ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/273833237

# Efficient biometric authenticated key agreements based on extended chaotic maps for telecare medicine information systems

**Article** *in* Journal of Medical Systems · May 2015

DOI: 10.1007/s10916-015-0240-4 · Source: PubMed

CITATIONS
4

READS
30

**3 authors:**

Der-Chyuan Lou
Chang Gung University
**118** PUBLICATIONS **1,212** CITATIONS
SEE PROFILE

Tian-Fu Lee
Tzu Chi University
**28** PUBLICATIONS **381** CITATIONS
SEE PROFILE

Tsung-Hung Lin
National Chin-Yi University of Technology
**21** PUBLICATIONS **175** CITATIONS
SEE PROFILE

All in-text references underlined in blue are linked to publications on ResearchGate, letting you access and read them immediately.

Available from: Der-Chyuan Lou
Retrieved on: 20 October 2016

J Med Syst (2015) 39:58
DOI 10.1007/s10916-015-0240-4

SYSTEMS-LEVEL QUALITY IMPROVEMENT

# Efficient biometric authenticated key agreements based on extended chaotic maps for telecare medicine information systems

**Der-Chyuan Lou**[1] · **Tian-Fu Lee**[2] · **Tsung-Hung Lin**[3]

Received: 23 November 2014 / Accepted: 9 March 2015
© Springer Science+Business Media New York 2015

**Abstract** Authenticated key agreements for telecare medicine information systems provide patients, doctors, nurses and health visitors with accessing medical information systems and getting remote services efficiently and conveniently through an open network. In order to have higher security, many authenticated key agreement schemes appended biometric keys to realize identification except for using passwords and smartcards. Due to too many transmissions and computational costs, these authenticated key agreement schemes are inefficient in communication and computation. This investigation develops two secure and efficient authenticated key agreement schemes for telecare medicine information systems by using biometric key and extended chaotic maps. One scheme is synchronization-based, while the other nonce-based. Compared to related approaches, the proposed schemes not only retain the same security properties with previous schemes, but also provide users with privacy protection and have fewer transmissions and lower computational cost.

**Keywords** Telecare medicine information system · Anonymity · Authentication · Biometric · Chaotic maps · Key agreement · Privacy protection

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

Der-Chyuan Lou and Tian-Fu Lee contributed equally to this work.

✉ Tian-Fu Lee
jackytflee@mail.tcu.edu.tw; tflee@ismail.csie.ncku.edu.tw

Der-Chyuan Lou
dclouprof@gmail.com

Tsung-Hung Lin
duke@ncut.edu.tw

[1] Department of Computer Science and Information Engineering, Chang Gung University, No. 259, Wenhua 1st Rd., Guishan Dist., Taoyuan City 33302, Taiwan, Republic of China

[2] Department of Medical Informatics, Tzu Chi University, No. 701, Zhongyang Road, Sec. 3, Hualien 97004, Taiwan, Republic of China

[3] Department of Computer Science and Information Engineering, National Chin-Yi University of Technology, No.57, Sec. 2, Zhongshan Rd., Taiping Dist., Taichung 41170, Taiwan, Republic of China

## Introduction

Authenticated key agreements for telecare medicine information systems (TMIS) enable system users, including patients at home and doctors at clinical centers or home health-care (HHC) agency, to establish secure and authenticated channels with an authentication server [1, 2]. Then these users can efficiently and conveniently access remote telemedicine services through an open network, as shown in Fig. 1. For example, home care's patients with chronic diseases can record personal physiological signals at any time. These electronic health records can be transmitted to the database server through TMIS. Then doctors at clinical centers and HHC agency rapidly obtain adequate medical information and clearly understand the situations of patients' home care by using this information platform. It has great help for reducing the probability of recurrence. Therefore, an authenticated key agreement scheme for TMIS is required to provide efficiency in communication and computation, entity authentication, data confidentiality and privacy protection.

An authenticated key agreements scheme for TMIS comprises initialization, registration, login and authentication, and password change phases. First, in the initialization phase, a registration center sets up the authentication system and issues secret information to authentication servers via a secure channel. Subsequently, in registration phase, a user registers his/her

Published online: 22 March 2015

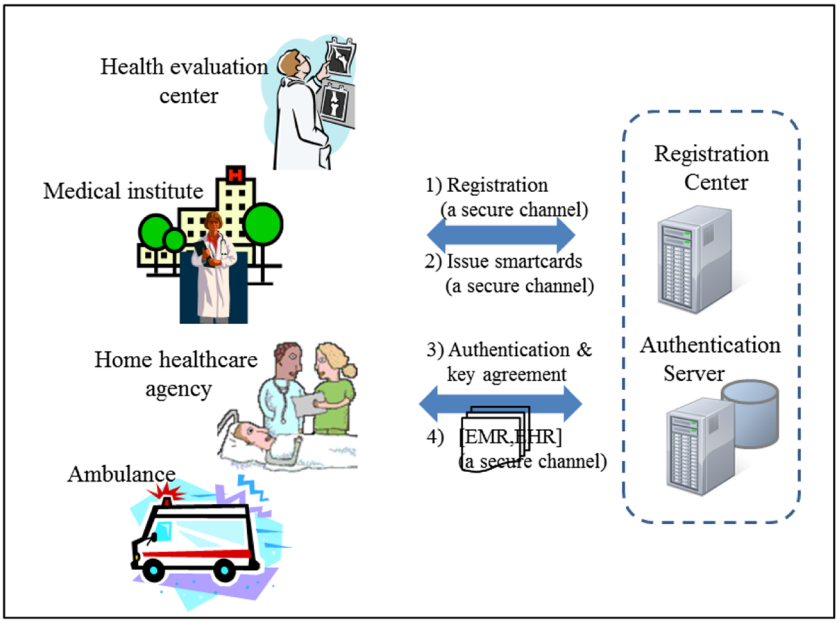


**Fig. 1** Users efficiently and conveniently access remote telemedicine services by using an authenticated key agreement scheme for TMIS

identifier, password and secret key to the registration center. The registration center also generates secret information, keeps this information in a smartcard, and issues the smartcard to the user via a secure channel. Then, the login and the authentication phase provides a legitimate user with login request services, and provides mutual authentication with the authentication server and a legitimate user, respectively. Finally, the password change phase provides that the smartcard identifies the user and updates the user's new password.

