A Novel and Provable Authenticated Key Agreement Protocol with Privacy Protection Based on Chaotic Maps towards Mobile Network

Hongfeng Zhu, Yifeng Zhang, Yan Zhang and Haiyang Li
(Corresponding author: Hongfeng Zhu)

Software College, Shenyang Normal University
No.253, HuangHe Bei Street, Huang Gu District, Shenyang, P.C 110034 - China
(Email:zhuhongfeng1978@163.com)

(Received Sept. 18, 2014; revised and accepted Jan. 16 & June 21, 2015)

Abstract

Key agreement is a crucial cryptographic primitive for building secure communication channels between two parties in a network. In the research literature a typical protocol aims for key secrecy and mutual authentication. However, there are many important practical scenarios where privacy protection is more desirable, especially for social network. Network privacy security means that the personal data and online data are not peep, intrusion, interference, illegal collection and utilization. In our paper, we propose a robust chaotic maps-based authentication key agreement scheme with privacy protection using smart cards. The key idea of our proposed scheme is to adopt chaotic maps for mutual authentication, not to encrypt/decrypt messages transferred between user and server, which can make our proposed scheme much more efficient. Next, we give the formal provable security under the random oracle model for our scheme. Finally, our proposed scheme can not only achieve privacy protection, but also avoid time-consuming modular exponentiation and scalar multiplication on elliptic curves. Meanwhile, it can resist various common attacks, and provide prefect forward secrecy and known-key secrecy. In brief, compared with related schemes, our proposed scheme is more secure, effective and practical.

Keywords: Chaotic maps, biometric, privacy protection, provable security, smart card

1 Introduction

1.1 Biometric Technology

At present, biometrics has widely used to certificate the identities of users. What is called biometrics is that through closely combining computer with the high-tech means of optical, acoustics, biological sensor and biological statistical principles, using physiological features (such as fingerprints, face, iris, etc) and behavior characteristics (such as voice, gait, etc) for certification of personal identity. Therefore, compared with traditional identification methods, biometric technology is safer and more convenient. It is not easy to forget, different to be stolen or counterfeit. In addition, it can be carry-on and available anytime and anywhere.

1.2 Chaotic System

Nowadays, chaos theory has widely used to cryptography. Compared with other related systems, chaotic system has numerous advantages, such as extremely sensitive to initial parameters, unpredictability, boundness, etc. Meanwhile, chaotic sequence generated by chaotic system has the properties of non-periodicity and pseudo-randomness. In a word, chaos theory and chaotic system have exploited a new way for cryptography.

1.3 Privacy Protection

In contemporary, with the rapid development of Internet, users can use personal computers or smart phones to login servers for a variety of services anytime and anywhere. However, in general, these intelligent terminals have automatic memory function. They can remember the passwords and identities of users. When these terminals of users are lost, stolen or being malicious attacked, the personal information of users is easy to leak. In consequence, it is a hot topic to protect the user privacy.

1.4 Relevant Work

In a client-server environment, authentication mechanism plays an important role in a secure protocol to certificate the identities of users. As everyone knows, in 1981, Lamport [12] firstly presented a remote authentication scheme based on password tables to certificate authored users over insecure channel. Form then on, many authentication schemes were presented and analyzed to improve the safety performance or the efficiency performance [4, 6, 9, 11, 13, 21]. Usually, alphanumeric passwords are widely used, and the security authentication of users is based on alphanumeric passwords. However, this kind of passwords is easily got by an adversary if he/she has enough time. Due to this reason, it is necessary to set up safer protection mechanisms to protect user information. Many existing schemes have been designed to solve this problem.

In 2000, Hwang et al. [9] firstly proposed the remote user authentication scheme using smart cards without a certification table to solve the problems of Lamport scheme [12]. But the passwords of users are maintained by the system. However, Chan et al. [3], Shen et al. [18] had pointed out that the scheme of [9] had flaws. In the last few years, many related schemes had been proposed, analyzed, and improved [1, 2, 7, 8, 10, 14, 15, 16, 19, 20, 22, 23, 24]. However, some of them still had defects. In 2009, Xu et al. [23] proposed a smart card based password authentication scheme with provable security. However, in 2010, Song [19] showed that the smart card authentication scheme [23] is vulnerable to internal and impersonation attacks, and proposed an efficient strong smart card authentication protocol. Unfortunately, Juan et al. [20] pointed out that the improved protocol by Song [19] cannot resist an off-line password guessing attack and also had some other weaknesses.

