulate as a legitimate sever to all other users.

3.3 User impersonation attack

This subsection shows a malicious user can impersonate to be any other user to communicate with a server. The sever does not identify the communication party's true identity.

- (1). U_j can get $h(x)$ by computing $AID_i \oplus ID_i$ as similar as step 1 in server impersonation, where AID_i is retrieved in his his smart card.
- (2). When another patient U_i initiates the login process and transmits the request $\{M_1, M_2, AID_i, T_1\}$ to S. U_j extracts AID_i from the request message and computes $ID_i = AID_i \oplus h(x)$. The adversary U_j terminates this session.
- (3). U_j selects a random nonce $d_u' \in Z_p^*$, current time stamp T_1, calculates $K = h(ID_i||h_2(x))$, $M_1' = K \oplus d_u'P$ and $M_2' = h(ID_i||T_1||d_u'P)$. Then U_j sends the login message $\{M_1', M_2', AID_i, T_1\}$ as the login message of U_i to S.
- (4). After receiving the login message, S verifies whether $|T_1 - T_s| \leq \Delta$. If not true, S aborts the session. Otherwise, S computes $ID_i = AID_i \oplus h(x)$. Then U_j chooses a random number $d_s \in Z_p^*$, and computes $M_3 = h(ID_i||h(x)) \oplus d_sP$, $SK = d_s(d_uP)$, $M_4 = h_1(K|T_2||SK'||d_uP|)$, where T_2 is the current time stamp. U_j sends $\{M_3, M_4, T_2\}$ to U_i
- (5). U_j computes $K \oplus M_3 = d_sP$, $SK = d_u(d_sP)$. Then checks whether $M_4^* = h(K||d_uP||SK||T_2) \stackrel{?}{=} M_4'$. U_j computes $M_5 = h(K||d_sP||SK||T_3)$ and then sends the message $\{M_3, T_3\}$ to S.
- (6). S checks the freshness of T_3 from the received message, and verifies $M_5' = h(K||d_sP||SK||T_3) \stackrel{?}{=} M_5$. S authenticates U_j as U_i and accepts SK as the session key.

From the above discussion, Lu et al.'s scheme is vulnerable to user impersonation attack.

4 Proposed scheme

In this section, we propose an improved three-factor authentication scheme. One achievement is that we replace the hashed value $h(x)$ with $h(ID_i||x)$ which can prevent to be leaked. Each user has different hashed value. In the following, we will describe the proposed scheme in details, which has four phases (Figs. 1, 2 and 3).

4.1 Registration phase

A user U_i selects his identity and password and then registers his identity to the server S. Server registers the user and provides the valid smart card in return.

- The patient U_i generates a random number r, and chooses his identity ID_i, password PW_i and his biometric B_i. He computes $MP_i = PW_i \oplus H(B_i) \oplus r$, and sends $\{ID_i, MP_i\}$ to the server S through a secure channel.
- The sever S computes $AID_i = h(ID_i||x)$, $K_i = h(AID_i)$, $V_i = AID_i \oplus MP_i$. Then, S generates a number a randomly and computes $CID_i = E_x(ID_i||a)$. The server issues a smartcard SC_i to the patient U_i which is stored by $\{K_i, V_i, CID_i, h(\cdot), H(\cdot)\}$.
- Upon receiving the smart card, U_i computes $R_i = r \oplus h(ID_i||PW_i||H(B_i))$, and stores R_i into SC_i.