Traditional authenticated key agreement scheme use a long-term secret stored in a smartcard and a weak password for user authentication [3–10]. In order to provide more security properties, many researches employed biometric key, which are based on physiological and behavioral characteristics of persons such as fingerprints, retinas, irises, faces, hand geometry, and palmprints, etc., to develop remote user authentication schemes since biometric keys are not easily lost or forgotten; biometric keys are extremely hard to copy, share, forge or distribute; and biometric keys are not easy to be guessed and break [11–15]. Therefore, authentication schemes which realize identification using passwords, smartcards and biometric keys may increase security, and thus are suitable for TMIS. Recently, Li and Hwang [13] in 2010 proposed an efficient biometric-based remote authentication scheme using smart cards. Das [14] in 2011 proposed an improvement biometric-based scheme in order to overcome the security flaws in the Li and Hwang's scheme. Later, Lee and Hsu [15] in 2013 showed that the Das's scheme cannot resist the privileged insider attack and the off-line password guessing attack, and cannot provide users with anonymity. Lee and Hsu also develop a secure biometric authenticated key agreement scheme which used extended chaotic maps and synchronized clocks. In 2013, Tan [16] proposed an efficient biometrics-based authentication scheme for the TMIS and claimed their scheme could withstand various attacks. Later, Yan et al. [17] stated out that Tan's scheme is vulnerable to the Denial-of-Service attack, and also proposed an improved scheme as an alternative. In addition, Awasthi and Srivastava [18] in 2013 developed an efficient biometric remote user authentication scheme for TMIS by using chaotic one-way hash function and bitwise XOR operations. However, Das and Goswami [19] in 2014 showed that the Awasthi- Srivastava scheme has several drawbacks, and proposed a novel and secure biometric-based remote user authentication scheme to withstand the security flaw found in the Awasthi-Srivastava's scheme. Li et al. [20] in 2014 also stated that the Awasthi-Srivastava scheme has several weaknesses in security, and developed biometric authentication scheme for TMIS by using modular exponential operations. It recently had been showed that cryptography using chaotic map operations is more efficient than cryptography using modular exponential computations and scalar multiplications on an elliptic curve [21–28]. Thus, these schemes in [15, 18, 19] using extended chaotic maps was more efficient than related approaches using modular exponential computations and scalar multiplications on an elliptic curve.

In authentication schemes, two methods are generally used for guaranteeing the freshness of messages and preventing replaying attacks. One is based on clock-synchronized technique and called synchronization-based, while the other uses nonces and challenge/response technique, and is called nonce-based. In synchronization-based authentication schemes, the communicating messages are permitted to contain the validating timestamps so that participants easily can provide authentication and message freshness by using one transmitted

message. Synchronization-based authentication schemes thus require fewer communicating messages than nonce-based authentication schemes. But, constructing synchronized clocks in a network environment is a complicated work [29–32]. Although the Lee and Hsu's biometric authenticated key agreement scheme is developed by using synchronized clocks, their scheme is still inefficient in communication due to the requirement of too many messages in transmission.

This investigation presents two secure and efficient biometric authenticated key agreement schemes for TMIS, which are one synchronization-based scheme and one nonce-based scheme. The proposed schemes are developed by using extended chaotic maps and rescheduling the communicating messages such that the participants can negotiate their common session key in early steps. Thus, the proposed schemes not only retain the security properties of previous schemes, but have fewer messages in transmission and lower computational cost.

The remainder of this investigation is organized as follows. The next section defines the notations and definitions used in this paper. The subsequent section reviews the biometric authenticated key agreement scheme of Lee and Hsu. The section entitled, "Proposed biometric authenticated key agreement schemes for TMIS", presents the proposed biometric synchronization-based and nonce-based authenticated key agreement schemes using extended chaotic maps for TMIS. The security and performance analyses are described in "Security analyses" and "Performance analyses". The final section draws conclusions.

## Preliminaries

This section first lists notations and definitions used in this paper, and then briefly reviews the biometric-based authenticated key agreement scheme of Lee and Hsu [15]. Assume that $R_i$ is a registration center, $C_i$ is a user and $S_i$ is a remote authentication server. Table 1 lists the notations used throughout this work.

**Table 1** Notation

| | |
|---|---|
| $ID_i$ | The identity of $C_i$ |
| $PW_i$ | The password shared between $C_i$ and $S_i$ |
| $B_i$ | The biometric template of $C_i$ |
| $p$ | A a large prime number |
| $X_S$ | A random integer chosen by $R_i$ |
| $s$ | A random number chosen by $R_i$ |
| $SPUB$ | The public key of $R_i$, where $SPUB \equiv T_{X_S}(s) \bmod p$ |
| $R_C$, $R_S$ | Two random integers selected by $C_i$ and $S_i$, respectively |
| $t_i$, $t'$ | The time-stamp for $i$=1, 2, 3 |
| $\Delta t$ | The predetermined legal time interval of transmission delay |
| $h(.)$ | A secure one-way hash function |
| $\oplus$ | The exclusive-or (XOR) operation |
| $A \rightarrow B : M$ | $A$ sends message $M$ to $B$ through a common channel |
| $M_1 \| M_2$ | Message $M_1$ concatenates to message $M_2$. |

### Definition

(1) Chebyshev Chaotic Maps [15, 21, 22]: The Chebyshev polynomial $T_n(x)$ is a polynomial in $x$ of degree $n$, defined by the following relation:

$T_n(x)=\cos n\theta$, where $x=\cos\theta$.

The recurrence relation of $T_n(x)$ is defined as:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x),$$

for any $n \geq 2$, with $T_0(x)=1$ and $T_1(x)=x$.

The Chebyshev polynomial satisfies the semi-group property and thus satisfies:

$$T_r(T_s(x)) = T_{sr}(x) = T_s(T_r(x)),$$

for $s,r \in Z^+$.

The Chebyshev polynomial also provides chaotic property: When $n > 1$, Chebyshev polynomial map $T_n:[-1,1] \rightarrow [-1,1]$ of degree $n$ is a chaotic map with its invariant density

$$f^*(x) = 1/\left(\pi\sqrt{1-x^2}\right),$$

for Lyaounov exponent $\ln n > 0$.

Zhang [33] in 2008 proved that the semi-group property and the commutative under composition still holds for the enhanced Chebyshev polynomials on interval $(-\infty,+\infty)$. That is,

$$T_n(x) \equiv (2xT_{n-1}(x) - T_{n-2}(x)) \bmod p,$$

where $n \geq 2$, $x \in (-\infty,+\infty)$ and $p$ is a large prime number. Then,

$$T_{rs}(x) \equiv T_r(T_s(x)) \equiv T_s(T_r(x)) \bmod p$$

holds.

The enhanced Chebyshev polynomials have the extended chaotic maps-based discrete logarithm and computational Diffie-Hellman problems [15, 33], which are assumed to be hard to solve within polynomial time, and described as follows.

