# An Improved Biometric Based Authentication Scheme with User Anonymity Using Elliptic Curve Cryptosystem

Lidong Han, Qi Xie, and Wenhao Liu

*(Corresponding author: Lidong Han)*

Key Laboratory of Cryptography and Network Security, Hangzhou Normal University

No.58, Haishu Rd, Yuhang District, Hangzhou 311121, China

(Email: ldhan@hznu.edu.cn)

*(Received Oct. 27, 2015; revised and accepted Feb. 21 & Apr. 6, 2016)*

## Abstract

Telecare medical information systems (TMIS) provides convenient health care services for patients in order to save the patients' time and expense. The protection of user's privacy and data security is significant over public communication. Recently, Lu et al. presented a three-factor based authentication protocol using elliptic curve cryptography. In this paper, we analyze the security of Lu et al.'s scheme. We demonstrate that Lu et al's scheme can't protect user anonymity and insecure against impersonation attack. To remedy the mentioned security weakness, we propose a new authentication scheme to improve on Lu et al.'s scheme. In comparison with recent schemes, our scheme can provide stronger security and more efficiency in implementation.

*Keywords: Authentication, password, user anonymity*

## 1 Introduction

With the rapid development of information and network technologies, connected health care can be applied in many fields, such as telecare medicine information system (TMIS). TMIS provides a convenient communication via public channels between patients (doctors) at home and medical servers. The merit of TMIS is that it enables patients accessing and updating patient's medical information in TIMS server, and it provides health-care services directly into the patient at home using internet, which can save patients much time and expenses. In order to protect patients' privacy and security, it is very important to achieve secure mutual authentication between patients and the medical server before diagnosis. which result in data security and user's privacy issues. The sensitive healthcare information should be protected and user's personal private information should not be leaked to the malicious users or adversaries. A secure and efficient authentication and key agreement scheme can provide various aspects of security for health data and user privacy. Recently, many authentication schemes using smart card have been presented to ensure secure and authorized access of data [4, 8, 9, 13, 14, 21, 22, 24, 27].

In 2009, Wu et al. [24] proposed an efficient authentication scheme using smart card for TMIS with precomputation. However, He et al. [8] found that Wu et al.'s scheme is not secure against impersonation attacks and insider attacks. To address these problems, He et al. gave an improved authentication scheme. Later, Wei et al. [22] showed both Wu et al.'scheme and He et al.'s scheme are not resistant to off-line password guessing attacks and cannot achieve two-factor authentication. They also presented an improved authentication scheme for TMIS and claimed that the improved scheme can achieve two-factor authentication. Unfortunately, Zhu [29] pointed out that Wei et al.'s scheme is also vulnerable to off-line password guessing attack using stolen smart card. Zhu designed a new RSA based authentication scheme and claimed that the new scheme is secure against various attacks.

However, in all password based remote user authentication schemes mentioned above, an adversary can obtain user's identity since the identity was transmitted in plaintext in authentication process. In 2004, Das et al. [7] proposed a dynamic ID-based password authentication scheme to solve this security weakness. Since then, many dynamic ID-based authentication schemes have been designed. Chen et al. [6] showed Khan et al.'s scheme [11] can not protect the user's anonymity and presented a dynamic ID-based password authentication scheme. However, Xie et al. [25] showed that Chen et al.'s scheme does not provide user privacy protection and perfect forward secrecy, and proposed an improved scheme. Until now, many researchers have analyzed the security of password-based authentication schemes. Also other researchers proposed their authentication and key agreement schemes.

All above mentioned authentication schemes are based on two factors password and smart cards [1, 19]. Lately, researchers focused on three factor based authentication and key agreement scheme employing biometric, which has stronger security than two factor based schemes [28]. In 2013, Tan [20] proposed a biometric based remote user authentication scheme for telecare medical information system to achieve mutual authentication and session key establishment. Awasthi and Srivastava [3] presented an efficient biometric based authentication scheme, which only uses the Xor operation and hash function to lower computational cost for smart cards. Tan showed that Awasthi-Srivastava's three-factor scheme is vulnerable to the reflection attacks and it fails to provide user anonymity and three-factor security. Recently, Lu et al. [15] put forward the security weakness of of Arshad et al.'s scheme [2], and proposed an biometric-based authentication schemes for TMIS using elliptic curve cryptosystem.

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 also employs lower computational operations such as ECC and hash function to lower its computational cost.

The remainder of this paper is organized as follows: In first section, we introduce some notations and definitions used in this paper. Section 3 will review the biometric -based authentication scheme by Lu et al. Section 4 analyzes the security problems of Lu et al.'s protocol. We present a new biometric -based authentication scheme based on ECC in Section 5. Section 6 will elaborate the security and efficiency of our new scheme briefly, and gives a comparison of several previous biometric based authentication schemes. And A comparison with some previous authentication schemes in the aspect of security and efficiency is given in Section 7. Finally, we give a conclusion in the last section.