4.2 Login and authentication phase

A legal user with valid smart card can establish secure and authorized session with the server. In this phase, user and server first authenticate each other and then agree on a

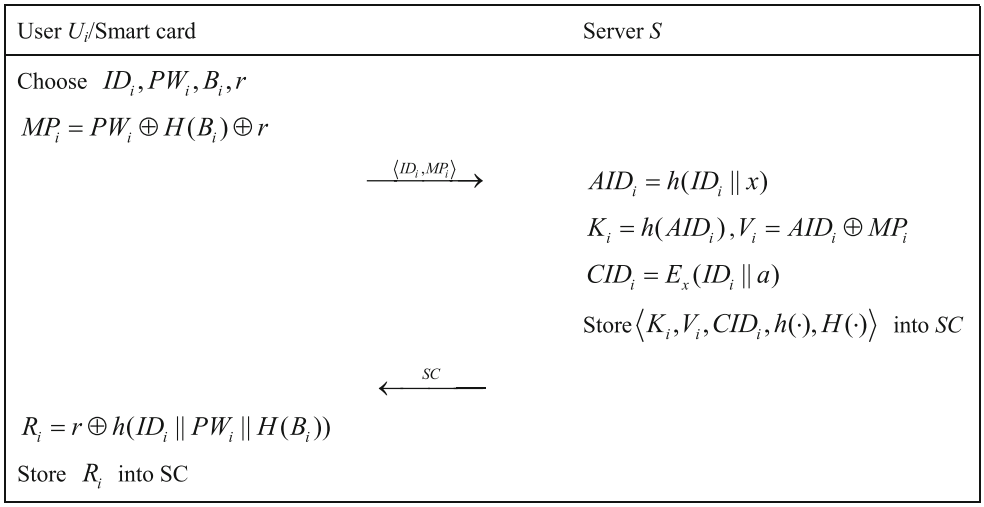


Fig. 1 Registration Phase of Proposed Scheme

session key that can be used for the secure transmission of data.

- U_i first inserts SC_i into the card reader, and enters his identity ID_i, password PW_i and biometric B_i. Then, smart card SC_i computes $r = R_i \oplus h(ID_i||PW_i||H(B))$, $MP_i = PW_i \oplus H(B_i) \oplus r$, and $AID_i = V_i \oplus MP_i$. The card checks whether $h(AID_i) \stackrel{?}{=} K_i$. If it holds, go to next step.
- SC_i generates a random nonce $d_u \in Z_p$, and computes$D = d_u P$, $M_1 = AID_i \oplus D$ and $M_2 = h(AID_i||D||T_1)$. SC_i transmits $\{M_1, M_2, CID_i, T_1\}$ to the server.
- After receiving the login request $\{M_1, M_2, CID_i, T_1\}$, S first checks the freshness of T_1 by verifies whether $|T_c - T_1| < \Delta T$, where T_c is the current time. If true, S retrieves ID_i by decrypting CID_i, and computes $AID_i = h(ID_i||x)$. Then he calculates $D = AID_i \oplus M_1$ and verifies whether $M_2 = h(AID_i||D||T_1)$ holds. If correct, the sever generates a' and $d_s \in Z_p$ randomly, and computes $E = d_s P$, $CID_i' = E_x(ID_i, a')$, $M_3 = AID_i \oplus E$, $SK = h(AID_i||d_s(D)||CID_i)$, $M_4 = h(CID_i'||SK||E||T_2)$, where T_2 is the current time. Then, S sends $\{M_3, M_4, CID_i', T_2\}$ to U.
- Upon receiving $\{M_3, M_4, CID_i', T_2\}$, SC_i checks the freshness of T_2. Then, U extracts E from computing $M_3 \oplus AID_i$, and computes $SK = h(AID_i||d_u(E)||CID_i)$, $M_4' = h(CID_i'||SK||E||T_2)$. Then, check whether $M_4' = M_4$ holds. If correct, SC_i replaces CID_i with CID_i', and computes $M_5 = h(E||SK||T_3)$ and then sends the message $\{M_5, T_3\}$ to S.
- S checks the validity of T_3, and verifies $h(E||SK||T_3) \stackrel{?}{=} M_5$. If both are correct, S authenticates U and accepts SK as the session key.

