MOBILE SYSTEMS

An Improvement of Robust and Efficient Biometrics Based Password Authentication Scheme for Telecare Medicine Information Systems Using Extended Chaotic Maps

Jongho Moon[1] · Younsung Choi[1] · Jiye Kim[1] · Dongho Won[1]

Received: 28 May 2015 / Accepted: 8 December 2015 / Published online: 7 January 2016

Abstract Recently, numerous extended chaotic map-based password authentication schemes that employ smart card technology were proposed for Telecare Medical Information Systems (TMISs). In 2015, Lu et al. used Li et al.'s scheme as a basis to propose a password authentication scheme for TMISs that is based on biometrics and smart card technology and employs extended chaotic maps. Lu et al. demonstrated that Li et al.'s scheme comprises some weaknesses such as those regarding a violation of the session-key security, a vulnerability to the user impersonation attack, and a lack of local verification. In this paper, however, we show that Lu et al.'s scheme is still insecure with respect to issues such as a violation of the session-key security, and that it is vulnerable to both the outsider attack and the impersonation attack. To overcome these drawbacks, we retain the useful properties of Lu et al.'s scheme to propose a new password authentication scheme that is based on smart card technology and requires the use of chaotic maps. Then, we show that our proposed scheme is more secure and efficient and supports security properties.

This article is part of the Topical Collection on *Mobile Systems*

Grants, communicated-by lines, or other notes about the article will be placed here between rules. Such notes are optional.

✉ Jongho Moon
jhmoon@security.re.kr

✉ Dongho Won
dhwon@skku.edu

[1] Information Security Group, Sungkyunkwan University,
2066 Seobu-ro, Suwon 16419, Korea

Keywords Chebyshev chaotic maps · User authentication · Smart cards · Telecare medicine information systems

Introduction

The Telecare Medical Information System (TMIS) provides an effective way to enhance the medical process between the doctors and nurses at a clinical center or a home healthcare (HHC) agency, and home-based patients. According to the traditional medical diagnosis process, a patient goes to a hospital or a clinic, and then consults a doctor; however, TMIS technology means that patients can remain within their home, as they can still access convenient and prompt medical treatment through the Internet or mobile networks [1, 2]. With a TMIS, patients can save a great amount of time and access doctors and specialists more easily; for example [2], by using a TMIS, a hypertension patient or a diabetes mellitus patient can directly exchange his/her daily medical data, collected by the patient at home, for the medical advice of doctors and/or nurses without needing to visit a hospital or a clinic; however, the user accesses the telecare medical services over a public network, exposing the exchange to security risks. It is therefore important, but also challenging, to enhance the security of TMIS technology so that a patient and a doctor can perform mutual authentication and session key establishment on a medical server without compromising the privacy of the patient.

Password authentication schemes have been widely used over the last two decades. Since Lamport [3] proposed the first password-based authentication scheme for insecure communication in 1981, password authentication schemes [4–8] have been extensively investigated. Recently, a remote user authentication protocol became essential for TMISs so that remote patients could access the resources on the telecare server. Several authenticated key agreement schemes [9–13] have been proposed for TMISs. In 2010, Wu et al. [14] proposed a low computation password-based authentication scheme; however, He et al. [15] pointed out that Wu et al.'s scheme is vulnerable to the insider and impersonation attacks. To overcome these weaknesses, He et al. proposed an improved scheme, but unfortunately, Wei et al. [16] demonstrated that the schemes of both Wu et al. and He et al. are vulnerable to the off-line password guessing attack. To solve the limitations of the schemes of Wu et al. and He et al., Wei et al. also developed an improved scheme; however, Zhu [17] later showed that Wei et al.'s scheme is insecure against the off-line password guessing attack and designed an authentication scheme to address this limitation. Nevertheless, the high computational overhead that is caused by modular exponential operations means that it is less feasible to practically apply these works.

With the rapid development of cryptography related chaos theory [18–20], an increasing number of chaos theory-based authentication schemes have been widely studied, as the performances of these schemes are more effective than that of traditional cryptography [21]. In 2007, Xiao et al. [22] developed the first chaotic map-based, authenticated key agreement protocol for which random numbers are used. Tseng et al. [23] then proposed a scheme that comprises a chaotic map-based authentication and key agreement and supposedly preserves user anonymity; unfortunately, Niu et al. [24] found that Tseng et al.'s scheme does not actually provide user anonymity and presented an improved scheme to overcome the weakness. Xue et al. [25], however, pointed out that Niu et al.'s scheme is vulnerable to the man-in-the-middle attack.

Recently, Guo et al. [26] proposed a chaotic map-based, password authenticated key agreement scheme for which smart cards are required; unfortunately, both Hao et al. [27] and Lin [28] pointed out that user anonymity is not guaranteed under Guo et al.'s scheme. To remedy the identified deficiency, Hao et al. and Lin presented their modified versions of Guo et al.'s scheme; however, Jiang et al. [29] and Lee [30] showed that Hao et al.'s scheme did not achieve fairness in terms of session key establishment and is vulnerable to the stolen smart card attack. Both Jiang et al. and Lee then developed improved schemes to overcome the flaws of Hao et al.'s scheme; unfortunately, Li et al. [31] demonstrated that the schemes of both Jiang et al. and Lee cannot withstand the service misuse attack for non-registered users and reveals the user's identity during the authentication phase.

While addressing the limitations of the schemes of Lee and Jiang et al., Li et al. presented a slightly modified version of Lee's scheme to prevent thecorresponding shortcomings. Afterward, Lu et al. [32] found that Li et al.'s modified scheme still comprises some weaknesses such as a violation of the session key security, a vulnerability to the user impersonation attack, and a lack of local verification, and they subsequently proposed a robust and efficient biometrics-based password authentication scheme for TMISs for which extended chaotic maps are used; however, we found that the authentication scheme of Lu et al. is still insecure with respect to the outsider attack, the impersonation attack, and the replay attack, among others. The contributions of the proposed article are two fold. First, we point out the security flaws of Lu et al.'s user authentication scheme, and secondly, we present a new chaotic map-based, remote user authentication scheme for TMISs; moreover, the proposed scheme is more secure than Lu et al.'s scheme.

The remainder of this paper is organized as follows: The section titled "Preliminaries" introduces some preliminaries about Chebyshev chaotic maps and hash functions; the review and security analysis of Lu et al.'s scheme are shown in "Review of Lu et al.'s Scheme" and "Security analysis of Lu et al.'s Scheme", respectively; "Our proposed authentication scheme" and "Security analysis" present our proposed scheme and an analysis of its security, respectively; "Functionality and performance comparison analysis" shows the comparisons of the performances and security features of the proposed scheme and other related schemes; and "Conclusion" is composed of a brief conclusion.

Preliminaries

In this section, we briefly introduce the one-way hash function [33] and Chebyshev chaotic maps [34, 35]. The Chebyshev polynomial $T_n(x)$ is an x polynomial of degree n.

Definition 1 A secure one-way hash function $h : \{0, 1\}^* \rightarrow \{0, 1\}^n$ that takes an input as an arbitrary length binary string $x \in \{0, 1\}^*$ and outputs a binary string $h(x) \in \{0, 1\}^n$. The probability of $\mathcal{A}$ finding a collision is defined as

$$Adv^{\mathcal{A}}_{HASH}(t_1) = Pr[\mathcal{A}((x, x'), x \neq x') : h(x) = h(x')].$$

Definition 2 Let n be an integer and x is a real number from the set $[-1, 1]$, so that the Chebyshev polynomial of degree n is defined as $T_n(x) = cos(n \cdot arccos(x))$.