(2) Extended Chaotic Maps-Based Discrete Logarithm Problem (DLP): Given $y$, $x$ and $p$, finding the integer $r$ such that $y=T_r(x) \bmod p$ is computationally infeasible.

(3) Extended Chaotic Maps-Based Computational Diffie-Hellman Problem (CDHP): Given $T_r(x)$, $T_s(x)$, $T(\cdot)$, $x$ and $p$, where $r$, $s \geq 2$, $x \in (-\infty, +\infty)$ and $p$ is a large prime number, calculating

$$T_{rs}(x) \equiv T_r(T_s(x)) \equiv T_s(T_r(x)) \bmod p$$

is computationally infeasible.

## Review of the authenticated key agreement scheme of Lee and Hsu

Lee and Hsu [15] in 2013 employed biometric authentication and extended chaotic maps to develop an authenticated key agreement scheme, which consists of initialization phase, registration phase, login and authentication phase, and password change phase. First, in the initialization phase, a registration center generates necessary random numbers $s$, a public information $SPUB$, and the master secret key $X_S$. Next, in registration phase, a user registers his/her password $PW_i$, identity $ID_i$, random number $N$ and personal biometric $B_i$ to the registration center. The registration center then computes secret information from the user's $PW_i$, $ID_i$ and $B_i$, and embeds this secret information in the user's smart card and sends it to the user via a secure channel. Afterwards, a legitimate user inserts his/her smartcard into the card reader, inputs his/her $B_i$ and $PW_i$, and sends out a service request. If the authentication server successfully verifies the request messages form the legitimate user, then computes and sends out messages for authentication and key agreement. Next, if the user successfully verifies the responses form the server, then computes and sends out messages for key agreement. Finally, the user and the server can negotiate a common session key and construct a secure and authenticated channel by using this session key. The authenticated key agreement scheme of Lee and Hsu works as follows.

### Initialization phase

(1) The registration center $R_i$ randomly selects $s$ and $X_S$.
(2) $R_i$ computes $SPUB \equiv T_{X_S}(s) \bmod p$.
(3) $R_i$ keeps the master secret key $X_S$.

### Registration phase

In the registration phase, the remote user $C_i$ performs the following steps to register and become a new legal user in the system.

(1) The user $C_i$ inputs his/her password $PW_i$, the identity $ID_i$, generates a random number $N$, and his/her personal biometric $B_i$. $C_i$ then computes $f_i = h(B_i)$ and sends $\{ID_i, f_i, h(PW_i||B_i||N)\}$ to $R_i$ via a secure channel.
(2) The registration center $R_i$ computes:
$P_i = h(ID_i||X_S)$, $r_i = h(PW_i||B_i||N) \oplus f_i$ and $e_i = P_i \oplus r_i$.
Then $R_i$ embeds $(ID_i, h(\cdot), e_i, s, SPUB, p)$ in the user's smart card and sends it to $C_i$ via a secure channel.
(3) On receiving the smart card, $C_i$ computes $BPW = B_i \oplus h(PW_i)$ and inserts $N$ and $BPW$ into the smart card.

### Login and authentication phase

The login and authentication phase provides a legal user $C_i$ and the server $S_i$ with realizing mutual authentication by performing the following steps when $C_i$ accesses $S_i$:

Step 1. $C_i \rightarrow S_i$: $m_1 = \{NID_i, M_1, \alpha, t_1\}$

(1) $C_i$ inserts his/her smart card into the card reader and inputs his/her biometric template $B_i$ and password $PW_i$.
(2) The smart card computes $B_i' = BPW \oplus h(PW_i)$ and verifies $B_i' = ? B_i$. If unsuccessful, the smart card rejects the request.
(3) The smart card generates a random integer $R_C$ and computes:

$$f_i = h(B_i), \quad r_i' = h\left(PW_i \middle|\middle| B_i \middle|\middle| N\right) \oplus f_i, \quad P_i' = e_i \oplus r',$$

$M_1 = T_{R_C}(s) \bmod p$, $M_2 = T_{R_C}(SPUB) \bmod p$, $NID_i = ID_i \oplus h(M_1||M_2)$ and $\alpha = h(ID_i||NID_i||P_i'||M_1||M_2||t_1)$, where $t_1$ is the current timestamp. $C_i$ then sends $m_1 = \{NID_i, M_1, \alpha, t_1\}$ to $S_i$.

Step 2. $S_i \rightarrow C_i$: $m_2 = \{M_3, \beta, t_2\}$

(1) $S_i$ verifies the validity of $t_1$ by checking whether $t' - t_1 \leq \Delta t$ holds or not, where $t'$ is the current timestamp and $\Delta t$ denotes the predetermined legal time interval of transmission delay. If unsuccessful, $S_i$ rejects this service request.
(2) $S_i$ computes $M_2' = T_{X_S}(M_1) \bmod p$, $ID_i' = NID_i \oplus h(M_1||M_2')$ and checks the validity of $ID_i'$.
(3) $S_i$ computes $P'' = h(ID_i'||X_S)$ and $a' = h(ID_i'||NID_i||P_i''||M_1||M_2'||t_1)$.
(4) Then $S_i$ verifies whether $a'$ equals to $\alpha$. If $a' \neq \alpha$, $S_i$ stops the session; Otherwise, $S_i$ randomly chooses $R_S$ and computes $M_3 \equiv T_{R_S}(s) \bmod p$ and $\beta = h(ID_i'||P_i''||M_2'||M_3||t_2)$. Then, $S_i$ sends $m_2 = \{M_3, \beta, t_2\}$ to $C_i$.

Step 3. $C_i \rightarrow S_i$: $m_3 = \{\gamma, t_3\}$

(1) Upon receiving $m_2$, $C_i$ checks $t_2$ by checking whether $t' - t_2 \leq \Delta t$ holds. If unsuccessful, $C_i$ aborts this request.
(2) Otherwise, $C_i$ computes $\beta' = h(ID_i||P_i'||M_2||M_3||t_2)$ and verifies whether $\beta' = ? \beta$. If unsuccessful, $C_i$ stops the session.

(3) Otherwise, $C_i$ computes $M_4 \equiv T_{R_C}(M_3) \equiv T_{R_C R_S}(s) \bmod p$ and $\gamma = h(ID_i || P_i' || M_2 || M_4 || t_3)$. $C_i$ then sends $m_3 = \{\gamma, t_3\}$ to $S_i$.

Step 4.