4.3 Password change phase

A valid user with smart card can change the password of the smart card as follows:

- U_i inserts the smart card into the device and inputs the ID_i, PW_i and B_i.
- SC_i computes $r = R_i \oplus h(ID_i||PW_i||H(B_i))$, $MP_i = PW_i \oplus H(B_i) \oplus r$, $AID_i = V_i \oplus MP_i$ and checks $h(AID_i) \stackrel{?}{=} K_i$. If holds, U_i inputs a new password PW_i^{new}, biometric B_i^{new} and a new random number r^{new}.
- SC_i computes $MP_i^{new} = PW_i^{new} \oplus H(B_i^{new}) \oplus r^{new}$, $V_i^{new} = AID_i \oplus MP_i^{new}$, $R_i^{new} = r^{new} \oplus h(ID_i||PW_i^{new}||H(B_i^{new}))$. Finally, it replaces R_i, V_i by R_i^{new}, V_i^{new} respectively.

5 Security

This section shows our proposed scheme gives the robust proof of the security of our new authentication scheme.

5.1 Proof by BAN-logic

BAN logic in [2] is a rule set for analyzing the belief which focuses on the beliefs of the legitimate principals involved in the protocol. Many researchers has analyzed the security of authentication schemes using BAN logic such as . In this

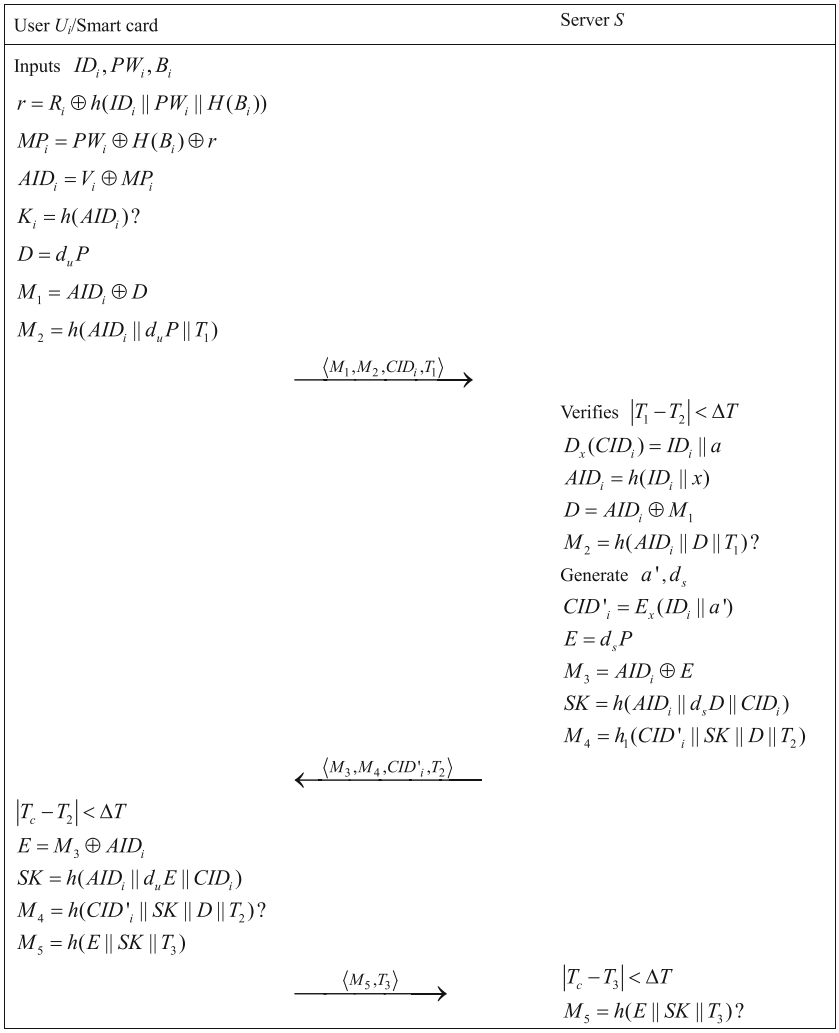


Fig. 2 Login and Authentication Phase of Proposed Scheme

section, we demonstrate that the proposed scheme is working correctly by achieving the authentication goals using BAN logic. The notations used in BAN logic analysis are defined as follows:

- $P| \equiv X$: The principal P believes a statement X or P would be entitled to believe X.
- $\sharp(X)$: 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).
- $\langle X \rangle_Y$: The formula X is xored with the formula Y.
- $(X)_Y$: The formula X is hashed under the key Y.
- $P \overset{K}{\longleftrightarrow} Q$: The principal P and Q share the key K.

