Journal of Network Intelligence ©2016 ISSN 2414-8105 (Online)
Taiwan Ubiquitous Information Volume **1**, Number **2**, May **2016**

On the Security of a Chaotic Maps-based Three-party Authenticated Key Agreement Protocol

Chien-Ming Chen

School of Computer Science and Technology
Harbin Institute of Technology Shenzhen Graduate School
Shenzhen, 518055, China
chienming.taiwan@gmail.com

Linlin Xu

School of Computer Science and Technology
Harbin Institute of Technology Shenzhen Graduate School
Shenzhen, 518055, China
980742703@qq.com

Tsu-Yang Wu

School of Computer Science and Technology
Harbin Institute of Technology Shenzhen Graduate School
Shenzhen, 518055, China
wutsuyang@gmail.com

Ci-Rong Li

Faculty of Management
Fuqing Branch of Fujian Normal University
Fujian, 350300, China
cirongli@gmail.com

(Communicated by Tsu-Yang Wu)

Abstract. *Chaotic map has been receiving increasing attention in the cryptographic literature. There are various scholars working on a particular type of authenticated key exchange protocol using chaotic map in the recent years. Very recently, Li et al. proposed a new three-party-authenticated key agreement protocol based on chaotic maps without storing a password table in a server. Compared with previous works, their protocol can completely resistant to password guessing attacks because of using no passwords. In this paper, we demonstrate that this protocol is still vulnerable to a user impersonation attack.*

Keywords: Cryptanalysis , Three-party Authenticated key agreement, Smart card.

1. **Introduction.** Information transmitted in an open network is required to be encrypted for confidentiality; thus, an Authenticated Key Exchange (AKE) scheme is necessary. An AKE scheme helps two communication entities to authenticate each other and establish a common session key. This session key is utilized for encrypting and decrypting their following communication. AKE schemes have been studied over the past few decades. So far, a huge number of AKE schemes have been proposed for many environments and applications [1, 2, 3, 4, 5].

Originally, an AKE scheme was designed for two-party situation. In most existing two-party authenticated key exchange (2AKE) schemes, two entities need to pre-share a common secret, e.g., a password. More specifically, each entity needs to remember different secrets for different entities who communication with. It means that 2AKE is not suitable for large-scale environments because of storage overhead. For this reason, AKE in a three-party (3AKE) setting is described. In a 3AKE scheme, a trusted server is involved. Any two entities establish a common session key with a trusted server's help. Compared with 2AKE, 3AKE is more practical in large-scale environments since each entity only requires to pre-share a secret with a trusted server.

The exiting AKE schemes are normally developed based on different cryptographic operations, such as modular exponentiation operations [6], bilinear pairing [7, 8, 9], etc. Recently, a chaotic system has received increasing attention, especially in designing cryptosystems [10, 11, 12]. Chaos is the well-defined universal, random-like and robust phenomenon in nonlinear system. With the property of better performance, chebyshev chaotic maps have been utilized in designing AKE schemes. So far, various chaotic maps-based AKE schemes have been proposed.

In 2012, Lai et al. [13] proposed a password-based 3AKE scheme using an enhanced Chebeshev chaotic map. This scheme uses a smart card to store sensitive information. However, Zhao et al. [14] demonstrated that this scheme is vulnerable to an off-line password guessing attack and a privileged insider attack. Zhao et al. then proposed an improved scheme which also uses a smart card. In 2013, Lee et al. [15] and Xie et al. [16] proposed their chaos-based 3AKE protocol without using smart cards respectively. Later, Farash et al. [17] proposed another chaos-based 3AKE scheme without using smart cards. Compared with Lee et al. [15] and Xie et al.'s schemes [16], Farash et al.'s scheme uses neither server's public key nor symmetric cryptosystems. Farash et al. [17] also provide a formal proof to demonstrate the security of this scheme. Hu et al. [18] further showed that Lee et al.'s scheme [15] is vulnerable to a man-in-the-middle attack and a user anonymity attack. In 2015, Lee et al. [19] demonstrated that Xie et al.'s scheme [16] also suffers from an on-line password guessing attack. They also describes a new chaotic-maps 3AKE scheme. Besides, Li et al. [20] proposed another chaotic maps-based 3AKE protocol. In these two schemes [19, 20], a server does not need to store a password table.

