International Journal of Security and Its Applications
Vol. 11, No. 9 (2017), pp.41-58
http://dx.doi.org/10.14257/ijsia.2017.11.9.04

Design of a Secure Dynamic Identity Authentication Scheme for Health Internet of Things

Chengqi Wang[1], Xiao Zhang[1,*], Lijia Xie[1] and Zhiming Zheng[1]

[1]*Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education, and School of Mathematics and Systems Science, Beihang University, Beijing 100191, China*
[*]*09621@buaa.edu.cn*

Abstract

To satisfy the security requirements of patients' privacy and data's security for health Internet of Things (IoT), various authentication schemes are proposed as guaranteed countermeasures. In particular, Wang et al. built an identity-based authentication scheme with extended Chebyshev chaotic maps. Nevertheless, considering service misuse attack and Denial-of-Service attack, Wang et al.'s method works inadequately. Also it is insufficient to provide efficient password change phase, fast error detection and session key agreement. As a remedy, we propose a novel dynamic identity authenticated key agreement scheme. Our scheme achieves resistance to the known attacks in order to meet the desirable security requirements. Furthermore, the presented scheme practically enables both user revocation/re-registration and biometric information protection, which are significant features ignored by most previous schemes. We confirm the effectiveness of our scheme via comprehensive comparisons in terms of resistance, functionality and performance.

Keywords*: Health Internet of Things, Authentication, Key agreement, Biometrics*

1. Introduction

As a pervasive infrastructure, Internet of Things (IoT) has been enhanced in the services' quality due to the advances in the information technology [1-2]. Recently, health IoT becomes more popular as emerging healthcare applications which are equipped with communication capabilities and contributes to more electronic medical services for example clinical diagnosis and health records. Thus a convenient way for communication between doctors and patients over public channels is able to be established [3–4]. Note that health IoT is almost implemented and patients' information is transmitted over the public networks. In other words, hackers, spywares and other threats in the public networks migrate to the health IoT. When facing multiple kinds of attacks, how to ensure the security and privacy of transmitted information becomes a great challenge [5-6]. In response, many authentication algorithms have been proposed to guarantee the secure communication between remote participants [7-12]. According to applied evidences, existing proposals can be separated into two categories, namely, certificate-based and identity-based [13-16]. Nevertheless, without high requirements of both computational resource and storage space, identity-based authentication schemes are now more generally adopted than certificate-based ones in the health IoT in order to provide convenient health-care services.

Besides, there are still some vulnerabilities for two-factor identity-based authentication algorithms which apply tokens and passwords to guarantee the security [17-19]. Specifically, patients usually feel difficult to use random and long passwords. But short

Received (January 17, 2017), Review Result (August 22, 2017), Accepted (August 30, 2017)

ISSN: 1738-9976 IJSIA

passwords can be easily cracked by dictionary attack because of low entropy. Moreover, common side channel attacks, for instance SPA and DPA, makes it feasible to acquire sensitive information saved in smart cards [20]. To overcome these weaknesses, many research papers focus on combination of passwords, tokens and biometrics, namely three-factor, to improve the security [21-22]. Since biometric information is unique and unforgeable [23-24], users are not required to remember their biometric information. However, without professional recognition mechanisms, imprinted biometric characteristics which may not be accepted for the same user increase the probability of rejection [25-26]. Thus, more work about authenticated key agreement algorithms in health IoT needs to be built with three-factor.

Furthermore, Wang et al. [27] recently proposed an identity-based authentication scheme for health IoT to meet the problems of previous proposals. Unfortunately, based on cryptanalysis provided in this paper, we identify that their algorithm is still vulnerable to service misuse attack, Denial-of-Service attack and flaws exist in the password change phase. Also we show that Wang et al.'s scheme fails to achieve fast error detection and session key agreement. In addition, there is no consideration of the revocation or re-registration phase in their scheme. To address these issues, we propose a three-factor identity-based authenticated key agreement scheme, which is built upon extended chaotic maps. Our scheme improves Wang et al.'s proposal and satisfies desirable requirements. Compared with other related algorithms, with the same level of overhead, our scheme guarantees more properties and functionalities, especially biometric information protection.

Remaining of this paper is organized as below. First, we briefly introduce fuzzy extractor, extended Chebyshev chaotic map and threat assumptions applied in our proposal during next section. Section 3 and Section 4 reviews the Wang et al.'s scheme and discusses the weaknesses of their proposal, respectively. Next, we specify the details of our proposal in Section 5. Then section 6 provides the resistance, functionality and performance analysis of our algorithm. Lastly, we present our conclusion in Section 7.

2. Preliminaries

During this section, we basically describe the fuzzy extractor, extended Chebyshev chaotic map and threat assumptions for better understanding of our scheme.

2.1. Fuzzy Extractor

As can be seen in Fig. 1, mechanism of fuzzy extractor includes two procedures.

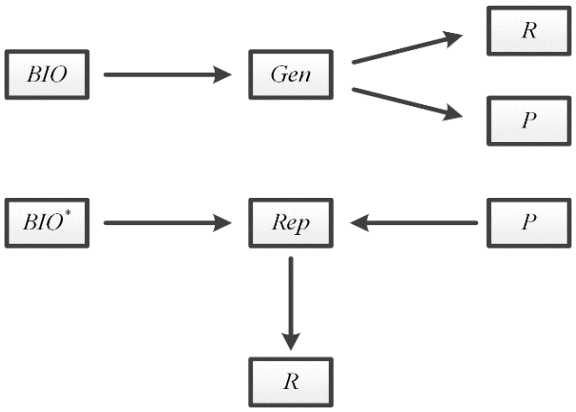


Figure 1. Mechanism of Fuzzy Extractor

Specifically, procedure *Gen* means a probabilistic generation function used to extract user's original biometrics input *BIO*. Its outputs cover nearly random binary string

$R \in \{0,1\}^l$ and auxiliary binary string $P \in \{0,1\}^*$. Analogously, procedure *Rep* denotes a deterministic reproduction function used to recover *R* with two inputs, namely, biometrics input BIO^* and corresponding string *P*. When $Gen(BIO) \to \langle R, P \rangle$ and $dis(BIO, BIO^*) \le t$, we obtain $Rep(BIO^*, P) = R$, in which error-tolerant technology makes it dependable to retrieve the string *R* from user's biometrics input BIO^*. Due to space constraints, we omit the details about the fuzzy extractor specified in the literature [25-26].

