Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **3**, May **2015**

An Efficient Authenticated Key Agreement Protocol Based on Chaotic Maps with Privacy Protection using Smart Card

Hongfeng Zhu, Xin Hao and Huiyan Liu

Software College, Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
zhuhongfeng1978@163.com;Hhaoxin20110202@163.com; 64356340@qq.com

Received September, 2014; revised February, 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 environment. Nowadays, social network environment becomes more open and complex, network privacy security becomes more important. What is the security? For users, it means that the personal data and online data are not peep, intrusion, interference, illegal collection and utilization. In our paper, we propose an efficient authenticated key agreement protocol based on chaotic maps with privacy protection using smart cards. Our key idea of the protocol is to adopt chaotic maps for mutual authentication, not to encrypt/decrypt messages transferred between user and server, which can make our protocol much more efficient. Our protocol not only can achieve privacy protection, but also can avoid time-consuming modular exponentiation and scalar multiplication on elliptic curves. Meanwhile, it can resist various common arracks, and provide prefect forward secrecy and known-key secrecy. In brief, compared with related protocols, our proposed protocol is more secure and practical.
Keywords: Chaotic maps, Biometrics, Privacy protection, Key agreement, Smart card

1. **Introduction.** As we all know, chaotic system has many advantages, for example, extremely sensitive to initial parameters, unpredictability, boundeness, etc. In addition, the chaotic sequence generated by chaotic system has two properties: non-periodicity and pseudo-randomness. In a word, chaos theory has exploited a new way for cryptography with chaotic system.

In contemporary, it is a hot topic to protect the user privacy. 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, these intelligent terminals have automatic memory function. They can remember the passwords and identities of users. When these terminals are lost, stolen or being malicious attacked, the personal information of users is easy to leak.

In a client-server environment, authentication mechanism has an important position in a protocol for communication entities to certificate the identities of themselves. As is known to all, as the first person, Lamport [1] proposed a remote authentication scheme based on password tables to certificate legitimate users over insecure channel in 1981.

Then many authentication protocols [2-7] were presented and analyzed to improve the performance of it. Under normal circumstances, alphanumeric passwords are widely used to achieve the security authentication of users. However, alphanumeric passwords are easily obtained by adversaries if they have enough time and energy. So it is necessary to build safer authentication mechanisms to protect users privacy information. Many existing protocols have been designed to solve this problem.

To solve the problems of [1], in 2000, Hwang et al. [2] firstly proposed the remote user authentication scheme using smart cards without a certification table. The users passwords were maintained by the system. However, Chan et al. [8], Shen et al. [9] had pointed out that the scheme of [2] had drawbacks. Few years later, many related schemes had been presented, and improved [10-22]. However, some still had defects. In 2009, Xu et al. [14] proposed a provable password authentication scheme based on a smart card. However, Song [15] showed that the scheme of [14] is vulnerable to internal and impersonation attacks, and proposed an efficient strong smart card authentication protocol in 2010. Unfortunately, Juan et al. [16] pointed out that the improved protocol of [15] cannot resist off-line password guessing attack and also had some other weaknesses. Then Juan et al. [16] proposed an advanced password authentication protocol based on smart card in 2011. In the same year, Awasthi et al. [17] proposed a remote user authentication scheme based on timestamp using smart card without any verification table. The scheme could avoid potential risks of verification tables. In [17], remote server only kept a secret key for computing the passwords of users.

Recently, many schemes based on chaos theory have been proposed [18-20]. These schemes based on chaotic maps are able to avoid many complex operations. In 2013, Guo et al. [20] proposed a key agreement protocol based on chaotic maps, which could avoid modular exponential computing and scalar multiplication on an elliptic curve. Nowadays, as the fast development of social network, privacy protection of users becomes more and more important. In 2014, Liu et al. [21] proposed a multi-function mutual authentication key agreement scheme based on passwords with privacy preserving on an elliptic curve cryptosystem. Due to modular exponential computing and scalar multiplication on an elliptic curve, the efficiency of [21] was lower than related scheme [22] based on chaotic maps. Considered the security and efficiency, we propose an efficient mutual authentication key agreement scheme with privacy protection based on biometrics and chaotic maps using smart card.