# 2 Preliminaries

This section lists the notations and definitions used in this paper, and briefly reviews the basic concepts of bio-hashing, ECC cryptosystem along with some hardness problems are introduced.

## 2.1 Notations

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

In Table 1, one-way hash function $h(\cdot)$ maps a string of arbitrary length to a string of fixed length which is called hashed value. It can be represented as $h : \{0,1\}^* \rightarrow \{0,1\}^n$. Such hash function is easy to compute on every input, but hard to invert given the image of a random input.

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 |
| $h_1(\cdot)$ | Hash function $h_1$: $\{0,1\}^* \rightarrow \{0,1\}^l$ |
| $h_2(\cdot)$ | Hash function $h_2$: $\{0,1\}^* \rightarrow Z_p^*$ |
| $H(\cdot)$ | 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 $x$ |

It is noted that, when the elliptic curve point $P = (x, y)$ as input in hash operation and $\oplus$ operation, $P$ is represented as a value by $x||y$.

## 2.2 Bio-hashing

The biometrics is of great importance to provide genuine user authentication in any authentication scheme. In general, imprint biometric characteristics (face, fingerprint, palmprint) may not be exactly same at each time. Therefore, high false rejection of valid users resulting low false acceptation, is often occurs in the verification of biometric systems. In order to resolve the high false rejection rate, Jin et al. [10] 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. Later, Lumini and Nanni [16] proposed the improvement of Bio-Hashing. As specified in [5], Bio-Hashing maps a user/patients biometric feature onto user specific random vectors in order to generate a code, called biocode and then discretizes the projection coefficients into zero and one. Biocode is also as secure as a hashed password.

# 3 Review of Lu et al.'s Scheme

In 2015, Lu et al. proposed an biometric-based authentication and key agreement scheme based on elliptic curve cryptosystem [15], which is based on Arshad et al.'s scheme [2]. It consists of four phases: registration, login, authentication, password change. In this section, we will briefly review these phases of Lu et al.'s scheme.

**Registration phase.**

In this phase, a new user $U_i$ registers to the server $S$ and achieves the personalized smart card via the following steps:

- The user $U_i$ selects his identity $ID_i$, password $PW_i$ and inputs his biometric $B_i$. He computes

$MP_i = PW \oplus H(B_i)$, and sends $\{ID_i, MP_i\}$ to the server $S$ through a secure channel.

- Upon receiving the registration request, $S$ calculates $AID_i = ID_i \oplus h_2(x)$ using the private key $x$, $V_i = h_1(ID_i||MP_i)$, and stores $\{AID_i, V_i, h_1(\cdot), h_2(\cdot), H(\cdot)\}$ into a smart card $SC_i$. $S$ issues $SC_i$ to the patient $U_i$.

**Login and Authentication phase.**

The user $U_i$ and the server $S$ execute the following steps in order to achieve authentication and session key agreement.

- $U_i$ first inserts the smart card $SC_i$, and inputs his identity $ID_i$, password $PW_i$ and biometric $B_i$. Then, $SC_i$ checks whether $h_1(ID_i||PW_i \oplus H(B_i)) = V_i$ holds or not. If it holds, go to the next step.
- The smart card $SC_i$ generates a random number $d_u$, and computes $K = h_1(ID_i||ID_i \oplus AID_i)$, $M_1 = K \oplus d_uP$ and $M_2 = h_1(ID_i||d_uP||T_1)$. $SC_i$ sends the login request $\{M_1, M_2, AID_i, T_1\}$ to $S$.
- After receiving $\{M_1, M_2, AID_i, T_1\}$, $S$ first examines whether $|T_c - T_1| < \Delta T$, where $T_c$ is the current time stamp. If true, $S$ computes $AID_i \oplus h_2(x)$ using his private key $x$ to extract $ID_i$, then he calculates $d_uP = h_1(ID_i||h_2(x)) \oplus M_1$ and verifies whether $M_2 = h_1(ID_i||d_uP||T_1)$ holds. If correct, $S$ chooses a number $d_s$ randomly, and computes $M_3 = K \oplus d_sP$, $SK = d_s(d_uP)$, $M_4 = h_1(K||d_uP||SK||T_2)$, where $T_2$ is the current time. Then, $S$ transmits $\{M_3, M_4, T_2\}$ to $U_i$.
- Upon receiving $\{M_3, M_4, T_2\}$, $SC_i$ checks the validity of $T_2$. Then, $U$ extracts $d_sP$ from computing $M_3 \oplus K$, and computes $SK = d_u(d_sP)$, $M_4' = h_1(K||d_uP||SK||T_2)$. Then, checks whether $M_4' = M_4$ holds. If correct, the smart card $SC_i$ computes $M_5 = h_1(K||d_sP||SK||T_3)$ and then sends the message $\{M_5, T_3\}$ to $S$.
- $S$ checks the freshness of $T_3$, and then verifies $h_1(K||d_sP||SK||T_3) \stackrel{?}{=} M_5$. If both are correct, $S$ authenticates $U_i$ and accepts $SK$ as the session key.