2.2. Extended Chebyshev Chaotic Map

In details, Chebyshev chaotic map $T_n(x)$ can be defined by following formula.

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

where $x = \cos\theta$ [28].

Furthermore, $T_n(x)$'s recurrence formula is defined as follows.

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

in which for any natural number $n \ge 2$, $T_0(x) = 1$ and $T_1(x) = x$.

As we know, Chebyshev chaotic map satisfies semi-group and commutative property under composition, namely, $T_r(T_s(x)) = T_s(T_r(x))$. The proof can be specified as follows.

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

in which for any natural number *s* and *r*.

Zhang [29] enhanced Chebyshev chaotic map in 2008. This paper [29] proved that the semi-group and commutative property under composition still hold when the interval extends to $(-\infty, +\infty)$. Hereby, we present the extended Chebyshev polynomial as follows.

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

in which $n \ge 2$, $x \in (-\infty, +\infty)$ and *p* is any large prime number. Similarly, $T_r(T_s(x)) = T_{rs}(x) = T_s(T_r(x)) \bmod p$ also holds.

There are two hard problems for extended Chebyshev polynomials [30], which we specify here as follows.

ECDLP: given *x*, *y* and *p*, finding an integer *r* which satisfies $y = T_r(x) \bmod p$ is hard.

ECDDHP: given $T_r(x)$, $T_s(x)$, $T_z(x)$ and *x*, determining whether $T_{rs}(x) = T_z(x) \bmod p$ holds is hard.

2.3. Threat Assumptions

We take side-channel attacks [20] and Dolev-Yao threat model [31] into consideration. And we list threat assumptions as below.

1. Attacker *E* might be a malicious user or an outsider in the health IoTs.
2. Attacker *E* eavesdrops on all transmitted messages between user U_i and server *S* via a public channel.
3. Attacker *E* enables to delete, modify, reroute and resend all eavesdropped messages.
4. Attacker *E* is able to extract sensitive information from stolen or obtained smart card SC_i by measuring the power consumption.

3. Review of Wang et al.'s Scheme

Wang et al.'s scheme [27] proceeds in four phases, namely, registration phase, login phase, verification phase and password change phase, respectively. Without loss of generality, server *S* selects a hash function $h(\cdot)$, generates a random variable $x \in [-1,1]$, selects a private key *s* and publishes $\{x, T_s(x), h(\cdot)\}$.

3.1. Registration Phase

1. The new user U_i chooses his identity ID_i and password PW_i. Then U_i generates a random integer t_i, computes $W_i = PW_i \oplus t_i$, and sends his registration request $\{ID_i, W_i\}$ to the server *S* via a secure channel.

2. Upon receiving this registration request, *S* calculates $H_i = h(s \| ID_i)$ and $n_i = h(W_i \| ID_i) \oplus H_i$, respectively. And *S* sends a smart card SC_i to user U_i, which includes $\{n_i, x, T_s(x)\}$ via a secure channel.

3. After obtaining the SC_i, U_i computes $N_i = h(ID_i \| PW_i) \oplus n_i \oplus h(W_i \| ID_i)$. Lastly, user U_i stores $\{N_i, x, T_s(x)\}$ into his smart card SC_i.

3.2. Login Phase

1. U_i inserts his SC_i into a smart card reader. And then U_i inputs his identity ID_i and password PW_i.

2. SC_i generates a random number *k*, and calculates $H_i = N_i \oplus h(ID_i \| PW_i)$, $Z = T_k(T_s(x))$, $CID_i = ID_i \oplus h(Z \| T_1)$, $C = T_k(x)$, and $V_i = h(CID_i \| C \| H_i \| Z \| T_1)$, respectively.

3. U_i sends his login request $M_1 = \{CID_i, C, V_i, T_1\}$ to the server *S* via a public channel.

3.3. Verification Phase

1. When obtaining a login request from SC_i, *S* validates whether $T_2 - T_1 \le \Delta T$ holds.

2. If it inequality satisfies, *S* computes $Z = T_s(C)$, $ID_i = CID_i \oplus h(Z \| T_1)$, $V_i' = h(CID_i \| C \| H_i \| Z \| T_1)$, respectively. And *S* verifies whether V_i is consistent with V_i'. Otherwise, *S* refuses this login request.

3. If they match, *S* calculates $\lambda = h(H_i \| CID_i \| V_i \| T_1 \| T_2 \| Z)$ and $V_S = h(\lambda \| H_i \| T_1 \| T_2 \| Z)$, respectively. And *S* issues his authentication request $M_2 = \{V_S, T_2\}$ to the user U_i. Otherwise, *S* stops this session.

4. After receiving this authentication request, SC_i firstly checks whether $T_2 - T_1 \le \Delta T$ holds. And SC_i retrieves $\lambda = h(H_i \| CID_i \| V_i \| T_1 \| T_2 \| Z)$ and $V_S' = h(\lambda \| H_i \| T_1 \| T_2 \| Z)$, respectively. Then SC_i checks whether $V_S' = V_S$ holds. If it holds, *S* is authenticated by U_i successfully. Otherwise, U_i refuses server *S*'s authentication request.

3.4. Password Change Phase

1. U_i inputs his identity ID_i, old password PW_i and new password PW_i^*, respectively.

2. SC_i computes $N_i^* = N_i \oplus h(ID_i \| PW_i) \oplus h(ID_i \| PW_i^*)$.
3. SC_i replaces N_i with N_i^* in the memory of his smart card SC_i.

4. Cryptanalysis of Wang et al.'s Scheme

Wang et al.'s scheme ensures the user anonymity and the forward confidentiality. Their scheme hereby performs efficient defense towards server spoofing attack and insider attack, yet it is insufficient to prevent the service misuse attack. In addition, input verification has not been not well considered in the design of their proposal, which may result in Denial-of-Service attack and weakness during password change phase. Furthermore, Wang et al.'s scheme fails to concern the fast error detection, session key agreement and user revocation/re-registration.