After reviewing the above schemes, we found that Li et al.'s protocol [20] has a security flaw. In their design, each user does not need to remember a password since using a low-entropy password easily suffers form password guessing attacks. Instead, each user is required to securely store a hashed value. It is obviously that remembering a hashed value is a difficult task for human beings. For this reason, users may store their hashed values in a smart card issued by a trusted server. However, smart cards could be stolen by a malicious attackers. Although the smart card may come with a tamper-resistant property, sensitive information stored in a smart card can be still extracted by some side channel attacks [21, 22]. In this paper, we will demonstrate that Li et al.'s protocol [20] is vulnerable to a user impersonation attack under the above assumptions.

2. **Review of Li et al.'s protocol.** In this section, we briefly review Li et al.'s protocol. The detailed steps can refer to [20].

In a registration phase, every client participant requires to register himself to a trusted server S. Assume a participant U_i desires to register himself to S, U_i selects his identity ID_i and submits ID_i to S. S then computes $h(ID_i||x)$ and submits it to U_i through a secure channel. U_i stores $h(ID_i||x)$ as a secret. Note that x is a master secret key of S and $h()$ denotes a secure one-way hash function.

Assume there are two client participants U_A and U_B desire to establish a session through S, they perform the authentication and key agreement phase described as follows.

Step 1. U_A generates a nonce a and computes (1)(2)(3).

$$K_A = T_a(X) \tag{1}$$
$$H_A = h(ID_A||ID_B||K_A) \tag{2}$$
$$C_1 = E_{h(ID_A||x)}(ID_A||ID_B||K_A||H_A) \tag{3}$$

Note that X means a public seed of Chebyshev chaotic maps generated from x and $E_{key}()$ denotes a symmetric encryption algorithm with key key. Then, U_A transmits (ID_A,C_1) to U_B.

Step 2. While receiving (ID_A,C_1) from U_A, U_B generates a nonce b and calculates (4)(5)(6).

$$K_B = T_b(X) \tag{4}$$
$$H_B = h(ID_B||ID_A||K_B) \tag{5}$$
$$C_2 = E_{h(ID_B||x)}(ID_B||ID_A||K_B||H_B) \tag{6}$$

B then transmits (ID_A,C_1,ID_B,C_2) to S.

Step 3. S first verifies if ID_A and ID_B are valid, then S decrypts C_1 with $h(ID_A||x)$ and C_2 with $h(ID_B||x)$ respectively. S now verifies the validity of ID_A and ID_B again. S also checks the integrity of H_A and H_B. If both hold, S computes (7)(8)(9).

$$H_{SAB} = h(ID_A||ID_B||K_A||K_B) \tag{7}$$
$$C_3 = E_{h(ID_B||x)}(ID_B||ID_A||K_B||K_A||H_{SAB}) \tag{8}$$
$$C_4 = E_{h(ID_A||x)}(ID_A||ID_B||K_A||K_B||H_{SAB}) \tag{9}$$

S then transmits (C_3,C_4) to U_B.

Step 4. U_B first decrypts C_3 received from S with $h(ID_B||x)$ and then verifies the integrity of H_{SAB}. If it holds, B computes (10)(11).

$$SK = T_b(K_A) = T_{ab}(X) \tag{10}$$
$$H_{BA} = h(ID_B||ID_A||SK||K_A) \tag{11}$$

U_B then transmits (C_4,H_{BA}) to U_A.

Step 5. While receiving the messages from U_B, U_A first decrypts C_4 with $h(ID_A||x)$ and then verifies the integrity of H_{SAB}. If it holds, U_A calculates $SK = T_a(K_B) = T_{ab}(X)$ and utilizes SK to verify the integrity of H_{BA}. After that, U_A computes H_{AB}=$h(ID_A||ID_B|| SK||K_B)$ and transmits H_{AB} to U_B.

Step 6. U_B first checks the integrity of H_{AB} received from U_A. Finally, U_A and U_B has established a common session key SK.

3. **Cryptanalysis on Li et al.'s protocol.**

In this section, we demonstrate that Li et al.'s protocol [20] is vulnerable to the user impersonate attack.