**Password change phase.**

If the patient $U_i$ wants to change his old password $PW_i$, $U_i$ inserts the smart card into the device and inputs the $ID_i, PW_i$, and $B_i$. Then $SC_i$ verifies $h_1(ID_i||PW_i \oplus H(B_i)) \stackrel{?}{=} V_i$. If holds, $U_i$ keys a new password $PW_i^{new}$, $SC_i$ computes $V_i^{new} = h_1(ID_i||PW_i^{new} \oplus H(B_i))$. Finally, it replaces $V_i$ by $V_i^{new}$.

# 4 Security Weakness of Lu et al.'s Scheme

In this section, we demonstrate that Lu et al.'s scheme fails to achieve their claimed security goals. In the attack model, it can be assumed that an adversary could get the values which are stored into a user $U_i$'s smart card by monitoring the power consumption [12, 17]. Also an adversary has the ability of controlling over the communication totally. That means that he can extract and modify the transmitting messages between $U_i$ and $S$. In the following, we will analyze the security of Lu et al.'s scheme in detail.

**Linkability.**

The linkability is that an adversary can determinate whether two login messages are sent by the same patient. Since the login request message $m_1 = \{AID_i, M_1, M_2, T_1\}$ contains the fixed value $AID_i = ID_i \oplus h_2(x)$ where $ID_i$ is the user's identity and $h_2(x)$ is a hash function with input $x$. Therefore, when an adversary intercepts two login messages $m_1$ and $m_1'$, he only decides whether the first part of $m_1$ and $m_1'$ are equal. If it's correct, we determine that two login messages must be from the same patient.

**Fails to protect user anonymity.**

In this subsection, we will show that Lu et al.'s scheme does not protect patient's anonymity for the insider users.

In Lu et al.'s scheme, the patient's identity is obscured by the form $AID_i = ID_i \oplus h_2(x)$, which is part of the transmitted message by public channel in login phase. For outside attackers, it's not efficient to retrieve the patient's identity without knowledge of the secret value $h_2(x)$. However, for a legal but malicious patient $U_j$, he can extracts $h_2(x)$ using his own identity $ID_j$ and the value $AID_j$ stored in smart card. Then, $U_j$ can easily compute any other patient's identity by computing $ID = AID \oplus h(x)$ where $AID$ can be intercepted in initiating login phase.

**Server impersonation attack.**

This subsection describes that a legitimate user in Lu et al.'s scheme can impersonate as a legal sever. Denote $U_j$ be a legal patient, who wants to simulate as legal TMIS server. $U_j$ will perform the following steps to impersonate as a legal server.

1) $U_j$ extracts the secret information $\{V_j, AID_j, h_1(\cdot), h_2(\cdot), H(\cdot)\}$ stored into his smart card by monitoring the power consumption or analyzing the leaked information. $U_j$ then computes $AID_j \oplus ID_j$ using his password $PW_j$ to obtain $h_2(x)$.
2) When a patient $U_i$ executes 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 $AID_i \oplus h_2(x)$ using the value $h_2(x)$ to retrieve the identity of $U_i$. Then $U_j$ chooses a random number $d'_s \in Z_p^*$, and computes $M'_3 = h_1(ID_i||h_2(x)) \oplus d'_s P$, $SK' = d'_s(d_u P)$, $M'_4 = h_1(K||d_u P||SK'||T_2)$, where $T_2$ is the current time stamp. $U_j$ sends $\{M'_3, M'_4, T_2\}$ to $U_i$
4) $U_i$ check the validity of $T_2$. Then computes $K \oplus M'_3 = d'_s P$, $SK = d_u(d'_s P)$,$M^*_4 = h_1(K||d_u P||SK||T_2) \stackrel{?}{=} M'_4$. $U_i$ accepts the session key $SK$ since the verification is correct and regards $U_j$ as a legitimate sever.

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

**User impersonation attack.**

Lu et al. claimed their scheme could withstand various attack. Now, we demonstrate that a legal but malicious patient $U_j$ can impersonate a patient to the server. The details of impersonation attack are presented in the following.

1) $U_j$ can get $h_2(x)$ by computing $AID_j \oplus ID_j$ as similar as step 1 in server impersonation, where $AID_j$ 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 $ID_i = AID_i \oplus h_2(x)$. 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 $K = h_1(ID_i||h_2(x))$, $M'_1 = K \oplus d'_u P$ and $M'_2 = h_1(ID_i||T_1||d'_u P)$. 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 $ID_i = AID_i \oplus h_2(x)$. Then $S$ chooses a random number $d_s \in Z_p^*$, and computes $M_3 = h_1(ID_i||h_2(x)) \oplus d_s P$, $SK = d_s(d_u P)$, $M_4 = h_1(K|T_2||SK'||d_u P|)$, where $T_2$ is the current time stamp. $U_j$ sends $\{M_3, M_4, T_2\}$ to $U_i$.
5) $U_j$ computes $K \oplus M_3 = d_s P$, $SK = d_u(d_s P)$. Then $U_j$ checks whether $M^*_4 = h_1(K||d_u P||SK||T_2) \stackrel{?}{=} M'_4$. $U_j$ computes $M_5 = h_1(K||d_s P||SK||T_3)$ 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 $M'_5 = h_1(K||d_s P||SK||T_3) \stackrel{?}{=} M_5$. $S$ authenticates $U_j$ as $U_i$ and accepts $SK$ as the session key.

