Multimed Tools Appl (2017) 76:24315–24341
DOI 10.1007/s11042-016-4198-0

An improved biometrics based authentication scheme using extended chaotic maps for multimedia medicine information systems

Chengqi Wang[1] · **Xiao Zhang**[1] · **Zhiming Zheng**[1]

Received: 15 May 2016 / Revised: 21 November 2016 / Accepted: 21 November 2016/
Published online: 1 December 2016

Abstract With the increase of security requirements, numerous biometrics based authentication schemes that apply the smart card technology are proposed for multimedia medicine information systems in the last several years. Recently, Lu et al. presented a biometrics based authentication and key agreement scheme using extended Chebyshev chaotic maps. Unfortunately, we find that their scheme is still insecure with respect to issues such as flaws in the both login phase and password change phase. And we show that their scheme is vulnerable to the Denial-of-Service attack, user impersonation attack and server masquerade attack, which also fails to achieve the user anonymity. In order to remedy these weaknesses, we retain the useful properties of Lu et al.'s scheme to propose a robust biometrics based authentication and key agreement scheme for multimedia medicine information systems. The informal and formal security analysis of our scheme are given respectively, which demonstrate that our scheme satisfies the desirable security requirements. Furthermore, the proposed scheme provides some significant features which are not considered in most of the related schemes, such as, biometric information protection and user re-registration or revocation. Thus, our scheme resists the known attacks and is efficient for practical applications in the multimedia medicine information systems.

Keywords Multimedia medicine information system · Extended Chebyshev chaotic map · Biometrics · Authentication · Key agreement

✉ Xiao Zhang
09621@buaa.edu.cn

Chengqi Wang
ChengqiWang@buaa.edu.cn

Zhiming Zheng
zzheng@pku.edu.cn

[1] Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education, and School of Mathematics and Systems Science, Beihang University, New Main Building Block F Room 427, No.37 XueYuan Road, Haidian district, Beijing 100191, China

1 Introduction

With the rapid development of wireless sensor networks, advances in the communication technology enhance the quality and efficiency of online services for multimedia medical information system (MMIS) [19, 52]. In recent years, MMIS becomes more popular as an emerging healthcare application, which is widely applied to enhance the medical process at a home healthcare (HHC) agency or a clinical center between patients and doctors [20, 21]. Compared with both traditional medical diagnosis process and paper-based medical system, MMIS provides the electronic media-based medical services such as clinical diagnosis, health guidance and health record, which measures the significant and private parameters (such as electrocardiogram, blood pressure, heart rate and so on) of patients and sends them to remote servers [2, 5, 11, 18, 43, 46]. With the assistance of MMIS, patients who suffer from diabetes mellitus, hypertension and coronary artery disease are able to directly exchange their daily medical data and access medical specialists more conveniently. Besides, in order to take better care of the aged people, remote medical clinical diagnostics and real-time monitoring of patients are considered as crucial parts of healthcare systems [22, 23]. However, general communication between doctors and patients is almost implemented through the Internet and is vulnerable to many different kinds of attacks so that how to ensure the security and privacy of e-healthcare information transmitted over the public networks becomes a great challenge from academia and industry [30, 49, 57, 58].

Over the last two decades, authentication schemes have been widely applied in a variety of information systems. Since the first one for open communication channels was proposed by Lamport, a great many of authentication schemes have been presented to achieve the authorized communication between remote entities [1, 9, 26, 34, 38, 44]. According to the evidences adopted in the protocols, most existing schemes are divided into two categories: identity-based and certificate-based [24, 27, 32, 50]. The latter category requires the large storage space and high computation overhead for the management of certificate store so that a good amount of identity-based authentication protocols are generally applied in the MMISs to provide the convenient and secure health-care services [10, 16, 17, 28, 41, 47, 51, 53, 55, 60].

In the last several years, there are many conventional authentication protocols for MMISs which are based on the elliptic curve cryptography (ECC) and traditional public key cryptography [17, 28, 51, 53, 55, 60]. In 2010, Wu et al. [53] presented an identity-based authentication scheme for MMISs adopting the RSA algorithm. However, He et al. [17] analyzed that Wu et al.'s scheme was unable to resist the impersonation attack and insider attack, and failed to achieve the mutual authentication. Then He et al. [17] put forward an improved identity-based authentication scheme. Unfortunately, Wei et al. [51] pointed out that Wu et al.'s scheme [53] and He et al.'s scheme [17] were still insecure against the off-line password guessing attack. In order to eliminate the security weakness, Wei et al. [51] proposed an enhanced authentication scheme to enhance the security of MMISs. In addition, Xu et al. [55] designed a novel dynamic identity-based authentication protocol using ECC in 2014. Islam and Khan [28] proved that Xu et al.'s scheme [55] failed to update the password correctly and was insecure against the strong replay attack. Then Islam and Khan [28] put forward an improved authentication for MMISs. However, Zhang and Zhu [60] examined that Islam and Khan's protocol [28] was unable to resist the off-line password guessing attack and server spoofing attack, and further proposed an enhanced authentication protocol.

The scalar point multiplication and modular exponentiation operation in the elliptic curve group are involved in the above schemes [17, 28, 51, 53, 55, 60], which are complicated to perform in the mobile environment where the computation overhead and storage space are constrained, especially in the MMISs. Benefit from the development of chaos theory, extended Chebyshev chaotic maps are implemented efficiently and have been added into the authentication schemes to solve these aforementioned problems [10, 16, 41, 47]. Thus, more work about authenticated key agreement schemes using extended chaotic maps needs to be studied. Furthermore, there are some security vulnerabilities to two-factor identity-based authentication schemes which apply the passwords and tokens for providing the authentication [6, 33, 36, 54]. In particular, it is difficult to remember long and random passwords for patients. Meanwhile, short passwords are easily compromised by the dictionary attack since their low entropy. Based on side channel attacks, such as SPA and DPA, it is feasible to extract the information stored in the smart cards [45]. To meet these problems, many researchers have combined the biometric information, passwords and tokens to enhance the security of authentication schemes [8, 25, 61], where the uniqueness of biometrics makes it extremely difficult for adversary to forge the biometric information [37, 39]. And authentication protocol does not request user to remember his biometrics. However, biometric characteristics imprinted by the same user are not exactly the same every time so that directly adopting them always results in the low acceptation of MMISs [3, 12, 13]. Thus, we introduce the fuzzy extractor to increase the probability of acceptance.

Recently, Lu et al. [42] put forward a biometrics based authentication scheme for MMISs using extended Chebyshev chaotic maps to overcome the weaknesses of previous schemes. Unfortunately, according to the analysis given in this paper, we find that their scheme is still insecure with respect to issues such as flaws in the both login phase and password change phase. And we show that their scheme is vulnerable to the Denial-of-Service attack, user impersonation attack and server masquerade attack, which also fails to achieve the user anonymity. In order to solve these problems, we retain the useful properties of Lu et al.'s scheme to propose a robust biometrics based authentication and key agreement scheme for MMISs. The presented scheme satisfies the desirable security requirements which are demonstrated in the informal and formal security analysis, respectively. Furthermore, the proposed scheme provides some significant features which are not considered in most of the related schemes, for example, biometric information protection and user re-registration or revocation. Compared with other related schemes, our scheme provides some more secure properties and significant functionalities with the same level of computation overhead, communication cost and storage space.

The remaining of this paper is organized as follows. Next section briefly introduces the fuzzy extractor, threat assumptions, one-way hash function and extended Chebyshev chaotic map which are applied in our scheme. Section 3 reviews the Lu et al.'s scheme. And Section 4 mainly discusses the weaknesses of Lu et al.'s scheme. Section 5 describes the proposed scheme in details. Then Section 6 provides the informal security analysis, security model, formal security analysis, verification about BAN logic, functionality analysis and performance comparison analysis, respectively. Last section gives the conclusion.

2 Preliminaries

In this section, we describe the details of fuzzy extractor, threat assumptions, one-way hash function and extended Chebyshev chaotic map which are adopted in the presented scheme.

2.1 Fuzzy extractor

The mechanism of fuzzy extractor which contains two procedures is illustrated in the Fig. 1. In particular, procedure Gen includes a probabilistic generation function, which extracts the biometric information BIO, and outputs an auxiliary binary string $R \in \{0,1\}^l$ and a nearly random binary string $P \in \{0,1\}^*$. Accordingly, procedure Rep contains a deterministic reproduction function, which recovers R with the assistance of biometrics BIO^* and corresponding auxiliary binary string P. If $Gen(BIO) \rightarrow \langle R, P\rangle$ and $dis(BIO, BIO^*) \leq t$, then we have $Rep(BIO^*, P) = R$. Otherwise, there is no guarantee provided by procedure Rep. The error-tolerant mechanism makes it dependable to retrieve a nearly uniform randomness R with the help of corresponding auxiliary string P from biometric information BIO^*, as long as it remains reasonably close to original biometrics BIO. More details about fuzzy extractor are explained in the literature [3, 12, 13].

2.2 Threat assumptions

During this subsection, we introduce the Dolev-Yao threat model [14] and consider the risk of side-channel attacks [31] to establish the following threat assumptions in the multimedia medicine information systems.

1. Adversary E may be an outsider or a malicious yet legitimate user.
2. Adversary E eavesdrops on the all communication between user and server through a public channel.
3. Adversary E reroutes, modifies, resends and deletes the eavesdropped information.
4. Adversary E extracts the sensitive stored messages from a lost or stolen smart card by examining the power consumption.