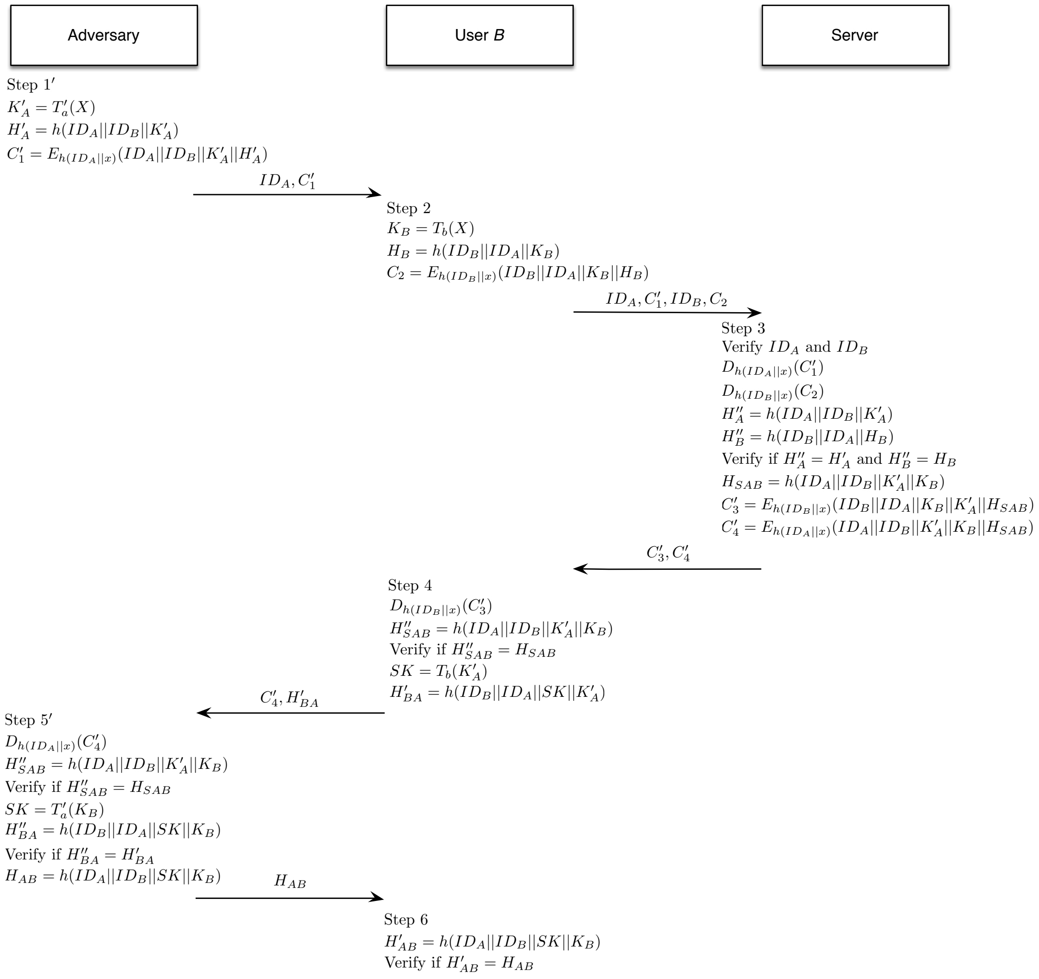
Adversary
User B
Server
Step 1′
$K'_A = T'_a(X)$
$H'_A = h(ID_A||ID_B||K'_A)$
$C'_1 = E_{h(ID_A||x)}(ID_A||ID_B||K'_A||H'_A)$
ID_A, C'_1
Step 2
$K_B = T_b(X)$
$H_B = h(ID_B||ID_A||K_B)$
$C_2 = E_{h(ID_B||x)}(ID_B||ID_A||K_B||H_B)$
ID_A, C'_1, ID_B, C_2
Step 3
Verify ID_A and ID_B
$D_{h(ID_A||x)}(C'_1)$
$D_{h(ID_B||x)}(C_2)$
$H''_A = h(ID_A||ID_B||K'_A)$
$H''_B = h(ID_B||ID_A||H_B)$
Verify if $H''_A = H'_A$ and $H''_B = H_B$
$H_{SAB} = h(ID_A||ID_B||K'_A||K_B)$
$C'_3 = E_{h(ID_B||x)}(ID_B||ID_A||K_B||K'_A||H_{SAB})$
$C'_4 = E_{h(ID_A||x)}(ID_A||ID_B||K'_A||K_B||H_{SAB})$
C'_3, C'_4
Step 4
$D_{h(ID_B||x)}(C'_3)$
$H''_{SAB} = h(ID_A||ID_B||K'_A||K_B)$
Verify if $H''_{SAB} = H_{SAB}$
$SK = T_b(K'_A)$
$H'_{BA} = h(ID_B||ID_A||SK||K'_A)$
C'_4, H'_{BA}
Step 5′
$D_{h(ID_A||x)}(C'_4)$
$H''_{SAB} = h(ID_A||ID_B||K'_A||K_B)$
Verify if $H''_{SAB} = H_{SAB}$
$SK = T'_a(K_B)$
$H''_{BA} = h(ID_B||ID_A||SK||K_B)$
Verify if $H''_{BA} = H'_{BA}$
$H_{AB} = h(ID_A||ID_B||SK||K_B)$
H_{AB}
Step 6
$H'_{AB} = h(ID_A||ID_B||SK||K_B)$
Verify if $H'_{AB} = H_{AB}$