Our contributions: (1) Our protocol can avoid modular exponential computing and scalar multiplication and resist various attacks. (2) In our protocol, 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.

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

2. **Theoretical concepts.** In this section, we introduce the concepts of one-way hash function, Chebyshev chaotic maps, biometrics certification in detail, respectively.

2.1 One-way hash function

A secure one-way hash function $h : a \to b$ has the following properties:

(1) h takes an arbitrary length of message as input and outputs a fixed length of message.

(2) Given a , it is easy to compute $h(a) = b$, but difficult to compute $h^{-1}(b) = a$.

(3) Given a , it is difficult to find a^* such that $a \neq a^*$, but $h(a) = h(a^*)$.

2.2 Chebyshev chaotic maps

Chebyshev polynomial and Chebyshev chaotic maps [12] have the following properties:

(1) Chebyshev polynomial $T_n(x) : [-1, 1] \to [-1, 1]$ is defined as

$$T_n(x) = \cos(narccos(x)). \tag{1}$$

Where n is an integer, x is a variable and the value of it belongs to the interval $[-1, 1]$ According to (1), the recurrence relation of Chebyshev polynomial is defined as

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), n \geq 2, whereT_0(x) = 1, andT_1(x) = x. \tag{2}$$

(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 lnn .

The semi-group property [23]: The semi-group property of Chebyshev polynomial defined on the interval $(-\infty, +\infty)$ holds, as follows:

$$T_n(x) \equiv (2xT_{n-1}(x) - T_{n-2}(x)) \bmod p \tag{3}$$

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

$$T_r(T_s(x)) \equiv T_{rs}(x) \equiv T_s(T_r(x)) \bmod p \tag{4}$$

In addition, the two following problems are supposed to be intractable within a 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 DiffieHellman 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 $T_s(T_r(x)) = T_{rs}(x)$.

2.3 Biometrics certification

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. In addition, it can be carry-on and available anytime and anywhere, and it is not easy to be forgot or stolen.

Fig.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.

3. The proposed scheme.

In this section, we introduce the proposed authenticated key agreement protocol based on chaotic maps with privacy protection using smart card in detail. The proposed protocol is made up of four phases: the initialization phase, the

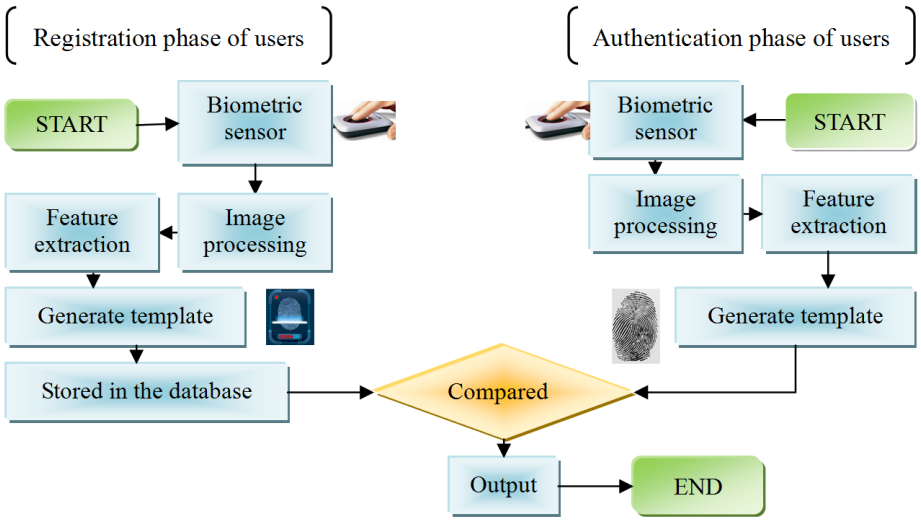

FIGURE 1. The composition of the proposed scheme

user registration phase, the authenticated key agreement phase, and the password and biometrics changing phase, respectively.

