Cryptanalysis and Improvements on Three-party-authenticated Key Agreement Protocols Based on Chaotic Maps

Chien-Ming Chen[1], Linlin Xu[1], King-Hang Wang[2], Shuai Liu[1], Tsu-Yang Wu[3,4,5]

[1] Harbin Institute of Technology Shenzhen Graduate School, China
[2] Hong Kong University of Science and Technology, Hong Kong
[3] College of Computer Science and Engineering, Shandong University of Science and Technology, China
[4] Fujian Provincial Key Laboratory of Big Data Mining and Applications, Fujian University of Technology, China
[5] National Demonstration Center for Experimental Electronic Information and Electrical Technology Education, Fujian University of Technology, China
chienming @hit.edu.cn, 980742703@qq.com, kevinw@cse.ust.hk, 362575680@qq.com, wutsuyang@gmail.com

Abstract

Chaotic map has been receiving more and more attention in the cryptographic literature. In recent years, there are some scholars working on a particular type of authenticated key exchange protocol using chaotic map. Some of them identified a vulnerability of their precedences and presented their patching protocols. In this paper, we also identify a vulnerability in some of these authenticated key exchange protocols. We first redesign a protocol and optimize it in computation efficiency. Then we present the security analysis by a logic proof based on BAN logic.

Keywords: Chaotic map, Cryptography, Authentication key exchange protocol

1 Introduction

Authenticated Key Exchange (AKE) [1-6] is an important cryptographic tool to establish a confidential channel between two or more entities over a public network. Usually the entities share a common secret like a password or a secret key. During an AKE protocol, each participating entity would be required to response to a cryptographic challenge with his knowledge on the common secret in order to prove his identity. Meanwhile, as the protocol is executed over a public network, it is assumed there are adversaries could eavesdrop and inject messages in the channel in order to either impersonate one of the participating entities or to learn the session key established for the confidential channel.

A particular type of AKE is called three-party AKE (or 3AKE) [7-9]. In 3AKE, there are normally one server participant shares secrets with each of two client participants. The protocol again assumes the existence of adversaries to establish a confidential channel for the two clients to communicate. Despite the long history 3AKE in the literature, to our best knowledge, 3AKE on chaos can only be traced to the year 2012. Lai et al. [10] proposed a password-based 3AKE protocol using an enhanced Chebeshev chaotic map [11] in 2012. However, Zhao et al. [12] found that this protocol is vulnerable to a privileged insider attack and an off-line password guessing attack, and they proposed their improved protocol. In 2013, Lee et al. [13] and Xie et al. [14] proposed their chaos-based 3AKE protocols. Hu et al. [15] further showed that Lee et al.'s [13] protocol is vulnerable to a man-in-the-middle attack and a user anonymity attack. In 2015, Lee et al. [16] showed that Xie et al.'s protocol [14] also suffers from an on-line password guessing attack. They also described a new chaotic based 3AKE protocol. Besides, Li et al. [17] proposed another chaotic based 3AKE protocol to improve the existing protocols. Very recently, Chen et al. [18] showed that Li et al.'s protocol [13] is vulnerable to a user impersonation attack.

Unfortunately, in this paper we find that Lee et al.'s protocol [16], Li et al.'s protocol [17] and Xie et al.'s protocol [14] are insecure against a message replay attack. Under this attack, a malicious attacker can impersonate two honest client entities to establish a confidential session with the server without holding the clients' secrets. We then propose a new 3AKE protocols based on chaotic maps. According the performance analysis, our protocol has better efficiency compared with previous protocols. We also present the security analysis by a logic proof based on BAN logic.

2 Chebyshev Chaotic Maps

Owing to its randomness feature, the family of

*Corresponding Author: Tsu-Yang Wu; E-mail: wutsuyang@gmail.com
DOI: 10.3966/160792642018051903006

chaotic maps receives more and more attention in the information security literatures [19-24] in the recent years. These high quality works demonstrate how to create secure cryptographic tools with using chaos as a primitive.