Then Juan et al. [20] proposed an advanced smart card based password authentication protocol in 2011. In the same year, Awasthi et al. [1] proposed a timestamp-based remote user authentication scheme using smart card without any verification table which can avoid potential risks of verification tables. In [1], remote server only kept a secret key for computing the passwords of users. Recently, many schemes based on chaos theory are proposed [2, 8, 14]. Compared with the related other schemes, these schemes based on chaotic maps avoid numerous complex operations. In 2013, Guo et al. [8] proposed a chaotic maps-based key agreement protocol which avoided modular exponential computing and scalar multiplication on elliptic curve.

Nowadays, with the fast development of Internet, privacy protection of users is a hot issue. In 2014, Liu et al. [16] proposed a multi-function password mutual authentication key agreement scheme with privacy preserving. However, this scheme was based on an elliptic curve. Its efficiency was lower than related scheme [15] based on chaotic maps because of modular exponential computing and scalar multiplication on elliptic curve. Considered the security and efficiency, we propose a robust mutual authentication key agreement scheme with privacy protection based on biometrics and chaotic maps using smart card.

1.5 Contributions

(1) Our scheme can avoid modular exponential computing and scalar multiplication and resist various attacks. (2) In our scheme, the identities of users are hidden in secure hash function. Users can anonymity login the server and do not leak any personal information. (3) Our scheme is based on chaotic maps. However, we do not use it to encrypt any message. It is only used to certificate users and server and establish a session key for their sessions. (4) Biometrics certification mechanism has many merits which can make our scheme faster and safer. According to these, we can show that our proposed scheme is more practical and effective.

1.6 Construction

The construction of our paper is organized as below: the theoretical concepts of one-way hash function and Chebyshev chaotic maps are explained in Section 2. Section 3 describes our proposed scheme in detail. Section 4 analyzes the security, functionality and efficiency of the proposed scheme. The paper is concluded in Section 5.

2 Theoretical Concepts

This section introduces the concepts of Chebyshev chaotic maps and biometrics authentication in detail.

2.1 Chebyshev Chaotic Maps

Chebyshev polynomial and Chebyshev chaotic maps [22] have the following properties:

1) Let n and x be an integer and a variable, respectively. The value of x belongs to the interval $[-1, 1]$. Chebyshev polynomial $T_n(x)$: $[-1, 1] \to [-1, 1]$ is defined as

$$T_n(x) = \cos(narccos(x)). \quad (1)$$

In terms of Equation (1), the recurrence relation of Chebyshev polynomial is defined as

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

where $T_0(x) = 1$ and $T_1(x) = x$.

2) Chebyshev polynomial has two properties: The chaotic property: When $n \geq 1$, Chebyshev polynomial map $T_n(x)$: $[-1, 1] \to [-1, 1]$ of degree n is a chaotic map with its invariant density $f^*(x) = 1/(\pi\sqrt{1-x^2})$, for positive Lyapunov exponent $\ln n$. The semi-group property [25]: The semi-group property of Chebyshev polynomial defined on the interval $(-\infty, +\infty)$ holds, as follows:

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

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

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

Besides, the following problems are assumed to be intractable within polynomial time.

3) Chaotic Maps-based Discrete Logarithm problem (CMDLP): Given two variables x and y, it is intractable to find the integer s, such that $T_s(x) = y$.

4) Chaotic Maps-Based Diffie-Hellman problem (CMDHP): Given x, $T_r(x)$, $T_s(x)$, it is intractable to find $T_{rs}(x)$, such that $T_r(T_s(x)) = T_{rs}(x)$ or $T_s(T_r(x)) = T_{rs}(x)$.

2.2 Biometrics certification

Figure 1 shows the flow chart of biometrics certification in detail. In the user registration phase, user inputs the biometrics in a biometric sensor, and then the system performs image processing, feature extraction, and generates template stored in the database. When performs the authentication phase, all the steps are the same until have been generated template. After that, the system draws on the database and compares the new generated template with the stored template, and then outputs the output result.

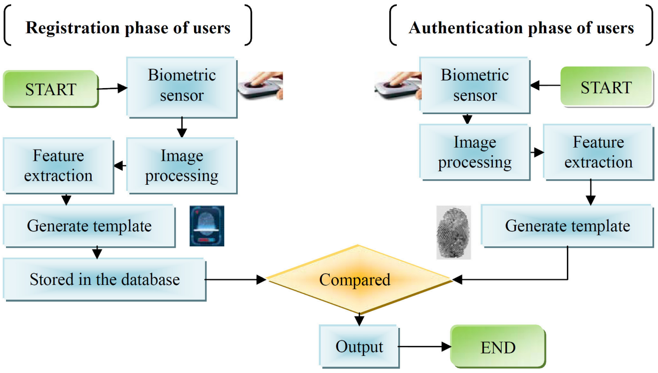


Figure 1: The composition of the proposed scheme

3 The Proposed Scheme

In this section, we introduce the proposed robust chaotic maps-based authentication key agreement scheme with privacy protection in detail. Firstly, we introduce the composition of the scheme. The proposed scheme is made up of four phases: the initialization phase, the user registration phase, the authentication key agreement phase, and the password and biometrics changing phase, respectively. Figure 2 shows the composition of the proposed scheme.