The notations used in the proposed protocol are shown in Table 1.

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
$(x, T_k(x)), k$	public key and secret key of the server, respectively
m, n	random integer number
sk	session key
$h(\cdot)$	secure one-way 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

Fig.2-1 shows the user registration phase as below:

(1) U_i computes $M_i = h(ID_i \parallel PW_i)$, $N_i = M_i \oplus h(B_i)$, 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 $R_{U_i} = h(h(B_i) \parallel k)$, $Z_i = R_{U_i} \oplus N_i$, stores Z_i , N_i , $h(\cdot)$, $d(\cdot)$, τ 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

Fig.2 shows the authentication key agreement phase as below:

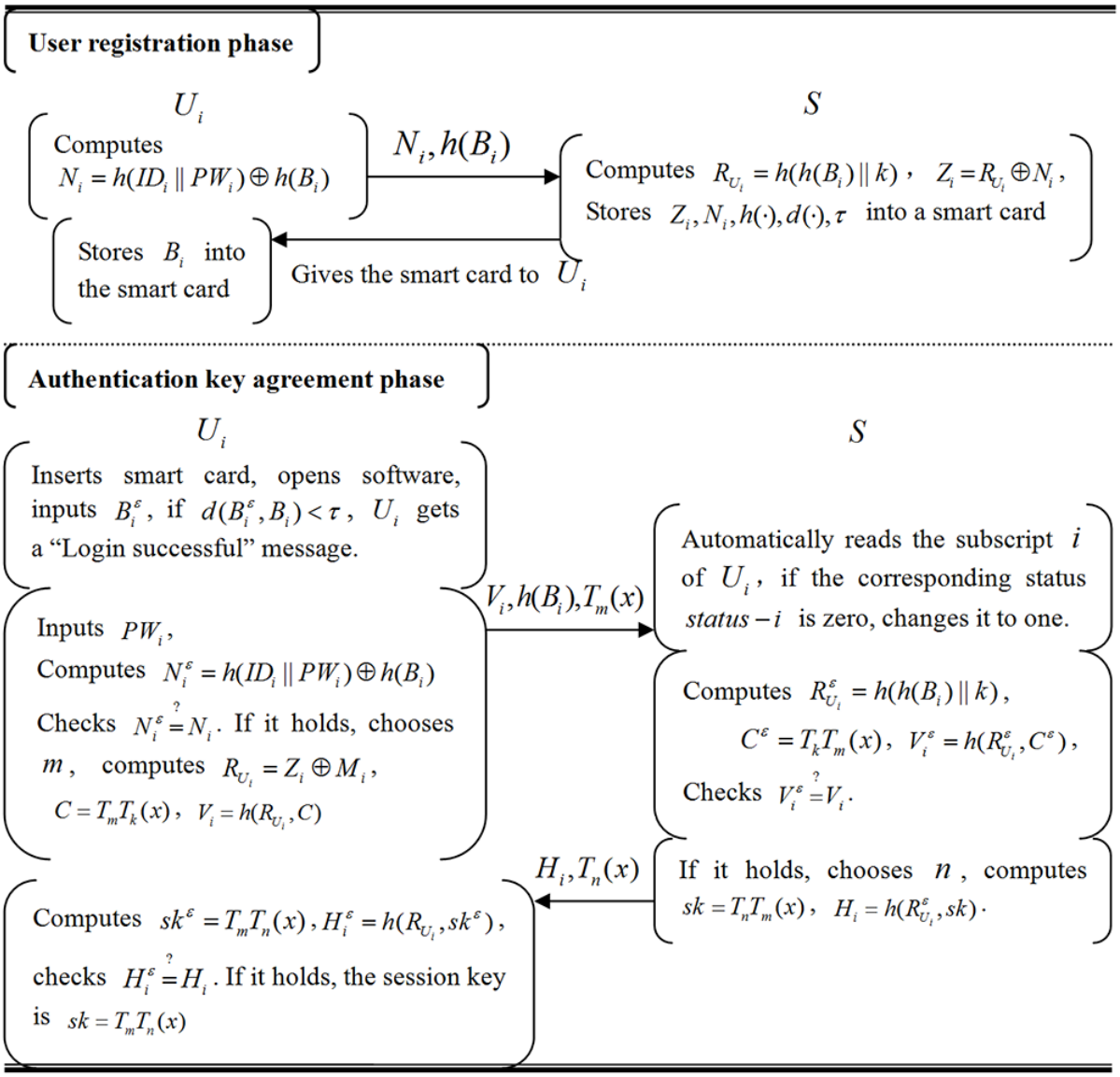

FIGURE 2. The user registration and authenticated key agreement phase

(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 $N_i^{\varepsilon} = h(ID_i \parallel PW_i) \oplus h(B_i)$, and then checks whether $N_i^{\varepsilon} =$

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 .

(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 V_i ; if $status - i$ is equal to zero, S changes the status $status - i$ from zero to one, and then computes $R_{U_i}^{\varepsilon} = h(h(B_i) \parallel k)$, $C^{\varepsilon} = T_k T_m(x)$, $V_i{}^{\varepsilon} = h(R_{U_i}^{\varepsilon}, c^{\varepsilon})$, and then checks whether $V_i{}^{\varepsilon} = V_i$ or not. If it does not hold, S stops this phase; If it holds, S chooses a random integer number n , computes $sk = T_n T_m(x)$, $H_i{}^{\varepsilon} = h(R_{U_i}^{\varepsilon}, sk)$, and then sends H_i , $T_n(x)$ to U_i .

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

3.4 Password and biometrics changing phase