Definition 3 Given the two elements x and $y \in Z_p^*$, the Chaotic Maps Discrete Logarithm Problem (CMDLP) is whe- ther the integer r can be found such that $y = T_r(x)$. The probability of $\mathcal{A}$ being able to solve the CMDLP is defined as $Adv^{\mathcal{A}}_{CMDLP}(t_2) = Pr[\mathcal{A}(x, y) = r : r \in Z^*_P, y = T_r(x) \; mod \; p]$.

Definition 4 Given the three parameters x, $T_r(x)$ and $T_s(x)$, the Chaotic Maps Diffie-Hellman Problem (CMDHP) is whe- ther $T_{rs}(x)$ can be computed such that $T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$.

Review of Lu et al.'s Scheme

In this section, we review Lu et al.'s biometrics-based password authentication scheme for TMISs for which chaotic maps are used. Their scheme consists of the following three phases: registration, login and authentication, and password updating. For convenience, some of the notations that are used in Lu et al.'s scheme are described in Table 1.

Registration

(1) U inputs his/her biometrics characteristic BIO, and selects an identity ID and a password PW. Then, U computes $PWD = h_1(PW||H(BIO))$ and sends $\{ID, PWD\}$ to S over a secure channel.

(2) S computes $K = h_1(ID||PWD)$ and $IM_1 = K \oplus h_1(k_s)$, where k_s is S's secret key. S then issues a smart card containing $\{IM_1, h_1(\cdot), h_2(\cdot), H(\cdot)\}$ to U.

(3) U selects a secret key k_u and computes $f = h_1(ID||k_u) \oplus PWD$. Then, U stores f onto the smart card; therefore, it is noted that the smart card of U contains the information $\{IM_1, f, h_1(\cdot), h_2(\cdot), H(\cdot)\}$.

Login and authentication

(1) U first inserts the smart card into a card reader and inputs his/her identity ID, password PW, and secret key k_u and also imprints his/her biometrics BIO at the sensor. U then checks whether $h_1(ID||k_u) \oplus h_1(PW||H(BIO)) \overset{?}{=} f$; if it holds, U computes $K = h_1(ID||h_1(PW|| \; H(BIO)))$, generates a random number u, and computes $R_1 = K \oplus ID$, $R_2 = ID \oplus T_u(K)$, and $R_3 = h_1(ID||T_u(K))$. Lastly, U sends the message $\{R_1, R_2, \; R_3\}$ to S.

(2) After receiving the login request message from U, S uses the secret key k_s to derive K by computing $K' = IM_1 \oplus \; h_1(k_s)$. He/she then computes $ID = R_1 \oplus K$ and $T_u(K) = ID \oplus R_2$, and checks $h_1(ID||T_u(K)) \overset{?}{=} R_3$; if it is correct, S then generates a random number v and computes $IM_2 = T_v(K) \oplus ID$, $sk = h_2(T_u(K), T_v(K), \; T_{uv} \; (K))$, and $Auth_s = h_1(K||T_v(K)||sk)$. Lastly, S sends the message $\{Auth_s, IM_2\}$ to U.

(3) Upon receiving the login response message from S, U derives $T_v(K)$ by computing $IM_2 \oplus ID$, and computes $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$ to verify whether $h_1 \; (K||T_v(K)||sk)$ is equal to the received $Auth_s$. If it is holds, U successfully authenticates S and computes $Auth_u = h_1(sk||T_v(K)||K)$, and then sends the message $\{Auth_u\}$ to S.

(4) Upon receiving the message from U, S validates whether $h_1(sk||T_v(K)||K) \overset{?}{=} Auth_u$. If it is true, S successfully authenticates U; otherwise, S aborts the request. Lastly, U and S have the common session key $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$.

Table 1 Notations used in Lu et al.'s scheme

Terms	Description
U	A user
S	A server
ID	An identity of an entity U
PW	A password of an entity U
BIO	A biometric characteristic of an entity U
$H(\cdot)$	Biohash function
$h_1(\cdot), h_2(\cdot)$	Hash function h_1: $\{0, 1\}^* \rightarrow \{0, 1\}^l$
	Hash function h_2: $[-1, 1] \rightarrow \{0, 1\}^l$
k_u, k_s	Secret key selected by U and S, respectively
$\oplus$	Exclusive-or operation
$\|\|$	Concatenation operation

Password change

If U wants to change his/her password, U inserts his/her smart card into the card reader and keys in ID, PW, k_u, and BIO. Then, the smart card checks whether $h_1(ID||k_u) \oplus h_1(PW||H(BIO)) \overset{?}{=} f$; if it holds, U submits a new password PW_{new} as well as a new secret key $k_{u(new)}$. The smart card then computes f_{new}, followed by the replacement of f with f_{new}.

Security analysis of Lu et al.'s Scheme

Lu et al. claimed that their scheme is resistant to the impersonation attack; however, we demonstrated that their scheme is still insecure against this attack type. We also found that their scheme is not secure against the outsider attack and the session key attack, and that it cannot support user anonymity; furthermore, some of the phases of Lu et al.'s scheme are not correct. We provide the details of these problems in the following subsections.

Incorrect login and authentication phase

In the login and authentication phase of Lu et al.'s scheme, the user U sends the login request message $\{R_1, R_2, R_3\}$ to server S, followed by the computation of $K' = IM_1 \oplus h_1(k_s)$ by server S. If, however, IM_1 is not the received value from U, this process is impossible; therefore, we assumed that user U sends the IM_1 to server S.

Incorrect password change phase

During the password change phase of Lu et al.'s scheme, if U wants to change his/her password, the smart card checks whether $h_1(ID||k_u) \oplus h_1(PW||H(BIO)) \overset{?}{=} f$; if it holds, U submits a new password PW_{new} and a new secret key $k_{u(new)}$, and the smart card then computes f_{new}, followed by the replacement of f with f_{new}. To update $IM_{1(new)}$, however, IM_1 is also required . If IM_1 is not updated, U will compute $K_u = h_1(ID||h_1(PW_{new}|| \ H(BIO)))$ after the password updating stage and S will compute $K_s = IM_1 \oplus h_1(k_s) = h_1(ID||h_1(PW||H(BIO)))$; therefore, U will compute $sk_u = h_2(T_u(K_u), T_v(K_s), T_{uv}(K_s))$ and S will compute $sk_s = h_2(T_u(K_u), T_v(K_s), T_{uv}(K_u))$. Lastly, both U and S cannot have the sheared session key sk.

Outsider attack

Let $\mathcal{A}$ be an active adversary [36] who owns a smart card and can extract [37] the information of the legal user $\{IM_1, h_1(\cdot), h_2(\cdot), f, H(\cdot)\}$. He/she can then easily obtain $h_1(k_s)$ that is the same for each legal user and is the hash value of the secret key that is selected by server S.

(1) $\mathcal{A}$ computes $PWD_{\mathcal{A}} = h_1(PW_{\mathcal{A}}||H(BIO_{\mathcal{A}}))$ and $K_{\mathcal{A}} = h_1(ID_{\mathcal{A}}||PWD_{\mathcal{A}})$; then, he/she can obtain $h_1(k_s)$ by calculating $IM_1 \oplus K_{\mathcal{A}}$.