Next, we introduce the notations used in the proposed scheme. Notations are shown in Table 1.

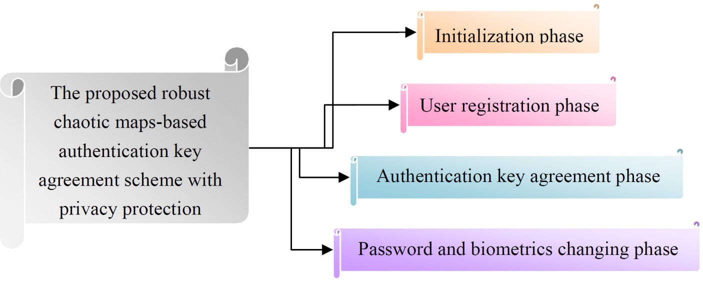

The proposed robust chaotic maps-based authentication key agreement scheme with privacy protection
Initialization phase
User registration phase
Authentication key agreement phase
Password and biometrics changing phase

Figure 2: The composition of the proposed scheme

Table 1: Notations

Notation	Definition
U_i, ID_i, PW_i	the ith user, the identity and password of the ith user, respectively
S	the server
B_i	the biometric sample of the ith user
τ	predetermined threshold for biometrics certification
$d(\cdot)$	symmetric parametric function
$(x, T_{k_i}(x)), k_i$	public key and secret key of the ith user maintained by server, respectively
m, n	random integer number
sk	session key
$h(\cdot)$	secure hash function
$\oplus$, $\|\|$	XOR operation, concatenation operation，respectively

3.1 Initialization Phase

In this phase, the server S chooses $(x, T_k(x)), k$ as its public key and secret key, and chooses a secure one-way hash function $h(\cdot)$; the ith user U_i chooses his/her identity ID_i, password PW_i and biometrics image sample B_i, respectively.

Additionally, U_i and S choose a symmetric parametric function $d(\cdot)$ and a predetermined threshold τ for biometrics certification. In each feature extraction, each different azimuth or origin of force will make the new extracted biometrics and the stored biometrics to have different degree of difference. $d(\cdot)$ is used to compute deviation degree between the results of feature extraction and the stored samples. The meaning of τ is the biggest deviation degree can be accepted.

3.2 User Registration Phase

1) U_i computes $M_i = h(ID_i || PW_i)$, $N_i = M_i \oplus h(B_i)$, and sends $N_i, h(B_i)$ to S via a secure channel.

2) S receives $N_i, h(B_i)$, stores the subscript i of N_i as an index. The subscript i is wrote in a form document which is made up of $< i, status - i >$ and $status - i$ means the login status of U_i. Then S computes $R_{U_i} = h(h(B_i)||k)$, $Z_i = R_{U_i} \oplus N_i$, stores $Z_i, N_i, h(\cdot), d(\cdot), \tau$ in a smart card, and gives the

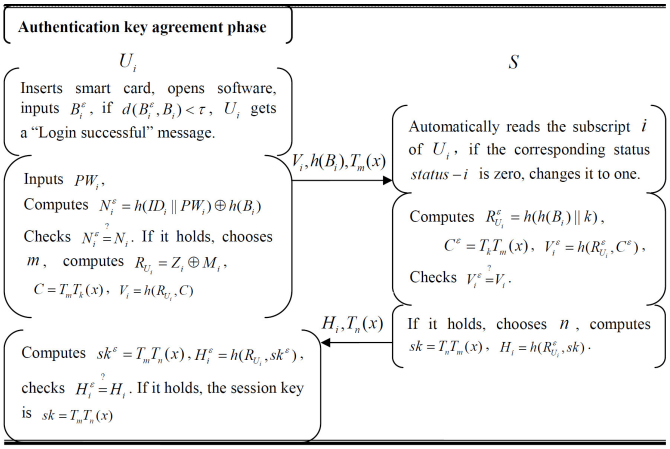
smart card to U_i via a secure channel. When U_i obtains the smart card, U_i stores B_i in it.