Fig. 3 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 $d(B_i{}^*, B_i) \geq \tau$ holds, U_i gets a Refused to change message; if $d(B_i{}^*, B_i) < \tau$ holds, U_i inputs the password PW_i , the smart card computes $N_i{}^* = h(ID_i \parallel PW_i) \oplus h(B_i)$, and then checks whether $N_i{}^* = N_i$ 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 $N_i{}^{new} = h(ID_i \parallel PW_i{}^{new}) \oplus h(B_i)$, $Z_i{}^{new} = Z_i \oplus N_i \oplus N_i{}^{new}$, 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 $N_i{}^{new} = h(ID_i \parallel PW_i{}^{new}) \oplus h(B_i{}^{new})$, and then sends Z_i , N_i , $N_i{}^{new}$, $h(B_i)$, $h(B_i{}^{new})$ to S . S checks whether $h(h(B_i) \parallel k) = Z_i \oplus N_i$, if it holds, S computes $R_{U_i}^{new} = h(h(B_i{}^{new}) \parallel k)$, $Z_i{}^{new} = R_{U_i}^{new} \oplus N_i{}^{new}$, 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 $N_i{}^{new} = h(ID_i \parallel PW_i{}^{new}) \oplus h(B_i{}^{new})$, 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.** In this section, we analyze the performance of the proposed protocol. We prove that it can satisfy various requests in some specific situations.

4.1 Security analysis

Security analysis is a kind of systematic analysis which can ensure that in the protocol exchange process, the illegal users cannot get more useful information than the protocol itself reflected. Assume that an adversary called Alice, she can obtain any message transferred and simulate a communicate between and . In the below subsections, we achieve the performance analysis in detail.

Perfect forward secrecy

Our proposed scheme can provide perfect forward secrecy because the establishment of a session key between communication entities does not depend on the previously established session keys. Even though Alice can intercept the parameters $T_m(x)$ and $T_n(x)$, which are usually transmitted on a channel. However, she cannot compute the following

