Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **5**, September **2017**

A New Authenticated Key Agreement Protocol based on Extended Chebyshev Maps

Aiwan Fan[1], Zhaofeng Yang [1*] and Haifeng Li[2]

[1]School of Computer Science
Pingdingshan University
Pingdingshan 467002,China
[2]School of Software
Dalian University of Technology
Dalian 116620, China
*corresponding author:yzfpds@163.com

Received February, 2017; revised June, 2017

Abstract. *A single server can provide services for all registered remote users. Therefore, they cannot acquire network service from different servers without registering in these servers. Although, some papers solve this problem, they cannot achieve strong security features. So we propose a new authenticated key agreement protocol based on Chebyshev maps and extended chotic maps under multi-server environment. The new scheme has the following three advantages: 1) user only need to register one time for different servers; 2) it has the strong anonymity, which can resist various Hacker attacks; 3) the new scheme does not need to use the verification sheet. At last, we compare the new scheme to some other authenticated key agreement protocols, the experiment results show that our scheme has the efficiency and security.*

Keywords: Strong security feature, Authenticated key agreement protocol, Chebyshev maps, Extended chotic maps, Multi-server environment, Verification sheet

1. **Introduction.** With the rapid development of electronic industry, small equipments with low energy consumption[1] (such as smart CARDS) are widely used, and relevant applications related to the smart card have been developing rapidly. In order to protect the privacy information of server, authentication protocols based on the password are concerned widely. At present, many researchers introduce smart card to the password authentication protocol to improve the efficiency and safety of this agreement[2-5]. Most of the above protocols are designed for single server environment. However, people need to login different servers to get more applications in real life. So multi-server authentication protocol has attracted more attention from researchers.

As we all know, chaotic maps has been developed rapidly in recent years. Due to the good properties (sensitivity, ergodicity and pseudo randomness) of chaotic maps, researchers use chaotic system to design symmetric cryptosystem [6,7], stream cipher [8,9] and hash function [10]. Lately, chaotic maps has been introduced into authentication protocol for single server environment, so authenticated key agreement protocols based on chaotic maps are proposed [11-14]. Additionally, Prof.Chen makes a great contribution to provably secure cloud-Assisted emergency system such as [15-18].

Li [19] presented a remote password authentication scheme for multiserver environments. The password authentication system was a pattern classification system based on an artificial neural network. In this scheme, the users only remembered user identity and password numbers to log in to various servers. Users could freely choose their password. Furthermore, the system was not required to maintain a verification table and could withstand the replay attack. Wang [20] proposed an improved dynamic ID-based remote user authentication scheme for multi-server environment. Besides, security analysis and performance analysis showed that compared with other remote user authentication schemes, the proposed scheme was more secure and possesses lower computation cost. Ruhul Amin [21] proposed an efficient three-party authenticated key exchange protocol using smart card based on the cryptographic one-way hash function. The formal security analysis proves that proposed protocol provides strong security protection on the relevant security attacks including the above-mentioned security weaknesses. Chuang [22] proposed an anonymous multi-server authenticating key agreement scheme based on trust computing using smart cards, password, and biometrics. The scheme not only supported multi-server environments but also achieved many security requirements. In addition, the scheme was a lightweight authentication scheme which only used the nonce and a hash function. Memon [23] described a new authentication method based on a cryptographic protocol including a zero-knowledge proof that each node must use to convince another node on the possession of certain secret without revealing anything about it, which allowed encrypted communication during authentication. The proposed protocol featured with the following characteristics: Firstly, it offered anonymous authentication: a message issuer can authenticate itself. Secondly, it provided confidential: the secrecy of the communication content could be protected. The address configuration scheme must lower the cost in order to enhance the scalability. Thirdly, it was efficient: it achieved low storage requirements, fast message verification and cost-effective identity tracking in case of a dispute. Lee [24] proposed an improved multiserver authentication protocol with key agreement based on extended chaotic maps. But this protocol does not have strong anonymous characteristics. In the multi-server environment, strong anonymity of agreement indicates that when legitimate users access to a server resource, the other legitimate users and other internal servers also cannot get related identity information of communicating parties.

So we propose a new authenticated key agreement protocol based on Chebyshev maps and extended chotic maps under multi-server environment. the results show that our scheme has the efficiency and security. The followings are the structures of this paper. In section2, we introduce Chebyshev chaotic mapping. Section3 detailed introduces the new scheme. We give the security analysis and performance analysis in section4 and section5. There is a conclusion in section6.