3.3 Authentication key agreement phase

Figure 3 shows the authentication key agreement phase as below:

1) U_i inserts the smart card into an intelligent card reader, opens the access software, inputs the biometrics B_i^ε via a sensor. Compared B_i^ε with the stored B_i, if $d(B_i^\varepsilon, B_i) \geq \tau$, U_i gets a Login failed message; if $d(B_i^\varepsilon, B_i) < \tau$, U_i gets a Login successful message.

2) After biometrics B_i login successful, U_i inputs his/her identity ID_i, password PW_i, the smart card computes $N_i^\varepsilon = h(ID_i||PW_i) \oplus h(B_i)$, and then checks whether $N_i^\varepsilon \overset{?}{=} N_i$ or not. If it does not hold, U_i gets a Wrong password message; If it holds, U_i computes $R_{U_i} = Z_i \oplus N_i$, and chooses a random integer number m, computes $C = T_m T_k(x)$, $V_i = h(R_{U_i}, C)$, and then sends $V_i, h(B_i), T_m(x)$ to S.



Inserts smart card, opens software, inputs B_i^ε, if $d(B_i^\varepsilon, B_i) < \tau$, U_i gets a "Login successful" message.

Inputs PW_i,
Computes $N_i^\varepsilon = h(ID_i \| PW_i) \oplus h(B_i)$
Checks $N_i^\varepsilon \overset{?}{=} N_i$. If it holds, chooses m, computes $R_{U_i} = Z_i \oplus M_i$,
$C = T_m T_k(x)$, $V_i = h(R_{U_i}, C)$

Automatically reads the subscript i of U_i, if the corresponding status $status - i$ is zero, changes it to one.

Computes $R_{U_i}^\varepsilon = h(h(B_i) \| k)$,
$C^\varepsilon = T_k T_m(x)$, $V_i^\varepsilon = h(R_{U_i}^\varepsilon, C^\varepsilon)$,
Checks $V_i^\varepsilon \overset{?}{=} V_i$.

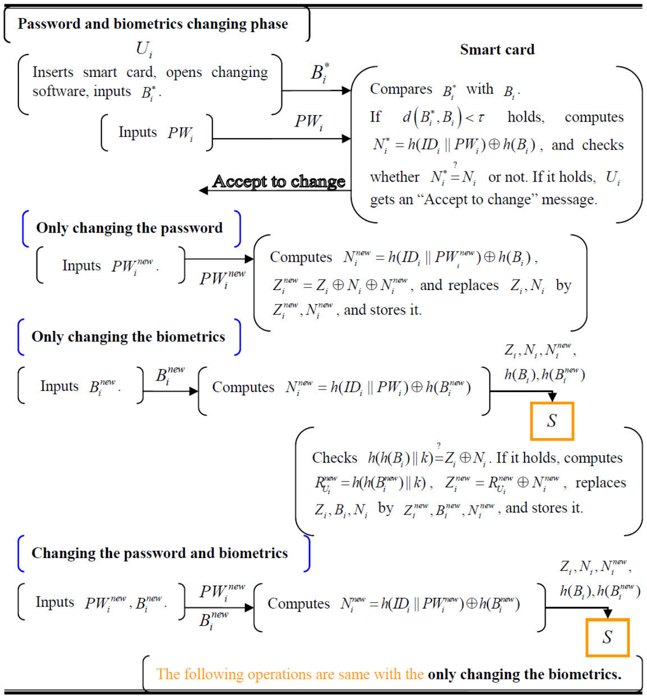
If it holds, chooses n, computes $sk = T_n T_m(x)$, $H_i = h(R_{U_i}^\varepsilon, sk)$.

Computes $sk^\varepsilon = T_m T_n(x)$, $H_i^\varepsilon = h(R_{U_i}, sk^\varepsilon)$,
checks $H_i^\varepsilon \overset{?}{=} H_i$. If it holds, the session key is $sk = T_m T_n(x)$

Figure 3: The user registration and authenticated key agreement phase

3) S reads the subscript i of V_i. If the corresponding status $status\!-\!i$ of i is equal to one, S gives a Refused to login request message to U_i; if $status - i$ is equal to zero, S changes the status $status - i$ from zero to one, and then computes $R_{U_i}^\varepsilon = h(h(B_i)||k)$, $C^\varepsilon = T_k T_m(x)$, $V_i^\varepsilon = h(R_{U_i}^\varepsilon, C^\varepsilon)$, and then checks whether $V_i^\varepsilon \overset{?}{=} V_i$ or not. If it does not hold, S stops this phase; If it holds, S chooses a random integer number n, computes $sk = T_n T_m(x)$, $H_i = h(R_{U_i}^\varepsilon, sk)$, and then sends $H_i, T_n(x)$ to U_i.

