Nonlinear Dyn (2013) 73:125–132
DOI 10.1007/s11071-013-0772-4

ORIGINAL PAPER

A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps

Cheng-Chi Lee · Chun-Ta Li · Che-Wei Hsu

Received: 21 November 2012 / Accepted: 10 January 2013 / Published online: 23 January 2013

Abstract In this paper, we propose a scheme utilizing three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps, which is more efficient and secure than previously proposed schemes. In order to enhance the efficiency and security, we use the extended chaotic maps to encrypt and decrypt the information transmitted by the user or the server. In addition, the proposed protocol provides user anonymity to guarantee the identity of users, which is transmitted in the insecure public network.

Keywords Anonymity · Chaotic maps · Authenticated key exchange · Password-based · Three-party

C.-C. Lee · C.-W. Hsu
Department of Library and Information Science, Fu Jen Catholic University, 510 Jhongjheng Rd., Sinjhuang City, New Taipei City 24205, Taiwan, ROC

C.-C. Lee
e-mail: cclee@mail.fju.edu.tw

C.-C. Lee
Department of Photonics & Communication Engineering, Asia University, No. 500, Lioufeng Road, Wufeng Shiang, Taichung 402, Taiwan, ROC

C.-T. Li (✉)
Department of Information Management, Tainan University of Technology, 529 Zhongzheng Road, Tainan 710, Taiwan, ROC
e-mail: th0040@mail.tut.edu.tw

1 Introduction

In order to guarantee the security of secret keys which are exchanged over the insecure public network, there are many related protocols [4, 5, 15, 16, 18, 24] which have been proposed by researchers, such as Password-Authenticated Key Exchange (PAKE) protocol. PAKE protocol allows two parties to keep one identical memorable password to agree on a common session key over the insecure public network [9, 19, 20, 26]. Generally, password-based authentication can resist both the brute force and the dictionary attacks if users choose strong passwords to provide enough entropy. Nevertheless, password-based authentication has one intrinsic problem: users are not adept in memorizing text strings. Hence, most users would select memorable passwords even if they know the passwords might be unsafe, so that it is not easy to protect the password information against various attacks. According to the protocol proposed by Lin et al. [17], we can divide the attacks into the following classes:

- Off-line dictionary attacks: The adversary first guesses a password and then verifies its guess in an off-line mode only by using the eavesdropped information. No participation of the honest client or the server is required, so these attacks cannot be noticed.
- Undetectable on-line dictionary attacks: The adversary attempts to verify a password guess in an on-line transaction. Nevertheless, a failed guess cannot

be detected by the honest client or by the server, since one of them is not able to distinguish a malicious request from an honest one.
- Detectable on-line dictionary attacks: Similar to above, the adversary tries to use a guessed password in an on-line transaction. The adversary verifies the correctness of its guess by using the response from the honest client or the server. But a failed guess can be detected by the honest client or the server.

Among these attacks, both off-line and undetectable on-line dictionary attacks can cause serious consequences against password-based authentication protocol. Hence, it is a crucial consideration to design a secure password-based authentication protocol, which can resist the mentioned above attacks.

In 1992, Bellovin and Merritt [2] proposed the first PAKE protocol. After a decade, many related protocols, such as both the two-party PAKE [4, 5, 18] and the three-party PAKE [11, 12, 15, 16, 24, 33] have been proposed. However, Hassan and Abdullah [8] pointed out that two-party PAKE protocols are not suitable in the large peer-to-peer architecture. Also, some of the three-party PAKE protocols are not secure or efficient enough to be used in practice. Recently, Abdalla et al. [1] and Lu et al. [22] proposed two efficient three-party password-based key exchange protocols in 2005 and 2007, respectively. Unfortunately, both of their protocols were still vulnerable to undetectable on-line dictionary attacks or off-line dictionary attacks. In 2009, Deng et al. [6] proposed a three party password-based key exchange protocol and declared that their protocol was secure under the universal composable framework (UC-SECURE). However, Yuan et al. [36] pointed out that Deng et al.'s protocol is insecure against offline dictionary attack by any other client. In 2011, Yoon and Yoo proposed a protocol [34] and pointed out that Huang's protocol [10] could not resist undetectable on-line dictionary attacks and key-compromise impersonation attack. Subsequently, Yoon and Yoo also proposed another protocol [35] and showed that Lou and Huang's protocol [21] was vulnerable to off-line password guessing attacks by an attacker. Later, Wu et al. [30] also found the security weaknesses of Huang's protocol [10] and proposed a three-party password-based authenticated key exchange protocol to solve the problems in Huang's protocol. However, Wu et al.'s protocol had many exponential computations, which required the highest computational complexity. Their protocol also could not provide user anonymity.