(1) Finally, upon receiving $m_3$, $S_i$ verifies the validity of $t_3$ by checking whether $t' - t_3 \le \Delta t$ holds or not. If unsuccessful, $S_i$ rejects this service request;
(2) Otherwise, $S_i$ computes $M_4' \equiv T_{R_S}(M_1) \equiv T_{R_S R_C}(s) \bmod p$ and $\gamma = h(ID_i' || P_i'' || M_2' || M_4' || t_3)$ and checks whether $\gamma' = ?\gamma$.
(3) If $\gamma' = \gamma$ holds, $S_i$ accepts this service request. Then $C_i$ and $S_i$ can use the common session key $M_4$ ($= M_4'$) to communicate by using a symmetric cryptosystem.

Since $M_2' \equiv T_{X_S}(M_1) \equiv T_{X_S}(T_{R_C}(s)) \equiv T_{R_C}(T_{X_S}(s)) \equiv T_{R_C}(SPUB) \equiv M_2 \bmod p$, where $SPUB \equiv T_{X_S}(s) \bmod p$, $M_1 \equiv T_{R_C}(s) \bmod p$, $M_2 \equiv T_{R_C}(SPUB) \bmod p$, $S_i$ can successfully authenticate $C_i$. Additionally, since $M_4' \equiv T_{R_C}(M_3) \equiv T_{R_C R_S}(s) \equiv T_{R_S R_C}(s) \equiv T_{R_S}(M_1) \equiv M_4 \bmod p$, where $M_3 \equiv T_{R_S}(s) \bmod p$, thus $C_i$ and $S_i$ can obtain the common session key $M_4$ (or $M_4'$).

### Password change phase

The password change phase provides that the smart card verifies the user's biometric template $B_i$ and old password $PW_i$ and updates the user's new password $PW_i^{new}$ by performing the following steps.

(1) $C_i$ inserts the smart card and inputs $B_i$ and $PW_i$.
(2) The smart card computes $B_i' = BPW \oplus h(PW_i)$ and verifies $B_i = ?B_i'$. If unsuccessful, the smart card rejects the request.
(3) If $C_i$ inputs a new password $PW_i^{new}$.
(4) The smart card computes $f_i = h(B_i)$, $r_i' = h(PW_i || B_i || N) \oplus f_i$, $r_i'' = h(PW_i^{new} || B_i || N) \oplus f_i$, $P_i' = e_i \oplus r_i'$ and $e_i' = P_i' \oplus r_i''$.
(5) Finally, The smart card replaces $e_i$ with $e_i'$.

## Proposed biometric authenticated key agreement schemes for TMIS

This section develops two secure and efficient biometric authenticated key agreement schemes by using extended chaotic maps. One is a synchronization-based (or timestamp-based, TB) authenticated key agreement scheme, while the other is a nonce-based (NB) authenticated key agreement scheme.

The proposed TB and NB authenticated key agreement schemes also consists of three phases, including initialization phase, registration phase, login and authentication phase, and password change phase. The initialization, registration and password change phases of the proposed schemes are similar to those of the Lee and Hsu's scheme, and thus are not described here.

### The proposed TB biometric authenticated key agreement scheme

In the login and authentication phase, a legitimate user inserts his/her smartcard into the card reader, inputs his/her $B_i$ and $PW_i$, and sends out a service request for authentication and key agreement. If the server successfully verifies the request messages form the user, then computes the session key, and sends out messages for authentication and key agreement. Next, if the user successfully verifies the responses form the server, then computes the session key. Thus, the user and the server can negotiate a common session key and construct a secure and authenticated channel in the early step. Figure 2 illustrates the login and authentication phase of the proposed TB scheme, which works as follows.

Step 1. $C_i \rightarrow S_i$: $m_1 = \{NID_i, M_1, \alpha, t_1\}$

(1) $C_i$ inserts his/her smart card into the card reader and inputs his/her biometric template $B_i$ and password $PW_i$.
(2) The smart card computes $B_i' = BPW \oplus h(PW_i)$ and verifies $B_i' = ?B_i$. If unsuccessful, the smart card rejects the request.
(3) The smart card generates a random integer $R_C$ and computes:

$$f_i = h(B_i), \quad r_i' = h\left(PW_i \left|\right| B_i \left|\right| N\right) \oplus f_i, \quad P_i' = e_i \oplus r',$$

$$M_1 = T_{R_C}(s) \bmod p, \quad M_2 = T_{R_C}(SPUB) \bmod p,$$

$NID_i = ID_i \oplus h(M_1 || M_2)$ and $\alpha = h(ID_i || NID_i || P_i' || M_1 || M_2 || t_1)$, where $t_1$ is the current timestamp. $C_i$ sends $m_1 = \{NID_i, M_1, \alpha, t_1\}$ to $S_i$.

Step 2. $S_i \rightarrow C_i$: $m_2 = \{M_3, \beta, t_2\}$

(1) $S_i$ verifies $t_1$ by checking whether $t' - t_1 \le \Delta t$ holds or not, where $t'$ is the current timestamp and. If unsuccessful, $S_i$ rejects this service request.
(2) $S_i$ computes $M_2' = T_{X_S}(M_1) \bmod p$, $ID_i' = NID_i \oplus h(M_1 || M_2')$ and checks the validity of $ID_i'$.
(3) $S_i$ computes $P'' = h(ID_i' || X_S)$ and $a' = h(ID_i' || NID_i || P_i' || M_1 || M_2' || t_1)$.
(4) Then $S_i$ verifies whether $a'$ equals to $\alpha$. If $a' \neq \alpha$, $S_i$ stops the session; Otherwise, $S_i$ accepts $C_i$'s login request, randomly chooses $R_S$ and computes $M_3 \equiv T_{R_S}(s) \bmod p$, $M_4 \equiv T_{R_S}(M_1) \equiv T_{R_C R_S}(s) \bmod p$ and $\beta = h(ID_i' || P_i'' || M_2' || M_3 || M_4 || t_2)$. Then, $S_i$ sends $m_2 = \{M_3, \beta, t_2\}$ to $C_i$.