Hence, a legal patient can impersonate himself as any other patients to sever $S$. Therefore, it is shown that Lu et al.'s scheme is vulnerable to user impersonation attack.

# 5 Proposed Scheme

From previous section, it is observed that the important weakness of Lu et al.'s scheme is the form of $AID_i$, which leaks some information of server's private key. That means any legal user can obtain $h_2(x)$ that can be used in attacking Lu et al.'s scheme. This section proposes an improved three-factor authentication scheme based on Lu et al.'s scheme. In the proposed scheme, in order to resist the impersonation attack, we employ a hash function with inputs the patient's identity and private key, which is related to the communicating patient. The four phases of our proposed scheme are described as follows.

**Registration phase.**

A new user $U_i$ chooses 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 $SC_i$.

**Login and authentication phase.**

A legal user with valid smart card can establish a secure and authorized session with the server. In this phase, user and server first authenticate each other and then agree on a 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 holds, go to next step.
- $SC_i$ generates a random nonce $d_u \in Z_p$, and computes $d_u P$, $M_1 = AID_i \oplus D$ and $M_2 = h(AID_i||d_u P||T_1)$. $SC_i$ 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 verifing 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

| User $U_i$/Smart card | | Server $S$ |
|---|---|---|
| Choose $ID_i, PW_i, B_i, r$ | | |
| $MP_i = PW_i \oplus H(B_i) \oplus r$ | | |
| | $\langle ID_i, MP_i \rangle \longrightarrow$ | $AID_i = h(ID_i \parallel x)$ |
| | | $K_i = h(AID_i), V_i = AID_i \oplus MP_i$ |
| | | $CID_i = E_x(ID_i \parallel a)$ |
| | | Store $\langle K_i, V_i, CID_i, h(\cdot), H(\cdot) \rangle$ into $SC$ |
| | $\longleftarrow SC$ | |
| $R_i = r \oplus h(ID_i \parallel PW_i \parallel H(B_i))$ | | |
| Store $R_i$ into SC | | |

Figure 1: Registration phase of proposed scheme

| User $U_i$/Smart card | | Server $S$ |
|---|---|---|
| Inputs $ID_i, PW_i, B_i$ | | |
| $r = R_i \oplus h(ID_i \parallel PW_i \parallel H(B_i))$ | | |
| $MP_i = PW_i \oplus H(B_i) \oplus r$ | | |
| $AID_i = V_i \oplus MP_i$ | | |
| $K_i = h(AID_i)?$ | | |
| $M_1 = AID_i \oplus d_u P$ | | |
| $M_2 = h(ID_i \parallel d_u P \parallel T_1)$ | | |
| | $\langle M_1, M_2, CID_i, T_1 \rangle \longrightarrow$ | |
| | | Verifies $\lvert T_1 - T_2 \rvert < \Delta T$ |
| | | $D_x(CID_i) = ID_i \parallel a$ |
| | | $AID_i = h(ID_i \parallel x)$ |
| | | $d_u P = AID_i \oplus M_1$ |
| | | $M_2 = h(ID_i \parallel d_u P \parallel T_1)?$ |
| | | Generate $a', d_s$ |
| | | $CID'_i = E_x(ID_i \parallel a')$ |
| | | $SK = d_s(d_u P)$ |
| | | $M_3 = AID_i \oplus d_s P$ |
| | | $M_4 = h_1(CID'_i \parallel SK \parallel d_u P \parallel T_2)$ |
| | $\longleftarrow \langle M_3, M_4, CID'_i, T_2 \rangle$ | |
| $\lvert T_c - T_2 \rvert < \Delta T$ | | |
| $d_s P = M_3 \oplus AID_i$ | | |
| $SK = d_u(d_s P)$ | | |
| $M_4 = h(CID'_i \parallel SK \parallel d_u P \parallel T_2)?$ | | |
| $M_5 = h(d_s P \parallel SK \parallel T_3)$ | | |
| | $\langle M_5, T_3 \rangle \longrightarrow$ | $\lvert T_c - T_3 \rvert < \Delta T$ |
| | | $M_5 = h(d_s P \parallel SK \parallel T_3)?$ |