Violation of the session key security

If $\mathcal{A}$ intercepts the communication between U and S, he/she can then obtain all of the messages $\{IM_1, R_1, R_2, R_3, Auth_s, \quad IM_2, Auth_u\}$; furthermore, he/she can also easily obtain the session key between U and S. The details are described as follows:

(1) $\mathcal{A}$ computes $K = IM_1 \oplus h_1(k_s)$, $ID = R_1 \oplus K$, $T_u(K) = R_2 \oplus ID$, and $T_v(K) = IM_2 \oplus ID$.
(2) Using the [37], $\mathcal{A}$ computes $u' = \frac{arcos(T_u(K))+2k\pi}{arccos(x)}$, $v' = \frac{arccos(T_v(K))+2k\pi}{arcos(x)}$, $\forall k \in Z$ to satisfy the equation $T_u(K) = T_{u'}(K)$, and $T_v(K) = T_{v'}(K)$. Then, he/she can compute $T_{uv}(K) = T_u(T_v(K)) = T_{u'}(T_{v'}(K))$ therefore, $\mathcal{A}$ can obtain the shared session key $sk = h_2(T_u(K), T_v(K)\ , T_{uv}(K))$.

User impersonation attack

As described in this subsection, an outsider adversary $\mathcal{A}$ can also impersonate a legal user U to cheat the server S because he/she can know the secret value K of U. The details are described as follows:

(1) $\mathcal{A}$ generates a random number u' and computes $T_{u'}(K)$, $R_2 = ID \oplus T_{u'}(K)$, and $R_3 = h_1(ID||T_{u'}(K))$. Then, $\mathcal{A}$ sends the login request message $\{IM_1, R_1, R_2, R_3\}$ to S.
(2) After receiving the login request message from $\mathcal{A}$ who pretends to be U, the messages can successfully pass S's verification and S performs the following scheme normally. Then, S sends the login response message $\{Auth_s, IM_2\}$ to $\mathcal{A}$, where v is the random number on the server side.
(3) Upon receiving the login response message from S, $\mathcal{A}$ computes $T_v(K) = IM_2 \oplus ID$, $T_{u'v}(K) = T_{u'}(T_v(K))$, $sk = h_2(T_{u'}(K), T_v(K), T_{u'v}(K))$, and $Auth_u = h_1(\ sk||T_v(K)||K)$. Then, $\mathcal{A}$ sends the authentication message $\{Auth_u\}$ to S.
(4) When receiving the message $\{Auth_u\}$ from $\mathcal{A}$, S continues to proceed with the scheme without being detected. Lastly, $\mathcal{A}$ and S "successfully" agree on a shared session key sk; however, an unfortunate outcome occurs, as S mistakenly believes that he/she is communicating with the legitimate user U.

Server impersonation attack

An outsider adversary $\mathcal{A}$ can also impersonate a server S to cheat user U because he/she knows the secret value $h_1(k_s)$ of server S. $\mathcal{A}$ performs the following steps:

(1) When U is sending the login request message $\{IM_1, R_1, \ R_2, R_3\}$ to server S, $\mathcal{A}$ can intercept this message and compute $K = IM_1 \oplus h_1(k_s)$, $ID = R_1 \oplus K$, and $T_u(K) = R_2 \ \oplus ID$.
(2) $\mathcal{A}$ generates a random number v' and computes $IM_2 = T_{v'}(K) \oplus ID$, $sk = h_2(T_u(K), T_{v'}(K), T_{uv'}(K))$, and $Auth_s = h_1(K||T_{v'}(K)||sk)$. Lastly, $\mathcal{A}$ sends the login response message $\{Auth_s, IM_2\}$ to U.
(3) After receiving the login response message $\{Auth_s, IM_2\}$ from $\mathcal{A}$, U continues to proceed with the scheme without being detected. Lastly, U and $\mathcal{A}$ "successfully" agree on a shared session key sk; however, an unfortunate outcome occurs, as U mistakenly believes that he/she is communicating with the server S.

Lack of user anonymity

Lu et al. claimed that their scheme can preserve the anonymity of an identity since ID cannot be derived from R_1 without the knowledge of K; additionally, K cannot be derived from IM_1 without the server's private key k_s. However, we found that if an outsider adversary $\mathcal{A}$ can obtain $h_1(k_s)$, then he/she can compute $K = IM_1 \oplus h_1(k_s)$ and $ID = R_1 \oplus K$. Lu et al.'s scheme is therefore unable provide user anonymity.

Our proposed authentication scheme

In this section, we propose a new biometrics-based password-authentication scheme for TMISs for which an extended chaotic map is used. Lu et al. verified that Biohasing is very efficient and lightweight compared to modular exponentiation and elliptic-curve point multiplication [38, 39]. We also adopted Biohasing to protect patient's biometrics, which can also counter a high number of false rejections that therefore decreases the probability that service access is denied [40]. Our proposed scheme consists of the following four phases: registration, login, authentication, and password changing. For convenience, some of the notations that are used in our proposed scheme are described in Table 2 and our proposed scheme consists of the following login and session key agreement phases as shown in Fig. 1.

Registration phase

(1) U inputs his/her biometrics characteristics BIO, and selects an identity ID and a password PW. Then U computes $PWD = h_1(PW||H(BIO))$ and sends $\{ID, PWD\}$ to server S over a secure channel.

Table 2 Notations used our proposed scheme

U	A user
S	A server
SC	A smart card
ID	An identity of an entity U
PW	A password of an entity U
BIO	Biometric characteristic of an entity U
$H(\cdot)$	Biohash function
$h_1(\cdot), h_2(\cdot)$	Hash function h_1: $\{0,1\}^* \rightarrow \{0,1\}^l$ Hash function h_2: $[-1,1] \rightarrow \{0,1\}^l$
k_u	A random number unique to U selected by S
k_s	Secret master key selected by S
$\oplus$	Exclusive-or operation
$\|\|$	Concatenation operation

(2) Upon receiving the registration request message from U, S checks whether or not ID is already in the database. If ID does not exist, S generates a random number k_u that is unique to U. Then, S computes $K = h_1(ID||PWD)$, $IM_1 = K \oplus h_1(k_u)$, $IM_2 = h_1(k_u||k_s) \oplus h_1(k_s)$ and $f = IM_1 \oplus h_1(ID \oplus PWD)$ where k_s is S's secret master key. Note that k_u is a fixed length value. Lastly, S stores $\{ID \oplus h_1(k_s||k_u), k_u \oplus k_s, h_1(k_u||k_s)\}$ in its database.

(3) S stores a smart card containing $\{IM_1, IM_2, f, h_1(\cdot), h_2(\cdot), H(\cdot)\}$ and sends a smart card SC to U through a secure channel, thereby completing the registration phase.

Login phase

(1) U first inserts the smart card into a card reader and enters his/her identity ID and password PW, and also imprints his/her biometric BIO at the sensor. SC then computes $PWD = h_1(PW||H(BIO))$ and checks whether $IM_1 \oplus h_1(ID \oplus PWD) \overset{?}{=} f$.