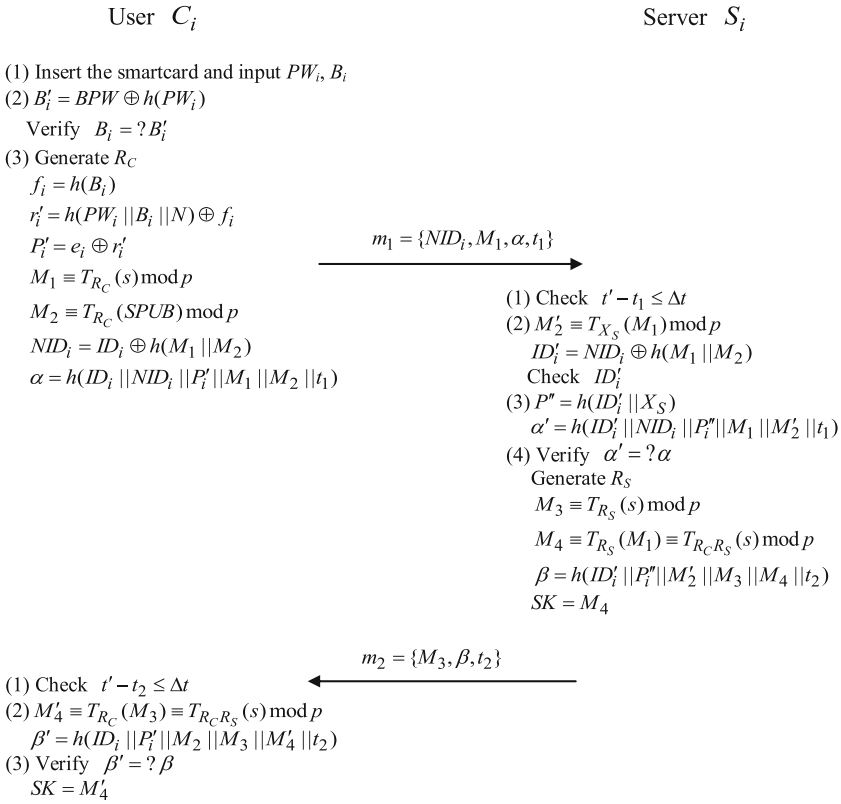


**Fig. 2** Login and authentication phase of the proposed TB scheme

Step 3.

(1) Upon receiving $m_2$, $C_i$ verifies $t_2$ by checking whether $t'-t_2 \le \Delta t$ holds or not. If unsuccessful, $C_i$ aborts this request.
(2) Otherwise, $C_i$ computes $M_4' \equiv T_{R_C}(M_3) \equiv T_{R_C R_S}(s) \bmod p$ and $\beta' = h(ID_i \| P_i' \| M_2 \| M_3 \| M_4' \| t_2)$.
(3) If $C_i$ successfully verifies $\beta' = \beta$, then $C_i$ successfully authenticates $S_i$; Otherwise, $C_i$ aborts this service request. Therefore, $C_i$ and $S_i$ have the common session key $SK = M_4 = M_4'$.

## The proposed NB biometric authenticated key agreement scheme

In the login and authentication phase, a legitimate user inserts his/her smartcard into the card reader, inputs his/her $B_i$ and $PW_i$, and sends out a service request for authentication and key agreement. If the authentication server successfully verifies the request messages form the legitimate user, then computes and sends out messages for authentication and key agreement. Next, if the user successfully verifies the responses form the server, then computes and sends out messages for key agreement. After that, the server can make sure message freshness since nonce-based schemes cannot provide authentication and message freshness by using one transmitted message. Finally, the user and the server negotiate a common session key and construct a secure and authenticated channel by using this session key. Figure 3 illustrates the login and authentication phase of the proposed NB scheme, which works as follows.

Step 1. $C_i \rightarrow S_i$: $m_1 = \{NID_i, M_1\}$

(1) $C_i$ inserts his/her smart card into the card reader and inputs his/her biometric template $B_i$ and password $PW_i$.
(2) The smart card computes $B_i' = BPW \oplus h(PW_i)$ and verifies $B_i' = ? B_i$. If unsuccessful, the smart card rejects the request.
(3) The smart card generates a random integer $R_C$ and computes:

$$f_i = h(B_i), \quad r_i' = h\left(PW_i \middle\| B_i \middle\| N\right) \oplus f_i, \quad P_i' = e_i \oplus r_i',$$

$M_1 = T_{R_C}(s) \bmod p$, $M_2 = T_{R_C}(SPUB) \bmod p$ and $NID_i = ID_i \oplus h(M_1 \| M_2)$. $C_i$ sends $m_1 = \{NID_i, M_1\}$ to $S_i$.

Step 2. $S_i \rightarrow C_i$: $m_2 = \{M_3, \beta\}$

(1) $S_i$ computes $M_2' = T_{X_S}(M_1) \bmod p$, $ID_i' = NID_i \oplus h(M_1 \| M_2')$ and verifies $ID_i'$.
(2) $S_i$ computes $P'' = h(ID_i' \| X_S)$, randomly chooses $R_S$ and computes $M_3 \equiv T_{R_S}(s) \bmod p$, $M_4 \equiv T_{R_C}(M_1) \equiv T_{R_C R_S}(s) \bmod p$ and $\beta = h(ID_i' \| P_i'' \| M_2' \| M_3 \| M_4)$. Then, $S_i$ sends $m_2 = \{M_3, \beta\}$ to $C_i$.