Figure 2: Login and authentication phase of proposed scheme

computes $AID_i = h(ID_i||x)$. Then he calculates $d_uP = AID_i \oplus M_1$ and verifies whether $M_2 = h(AID_i||d_uP||T_1)$ holds. If correct, The sever generates $d_s \in Z_p$ and $a'$ randomly, and computes $E = d_sP$, $CID'_i = E_x(ID_i, a')$, $M_3 = AID_i \oplus E$, $SK = h(AID_i||d_s(d_uP)||CID_i)$, $M_4 = h(CID'_i||SK||d_sP||T_2)$, 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 $d_sP$ from computing $M_3 \oplus AID_i$, and computes $SK = h(AID_i||d_u(d_sP)||CID_i)$, $M'_4 = h(CID'_i||SK||d_sP||T_2)$. Then, check whether $M'_4 = M_4$ holds. If correct, $SC_i$ replaces $CID_i$ with $CID'_i$, and computes $M_5 = h(d_sP||SK||T_3)$ and then sends the message $\{M_5, T_3\}$ to $S$.
- $S$ checks the validity of $T_3$, and verifies $h(d_sP||SK||T_3) \stackrel{?}{=} M_5$. If both are correct, $S$ authenticates $U$ and accepts $SK$ as the session key.

**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 it 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.

## 6 Security Analysis

In this section, we demonstrate that our scheme can resist a number of possible attack types.

**User anonymity.**

Suppose an adversary eavesdrops the login request $\{M_1, M_2, CID_i, T_1\}$ during the login phase, and the authentication message $\{M_3, M_4, CID'_i, T_2\}$ during the authentication and key agreement phase, where $M_1 = AID_i \oplus D, M_2 = h(AID_i||D||T_1)$, $CID_i = E_x(ID_i||a), M_3 = AID_i \oplus d_sP, M_4 = h(CID'_i||SK||E||T_2)$, $CID'_i = E_x(ID_i||a')$. Note that $CID_i, CID'_i$ are encrypted ciphertexts of $ID_i$ by $x$, and nobody other than the server has the private key. And remaining parts $M_1, M_2, M_3, M_4$ are the form of output hash function of with a user's identity. Due to one-way property of collision-resistant hash function, it is hard to compute the ID from these eavesdropped message. Hence, our proposed scheme provide patient's anonymity.

**Replay attack.**

In proposed scheme, the current timestamp is included in the login message $\{M_1, M_2, CID_i, T_1\}$ and the response message $\{M_3, M_4, CID'_i, T_2\}$, where $M_1 = AID_i \oplus D$, $M_2 = h(AID_i||D||T_1)$, $M_3 = AID_i \oplus E$, $M_4 = h(CID'_i||SK||E||T_2)$. If the attacker wants to send the login message or authentication message only altering time stamp, the patient and the server could detect the replay attack by checking the validity of $T_1$ and $T_2$ respectively. If the attacker generates $M_1, M_2$ or $M_3, M_4$ by himself, $M_1$ and $M_3$ are computed from value $AID_i$, which needs the knowledge of $PW_i, B_i$(or $x$), and $M_2$ and $M_4$ are protected by a hash function. Hence, our scheme can present replay attack.

**User impersonation attack.**

If the adversary wants to impersonate the legitimate user to the server, he has to generate a valid login request message $\{M_1, M_2, CID_i, T_1\}$, where $M_1 = AID_i \oplus D, M_2 = h(AID_i||D||T_1),$. It is clear that the adversary can generate a random element in $Z_p^*$ and guess the patient's identity to compute $M_2$, and the third part $CID_i$ can be retrieved from the eavesdropped message $\{M_3, M_4, CID'_i, T_2\}$ in authentication phase. But, it is very difficult to calculate the valid number $M_1$ without the knowledge of $AID_i$. $AID_i$ can be computed by the pair $(ID_i, PW_i, B_i)$ and $V_i$. Then the server could detect the attack by checking the correctness of $M_1$ and $M_2$. Therefore, the proposed scheme can prevent the user impersonation attack.

**Server spoofing attack.**

To masquerade as the legal server, an attacker aims to generate the forged response message $\{M_3, M_4, CID_i, T_1\}$, where $M_3 = AID_i \oplus D$, and $M_4 = h(CID'_i||SK||E||T_2)$. It is easy to obtain the part $CID'_i$ by monitoring the communicating channel. However, $M_3$ cannot made without the value $AID_i$, and $M_4$ is a one-way hash function with private parameters $SK$. Computing both valid $M_3, M_4$ are hard for the attacker without server's secret key $x$. Therefore, the proposed scheme can withstand the server impersonation attack.

**Off-line password guessing attack.**

For this attack model, an adversary is assumed that he is able to extract all the secret information stored in the memory of smart card by power analysis attack. Thus, he obtain the parameters $\{K_i, V_i, CID_i, R_i\}$, where only $V_i$ and $R_i$ are related with the patient's password. In the following, we show that the adversary can not extract successfully the patient's password by off line password guessing attack.