4) U_i computes $sk^\varepsilon = T_m T_n(x)$, $H_i^\varepsilon = h(R_{U_i}, sk^\varepsilon)$, and then checks whether $H_i^\varepsilon \overset{?}{=} H_i$ or not. If it does not hold, U_i stop.s this phase; If it holds, U_i and S authenticate each other and the session key is $sk = T_m T_n(x)$.



Inserts smart card, opens changing software, inputs B_i^*.

Inputs PW_i

Compares B_i^* with B_i. If $d\left(B_i^*, B_i\right) < \tau$ holds, computes $N_i^* = h(ID_i \| PW_i) \oplus h(B_i)$, and checks whether $N_i^* \overset{?}{=} N_i$ or not. If it holds, U_i gets an "Accept to change" message.

Inputs PW_i^{new}.

Computes $N_i^{new} = h(ID_i \| PW_i^{new}) \oplus h(B_i)$, $Z_i^{new} = Z_i \oplus N_i \oplus N_i^{new}$, and replaces Z_i, N_i by Z_i^{new}, N_i^{new}, and stores it.

Inputs B_i^{new}.

Computes $N_i^{new} = h(ID_i \| PW_i) \oplus h(B_i^{new})$

Checks $h(h(B_i) \| k) \overset{?}{=} Z_i \oplus N_i$. If it holds, computes $R_{U_i}^{new} = h(h(B_i^{new}) \| k)$, $Z_i^{new} = R_{U_i}^{new} \oplus N_i^{new}$, replaces Z_i, B_i, N_i by $Z_i^{new}, B_i^{new}, N_i^{new}$, and stores it.

Inputs PW_i^{new}, B_i^{new}.

Computes $N_i^{new} = h(ID_i \| PW_i^{new}) \oplus h(B_i^{new})$

The following operations are same with the **only changing the biometrics.**

Figure 4: The password and biometrics changing phase

3.4 Password and Biometrics Changing Phase

Figure 4 shows the authentication key agreement phase as below:

1) U_i inserts the smart card into an intelligent card reader, opens the password and biometrics changing software, and inputs biometrics B_i^* at a sensor.

2) The biometrics certification process stored in the smart card compares B_i^* with B_i. If $d\left(B_i^*, B_i\right) \geq \tau$ holds, U_i gets a Refused to change message; if $d\left(B_i^*, B_i\right) < \tau$ holds, U_i inputs the password PW_i, the smart card computes $N_i^* = h(ID_i||PW_i) \oplus h(B_i)$, and then checks whether $N_i^* \overset{?}{=} N_i$ or not. If it does not hold, U_i gets a Refuse to change message; if it holds, U_i gets an Accept to change message.

If only changing the password PW_i, U_i inputs the new password PW_i^{new}, the smart card computes $N_i^{new} = h(ID_i||PW_i^{new}) \oplus h(B_i)$, $Z_i^{new} = Z_i \oplus N_i \oplus N_i^{new}$, and then replaces Z_i, N_i by Z_i^{new}, N_i^{new}, and stores it.

If only changing the biometrics B_i, U_i inputs the new biometrics B_i^{new}, and computes $N_i^{new} = h(ID_i||PW_i) \oplus h(B_i^{new})$, and then sends $Z_i, N_i, N_i^{new}, h(B_i), h(B_i^{new})$ to S. S checks whether $h(h(B_i)||k) \overset{?}{=} Z_i \oplus N_i$, if it holds, S computes $R_{U_i}^{new} = h(h(B_i^{new})||k)$, $Z_i^{new} = R_{U_i}^{new} \oplus N_i^{new}$, and then sends Z_i^{new} to the smart card. Then smart card replaces Z_i, B_i, N_i, by $Z_i^{new}, B_i^{new}, N_i^{new}$, and stores it.

If changing the password and biometrics in the same time, U_i inputs the new password PW_i^{new} and the new biometrics B_i^{new}, and computes $N_i^{new} = h(ID_i||PW_i^{new}) \oplus h(B_i^{new})$, and then sends $Z_i, N_i, N_i^{new}, h(B_i), h(B_i^{new})$ to S. The following operations are same with the only changing the biometrics.

4 Performance Analysis

4.1 Provable Security under the Random Oracle Model

The adversarial model of a mutual authentication and key agreement protocol is introduced as follows. Assume that a client-server environment contains two types of participants: n users U $= \{U_1, U_2, \cdots, U_i, \cdots, U_n\}$ and a server S. The ith instance of U_i is denoted by $\prod_U^i$, and the instance of the server is denoted by $\prod_S$. An adversary named A is a probabilistic polynomial time machine. Assume that A is able to potentially control all common communications in the proposed scheme via accessing to a set of oracles (as defined below). The public parameters are known by each participant.