2.3 One-way hash function

The one-way hash function $h = h(x) : \{0,1\}^* \rightarrow \{0,1\}^n$ is a deterministic algorithm, which outputs a fixed length binary string $\{0,1\}^n$ according to the arbitrary length binary

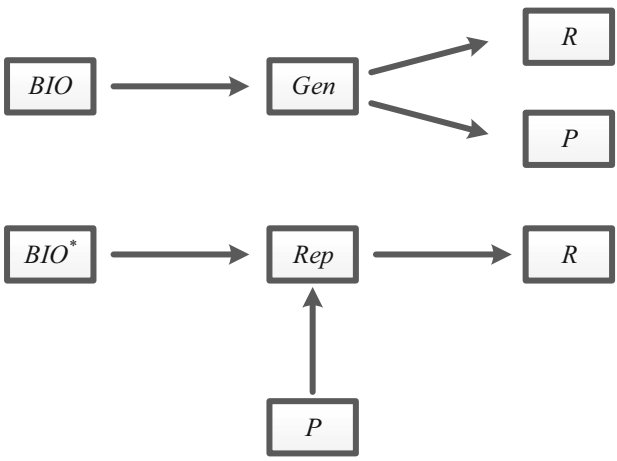

Fig. 1 The mechanism of fuzzy extractor

string $\{0, 1\}^*$ [7]. Also it is computationally infeasible to retrieve the input x from the given hash value and hash function, which is called the one-way property. Furthermore hash function possesses the both weak and strong collision resistant property. For a given input x, finding any input $y \neq x$ so that $h(x) = h(y)$ is computationally infeasible. For a given pair of inputs (x, y) with $x \neq y$, $h(x) = h(y)$ is computationally infeasible.

2.4 Extended Chebyshev chaotic map

The Chebyshev chaotic map $T_n(x)$ is a polynomial in x of degree n, which is defined by the following equation.

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

in which $x = \cos\theta$ [4]. Besides, recurrence equation of $T_n(x)$ is defined as the equation below.

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

for any natural number $n \geq 2$, with $T_0(x) = 1$ and $T_1(x) = x$. The Chebyshev chaotic map satisfies the semi-group property and commutative under composition so that $T_r(T_s(x)) = T_s(T_r(x))$. It is proved by the following relation.

$$\begin{aligned} T_r(T_s(x)) &= \cos\left(r \cdot \cos^{-1}\left(\cos(s \cdot cos^{-1}(x))\right)\right) \\ &= \cos(rs \cdot \cos^{-1}(x)) = T_{sr}(x) = T_s(T_r(x)), \end{aligned}$$

for any natural number $s, r \in Z^+$. In 2008, Zhang [59] further enhanced the Chebyshev chaotic map, then he proved that semi-group property and commutative under composition still hold on the interval $(-\infty, +\infty)$. The extended Chebyshev polynomial is defined by the following relation.

$$T_n(x) = (2x \cdot T_{n-1}(x) - T_{n-2}(x)) \mod p,$$

where $n \geq 2$, $x \in (-\infty, +\infty)$ and p is a large prime number. Also $T_r(T_s(x)) = T_{rs}(x) = T_s(T_r(x)) \mod p$ holds. There are two computationally infeasible problems for extended Chebyshev chaotic map [35], which are explained as follows.

Extended Chebyshev chaotic map discrete logarithm problem (ECDLP): given p, x and y, finding an integer r satisfying $y = T_r(x) \mod p$ is computationally infeasible.

Extended Chebyshev chaotic map decisional Diffie-Hellman problem (ECDDHP): given x, $T_r(x)$, $T_s(x)$ and $T_z(x)$, deciding whether $T_{rs}(x) = T_z(x) \mod p$ holds is computationally infeasible.

3 Review of Lu et al.'s scheme

Recently, Lu et al. [42] proposed a biometrics based authentication scheme for multimedia medicine information systems using extended Chebyshev chaotic maps. There are three phases relating to the Lu et al.'s scheme, which are registration phase, login and authentication phase, and password change phase, respectively. Server S selects two hash functions $h_1(\cdot)$ and $h_2(\cdot)$. For convenience, Table 1 lists the symbols and notations applied in their scheme.

Table 1 Symbols and notions in Lu et al.'s scheme

Symbol	Notion
U, S	User and server, respectively
ID, PW	U's identity and password, respectively
$H(\cdot)$	Biohash function
$h_1(\cdot)$	Hash function $h_1 : \{0, 1\}^* \rightarrow \{0, 1\}^n$
$h_2(\cdot)$	Hash function $h_2 : [-1, 1] \rightarrow \{0, 1\}^n$
k_u, k_s	Secret key selected by U and S, respectively
$\oplus, \|\|$	EOR operation and concatenation operation, respectively

3.1 Registration phase

1. New user U selects the identity ID and password PW, and imprints the biometrics BIO. Then U calculates $PWD = h_1(PW||H(BIO))$, and sends $\{ID, PWD\}$ to server S over a secure channel.
2. After receiving the request message, S computes $K = h_1(ID||PWD)$ and $IM_1 = K \oplus h_1(k_s)$, in which k_s is S's secret key. S issues the smart card SC to U, which contains $\{IM_1\}$ through a secure channel.
3. Upon receiving the smart card, U selects a secret key k_u and calculates $f = h_1(ID||k_u) \oplus PWD$. Finally, user U stores f into the SC which contains $\{IM_1, f, h_1(\cdot), h_2(\cdot), H(\cdot)\}$.

3.2 Login and authentication phase

1. U inserts the SC into a device reader, inputs the identity ID, password PW, selects a secret key k_u and biometrics BIO. Then U verifies whether $h_1(ID||k_u) \oplus h_1(PW||H(BIO))$ is consistent with f. If it holds, U calculates $K = h_1(ID||h_1(PW||H(BIO)))$, 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 login request $\{R_1, R_2, R_3\}$ to S over a public channel.
2. When receiving the login request from U, S adopts his secret key k_s to compute $K' = IM_1 \oplus h_1(k_s)$, $ID = R_1 \oplus K$, $T_u(K) = R_2 \oplus ID$, and checks whether $h_1(ID||T_u(K))$ is consistent with R_3. If they are equal, S generates a random number v, and calculates $IM_2 = T_v(K) \oplus ID$, $Auth_S = h_1(K||T_v(K)||sk)$, $T_{uv}(K)$ and $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$. Finally, S submits the message $\{Auth_S, IM_2\}$ to U.
3. Upon receiving the authentication request message, U retrieves $T_v(K)$ by calculating $IM_2 \oplus ID$ and computes $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$ to check whether $Auth'_S = h_1(K||T_v(K)||sk)$ is equal to $Auth_S$. If it holds, S is authenticated successfully and calculates $Auth_U = h_1(sk||T_v(K)||K)$ to send the message $\{Auth_U\}$ to S.
4. Once receiving the message, S validates whether $h_1(sk||T_v(K)||K)$ is consistent with $Auth_U$. If it is true, U is authenticated successfully. Otherwise, S refuses the request. Lastly, U and S have a common session key $sk = h_2(T_u(K), T_v(K), T_{uv}(K))$.

3.3 Password change phase

1. U inputs the identity ID, old password PW, secret key k_u and biometrics BIO.
2. SC validates whether $h_1(ID||k_u) \oplus h_1(PW||H(BIO))$ is consistent with f.

3. If it is true, U selects new password PW^{new} and new secret key k_u^{new} to calculate f^{new}.
4. SC replaces f with f^{new} in the memory.

4 Cryptanalysis of Lu et al.'s scheme

Lu et al.'s scheme efficiently resists the insider attack and password guessing attack. In addition, their scheme ensures the forward secrecy. Unfortunately, their scheme is still vulnerable to the Denial-of-Service attack. Moreover, their scheme is insecure against the user impersonation attack and server masquerade attack. We also find that some phases of Lu et al.'s scheme are not correct. Furthermore, Lu et al.'s scheme does not provide the user anonymity and user re-registration/revocation. We describe the details of these problems in the following subsections.

4.1 Flaws in login and authentication phase

During the registration phase of Lu et al.'s scheme, server S computes $IM_1 = K \oplus h_1(k_s)$ which is stored in the smart card SC and transmits it to U through a secure channel. There are no extra operations and storage spaces for storing every user's IM_1 in the database of server S in their scheme. In the login and authentication phase, user U sends the login request $\{R_1, R_2, R_3\}$ to server S over a public channel and then S adopts his secret key k_s to compute $K' = IM_1 \oplus h_1(k_s)$ as planned. However, IM_1 is not submitted to S by U in the login phase so that S is unable to retrieve K' without IM_1. Thus, this operation is impossible in the Lu et al.'s scheme. Therefore we demonstrate that there are flaws in the login and authentication phase, especially user U should send $\{R_1, R_2, R_3, IM_1\}$ to server S instead of $\{R_1, R_2, R_3\}$.

4.2 Flaws in password change phase

In the password change phase of Lu et al.'s scheme, user U inputs his identity ID, old password PW^{old}, secret key k_u and biometrics BIO. Then smart card SC validates whether $h_1(ID||k_u) \oplus h_1(PW||H(BIO))$ is consistent with f. If it is true, U selects new password PW^{new} and new secret key k_u^{new} to calculate f^{new}. Finally, SC replaces f with f^{new} in the memory as planned. However, during the next login phase, U calculates his new $K_U = h_1(ID||h_1(PW^{new}||H(BIO)))$ and transmits IM_1^{old} to server S. On the other hand, S computes his new $K_S = IM_1^{old} \oplus h_1(k_s)$ during the further authentication phase, that is, $K_S = h_1(ID||h_1(PW^{old}||H(BIO)))$ according to $K_S = h_1(ID||PWD^{old})$ and $PWD^{old} = h_1(PW^{old}||H(BIO))$. As we know, U calculates $sk_U = h_2(T_u(K_U), T_v(K_S), T_{uv}(K_S))$ and S computes $sk_S = h_2(T_u(K_U), T_v(K_S), T_{uv}(K_U))$. Due to $PW^{old} \neq PW^{new}$, $K_S \neq K_U$ so that U and S have different session keys. Thus there are flaws in password change phase, especially IM_1 needs to be updated.