4.1. Service Misuse Attack

In Wang et al.'s scheme, server S maintains the private key s and random variable x without keeping the password tables or verifiers for all registered users. Thereby, Wang et al.'s scheme is resilient against the stolen verifier attack. Nevertheless, when facing the service misuse attack, Wang et al.'s scheme works inadequately due to the exposure of several secret parameters among non-registered users. Suppose that a legal user U_i wants to misuse the medical services of health IoT for n non-registered users U_j, where $j = 1, 2, \cdots, n$. The user U_i shares the secret parameters pair $\{ID_i, PW_i\}$ with U_j so that U_j has the knowledge of $\{ID_i, PW_i\}$. As a result, U_j is able to login to the server S anytime, remaining concealed towards the server. The details of service misuse attack are described as follows. Each non-registered user U_j generates the corresponding random number kj, and computes $H_{ij} = N_{ij} \oplus h(ID_i \| PW_i)$, $Z_j = T_{kj}(T_s(x))$, $CID_{ij} = ID_i \oplus h(Z_j \| T_{1j})$, $C_j = T_{kj}(x)$ and $V_{ij} = h(CID_{ij} \| C_j \| H_{ij} \| Z_j \| T_{1j})$, respectively, with the knowledge of secret parameters ID_i and PW_i, where T_{1j} is U_j's current timestamp and $j = 1, 2, \cdots, n$. After receiving U_j's login request, server S checks the verification information V_i with private key s. Lastly, server S allows the all non-registered users who knows secret parameters $\{ID_i, PW_i\}$ to login to the system simultaneously. Therefore, in order to resist the service misuse attack, login records need to be added to restrict the access of non-registered users.

4.2. Denial-of-Service Attack

The Denial-of-Service (DoS) attack, a major menace of service unavailability, is able to interrupt or suspend the services of a host indefinitely. Wang et al.'s scheme does not enable input verification of old password during the password change phase. As a consequence, attacker E is able to get a temporary access to U_i's smart card SC_i by launching the DoS attack. Specifically, attacker E first inserts the smart card SC_i to initiate the password change procedure. Then he inputs two distinct random passwords PW_a and PW_a^* as old password and new password, respectively. Smart card SC_i calculates $N_i^* = N_i \oplus h(ID_i \| PW_a) \oplus h(ID_i \| PW_a^*)$ and then replaces N_i with N_i^*. In this way, it is clear that attacker E successfully updates N_i, enabling user U_i to compute V_i to generate a valid login request $\{CID_i, C_i, V_i, T_1\}$. Yet, U_i fails to achieve a correct verification information V_i with his valid password PW_i as $PW_a \neq PW_i$. Smart card SC_i calculates $H_i^* = N_i \oplus h(ID_i \| PW_a) \oplus h(ID_i \| PW_a^*) \oplus h(ID_i \| PW_i)$, that is,

$H_i^* = h(s \| ID_i) \oplus h(ID_i \| PW_a) \oplus h(ID_i \| PW_a^*)$. Furthermore, SC_i computes $V_i^* = h(CID_i \| C \| H_i^* \| Z \| T_1)$ and submits his login request $\{CID_i, C, V_i^*, T_1\}$ to the server *S*. While receiving U_i's login request, server *S* calculates $Z = T_s(C)$, $ID_i = CID_i \oplus h(Z \| T_1)$ $H_i' = h(s \| ID_i)$, and $V_i' = h(CID_i \| C \| H_i' \| Z \| T_1)$, respectively. Thus this login request is considered invalid by server *S*, since $PW_a \neq PW_a^*$, $H_i^* \neq H_i'$ and $V_i^* \neq V_i'$. Attacker *E* changes the password PW_i without knowing the user's credentials like identity or old password, making service unavailable to users. To avoid this problem, we add the input verification of old password in our proposal.

4.3. Weakness During Password Change Phase

Due to inefficient password change phase, user U_i may make a single mistake and cause the Denial-of-Service by himself. Since user U_i may forget the password or just type wrongly by accident, thus resulting an incorrect old password input PW_e. Namely, user U_i inputs an incorrect old password PW_e and a new password PW_i^* to update PW_i. Then smart card SC_i calculates $N_i^* = N_i \oplus h(ID_i \| PW_e) \oplus h(ID_i \| PW_i^*)$ and achieve the updating with N_i^*. Hence, U_i is unable to login to the remote server *S* with his new password PW_i^* as $PW_e \neq PW_i$, leading to the denial of service. It becomes clear why password change phase of Wang et al.'s scheme works inefficiently.

4.4. No Fast Error Detection

It is necessary to enforce fast error detection, namely, smart card SC_i is expected to timely examine the incorrect passwords. During the login phase of Wang et al.'s scheme, SC_i fails to detect the errors immediately. In other words, user U_i inserts the smart card SC_i and inputs mistaken information, namely, inaccurate identity ID_e or incorrect password PW_e. Without fast error detection, SC_i executes the following procedures as planned but cannot detect the errors locally. Then smart card SC_i submits U_i's login request to server *S*. However, it doesn't work due to wrong inputs. With the above problem unsolved, fast error detection is urged to be added during the login phase.

4.5. No Session Key Agreement

Note that Wang et al.'s scheme does not perform the process of session key agreement. Hereby, user U_i and server *S* are incapable of establishing a session key used for subsequent communication. In order to provide the session key agreement, we add the corresponding procedure to generate the session keys in our proposal.

4.6. No User Revocation/Re-registration Phase

Moreover, Wang et al.'s scheme lacks user revocation/re-registration. As a result, when smart card SC_i of the user U_i is stolen or lost, U_i cannot revoke his privilege or re-register. To promote the functionality, we correspondingly design the revocation/re-registration phase, which meets the requirements in the Health IoT. The details are specified in the following section.

5. The Proposed Scheme

Benefit from cryptanalysis of Wang et al.'s scheme, we present a novel robust biometrics based authentication and key agreement proposal for Health IoT. The proposed scheme has do several improvements on the Wang et al.'s scheme, which we specify here as follows: 1) it enables the resilience to service misuse attack by adding login records in

the memory of server, 2) it applies the biometric information to enhance the entropy of secret parameters, 3) it enforces the input verification to achieve the defense against the DoS attack, 4) it leverages the fast error detection and session key agreement to guarantee better performance, and 5) it designs an additional revocation/re-registration phase to meet the requirements of users. Then in the following subsections, we demonstrate our proposal in five aspects, namely, registration phase, login phase, authentication phase, password change phase and user revocation/re-registration phase.

Without loss of generality, two participants are presented here, namely, user U_i and server S. All notations applied in our scheme are listed in Table 1. In the initialization of medicine system, server S first selects a hash function $h(\cdot)$. Next, server S generates a pre shared key s and a random variable $x \in [-1,1]$ for the later calculation. Finally, S calculates $T_s(x)$ and publishes $\{x, T_s(x), h(\cdot)\}$.