(2) If it holds, SC computes $K = h_1(ID||PWD)$ and generates a random number u. Then, SC computes $R_1 = ID \oplus T_u(K)$ and $R_2 = h_1(ID||K||T_u(K))$; otherwise, SC rejects the login request. Lastly, SC sends the login request message $\{IM_1, IM_2, R_1, R_2\}$ to S.

Authentication phase

(1) After receiving the login request message from U, S uses his/her secret key k_s to derive $h_1(k_u||k_s)$ by computing $h_1(k_u||k_s) = IM_2 \oplus h_1(k_s)$; then he/she checks whether or not $h_1(k_u||k_s)$ is already in the database. If $h_1(k_u||k_s)$ does exist, S computes $K = IM_1 \oplus h_1(k_u)$ and $T_u(K) = ID \oplus R_1$ and checks whether $h_1(ID||K|| T_u(K)) \overset{?}{=} R_2$; if it holds, S then generates a random number v and computes $IM_3 = T_v(K) \oplus ID$, $sk = h_2(T_u(K), T_v(K), T_{vu}(K))$, and $Auth_s = h_1(K|| T_v(K)||sk)$. Lastly, S sends the login response message $\{Auth_s, IM_3\}$ to U.

(2) Upon receiving the login response message from S, SC derives $T_v(K)$ by computing $IM_3 \oplus ID$, and $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$ is also computed to verify whether h_1 $(K||T_v(K)||sk)$ is equal to the received $Auth_s$; if it is holds, U successfully authenticates S and computes $Auth_u = h_1(sk||T_v(K)||K)$ and the authentication response message $\{Auth_u\}$ is sent to S.

(3) When receiving the authentication response message from U, S validates whether $h_1(sk||T_v(K)||K) \overset{?}{=} Auth_u$. If it is true, S successfully authenticates U; otherwise, S aborts this request. Lastly,

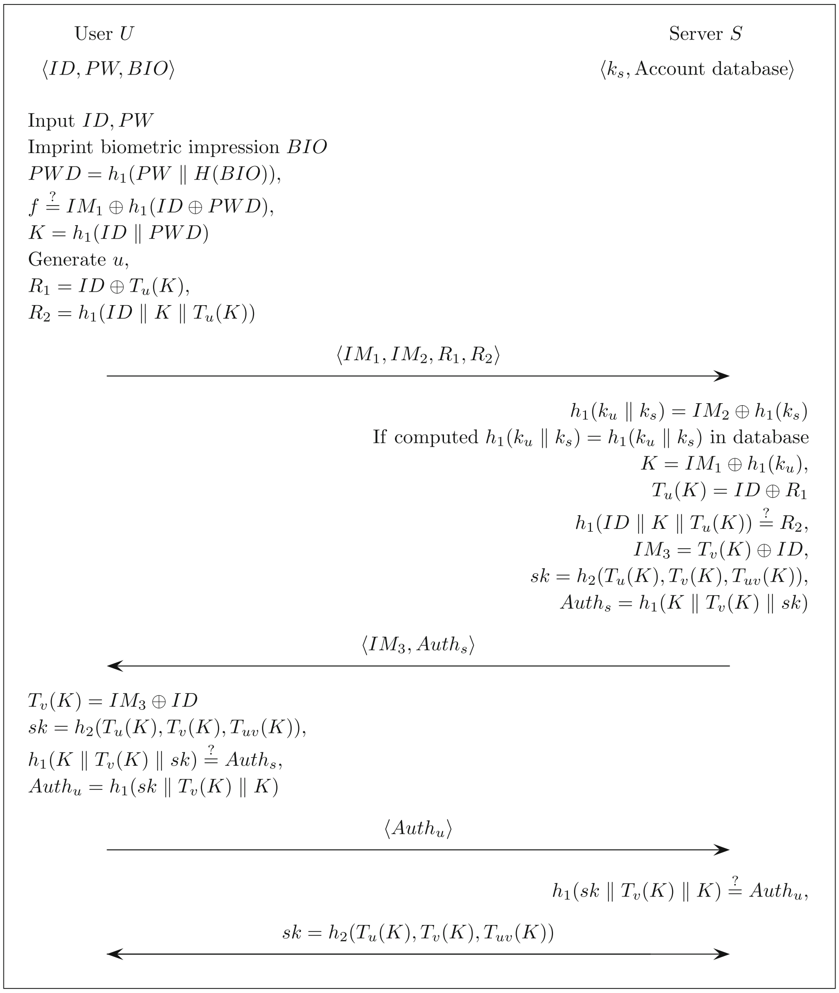

Fig. 1 Login and session key agreement phase of our scheme

User U | Server S

$\langle ID, PW, BIO\rangle$ | $\langle k_s, \text{Account database}\rangle$

Input ID, PW
Imprint biometric impression BIO
$PWD = h_1(PW \parallel H(BIO))$,
$f \overset{?}{=} IM_1 \oplus h_1(ID \oplus PWD)$,
$K = h_1(ID \parallel PWD)$
Generate u,
$R_1 = ID \oplus T_u(K)$,
$R_2 = h_1(ID \parallel K \parallel T_u(K))$

$\xrightarrow{\langle IM_1, IM_2, R_1, R_2\rangle}$

$h_1(k_u \parallel k_s) = IM_2 \oplus h_1(k_s)$
If computed $h_1(k_u \parallel k_s) = h_1(k_u \parallel k_s)$ in database
$K = IM_1 \oplus h_1(k_u)$,
$T_u(K) = ID \oplus R_1$
$h_1(ID \parallel K \parallel T_u(K)) \overset{?}{=} R_2$,
$IM_3 = T_v(K) \oplus ID$,
$sk = h_2(T_u(K), T_v(K), T_{uv}(K))$,
$Auth_s = h_1(K \parallel T_v(K) \parallel sk)$

$\xleftarrow{\langle IM_3, Auth_s\rangle}$

$T_v(K) = IM_3 \oplus ID$
$sk = h_2(T_u(K), T_v(K), T_{uv}(K))$,
$h_1(K \parallel T_v(K) \parallel sk) \overset{?}{=} Auth_s$,
$Auth_u = h_1(sk \parallel T_v(K) \parallel K)$

$\xrightarrow{\langle Auth_u\rangle}$

$h_1(sk \parallel T_v(K) \parallel K) \overset{?}{=} Auth_u$,

$\xleftrightarrow{sk = h_2(T_u(K), T_v(K), T_{uv}(K))}$

U and S have a common session key $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$.

Password change phase

If U wants to change his/her password, he/she inserts his/her smart card into a card reader, and then enters his/her ID, PW, and BIO. The smart card then performs the following steps:

(1) SC computes $PWD = h_1(PW||H(BIO))$ and checks whether $IM_1 \oplus h_1(ID \oplus PWD) \overset{?}{=} f$. If it is equal, SC computes $K = h_1(ID||PWD)$ and accepts U who can enter a new password PW_{new}; otherwise, the smart card rejects the password change request.
(2) After U submits a new password PW_{new}, SC then computes $PWD_{new} = h_1(PW_{new}||H(BIO))$, $K_{new} = h_1(ID|| PWD_{new})$, $IM_{1(new)} = IM_1 \oplus K \oplus K_{new}$, and $f_{new} = IM_{1(new)} \oplus h_1(ID \oplus PWD_{new})$.
(3) SC then updates IM_1, f so that it becomes $IM_{1(new)}$, f_{new}.