2. **Chebyshev chaotic mapping.** In this section, we define three concepts to illustrate Chebyshev chaotic mapping.

1. **Definition 1**. In Chebyshev polynomials $T_n(x)$, $x \in [-1, 1]$ is variable, n is the order of polynomials. $T_n(x) : [-1, 1] \to [-1, 1]$ is defined as:

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

So $T_n(x)$ can be written as:

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

Where $T_0(x) = 1$, $T_1(x) = x$. $T_n(x)$ has Chaos and semigroup characteristics.

- Chaos characteristics. When $n > 1$, $T_n(x)$ is Chaos maps and its measure is $f^*(x) = \frac{1}{\pi\sqrt{1-x^2}}$.

- Semigroup characteristics.

$$T_r(T_s(x)) = cos(rcos^{-1}(scos^{-1}(x))) = T_{sr}(x) = T_s(T_r(x)). \tag{3}$$

Chebyshev polynomial semigroup features can be extended and is proved that it still has the semigroup features in $(-\infty, +\infty)$.

$$T_n(x) \equiv 2xT_{n-1}(x) - T_{n-2}(x)modP. \tag{4}$$

Where $x \in (-\infty, +\infty), n \geq 2$. Obviously,

$$T_r(T_s(x)) \equiv T_{sr}(x) \equiv T_s(T_r(x))modP. \tag{5}$$

The extended Chebyshev polynomials has two polynomial time problems.

2. **Definition 2**. Discrete logarithm problem (DLP). Given two elements y and $x \in (-\infty, +\infty)$ and a prime number P. Find an integer s, make $T_s(x) \equiv ymodP$.
3. **Definition 3**. (Computational Diffie-Hellman problem, CDHP)[21,22]. Given three elements x, $T_r(x)modP$ and $T_s(x)modP$, compute $T_{rs}(x)modP$.

3. **New authenticated key agreement protocol.** There are three main members in this protocol: legal users U_i, servers $S = S_1, \cdots, S_n$ and registration center (RC). In the initial stage, RC first selects a random number x and a number sr as master key. Then it calculates $\omega_i = h(sr||S_i)$ and sends ω_i to server S_i through secure channel. Protocol includes two stages: register stage and login, key agreement stage.

1. Register stage. U_i needs to register as a valid user which can acquire the service from server $S = S_1, \cdots, S_n$. The detailed register processes are as follows (flow chart is as figure1).
   - Firstly, U_i selects his own identify ID_i, password pw_i and a random number N_i, then it sends the message $(ID_i, pw_i \oplus N_i)$ to RC.
   - RC calculates $v_{ij} = h(ID_i||P_{ij}||\omega_j$ and $u_{ij} = v_{ij} \oplus pw_i \oplus N_i$. Where P_{ij} is period of validity of the server j. Then it keeps the $(ID_i, u_{ij}, P_{ij}, x, T_{\omega_j}(x), h(\cdot), P)$ into the smart card of U_i. The smart card will be sent to U_i.
   - After receiving smart card, it computes $u'_{ij} = u_{ij} \oplus N_i$ and replaces u'_{ij} by using u_{ij}.
2. Login, key agreement stage. In this stage, user U_i has to login server S_j to start secure communication. This stage's flow chart is as figure2. The detailed processes are as follows:
   - U_i inserts his own smart card into card reader and inputs password pw'_i.
   - Smart card first computes $v'_{ij} = u_{ij} \oplus pw'_i$ and then selects a random number r to calculate,

$$C_1 = T_r(x)modP. \tag{6}$$

$$C_2 = T_r(T_{\omega_j}(x))modP. \tag{7}$$

$$C_3 = E_{C_2}(ID_i||P_{ij}||v'_{ij}). \tag{8}$$

   - U_i sends message $M_1 = (x, C_1, C_3)$ to server S_j.

   After receiving message M_1, server S_j dose the following operation,
   - S_j computes $C'_2 = T_{\omega_j}(C_1)modP$.
   - It uses C'_2 to decrypt C_3 and gets $ID_i||P_{ij}||v'_{ij}$. It checks the validity of P_{ij}, if it exceeds the validity, S_j stops the service for U_i.
   - It calculates $v_{ij} = h(ID_i||P_{ij}||\omega_j)$. If v_{ij} is not equal to v'_{ij}, S_j stops the service for U_i.