In order to enhance the efficiency and security, we propose a three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps. In the past decade, cryptography based on Chebyshev chaotic maps has been studied widely, such as symmetric encryption protocols [25, 27, 29], S-boxes [28], and hash functions [31, 32]. The proposed protocol uses the extended chaotic maps both to encrypt and to decrypt the information transmitted by the user or the server. The proposed protocol can also provide mutual authentication between user and server and user anonymity to guarantee the identity of users, which is transmitted in the insecure public network. The security and performance analysis show that the proposed protocol has low computation and communication cost and can also resist against various attacks.

The remainder of this paper is organized as follows. Section 2 briefly introduces the definitions of Chebyshev chaotic maps. The proposed protocol is presented in Sect. 3. Then we analyze the proposed protocol and show that the protocol can resist against several attacks in Sect. 4. In Sect. 5, we will compare the performance of our protocol with the previous protocols. Finally, our conclusion is presented in Sect. 6.

2 Preliminaries

In this section, we will introduce some concepts used in our protocol, such as the Chebyshev chaotic maps, the DLP and the DHP problems.

2.1 Chebyshev polynomials

We first briefly describe Chebyshev polynomials [23] as follows. The Chebyshev polynomial $T_n(x)$ is a polynomial in x of degree n. Let n be an integer, and x be a variable taking value over the interval $[-1,\ 1]$. The Chebyshev polynomial $T_n(x) : [-1,\ 1] \rightarrow [-1,\ 1]$ is defined as

$$T_n(x) = \cos\big(n \cdot \arccos(x)\big).$$

The recurrence relations of Chebyshev polynomials are given by

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), \quad n \geq 2,$$
$$T_0(x) = 1,$$
$$T_1(x) = x.$$

Table 1 The notations used in our protocol

Notation	Definition
A, B	two identity of clients (users)
TS	a TS (remote server)
PW_A, PW_B	the password shared between user A (resp. B) and server TS
p	a large prime number
s	a random integer chosen by TS
r	a random number chosen by TS
Q	the public key of TS, where $Q \equiv T_s(r) \bmod p$
SK	the session key used between user A and B
x, y	two random integers
t_1	the time-stamp
$h(\cdot)$	a secure hash function
$\|$	the concatenation operation
$\oplus$	the exclusive-or (XOR) operation

The $\cos(x)$ and $\arccos(x)$ are the trigonometric functions [3]. They are defined as $\cos: R \to [-1, 1]$ and $\arccos: [-1, 1] \to [0, \pi]$. There are some examples of Chebyshev polynomials that are shown as follows:

$$T_2(x) = 2x^2 - 1,$$
$$T_3(x) = 4x^3 - 3x,$$
$$T_4(x) = 8x^4 - 8x^2 + 1,$$
$$T_5(x) = 16x^5 - 20x^3 + 5x.$$

The Chebyshev polynomials exhibit the following two important properties [7, 14]: the semigroup property and the chaotic property.

(1) The semigroup property:

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

r and s are positive integer numbers and $x \in [-1, 1]$.

(2) The chaotic property:

When the degree $n > 1$, the 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 $\lambda = \ln n > 0$.

In 2008, Zhang [37] proved that the semigroup property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$, which can enhance the property, as follows:

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

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

$$T_r\big(T_s(x)\big) \equiv T_{sr}(x) \equiv T_s\big(T_r(x)\big) \bmod p,$$

so the semigroup property still holds and the enhanced Chebyshev polynomials also commute under composition.

2.2 The DLP and the DHP problems

The Chebyshev polynomials have the following two problems, which are assumed to be difficult to handle within a polynomial time algorithm:

(1) The discrete logarithm problem (DLP) is described as follows: given two elements x and y, find the integer r, such that $T_r(x) = y$.
(2) The Diffie-Hellman problem (DHP) is described as follows: given three elements x, $T_r(x)$, and $T_s(x)$, compute the value $T_{rs}(x)$.