Security analysis

In this section, we demonstrate that our scheme can withstand a number of possible attack types. We also show that our scheme, which keeps the merits of Lu et al.'s scheme, supports several security properties. The security analysis of our proposed scheme was conducted under the following four assumptions:

(1) An adversary $\mathcal{A}$ can be either a user or a server; furthermore, both a registered user and a registered server can act as an adversary.
(2) An adversary $\mathcal{A}$ can eavesdrop on every communication that occurs over public channels; consequently, he/she can capture any message that is exchanged between a user and a server.

(3) An adversary $\mathcal{A}$ has the ability to alter, delete, or reroute a captured message.
(4) Information can be extracted from a smart card by examining the power consumption of the card.

Formal security analysis

In this subsection, we demonstrate the formal security analysis of our proposed scheme and show that the scheme is secure. First, we define the following hash function [41].

Definition 1 A secure one-way hash function $h : \{0, 1\}^* \rightarrow \{0, 1\}^n$, which takes an input as an arbitrary length binary string $x \in \{0, 1\}^*$ and outputs a binary string $h(x) \in \{0, 1\}^n$ and satisfies the following requirements: a. Given $y \in Y$, it is computationally infeasible to find an $x \in X$ such that $y = h(x) : b$. Given $x \in X$, it is computationally infeasible to find another $x' \neq x \in X$, such that $h(x') = h(x) : c$. It is computationally infeasible to find a pair $(x', x) \in X' \times X$, with $x' \neq x$, such that $h(x') = h(x)$.

Theorem 1 Under the assumption that the one-way hash function $h(\cdot)$ closely behaves like an oracle, then our proposed scheme is provably secure against an adversary $\mathcal{A}$ for the protection of a user's personal information including his/her identity ID, the shared session key sk, the user's unique value k_u, and the server's secret number k_s that is selected by S.

Proof The formal security proof of our proposed scheme is similar to those that are in [42–44]. Use the following oracle to construct $\mathcal{A}$, who will have the ability to derive the user U's ID, the shared session key sk, the user's unique value k_u, and the server's secret number k_s that is selected by S.

Reveal: This random oracle will unconditionally output the input x from the given hash result $y = h(x)$. Now, an adversary $\mathcal{A}$ runs the experimental algorithm that is shown in Table 3, which is $EXP^{JKMSE}_{HASH,A}$ or JKMSE, for our proposed scheme. By defining the success probability for $EXP^{JKMSE}_{HASH,A}$ as $Success^{JKMSE}_{HASH,A} = |Pr[EXP^{JKMSE}_{HASH,A} = 1] - 1|$, the advantage function for this experiment then becomes

$$Adv^{JKMSE}_{HASH,A}(t, q_R) = max_A \; Success^{JKMSE}_{HASH,A}$$

where the maximum is taken over all of $\mathcal{A}$ with the execution time t and the number of queries q_R that are made to the Reveal oracle. Consider the experiment that is shown in Table 3 for $\mathcal{A}$. If $\mathcal{A}$ has the ability to solve the hash function problem that is provided in Definition 1, then he/she can directly derive U's identity ID, the shared session key sk, the user's unique value k_u, and the server's secret number k_s. In this case, $\mathcal{A}$ will discover the complete connections between U and S; however, it is a computationally infeasible problem to invert the input from a given hash value, i.e., $Adv^{JKMSE}_{HASH,A}(t) \leq \epsilon$, $\forall \epsilon > 0$. We then have $Adv^{JKMSE}_{HASH,A}(t, q_R) \leq \epsilon$, since $Adv^{JKMSE}_{HASH,A}(t, q_R)$ depends on $Adv^{JKMSE}_{HASH,A}(t)$. As a result, there is no way for $\mathcal{A}$ to discover the complete connections between U and S, and our proposed scheme is therefore provably secure against an adversary that seeks to derive (ID, PW, BIO, k_u, k_s).

Table 3 Algorithm $EXP^{JKMSE}_{HASH,A}$

```
Eavesdrop login request message $\{IM_1, IM_2, R_1, R_2\}$
Call the Reveal oracle. Let $(ID', K', T_u(K)') \leftarrow Reveal(R_2)$
Eavesdrop login response message $\{Auth_s, IM_3\}$
Call the Reveal oracle. Let $(K'', T_v(K)', sk') \leftarrow Reveal(M_4)$
**if** $(K' = K'')$ **then**
  Call the Reveal oracle. Let $(k'_u) \leftarrow Reveal(IM_1)$
  Call the Reveal oracle. Let $(k''_u, k'_s) \leftarrow Reveal(IM_2)$
  **if** $(k'_u = k''_u)$ **then**
    Accept $ID'_i, k'_u$ as the correct $ID$ and $k_u$ of $U$
    $sk'$ and $k_s$ as the session key between $U$ and $S$, and the secret key of $S$
    **return 1**
  **else**
    **return 0**
  **end if**
**else**
  **return 0**
**end if**
```

Verification of authentication scheme with BAN logic

Burrows-Abadi-Needham (BAN) logic [45] is a set of rules for the definition and analysis of information-exchange protocols. Concretely, BAN logic helps its users to decide whether ex-changed information is trustworthy and secured against eavesdropping, or both. In this section, we prove that a shared session key between a user and a server can be correctly generated within the authentication process using BAN logic. Some of the notations and logical postulates [46] that are used in BAN logic are described in Table 4.

Table 4 Notations used in BAN Logic

$\mathcal{P} \mid\equiv \mathcal{X}$	The principal $\mathcal{P}$ believes the statement X.
$\#(\mathcal{X})$	The formula $\mathcal{X}$ is fresh
$\mathcal{P} \Rightarrow \mathcal{X}$	The principal $\mathcal{P}$ has jurisdiction over the statement $\mathcal{X}$
$\mathcal{P} \overset{\mathcal{K}}{\leftrightarrow} \mathcal{Q}$	The principals $\mathcal{P}$ and $\mathcal{Q}$ may use the shared key $\mathcal{K}$
$\mathcal{P} \triangleleft \mathcal{X}$	The principal $\mathcal{P}$ sees the statement $\mathcal{X}$
$\mathcal{P} \mid\sim \mathcal{X}$	The principal $\mathcal{P}$ once said the statement $\mathcal{X}$
$\{\mathcal{X}\}_{\mathcal{K}}$	The formula $\mathcal{X}$ encrypted under the key $\mathcal{K}$
$(\mathcal{X})_{\mathcal{K}}$	The formula $\mathcal{X}$ hashed under the key $\mathcal{K}$
$\langle\mathcal{X}\rangle_{\mathcal{Y}}$	The formula $\mathcal{X}$ combined with the key $\mathcal{Y}$
$\mathcal{P} \overset{\mathcal{X}}{\rightleftharpoons} \mathcal{Q}$	The formula $\mathcal{X}$ is a secret known only to P and Q.