Table 1. Symbols and Notions in Our Scheme

Symbol	Notion
U_i, S, E	ith user, server and adversary
SC_i, ID_i,	U_i's smart card and U_i's identity
AID_i	U_i's dynamic identity
PW_i, BIO_i	U_i's password and U_i's biometric information
R_i,	U_i's nearly random binary string
P_i	U_i's auxiliary binary string
s, x	Pre shared key and random variable
$h(\cdot)$, $\oplus$, $\|\|$	Hash function, XOR operation and concatenation operation

5.1. Registration Phase

User U_i and server S perform the registration phase via a secure channel, in which registration phase is shown in the Figure 2 and details are specified as follows.

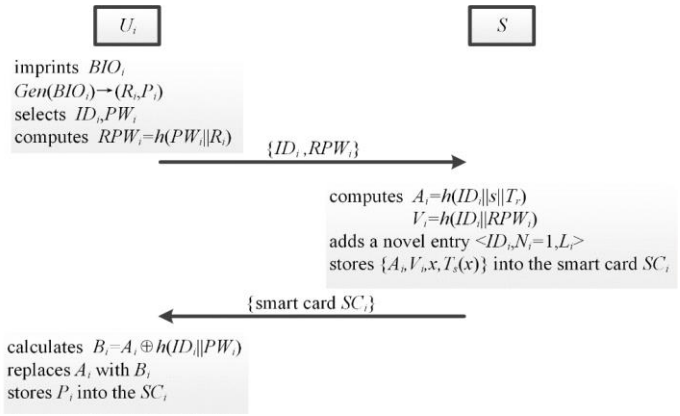


Figure 2. The Registration Phase

1. User U_i first imprints his biometrics BIO_i on the sensor. Next sensor helps user U_i sketches his BIO_i, execute $Gen(BIO_i) \rightarrow (R_i, P_i)$, and stores P_i, respectively. Then U_i chooses his identity ID_i and password PW_i, and computes $RPW_i = h(PW_i \| R_i)$. Finally, he submits his registration request $\{ID_i, RPW_i\}$ to the server S via a secure channel.

2. Upon receiving this registration request, S calculates $A_i = h(ID_i \| s \| T_r)$ and $V_i = h(ID_i \| RPW_i)$, where T_r is registration time. And S adds a novel array $\langle ID_i, N_i = 1, L_i \rangle$ to the server's database, in which N_i means the number of user registration and L_i records the login status of U_i, respectively. Particularly, if U_i is logged-into the server S, L_i is set to 1. Otherwise, L_i is set to 0.

3. S sends a smart card SC_i to U_i, which includes $\{A_i, V_i, x, T_s(x)\}$ over a secure channel.

4. After receiving the SC_i, U_i calculates $B_i = A_i \oplus h(ID_i \| PW_i)$. Then U_i replaces A_i with B_i and further stores P_i into the SC_i.

5.2. Login Phase

In the login phase, smart card SC_i enables to check the errors immediately with U_i's identity, password, and biometrics, in which flow of login phase is illustrated in the Figure 3 and details are explained as follows.

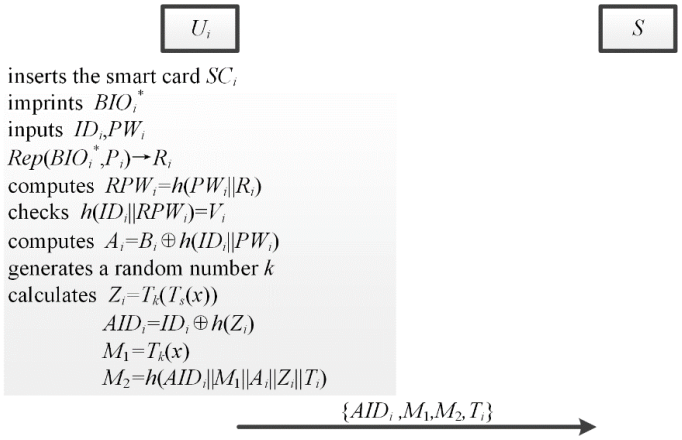


Figure 3. The Login Phase

1. U_i first inserts his smart card SC_i and imprints his biometrics BIO_i^*, identity ID_i and password PW_i, respectively. Then sensor sketches U_i's BIO_i^* and performs $Rep(BIO_i^*, P_i) \rightarrow (R_i,)$.

2. SC_i computes $RPW_i = h(PW_i \| R_i)$ and needs to check whether $h(ID_i \| RPW_i) = V_i$ holds. If they matches, SC_i further calculates $A_i = B_i \oplus h(ID_i \| PW_i)$. Otherwise, SC_i terminates this login.

3. SC_i chooses a random number k, and calculates $Z_i = T_k(T_s(x))$, $AID_i = ID_i \oplus h(Z_i)$, $M_1 = T_k(x)$ and $M_2 = h(AID_i \| M_1 \| A_i \| Z_i \| T_i)$, in which T_i is a timestamp.

4. SC_i sends his login request $\{AID_i, M_1, M_2, T_i\}$ to the server S via a public channel.

5.3. Authentication Phase

During the authentication phase, server *S* confirms the freshness of login request, in which authentication phase is illustrated in the Figure 4 and details are described as follows.

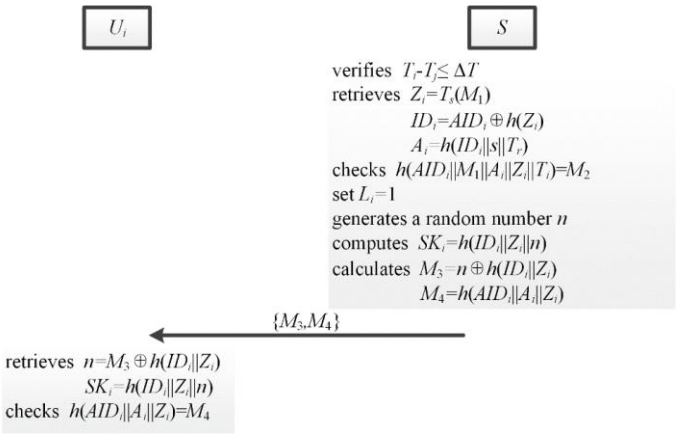


Figure 4. The Authentication Phase

1. Upon receiving U_i's login request, server *S* needs to verify whether $T_i - T_j \leq \Delta T$ is valid, in which ΔT is a time interval and T_j is the time when obtaining U_i's login request. If this verification holds, *S* continues to execute the next step. Otherwise, U_i's login request is rejected by *S*.