4.3 Denial-of-service attack

Although targets and means may vary, Denial-of-Service (DoS) attack is generally an attempt to make network resources unavailable for malicious users and adversaries, which indefinitely or temporarily interrupts the services of hosts. In the Lu et al.'s scheme, adversary E is able to carry out the DoS attack without difficulty. Figure 2 shows the procedure and effect of DoS attack on the Lu et al.'s scheme. Particularly, E collects the previous

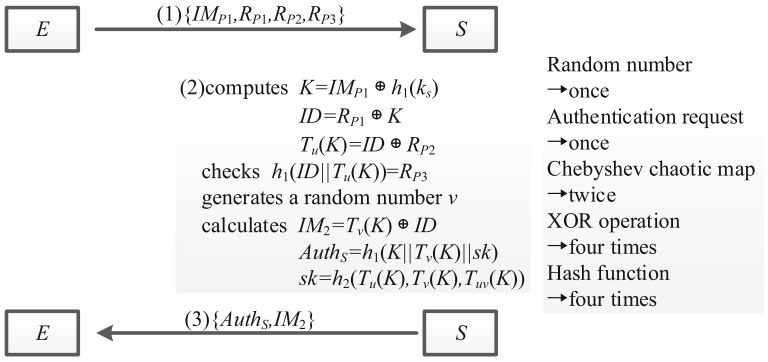

Fig. 2 The DoS attack on the Lu et al.'s scheme

login request message $\{R_{P1}, R_{P2}, R_{P3}, IM_{P1}\}$ from a public channel and then forwards it to server S. After receiving the login request message, S does not know whether received messages are outdated and as always executes the operation (2) which includes generating the random number once, sending the authentication request message once, executing the Chebyshev chaotic map operation twice, calculating the XOR operation four times and performing the hash function four times. By adopting the intercepted login request message repeatedly, E is able to make the services or network resources unavailable in the multimedia medicine information system so that Lu et al.'s scheme becomes vulnerable to the DoS attack. To solve this problem, timestamp needs to be added in the login request message, which helps servers check the freshness of messages in order to resist the DoS attack to a certain extent.

4.4 User impersonation attack

Let E be a malicious yet legitimate user in the multimedia medicine information system, who possesses his smart card and extracts the information of smart card $\{IM_{1E}, f_E, h_1(\cdot), h_2(\cdot), H(\cdot)\}$. And E is able to impersonate another legal user U to cheat the server S so that Lu et al.'s scheme is vulnerable to the user impersonation attack. E carries out the following steps.

1. E calculates $PWD_E = h_1(PW_E||H(BIO_E))$ and $K_E = h_1(ID_E||PWD_E)$. Then he retrieves $h_1(k_s) = K_E \oplus IM_{1E}$.
2. E collects the user U's login request message $\{R_1, R_2, R_3, IM_1\}$, and computes $K = IM_1 \oplus h_1(k_s)$ and $ID = R_1 \oplus K$ for user impersonation attack.
3. E generates a random number w and computes $R_{1E} = K \oplus ID$, $R_{2E} = ID \oplus T_w(K)$, and $R_{3E} = h_1(ID||T_w(K))$. Then E submits his login request message $\{R_{1E}, R_{2E}, R_{3E}, IM_1\}$ to S.
4. Upon receiving the login request, S authenticates E who impersonates U successfully, executes the following operations and submits the message $\{Auth_S, IM_2\}$ to E.
5. When receiving the message, E retrieves $T_v(K) = IM_2 \oplus ID$, computes $T_{wv}(K) = T_w(T_v(K))$ and $sk = h_2(T_w(K), T_v(K), T_{wv}(K))$, and calculates $Auth_E = h_1(sk||T_v(K)||K)$ to send the authentication message $\{Auth_E\}$ to S.
6. Finally, E and S agree on a common session key $sk = h_2(T_w(K), T_v(K), T_{wv}(K))$ successfully. However, E performs a user impersonation attack since S believes that he is communicating with U.

4.5 Server masquerade attack

As described in this subsection, Lu et al.'s scheme is vulnerable to the server masquerade attack. More narrowly, adversary E who is a malicious yet legitimate user can be authenticated by another legitimate user U using the S's secret value $h_1(k_s)$. The details are showed as follows.

1. Upon intercepting the login request message $\{R_1, R_2, R_3, IM_1\}$ from U, E calculates $K = IM_1 \oplus h_1(k_s)$, $ID = R_1 \oplus K$ and $T_u(K) = R_2 \oplus ID$.
2. E generates a random number w and computes $IM_2 = T_w(K) \oplus ID$, $sk = h_2(T_u(K), T_w(K), T_{uw}(K))$ and $Auth_E = h_1(K||T_w(K)||sk)$. Then he submits the message $\{Auth_E, IM_2\}$ to U.
3. When receiving the message from E, U executes the following operations and then authenticates E.
4. Finally, E and U agree on a common session key $sk = h_2(T_u(K), T_w(K), T_{uw}(K))$ successfully. However, E performs a server masquerade attack since U believes that he is communicating with S.

4.6 Lack of user anonymity

Unfortunately, since identity of user U is derived from R_1 by using the secret value $h_1(k_s)$, their scheme cannot achieve the user anonymity. First E calculates $PWD_E = h_1(PW_E||H(BIO_E))$ and $K_E = h_1(ID_E||PWD_E)$. Then he retrieves $h_1(k_s) = K_E \oplus IM_{1E}$. Next E collects the U's login request message $\{R_1, R_2, R_3, IM_1\}$. Finally he computes $K = IM_1 \oplus h_1(k_s)$ and $ID = R_1 \oplus K$ to thieve the identity of legitimate user. Therefore Lu et al.'s scheme is unable to provide the user anonymity.

4.7 Lack of user re-registration/revocation

There is no user re-registration/revocation phase in the Lu et al.'s scheme so that user U is unable to re-register or revoke his privilege if his smart card SC is lost or stolen. In order to promote the functionality of multimedia medicine information system, we design the corresponding re-registration/revocation phase and more details are described in the following section.

5 The proposed scheme

Based on the cryptanalysis of Lu et al.'s scheme, we propose a novel biometric-based authentication and key agreement scheme for multimedia medicine information systems. Our scheme consists of the following four phases: registration phase, login and authentication phase, password change phase and re-registration/revocation phase. The presented scheme improves the Lu et al.'s scheme in the several aspects: 1) it resists the Denial-of-Service attack by adding a timestamp in the login request message, 2) it hides the server S's secret value to prevent the user impersonation attack and server masquerade attack, 3) it provides the user anonymity to enhance the performance of multimedia medicine information systems, and 4) it adds the user re-registration/revocation phase for practical requirements. More details are described in the following subsections. For convenience, Table 2 lists the symbols and notations applied in our scheme.

Table 2 Symbols and notions in our scheme

Symbol	Notion
U_i, S	ith user and server, respectively
SC_i, ID_i	U_i's smart card and identity, respectively
CID_i	U_i's dynamic identity
PW_i, BIO_i	U_i's password and biometrics, respectively
R_i	U_i's nearly random binary string
P_i	U_i's auxiliary binary string
s, x	Master secret key and secret key selected by S, respectively
$h_1(\cdot)$	Hash function $h_1 : \{0, 1\}^* \rightarrow \{0, 1\}^n$
$h_2(\cdot)$	Hash function $h_2 : [-1, 1] \rightarrow \{0, 1\}^n$
$\oplus$, $\|\|$	EOR operation and concatenation operation, respectively

5.1 Registration phase

New user U_i executes the registration phase with server S over a secure channel. The registration phase is illustrated in the Fig. 3 and is described as follows.

1. Firstly, new user U_i imprints his personal biometric information BIO_i at the sensor. Next sensor sketches BIO_i, extracts (R_i, P_i) from $Gen(BIO_i) \rightarrow (R_i, P_i)$, and stores P_i in the memory. U_i selects his identity ID_i and password PW_i, and calculates $RPW_i = h_1(PW_i||R_i)$.
2. Then he sends the registration request message $\{ID_i, RPW_i\}$ to server S through a secure channel.
3. After receiving the registration request, S computes $A_i = h_1(ID_i||s)$, $CID_i = ENC_x(ID_i||k_u)$ and $V_i = h_1(ID_i||RPW_i)$, in which k_u is selected by S and has a fixed length. Then S adds a novel entry $\langle ID_i, N_i = 1\rangle$ to the database, where N_i means the times of user registration.

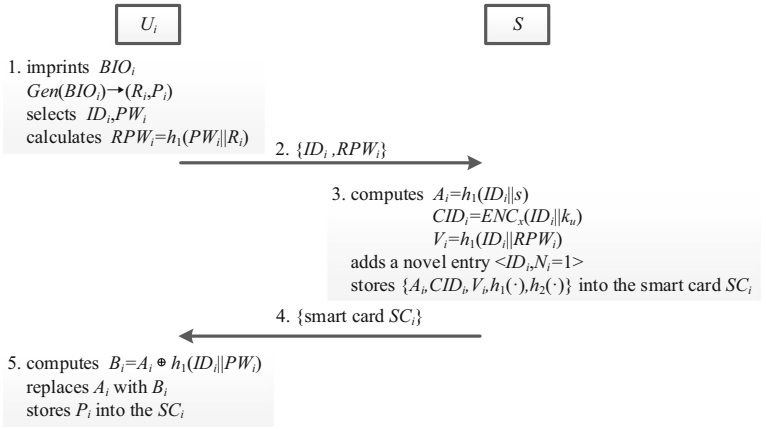

Fig. 3 The registration phase

4. S issues U_i with his smart card SC_i which contains $\{A_i, CID_i, V_i, h_1(\cdot), h_2(\cdot)\}$ via a secure channel.
5. Upon receiving the SC_i, U_i computes $B_i = A_i \oplus h_1(ID_i||PW_i)$, replaces A_i with B_i and stores P_i into the SC_i. Thereby it is noted that smart card SC_i contains $\{B_i, CID_i, P_i, V_i, h_1(\cdot), h_2(\cdot)\}$.

5.2 Login and authentication phase

During the login and authentication phase, smart card SC_i is able to verify the U_i's identity, password, and biometric information immediately. Also server S confirms the freshness of login request message. The login and authentication phase is showed in the Fig. 4 and is explained below.

1. User U_i inserts his smart card SC_i into the reader, imprints his biometrics BIO_i^* at the sensor, and inputs his identity ID_i and password PW_i. Then sensor sketches BIO_i^* and recovers R_i from $Rep(BIO_i^*, P_i) \rightarrow R_i$.
2. U_i calculates $RPW_i = h_1(PW_i||R_i)$ and verifies whether $h_1(ID_i||RPW_i) = V_i$ holds. If it holds, U_i further computes $A_i = B_i \oplus h_1(ID_i||PW_i)$. Otherwise, SC_i terminates the U_i's login.