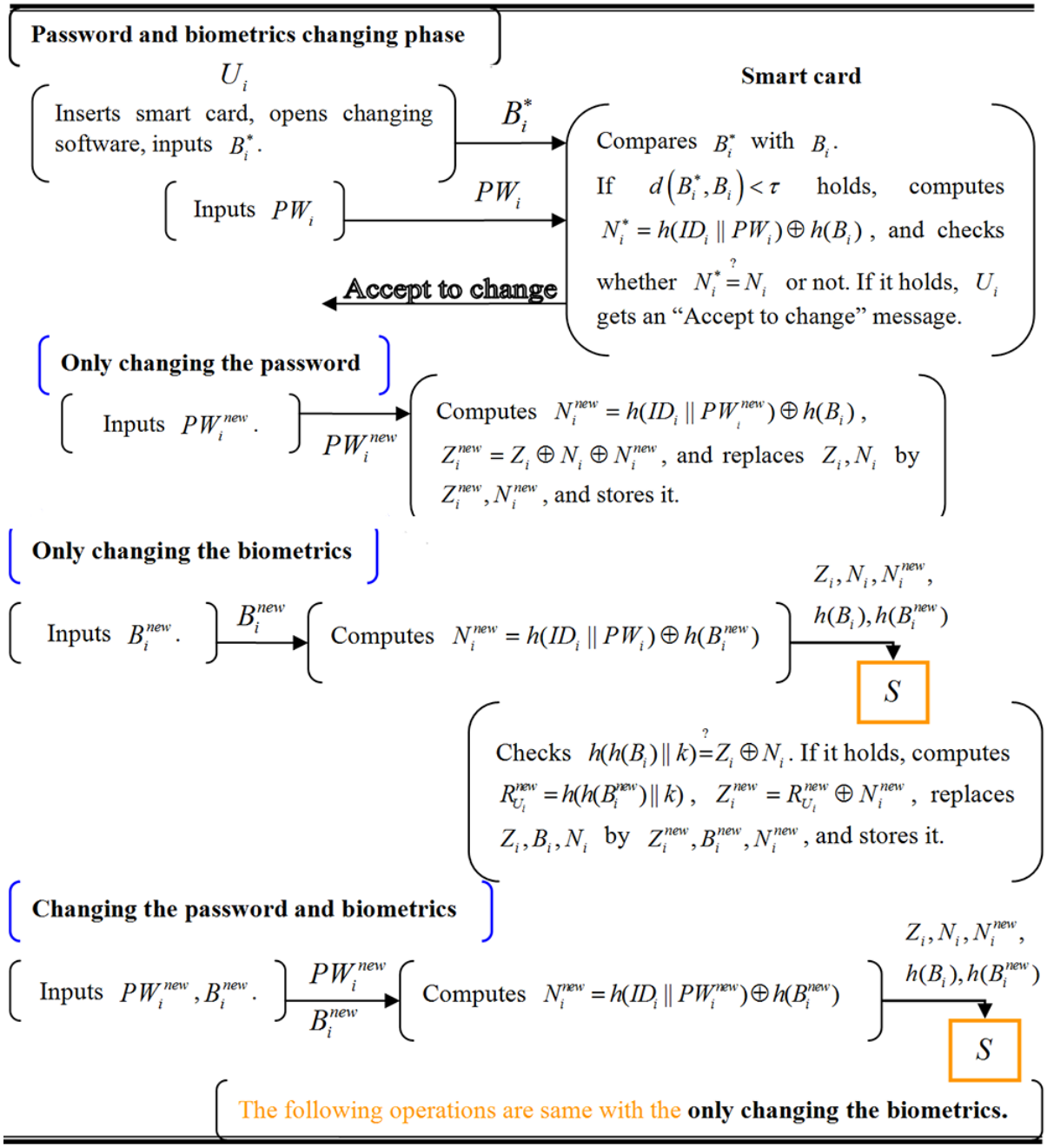

FIGURE 3. The password and biometrics changing phase

session key $sk = T_m(T_n(x))$ due to the intractability of CMDHP and CMDLP, Alice cannot previously obtain the following established session key.

Known-key secrecy

Our proposed scheme can provide known-key secrecy because the following session keys cannot be disclosed even if the previous session keys are intercepted by Alice. Supposing that Alice intercepts a session key $sk = T_m(T_n(x))$ and knows random parameters m and n , she cannot gain the previous and the future session keys due to unknown the corresponding random parameters.