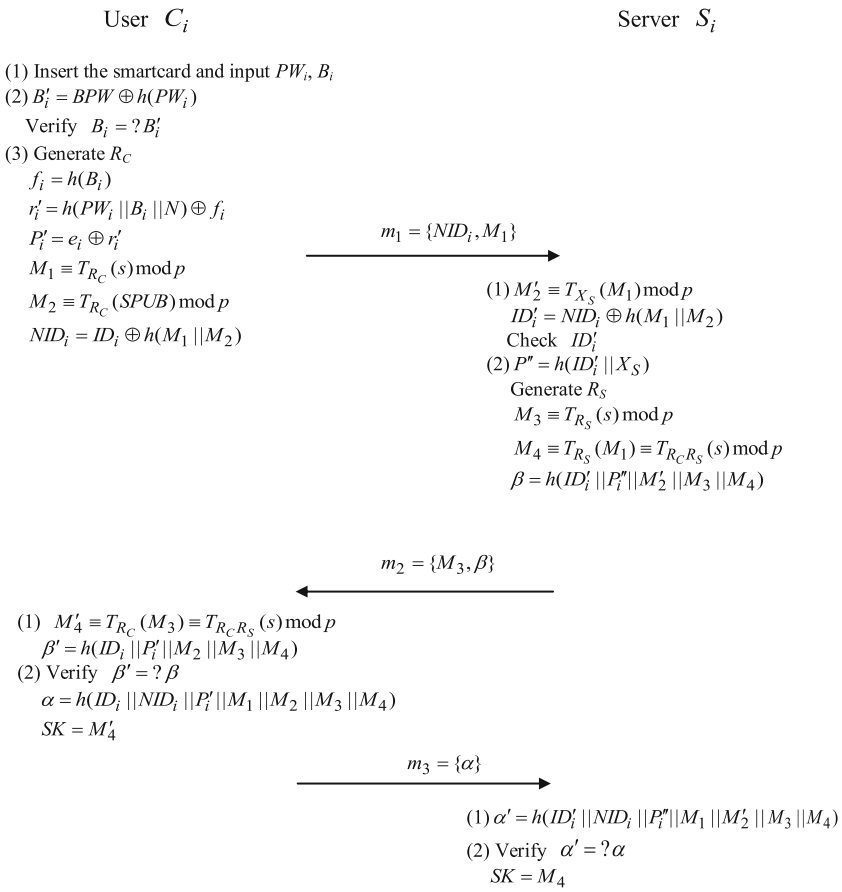


**Fig. 3** Login and authentication phase of the proposed NB scheme

Step 3 $C_i \rightarrow S_i$: $m_3=\{\gamma, t_3\}$

(1) Upon receiving $m_2$, $C_i$ computes $M_4' \equiv T_{R_C}(M_3) \equiv T_{R_C R_S}(s) \bmod p$ and $\beta' = h(ID_i \| P_i' \| M_2 \| M_3 \| M_4')$.
(2) If $C_i$ successfully verifies $\beta' = \beta$, then $C_i$ computes $\alpha = h(ID_i \| NID_i \| P_i' \| M_1 \| M_2 \| M_3 \| M_4')$ and sends $m_3 = \{\alpha\}$ to $S_i$; Otherwise, $C_i$ aborts this request.

Step 4.

(1) Finally, upon receiving $m_3$ form $C_i$, $S_i$ computes $a' = h(ID_i' \| NID_i \| P_i'' \| M_1 \| M_2' \| M_3 \| M_4)$ and checks whether $a' = ?\, \alpha$.
(2) If $a' = \alpha$ holds, $S_i$ successfully authenticates $C_i$ and accepts this login request; Otherwise, $S_i$ rejects this service request. Therefore, $C_i$ and $S_i$ obtain the common session key $SK = M_4 = M_4'$.

## Security analyses

This section analyzes security properties of the proposed authentication schemes, which are session key security and mutual authentication, anonymity of users, perfect forward secrecy, known-key security, and withstand possible attacks, including privileged insider attacks, replay attacks, off-line password guessing attacks, stolen-verifier attacks and lost smart card attacks.

### Security analyses of the proposed TB scheme

(1) Providing mutual authentication: $M_2 \equiv T_{X_S}(M_1) \equiv T_{X_S R_C}(s) \bmod p$ cannot be determined without knowledge of $X_S$ and $R_C$ since no polynomial algorithm has been found to solve the Extended Chaotic Maps-Based DLP and CDHP. Thus, only $C_i$ and $S_i$ can have $ID_i$ and $\alpha$, where $\alpha = h(ID_i \| NID_i \| P_i \| M_1 \| M_2 \| t_1)$, $NID_i = ID_i \oplus h(M_1 \| M_2)$, $P = h(ID_i \| X_S)$, and $S_i$ can authenticate $C_i$ by verifying $t_1$, $ID_i$ and $\alpha$ in Step 2. Similarly, $M_4 \equiv T_{R_C}(M_3) \equiv T_{R_C R_S}(s) \bmod p$ cannot be determined without knowledge of $R_S$ and $R_C$ because of the Extended Chaotic Map-Based DLP and CDHP. Then, $C_i$ can authenticate $S_i$ by verifying $t_2$ and $\beta$ in Step 3, where $\beta = h(ID_i \| P_i \| M_2 \| M_3 \| M_4 \| t_2)$. Therefore, the proposed TB scheme realizes mutual authentication.
(2) Providing session key security: Given $T_{R_C}(x)$, $T_{R_S}(x)$, $T(\cdot)$ and $x$, the session key $SK = T_{R_C}(T_{R_S}(x))$ or $SK = T_{R_S}(T_{R_C}(x))$ is computationally infeasible without knowledge of $R_C$ or $R_S$ since no polynomial algorithm has been found to solve the Extended Chaotic Maps-Based DHP.

Therefore, the session key security of the proposed TB scheme is based on the Extended Chaotic Maps-Based CDHP.

(3) Providing users with anonymity: An attacker tries to derive the user's identity $ID_i$ from the communicating messages between user $C_i$ and server $S_i$. Since the identity $ID_i$ is encrypted by $h(M_1||M_2)$, where $M_2 \equiv T_{R_C}(SPUB) \bmod p$, $M_1 \equiv T_{R_C}(s) \bmod p$ and $SPUB \equiv T_{X_S}(s) \bmod p$, the value of $M_2$ is required to derive the identity $ID_i$. However, the attacker fails to obtain $M_2$ without knowledge of $R_C$ because of the Extended Chaotic Map-Based CDHP. Therefore, the proposed scheme provides users with anonymity.

(4) Providing perfect forward secrecy: The temporary random numbers $R_C$ and $R_S$ are randomly and independently selected among executed authentication schemes. Thus, a compromised password $PW_i$ does not compromise previous session keys $SK(= T_{R_C \cdot R_S}(x) \bmod p)$. Therefore, the proposed scheme provides perfect forward secrecy.

(5) Providing known-key security: The session keys $SK$ $(= T_{R_C \cdot R_S}(x) \bmod p)$ generated in different runs are independent. The random numbers $R_C$ and $R_S$ are randomly selected and independent among executed authentication schemes. Then an adversary cannot derive another session key by using a compromised session key. Thus, the proposed scheme is secure against known-key attacks.

(6) Resisting privileged insider attacks: In the registration phase of the proposed scheme, the remote user $C_i$ sends $h(PW_i||B_i||N)$ to the registration center $R_i$. The privileged insider fails to derive the password $PW_i$ without the knowledge of $B_i$ and $N$. Therefore, the proposed scheme resists the privileged insider attack.

(7) Resisting replay attack: An adversary tries to replay the previous communicating messages containing timestamps $t_1$ and $t_2$. The server $S_i$ will detect a failed login; and the user $C_i$ will detect a failed response, respectively. Thus, the proposed scheme provides the freshness of communicating messages and is secure against replay attacks.

(8) Resisting off-line password guessing attacks: Assume that an adversary can intercept the communicating messages $m_1 = \{NID_i, M_1, \alpha, t_1\}$ and $m_2 = \{M_3, \beta, t_2\}$, and get $e_i$ kept in the smart card. The adversary cannot verify the correctness of the guessing password without the knowledge of $r_i$, $B_i$, $f_i$ and $P_i$ since the password $PW_i$ is protected by $r_i$, $B_i$, $f_i$ and $P_i$, where $e_i = P_i \oplus r_i$, $P_i = h(ID_i||X_S)$ and $r_i = h(PW_i||B_i||N) \oplus f_i$. Additionally, the adversary fails to derive $P_i$ from $\alpha$ and $\beta$, where $\alpha = h(ID_i||NID_i||P_i||M_1||M_2||t_1)$ and $\beta = h(ID_i||P_i||M_2||M_3||M_4||t_2)$, owing to the one-way property of the hash function. Thus, off-line password guessing attacks are unsuccessful against the proposed scheme.