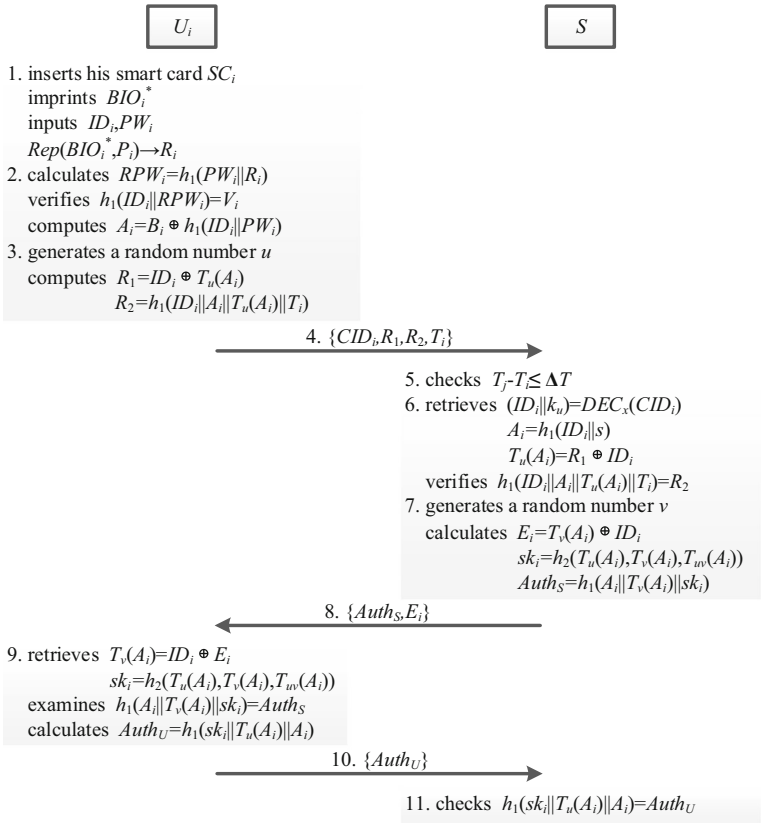

Fig. 4 The login and authentication phase

3. U_i selects a random number u, and computes $R_1 = ID_i \oplus T_u(A_i)$ and $R_2 = h_1(ID_i||A_i||T_u(A_i)||T_i)$, where T_i is an additional timestamp.
4. U_i submits the login request message $\{CID_i, R_1, R_2, T_i\}$ to S over a public channel.
5. When receiving the login request message from U_i, server S checks whether $T_j - T_i \leq \Delta T$ is valid, where ΔT is time interval and T_j is the time when receiving the login request message. If it holds, S performs the following steps. Otherwise, login request message is rejected by S.
6. S retrieves $(ID_i||k_u) = ENC_x(CID_i)$, $A_i = h_1(ID_i||s)$ and $T_u(A_i) = R_1 \oplus ID_i$. Then S verifies whether $h_1(ID_i||A_i||T_u(A_i)||T_i)$ is consistent with R_2.
7. If this verification holds, S generates a random number v, and calculates $E_i = T_v(A_i) \oplus ID_i$, $sk_i = h_2(T_u(A_i), T_v(A_i), T_{uv}(A_i))$ and $Auth_S = h_1(A_i||T_v(A_i)||sk_i)$. Otherwise, S terminates the authentication request.
8. S sends the authentication request message $\{Auth_S, E_i\}$ to U_i through a public channel.
9. Upon receiving the authentication request message, U_i retrieves $T_v(A_i) = ID_i \oplus E_i$, $sk_i = h_2(T_u(A_i), T_v(A_i), T_{uv}(A_i))$ and then examines whether $h_1(A_i||T_v(A_i)||sk_i) = Auth_S$ holds. If it holds, U_i authenticates S successfully and calculates $Auth_U = h_1(sk_i||T_u(A_i)||A_i)$. Otherwise, U_i rejects the authentication request.
10. Then U_i submits the authentication request message $\{Auth_U\}$ to S through a public channel.
11. After receiving the authentication request message, S checks whether $h_1(sk_i||T_u(A_i)||A_i) = Auth_U$ holds. If this verification holds, S authenticates U_i successfully. Otherwise, authentication request is rejected by S. Finally, U_i and S have a common session key sk_i for further communication.

5.3 Password change phase

During the password change phase, U_i updates the password without any help from server S. This phase includes the following four steps.

1. User U_i inserts his smart card SC_i, imprints his biometrics BIO_i^* at the sensor, and inputs ID_i and PW_i. Then sensor sketches BIO_i^* and recovers R_i from $Rep(BIO_i^*, P_i) \rightarrow R_i$.
2. U_i computes $RPW_i = h_1(PW_i||R_i)$ and verifies whether $h_1(ID_i||RPW_i) = V_i$ holds. If this verification holds, SC_i asks U_i for a new password. Otherwise, password change request is rejected immediately by SC_i.
3. U_i selects new password PW_i^{new} and further calculates $RPW_i^{new} = h_1(PW_i^{new}||R_i)$, $B_i^{new} = B_i \oplus h_1(ID_i||PW_i) \oplus h_1(ID_i||PW_i^{new})$ and $V_i^{new} = h_1(ID_i||RPW_i^{new})$.
4. U_i replaces B_i with B_i^{new} and V_i with V_i^{new} in the memory, respectively.

5.4 User revocation/re-registration phase

The user re-registration/revocation phase helps user U_i re-register or revoke his privilege when his smart card SC_i is lost or stolen. If U_i wants to re-register, he sends a re-registration request to server S via a secure channel. Then S executes the registration steps which are described in the previous section and replaces $\langle ID_i, N_i \rangle$ with $\langle ID_i, N_i = N_i + 1 \rangle$ to assist U_i re-register. Similarly, upon receiving a revocation request through a secure channel, S modifies the corresponding entry by setting at $\langle ID_i, N_i = 0 \rangle$.

6 Analysis of our scheme

The authentication and key agreement schemes proposed for multimedia medicine information systems need to possess two essential requirements which are security and functionality. During this section, we analysis how the presented scheme is satisfied with these requirements, and compare our scheme with other related authentication and key agreement schemes.

6.1 Informal security analysis

In this subsection, we analyze the strength of our scheme against the following common attacks.

Resistance to replay attack Replay attack means that adversary E intercepts the submitted messages to apply these data in some manner, which includes copying and possibly altering these data. Although adversary E intercepts the previous login request message $\{CID_i, R_1, R_2, T_i\}$ and transmits it to server, S verifies the legality of message by verifying T_i and R_2 as follows.

$$R_2 = h_1(ID_i||A_i||T_u(A_i)||T_i),$$

in which T_i is different during every session so that E is unable to be authenticated by S. Therefore the proposed scheme resists the replay attack by adding the timestamp T_i into verification information R_2.

Resistance to modification attack Though adversary E attempts to modify the intercepted messages, the presented scheme examines whether the received messages are modified with the help of one-way hash function. E does not have the capabilities to retrieve u, ID_i and A_i from the intercepted information so that he cannot generate a legitimate login or authentication message. Thus our scheme is secure against the modification attack.

Resistance to stolen-verifier attack In our scheme, server S does not save the biometrics or passwords of legitimate users so that adversary E is unable to steal the biometrics-verifier or passwords-verifier of users even if he has an authorized database access. As a result, the presented scheme prevents the stolen-verifier attack.

Resistance to password guessing attack With the assistance of side-channel attacks, adversary E acquires B_i, P_i, CID_i, and V_i. But he cannot check the U_i's password in the off-line or on-line environment without relevant information about BIO_i and x. At the same time, U_i's password is protected by $h_1(PW_i||R_i)$, in which R_i possesses the high entropy. Besides, there is no the same biometric template between any two people. Consequently, our scheme is secure against the password guessing attack.

Resistance to user impersonation attack User impersonation attack means that a malicious yet legitimate user E attempts to impersonate another user for authentication and key agreement. During the communication between user U_i and server S, U_i's real identity ID_i is protected by $CID_i = ENC_x(ID_i||k_u)$ and $R_1 = ID_i \oplus T_u(A_i)$. Furthermore, random number k_u changes in every registration phase and u changes in each session so that E

is unable to acquire another legitimate user's identity. In conclusion, the proposed scheme prevents the user impersonation attack.

Resistance to server masquerade attack Upon receiving the login request message from U_i, adversary E tries to masquerade as server S by applying the previous authentication request message $\{Auth_S^{old}, E_i^{old}\}$, in which $Auth_S^{old} = h_1(A_i||T_v(A_i)^{old}||sk_i^{old})$, $sk_i^{old} = h_2(T_u(A_i)^{old}, T_v(A_i)^{old}, T_{uv}(A_i)^{old})$ and $E_i^{old} = T_v(A_i)^{old} \oplus ID_i$. However U_i adopts the different random numbers during the different sessions, that is, $T_u(A_i)^{old} \neq T_u(A_i)^{new}$ so that E's attempt fails. Therefore, our scheme resists the server masquerade attack.

Resistance to insider attack Malicious insider E has the authority to access the system and is familiar with system procedures, who tries to acquire user U_i's private messages such as biometrics and password. Server S cannot recover the biometrics BIO_i or password PW_i from $RPW_i = h_1(PW_i||R_i)$. Furthermore S does not store RPW_i in the database. So the presented scheme prevents the insider attack.

Resistance to Denial-of-Service attack Adversary E carries out the Denial-of-Service (DoS) attack to diminish or eliminate server's capability, which usually makes server S unavailable. With the help of timestamp T_i, server S verifies the freshness and legality of $R_2 = h_1(ID_i||A_i||T_u(A_i)||T_i)$ in the login request message. The current timestamp is unable to match the previous R_{P2} which is submitted by adversary E. Besides, input verification of password and identity has been added in the proposed scheme, which avoids the invalid input and malicious tampering. Also our scheme adopts the fuzzy extractor to satisfy the usage requirements of biometrics. As a result, the proposed scheme is secure against the DoS attack.