2. *S* retrieves $Z_i = T_s(M_1)$, $ID_i = AID_i \oplus h(Z_i)$, $A_i = h(ID_i \| s \| T_r)$, respectively, and checks whether $h(AID_i \| M_1 \| A_i \| Z_i \| T_i)$ is consistent with M_2.

3. If they matches, *S* set the login bit L_i of status entry to 1, generates a random number n and computes a session key $SK_i = h(ID_i \| Z_i \| n)$. Otherwise, *S* terminates this authentication.

4. *S* calculates $M_3 = n \oplus h(ID_i \| Z_i)$ and $M_4 = h(AID_i \| A_i \| Z_i)$. Then *S* submits his authentication request $\{M_3, M_4\}$ to the user U_i via a public channel.

5. After obtaining server *S*'s authentication request, SC_i retrieves $n = M_3 \oplus h(ID_i \| Z_i)$, $SK_i = h(ID_i \| Z_i \| n)$ and then verifies whether $h(AID_i \| A_i \| Z_i) = M_4$ holds. If they matches, U_i adopts this session key SK_i to communicate with *S*. Otherwise, authentication is rejected by U_i.

5.4. Password Change Phase

U_i is able to update his new password by himself in password change phase, in which details are specified as follows.

1. U_i imprints his BIO_i^*, ID_i and PW_i, respectively. After that, sensor sketches U_i's BIO_i^* and performs $ReP(BIO_i^*, P_i) \rightarrow (R_i,)$.

2. SC_i calculates $RPW_i = h(PW_i \| R_i)$ and then checks whether $h(ID_i \| RPW_i) = V_i$ holds. If they matches, U_i enables to choose a new password. Otherwise, this phase is terminated immediately by SC_i.

3. U_i inputs new password PW_i^{new} and SC_i computes $RPW_i^{new} = h(PW_i^{new} \| R_i)$, $B_i^{new} = B_i \oplus h(ID_i \| PW_i) \oplus h(ID_i \| PW_i^{new})$ and $V_i^{new} = h(ID_i \| RPW_i^{new})$, respectively.

4. Finally, SC_i replaces B_i and V_i with B_i^{new} and V_i^{new} in the memory.

5.5. User Revocation/Re-registration Phase

When smart card SC_i is stolen or lost, user revocation/re-registration enables user U_i to revoke his privilege or re-register his account. If U_i wants to revoke his privilege, he sends his revocation request to the server S via a secure channel. Next S alters the corresponding array by setting $\langle ID_i, N_i = 0, L_i \rangle$. Similarly, after obtaining U_i's re-registration request, S performs the registration steps which are specified in the registration phase and then replaces $\langle ID_i, N_i = N_i + 1, L_i \rangle$ with $\langle ID_i, N_i, L_i \rangle$ to help U_i achieve the re-registration. Thus, user revocation/re-registration makes the presented proposal more robust.

6. Analysis of our Scheme

An authentication and key agreement proposal applied for health IoT is expected to perform both security and functionality. In this section, we analysis the performance of our scheme, and compare the proposed scheme with some related proposals.

6.1. Security Analysis

We start with the security analysis of the resistance of ours against these common attacks as follows.

6.1.1. Resistance Against Password Guessing Attack: By launching side-channel attacks for instance SPA or DPA, attacker E is able to obtain B_i, P_i, V_i, x and $T_s(x)$. However, without information about BIO_i, Z_i and s, this attacker cannot verify U_i's password whether in the on-line or off-line environment. Furthermore, one-way hash function provides a protection for U_i's password, namely, $h(PW_i \| R_i)$, where R_i has a high entropy. Note that any two users hold different biometric templates due to the uniqueness. Hence, our proposal resists password guessing attack.

6.1.2. Resistance Against Denial-of-Service Attack: DoS attack usually makes server S unavailable, thus server S's expected capability diminishes dramatically. Server S is able to verify the freshness of $M_2 = h(AID_i \| M_1 \| A_i \| Z_i \| T_i)$ by checking the timestamp T_i during the authentication phase. If M_2 is sent by adversary E, there is a mismatch due to the wrong timestamp. The presented scheme enables input verification of identity and password, avoiding invalid input or malicious tampering. Moreover, fuzzy extractor is employed in our scheme to satisfy the input requirements of biometric information. In conclusion, our proposal is resilient against DoS attack.

6.1.3. Resistance Against Smart Card Attack: Smart card attacker E attempts to achieve the authentication by applying some information stored in U_i's smart card SC_i. It

is unnegligible that E enable to acquire B_i, P_i, V_i, x and $T_s(x)$ through SPA or DPA. We present the generation of one session key between user and server as follow.

$$Z_i = T_s(M_1),$$
$$ID_i = AID_i \oplus h(Z_i),$$
$$n = M_3 \oplus h(ID_i \| Z_i),$$
$$SK_i = h(ID_i \| Z_i \| n).$$

Though acquiring AID_i, M_1 and M_3 via a public channel, E is unable to retrieve Z_i, ID_i and n because of the lack of random numbers s and k. As a result, our proposal confines the influence of smart card attack.

6.1.4. Resistance Against User Impersonation Attack: During the user impersonation attack, similar to smart card attack, adversary E impersonates user U_i adopting smart card SC_i without U_i's password or biometrics. The random numbers s and k are employed to protect Z_i, ID_i and n. Thus, E cannot calculate the session keys even if E obtains B_i, P_i, V_i, x and $T_s(x)$ by side channel attacks. Consequently, user impersonation attack has no effect on our scheme.

6.1.5. Resistance Against Server Spoofing Attack: After obtaining U_i's login request, adversary E attempts to spoof as server S by replaying old authentication request $\{M_3^{old}, M_4^{old}\}$, where $M_3^{old} = n^{old} \oplus h(ID_i \| Z_i^{old})$ and $M_4^{old} = h(AID_i^{old} \| A_i \| Z_i^{old})$. However, U_i applies distinct random numbers for different sessions, namely, $Z_i^{old} \neq Z_i^{new}$. Thus, this attack does not work. Furthermore, due to the inaccessibility of both s and n, E cannot retrieve Z_i and A_i. In conclusion, our proposal prevents server spoofing attack.

6.1.6. Resistance Against Service Misuse Attack: For the service misuse attack, a registered user E intentionally shares some secret parameters to other non-registered users. As a result, each one that knows these parameters, such as identity and password, may login to server S anytime. However, in our improved scheme, S maintains a login bit L_i in the status entry for each legal user. Since L_i is set to one once a user is logged in, two or more people who know the same registration information cannot to login to S at the same time. Consequently, the presented scheme performs resistance against service misuse attack.