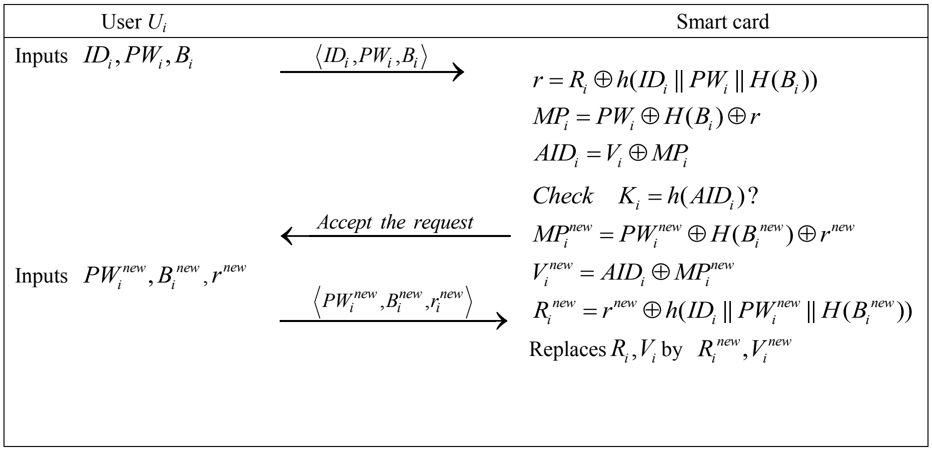


Figure 3: Password change phase of proposed scheme

- We know that $V_i = AID_i \oplus PW_i \oplus H(B_i) \oplus r$, where $AID_i$ is computed by $ID_i$ and server's private key $x$, $r$ is a random number. Given $ID_i, PW_i$, it is computationally hard to get $x$, user's biometric $B_i$ and $r$. Hence, the attacker can not check whether the equation of $V_i$ holds by guessing a patient's identity and password.
- For $R_i$, we have $R_i = r \oplus h(ID_i||PW_i||H(B_i))$. In order to utilize the above equality, the attacker not only needs the parameters $ID_i, PW_i$ but also have to know both private biometric $B_i$ and $r$.
- Combining $V_i$ and $R_i$, $r$ can be represented by $R_i \oplus h(ID_i||PW_i||H(B_i))$. That is to say, $V_i = h(ID_i||x) \oplus PW_i \oplus H(B_i) \oplus R_i \oplus h(ID_i||PW_i||H(B_i))$. It only works efficiently to know $(ID_i, PW_i, B_i, x)$ for the adversary by executing off-line password guessing attack.

From above analysis, the adversary has to check the validity of pair $(ID_i,\ PW_i, B_i, x)$ by combining $V_i$ and $R_i$. It is infeasible for doing an exhausted search for all possible $(ID_i, PW_i, B_i, x)$ pairs. Hence, the proposed scheme could resist off-line password guessing attack.

**Perfect forward secrecy.**
An authentication and key agreement protocol can provide perfect forward secrecy if an adversary knowing both user's password $PW_i$ and server's secret key $x$, but still can not compute previous session keys. For a session key $SK = h(AID_i||d_s(D)||CID_i)$ in our proposed scheme, $U_i$ selects a random $d_u$ and $S$ chooses a random $d_s$ for each session, the attacker needs to know $d_u$ and $d_s$ in order to get the session key. However, he only get $d_uP$ and $d_sP$ from $PW_i$ ,$x$ and the eavesdropped messages. That means an adversary need to compute $d_sd_uP$ from $d_uP$ and $d_sP$. It's a Diffie-Hellman problem in elliptic curve, which has no efficient polynomials algorithm solving it. Therefore, our authentication scheme posses perfect forward secrecy.

**Mutual authentication.**
In our scheme, an user $U$ validates the message $\{M_3, M_4, CID'_i, T_2\}$ by checking both the timestamp $T_2$ and the condition $M'_4 = M_4$ are valid or not. $S$ validates the message $\{M_5, T_3\}$ sent by patient using checking whether both the timestamp $T_3$ and the condition $M'_5 = M_5$ hold. Also, an user and the server agree with a session key which is known with themselves.

**Efficient login and password change.**
In the login and password change phase of our proposed scheme, the smart card must verify $K_i \stackrel{?}{=} (V_i \oplus MP_i)$, where $MP_i = PW_i \oplus H(B_i) \oplus R_i \oplus h(ID_i||PW_i||H(B))$, which includes the patient's identity, password, and biometric. If it's not true, the smart card rejects the user's login and password changing request. The quick detection of incorrect identity, password and biometric make the proposed scheme efficient. Also, this verification can present denial of service attack well.

# 7 Discussion

This section give a comparison of security and performance of recent biometric-based authentication and key agreement schemes for TMIS [2, 3, 15, 18, 23, 26]. Table 2 describes that the flaws of security and efficiency for biometric based authentication schemes for TMIS.