Resistance to stolen smart card attack Stolen smart card attack means that adversary E tries to use the information stored in the smart card SC_i to be authenticated by server S without biometrics or password. With the assistance of SPA or DPA, E is able to obtain B_i, P_i, CID_i and V_i. In the presented scheme, a session key between user U_i and server S is generated below.

$$(ID_i||k_u) = DEC_x(CID_i),$$
$$T_u(A_i) = R_1 \oplus ID_i,$$
$$T_v(A_i) = ID_i \oplus E_i,$$
$$sk_i = h_2(T_u(A_i), T_v(A_i), T_{uv}(A_i)).$$

Although E obtains CID_i, R_1 and E_i over public channels, it is difficult for him to retrieve A_i and ID_i without secret values u, v and x. Above all, our scheme resists the smart card attack.

6.2 Security model

Based on He et al.'s work [21] and Dolev-Yao threat model [14], we define the capabilities of adversary E in the security model. We establish the threat assumptions as mentioned in the Subsection 2.2 and further allow E potentially control the all communications over the public network during a probabilistic polynomial time. We consider a game between adversary and oracle in which adversary E asks some queries to the oracle and oracle responses to the adversary. These queries simulate the attacks which adversary E may execute in the

real system. We consider the following types of queries for the proposed authentication and key agreement scheme. Let $\Pi_{U_i}^l$ denotes the lth instance of participant U_i.

1. $Extract(ID_i)$: When E executes this query with user U_i's identity ID_i, oracle allows E to get the long-term secret key of ID_i.
2. $Execute(U_i, S)$: This query simulates the passive attacks, in which E eavesdrops an execution of scheme and gets back the complete transcripts between U_i and S.
3. $Send(\Pi_{U_i}^l, M)$: When E executes this query with message M, oracle executes the authentication and key agreement protocol according to its specification and returns the result to E, which leads to some active attacks such as impersonation attacks and man-in-the-middle attacks.
4. $Reveal(\Pi_{U_i}^l)$: This query simulates the known key attacks in the real system, where oracle returns the session key for instance $\Pi_{U_i}^l$ to E.
5. $Corrupt(ID_i)$: When E executes this query with user U_i's identity ID_i, oracle exposes the long-term secret key held by U_i.
6. $Test(\Pi_{U_i}^l)$: This query is used to define the advantage of E. When adversary E asks this query to instance $\Pi_{U_i}^l$, a random bit b is chosen. If $b = 1$, then session key is returned. Otherwise a random string with the same length of the session key is returned to E.

6.3 Formal security analysis

With the assistance of formal security analysis, we demonstrate that our scheme is secure against the adversary E. In this subsection, we adopt the oracle $Reveal$ as described above. It unconditionally outputs x from the one-way hash function $y = h_1(x)$. In particular, the following two theorems provide the formal security analysis for our scheme.

Theorem 1 *Under the assumption that hash function $h_1(x)$ closely behaves like the oracle Reveal, our scheme is provably secure against the adversary E for recovering the identity ID_i of user U_i, secret key s of server S, and session key sk_i between U_i and S, respectively.*

Proof We need to establish the capacity of E who is able to retrieve the identity ID_i of U_i, secret key s of S, and session key sk_i between U_i and S, respectively. Adversary E adopts the oracle $Reveal$ to perform the experimental algorithm $EXP1_{E,BAKAS}^{HASH}$, in which the $BAKAS$ means the presented biometrics based authentication and key agreement scheme. Particularly, details of Algorithm $EXP1_{E,BAKAS}^{HASH}$ are showed in the Table 3. □

We define the success probability of $EXP1_{E,BAKAS}^{HASH}$ as $Success1 = \left|P(EXP1_{E,BAKAS}^{HASH} = 1) - 1\right|$, in which $P(\cdot)$ means the probability of $EXP1_{E,BAKAS}^{HASH}$. The advantage function for algorithm $EXP1_{E,BAKAS}^{HASH}$ becomes $Adv1(et_1, q_{Reveal}) = \max_E\{Success1\}$, in which the maximum for adversary E depends on the execution time et_1 and number of queries q_{Reveal} made to the oracle $Reveal$. The proposed scheme is provably secure against adversary E, if $Adv1(et_1, q_{Reveal}) \leq \varepsilon_1$, for any sufficiently small $\varepsilon_1 > 0$. If adversary E has the capacity to retrieve x from the hash function $y = h_1(x)$, he can easily retrieve the identity ID_i, secret key s, and session key sk_i to win the game. However, it is a computationally infeasiblebproblem to derive the inputs of hash function. Therefore $\max_E\{Success1\} = Adv1(et_1, q_{Reveal}) \leq \varepsilon_1$, for any sufficiently small $\varepsilon_1 > 0$. In conclusion, our scheme is provably secure against the adversary E for retrieving the identity ID_i, secret key s, and session key sk_i.

Table 3 Algorithm $EXP1^{HASH}_{E,BAKAS}$

1. Eavesdrop the login request message $\{CID_i, R_1, R_2, T_i\}$ in the login phase,
in which $CID_i = ENC_x(ID_i||k_u)$, $R_1 = ID_i \oplus T_u(A_i)$, $R_2 = h_1(ID_i||A_i||T_u(A_i)||T_i)$ and $A_i = h_1(ID_i||s)$.
2. Apply the oracle *Reveal* to retrieve $ID_i^I, A_i^I, T_u(A_i)^I$ and T_i^I from $Reveal(R_2) \rightarrow (ID_i^I||A_i^I||T_u(A_i)^I||T_i^I)$.
3. Further apply the oracle *Reveal* to retrieve ID_i^{II} and s^{II} from $Reveal(A_i^I) \rightarrow (ID_i^{II}||s^{II})$.
4. Eavesdrop the authentication request message $\{Auth_S, E_i\}$ during the authentication phase,
where $Auth_S = h_1(A_i||T_v(A_i)||sk_i)$ and $E_i = T_v(A_i) \oplus ID_i$.
5. Apply the oracle *Reveal* to retrieve $A_i^{II}, T_v(A_i)^{II}$ and sk_i^{II} from $Reveal(Auth_S) \rightarrow (A_i^{II}||T_v(A_i^{II})||sk_i^{II})$.
6. **if** $(A_i^I = A_i^{II})$ and $(ID_i^I = ID_i^{II})$ **then**
7. Accept ID_i^I, s^{II} and sk_i^{II} as the identity ID_i of user U_i, secret key s of server S,
and session key sk_i between U_i and S, respectively.
8. **return** 1 (Success)
9. **else**
10. **return** 0 (Failure)
11. **end if**

Theorem 2 *Under the assumption that hash function $h_1(\cdot)$ closely behaves like the oracle Reveal, our scheme is provably secure against adversary E for deriving the password PW_i of user U_i, even if smart card SC_i is stolen.*

Proof We need to construct the adversary E who can retrieve the password PW_i. Adversary E extracts all the information $\{B_i, CID_i, P_i, V_i\}$ from the stolen smart card SC_i and adopts the oracle *Reveal* to execute the experimental algorithm $EXP2^{HASH}_{E,BAKAS}$. In particular, details of algorithm $EXP2^{HASH}_{E,BAKAS}$ are described in the Table 4. □

We define the success probability of $EXP2^{HASH}_{E,BAKAS}$ as $Success2 = \left|P(EXP2^{HASH}_{E,BAKAS} = 1) - 1\right|$, where $P(\cdot)$ means the probability of $EXP2^{HASH}_{E,BAKAS}$. The advantage function for algorithm $EXP2^{HASH}_{E,BAKAS}$ becomes $Adv2(et_2, q_{Reveal}) = \max_E\{Success2\}$, where the

Table 4 Algorithm $EXP2^{HASH}_{E,BAKAS}$

1. Extract all the information $\{B_i, CID_i, P_i, V_i\}$ from the stolen smart card SC_i with the assistance of side channel attacks, where $V_i = h_1(ID_i||RPW_i)$ and $RPW_i = h_1(PW_i||R_i)$.
2. Apply the oracle *Reveal* to retrieve ID_i^I and RPW_i^I from $Reveal(V_i) \rightarrow (ID_i^I||RPW_i^I)$.
3. Eavesdrop the login request message $\{CID_i, R_1, R_2, T_i\}$ during the login phase,
in which $CID_i = ENC_x(ID_i||k_u)$, $R_1 = ID_i \oplus T_u(A_i)$ and $R_2 = h_1(ID_i||A_i||T_u(A_i)||T_i)$.
4. Apply the oracle *Reveal* to retrieve ID_i^{II}, A_i^{II}, $T_u(A_i)^{II}$ and T_i^{II}
from $Reveal(R_2) \rightarrow (ID_i^{II}||A_i^{II}||T_u(A_i^{II})||T_i^{II})$.
5. **if** $(ID_i^I = ID_i^{II})$ **then**
6. Apply the oracle *Reveal* to retrieve PW_i^I and R_i^I from $Reveal(RPW_i^I) \rightarrow (PW_i^I||R_i^I)$.
7. Accept PW_i^I as the password PW_i of user U_i.
8. **return** 1 (Success)
9. **else**
10. **return** 0 (Failure)
11. **end if**

maximum for adversary E depends on the execution time et_2 and number of queries q_{Reveal} made to the oracle $Reveal$. The presented scheme is provably secure against the adversary E, if $Adv2(et_2, q_{Reveal}) \leq \varepsilon_2$, for any sufficiently small $\varepsilon_2 > 0$. If adversary E is able to retrieve x from the hash function $y = h_1(x)$, he can easily retrieve the password PW_i to win the game. However, it is a computationally infeasible problem to retrieve the inputs of hash function. Thus $\max_E\{Success2\} = Adv2(et_2, q_{Reveal}) \leq \varepsilon_2$, for any sufficiently small $\varepsilon_2 > 0$. Above all, our scheme is provably secure against the adversary E for retrieving the password PW_i.

6.4 Verifying the security with BAN logic

The Burrows-Abadi-Needham (BAN) logic includes a set of rules, which is applied to define and analyze the information exchange schemes [42]. During this section, we introduce some symbols and notations of BAN logic in the Table 5 and adopt the BAN logic to verify that a session key between U_i and S is correctly generated in our authentication scheme.