6.2. Functionality Analysis

In previous studies, various functionality requirements for an authentication and key agreement scheme are discussed. We present how our scheme achieves these functionalities during this section.

6.2.1. Anonymity: To perform anonymity, user's real identity cannot be disclosed to another unauthorized party. In our proposal, user U_i calculate his dynamic identity AID_i as $AID_i = ID_i \oplus h(Z_i)$. Since Z_i does not leak out from U_i's request over a public channels, adversary E is unable to compute the user's identity ID_i. On the other hand, server S can retrieve $Z_i = T_s(M_1)$, and further calculate ID_i from $ID_i = AID_i \oplus h(Z_i)$. So the authorized server S is able to confirm U_i's real identity. In conclusion, E keeps unknown to user's real identity, but U_i can be authenticated by S.

6.2.2. Session Key Agreement: Through session key agreement, user and server are able to securely establish their session key used for subsequent communication. In our proposal, session key can be calculated by user U_i and server S as $SK_i = h(ID_i \| Z_i \| n)$, where Z_i and n are changeable. Namely, session keys are distinct in different sessions. Hence, previous session keys is difficult to be retrieved by adversary E.

6.2.3. Perfect Forward Secrecy: In order to discuss perfect forward secrecy, we give the calculation of a session key as follow.

$$Z_i = T_s(M_1),$$
$$ID_i = AID_i \oplus h(Z_i),$$
$$n = M_3 \oplus h(ID_i \| Z_i),$$
$$SK_i = h(ID_i \| Z_i \| n).$$

Although user's long-term key A_i is compromised, adversary E cannot calculate s, k and B_i. Thus, this adversary is not able to retrieve Z_i, ID_i and n to generate a session key between U_i and S. Consequently, our proposal provides perfect forward secrecy.

6.2.4. Biometric Information Protection: In some previous schemes, U_i's biometrics is directly saved in his smart card SC_i. In this way, adversary E is able to obtain user's biometric information from smart card through side channel attacks. To avoid this, a high security mechanism is applied in our scheme. We leverages one-way secure hash function to protect a nearly random string R_i. What is more, this string R_i can only be extracted from biometric information BIO_i with the help of fuzzy extractor, making it impossible for attacker E to obtain the biometrics. Thus, our scheme achieves biometric information protection.

6.2.5. User Revocation/Re-registration: If user U_i wants to revoke his own privilege or re-register, a revocation/re-registration request is required to be sent to server S over a secure channel. Upon receiving this request, S can thereby modify $\langle ID_i, N_i, L_i \rangle$ in the database to revoke privilege or re-register of user U_i, which also meets a practical requirement.

6.2.6. Fast Error Detection: Through the fast error detection, smart card SC_i is able to verify some discrepancies quickly, for example incorrect passwords, inaccurate identities and false biometrics. During both login and password change phases, SC_i can immediately detects the errors without the assistance of server S. Therefore, our scheme realizes fast error detection.

6.3. Comparisons with Related Schemes

In this section, we concretely compare some properties which includes resistance, functionality and performance between our proposal and other related identity-based authentication schemes, including Lin's scheme [32], Li et al.'s scheme [33] and Wang et al.'s scheme [27].

Table 2 shows the result of resistance comparison among these authenticated key agreement schemes. For simplicity, we define some following notations listed in Table 2, namely, R1: resistance against password guessing attack, R2: resistance against Denial-of-Service attack, R3: resistance against smart card attack, R4: resistance against user impersonation attack, R5: resistance against server spoofing attack and R6: resistance

against service misuse attack. Result indicates that our proposal outperforms other schemes by achieving the requirements of resistance.

Table 2. The Resistance Comparison

	Lin's scheme [32]	Li et al.'s scheme [33]	Wang et al.'s scheme [27]	Our scheme
R1	Yes	Yes	Yes	Yes
R2	No	No	No	Yes
R3	Yes	Yes	Yes	Yes
R4	No	No	Yes	Yes
R5	No	Yes	Yes	Yes
R6	Yes	Yes	No	Yes

Table 3 specifies the result of functionality comparison among these schemes mentioned above, in which we adopt some following notations, namely, F1: anonymity, F2: session key agreement, F3: perfect forward secrecy, F4: biometric information protection, F5: user revocation/re-registration and F6: fast error detection. It becomes clearly that our proposal provides more functionalities for health IoT, which also makes ours more robust.

Table 3. The Functionality Comparison

	Lin's scheme [32]	Li et al.'s scheme [32]	Wang et al.'s scheme [27]	Our scheme
F1	No	Yes	Yes	Yes
F2	No	Yes	No	Yes
F3	No	No	No	Yes
F4	No	No	No	Yes
F5	No	No	No	Yes
F6	No	No	No	Yes

Moreover, we compare the presented scheme with above schemes to evaluate the computational costs during login and authentication phases. Note that the computational cost of XOR operation is negligible. Hence, we treat hash function and extended Chebyshev chaotic map as time complexity in the measurement. In Table 4, T_h denotes the time cost about executing a hash function and T_c means the time cost about performing an extended Chebyshev chaotic map. Benefited from Xue et al.'s work [34], processing time of a hash function and an extended Chebyshev chaotic map is 0.2ms and 32.2ms, respectively. As can be seen in Table 4 and Fig. 5, our proposal requires slightly more computation cost than Lin's scheme and Wang et al.'s scheme. But compared to Li et al.'s scheme, our scheme has advantage on computation costs.