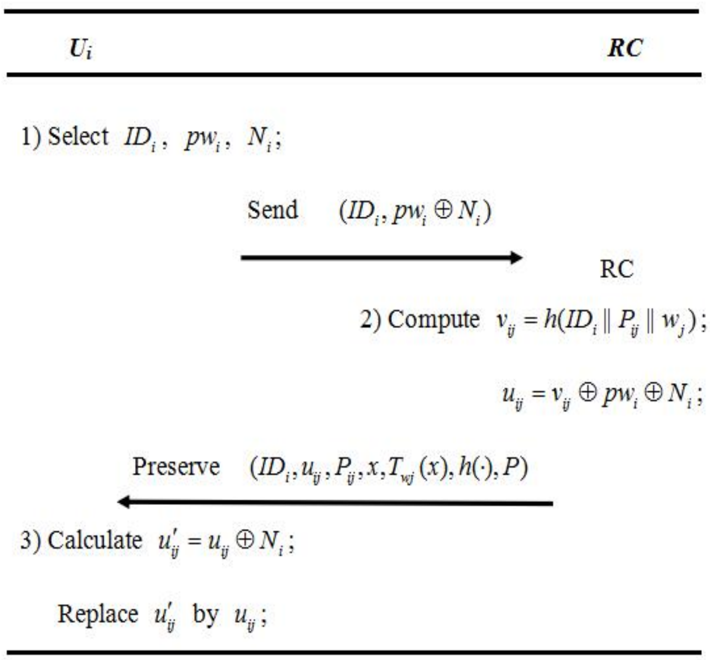

FIGURE 1. Flow chart of register stage

- S_j randomly generates a number s, it computes $C_4 = T_s(x) mod P$ and $SK = T_s(C_1) mod P$.
- S_j computes $C_5 = E_{C'_2}(ID_i||S_j||C_4)$.
- S_j sends message $M_2 = C_5$ to user U_i.

After receiving the message M_2, user U_i does the following operation,

- It uses C_2 to decrypt C_5 and gets $ID_i||S_j||C_4$. It checks the validity of S_j and ID_i, if it exceeds the validity, this session will exit.
- It calculates $SK' = T_r(C_4) mod P$.
- It calculates $C_6 = h(C_4||SK')$.
- U_i sends message $M_3 = C_6$ to user server S_j.

After receiving message M_3, server S_j does the following operation,

- It computes $C_7 = h(C_4||SK)$.
- If $C_7 \neq C_6$, then it exists this session.

According to semigroup feature, $SK = SK'$ is right. U_i and S_j generates a same session key which can protect the later communication.

4. **Formal security proof.** In this section, formal security proof of our new scheme can be demonstrated through six attack aspects.

1. New protocol can resist privileged users' attack. In the contemporary world, users would use the resources from different servers. So users may use same passwords to access different servers. The password may be leaked to the privileged users in one server. In the new protocol, U_i can send message $(pw_i \oplus N_i)$ to RC in register stage (namely, it uses random number N_i to hide pw_i). For each privileged user, $(pw_i \oplus N_i)$ only is a random number, so other users cannot acquire the related information of password pw_i). Therefore, privileged users cannot attack the new protocol effectively.
2. New protocol has strong anonymity. This indicates that knowing session key attack can be defended with our new protocol. In the multi-server environment, it requires that other servers cannot get the identify in one session.