3 Our proposed protocol

In this section, the proposed protocol with user anonymity using extended chaotic maps is described in detail, which is based on Wu et al.'s protocol [30]. The notations used in our protocol are summarized in Table 1.

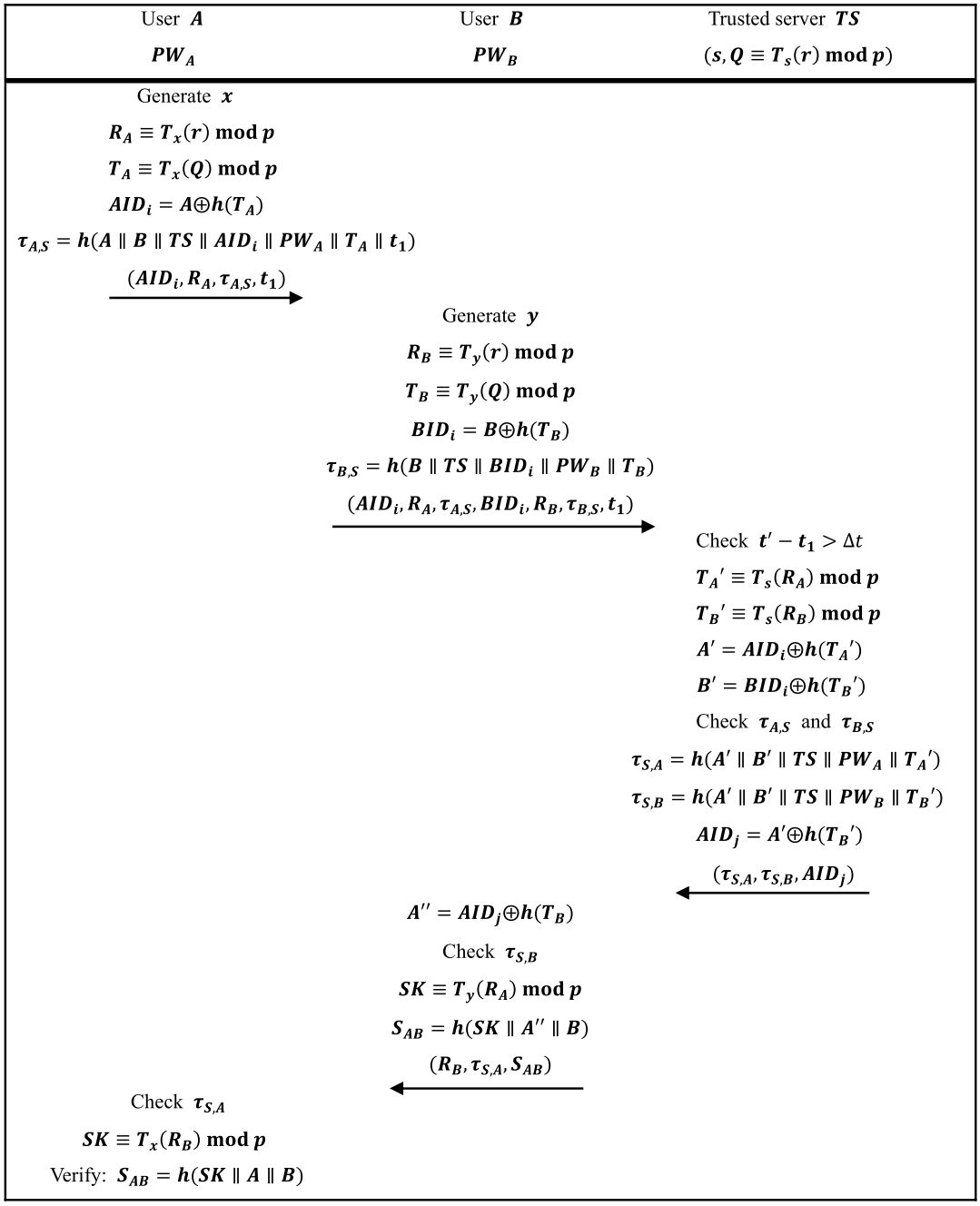

Fig. 1 Our proposed protocol

In the beginning, the remote server *TS* selects a random number r, a random integer s, and computes its public key $Q \equiv T_s(r) \bmod p$. The remote server *TS* keeps its private key s secretly. In our protocol, we assume the two users A and B have already established the common secret key share passwords PW_A, PW_B with the remote server *TS*, respectively. The remote server *TS* distributes the public parameters $(Q, r, h(\cdot), p)$ to all parties in the network. The simplified description of the proposed protocol is shown in Fig. 1. From this point, the details of the proposed protocol are described in the following steps:

(1) User A chooses a random integer x and computes the following:

$$R_A \equiv T_x(r) \bmod p,$$
$$T_A \equiv T_x(Q) \bmod p,$$
$$AID_i = A \oplus h(T_A),$$
$$\tau_{A,S} = h(A \parallel B \parallel TS \parallel AID_i \parallel PW_A \parallel T_A \parallel t_1).$$

User A sends $(AID_i, R_A, \tau_{A,S}, t_1)$ to user B.

(2) After receiving $(AID_i, R_A, \tau_{A,S}, t_1)$, user B chooses a random integer y and computes the following:

$$R_B \equiv T_y(r) \bmod p,$$
$$T_B \equiv T_y(Q) \bmod p,$$
$$BID_i = B \oplus h(T_B),$$
$$\tau_{B,S} = h(B \parallel TS \parallel BID_i \parallel PW_B \parallel T_B).$$

Then user B sends $(AID_i, R_A, \tau_{A,S}, BID_i, R_B, \tau_{B,S}, t_1)$ to the remote server TS.

(3) Upon receiving $(AID_i, R_A, \tau_{A,S}, BID_i, R_B, \tau_{B,S}, t_1)$, the server TS first checks the validity of t_1 by checking whether the equation $t' - t_1 > \Delta t$ holds, where the t' is the time when the server receives the messages from B. Δt denotes the predetermined legal time interval of transmission delay. If the equation does not hold, then the server TS calculates $T'_A \equiv T_s(R_A) \bmod p$, $T'_B \equiv T_s(R_B) \bmod p$, $A' = AID_i \oplus h(T'_A)$, and $B' = BID_i \oplus h(T'_B)$ and uses them to check $\tau_{A,S}$ and $\tau_{B,S}$, respectively. If the values are invalid, TS terminates the protocol. Otherwise, TS computes $\tau_{S,A} = h(A' \parallel B' \parallel TS \parallel PW_A \parallel T'_A)$, $\tau_{S,B} = h(A' \parallel B' \parallel TS \parallel PW_B \parallel T'_B)$, and $AID_j = A' \oplus h(T'_B)$ and then sends $(\tau_{S,A}, \tau_{S,B}, AID_j)$ to user B.

(4) After receiving $(\tau_{S,A}, \tau_{S,B}, AID_j)$, user B first computes $A'' = AID_j \oplus h(T_B)$ and checks the validity of $\tau_{S,B}$ using T_B. If the value is invalid, B terminates the protocol. Otherwise, both server TS and user B are authenticated and user B computes the common session key $SK \equiv T_y(R_A) \bmod p$ and $S_{AB} = h(SK \parallel A'' \parallel B)$. Finally, B sends $(R_B, \tau_{S,A}, S_{AB})$ to user A.

(5) Upon receiving $(R_B, \tau_{S,A}, S_{AB})$, user A first checks the validity of $\tau_{S,A}$ using T_A. If the value is invalid, A terminates the protocol. Otherwise, user A computes the common session key $SK \equiv T_x(R_B) \bmod p$ and checks the validity of $S_{AB} = h(SK \parallel A \parallel B)$. If it does not hold, A terminates the protocol. Otherwise, both server TS and user A are authenticated and the common session key SK is agreed upon. Then, both user A and user B can use the common session key SK for secure communication. The common session key SK is only used for one session.

4 Security analysis

In this section, we analyze the security and performance of our protocol and show it could resist against various attacks. Here, we describe several security analyses in our proposed protocol.