The BAN logical postulates

1. The message-meaning rule, that is $\frac{A|\equiv A \overset{K}{\longleftrightarrow} B, A \lhd \{X\}_K}{A|\equiv B|\sim X}$. In particular, if A believes that session key K is shared by A and B, and A sees that statement X is encrypted with session key K, then A believes that B said the statement X.
2. The nonce-verification rule, that is $\frac{A|\equiv \#X, A|\equiv B|\sim X}{A|\equiv B|\equiv X}$. In detail, if A believes that statement X is fresh and B said the statement X, then A believes that B believes the statement X.
3. The belief rule, that is $\frac{A|\equiv X, A|\equiv Y}{A|\equiv (X,Y)}$. Particularly, if A believes statement X and statement Y, then A believes (X, Y).
4. The fresh conjuncatenation rule, that is $\frac{A|\equiv \#X}{A|\equiv \#(X,Y)}$. In particular, if A believes that statement X is fresh, then A believes (X, Y) is fresh.
5. The jurisdiction rule, that is $\frac{A|\equiv B \Rightarrow X, A|\equiv B|\equiv X}{A|\equiv X}$. In detail, if A believes that B has the jurisdiction over statement X and B believes the truth of statement X, then A believes the statement X.

The idealized scheme

$$U_i :< ID_i >_{\{U_i \overset{A_i}{\longleftrightarrow} S\}_u}, (ID_i, A_i)_{\{U_i \overset{A_i}{\longleftrightarrow} S\}_u}, (U_i \overset{sk_i}{\longleftrightarrow} S, \{U_i \overset{A_i}{\longleftrightarrow} S\}_v)_{U_i \overset{A_i}{\longleftrightarrow} S}.$$

$$S :< ID_i >_{\{U_i \overset{A_i}{\longleftrightarrow} S\}_v}, (U_i \overset{sk_i}{\longleftrightarrow} S, \{U_i \overset{A_i}{\longleftrightarrow} S\}_u)_{U_i \overset{A_i}{\longleftrightarrow} S}.$$

The establishment of security goals

$g1.$ $U_i| \equiv S| \equiv U_i \overset{sk_i}{\longleftrightarrow} S$

$g2.$ $U_i| \equiv U_i \overset{sk_i}{\longleftrightarrow} S$

$g3.$ $S| \equiv U_i| \equiv U_i \overset{sk_i}{\longleftrightarrow} S$

$g4.$ $S| \equiv U_i \overset{sk_i}{\longleftrightarrow} S$

Table 5 Symbols and notions in the BAN logic

Symbol	Notion
$A\mid\equiv X$	A believes the statement X.
$A\overset{K}{\longleftrightarrow}B$	The session key K is shared by A and B.
$\#X$	The statement X is fresh.
$A\triangleleft X$	A sees the statement X.
$A\mid\sim X$	A said the statement X.
$\{X,Y\}_K$	The statement X and Y are encrypted with session key K.
$(X,Y)_K$	The statement X and Y are hashed with session key K.
$<X>_K$	The statement X is XORed with session key K.

The initiative premises

$p1.$ $U_i\mid\equiv\#u$
$p2.$ $S\mid\equiv\#v$
$p3.$ $U_i\mid\equiv U_i\overset{A_i}{\longleftrightarrow}S$
$p4.$ $S\mid\equiv U_i\overset{A_i}{\longleftrightarrow}S$
$p5.$ $U_i\mid\equiv S\Rightarrow(U_i\overset{sk_i}{\longleftrightarrow}S)$
$p6.$ $S\mid\equiv U_i\Rightarrow(U_i\overset{sk_i}{\longleftrightarrow}S)$

The security analysis

$a1.$ Since $p3$ and $U_i\triangleleft(U_i\overset{sk_i}{\longleftrightarrow}S,\{U_i\overset{A_i}{\longleftrightarrow}S\}_u)_{U_i\overset{A_i}{\longleftrightarrow}S}$, we adopt the message-meaning rule to acquire $U_i\mid\equiv S\mid\sim(U_i\overset{sk_i}{\longleftrightarrow}S,\{U_i\overset{A_i}{\longleftrightarrow}S\}_u)$.
$a2.$ Because of $p1$ and $a1$, we use the fresh conjuncatenation rule and nonce-verification rule to get $U_i\mid\equiv S\mid\equiv(U_i\overset{sk_i}{\longleftrightarrow}S,\{U_i\overset{A_i}{\longleftrightarrow}S\}_u)$.
$g1.$ Since $a2$ and $p3$, we apply the belief rule to acquire $U_i\mid\equiv S\mid\equiv U_i\overset{sk_i}{\longleftrightarrow}S$.
$g2.$ Because of $p5$ and $g1$, we adopt the jurisdiction rule to get $U_i\mid\equiv U_i\overset{sk_i}{\longleftrightarrow}S$.
$a3.$ Since $p4$ and $S\triangleleft(U_i\overset{sk_i}{\longleftrightarrow}S,\{U_i\overset{A_i}{\longleftrightarrow}S\}_v)_{U_i\overset{A_i}{\longleftrightarrow}S}$, we use the message-meaning rule to acquire $S\mid\equiv U_i\mid\sim(U_i\overset{sk_i}{\longleftrightarrow}S,\{U_i\overset{A_i}{\longleftrightarrow}S\}_v)$.
$a4.$ Because of $p2$ and $a3$, we apply the fresh conjuncatenation rule and nonce-verification rule to get $S\mid\equiv U_i\mid\equiv(U_i\overset{sk_i}{\longleftrightarrow}S,\{U_i\overset{A_i}{\longleftrightarrow}S\}_v)$.
$g3.$ Since $a4$ and $p4$, we adopt the belief rule to acquire $S\mid\equiv U_i\mid\equiv U_i\overset{sk_i}{\longleftrightarrow}S$.
$g4.$ Because of $g3$ and $p6$, we use the jurisdiction rule to get $S\mid\equiv U_i\overset{sk_i}{\longleftrightarrow}S$.

Above all, results show that our scheme is able to generate a session key sk_i correctly between $U_i and S$.

6.5 Functionality analysis

A variety of requirements in the respect of functionality for authentication and key agreement schemes have been suggested in the previous studies. During this section, we show that our scheme provides these functionalities which are described below.

Biometric information protection In the conventional schemes, biometric information of user U_i is directly stored in the smart card SC_i so that adversary E obtains the biometrics from the lost or stolen smart cards with the help of side channel attacks. We adopt a secure mechanism to solve this problem, where the nearly random string R_i is protected by one-way hash function and is extracted from the biometrics BIO_i by fuzzy extractor. It makes impossible for E to acquire the biometric information. Therefore, our scheme provides the biometric information protection.

Fast error detection It is essential to provide the fast error detection, which makes smart card SC_i examine the incorrect passwords or any other mistakes immediately. In the login and password change phases, SC_i detects the errors quickly, such as the incorrect identities, inaccurate passwords and false biometric information without the assistance of server S. As a result, the proposed scheme provides the fast error detection.

Mutual authentication Mutual authentication means that both communicating parties authenticate each other. In the presented scheme, both user U_i and server S approve each other by applying u, v, x, sk_i and A_i. During the authentication phase, U_i authenticates S by checking whether $h_1(A_i||T_v(A_i)||sk_i) = Auth_S$ holds. And S verifies whether $Auth_U$ is consistent with $h_1(sk_i||T_u(A_i)||A_i)$ to authenticate the U_i. In conclusion, our scheme achieves the mutual authentication.

Session key agreement For the session key agreement, user U_i and server S establish a session key which is adopted to protect the subsequent communication. In the proposed scheme, session key $sk_i = h_2(T_u(A_i), T_v(A_i), T_{uv}(A_i))$ is generated by U_i and S, in which u and v are different in every session. Above all, session keys are various in the different sessions so that it is hard for adversary E to retrieve the previous session keys from the intercepted communication messages.

Secure and simple password modification According to secure and simple password modification, user U_i has the ability to change their passwords without the help of any third trusted party and the authenticity is verified by his smart card SC_i. In the proposed scheme, U_i changes the password independently and does not need any communication with server S. Furthermore, SC_i examines whether $h_1(ID_i||RPW_i) = V_i$ holds during each password change phase so that adversary E is unable to change the password even if he acquires the smart card and password. Thus, the presented scheme provides the secure and simple password modification.

User re-registration/revocation User U_i sends a re-registration/revocation request message to the server S through a secure channel if he wants to re-register or revoke his privilege. And then S helps U_i achieve the re-registration or revocation by modifying $\langle ID_i, N_i \rangle$ in the database. In conclusion, user re-registration/revocation improves the performance of practical applications, which makes our scheme more robust than other related schemes.

Anonymity Anonymity means that user U_i's real identity is not disclosed to other unauthorized parties. In the proposed scheme, dynamic identity CID_i is computed from $CID_i = ENC_x(ID_i||k_u)$, in which x and k_u are not leaked out from the intercepted messages via public channels. Thus, adversary E cannot calculate the U_i's identity ID_i without x and k_u. Server S retrieves ID_i from $(ID_i||k_u) = ENC_x(CID_i)$. However, only authorized server

S confirms the real identity of U_i. Above all, E is unable to obtain the U_i's real identity, but U_i is accurately authenticated by S.

Perfect forward secrecy The perfect forward secrecy implies that a session key derived from a set of long-term keys will not be retrieved even if one of the user's long-term keys is compromised in the future. In the proposed scheme, a session key between user U_i and server S is acquired below.

$$(ID_i||k_u) = ENC_x(CID_i),$$
$$T_u(A_i) = R_1 \oplus ID_i,$$
$$T_v(A_i) = ID_i \oplus E_i,$$
$$sk_i = h_2(T_u(A_i), T_v(A_i), T_{uv}(A_i)).$$

Although U_i's long-term key k_u is compromised, adversary E is not able to calculate x, u and v so that he is unable to retrieve ID_i, $T_u(A_i)$, $T_v(A_i)$ and $T_{uv}(A_i)$ to calculate session keys between U_i and S. Therefore, the presented scheme achieves the perfect forward secrecy.

6.6 Comparisons with related schemes

During this subsection, we compare the resistance, functionality and performance of our scheme with other related authentication schemes, such as Guo et al.'s scheme [15], Lin et al.'s scheme [40], Jiang et al.'s scheme [29] and Lu et al.'s scheme [42].