FIGURE 1. The Detailed Steps of Our Attack

3.1. **The secrecy of $h(ID_i||x)$.** In Li et al.'s protocol [20], the authors assume that any client participate U_i must stores $h(ID_i||x)$ as a secret. Certainly, keeping this hashed value in mind may be the securest may, but remembering it is indeed a infeasible task for human beings. Consequently, storing this hashed value in a smart card seems a reasonable and acceptable choice. Unfortunately, smart cards could be stolen by a malicious attackers. Although the smart card may come with a tamper-resistant property, sensitive information stored in a smart card can be still extracted by some side channel attacks [21, 22].

3.2. **Our Attack.** Assume a malicious adversary U_E steals U_A's smart card and extracts $h(ID_A||x)$ stored in this smart card. Figure 1 illustrates the detailed procedures of our attack. The steps of the proposed attack are listed as follows.

Step 1′. U_E generates a nonce a' and computes K'_A=$T'_a(X)$, $H'_A = h(ID_A||ID_B||K'_A)$ and C'_1=$E_{h(ID_A||x)}(ID_A||ID_B||K'_A||H'_A)$. Then, U_E submits (ID_A,C'_1) to U_B.

Step 2. After receiving (ID_A,C'_1), U_B believes that U_A desires to establish a session key with him. Then, U_B generates a nonce b and computes K_B=$T_b(X)$, $H_B = h(ID_B||ID_A||K_B)$ and C_2=$E_{h(ID_B||x)}(ID_B||ID_A||K_B||H_B)$. After that, U_B submits (ID_A,C'_1,ID_B,C_2) to S.

Step 3. According to the received messages, S believes that U_A and U_B attempt to authenticate to each other and further establish a session key. S first assures that U_A and U_B are both legitimate user, S then decrypts C_1' with $h(ID_A||x)$ and C_2 with $h(ID_B||x)$ respectively. S further verifies the validity of ID_A and ID_B again and checks the integrity of H_A' and H_B. At last, S calculates $H_{SAB}{=}h(ID_A||ID_B||K_A'||K_B)$, $C_3'{=}E_{h(ID_B||x)}(ID_B||ID_A||K_B||K_A'||H_{SAB})$ and $C_4'{=}E_{h(ID_A||x)}(ID_A||ID_B||K_A'||K_B||H_{SAB})$. Now S transmits (C_3', C_4') to U_B.

Step 4. Upon obtaining (C_3', C_4'), U_B decrypts C_3' with $h(ID_B||x)$ and then verifies the integrity of H_{SAB}. If it holds, B calculates $SK{=}T_b(K_A')$ and $H_{BA}'{=}h(ID_B||ID_A||SK||K_A')$. U_B then submits (C_4', H_{BA}') to U_A. U_B believes (C_4', H_{BA}') are sent to U_A; however, these messages are sent to U_E.

Step $5'$. U_E decrypts C_4' with $h(ID_A||x)$ and verifies the integrity of H_{SAB}. Then, U_E computes $SK = T_a'(K_B)$ and utilizes SK to verify the integrity of H_{BA}. Now U_E computes $H_{AB}{=}h(ID_A||ID_B||SK||K_B)$ and transmits H_{AB} to U_B.

Step 6. U_B first checks the integrity of H_{AB}. At this time, U_E and U_B has established a common session key SK.

4. **Conclusion.**

There are many three-party-authenticated key agreement schemes in the literature which apparently seem to work but they have been shown to be insecure. However, the very recent Li et al.'s protocol is shown to suffer from a user impersonation attack in this paper.

Acknowledgement. The work of C.-M. Chen was supported in part by the Project NSFC (National Natural Science Foundation of China) under Grant number 61402135. The work of T.-Y. Wu was supported in part by the Natural Scientific Research Innovation Foundation in Harbin Institute of Technology under Grant number HIT.NSRIF.2015089. The work of C.-R. Li was supported in part by the Natural Science Foundation of Fujian Province, China, under Grant number 2015R0031 and in part by the Humanity and Social Science on Youth Fund of the Ministry of Education under Grant number 15YJCZH084. The corresponding author is Prof. Tsu-Yang Wu.