A. Off-line dictionary attacks The attacker may intercept the messages $(AID_i, R_A, \tau_{A,S}, t_1)$ or $(AID_i, R_A, \tau_{A,S}, BID_i, R_B, \tau_{B,S}, t_1)$ and try to guess the password from the element $\tau_{A,S}$ or $\tau_{B,S}$. However, the attacker cannot successfully verify the password without knowing T_A or T_B, which are generated by user A and B respectively based on the difficulty of the DLP problem. Hence, our protocol is secure against the off-line dictionary attacks.

B. Undetectable on-line dictionary attacks The attacker may intercept the messages $(AID_i, R_A, \tau_{A,S}, t_1)$ or $(AID_i, R_A, \tau_{A,S}, BID_i, R_B, \tau_{B,S}, t_1)$ and try to impersonate a legal user. But the attacker cannot send a new valid message $(AID_i, R_A, \tau_{A,S}, BID_i, R_B, \tau_{B,S}, t_1)$ to the trusted server unless he/she has guessed the correct password. Moreover, if the attacker tries to guess the password, he/she will face the DLP problem. Therefore, our protocol can resist the undetectable on-line dictionary attacks.

C. Detectable on-line dictionary attacks The attacker may intercept the messages $(AID_i, R_A, \tau_{A,S}, t_1)$ or $(AID_i, R_A, \tau_{A,S}, BID_i, R_B, \tau_{B,S}, t_1)$ and try to impersonate a legal user. But the attacker cannot send a new valid message $(AID_i, R_A, \tau_{A,S}, BID_i, R_B, \tau_{B,S}, t_1)$ to the trusted server unless he/she has guessed the correct password. Moreover, the server will check the correctness of $\tau_{A,S}$ and $\tau_{B,S}$. Hence, the attacker will be detected if he/she sends an invalid message to the server. In that case our protocol is secure against the detectable on-line dictionary attacks.

Table 2 Comparison of security properties

	Huang's protocol	Lou and Huang's protocol	Lee et al.'s protocol	Wu et al.'s protocol	Our protocol
Off-line dictionary attacks	Yes	No	Yes	Yes	Yes
Undetectable on-line dictionary attacks	No	Yes	Yes	Yes	Yes
Replay attack	No	Yes	Yes	Yes	Yes
User anonymity	No	No	No	No	Yes
Mutual authentication	No	Yes	Yes	Yes	Yes

Table 3 Comparison of performance

	Huang's protocol		Lou and Huang's protocol		Lee et al.'s protocol		Wu et al.'s protocol		Our protocol	
	U	S	U	S	U	S	U	S	U	S
Modular exponential	4	2	0	0	6	4	8	2	0	0
Hash/TDF operation	6	4	4	2	2	2	6	2	6	5
Chebyshev chaotic map operation	0	0	0	0	0	0	0	0	6	2
Random number	2	1	2	1	4	1	4	0	2	0
XOR operation	4	4	2	2	2	2	2	2	3	3
Round	5		5		5		5		4	

D. Replay attack The attacker may intercept the messages from a user and replay them to the server in the next run. Nevertheless, the server could find the attack by checking the validity of the time-stamp t_1. The attacker may also intercept the messages from the server and replay it to user. However, the users have generated the new random integers x and y. Then user A and B could find the attack by verifying the correctness of $\tau_{S,A}$ and $\tau_{S,B}$, respectively. Hence, our protocol can resist the replay attack.

E. User anonymity The attacker may eavesdrop the communication between the user and the trusted server, and try to trace the user's real identity to find some security-sensitive information of the user. In our proposed protocol, the real identity of user A and B are protected by $AID_i = A \oplus h(T_A)$ and $BID_i = B \oplus h(T_B)$, respectively. In order to compute T_A and T_B, the attacker will face the DLP problem. Hence, our protocol can provide the user with a high degree of anonymity.

F. Mutual authentication Our protocol can achieve mutual authentication between the user and the server. In step 3 of our protocol, the server TS must verify the validity of $\tau_{A,S}$ and $\tau_{B,S}$ in order to authenticate user A and B. User A and B also must verify the validity of $\tau_{S,A}$ and $\tau_{S,B}$, respectively, in order to authenticate server TS. If there is an attacker who wants to forge messages, he/she will face not only the DLP but also the DHP problems. Therefore, as both the user and the trusted server can authenticate each other, the mutual authentication between them is achieved.