According to the Table 6, it shows the resistance comparison of various related authentication schemes. We define the following notations: R1: resistance to replay attack, R2: resistance to modification attack, R3: resistance to stolen-verifier attack, R4: resistance to password guessing attack, R5: resistance to user impersonation attack, R6: resistance to server masquerade attack, R7: resistance to insider attack, R8: resistance to Denial-of-Service attack and R9: resistance to stolen smart card attack in the Table 6. It can be seen that our scheme provides the all resistance requirements and is more secure.

Table 7 lists the functionality comparison of the presented scheme with other related schemes, where we apply the following notations: F1: biometric information protection, F2: fast error detection, F3: mutual authentication, F4: session key agreement, F5: secure and simple password modification, F6: user re-registration/revocation, F7: anonymity and F8: perfect forward secrecy. And then we further compare our scheme with Moon et al.'s scheme

Table 6 The resistance comparison

	Guo et al.'s [15]	Lin et al.'s [40]	Jiang et al.'s [29]	Lu et al.'s [42]	Ours
R1	Yes	Yes	Yes	Yes	Yes
R2	Yes	Yes	Yes	Yes	Yes
R3	Yes	Yes	Yes	Yes	Yes
R4	No	No	No	Yes	Yes
R5	No	No	No	No	Yes
R6	Yes	Yes	Yes	No	Yes
R7	No	Yes	Yes	Yes	Yes
R8	No	No	No	No	Yes
R9	Yes	No	No	Yes	Yes

Table 7 The functionality comparison

	Guo et al.'s [15]	Lin et al.'s [40]	Jiang et al.'s [29]	Lu et al.'s [42]	Moon et al.'s [48]	Ours
F1	No	No	No	No	No	Yes
F2	No	No	No	Yes	Yes	Yes
F3	Yes	Yes	Yes	Yes	Yes	Yes
F4	Yes	No	No	Yes	Yes	Yes
F5	No	No	Yes	No	Yes	Yes
F6	No	No	No	No	No	Yes
F7	No	Yes	Yes	No	Yes	Yes
F8	No	No	No	Yes	Yes	Yes

[48] which is another improved scheme. The result demonstrates that our scheme provides the enough functionalities and is more practical for multimedia medicine information systems.

We compare our scheme with these relevant authentication schemes for computational costs involved in the both login phase and authentication phase. In order to measure the computation complexity, we treat the one-way hash function operation, extended Chebyshev chaotic map operation and symmetric encryption/decryption operation as the time complexity since the XOR operation requires very little computational cost, in which T_h denotes the time of executing a one-way hash function, definition of T_s is the time of running a symmetric encryption/decryption operation and T_c means the time of performing an extended Chebyshev chaotic map, respectively. According to the Xue et al.'s work [56], we learn that the executing time of a one-way hash function is 0.2 ms on average, the running time of a symmetric encryption/decryption operation is about 0.45 ms and the performing time of an extended Chebyshev chaotic map is around 32.2 ms in the operational environment (CPU: 3.2 GHz, RAM: 3.0 G). Table 8 and Fig. 5 show the computation cost comparison among our scheme and other related schemes in terms of the computation cost. In the Table 8, we use the notations as follow: C1: computation overhead in the user side, C2: execution overhead in the user side, C3: computation overhead in the server side, C4: execution overhead in the server side and C5: total execution overhead. The computation cost requested in the presented scheme is lower than that in the Guo et al.'s scheme, Lin et al.'s scheme and Jiang et al.'s scheme.

To estimate the communication cost, we assume the length of security parameters, such as, bit length of timestamp is 16, bit length of user identity is 160, bit length of random number is 160, output bit length of hash function is 160 and output bit length of extended Chebyshev chaotic map is 160. In our scheme, user U_i transmits the login

Table 8 The computation cost comparison

	Guo et al.'s [15]	Lin et al.'s [40]	Jiang et al.'s [29]	Lu et al.'s [42]	Moon et al.'s [48]	Ours
C1	$2T_h+2T_s+3T_c$	$3T_h+2T_s+3T_c$	$2T_h+1T_s+3T_c$	$7T_h+2T_c$	$7T_h+2T_c$	$7T_h+2T_c$
C2	97.90 ms	98.10 ms	97.45 ms	65.80 ms	65.80 ms	65.80 ms
C3	$2T_h+3T_s+3T_c$	$2T_h+3T_s+3T_c$	$1T_h+2T_s+3T_c$	$5T_h+2T_c$	$7T_h+2T_c$	$5T_h+1T_s+2T_c$
C4	98.35 ms	98.35 ms	97.70 ms	65.40 ms	65.80 ms	65.85 ms
C5	196.25 ms	196.45 ms	195.15 ms	131.20 ms	131.60 ms	131.65 ms

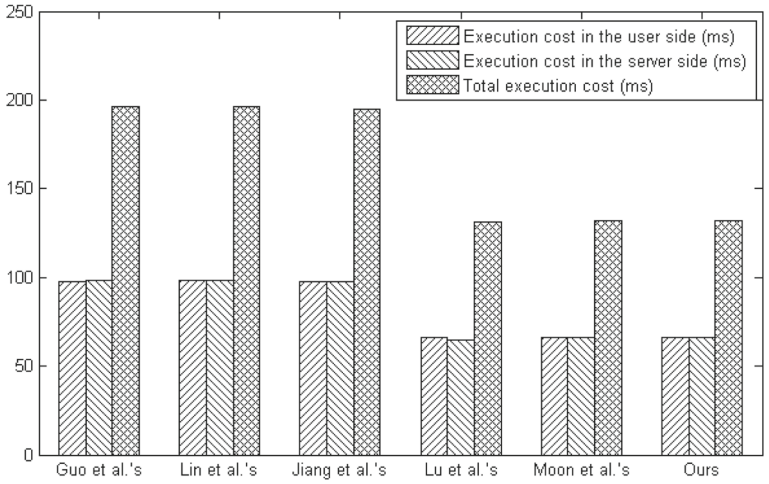

Fig. 5 The computation cost comparison

request message $\{CID_i, R_1, R_2, T_i\}$ to server S during the login phase, and its length is $[(160 + 160) + 160 + 160 + 16]/8 = 82$ bytes. And during the stage of authentication, communication cost is $[(160 + 160) + 160]/8 = 60$ bytes, which contains the authentication request messages $\{Auth_S, E_i\}$ and $\{Auth_U\}$. So total communication cost of the proposed scheme is $82 + 60 = 142$ bytes. Analogously, we estimate the communication cost of other related schemes. In order to measure the storage requirement, we consider the information stored in the smart card and compute the byte length of stored message as storage cost. In the proposed scheme, stored message $\{B_i, CID_i, P_i, V_i\}$ requires $[160+(160+160)+160+160]/8 = 100$ bytes. Similarly, we measure the storage requirement of other relevant schemes. As shown in the Table 9 and Fig. 6, we demonstrate the comparison regarding on the communication and storage costs of various authentication schemes. We provide the notations below: S1: communication overhead in the login phase, S2: communication overhead in the authentication phase, S3: total communication overhead and S4: storage overhead in the Table 9. With the same level of communication overhead and storage cost, the proposed scheme obviously has advantages in the computation complexity by considering the computation overhead between other related schemes and ours. From the results of these comparisons given above, we conclude that our scheme has better efficiency among resistance, functionality and performance than other related authentication schemes.

Table 9 The communication and storage costs comparison

	Guo et al.'s [15]	Lin et al.'s [40]	Jiang et al.'s [29]	Lu et al.'s [42]	Moon et al.'s [48]	Ours
S1	60 bytes	40 bytes	40 bytes	80 bytes	80 bytes	82 bytes
S2	20 bytes	20 bytes	42 bytes	60 bytes	60 bytes	60 bytes
S3	80 bytes	60 bytes	82 bytes	140 bytes	140 bytes	142 bytes
S4	80 bytes	60 bytes	80 bytes	40 bytes	60 bytes	100 bytes

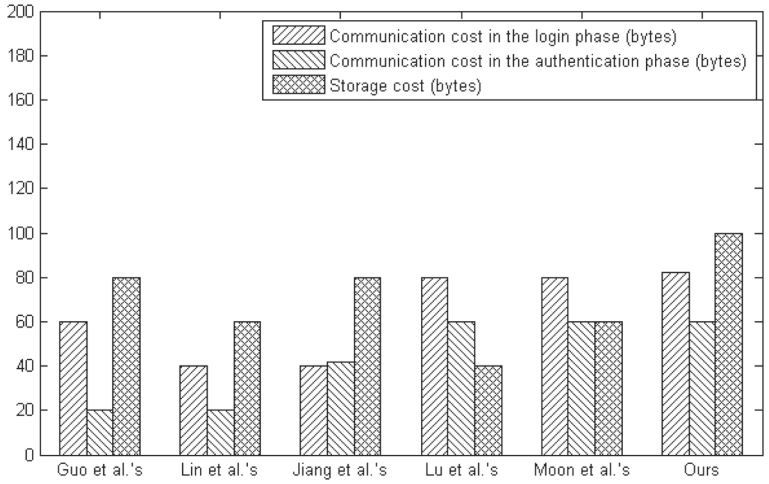

Fig. 6 The communication and storage costs comparison

7 Conclusion

With the increase of security requirements, a great number of authentication schemes come to be widely deployed in the multimedia medicine information systems over the last several years. In this study, we analyze the weaknesses of Lu et al.'s scheme. We find that there are flaws in the both login phase and password change phase. And we show that their scheme is vulnerable to the Denial-of-Service attack, user impersonation attack and server masquerade attack, which also fails to achieve the user anonymity. Based on the cryptanalysis of Lu et al.'s scheme, we retain the useful properties of their scheme to propose a robust biometrics based authentication and key agreement scheme using extended Chebyshev chaotic maps. The presented scheme satisfies the desirable security requirements which are demonstrated in the informal and formal security analysis, respectively. Furthermore, the proposed scheme provides some significant features which are not considered in most of the related schemes, for example, biometric information protection and user re-registration or revocation. With the same level of computation overhead, communication cost and storage space, our scheme provides some more secure properties and significant functionalities. In conclusion, we confirm that the proposed scheme resists the known attacks and is efficient for practical applications in the multimedia medicine information systems.