1) *Extract*(ID_i) query:In Extract query model, A is able to obtain the private key of ID_i.

2) *Send*$(\prod_c^k, M)$ query: In Send query model, A can send a message M to the oracle $\prod_c^k$, where $c \in \{U, S\}$. When receiving the message M, $\prod_c^k$ responds to A according to the proposed scheme.

3) $h(m_i)$ query: In this query, when A makes this hash query with message m_i, the oracle $\prod_c^k$ returns a random number r_1 and records (m_i, r_1) into a list L_H. The list is initially empty.

4) *Reveal*$(\prod_c^k)$ query:In this query model, A can obtain a session key sk from the oracle $\prod_c^k$ if the oracle has accepted. Otherwise, $\prod_c^k$ returns a null to A.

5) *Corrupt*(ID_i) query: A can issue this query to ID_i and gets back its private key.

6) *Test*$(\prod_c^k)$ query: When A asks this query to an oracle $\prod_c^k$, the oracle chooses a random bit $b \in \{0, 1\}$. If $b = 1$, then $\prod_c^k$ returns the session key. Otherwise, it returns a random value. This query measures the semantic security of the session key.

In this model, A can make Send, Reveal, Corrupt and Test queries. Note that the capabilities of the adversary can make finite queries under adaptive chosen message attacks.

In next part, we show that the proposed scheme can provide the secure authentication and key agreement under the computational Chaotic Maps-Based DiffieHellman problem (CMDHP) assumption.

Theorem 1. *Assume that A can violate the proposed scheme with a non-negligible advantage ε and makes at most q_u, q_s, q_h queries to the oracle of the user $\prod_U^i$, oracle of the server S, and h, respectively. Then we can construct an algorithm to solve the CMDHP problem with a non-negligible advantage.*

Proof. We first assume the type of attack which is impersonating the user to communicate with server. Then we can construct an algorithm to solve the CMDHP problem.

For an instance of CMDHP problem $\{x, P_1 = T_{k_i}(x), P_2 = k_i\}$, B simulates the system initializing algorithm to generate the system parameters $\{x, P_{pub-u} = P_1, h\}$, is random oracles controlled by B. Then, B gives the system parameters to A. B interacts with A as follows.

h - query: B maintains a list L_h of tuples (str_i, h_i). When A queries the oracle h on (str_i, h_i), B responds as follows:

If str_i is on L_h, then B responds with h_i. Otherwise, B randomly chooses an integer h_i that is not found in L_h, and adds (str_i, h_i) into L_h, then responds with h_i.

Reveal - query: When the adversary A makes a *Reveal*$(\prod_c^m)$ query, B responds as follows. If $\prod_c^m$ is not accepted, B responds none. Otherwise, B examines the list L_h and responds with the corresponding h_i.

Send - query: When the adversary A makes a *Send*$(\prod_c^m, start)$ query, B responds as follows.

If $\prod_c^m = \prod_u^m$, B sets $T_m(x) \leftarrow P_1$, and randomly generates the values V_i and M_i. Otherwise, B generates a random number m^*, and computes $T_m(x) \leftarrow T_{m^*}(x)$, $C^* = T_{P_2}(T_{m^*}(x))$, $V_{i^*} = h(M_{i^*}, C^*)$, and responds with $\{V_{i^*}, M_{i^*}, T_{m^*}(x)\}$, where M_{i^*} is generated by B. The simulation works correctly since A cannot distinguish whether M_{i^*} is valid or not unless A knows the identity ID_i and the password PW_i.

When the adversary A makes a *Send*$(\prod_c^m, (V_{i^*}, M_{i^*}, T_{m^*}(x)))$ query, B responds as follows. If $\prod_c^m = \prod_u^m$, B cancels the game. Otherwise, B computes $C^* = T_{m^*}(T_{P_2}(x))$, then checks whether $V_i = h(M_{i^*}, C^*) \overset{?}{=} V_{i^*}$ to authenticate the U_i. If it holds, B computes the session key $sk = T_nT_m(x)$, $H_i = h(M_i, sk)$. Then B responds the corresponding message according to the description of the proposed scheme.

When the adversary A makes a *Send*$(\prod_c^m, (H_i, T_n(x)))$ query, B responds as follows. If $\prod_c^m = \prod_s$, B cancels the game. Otherwise, B computes $sk^* = T_n(T_{m^*}(x))$, $H_{i^*} = h(M_{i^*}, sk^*)$. If A can violate a user to the authentication, it means that A can get the values of sk and $M_i = h(h(ID_i||PW_i)||B_i)$ from the list L_h and then know the value of the session key $sk = T_mT_n(x)$. Therefore, if A an violate a user to the server authentication, then B is able to solve the CMDHP problem with non-negligible probability. It is a contradicting to the intractability of the CMDHP problem. From the above analysis, we can see that the probability that A can violate the user to the server authentication is negligible.