5 Performance discussion

In this section, we discuss the performance of our proposed protocol. We compare the security properties of our protocol with Huang's protocol [10], Lou and Huang's protocol [21], Lee et al.'s protocol [13], and Wu et al.'s protocol [30] in Table 2.

In Table 2, we can see that our protocol is more secure than other protocols. We also compare the performance of our protocol with other protocols in Table 3. In Table 3, U denotes the user and S denotes the server. The computational complexity of modular

exponential is higher than all other operations such as hash computation and Chebyshev chaotic maps, which can be done efficiently. Our protocol is more efficient than other protocols even if the costs of our protocol are slightly higher than Lou and Huang's protocol. However, Lou and Huang's protocol is vulnerable to the off-line dictionary attacks and also cannot provide user anonymity. As shown in Table 2, none of the other protocols can provide user anonymity. Hence, our protocol is more efficient and secure than others since our protocol only uses hash operation and XOR operation and also can provide user anonymity.

6 Conclusion

In this article, we propose a three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps, which is more efficient and secure than previously proposed schemes. In order to enhance the efficiency and security, we use the extended chaotic maps both to encrypt and to decrypt the information transmitted by either the user or the server. In security and performance analysis, we have shown that our protocol is more efficient and secure than others since our protocol only uses hash operation and XOR operation. Furthermore, our protocol can also provide user anonymity to guarantee the identity of users, which is transmitted in the insecure public network.

Acknowledgements This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 101-2221-E-030-018 and NSC 101-2221-E-165-002. We also thank Morton W. Belcher, III, M.S.L.S., for his opinions with regard to this research project.

References

1. Abdalla, M., Pointcheval, D.: Interactive Diffie-Hellman Assumptions with Applications to Password-Based Authentication. Lecture Notes in Computer Science, vol. 3570, pp. 341–356 (2005)
2. Bellovin, S.M., Merritt, M.: Encrypted key exchange: password-based protocols secure against dictionary attacks. In: Proceedings of IEEE Computer Society Symposium on Security and Privacy, pp. 72–84 (1992)
3. Bergamo, P., D'Arco, P., De Santis, A., Kocarev, L.: Security of public-key cryptosystems based on Chebyshev polynomials. IEEE Trans. Circuits Syst. I **52**(7), 1382–1393 (2005)
4. Chang, T.Y., Hwang, M.S., Yang, W.P.: A communication-efficient three-party password authenticated key exchange protocol. Inf. Sci. **181**, 217–226 (2011)
5. Chang, T.Y., Yang, W.P., Hwang, M.S.: Simple authenticated key agreement and protected password change protocol. Comput. Math. Appl. **49**, 703–714 (2005)
6. Deng, M., Ma, J., Le, F.: Universally composable three party password-based key exchange protocol. China Commun. **6**(3), 150–154 (2009)
7. Han, S., Chang, E.: Chaotic map based key agreement with/out clock synchronization. Chaos Solitons Fractals **39**(3), 1283–1289 (2009)
8. Hassan, M.I., Abdullah, A.: A new grid resource discovery framework. Int. Arab J. Inf. Technol. **8**(1), 99–107 (2011)
9. He, D., Chen, Y., Chen, J.: Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. Nonlinear Dyn. **69**(3), 1149–1157 (2012)
10. Huang, H.F.: A simple three-party password-based key exchange protocol. Int. J. Commun. Syst. **22**(7), 857–862 (2009)
11. Lee, C.C., Chang, R.X., Ko, H.J.: Improving two novel three-party encrypted key exchange protocols with perfect forward secrecy. Int. J. Found. Comput. Sci. **21**(6), 979–991 (2010)
12. Lee, C.C., Chang, Y.F.: On security of a practical three-party key exchange protocol with round efficiency. Inf. Technol. Control **37**(4), 333–335 (2008)
13. Lee, C.C., Chen, S.D., Chen, C.L.: A computation-efficient three-party encrypted key exchange protocol. Appl. Math. Inf. Sci. **6**(3), 573–579 (2012)
14. Lee, C.C., Chen, C.L., Wu, C.Y., Huang, S.Y.: An extended chaotic maps-based key agreement protocol with user anonymity. Nonlinear Dyn. **69**(1–2), 79–87 (2012)
15. Lee, T.F., Hwang, T., Lin, C.L.: Enhanced three-party encrypted key exchange without server public keys. Comput. Secur. **23**(7), 571–577 (2004)
16. Lee, S.W., Kim, H.S., Yoo, K.Y.: Efficient verifier-based key agreement protocol for three parties without server's public key. Appl. Math. Comput. **167**(2), 996–1003 (2005)
17. Lin, C.L., Sun, H.M., Steiner, M., Hwang, T.: Three-party encrypted key exchange without server public keys. IEEE Commun. Lett. **5**(12), 497–499 (2001)
18. Lin, J.P., Fu, J.M.: Authenticated key agreement scheme with privacy-protection in the three-party setting. Int. J. Netw. Secur. **15**(3), 149–159 (2013)
19. Lo, J.W., Lee, J.Z., Hwang, M.S., Chu, Y.P.: An advanced password authenticated key exchange protocol for imbalanced wireless networks. J. Internet Technol. **11**(7), 997–1004 (2010)
20. Lo, J.W., Lin, S.C., Hwang, M.S.: A parallel password-authenticated key exchange protocol for wireless environments. Inf. Technol. Control **39**(2), 146–151 (2010)
21. Lou, D.C., Huang, H.F.: Efficient three-party password-based key exchange scheme. Int. J. Commun. Syst. **24**(4), 504–512 (2011)
22. Lu, R., Cao, Z.: Simple three-party key exchange protocol. Comput. Secur. **26**(1), 94–97 (2007)
23. Mason, J.C., Handscomb, D.C.: Chebyshev Polynomials. Chapman & Hall/CRC Press, London (2003)
24. Pathak, H.K., Sanghi, M.: Simple three party key exchange protocol via twin Diffie-Hellman problem. Int. J. Netw. Secur. **15**(4), 201–209 (2013)