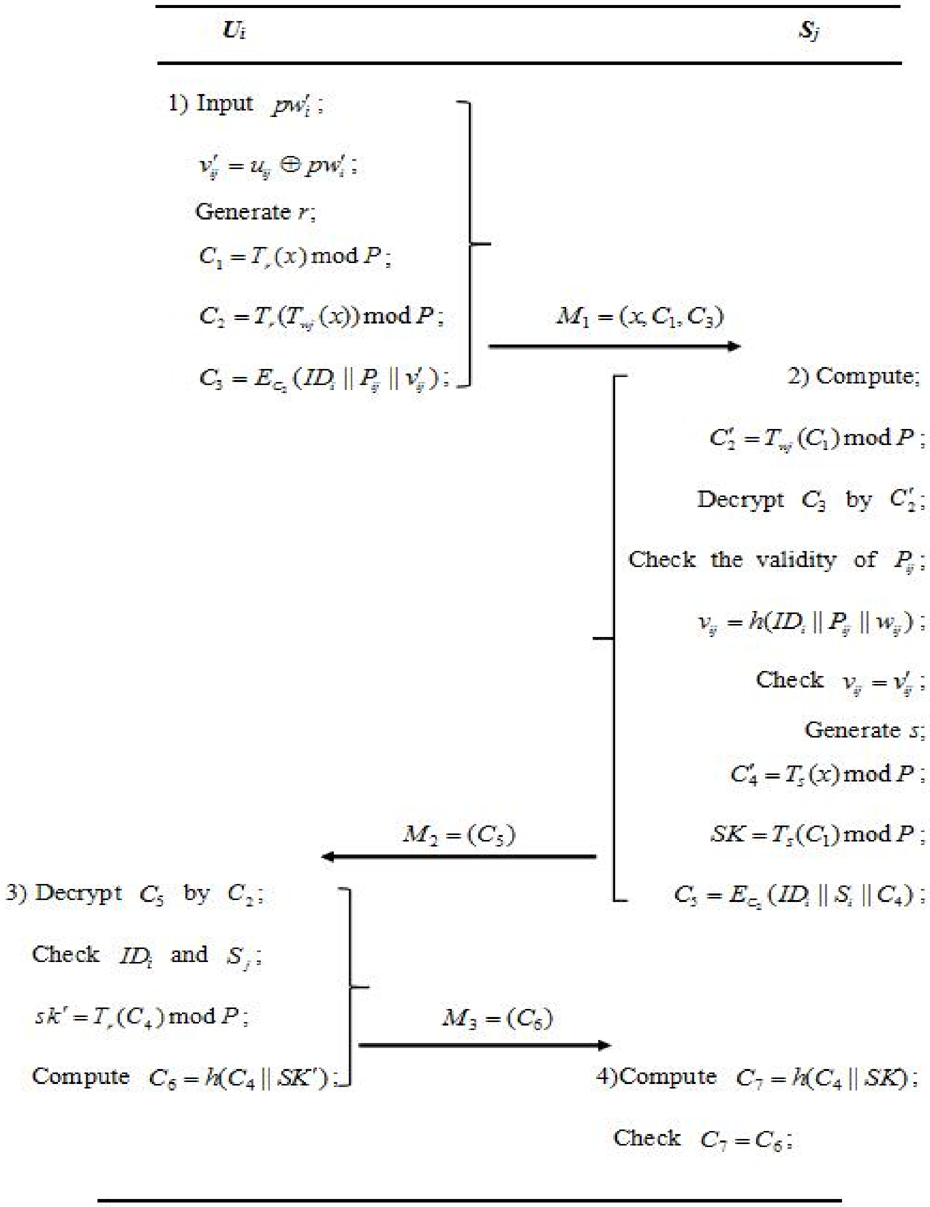

FIGURE 2. Flow chart of login, key agreement stage

Attacker controls the communication channel between user and server and tries to find the identify of user or server. In this new protocol, user sends message $M_1 = (x, C_1, C_3)$ and $M_3 = (C_6)$ to server. In $M_1 = (x, C_1, C_3)$, the user's identify information hides in $C_3 = E_{C_2}(ID_i||P_{ij}||v_{ij}'$. If attacker wants to acquire the user's identify information, it must decrypt massage C_3. Because attacker does not know private key ω_j, if it calculates C_2, the DLP of extended chebyshev polynomial must be solves. In each session, users always select a random number,so in message M_1, second item and third item of chebyshev polynomial is changing. Attacker cannot find the connection between user's identify and message M_1. In the authentication message $M_3 = (C_6)$, there is no identify information, so there is no help for attacker cracking the anonymity.

3. New protocol can resist replay attack. If attacker eavesdrops the communication between user U_i and server S_j, then it can get the message (M_1, M_2, M_3) of many sessions. In the later communication, attacker replays message (M_1). In that the

temporary private key is different in every session, when attacker receives message (M_2), so it cannot generate correct validation message (M_3). Finally, the server gives up this session. If attacker replays this message (M_2), due to new random number used in this session, it cannot be through the user's authentication and user will give up this session. Similarly, attacker replays this message (M_3), it cannot be through the server's authentication.