Some main logical postulates of BAN logic are defined as follows:

- the message-meaning rule: $\frac{P| \equiv Q \overset{K}{\longleftrightarrow} P, P \triangleleft \langle X \rangle_K}{P| \equiv Q| \sim X}$
- the freshness-conjuncatenation rule: $\frac{P| \equiv \sharp(X)}{P| \equiv \sharp(X, Y)}$
- the nonce-verification rule: $\frac{P| \equiv \sharp(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$
- the jurisdiction rule: $\frac{P| \equiv \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}$, $\frac{P| \equiv (X,Y)}{P| \equiv X}$, $\frac{P| \triangleleft (X,Y)}{P| \triangleleft X}$

(2) Idealized scheme:

$U : \langle D \rangle_{U \overset{AID}{\longleftrightarrow} S}, (U \overset{SK}{\longleftrightarrow} S, D, T_1)_{U \overset{AID}{\longleftrightarrow} S}, T_1, (U \overset{SK}{\longleftrightarrow} S, T_3)_{U \overset{AID}{\longleftrightarrow} S}$

$S : \langle E \rangle_{U \overset{AID}{\longleftrightarrow} S}, (U \overset{SK}{\longleftrightarrow} S, CID'_i, E, T_2)_{U \overset{AID}{\longleftrightarrow} S}, T_2$

(3) Security goals

G1: $U| \equiv S| \equiv (U \overset{SK}{\longleftrightarrow} S)$

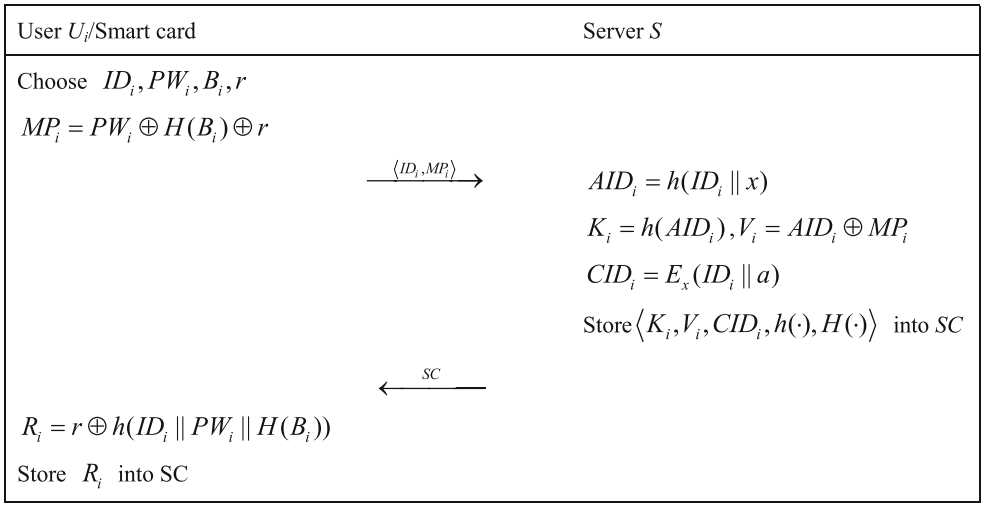


Fig. 3 Password Change Phase of Proposed Scheme

G2: $U| \equiv (U \overset{SK}{\longleftrightarrow} S)$
G3: $S| \equiv U| \equiv (U \overset{SK}{\longleftrightarrow} S)$
G4: $S| \equiv (U \overset{SK}{\longleftrightarrow} S)$
(4) Initiative premises
A.1 $U \mid \equiv \sharp(T_2)$
A.2 $S \mid \equiv \sharp(T_1)$
A.3 $S \mid \equiv \sharp(T_3)$
A.4 $U \mid \equiv U \overset{AID}{\longleftrightarrow} S$
A.5 $S \mid \equiv U \overset{AID}{\longleftrightarrow} S$
A.6 $U \mid \equiv S \Rightarrow (U \overset{SK}{\longleftrightarrow} S, CID_i', E, T_2)$
A.7 $S \mid \equiv U \Rightarrow (U \overset{SK}{\longleftrightarrow} S, T_3)$