(9) Resisting stolen-verifier attacks: In the proposed scheme, the server does not maintain any security-sensitive information in its database. An adversary cannot steal any verification table from the server to masquerade as a legitimate user. Hence, the proposed scheme resists stolen-verifier attacks.

(10) Resisting lost smart card attacks: An adversary has ability to extract the information $(ID_i, h(\cdot), e_i, s, SPUB, p, N, BPW)$ from the smart card by using the side channel attack [15, 34, 35], where $e_i = P_i \oplus r_i$, $P_i = h(ID_i||X_S)$ and $r_i = h(PW_i||B_i||N) \oplus f_i$, and tries to derive the password $PW_i$ from the information. Since the password $PW_i$ is protected by $r_i$, $B_i$, $f_i$ and $P_i$, the adversary cannot pass the biometric verification without the user's biometric template $B_i$. Then the adversary fails to obtain $r_i$, $f_i$, $P_i$ and $PW_i$, and thus the proposed scheme is secure against the smart card loss attacks.

## Security analyses of the proposed NB scheme

The arguments of exhibiting session key security, anonymity of users, perfect forward secrecy, known-key security and withstanding privileged insider attacks, off-line password guessing attacks, stolen-verifier attacks and lost smart card attacks, in the proposed NB scheme are similar to those made for the proposed TB scheme, and thus are not detailed here. The following descriptions analyze that the

**Table 2** Performance and security properties comparison

| | | [37] | [38] | [15] | [16] | [17] | [18] | [19] | Our TB | Our NB |
|---|---|---|---|---|---|---|---|---|---|---|
| Compu-tations | Client | $6T_H+2T_C$ | $5T_H+3T_C$ | $10T_H+3T_C$ | $7T_H+T_S$ | $6T_H$ | $T_B+4T_C$ | $2T_H+8T_C$ | $9T_H+3T_C$ | $9T_H+3T_C$ |
| | Server | $6T_H+2T_C$ | $5T_H+3T_C$ | $7T_H+3T_C$ | $5T_H+T_S$ | $5T_H$ | $3T_C$ | $4T_C$ | $6T_H+3T_C$ | $6T_H+3T_C$ |
| | Total | $12T_H+4T_C$ | $10T_H+6T_C$ | $17T_H+6T_C$ | $12T_H+2T_S$ | $11T_H$ | $T_B+7T_C$ | $2T_H+12T_C$ | $15T_H+6T_C$ | $15T_H+6T_C$ |
| Type | | TB | TB | TB | NB | NB | TB | TB | TB | NB |
| Transmissions | | 2 | 2 | 3 | 3 | 3 | 2 | 2 | 2 | 3 |
| User anonymity | | No | Yes | Yes | No | No | No | Yes | Yes | Yes |
| Resisting possible attacks | | No | No | Yes | No | Yes | No | Yes | Yes | Yes |

proposed NB scheme exhibits mutual authentication and resists replay attacks.

(1) Providing mutual authentication: $M_4 \equiv T_{R_C}(M_3) \equiv T_{R_C R_S}(s) \bmod p$ cannot be determined without knowledge of $R_S$ and $R_C$ because of the Extended Chaotic Maps-Based DLP and CDHP. Then, $C_i$ can authenticate $S_i$ by verifying $\beta$ in step 3, where $\beta = h(ID_i||P_i||M_2||M_3||M_4)$. Similarly, $M_2 \equiv T_{X_S}(M_1) \equiv T_{X_S R_C}(s) \bmod p$ cannot be determined without knowledge of $X_S$ and $R_C$ because of the Extended Chaotic Maps-Based DLP and DHP. Then, $S_i$ can authenticate $C_i$ by verifying $ID_i$ and $\alpha$ in step 4, where $\alpha = h(ID_i||NID_i||P_i||M_1||M_2||M_3||M_4)$. Therefore, the proposed NB scheme realizes mutual authentication.

(2) Resisting replay attacks: The proposed scheme provides the freshness of communicating messages by adopting the challenge/response interactive technique [29, 32, 36]. The user $C_i$ guarantees the freshness of communicating messages by verifying $\beta$ conatining the nonce $R_C$ selected by $C_i$ in $M_2$. Similarly, the server $S_i$ guarantees the freshness of communicating messages by verifying $\alpha$ conatining the nonce $R_S$ selected by $S_i$ in $M_3$. Therefore, the proposed scheme is secure against replay attacks.

## Performance analyses

Table 2 lists the performance and security properties comparisons of the related schemes, including the Lee et al.'s scheme [37], the He et al.'s scheme [38] and the Lee-Hsu's scheme [15], the Tan's scheme [16], the Yan et al.'s scheme [17], the Awasthi-Srivastava's scheme [18], the Das-Goawami's scheme [19] and the proposed TB and NB schemes, where $T_C$ denotes the time of executing a chebyshev chaotic map (or a chaotic hash) operation, $T_S$ denotes the time of executing a symmetric encryption/decryption operation; $T_B$ denotes the time of executing a biometrics verification and $T_H$ denotes the time of executing a hash operation, respectively.

The first comparison item is used computational cost. The Tan's scheme [16] employs symmetric encryption/decryption operations and $T_H < T_C < T_S$ [39, 40], and thus the Tan's scheme requires more computational cost than related schemes. The proposed schemes employ fewer Chebyshev polynomial operations than related schemes. Therefore, the proposed schemes are more efficient than related schemes.

The next two comparison items are the type, which proposed schemes and related schemes belong to, and the required transmissions. The schemes in [15, 18, 19, 37, 38] and the proposed TB scheme are synchronization-based (TB) authentication schemes. The schemes in [16, 17] and the proposed NB scheme are nonce-based (NB) authentication schemes. Except for the Lee-Hsu' TB scheme [15], these TB authentication schemes require fewer transmissions than NB authentication schemes.

The subsequent comparison items are providing user anonymity and resisting possible attacks. Only the Lee-Hsu's scheme [15], the Das-Goawami's scheme [19] and the proposed schemes provide user anonymity and resist possible attacks. However, the proposed TB scheme is more efficient than the Lee-Hsu's scheme [15] and the Das-Goawami's scheme [19] in transmission and in computation. The proposed NB scheme is more efficient than the Lee-Hsu's scheme [15] and the Das-Goawami's scheme [19] in computation.

Although the proposed NB scheme requires more messages in transmission than the Das-Goawami's scheme [19] and the proposed TB scheme, the proposed NB scheme does not require constructing complicated synchronized clocks in a network environment [29–32].