25. Sheu, L.J.: A speech encryption using fractional chaotic systems. Nonlinear Dyn. **65**(1–2), 103–108 (2011)
26. Tsai, C.S., Lee, C.C., Hwang, M.S.: Password authentication schemes: current status and key issues. Int. J. Netw. Secur. **3**(2), 101–115 (2006)
27. Wang, X., Wang, X., Zhao, J., Zhang, Z.: Chaotic encryption algorithm based on alternant of stream cipher and block cipher. Nonlinear Dyn. **63**(4), 587–597 (2011)
28. Wang, Y., Wong, K.W., Liao, X., Xiang, T.: A block cipher with dynamic s-boxes based on tent map. Commun. Nonlinear Sci. Numer. Simul. **14**(7), 3089–3099 (2009)
29. Wang, X.Y., Yang, L., Liu, R., Kadir, A.: A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn. **62**(3), 615–621 (2010)
30. Wu, S., Chen, K., Zhu, Y.: Enhancements of a Three-Party Password-Based Authenticated Key Exchange Protocol. Int. Arab J. Inf. Technol. **10**(3) (2013)
31. Xiao, D., Liao, X., Deng, S.: One-way Hash function construction based on the chaotic map with changeable-parameter. Chaos Solitons Fractals **24**(1), 65–71 (2005)
32. Xiao, D., Shih, F., Liao, X.: A chaos-based hash function with both modification detection and localization capabilities. Commun. Nonlinear Sci. Numer. Simul. **15**(9), 2254–2261 (2010)
33. Yong, Z., Jianfeng, M., Moon, S.: An improvement on a three-party password-based key exchange protocol using Weil pairing. Int. J. Netw. Secur. **11**(1), 17–22 (2010)
34. Yoon, E.J., Yoo, K.Y.: Cryptanalysis of a simple three-party password-based key exchange protocol. Int. J. Commun. Syst. **24**(4), 532–542 (2011)
35. Yoon, E.J., Yoo, K.Y.: Cryptanalysis of an efficient three-party password-based key exchange scheme. Proc. Eng. **29**, 3972–3979 (2012)
36. Yuan, W., Hu, L., Li, H., Chu, J.: Offline dictionary attack on a universally composable three-party password-based key exchange protocol. Proc. Eng. **15**, 1691–1694 (2011)
37. Zhang, L.: Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fractals **37**(3), 669–674 (2008)