(1) BAN logical postulates.

a. Message-meaning rule: $\frac{\mathcal{P}|\equiv\mathcal{P}\overset{\mathcal{K}}{\leftrightarrow}\mathcal{Q},\mathcal{P}\lhd\{\mathcal{X}\}_{\mathcal{K}}}{\mathcal{P}|\equiv\mathcal{Q}|\sim\mathcal{X}}$: If principal $\mathcal{P}$ believes that he/she shares the secret key $\mathcal{K}$ with $\mathcal{Q}$, and $\mathcal{P}$ sees the statement $\mathcal{X}$ encrypted under $\mathcal{K}$, then $\mathcal{P}$ believes that $\mathcal{Q}$ once said $\mathcal{X}$.
b. Nonce-verification rule: $\frac{\mathcal{P}|\equiv\#(\mathcal{X}),\mathcal{P}|\equiv\mathcal{Q}|\sim\mathcal{X}}{\mathcal{P}|\equiv\mathcal{Q}|\equiv\mathcal{X}}$: If principal $\mathcal{P}$ believes that $\mathcal{X}$ is fresh and that $\mathcal{Q}$ once said $\mathcal{X}$, then $\mathcal{P}$ believes that $\mathcal{Q}$ believes $\mathcal{X}$.
c. The belief rule: $\frac{\mathcal{P}|\equiv\mathcal{X},\mathcal{P}|\equiv\mathcal{Y}}{\mathcal{P}|\equiv(\mathcal{X},\mathcal{Y})}$: If principle $\mathcal{P}$ believes $\mathcal{X}$ and $\mathcal{Y}$, then $\mathcal{P}$ believes $(\mathcal{X}, \mathcal{Y})$.
d. Freshness-conjuncatenation rule: $\frac{\mathcal{P}|\equiv\#(\mathcal{X})}{\mathcal{P}|\equiv\#(\mathcal{X},\mathcal{Y})}$: If principle $\mathcal{P}$ believes that $\mathcal{X}$ is fresh, then $\mathcal{P}$ believes that $(\mathcal{X}, \mathcal{Y})$ is fresh.
e. Jurisdiction rule: $\frac{\mathcal{P}|\equiv\mathcal{Q}|\Rightarrow\mathcal{X},\mathcal{P}|\equiv\mathcal{Q}|\equiv\mathcal{X}}{\mathcal{P}|\equiv\mathcal{X}}$: If principle $\mathcal{P}$ believes that $\mathcal{Q}$ has jurisdiction over $\mathcal{X}$ and $\mathcal{P}$ believes that $\mathcal{Q}$ believes $\mathcal{X}$, then $\mathcal{P}$ believes $\mathcal{X}$.

(2) Idealized scheme

U: $\langle ID\rangle_{U\overset{K}{\leftrightarrow}S}, \langle ID\rangle_{\{U\overset{K}{\leftrightarrow}S\}_u}, (ID)_{\{U\overset{K}{\leftrightarrow}S\}_u},$
$(U \overset{sk}{\leftrightarrow} S, \{U \overset{K}{\leftrightarrow} S\}_v)_{U\overset{K}{\leftrightarrow}S}$

S: $(U \overset{sk}{\leftrightarrow} S, \{U \overset{K}{\leftrightarrow} S\}_u)_{U\overset{K}{\leftrightarrow}S}, \langle ID\rangle_{\{U\overset{K}{\leftrightarrow}S\}_v}$

(3) Establishment of security goals

$g_1.$ $U|\equiv S|\equiv U \xleftrightarrow{sk} S$
$g_2.$ $U|\equiv U| \xleftrightarrow{sk} S$
$g_3.$ $S|\equiv U|\equiv U \xleftrightarrow{sk} S$
$g_4.$ $S|\equiv U \xleftrightarrow{sk} S$

(4) Initiative premises

$p_1.$ $U|\equiv \#u$
$p_2.$ $S|\equiv \#v$
$p_3.$ $U|\equiv U \overset{K}{\leftrightarrow} S$
$p_4.$ $S|\equiv U \overset{K}{\leftrightarrow} S$
$p_5.$ $U|\equiv S \Rightarrow (U \xleftrightarrow{sk} S)$
$p_6.$ $S|\equiv U \Rightarrow (U \xleftrightarrow{sk} S)$

(5) Our proposed scheme analysis

$a_1.$ Since p_3 and $U \lhd (U \overset{sk}{\leftrightarrow} S, \{U \overset{K}{\leftrightarrow} S\}_u)_{U\overset{K}{\leftrightarrow}S}$, we apply the message-meaning rule to obtain: $U| \equiv S| \sim (U \overset{sk}{\leftrightarrow} S, \{U \overset{K}{\leftrightarrow} S\}_u)$.

$a_2.$ Since p_1 and a_1, we apply the fresh conjuncatenation rule and nonce-verification rule to obtain: $U| \equiv S| \equiv (U \overset{sk}{\leftrightarrow} S, \{U \overset{K}{\leftrightarrow} S\}_u)$.

$g_1.$ Since a_2 and p_3, we apply the belief rule to obtain: $U| \equiv S| \equiv U \overset{sk}{\leftrightarrow} S$.

$g_2.$ Since p_5 and g_1, we apply the jurisdiction rule to obtain: $U| \equiv U \overset{sk}{\leftrightarrow} S$.

$g_3.$ Since p_4 and $S \lhd (U \overset{sk}{\leftrightarrow} S, \{U \overset{K}{\leftrightarrow} S\}_v)_{U\overset{K}{\leftrightarrow}S}$, we apply the message-meaning rule to obtain: $S| \equiv U| \sim (U \xleftrightarrow{sk} S, \{U \overset{K}{\leftrightarrow} S\}_v)$.

$g_4.$ Since p_2 and a_3, we apply the belief rule to obtain: $S| \equiv U| \equiv (U \xleftrightarrow{sk} S, \{U \overset{K}{\leftrightarrow} S\}_v)$.

$g_3.$ Since a_4 and p_4, we apply the belief rule to obtain: $S| \equiv U| \equiv U \xleftrightarrow{sk} S$.

$g_4.$ Since g_3 and p_6, we apply the jurisdiction rule to obtain: $S| \equiv U \xleftrightarrow{sk} S$.

As a result, our proposed scheme is truly capable of achieving the goals.

Resisting the outsider attack

Suppose an outsider adversary $\mathcal{A}$ extracts all of the information $\{IM_1,\ IM_2, h_1(\cdot),\ h_2(\cdot),\ f,\ H(\cdot)\}$ from an owned smart card by using a side channel attack [37]; however, he/she cannot obtain of the secret information of S. Although $\mathcal{A}$ can compute $h_1(k_u) = IM_1 \oplus K$, the value k_u is a random number that is selected by S and is unique to the user; therefore, $\mathcal{A}$ does not know this value and our proposed scheme can resist the outsider attack.

Resisting the impersonation attack

Suppose $\mathcal{A}$ intercepts all of the messages $\{IM_1, IM_2, R_1, R_2, IM_3,\ Auth_s,\ Auth_u\}$ that are transmitted over a public channel between U and S; however, $\mathcal{A}$ cannot generate the legal login request message $\{IM_1, IM_2, R_1, R_2\}$, where $IM_1 = K \oplus h_1(k_u)$, $IM_2 = h_1(k_u||k_s) \oplus h_1(k_s)$, $R_1 = K \oplus ID$, $R_2 = ID \oplus T_u(K)$, and $K = h_1(ID||h_1(PW||\ H(BIO)))$, because the value k_u is a random number that is selected by S and is unique to user, and u is a random number that is generated by U. Furthermore, $\mathcal{A}$ cannot generate the login response message $\{Auth_s, IM_3\}$ without the random number v. Our proposed scheme can therefore resist the impersonation attack.