□

4.2 Functionality Analysis

In this subsection, Table 2 shows the functionality comparisons between our proposed scheme and related schemes about three aspects as below:

No timestamp mechanism.
Timestamp is a string produced by the current time of communication entities which can replace the random numbers at some nodes with a nonce. Unfortunately, if Alice delays delivery of the message, it may bring about the interval time for message transfer is equal or greater than ΔT,then the protocol will be stopped.

Table 2: Functionality comparisons

Functionality comparisons			
	F1	F2	F3
[20]	N	Y	N
[21]	Y	Y	N
[22]	N	Y	N
Our scheme	Y	Y	Y

Annotation : F1: No timestamp mechanism; F2: Privacy protection;
F3: Biometrics certification
--: Not mentioned or not involve
Y/N: Support/Not support

Privacy protection.
Usually, personal information of users is easy to leak. To solve this problem, our proposed scheme makes the sensitive information PW_i and ID_i hidden in a secure hash function, even if the message transferred over the insecure channel is intercepted by Alice, she cannot gain any useful information from the intercepted hash function.

Biometrics certification.
Biometric technology is safer. It is not easy to forget, different to be stolen or counterfeit. In addition, it can be carry-on and available anytime and anywhere. In our proposed scheme, we use it as the first checkpoint of the authentication phase, not only can improve the security of our scheme, but also can increase the practicability of our scheme.

4.3 Efficiency Analysis

In this subsection, we analyze the efficiency of the proposed scheme, According to the required operations for communication entities in different phases, Table 3 summarizes the communication costs of our proposed scheme and related schemes in registration phase and authentication key agreement phase.

Table 3: Communication costs

Communication costs					
		[20]	[21]	[22]	Our scheme
P1	U_i	1H	1H	1H	2H
	S	1S	1E	2H	1H
	Total	1H+1S	1H+1E	3H	3H
P2	U_i	2H+2S+2C	2H+2E	5H+2C	4H+2C
	S	2H+2S+2C	2H +5E	4H+2C	2H+2C
	Total	4H+4S+4C	4H+7E	9H+4C	6H+4C

Annotation :P1: User registration phase; P2: Authentication key agreement phase
H: Hashing operation; C: Chebyshev chaotic maps operation;
S: Symmetric encryption/decryption; E: Elliptic curve multiplication

In Chang et al. [5] scheme, they showed that the average time for one time hash function operation was 0.605ms. In [14], Lee showed that one hash function operation was about one time faster than one Chebyshev chaotic maps operation. We can infer that the average time for one Chebyshev chaotic maps operation was about 1.21ms. In addition, according to [17], we can conclude that one hash function operation is about 10 times faster than a symmetric encryption/decryption. So a symmetric encryption/decryption operation was about 6.05ms.

According to Table 3, we can know that in registration phase, our proposed scheme only uses hash function operation, the execution time of registration phase is about 1.815ms; in the authentication phase, our proposed scheme uses hash operation and Chebyshev chaotic maps operation, the execution time of it is about 8.47ms. So compared with related schemes, the execution of our proposed scheme is acceptable, and our proposed scheme is more practical.

5 Conclusion

In the proposed scheme, we propose a robust chaotic maps-based authentication key agreement scheme with privacy protection using smart card. Our scheme has many practical merits: it refuses timestamp, modular exponentiation and scalar multiplication on an elliptic curve, and provides secure biometric authentication, chaotic maps-based authenticated key agreement, secure update protocol. Besides, chaos theory is only used to authenticate which can improve the efficiency of the proposed scheme. In the same time, the proposed scheme can resist various common attacks. In a word, compared with related schemes, the proposed scheme is safer and more practical.

References

[1] A. K. Awasthi, K. Srivastava, R. C. Mittal, "An improved timestamp-based remote user authentication scheme," *Computers and Electrical Engineering*, vol. 37, no. 6, pp. 69–874, 2011.

[2] K. Chain, W. C. Kuo, "A new digital signature scheme based on chaotic maps," *Nonlinear Dynamics*, vol. 74, no. 4, pp. 003–1012, 2013.

[3] C. K. Chan, L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, pp. 992–993, 2000.

[4] C. C. Chang, J. S. Lee, "An efficient and secure multi-server password authentication scheme using smart cards," in *IEEE Information Conference on Cyberworlds*, pp. 417–422, 2004.