(5) Scheme Analysis
Based on the above-mentioned assumptions and rules of BAN logic, we analyze the idealized form of the proposed scheme and the main procedures of proof as follows:

s1. According to the message $S \triangleleft (U \overset{SK}{\longleftrightarrow} S, T_3)_{U \overset{AID}{\longleftrightarrow} S}$ and A.5, we apply the message-meaning rule to obtain:

$$S \equiv U \sim (U \overset{SK}{\longleftrightarrow} S, T_3)$$

s2. Since A.3 and s1, based on the fresh conjuncatenation rule and nonce-verification rule we get:

$$S \equiv U \equiv (U \overset{SK}{\longleftrightarrow} S, T_3)$$

G3. Since s2, we achieve the third goal by applying the belief rule:

$$S \equiv U \equiv U \overset{SK}{\longleftrightarrow} S$$

G4. Using $A.7$ and $G3$, we obtain:

$$S \equiv U \overset{SK}{\longleftrightarrow} S$$

s3. Since the message $(U \overset{SK}{\longleftrightarrow} S, CID_i', E, T_2)_{U \overset{AID}{\longleftrightarrow} S}$ and A.4, applying the message-meaning rule we obtain:

$$U| \equiv S| \sim (U \overset{SK}{\longleftrightarrow} S, CID_i', E, T_2)$$

s4. Since the Assumption A.1 and s3, we use the freshness-conjuncatenation rule and the nonce-verification rule to prove

$$U| \equiv S \equiv (U \overset{SK}{\longleftrightarrow} S, CID_i', E, T_2)$$

G1. Since s4, according to the belief rule, we obtain:

$$U| \equiv S| \equiv U \overset{SK}{\longleftrightarrow} S$$

G2. According to the assumption A.6 andG2, we obtain:

$$U| \equiv U \overset{SK}{\longleftrightarrow} S$$

Hence, we apply the BAN logic to analyze the security of our proposed scheme. The results demonstrate that our authentication scheme can achieve mutual authentication between the user U and the server S.

5.2 Formal security analysis

In this section, we demonstrate that our proposed scheme is provably secure against a probabilistic polynomial-time adversary under the random oracle model, which means that the new scheme is secure for $\mathcal{A}$ to derive the session key between a user and a server. We use the method of

contradiction in [8] to give the formal security proof. The the similar proof is followed as in [10, 22]. It is noted that one can also give the formal security proof in the standard model. However, in this literature, we have performed the formal security analysis under the generic group model of cryptography.

In order to apply the technique of contradiction proof, we assume the following oracle exists for an adversary $\mathcal{A}$.

– *Reveal*: This oracle will unconditionally output the input string x from the corresponding hash function $y = h(x)$

Theorem 1 *Under the assumption that one-way hash function closely behaves like an random oracle, our proposed authentication scheme is secure against an adversary $\mathcal{A}$ for deriving the user U_i's identity ID_i and the session key SK between U_i and S.*

Proof In our proof, we first construct an adversary $\mathcal{A}$ who can derive a legal user U_i's identity ID_i and the session key SK between U_i and the server S. The adversary $\mathcal{A}$ uses the *Reveal* oracle run the in the experiment $EXP1^{HASH}_{\mathcal{A},SEUATPAS}$ provided in Algorithm 1 for our new secure and efficient user anonymity-preserving three-factor authentication scheme, define as SEUATPAS. The successful probability of $EXP1^{HASH}_{\mathcal{A},SEUATPAS}$ is defined as $Succ1 = |Pr[EXP1^{HASH}_{\mathcal{A},SEUATPAS} = 1] - 1|$. We define the advantage function for this experiment as $Adv1(et_1, q_R) = \max_{\mathcal{A}} Succ1$, where the maximum is taken over all $\mathcal{A}$ with execution time et_1, and query time q_R to *Reveal*. Our protocol is proven to be secure against $\mathcal{A}$ for deriving U_i's identity ID_i and the session key SK, if $Adv1 \leq \epsilon$, for any sufficiently small $\epsilon > 0$.