Acknowledgments Authors thank the editor and reviewers a lot for their valuable suggestions. This research is supported by the Major Program of National Natural Science Foundation of China (No.: 11290141), the National Natural Science Foundation of China (No.: 61402030), and the Fundamental Research of Civil Aircraft (No.: MJ-F-2012-04).

References

1. Amin R, Islam SKH, Biswas GP, Khan MK, Obaidat MS (2015) Design and analysis of an enhanced patient-server mutual authentication protocol for telecare medical information system. J Med Syst 39(11):1–20

2. Arshad H, Teymoori V, Nikooghadam M, Abbassi H (2015) On the security of a two-factor authentication and key agreement scheme for telecare medicine information systems. J Med Syst 39(8):1–10
3. Benhammadi F, Bey KB (2014) Password hardened fuzzy vault for fingerprint authentication system. Image Vision Comput 32(8):487–496
4. Bergamo P, D'Arco P, De Santis A, Kocarev L (2005) Security of public-key cryptosystems based on Chebyshev polynomials. IEEE Trans Circuits Syst Regul Pap 52(7):1382–1393
5. Chaudhry SA (2015) A secure biometric based multi-server authentication scheme for social multimedia networks. Multimedia Tools and Applications:1–21
6. Chen TH, Hsiang HC, Shih WK (2011) Security enhancement on an improvement on two remote user authentication schemes using smart cards. Futur Gener Comput Syst 27(4):377–380
7. Dang Q (2013) Changes in federal information processing standard (FIPS) 180-4, secure hash standard. Cryptologia 37(1):69–73
8. Das AK (2011) Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. IET Inf Secur 5(3):145–151
9. Das AK, Bruhadeshwar B (2013) An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system. J Med Syst 37(5):1–17
10. Das AK, Goswami A (2014) An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. J Med Syst 38(6):1–19
11. David DB (2016) Mutual authentication scheme for multimedia medical information systems. Multimedia Tools and Applications:1–19
12. Dodis Y, Kanukurthi B, Katz J, Reyzin L, Smith A (2012) Robust fuzzy extractors and authenticated key agreement from close secrets. IEEE Trans Inf Theory 58(9):6207–6222
13. Dodis Y, Ostrovsky R, Reyzin L, Smith A (2008) Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM J Comput 38(1):97–139
14. Dolev D, Yao A (1983) On the security of public key protocols. IEEE Trans Inf Theory 29(2):198–208
15. Guo C, Chang CC (2013) Chaotic maps-based password-authenticated key agreement using smart cards. Commun Nonlinear Sci Numer Simul 18(6):1433–1440
16. Hao XH, Wang JT, Yang QH, Yan XP, Li P (2013) A chaotic map-based authentication scheme for telecare medicine information systems. J Med Syst 37(2):1–7
17. He DB, Chen JH, Zhang R (2012) A more secure authentication scheme for telecare medicine information systems. J Med Syst 36(3):1989–1995
18. He DB, Khan MK, Kumar N (2015) A new handover authentication protocol based on bilinear pairing functions for wireless networks. Int J Ad Hoc Ubiquitous Comput 18(1-2):67–74
19. He DB, Kumar N, Chilamkurti N, Lee JH (2014) Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. J Med Syst 38(10):1–6
20. He DB, Kumar N, Shen H (2015) One-to-many authentication for access control in mobile pay-TV systems. SCIENCE CHINA Inf Sci 59(5):1–14
21. He DB, Kumar N, Wang HQ, Wang LN, Choo KKR, Vinel A (2016) A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network. IEEE Trans Dependable Secure Comput PP(99):1–13
22. He DB, Zeadally S, Kumar N, Lee JH (2016) Anonymous authentication for wireless body area networks with provable security. IEEE Syst J PP(99):1–12
23. He DB, Zeadally S, Wu LB (2015) Certificateless public auditing scheme for cloud-assisted wireless body area networks. IEEE Syst J PP(99):1–10
24. Huang H, Cao ZF (2011) IDOAKE: strongly secure ID-based one-pass authenticated key exchange protocol. Security and Communication Networks 4(10):1153–1161
25. Islam SKH (2014) Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps. Nonlinear Dyn 78(3):2261–2276
26. Islam SKH, Biswas GP (2012) A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. Annals of Telecommunications-Annales des Té,lécommunications 67(11-12):547–558
27. Islam SKH, Biswas GP (2013) Provably secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography. Int J Comput Math 90(11):2244–2258
28. Islam SKH, Khan MK (2014) Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems. J Med Syst 38(10):1–16
29. Jiang Q, Ma JF, Lu X, Tian YL (2014) Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. J Med Syst 38(2):1–8
30. Kim JS, Kwak J (2015) Design of USIM-based secure user authentication scheme in a mobile office environment. Multimedia Tools and Applications:1–16

31. Kocher P, Jaffe J, Jun B, Rohatgi P (2011) Introduction to differential power analysis. J Cryptogr Eng 1(1):5–27
32. Kounga G, Mitchell CJ, Walter T (2012) Generating certification authority authenticated public keys in ad hoc networks. Security and Communication Networks 5(1):87–106
33. Kumari S, Khan MK, Kumar R (2013) Cryptanalysis and improvement of 'a privacy enhanced scheme for telecare medical information systems'. J Med Syst 37(4):1–11
34. Lamport L (1981) Password authentication with insecure communication. Commun ACM 24(11):770–772
35. Lee TF (2014) Verifier-based three-party authentication schemes using extended chaotic maps for data exchange in telecare medicine information systems. Comput Methods Prog Biomed 117(3):464–472
36. Li CT, Lee CC, Weng CY, Fan CI (2015) A secure dynamic identity based authentication protocol with smart cards for multi-server architecture. J Inf Sci Eng 31(6):1975–1992
37. Li CT, Hwang MS (2010) An efficient biometrics-based remote user authentication scheme using smart cards. J Netw Comput Appl 33(1):1–5
38. Li X, Niu JW, Kumari S, Khan MK, Liao JG, Liang W (2015) Design and analysis of a chaotic maps-based three-party authenticated key agreement protocol. Nonlinear Dyn 80(3):1209–1220
39. Li X, Niu JW, Ma J, Wang WD, Liu CL (2011) Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. J Netw Comput Appl 34(1):73–79
40. Lin HY (2015) Improved chaotic maps-based password-authenticated key agreement using smart cards. Commun Nonlinear Sci Numer Simul 20(2):482–488
41. Lou DC, Lee TF, Lin TH (2015) Efficient biometric authenticated key agreements based on extended chaotic maps for telecare medicine information systems. J Med Syst 39(5):1–10
42. Lu YR, Li LX, Peng HP, Xie D, Yang YX (2015) Robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. J Med Syst 39(6):1–10
43. Lu YR, Li LX, Peng HP, Yang YX (2015) An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem. J Med Syst 39(3):1–8
44. Lu YR, Li LX, Yang X, Yang YX (2015) Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards. PLoS One 10(5):e0126323
45. Messerges TS, Dabbish EA, Sloan RH (2002) Examining smart-card security under the threat of power analysis attacks. IEEE Trans Comput 51(5):541–552
46. Mishra D, Das AK, Mukhopadhyay S (2016) A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card. Peer-to-Peer Networking and Applications 9(1):171–192
47. Mishra D, Srinivas J, Mukhopadhyay S (2014) A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information systems. J Med Syst 38(10):1–10
48. Moon J, Choi Y, Kim J, Won D (2016) An improvement of robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps. J Med Syst 40(3):1–11
49. Siddiqui Z, Abdullah AH, Khan MK, Alghamdi AS (2014) Smart environment as a service: Three factor cloud based user authentication for telecare medical information system. J Med Syst 38(1):1–14
50. Ustaoğlu B (2011) Integrating identity-based and certificate-based authenticated key exchange protocols. Int J Inf Secur 10(4):201–212
51. Wei JH, Hu XX, Liu WF (2012) An improved authentication scheme for telecare medicine information systems. J Med Syst 36(6):3597–3604
52. Wen FT (2014) Guo, DL. An improved anonymous authentication scheme for telecare medical information systems. J Med Syst 38(5):1–11
53. Wu ZY, Lee YC, Lai FP, Lee HC, Chung YF (2012) A secure authentication scheme for telecare medicine information systems. J Med Syst 36(3):1529–1535
54. Xu J, Zhu WT, Feng DG (2011) An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. Comput Commun 34(3):319–325
55. Xu X, Zhu P, Wen QY, Jin ZP, Zhang H, He L (2014) A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. J Med Syst 38(1):1–7
56. Xue KP, Hong PL (2012) Security improvement on an anonymous key agreement protocol based on chaotic maps. Commun Nonlinear Sci Numer Simul 17(7):2969–2977
57. Yang TC, Lo NW, Liaw HT, Wu WC (2016) A secure smart card authentication and authorization framework using in multimedia cloud. Multimedia Tools and Applications:1–23
58. Yau WC, Phan RCW (2013) Security analysis of a chaotic map-based authentication scheme for telecare medicine information systems. J Med Syst 37(6):1–9

59. Zhang LH (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos, Solitons Fractals 37(3):669–674
60. Zhang LP, Zhu SH (2015) Robust ECC-based authenticated key agreement scheme with privacy protection for telecare medicine information systems. J Med Syst 39(5):1–11
61. Zhang M, Zhang JS, Zhang Y (2015) Remote three-factor authentication scheme based on Fuzzy extractors. Security and Communication Networks 8(4):682–693

Chengqi Wang received the B.S. degree with distinction from Beihang University, Beijing, China, in 2012. He is currently a Ph.D. candidate at Key Laboratory of Mathematics, Informatics and Behavioral Semantics and School of Mathematics and Systems Science, Beihang University. His research interests include network security and applied cryptography.

Xiao Zhang received the Ph.D degree from Beihang University, Beijing, China, in 2013. She is currently the associate professor of Mathematics at Beihang University and the member of Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education. Her research interests include cryptography, information security and complex information system.

Zhiming Zheng received the Ph.D. degree from Peking University, Beijing, China, in 1987. He is currently the Professor of Mathematics at Beihang University and the Director of Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education. His research interests include information security, complex information system, and dynamic system. He is the Editor in Chief of the journal Mathematical Biosciences and Engineering published by SPRINGER, and the journal Mathematics in Computer Science published by BIRKHAUSER.