REFERENCES

[1] H.-M. Sun, B.-Z. He, C.-M. Chen, T.-Y. Wu, C.-H. Lin, and H. Wang, "A provable authenticated group key agreement protocol for mobile environment," *Information Sciences*, vol. 321, pp. 224–237, 2015.

[2] B.-Z. He, C.-M. Chen, T.-Y. Wu, and H.-M. Sun, "An efficient solution for hierarchical access control problem in cloud environment," *Mathematical Problems in Engineering*, vol. 2014, 2014.

[3] C.-M. Chen, S.-M. Chen, X. Zheng, L. Yan, H. Wang, and H.-M. Sun, "Pitfalls in an ecc-based lightweight authentication protocol for low-cost rfid," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 4, pp. 642–648, 2014.

[4] C.-M. Chen, K.-H. Wang, T.-Y. Wu, J.-S. Pan, and H.-M. Sun, "A scalable transitive human-verifiable authentication protocol for mobile devices," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 8, pp. 1318–1330, 2013.

[5] K. Wei-Chi, C. Chien-Ming, and L. Hui-Lung, "Cryptanalysis of a variant of peyravian-zunic's password authentication scheme," *IEICE Transactions on Communications*, vol. 86, no. 5, pp. 1682–1684, 2003.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[7] Y. J. Choie, E. Jeong, and E. Lee, "Efficient identity-based authenticated key agreement protocol from pairings," *Applied Mathematics and Computation*, vol. 162, no. 1, pp. 179–188, 2005.

[8] X. Cao, W. Kou, and X. Du, "A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges," *Information Sciences*, vol. 180, no. 15, pp. 2895–2903, 2010.

[9] T.-Y. Wu and Y.-M. Tseng, "An efficient user authentication and key exchange protocol for mobile client–server environment," *Computer Networks*, vol. 54, no. 9, pp. 1520–1530, 2010.

[10] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[11] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, 2010.

[12] L. J. Sheu, "A speech encryption using fractional chaotic systems," *Nonlinear Dynamics*, vol. 65, no. 1-2, pp. 103–108, 2011.

[13] H. Lai, J. Xiao, L. Li, and Y. Yang, "Applying semigroup property of enhanced chebyshev polynomials to anonymous authentication protocol," *Mathematical Problems in Engineering*, vol. 2012, 2012.

[14] F. Zhao, P. Gong, S. Li, M. Li, and P. Li, "Cryptanalysis and improvement of a three-party key agreement protocol using enhanced chebyshev polynomials," *Nonlinear Dynamics*, vol. 74, no. 1-2, pp. 419–427, 2013.

[15] C.-C. Lee, C.-T. Li, and C.-W. Hsu, "A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps," *Nonlinear Dynamics*, vol. 73, no. 1-2, pp. 125–132, 2013.

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

[17] M. S. Farash and M. A. Attari, "An efficient and provably secure three-party password-based authenticated key exchange protocol based on chebyshev chaotic maps," *Nonlinear Dynamics*, vol. 77, no. 1-2, pp. 399–411, 2014.

[18] X. Hu and Z. Zhang, "Cryptanalysis and enhancement of a chaotic maps-based three-party password authenticated key exchange protocol," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 1293–1300, 2014.

[19] C.-C. Lee, C.-T. Li, S.-T. Chiu, and Y.-M. Lai, "A new three-party-authenticated key agreement scheme based on chaotic maps without password table," *Nonlinear Dynamics*, vol. 79, no. 4, pp. 2485–2495, 2015.

[20] X. Li, J. Niu, S. Kumari, M. K. Khan, J. Liao, and W. Liang, "Design and analysis of a chaotic maps-based three-party authenticated key agreement protocol," *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1209–1220, 2015.

[21] Q. Xie, "A new authenticated key agreement for session initiation protocol," *International Journal of Communication Systems*, vol. 25, no. 1, pp. 47–54, 2012.

[22] M. S. Farash, S. Kumari, and M. Bakhtiari, "Cryptanalysis and improvement of a robust smart card secured authentication scheme on sip using elliptic curve cryptography," *Multimedia Tools and Applications*, pp. 1–20, 2015.