Consider the experiment $EXP1^{HASH}_{\mathcal{A},SEUATPAS}$ in Algorithm 1. Based on this experiment, $\mathcal{A}$ has the ability to derive the identity ID_i and the session key SK between U_i and S, if $\mathcal{A}$ has access to the oracle *Reveal*. But it is a computationally infeasible problem due to collision-resistant property, that is $Adv^{HASH}_{\mathcal{A}}(t) \leq \epsilon 1$ for any small $\epsilon 1 > 0$. Therefore, our scheme is provably secure against $\mathcal{A}$ for a user's identity ID_i and the session key SK between a user and the server. □

6 Comparison

In this section we discuss the security attributes and performance of our proposed scheme and give a comparison between our scheme and some previous schemes in [1, 18, 29, 30]. Table 2 lists that the flaws of security and efficiency for biometric based authentication schemes.

In the literature, we use √ to represent the scheme prevents attack or satisfies the attribute and × represents the scheme fails to prevent attack or does not satisfy the attribute. From Table 2, the schemes [1, 29, 30] are vulnerable to off-line password guessing attack. That means that an adversary can derive the correct password by an off-line exhaustive search since password is short in order to remember easily. Arshad et al.'s schemes [1] can not protect user anonymity and the identity of an entity is leaked to the attacker. Therefore, an ID-based authentication scheme should ensure user anonymity and provide unlinkability. Wu et al.'s scheme [29] and Lu et al.'s scheme [18] can not resist impersonation attack, which means that an adversary could impersonate as a legal user to access any services.

From Table 2, in Yeh et al.'scheme [30] and Arshad et al.'scheme [1], it's clear that if the server's master key is leaked, the malicious people can compute all previous session key between a user and a server. They does not provide the security attribute of strong forward secrecy. In Yeh et al.'s scheme [30], the sever and the user do not verify the correctness of the session key. In general, an scheme with session key verification needs to transmit the messages by three times attack.

Table 3 discusses the computation overhead of these schemes in login and authentication phase, where T_{sym}, T_h, T_{mm}, T_M and T_A denote the time complexity of symmetric encryption/decryption, hash function, the biometric

Table 2 Security attributes comparison of biometric based authentication schemes

Security attributes \ Schemes	[1]	[18]	[29]	[30]	Ours
User anonymity	√	×	√	√	√
Off-line password guessing attack	×	√	×	×	√
Stolen smart card attack	√	√	√	√	√
Impersonation attack	√	×	×	√	√
Replay attack	√	√	√	√	√
Strong forward secrecy	×	√	√	×	√
Session key verification	√	√	√	×	√

Algorithm 1 $EXP1_{\mathcal{A},SEUATPAS}^{HASH}$

1. Intercept the login request $\{M_1, M_2, CID_i, T_1\}$ during the login phase.
2. Intercept the message $\{M_3, M_4, CID_i', T_2\}$ during the login and authentication phase.
3. Call $Reveal$ oracle on M_2 to extract the information AID_i', D', T_1'
4. Compute $D'' = AID_i' \oplus M_1$
5. **If** (T_1=T_1') and $D' = D''$ **then**
6. Accept AID_i' as the correct form
7. Call $Reveal$ oracle on input AID_i' to extract the information ID', x
8. Call $Reveal$ oracle on input M_4 to extract CID'', SK, D''', T_2'
9. **If** (T_2=T_2') and $CID' = CID''$ **then**
10. Accept SK as the correct session key
11. **return 1**(Success)
12. **else**
13. **return 0**(Failure)
14. **end if**
15. **else**
16. **return 0**(Failure)
17. **end if**