## Conclusions

This investigation reviews the advantages of biometric authentication for TMIS and the concepts of extended chaotic maps. In order to be more suitable for practical environment, we also develop two efficient and secure biometric-based authenticated key agreement schemes based on extended chaotic maps for TMIS. One scheme is synchronization-based, while the other is nonce-based. Compared with comparable approaches, the proposed synchronization-based and nonce-based schemes not only resist possible attacks, but also have lower computational cost and fewer communicating messages. Therefore, the proposed schemes are superior to comparable approaches.

**Acknowledgments** This research was supported by Ministry of Science and Technology under the grants MOST 103-2221-E-320 -003 and MOST 103-2221-E-182-032-MY3.

## 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. Zhu, Z., An efficient authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6):3833–3838, 2012.
3. Juang, W. S., Chen, S. T., and Liaw, H. T., Robust and efficient password-authenticated key agreement using smart card. *IEEE Trans. Ind. Electron.* 55:2551–2556, 2008.
4. Yeh, K. H., Su, C., Lo, N. W., Li, Y. J., and Hung, Y. X., Two robust remote user authentication protocols using smart cards. *J. Syst. Softw.* 83:2556–2565, 2010.
5. 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.

6. Wei, J., Hu, X., and Liu, W., An improved authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(6): 3597–3604, 2012.
7. Guo, C., and Chang, C. C., Chaotic maps-based password-authenticated key agreement using smart cards. *Commun. Nonlinear Sci. Numer. Simul.* 18:1433–1440, 2013.
8. 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(9919):1–7, 2013.
9. Lee, T.-F., and Liu, C.-M., A secure smart-card based authentication and key agreement scheme for telecare medicine information systems. *J. Med. Syst.* 37(3):9933, 2013. 1–8.
10. Lee, T.-F., An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems. *J. Med. Syst.* 37(9958):1–9, 2013.
11. Lin, C. H., and Lai, Y. Y., A flexible biometric remote user authentication scheme. *Comput. Stand. Interfaces* 27(1):19–23, 2004.
12. Khan, M. K., Zhang, J., and Wang, X., Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. *Chaos, Solitons Fractals* 35(3):519–524, 2008.
13. Li, C. T., and Hwang, M. S., An efficient biometric-based remote authentication scheme using smart cards. *J. Netw. Comput. Appl.* 33(1):1–5, 2010.
14. Das, A. K., Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. *IET Inf. Secur.* 5(3):145–151, 2011.
15. 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.
16. Tan, Z., An efficient biometrics-based authentication scheme for telecare medicine information systems. *Przeglad Elektrotechniczny* 89(5):200–204, 2013.
17. Yan, X., Li, W., Li, P., Wang, J., Hao, X., and Gong, P., A secure biometrics-based authentication scheme for telecare medicine information systems. *J. Med. Syst.* 37:9972, 2013. doi:10.1007/s10916-013-9972-1.
18. Awasthi, A. K., and Srivastava, K., A biometric authentication scheme for telecare medicine information systems with nonce. *J. Med. Syst.* 37(5):1–4, 2013.
19. 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.* 38:27, 2014. doi:10.1007/s10916-014-0027-z.
20. Li, X., Wen, Q., Li, W., Zhang, H., and Jin, Z., Secure privacy-preserving biometric authentication scheme for telecare medicine information systems. *J. Med. Syst.* 38:139, 2014. doi:10.1007/s10916-014-0139-5.
21. Kocarev, L., and Tasev, Z., Public-key encryption based on Chebyshev maps. In: *Proc. Int. Symp. Circuits Syst.* 3:III-28–III-31, 2003.
22. Mason, J. C., and Handscomb, D. C., *Chebyshev polynomials*. Chapman & Hall/CRC, Boca Raton, 2003.
23. Bergamo, P., D'Arco, P., Santis, A., and Kocarev, L., Security of public-key cryptosystems based on Chebyshev polynomials. *IEEE Trans. Circuits Syst.* 52:1382–1393, 2005.
24. Han, S., Security of a key agreement protocol based on chaotic maps. *Chaos, Solitons Fractals* 38:764–768, 2008.
25. Guo, X. F., and Zhang, J. S., Secure group key agreement protocol based on chaotic hash. *Inform. Sci.* 180:4069–4074, 2010.
26. Niu, Y., and Wang, X., An anonymous key agreement protocol based on chaotic maps. *Commun. Nonlinear Sci. Numer. Simul.* 16:1986–1992, 2011.
27. Wang, X., and Zhao, J., An improved key agreement protocol based on chaos. *Commun. Nonlinear Sci. Numer. Simul.* 15:4052–4057, 2010.
28. Farash, M. S., and Attari, M. A., An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps. *Nonlinear Dyn.* 77(1–2):399–411, 2014.
29. Stallings, W., *Cryptography and network security: principles and practice*, 2nd edition. Prentice Hall, Upper Saddle River, 1999.
30. Denning, D. E., and Sacco, G. M., Timestamps in key distribution protocols. *Commun. ACM* 24(8):533–536, 1981.
31. Gong, L., A security risk of depending on synchronized clocks. *ACM Oper Syst Rev* 26(1):49–53, 1992.
32. Lee, T. F., and Hwang, T., Provably secure and efficient authentication techniques for the global mobility network. *J. Syst. Softw.* 84: 1717–1725, 2011.
33. Zhang, L., Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos, Solitons Fractals* 37(3):669–674, 2008.
34. Kocher, P., Jaffe, J., and Jun, B., Differential power analysis. *Lect. Notes Comput. Sci* 1666:388–397, 1999.
35. Messerges, T., Dabbish, E., and Sloan, R., Examining smartcard security under the threat of power analysis attacks. *IEEE Trans. Comput.* 51(5):541–552, 2002.
36. Suzuki, S., and Nakada, K., An authentication technique based on distributed security management for the global mobility network. *IEEE J. Sel. Areas Commun.* 15:1608–1617, 1997.
37. Lee, C. C., Chen, C. L., Wu, C. Y., and Huang, S. Y., An extended chaotic maps-based key agreement protocol with user anonymity. *Nonlinear Dyn.* 69(1–2):79–87, 2012.
38. He, D., Chen, Y., and Chen, J., Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. *Nonlinear Dyn.* 69(3):1149–1157, 2012.
39. Wu, S., and Chen, K., An efficient key-management scheme for hierarchical access control in e-medicine system. *J. Med. Syst.* 36(4):2325–2337, 2012.
40. Cheng, Z. Y., Liu, Y., Chang, C. C., and Chang, S. C., Authenticated RFID security mechanism based on chaotic maps. *Secur. Comm. Netw.* 6:247–256, 2013.