Table 4. The Computation Cost Comparison

	Lin's scheme [32]	Li et al.'s scheme [33]	Wang et al.'s scheme [27]	Our scheme
Computational cost (User)	$4T_h+2T_c$	$8T_h+2T_c$	$5T_h+2T_c$	$8T_h+2T_c$
Execution cost (User)	65.2ms	66.0ms	65.4ms	66.0ms
Computational cost (Server)	$3T_h+1T_c$	$9T_h+2T_c$	$4T_h+1T_c$	$6T_h+1T_c$
Execution cost (Server)	32.8ms	66.2ms	33.0ms	33.4ms
Total execution cost	98.0ms	132.2ms	98.4ms	99.4ms

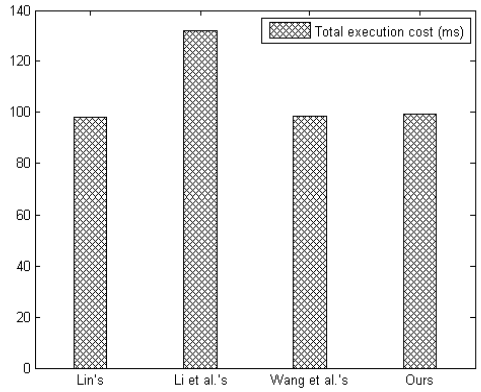


Figure 5. The Computation Cost Comparison

Additionally, we evaluate the performance of our scheme by measuring the communication cost of these methods mentioned above. Without loss of generality, we assume that length of timestamp is 16 bit and the length of some other security parameters is 160 bit, including random number, identity input and hash function output. Hereby, length of login request $\{AID_i, M_1, M_2, T_i\}$, which user U_i submits to server S, is $160+160+160+16=496$ bits. And in our authentication phase, communication overhead is $160+160=320$ bits, containing authentication request $\{M_3, M_4\}$. As a result, total communication overhead of our proposal is $496+320=816$ bits. We consider the communication overhead of other schemes analogously. As for storage requirement, we estimate the information saved in the smart card SC_i and calculate the bit length of stored information as storage overhead. Thus, in our proposal, requirement about stored message $\{B_i, P_i, V_i, x, T_s(x)\}$ contains $160+160+160+160+160=800$ bits. Similarly, we estimate the requirement about storage of other schemes and detailed testing results are presented as below. Table 5 and Fig. 6 show the comparison regarding on both communication cost and storage cost of these schemes. Compared with others, our scheme achieves better efficiency by synthesizing the security, functionality and performance.

Table 5. The Communication and Storage Costs Comparison

	Lin's scheme [32]	Li et al.'s scheme [33]	Wang et al.'s scheme [27]	Our scheme
Communication cost in the login phase	656bits	656bits	496bits	496bits
Communication cost in the authentication phase	176bits	832bits	176bits	320bits
Total communication cost	832bit	1488bits	672bits	816bits
Storage cost	480bits	960bits	480bits	800bits

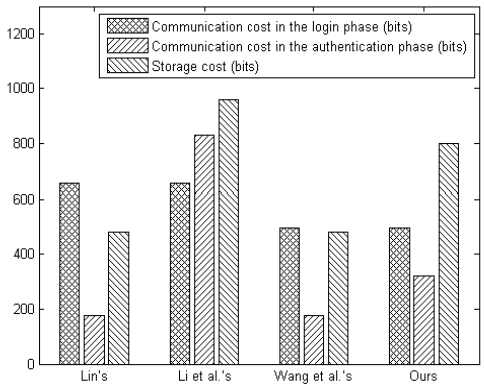


Figure 6. The Communication and Storage Costs Comparison

7. Conclusion

This paper has proposed a robust three-factor identity-based authentication and key agreement scheme based on extended chaotic maps for health IoT. According to our comprehensive cryptanalysis, our scheme guarantees effective defense to typical security menaces. Besides, the presented proposal realizes additional significant features than most previous schemes, namely, biometric information protection and user revocation/re-registration. Under the same level of computation cost, communication overhead and storage requirement, our scheme achieves better security with more functionalities. We conclude that the proposed proposal is secure against known attacks, which is also efficient for health IoT.

Acknowledgments

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] Z. Y. Sun, X. H. Ji and Y. B. Li, "HSKAS: A Novel Hierarchical Shared Key Authentication Scheme in Wireless Sensor Networks", International Journal of Security and Its Applications, vol. 10, no. 4, **(2016)**, pp. 105-116.

[2] J. Srinivas, S. Mukhopadhyay and D. Mishra, "Secure and Efficient User Authentication Scheme for Multi-gateway Wireless Sensor Networks", Ad Hoc Networks, vol. 54, **(2017)**, pp. 147-169.

[3] S. K. H. Islam, M. K. Khan, M. S. Obaidat and F. T. Bin Muhaya, "Provably Secure and Anonymous Password Authentication Protocol for Roaming Service in Global Mobility Networks Using Extended Chaotic Maps", Wireless Personal Communications, vol. 84, no. 3, **(2015)**, pp. 2013-2034.

[4] Y. R. Lu, L. X. Li, H. P. Peng and Y. X. Yang, "An Enhanced Biometric-based Authentication Scheme for Telecare Medicine Information Systems Using Elliptic Curve Cryptosystem", Journal of Medical Systems, vol. 39, no. 3, **(2015)**, pp. 1-8.

[5] X. Li, J. G. Liao, S. Kumari, W. Liang, F. Wu and M. K. Khan, "A New Dynamic ID-based User Authentication Scheme Using Mobile Device: Cryptanalysis, The Principles and Design", Wireless Personal Communications, vol. 85, no. 1, **(2015)**, pp. 263-288.

[6] C. Q. Wang, X. Zhang and Z. M. Zheng, "Cryptanalysis and Improvement of a Biometric-Based Multi-Server Authentication and Key Agreement Scheme", PLoS One, vol. 11, no. 2, **(2016)**, pp. e0149173.

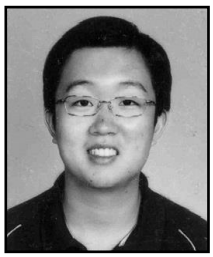
[7] T. Wan, N. Jiang, J. F. Ma and L. Yang, "Cryptanalysis of a Biometric-based Multi-Server Authentication Scheme", International Journal of Security and Its Applications, vol. 10, no. 2, **(2016)**, pp. 163-170.

[8] A. K. Das and B. Bruhadeshwar, "An Improved and Effective Secure Password-based Authentication and Key Agreement Scheme Using Smart Cards for the Telecare Medicine Information System", Journal of Medical Systems, vol. 37, no. 5, **(2013)**, pp. 1-17.