Table 3 Performance evaluation of biometric based authentication schemes

Schemes	User computation	Server computation
Arshad et al.'s scheme [1]	$2T_M + T_{mm} + 8T_h$	$2T_M + 2T_{mm} + 7T_h$
Lu et al.'s scheme [18]	$2T_M + 5T_h$	$T_M + 5T_h$
Wu's scheme [29]	$2T_M + 6T_h + 2T_{sym}$	$2T_M + 6T_h + 2T_{sym}$
Yeh et al.'s scheme [30]	$2T_M + 6T_A + 8T_h$	$2T_M + 6T_A$
Our scheme	$2T_M + 6T_h$	$T_M + 5T_h + 2T_{sym}$

function, modular multiplication, elliptic curve point multiplication and point addition, respectively. It is noted that, $T_M > T_A > T_{mm} > T_{sym} > T_h$. Since the login and authentication phases are executed for each session while the registration and password change phases occur once, we only discuss the computational cost of the login and authentication phases. Table 3 shows our scheme costs less computation to achieve the mutual authentication and key agreement than the schemes [1, 18, 29] and takes almost identical to the protocol [30].

7 Conclusions

In this paper, we analyzed the security of Lu et al.'s biometric based authentication scheme. We showed that their scheme is unable to protect user anonymity and is insecure against impersonation attacks which leads an adversary could impersonate as a legal user to access any services provided by the server, and cheat an honest user as a legal server. Moreover, we employ bio-hash functions and elliptic curve Diffie-Hellman problem to propose a secure and efficient three factor based authentication protocol. Our new scheme is proven accurate by BAN logic tool and robustly secure under a random oracle model. Finally, we give a comparison of our new authentication protocol and others in efficiency and security attributes.

Acknowledgments This research is supported by National Basic Research Program of China (Grant No. 2013CB834205), Natural Science Foundation of Zhejiang Province (Grant No. LZ12F02005) and Opening project of Key Laboratory of Public Security Information Application Based on Big-data Architecture, Ministry of Public Security (Grant No. 2014DSJSY004).

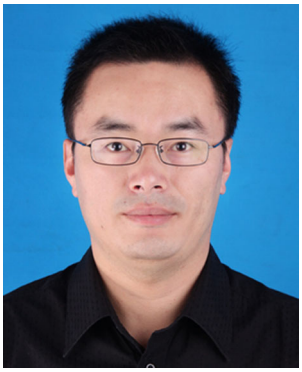
References

1. Arshad H, Nikooghadam M (2014) Three-Factor Anonymous authentication and key agreement scheme for telecare medicine information systems. J Med Syst 38(12):136–147
2. Burrow M, Abadi M, Needham R (1990) A logic of authentication. ACM Trans Comput Syst 8:18–36