Table 5 Security attributes comparison

Security attributes/Schemes	Ours	[26]	[28]	[29]	[30]	[31]	[32]	[34]	[35]	[47]
User anonymity	√	×	√	√	√	√	×	√	√	×
Mutual authentication	√	√	√	√	√	√	√	√	√	√
Stolen smart card attack	√	√	×	×	√	√	√	√	√	√
Perfect forward secrecy	√	×	×	×	×	×	×	×	×	×
Session key security	√	×	×	×	√	√	×	×	×	×
Insider attack	√	×	√	√	√	×	√	×	√	√
Impersonation attack	√	×	×	×	√	×	×	√	√	√
Denial of service attack	√	×	×	×	×	×	×	×	√	×
Off-line password guessing attack	√	×	×	×	√	√	√	√	√	√
No time synchronization	√	×	×	×	×	×	√	√	×	√

Resisting the smart card stolen attack

Suppose that $\mathcal{A}$ steals the smart card of a legal user U; then, he/she can extract all of the information $\{IM_1, IM_2, h_1(\cdot), h_2(\cdot), f, H(\cdot)\}$ from the smart card by using the side channel attack [37]. $\mathcal{A}$, however, cannot obtain any of the secret information of U. The password PW is protected by the elements ID and BIO that $\mathcal{A}$ does not know. Our proposed scheme can therefore resist the smart card stolen attack.

User anonymity

Our proposed scheme can preserve the anonymity of an identity since ID cannot be derived from R_1 without the knowledge of K; furthermore, K cannot be derived from IM_1 without the random number k_u because of the one-way hash function. Our proposed scheme therefore provides user anonymity.

Perfect forward secrecy

In our proposed scheme, the shared session key $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$ is related to the value K and the two random numbers u and v. The value K is hidden by the random number k_u and is computed by using the user's password PW and the biometrics BIO that, with the exception of U, nobody knows; moreover, two random numbers are chosen by U and S. If the adversary $\mathcal{A}$ wants to compute u and v from $T_u(K)$ and $T_v(K)$, he/she must first obtain the value K and will face the CMDLP. Our proposed scheme can therefore provide perfect forward secrecy.

Session key security

Suppose that $\mathcal{A}$ intercepts all of the messages $\{IM_1, IM_2, R_1, R_2, IM_3, Auth_s, Auth_u\}$ that are transmitted across a public channel between the user U and the server S, and steals the smart card of U, and then extracts

Table 6 Performance comparison

Schemes	Registration	Authentication and key agreement	Total	Time(ms)	Message exchange
Our proposed	$7T_H$	$14T_H$+$4T_{CCM}$	$21T_H$+$4T_{CCM}$	133.0	3
Guo et al. [26]	$1T_H$+$1T_E$+$1T_{CCM}$	$4T_H$+$5T_E$+$6T_{CCM}$	$5T_H$+$6T_E$+$7T_{CCM}$	229.1	2
Lin et al. [28]	$1T_H$+$1T_E$+$1T_{CCM}$	$4T_H$+$5T_E$+$6T_{CCM}$	$5T_H$+$6T_E$+$7T_{CCM}$	229.1	2
Jiang et al. [29]	$1T_H$+$1T_E$+$1T_{CCM}$	$3T_H$+$3T_E$+$5T_{CCM}$	$4T_H$+$4T_E$+$7T_{CCM}$	228.0	2
Lee et al. [30]	$4T_H$	$15T_H$+$4T_{CCM}$	$19T_H$+$4T_{CCM}$	132.6	2
Li et al. [31]	$5T_H$	$18T_H$+$4T_{CCM}$	$23T_H$+$4T_{CCM}$	133.6	3
Lu et al. [32]	$5T_H$	$13T_H$+$4T_{CCM}$	$18T_H$+$4T_{CCM}$	132.4	3
Li et al. [34]	$3T_H$	$11T_H$+$6T_{CCM}$	$14T_H$+$6T_{CCM}$	196.0	3
Lee et al. [35]	$4T_H$	$12T_H$+$6T_{CCM}$	$16T_H$+$6T_{CCM}$	196.4	3
Lee et al. [47]	$2T_H$	$11T_H$+$6T_{CCM}$	$13T_H$+$6T_{CCM}$	195.8	3

the all of the information $\{IM_1, IM_2, h_1(\cdot), h_2(\cdot), f, H(\cdot)\}$; however, $\mathcal{A}$ cannot compute the session key $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$. To compute $T_u(K)$ and $T_v(K)$ from R_2 and IM_3, U's identity ID is needed. To retrieve ID from R_1, $\mathcal{A}$ needs to know the PW and $H(BIO)$. Since only U can imprint his/her biometrics BIO at the sensor, an adversary $\mathcal{A}$ cannot attain U's ID and PW. Alternatively, anyone, with the exception of U and S, is required to compute $T_{uv}(K)$ from $T_u(K)$ and $T_v(K)$ if he/she wants to obtain the session key, then he/she will be required to solve the CMDHP. Our proposed scheme can therefore provide session key security.

Functionality and performance comparison analysis

In this section, we evaluate the functionality comparisons between our proposed scheme and the other related schemes of [26, 28–32, 34, 35, 47] are given. Table 5 shows that our proposed scheme is more secure and robust than the other related schemes and that it achieves a greater number of functionality features. For the performance comparison, the definitions of T_{CCM}, T_E, and T_H are the performance times of a Chebyshev chaotic map operation, a symmetric encryption/decryption operation, and a hash function, respectively; Recently, Xue and Hong [25] estimated the running time of different cryptographic operations whereby T_{CCM} is nearly 32.2 ms on average, T_E is nearly 0.45 ms on average, and T_H is below 0.2 ms on average in the environment (CPU:3.2 GHz, RAM: 3.0 G). Table 6 shows that our proposed scheme performs two further hash functions than Lu et al.'s scheme to accomplish mutual authentication and key agreement; however, a very brief amount of time consumed by this operation.

Conclusion

In 2015, Lu et al. proposed an enhanced TMIS scheme based on Li et al.'s scheme and demonstrated its resistance to the typical attack types; however, we found that Lu et al.'s scheme is not secure against the outsider attack, the impersonation attack, and the replay attack, among others. In this paper, to solve these security vulnerabilities, we propose an improved authentication scheme for TMISs that maintains the merits of Lu et al.'s scheme and is more secure; furthermore, the computational cost of our proposed scheme is lower than that of Lu et al.'s scheme. The performed security analysis confirms that our proposed scheme rectifies the weaknesses of Lu et al.'s scheme.