Mutual authentication and key agreement

Mutual authentication and key agreement means U_i and S can authenticate each other and establish a session key. In the user registration phase, after receiving N_I,$h(B_i)$ from U_i

, S uses its secret key k to compute $R_{U_i} = h(h(B_i) \parallel k)$. In the authenticated key agreement phase, U_i extracts $R_{U_i} = Z_i \oplus N_i$, and 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 . After S ensures that $status - i$ is equal to zero which means U_i is legal login, S computes $R^{\varepsilon}_{U_i} = h(h(B_i) \parallel k)$,$C^{\varepsilon} = T_k T_m(x)$,$V_i^{\varepsilon} = h(R^{\varepsilon}_{U_i}, C^{\varepsilon})$, and then checks whether $V_i^{\varepsilon} = V_i$ or not. If it holds, that means that S authenticates U_i successfully. Then S chooses n , computes $sk = T_n T_m(x)$,$H_i = h(R^{\varepsilon}_{U_i}, sk)$, and then sends H_i, $T_n(x)$ to U_i .U_i computes $sk^{\varepsilon} = T_n T_m(x)$,$H_i^{\varepsilon} = h(R_{U_i}, sk^{\varepsilon})$, and checks whether $H_i^{\varepsilon} = H_i$ or not. If it holds, that means that U_i authenticates S successfully. Then U_i and S authenticate each other and establish a session key $sk = T_n T_m(x)$.

Secure password and biometrics changing protocol

For users, it is crucial to change freely their passwords and biometrics which can be easily remembered in a secure environment. In our proposed protocol, even though the smart card is stolen by Alice, she cannot obtain any information because all of the information is protected in a one-way hash function. In addition, when changing the password or the biometrics, the changing protocol can use N_i to certificate the correctness of B_i and PW_i .

Resist various attacks

(1)Login-in/Password guessing/Impersonation/Man-in-the-middle attack

In the authenticated key agreement phase, assume that Alice can pass the biometrics certification, Alice inputs PW_{Alice} , the smart card computes $N_i^{Alice} = h(ID_i \parallel PW_{Alice}) \oplus h(B_i)$, and then checks whether $N_i^{Alice} = N_i$ or not. If it does not hold, U_i gets a Wrong password message. However, ID_i,PW_i is protected in a one-way hash function, it is a virtual impossibility for Alice to guess the correct password. So our proposed protocol can resist password guessing attack.

Assume that Alice impersonate U_i and send V_i,$h(B_i)$,$T_m(x)$ to S . However, if U_i is landing and the status $status - i$ of it is equal to one. When Alice sends V_i,$h(B_i)$,$T_m(x)$ to S , and S checks whether $status - i$ is equal to zero or not. If it does not hold, S refuses to the login request. So the proposed protocol can resist login-in attack; if U_i is off-line, S changes $status - i$ from zero to one, and then computes $R^{\varepsilon}_{U_i} = h(h(B_i) \parallel k)$, $C^{\varepsilon} = T_k T_m(x)$, $V_i^{\varepsilon} = h(R^{\varepsilon}_{U_i}, C^{\varepsilon})$, and then checks whether $V_i^{\varepsilon} = V_i$ or not. If it holds, S chooses n , computes $sk = T_n T_m(x)$,$H_i = h(R^{\varepsilon}_{U_i}, sk)$, and then sends H_i,$T_n(x)$ to Alice. Even though Alice has got the parameters $T_m(x)$ and $T_n(x)$, she cannot obtain sk because of the intractability of CMDHP and CMDLP. In the same reason, Alice cannot obtain sk as a man in the middle. Above all, our proposed protocol can resist impersonation attack and man-in-the-middle attack.

(2) Server spoofing attack

Our proposed scheme can resist server spoofing attack. In the user registration phase, k is the secret key of S , only S knows k . Others are impossible to know the value of k , and cannot compute R_{U_i} . Without the value of R_{U_i} , Alice cannot pass the authentication of U_i in the authenticated key agreement phase.

(3) Insider attack

Our proposed scheme can resist insider attack. As a malicious insider attacker, Alice always attempts to maliciously gain the personal information of users using his/her authorized access. However, in our proposed, and are protected in a secure hash function, Alice is impossible to know and from the hash function.