4. New protocol has two-way authentication feature. Public key system based on the extended chebyshev polynomial is introduced into authentication protocol. Based on the principle of digital envelope, we use the public symmetric key generated by public key system and send the encrypted message to the opposite side. After receiving ciphertext, receiver uses the public key to decrypt ciphertext and verifies the the opposite side's identify by using decrypted plaintext. Therefore, ciphertext not only has security, but has authentication. Because attacker cannot acquire the private key of both communication sides, it cannot get the correct symmetric key. So it cannot generate correct encryption message to complete the verification.
5. New protocol can resist impersonation attack. Namely, it also can resist password-guessing attack. Password-guessing attack is divided into online and offline guessing. Online guessing is active attack. In a real environment, it usually limits the login number to prevent on;line password guessing attack. Offline guessing is passive attack, if attacker gets the secret message of smart card through energy analysis or side-channel attack, it can combine offline guessing to attack authentication protocol, which will lead to greatly harm.

   In the new scheme, assuming that attacker gets smart card information $(u_{ij}, P_{ij}, x, T_{\omega_j}(x))$ of valid user U_i and monitors the message $(M_1 = (x, C_1, C_3))$. Attacker launches an offline guessing attack by using the following ways.
   - Attacker guesses that the password of U_i is pw'.
   - Compute $v_{ij} = u_{ij} \oplus pw'_i$.
   - Compare the v_{ij} to v'_{ij} in C_3. If they are the same, the guessing is correct. Otherwise, repeat step1.

   However, attacker does not know the temporary private key and ω_j in $T_{\omega_j}(x)$. If it computes C_2, the CDHP of extended chebyshev polynomial must be solved. So attacker cannot verify the guessing password. Similarly, although attacker monitors the message $M_2 = C_5$, it cannot verify the guessing password too.
6. New protocol can resist compromise impersonation attack. In that our new scheme has forward security characteristic, which indicates that both communication sides leak private key long time. But the security of previous session key is not affected. In new protocol, supposing that attacker gets password pw_i and ω_j, then attacker can obtain $T_r(x) mod P$ and $T_s(x) mod P$. But it calculates the session key, the $T_{rs}(x) mod P$ must be computed.

5. **Performance analysis.** In this section, we make comparison to other schemes (Reference[27], Reference[28], Reference[29], CDC[24]) to illustrate the performance of our method(CMEC). Table1 is the comparison results. a denotes the time of running Chebyshev polynomials; b denotes the time of running symmetric encryption or decryption algorithm; c denotes the time of running one-way hash function.

As we all know, computational complexity relation: $a \approx 70b \approx 175c$ and $b \approx 2.5c$. Compared to the above three operations, computational complexity of XOR operation is low, so it can be ignored. Supposing that the output of random number and hash function is 128bit, public-key encryption output based on chaotic mapping is 128bit too. In table1, MSECC only uses one-way hash function to realize authentication

Table 1. Security comparison with different schemes

Scheme	Register stage	Authentication stage	Total computation complexity
Reference[23]	3c	8c	11c
Reference[24]	4c+a	6c+4a+3b	$\approx 28c$
Reference[25]	4c+a	6c+4a+3b	$\approx 28c$
CDC	3c	11c+6a	$\approx 1064c$
CMEC	2c	3c+4b+6a	$\approx 1064c$

protocol, so the computational complexity is very low. Compared to other protocols, MSECC needs RC to participate in authentication stage, which adds the burden of RC and reduces the flexibility of protocol. In addition, MSECC cannot resist internal privileged user attack, replay attack and offline password guessing attack without strong anonymity. ABM and LLW do not use public key cryptography scheme based on chaotic mapping, so they has lower computational complexity than new protocol. But they cannot resist internal privileged user attack, replay attack and offline password guessing attack without strong anonymity and forward security characteristic. CDC has the same computational complexity with new scheme and they also can resist various attacks. However, CDC has not strong anonymity. New scheme realizes the authentication with less time. Therefore, our scheme has security and high-efficiency.

We also make security comparison to Reference[23], Reference[23], Reference[25], CDC[20] with our new scheme. Supposing that G_T is bilinear target group. Table2 is the computation complexity with different schemes. Where symbols p, e_T, e and h denote bilinear pairings operation, exponential operation in G_T, exponential operation in G and Hash operation. Their coefficients are operation numbers. From the table, we can know that our new scheme needs the least operation time. In addition, it has the optimal encryption results.