Acknowledgements This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No.R0126-15-1111, The Development of Risk-based Authentication·Access Control Platform and Compliance Technique for Cloud Security)

References

1. Lambrinoudakis, C., and Gritzalis, S., Managing medical and insurance information through a smart-card-based information system. *J. Med. Syst* 24(4):213–234, 2000.
2. Xie, Q., Hu, B., Dong, N., and Wong, D.S., Anonymous three-party password-authenticated key exchange scheme for telecare medical information systems. *PLoS ONE* 9(7):e102747, 2014. doi:10.1371/journal.pone.0102747.
3. Lamport, L., Password authentication with insecure communication. *Commun. ACM.* 24(11):770–772, 1981.
4. Son, K., Han, D., and Won, D., A privacy-protecting authentication scheme for roaming services with smart cards. *IEICE trans.* 95(5):1819–1821, 2012.
5. Jeon, W., Kim, J., Nam, J., Lee, Y., and Won, D., An enhanced secure authentication scheme with anonymity for wireless environments. *IEICE trans.* 95(7):2505–2508, 2012.
6. Kim, J., Lee, D., Jeon, W., Lee, Y., and Won, D., Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks. *Sens.* 14(4):6443–6462, 2014.
7. Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J., and Won, D., Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sens.* 14(6):10081–10106, 2014.
8. Choi, Y., Nam, J., Lee, D., Kim, J., Jung, J., and Won, D., Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics. *Sci. Wor. J.*, 2014. doi:10.1155/2014/281305. Article ID 281305, 15p, 2015.
9. Lu, Y.R., Li, L.X., Peng, H.P., Yang, X., and Yang, Y.X., A lightweight ID based authentication and key agreement protocol for multi-server architecture. *Int. J. Distrib. Sens. N.*, 2015. doi:10.1155/2015/635890. Article ID 635890, 9p, 2015.
10. Lu, Y.R., Li, L.X., Peng, H.P., and Yang, Y.X., An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. *J. Med. Syst* 39(3):1–8, 2015.
11. Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, M.K., and Chaturvedi, A., Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. *J. Med. Syst.* 38(5):1-11, 2014. doi:10.1007/s10916-014-0041-1.
12. Arshad, H., and Nikooghadam, M., Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems. *J. Med. Syst.* 38(12):1-12, 2014. doi:10.1007/s10916-014-0136-8.
13. Arshad, H., Teymoori, V., Nikooghadam, M., and Abbassi, H., On the security of a two-factor authentication and key agreement scheme for telecare medicine information systems. *J. Med. Syst.* 39(7):1-10, 2015. doi:10.1007/s10916-015-0259-6.
14. Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C., and Chung, Y., A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1529–1535, 2012.
15. He, D.B., Chen, J.H., and Zhang, R., A More Secure Authentication Scheme for Telecare Medicine Information Systems. *J. Med. Syst.* 36(3):1989–1995, 2012.

16. Wei, J., Hu, X., and Liu, W., An improved authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3597–3604, 2012.
17. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3833–3838, 2012.
18. Özkaynak, F., and Yavuz, Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dyn.* 74(3):551–557, 2013.
19. Khan, M., Shah, T., Mahmood, H., and Gondal, M.A., An efficient method for the construction of block cipher with multichaotic systems. *Nonlinear Dyn.* 71:489–492, 2013.
20. Mishra, D., Srinivas, J., and Mukhopadhyay, S., A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information. *J. Med. Syst.* 38(10):1-10, 2014. doi:10.1007/s10916-014-0120-3.
21. Gao, B., Shi, Y.F., Yang, C.L., Li, L.X., Wang, L.C., and Yang, Y.X. *STP-LWE: A variant of learning with error for a flexible encryption*. Vol. 341490, pp. 1-7, 2014. Article ID 2014.
22. Xiao, D., Liao, X.F., and Wong, K.W., An efficient entire chaos based scheme for deniable authentication. *Chaos Soliton Fract.* 23:1327–1331, 2005.
23. Tseng, H., Jan, R., and Yang, W., A chaotic maps-based key agreement protocol that preserves user anonymity. *IEEE Int. Conf. Commun.* 1-6, 2009. ICC09.
24. Niu, Y., and Wang, X., An anonymous key agreement protocol based on chaotic maps. *Commun. Nonlinear Sci. Numer. Simul.* 16(4):1986–1992, 2011.
25. Xue, K., and Hong, P., Security improvement on an anonymous key agreement protocol based on chaotic maps. *Commun. Nonlinear Sci. Numer. Simul.* 17(7):2969–2977, 2012.
26. Guo, C., and Chang, C., Chaotic maps-based passwordauthenticated key agreement using smart cards. *Commun. Nonlinear Sci. Numer. Simul.* 18(6):1433–1440, 2013.
27. Hao, X., Wang, J., Yang, Q., Yan, X., and Li, P., A chaotic map-based authentication scheme for telecare medicine information systems. *J. Med. Syst.* 37(2):9919, 2013.
28. Lin, H.Y., Improved chaotic maps-based password-authenticated key agreement using smart cards. *Commun. Nonlinear Sci. Numer, Simul.*, 2014. doi:10.1016/j.cnsns.2014.05.027.
29. Jiang, Q., Ma, J., Lu, X., and Tian, Y., Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. *J. Med. Syst.* 38(2):12, 2014.
30. Lee, T.F., An efficient chaotic map-based authentication and key agreement scheme using smart cards for telecare medicine information systems. *J. Med. Syst.* 37(6):9985, 2013.
31. Li, C.T., Lee, C.C., and Weng, C.Y., A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. *J. Med. Syst.* 38(9):1–11, 2014.
32. Lu, Y.R., Li, L.X., Peng, H.P., Xie, D., and Yang, Y.X., Robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. *J. Med. Syst.* 39(6):1–10, 2015.
33. Stallings, W. *Cryptography and Network Security: Principles and Practices. 3rd edn*: Prentice Hall, 2003.
34. Li, C.T., Lee, C.C., and Weng, C.Y., An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments. *Nonlinear Dyn.* 74:1133–1143, 2013.
35. Lee, C.C., and Hsu, C.W., A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. *Nonlinear Dyn.* 71:201–211, 2013.
36. Zhao, D.W., Peng, H.P., Wang, C., and Yang, Y.X., A secret sharing scheme with a short share realizing the (t, n) threshold and the adversary structure. *Comput. Math. Appl.* 64(4):611–615, 2012.
37. Messerges, T.S., Dabbish, E.A., and Sloan, R.H., Examining smartcard security under the threat of power analysis attacks. *IEEE Trans. Comput.* 51(5):541–552, 2002.
38. Bergamo, P., Arco, P., Santis, A., and Kocarev, L., Security of public key cryptosystems based on Chebyshev polynomials. *IEEE. Trans. Circ. Syst.* I(52):1382–1393, 2005.
39. Lumini, A., and Nanni, L., An improved biohashing for human authentication. *Pattern Recogn.* 40(3):1057–1065, 2007.
40. Das, A.K., and Goswami, A., An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. *J. Med. Syst* 38(6):27, 2014.
41. Stallings, W. *Cryptography and network security:principles and practices, 3th edition*: Prentice Hall, 2003.
42. Mishra, D., Das, A.K., and Mukhopadhyay, S., A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. *Expert Sys. Appl.* 41(18):8129–8143, 2014.
43. Das, A.K., Paul, N.R., and Tripathy, L., Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem. *Information Sci.* 209:80–92, 2012.
44. Das, A.K., A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications. *Networking Sci.* 2(1-2):12–27, 2013.
45. Burrow, M., Abadi, M., and Needham, R., A logic of authentication. ACM Trans. *Compu. Syst.* 8:18–36, 1990.
46. Zhao, D.W., Peng, H.P., Li, L.X., Yang, Y.X., and A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wireless Pers. Commun.* 78:247–269, 2013.
47. Lee, C.C., Lou, D.C., Li, C.T., and Hsu, C.W., An extended chaotic maps-based protocol with key agreement for multiserver environments. *Nonlinear Dyn.* 76(1):853–866, 2014.