All of above prove that our proposed scheme is secure. Table 2 shows the security comparisons between our proposed scheme and related schemes.

TABLE 2. Security comparisons

Security comparisons										
	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
[20]	Y	Y	Y	Y/--	--	--	--	--	--	Y
[21]	Y	Y	Y	Y/--	Y	Y	Y	Y	Y	Y
[22]	Y	Y	Y	N/N	--	Y	--	--	--	Y
Our scheme	Y	Y	Y	Y/Y	Y	Y	Y	Y	Y	Y

Annotation : S1: Perfect forward secrecy; S2: Known-key secrecy;
S3: Mutual authentication and key agreement;
S4: Secure password/biometrics changing protocol; S5: Resist login-in attack
S6: Resist password guessing attack; S7: Resist impersonation attack;
S8: Resist man-in-the-middle attack; S9: Server spoofing attack;
S10: Resist insider attack
--: Not mentioned or not involve Y/N: Support/Not support

4.2 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.

In Chang et al. [24] scheme, they showed that the average time for one time hash function operation was 0.605ms. In [25], 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 [26], 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.

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

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 an efficient 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] Lamport L, Password authentication with insecure communication. *Communications of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.

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

[3] C.C. Chang and J.S. Lee. An efficient and secure multi-server password authentication scheme using smart cards, *IEEE information conference on Cyberworlds*, pp. 417-422, 2004..

[4] J. Kim and S. Jun, *Authentication and key agreement method for home networks using a smart card*, LNCS 4705, Springer, pp. 655-665, 2007.

[5] S. Laur and S. Pasini, *SAS-based group authentication and key agreement protocols*, LNCS 4939, Springer, pp. 197-213, 2008.

[6] F. Farhat and S. Salimi and A. Salahi. *An extended authentication and key agreement protocol of UMTS*, LNCS 5451, Springer, pp. 230-244, 2009.

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

[8] C.K. Chan, L.M. Cheng. Cryptanalysis of a remote user authentication scheme using smart cards, *IEEE Trans. Consumer Electronics*, vol. 46, pp. 992-993, 2000.

[9] J.J. Shen, C.W. Lin and M.S. Hwang. A modified remote user authentication scheme using smart cards, *IEEE Trans. Consumer Electronics*, vol. 49, no. 2, pp. 414-416, 2003.

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

[11] E.J. Yoon and 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.

[12] 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.

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

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

[15] R. Song. Advanced smart card based password authentication protocol, *Journal of Computer Standards & Interfaces*, vol. 32, no. 5, pp. 321-325, 2010.

[16] Tapiador. Juan E., Hernandez-Castro. Julio C., Peris-Lopez P. and Clark John A, Cryptanalysis of Songs advanced smart card based password authentication protocol, 2011

[17] A.K. Awasthi, K. Srivastava andR.C. Mittal, An improved timestamp-based remote user authentication scheme, *Computers and Electrical Engineering*, vol. 37, no. 6, pp. 869-874, 2011.

[18] C.C. Lee. A simple key agreement scheme based on chaotic maps for VSAT satellite communications, *International Journal of Satellite Communications and Networking*, Published online: 21 June 2013.

[19] K. Chain and W.C. Kuo. A new digital signature scheme based on chaotic maps, *Nonlinear Dynamics*, vol. 74, no. 4, pp. 1003-1012, 2013.
[20] C. Guo and 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.
[21] T.H. Liu, Q. Wang and 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.
[22] C.C Lee, C.L. Chen, C.Y. Wu and 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.
[23] L.H. Zhang, Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fract, 2008.
[24] C.C. Chang and C.Y. Sun, A Secure and Efficient Authentication Scheme for E-coupon Systems, *Wireless Personal Communications*, Published online: 11, 2014.
[25] C.C Lee, A simple key agreement scheme based on chaotic maps for VSAT satellite communications, *International Journal of Satellite Communications and Networking*, Published online: 21, 2013.
[26] Schneier B., *Applied cryptography, protocols, algorithms, and source code in C* (2nd ed.). New York, USA: Wiley. 2013.