Table 2. Computation complexity with different schemes

Stage	Reference[23]	Reference[23]	Reference[25]	CDC	New scheme
Encryption	$p + e_T + 3e + 2h$	$2p + e_T + 2e + h$	$2e + 2h$	$3e + e_T$	$2e$
Deryption	$2p + 2e_T + h$	$3p + 3e + h$	$3e + p + 2h$	$2p + e$	$3e$
ReEnryption	$3\|G\|$	$\|G_T\| + \|G\|$	$\|2Z_q^*\|$	$\|2Z_q^*\|$	$\|Z_q^*\|$
ReDeryption	$3p + e_T + e + 2h$	$2p + e_T + e + h$	$3e + e_T + T$	$4e + 3p$	$4e$

6. **Conclusions.** Chaotic mapping with its high efficiency has attracted widely attention by the researchers. So we propose a new authenticated key agreement protocol based on Chebyshev maps and extended chotic maps. New protocol uses the public key cryptosystem based on chaotic maps to generate shared symmetric key and sends uses the encrypted message to the other parties. After receiving information, receiver adopts the semigroup of chaotic mapping feature to calculate the session key. At last, security analysis shows that the new protocol can resist various attacks. Performance analysis shows that the new protocol does not increase the computational complexity and strong anonymity is realized. As a result, the new agreement has both security and efficiency.

Acknowledgment. This work is supported by Science & Technology Planning Project of Henan Province under Grant No. 152102210193.

REFERENCES

[1] D. Kolokotsa , M. Santamouris Review of the indoor environmental quality and energy consumption studies for low income households in Europe, *Journal of Science of the Total Environment,* vol. 536, pp. 316-330, 2015.

[2] J. Moon, Y. Choi, J. Kim, et al., An Improvement of Robust and Efficient Biometrics Based Password Authentication Scheme for Telecare Medicine Information Systems Using Extended Chaotic Maps, *Journal of Journal of Medical Systems*, vol. 40, no. 3, pp. 70, 2016.

[3] Jiang Q, Ma J, Lu X, et al. Robust Chaotic Map-based Authentication and Key Agreement Scheme with Strong Anonymity for Telecare Medicine Information Systems, *Journal of Journal of Medical Systems*, vol. 38, no. 38, pp. 12, 2014.

[4] C. T. Li , C. C. Lee , C. C. Wang , et al., Design Flaws in a Secure Medical Data Exchange Protocol Based on Cloud Environments, *Algorithms and Architectures for Parallel Processing. Springer International Publishing*, 2015.

[5] H. Y.Lin, Chaotic Map Based Mobile Dynamic ID Authenticated Key Agreement Scheme, *Journal of Wireless Personal Communications*, vol. 78, no. 2, pp. 1487-1494, 2014.

[6] Yap W S, Phan C W, Yau W C, et al. Cryptanalysis of a new image alternate encryption algorithm based on chaotic map, *Journal of Nonlinear Dynamics*, vol. 80, no. 3, pp. 1483-1491, 2015.

[7] Liu Q, Li P Y, Zhang M C, et al. A novel image encryption algorithm based on chaos maps with Markov properties, *Journal of Communications in Nonlinear Science & Numerical Simulation,* vol. 20, no. 2), pp. 506-515, 2015.

[8] M. Almazrooie , A. Samsudin ,M. M. Singh Improving the Diffusion of the Stream Cipher Salsa20 by Employing a Chaotic Logistic Map, *Journal of Journal of Information Processing Systems*, vol. 11, no. 2, pp. 310 324, 2015.

[9] M. A. A. Wasi, S. Windarta, Modified SNOW 3G: Stream cipher algorithm using piecewise linear chaotic map *American Institute of Physics Conference Series. AIP Publishing LLC*,, pp. 47-58, 2016.

[10] San-Um W, Srichavengsup W. A Robust Hash Function Using Cross-Coupled Chaotic Maps with Absolute-Valued Sinusoidal Nonlinearity, Journal of International Journal of Advanced Computer Science & Applications, 2016, 7, no. 1).

[11] T. F.Lee, Enhancing the security of password authenticated key agreement protocols based on chaotic maps, *Journal of Information Sciences*, vol. 290, pp. 63-71, 2015.