[5] C. C. Chang, C. Y. Sun, "A Secure and Efficient Authentication Scheme for E-coupon Systems," *Wireless Personal Communications*, vol. 77, no. 4, pp. 2981–2996, 2014.

[6] F. Farhat, S. Salimi, A. Salahi, "An extended authentication and key agreement protocol of UMTS," in *Information Security Practice and Experience*, LNCS 5451, pp. 230–244, Springer, 2009.

[7] P. Gong, P. Li, W. B. Shi, "A secure chaotic maps-based key agreement protocol without using smart cards," *Nonlinear Dynamics*, vol. 70, no. 4, pp. 2401–2406, 2012.

[8] C. Guo, C. C. Chang, "Chaotic maps-based password-authenticated key agreement using smart cards," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 6, pp. 1433–1440, 2013.

[9] M. S. Hwang, L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.

[10] M. K. Khan, J. S. Zhang, X. M. Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," *Chaos, Solitons and Fractals*, vol. 35, no. 3, pp. 519–524, 2008.

[11] J. Kim, S. Jun, "Authentication and key agreement method for home networks using a smart card," in *Computational Science and Its Applications (ICCSA'07)*, LNCS 4705, pp. 655–665, Springer, 2007.

[12] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[13] S. Laur, S. Pasini, "SAS-based group authentication and key agreement protocols," in *Public Key Cryptography (PKC'08)*, LNCS 4939, pp. 197–213, Springer, 2008.

[14] C. C. Lee, "A simple key agreement scheme based on chaotic maps for VSAT satellite communications," *International Journal of Satellite Communications and Networking*, vol. 31, no. 4, pp. 177–186, 2013.

[15] C. C. Lee, C. L. Chen, C. Y. Wu, S. Y. Huang, "An extended chaotic maps-based key agreement protocol with user anonymity," *Nonlinear Dynamics*, vol. 69, no. 1-2, pp. 79–87, 2012.

[16] T. H. Liu, Q. Wang, H. F. Zhu, "A multi-function password mutual authentication key agreement scheme with privacy preserving," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 2, pp. 165–178, 2014.

[17] B. Schneier, *Applied Cryptography, Protocols, Algorithms, and Source Code in C (2nd ed.)*, New York, Wiley, 1996.

[18] J. J. Shen, C. W. Lin, M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414–416, 2003.

[19] R. Song, "Advanced smart card based password authentication protocol," *Journal of Computer Standards and Interfaces*, vol. 32, no. 5, pp. 321–325, 2010.

[20] J. E. Tapiador, J. C. Hernandez-Castro, P. Peris-Lopez, J. A. Clark, "Cryptanalysis of Song's advanced smart card based password authentication protocol," in *Cryptography and Securityin*, Nov. 11, 2011. (http://www. docin. com/ p-380824051.html)

[21] S. B. Wu, C. S. Li, "Identity-based SIP authentication and key agreement," *Advances in Intelligent and Soft Computing*, vol. 146, pp. 765–771, 2012.

[22] Q. Xie, J. M. Zhao, X. Y. Yu, "Chaotic maps-based three-party password-authenticated key agreement scheme," *Nonlinear Dynamics*, vol. 74, no. 4, pp. 1021–1027, 2013.

[23] J. Xu, W. T. Zhu, D. G. Feng, "An improved smart card based password authentication scheme with provable security," *Journal of Computer Standards and Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[24] E. J. Yoon, K. Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *The Journal of Supercomputing*, vol. 63, no. 1, pp. 235–255, 2013.

[25] L. H. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons & Fractals*, vol. 37, no. 3, pp. 669–674, 2008.

Hongfeng Zhu obtained his Ph.D. degree in Information Science and Engineering from Northeastern University. Hongfeng Zhu is a full associate professor of the Kexin software college at Shenyang Normal University. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Dr. Zhu had published more than 50 international journal and international conference papers on the above research fields.

Yifeng Zhang, 24 years old, an undergraduate from Shenyang Normal University, major in information security management. During the four years of college, after completing her studies, he enjoys reading the book related to this major. Under the guidance of the teacher, he has published two articles in EI journals.

Yan Zhang, 23 years old, an undergraduate from Shenyang Normal University, major in information security management. In the four years of college, after completing her studies, she enjoys reading the book related to this major. Under the guidance of the teacher, she has published two articles in EI journals.

Haiyang Lee, graduate, graduated from Liaoning University Population Research Institute, Master demographic now at Shenyang Normal University Dean's Office Examination Management Division, lecturers title. He researches on labor and social security, wireless computer networks, network security.