[9] Y. P. Lin, K. H. Wang, B. C. Zhang, Y. Z. Liu and X. Li, "An Enhanced Biometric-Based Three Factors User Authentication Scheme for Multi-server Environments", International Journal of Security and Its Applications, vol. 10, no. 1, **(2016)**, pp. 315-328.
[10] B. J. Huang, M. K. Khan, L. B. Wu, F. T. Bin Muhaya and D. B. He, "An Efficient Remote User Authentication with Key Agreement Scheme Using Elliptic Curve Cryptography", Wireless Personal Communications, vol. 85, no. 1, **(2015)**, pp. 225-240.
[11] S. K. H. Islam and G. P. Biswas, "A Pairing-free Identity-based Authenticated Group Key Agreement Protocol for Imbalanced Mobile Networks", Annals of Telecommunications, vol. 67, no. 11-12, **(2012)**, pp. 547–558.
[12] C. H. Ye, Z. G. Xiong, Y. M. Ding, X. M. Zhang, G. W. Wang and F. Xu, "Secure Multimedia Content Distribution for M2M Communication", International Journal of Security and Its Applications, vol. 10, no. 4, **(2016)**, pp. 279-288.
[13] D. H. Lee and N. Park, "Security Enhancement Scheme Supporting Range Queries on Encrypted DB for Secure E-Navigation Era", International Journal of Security and Its Applications, vol. 10, no. 2, **(2016)**, pp. 141-150.
[14] B. Ustaoğlu, "Integrating Identity-based and Certificate-based Authenticated Key Exchange Protocols", International Journal of Information Security, vol. 10, no. 4, **(2011)**, pp. 201-212.
[15] S. K. H. Islam and G. P. Biswas, "Provably Secure and Pairing-free Certificateless Digital Signature Scheme Using Elliptic Curve Cryptography", International Journal of Computer Mathematics, vol. 90, no. 11, **(2013)**, pp. 2244–2258.
[16] H. B. Yang, J. H. Chen and Y. Y. Zhang, "An Improved Two-party Authentication Key Exchange Protocol for Mobile Environment", Wireless Personal Communications, vol. 85, no. 3, **(2015)**, pp. 1399-1409.
[17] S. Kumari, M. K. Khan and R. Kumar, "Cryptanalysis and Improvement of 'a Privacy Enhanced Scheme for Telecare Medical Information Systems", Journal of Medical Systems, vol. 37, no. 4, **(2013)**, pp. 1-11.
[18] H. F. Zhu, "Flexible and Password-authenticated Key Agreement Scheme Based on Chaotic Maps for Multiple Servers to Server Architecture", Wireless Personal Communications, vol. 82, no. 3, **(2015)**, pp. 1697-1718.
[19] C. Q. Wang, X. Zhang and Z. M. Zheng, "An Improved Biometrics Based Authentication Scheme Using Extended Chaotic Maps for Multimedia Medicine Information Systems", Multimedia Tools and Applications, **(2016)**, pp. 1-27.
[20] T. S. Messerges, E. Dabbish and R. H. Sloan, "Examining Smart-card Security Under the Threat of Power Analysis Attacks", IEEE Transactions on Computers, vol. 51, no. 5, **(2002)**, pp. 541-552.
[21] S. K. H. Islam, "Provably Secure Dynamic Identity-based Three-factor Password Authentication Scheme Using Extended Chaotic Maps", Nonlinear Dynamics, vol. 78, no. 3, **(2014)**, pp. 2261-2276.
[22] M. Zhang, J. Zhang and Y. Zhang, "Remote Three-factor Authentication Scheme Based on Fuzzy Extractors", Security and Communication Networks, vol. 8, no. 4, **(2015)**, pp. 682-693.
[23] C. T. Li and M. S. Hwang, "An Efficient Biometrics-based Remote User Authentication Scheme Using Smart Cards", Journal of Network and Computer Applications, vol. 33, no. 1, **(2010)**, pp. 1-5.
[24] X. Li, J. W. Niu, J. Ma, W. D. Wang and C. L. Liu, "Cryptanalysis and Improvement of a Biometrics-Based Remote User Authentication Scheme Using Smart Cards", Journal of Network and Computer Applications, vol. 34, no. 1, **(2011)**, pp. 73-79.
[25] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", SIAM Journal on Computing, vol. 38, no. 1, **(2008)**, pp. 75-80.
[26] Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin and A. Smith, "Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets", IEEE Transactions on Information Theory, vol. 58, no. 9, **(2012)**, pp. 6207-6222.
[27] Z. H. Wang, Z. Q. Huo and W. B. Shi, "A Dynamic Identity Based Authentication Scheme Using Chaotic Maps for Telecare Medicine Information Systems", Journal of Medical Systems, vol. 39, no. 1, **(2015)**, pp. 1-8.
[28] P. Bergamo, P. D'Arco, A. De Santis and L. Kocarev, "Security of Public-key Cryptosystems Based on Chebyshev Polynomials", IEEE Transactions on Circuits and Systems-I: Regular Papers, vol. 52, no. 7, **(2005)**, pp. 1382–1393.
[29] L. Zhang, "Cryptanalysis of the Public Key Encryption Based on Multiple Chaotic Systems", Chaos, Solitons & Fractals, vol. 37, no. 3, **(2008)**, pp. 669–674.
[30] T. F. Lee, "Verifier-based Three-party Authentication Schemes Using Extended Chaotic Maps for Data Exchange in Telecare Medicine Information Systems", Computer Methods and Programs in Biomedicine, vol. 117, no. 3, **(2014)**, pp. 464-472.
[31] D. Dolev and A. Yao, "On the Security of Public Key Protocols", IEEE Transactions on Information Theory, vol. 29, no. 2, **(1983)**, pp. 198–208.
[32] H. Lin, "Chaotic Map Based Mobile Dynamic ID Authenticated Key Agreement Scheme", Wireless Personal Communications, vol. 78, no. 2, **(2014)**, pp. 1487-1494.

[33] C. T. Li, C. L. Cheng and Y. W. Chi, "A Secure Chaotic Maps and Smart Cards Based Password Authentication and Key Agreement Scheme with User Anonymity for Telecare Medicine Information Systems", Journal of Medical Systems, vol. 38, no. 9, **(2014)**, pp. 1-11.
[34] K. P. Xue and P. L. Hong, "Security Improvement on an Anonymous Key Agreement Protocol Based on Chaotic Maps", Communications in Nonlinear Science and Numerical Simulation, vol. 17, no. 7, **(2012)**, pp. 2969–2977.

Authors



Chengqi Wang, received the B.S. degree with distinction from Beihang University, Beijing, China, in 2012. He was a Ph.D. candidate at Key Laboratory of Mathematics, Informatics and Behavioral Semantics and School of Mathematics and Systems Science, Beihang University. He received the Ph.D degree from Beihang University, Beijing, China, in 2017. 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.

Lijia Xie, received the B.S. degree with distinction from Beihang University, Beijing, China, in 2016. She is currently a Master student at Key Laboratory of Mathematics, Informatics and Behavioral Semantics and School of Mathematics and Systems Science, Beihang University. Her research interests include network security and applied cryptography.

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.