In Table 2, we represent $\surd$ as the scheme which prevents attack or satisfies the attribute and $\times$ as the scheme which fails to prevent attack or does not satisfy the attribute. From Table 2, it is clear to see that most of previous biometric authentication schemes do not satisfy desirable security attributes. However, Yan et al.'s

Table 2: Security attributes comparison of biometric based authentication schemes

| Security attributes \ Schemes | [15] | [26] | [3] | [23] | [2] | [18] | Ours |
|---|---|---|---|---|---|---|---|
| User anonymity | × | × | × | × | √ | √ | √ |
| Off-line password guessing attack | √ | × | × | × | × | √ | √ |
| Stolen smart card attack | √ | √ | √ | √ | √ | √ | √ |
| Impersonation attack | × | √ | √ | √ | √ | × | √ |
| Replay attack | √ | √ | × | √ | √ | √ | √ |
| Denial of service attack | √ | √ | × | √ | √ | √ | √ |
| Strong forward secrecy | √ | √ | √ | × | × | × | √ |
| Session key verification | √ | √ | × | √ | √ | √ | √ |
| Efficient password change | √ | × | × | √ | √ | √ | √ |

scheme [26] and Awasthi-Srivastava's scheme [3] with hash function computation have less computation overhead as compare to [2, 15] which have elliptic curve point multiplication costs, which is also shown in Table 3. Lu et al.'s scheme [15], Yan et al.'s scheme [26], Awasthi-Srivastava and Wen's schemes [3, 23] have the failure of protecting user anonymity. However, user anonymity during message exchange ensures consumer's privacy by preventing an attacker from acquiring consumer's sensitive personal information. Thus, an ID-based authentication scheme should ensure anonymity and unlinkability. The schemes [2, 3, 23, 26] can't resist against the off-line password guessing attack, which means an attacker is able to find user's correct password using an off-line exhaustive search for all possible passwords. Hence, a password-based authentication scheme should resist on-line and off-line password guessing attacks.

Lu et al.'s scheme [15] and Mishra et al.'s scheme [18] is vulnerable to impersonation attack, which means that an adversary could impersonate as a legal user to access any services. Awasthi-Srivastava's scheme [3] does not resist replay attack. In general, their schemes can remedy this security flaw by adding time stamp or a counter. Therefore, an secure authentication scheme should be secure against replay attack.

In the above discussed schemes of Table 2, the smart card cannot correctly identify the correctness of input which causes extra computation and communication overhead. The scheme [3] has flaws in password change phase and the schemes [3, 26] have inefficient password change phase. It is clear from the study that inefficient password change can cause DOS attack in case of incorrect input in password change phase, i.e., onetime mistake in password change phase, a valid user no longer login to the server using the same smart card. The authentication schemes could detect incorrect input quickly so that denial of service attack, and extra communication and computation overhead can be avoided.

Table 3 discusses the computation overhead of these schemes in login and authentication phase, where $T_{sym}, T_h, T_H, T_{ME}$ and $T_{ECC}$ denote the time complexity of symmetric encryption/decryption, hash function, biometric hash function, modular exponentiation and elliptic curve point multiplication, respectively. It is noted that, $T_{ECC} > T_{ME} \gg T_{sym} \gg T_H \gg T_h$. 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.

# 8 Conclusions

We have analyzed the security of Lu et al.'s biometric based authentication schemes for TMIS. It is shown that their scheme is vulnerable to protect user anonymity, and an adversary could determine whether two messages are transmitted from the same user. The scheme is also insecure against impersonation attack which leads to an adversary could impersonate as a legal user to access any services provided by telecare server, and cheat a honest user as a legal server. Moreover, we employ biometric hash function and elliptic curve Diffie C Hellman problem to improve the security and efficiency of Lu et al.'s scheme. It is noted that the enhanced scheme does not provide all security attributes of three-factor authentication schemes.

# 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] 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, 2016.

Table 3: Performance evaluation of biometric based authentication schemes

| Schemes | User computation | Server computation |
|---|---|---|
| Lu et al.'s scheme [15] | $2T_{ECC} + T_H + 5T_h$ | $T_{ECC} + 5T_h$ |
| Yan et al.'s scheme [26] | $6T_h$ | $5T_h$ |
| Awasthi-Srivastava's scheme [3] | $4T_h + T_vb$ | $3T_h$ |
| Wen's scheme [23] | $2T_{sym} + 9T_h$ | $2T_{sym} + 6T_h$ |
| Arshad et al.'s scheme [2] | $2T_{ECC} + T_m + 8T_h$ | $2T_{EEC} + 2T_m + 7T_h$ |
| Mishra et al.'s scheme [18] | $T_H + 6T_h$ | $2T_{sym} + 7T_h$ |
| Our scheme | $2T_{ECC} + T_H + 5T_h$ | $2T_{ECC} + 4T_h + T_{sym}$ |


[2] H. Arshad and M. Nikooghadam, "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 38, no. 12, pp. 136–147, 2014.