[12] H. F. Zhu , H. Y. Liu , Y. F, Zhang et al., Three-party authentication key agreement protocol based on chaotic maps in the standard model with privacy preserving , *Journal of Information Hiding & Multimedia Signal Processing*, vol.6, no. 6, pp. 1077-1087, 2015.

[13] Zhu H, Hao X. An Efficient Authenticated Key Agreement Protocol Based on Chaotic Maps with Privacy Protection Using Smart Card, Journal of Nonlinear Dynamics, 2015, 81(1-2).

[14] M. S. Farash , M. A. Attari, An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps, *Journal of Nonlinear Dynamics*, vol. 77, no. 1-2, pp. 1-13, 2014.

[15] C.M. Chen, C.T. Li, S. Liu, T.Y. Wu, J.S. Pan, "Design of A Provably Secure Cloud-Assisted Emergency System for Mountaineering Events, *Journal of IEEE Access*, vol. 5, no. 1, pp. 3410-3422, 2017.

[16] C.M. Chen, W. Fang, K.H. Wang, T.Y. Wu, Comments on An improved secure and efficient password and chaos-based two-party key agreement protocol, *Nonlinear Dynamics,* vol. 87, no. 3, pp 2073-2075, 2017.

[17] Y. Chen, C.M. Chen, J. S. Pan, T.Y. Wu, S. Liu, Security improvement on a three party password based authenticated key exchange scheme using chaotic maps, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1365-1372, 2016.

[18] C.M. Chen, L. Xu, T.Y. Wu, C.R. Li, On the Security of a Chaotic Maps-based Three-party Authenticated Key Agreement Protocol, *Journal of Network Intelligence,* vol .1 , no. 2, 61-66, May 2016.

[19] L. H.Li. L. C. Lin , M. S. Hwang A remote password authentication scheme for multiserver architecture using neural networks ., *Journal of IEEE Transactions on Neural Networks,* vol. 12, no. 6, pp. 1498-1504, 2001.

[20] Z. Z. Wang , J. K. Ding , Z. P. Jin , et al., Improvement of a Dynamic ID-Based Remote User Authentication Scheme for Multi-Server Environment Using Smart Card, *Journal of Applied Mechanics & Materials*, no. 380-384, pp. 286-289, 2013.

[21] R. Amin, G. P. Biswas, Cryptanalysis and Design of a Three-Party Authenticated Key Exchange Protocol Using Smart Card, *Journal of Arabian Journal for Science & Engineering*, vol. 40, no. 11), pp. 1-15, 2015.

[22] Chuang M C, Chen M C. An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics, Journal of Expert Systems with Applications, 2014, 41, no. 4, pp. 1411-1418.

[23] I. Memon, A Secure and Efficient Communication Scheme with Authenticated Key Establishment Protocol for Road Networks, *Journal of Wireless Personal Communications An International Journal*, vol. 85, no. 3, pp. 1-25, 2015.

[24] Lee C C, Lou D C, Li C T, et al. An extended chaotic-maps-based protocol with key agreement for multiserver environments, *Journal of Nonlinear Dynamics,* vol. 76, no. 1, pp. 853-866, 2013.

[25] H. Li, S. L. Yin, C. Zhao and T. Lin, A Proxy Re-Encryption Scheme Based on Elliptic Curve Group. Journal of Information Hiding and Multimedia Signal Processing, Vol. 8, No. 1, pp. 218-227, January 2017.

[26] S. L. Yin, H. Li and J. Liu, A New Provable Secure Certificateless Aggregate Signcryption Scheme. *Journal of Information Hiding and Multimedia Signal Processing,* vol. 7, no. 6, pp. 1274-1281, November 2016.

[27] Jian Shu. An efficient three-party password-based key agreement protocol using extended chaotic maps, *Journal of Chinese Physics B*, vol. 24, no. 6):231-238, 2015.

[28] Lee T F. Efficient three-party authenticated key agreements based on Chebyshev chaotic map-based DiffieCHellman assumption, *Journal of Nonlinear Dynamics*, vol. 81, no. 4, pp. 2071-2078, 2015.

[29] X. Wang , S. Wang , Z. Wang, et al., A new key agreement protocol based on Chebyshev chaotic maps, *Journal of Security & Communication Networks*, 2016.