3. Chang C-C, Wu T-C (1991) Remote password authentication with smart cards. Comput Digit Tech IEE Proc E 138(3):165–168
4. Chang C-C, Hwang S-J (1993) Using smart cards to authenticate remote passwords. Comput Math Appl 26(7):19–27
5. Chang YF, Yu SH, Shiao DR (2013) An uniqueness and anonymity-preserving remote user authentication scheme for connected health care. J Med Syst 37(12):9902–9910
6. Chen C, Lee C, Hsu C (2012) Mobile device integration of a fingerprint biometric remote authentication scheme. Int J Commun Syst 25(2):585–597
7. Chiou S-Y, Ying Z, Liu J (2016) Improvement of a privacy authentication scheme based on cloud for medical environment. J Med Syst 40:101
8. Chuang YH, Tseng YM (2010) An efficient dynamic group key agreement protocol for imbalanced wireless networks. Int J Netw Manag 20(4):167–180
9. Das ML, Saxena A, Gulati VP (2004) A dynamic ID-based remote user authentication scheme. IEEE Trans Consum Electron 50(2):629–631
10. Das AK (2015) A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. Peer-to-peer Netw Appl 9(1):223–244
11. He DB, Chen JH, Zhang R (2012) A more secure authentication scheme for telecare medicine information systems. J Med Syst 36(2):1989–1995
12. Jin AT, Ling D, Goh A (2004) Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn 37(11):2245–2255
13. Khan MK, Kim KS, Alghathbar K (2010) Cryptanalysis and security enhancement of a more efficient secure dynamic idbased remote user authentication scheme. Comput Commun 34(3):305–309
14. Khan M, Kuman C, Gupta M (2014) More efficient key-hash based fingerprint remote authentication scheme using device. Computing 96(9):793–816
15. Kocher P, Jaffe J, Jun B (1999) Differential power analysis, Proceedings of 19th Annual International Cryptology conference(CRYPTO'99). LNCS 1666:388–397
16. Ku W, Chen S (2004) Impersonation attack on a dynamic ID based remote user authentication using smartcards. IEICE Trans Commun E88-B:2165–2167
17. Lamport (1981) Password authentication with insecure communication. Commun ACM 24(11):770–772
18. Lu Y, Li L, Peng H, Yang Y (2015) An enhanced Biometric-Based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. J Med Syst 39(2):1–9
19. Lu Y, Li L, Peng H, Yang Y (2016) A secure and efficient mutual authentication scheme for session initiation protocol. Peer-to-Peer Netw Appl 9(1):449–459
20. Lumini A, Nanni L (2007) Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn 40(3):1057–1065
21. Messerges TS, Dabbish EA, Sloan RH (2002) Examining smartcard security under the threat of power analysis attacks. IEEE Trans Comput 51(5):541–552
22. Mir O, Munilla J, Kumari S (2015) Efficient anonymous authentication with key agreement protocol for wireless medical sensor networks. Peer-to-Peer Netw Appl:1–13
23. Mishra D, Das AK, Mukhopadhyay S (2016) A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card. Peer-to-Peer Netw Appl 9(1):171–192
24. Moon J, Choi Y, Kim J, Won D (2016) An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. J Med Syst 40:70
25. Siddiqui Z, Abdullah A-H, Khan M-K, Lee H-C, Alghamdi A-S (2015) Cryptanalysis and improvement of 'a secure authentication scheme for telecare medical information system' with nonce verification, Peer-to-Peer Netw Appl, pp 1–13. doi:10.1007/s12083-015-0364-9
26. Wang YY, Kiu JY, Xiao FX, Dan J (2009) A more efficient secure dynamic ID-based remote user authentication. Comput Commun 32:583–585
27. Wang XM, Zhang WF, Zhang JS, Khan MK (2007) Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards. Comput Stander Interface 29:507–512
28. Wu Z-Y, Lee Y-C, Lai F, Lee H-C, Chung Y (2012) A secure authentication scheme for telecare medicine information systems. J Med Syst 36(3):1529–1535
29. Wu F, Xu L, Kumari S, Li X (2015) A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client server networks. Comput Electr Eng 45(C):274285
30. Yeh H-L, Chen T-H, Hu K-J, Shih W-K (2013) Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data. IET Inf Secur 7(3):247252

Lidong Han received his Ph.D. degree from School of Mathematics, Shandong University, China, in 2010. Currently, he is working at Hangzhou Normal University. His current research interests include Cryptography, cloud computing and remote user authentication.

Xiao Tan received his Ph.D. degree from Department of Computer Science, City University of Hong Kong in 2014. Currently, he is working at Hangzhou Normal University. His current research interests include encryption schemes, digital signatures and cloud storage.



Shengbao Wang received his Ph.D. degree in computer science from Shanghai Jiao Tong University in 2008 and is now working as an associate professor at the Department of Computer Science and Engineering, Hangzhou Normal University, China. His research interests lie in public key cryptography, especially focus on public key encryption and key agreement protocols.

Xikun Liang received his Ph.D. degree from school of computer and information in HeFei university of technology in 2003. Currently, he is an associate professor in Hangzhou institute of service engineering of Hangzhou normal university. His current research interests include intelligent information processing and service computing.