[3] A. K. Awasthi and K. Srivastava, "An enhanced biometric authentication scheme for telecare medicine information systems with nonce," *Journal of Medical Systems*, vol. 37, no. 12, pp. 9964–9976, 2013.

[4] C. C. Chang, W. Y. Hsueh, and T. F. Cheng, "An advanced anonymous and biometrics-based multi-server authentication scheme using smart cards," *International Journal of Network Security*, vol. 18, no. 6, pp. 1010–1021, 2016.

[5] Y. F. Chang, S. H. Yu, and D. R. Shiao, "An uniqueness and anonymity-preserving remote user authentication scheme for connected health care," *Journal of Medical Systems*, vol. 37, no. 12, pp. 9902–9910, 2013.

[6] H. M. Chen, J. W. Lo, and C. K. Yeh, "An efficient and secure dynamic id-based authentication scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3907–3915, 2012.

[7] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic id-based remote user authentication scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, 2004.

[8] D. B. He, J. H. Chen, and R. Zhang, "A more secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 2, pp. 1989–1995, 2012.

[9] S. H. Islam and G. P. Biswas, "Design of improved password authentication and update scheme based on elliptic curve cryptography," *Mathematical and Computer Modelling*, vol. 57, no. 12, pp. 2703–2717, 2013.

[10] A. T. Jin, D. Ling, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[11] M. K. Khan, K. S. Kim, and K. Alghathbar, "Cryptanalysis and security enhancement of a more efficient secure dynamic idbased remote user authentication scheme," *Computer Communications*, vol. 34, no. 3, pp. 305–309, 2010.

[12] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of 19th Annual International Cryptology Conference (CRYPTO'99)*, pp. 388–397, Santa Barbara, California, USA, Aug. 1999.

[13] H. D. Le, N. T. Nguyen, and C. C. Chang, "Provably secure and efficient three-factor authenticated key agreement scheme with untraceability," *International Journal of Network Security*, vol. 18, no. 2, pp. 335–344, 2016.

[14] C. T. Li, "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card," *IET Inforamtion Security*, vol. 7, no. 1, pp. 3–10, 2012.

[15] Y. Lu, L. Li, H. Peng, and Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 39, no. 32, pp. 1–9, 2015.

[16] A. Lumini and L. Nanni, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 40, no. 3, pp. 1057–1065, 2007.

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

[18] D. Mishra, S. Mukhopadhyay, A. Chaturvedi, S. Kumari, and M. K. Khan, "Cryptanalysis and improvement of yan et al.'s biometric-based authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 38, no. 24, pp. 1–12, 2014.

[19] E. O. Osei, J. B. Hayfron-Acquah, "Cloud computing login authentication redesign," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 1–8, 2014.

[20] Z. Tan, "An efficient biometrics-based authentication scheme for telecare medicine information systems," *Network*, vol. 2, no. 3, pp. 200–204, 2013.

[21] R. Wang amd W. Juang and C. Lei, "Robust authtication and key agreement scheme preserving the privacy of secret key," *Computer Communications*, vol. 34, no. 3, pp. 274–280, 2011.

[22] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3597–3604, 2012.

[23] F. T. Wen, "A robust uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care," *Journal of Medical Systems*, vol. 37, no. 6, pp. 1–9, 2013.

[24] Z.Y. Wu, Y.C. Lee, F. Lee, H.C. Lee, and Y. Chung, "A secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1529–1535, 2012.

[25] Q. Xie, J. Zhang, and N. Dong, "Robust anonymous authentication scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 37, no. 2, pp. 1–8, 2013.

[26] X. Yan, W. Li, P. Li, J. Wang, X. Hao, and P. Gong, "A secure biometrics-based authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 37, no. 5, pp. 9972–9977, 2013.

[27] H. Zhu, "Secure chaotic maps-based group key agreement scheme with privacy preserving," *International Journal of Network Security*, vol. 18, no. 6, pp. 1001–1009, 2016.

[28] H. Zhu, Y. Zhang, H. Li, and L. Lin, "A novel biometrics-based one-time commitment authenticated key agreement scheme with privacy protection for mobile network," *International Journal of Network Security*, vol. 18, no. 2, pp. 209–216, 2016.

[29] Z. Zhu, "An efficient authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3833–3838, 2012.

# Biography

**Lidong Han** received his Ph.D. degree from School of Mathematics, Shandong University, China, in 2010. Now, he work at Hangzhou Normal University. His research interests include Cryptography and cloud computing.

**Qi Xie** is a professor in Hangzhou Normal University of China. And he received his Ph.D. degree from Department of Mathematics(School of Mathematical Sciences), Zhejiang University, China, in 2010. His research interests include authentication and key exchange.

**Wenhao Liu** received his Ph.D. degree from University of Electronic Science and Technology of China in 2010. Now, he work at Key Laboratory of Cryptography and Network Security of Hangzhou Normal University. His research interests include signature and data security in cloud.