In this section, we introduce some basic concepts and preliminaries of the chaotic maps. We select the extended Chebyshev's polynomial [11]

$$T_n(x) = \begin{cases} 1, & if\ n = 0 \\ x, & if\ n = 1 \\ 2xT_{n-1}(x) - T_{n-2}(x), & if\ n \geq 2 \end{cases}$$

which developed from Chebyshev's polynomial [25] as an instantiation of the chaotic map.

By the above recursive approach, we can obtain some examples of the Chebyshev's polynomial:

$T_2(x) = 2xT_1(x) - T_0(x) = 2x^2 - 1$.
$T_3(x) = 2xT_2(x) - T_1(x) = 4x^3 - 3x$.
$T_4(x) = 2xT_3(x) - T_2(x) = 8x^4 - 8x^2 + 1$.

It is easy to see that $T_n(x)$ is a polynomial of degree n. If the variable $x \in [-1,1]$, then we have $T_n(x) \in [-1,1]$. Hence, we can define a special case of Chebyshev polynomial $T_n(x)$: $[-1,1] \rightarrow [-1,1]$ by $T_n(x) = \cos(n \cdot \arccos(x))$.

For $n \geq 2$, the Chebyshev's polynomial $T_n(x)$ satisfies the following two properties:

(1) The semi group property.

$$\begin{aligned} T_a(T_b(x)) &= \cos(a \arccos(\cos(b\, ar\cos s(x)))) \\ &= \cos(ab \arccos(x)) \\ &= T_{ab}(x) \\ &= T_{ab}(T_a(x)) \end{aligned}$$

for any positive integers a, b and $x \in [-1, 1]$.

(2) The chaotic property. $T_n(x)$ is a prototype of a chaotic map. It has a unique absolutely continuous invariant measure $\mu(x) = \frac{1}{\pi\sqrt{1-x^2}}$ with positive Lyapunov exponent $\lambda = \ln n$.

An enhanced Chebeshev's polynomial is defined on $(-\infty, \infty)$, $T_n(x) \equiv 2xT_{n-1}(x) - T_{n-2}(x) \bmod p$ for $n \geq 2$ and p is a large prime while the semi group property, $T_a(T_b(x)) = T_{ab}(x) = T_b(T_a(x)) \bmod p$ for any a, $b \geq 2$ still holds.

3 Cryptanalysis of Previous Protocol

In this section we would like to identify a vulnerability that appears in some of these protocols. The Lee et al.'s protocol [16] is selected for the purpose of illustration while similar vulnerability appears in other protocols as well [14, 17].

3.1 Review Lee et al.'s Protocol

Here we briefly review Lee et al.'s protocol [16]. The steps of it are illustrated in Figure 1. The setting of the protocol assumes there is a single honest server S and a set of clients $\{U_1, U_2, \ldots\}$. Each client may desire to establish a confidential channel with another client through the server over a public network. The client will initiate the protocol while all messages sent in the protocol can be eavesdropped and changed by a network attacker. The goal of the attacker is to either convince a client or a server to authenticate a wrong client (impersonation) or to learn the session key of the confidential channel. We assume the attacker may exploit a small set of clients' secrets or passwords.

Here we describe the protocol. Assume there are two client participants U_A and U_B desire to establish a session through a trusted server S. Each client has a certificate issued by S prior to the protocol. $T_k(ID_A)$ and $T_k(ID_B)$ are the certificate of U_A and U_B respectively.

Step 1. U_A selects a random number $a \in [1, p-1]$ and computes $K_{AS} = T_aT_k(ID_A)$, $H_A = h(T_a(ID_A)||ID_A||ID_B)$ and $C_A = E_{K_{AS}}(ID_A \,||\, ID_B \,||\, H_A \,||\, T_a(ID_B))$. Note that $h()$ denotes a one-way hash function based on chaotic maps, $E_K()$ means symmetric encryption function with key K, and ID_A, ID_B means U_A's and U_B's identity respectively. Then, U_A sends $m_1 = \{T_a(ID_A), C_A\}$ to U_B.

Step 2. While receiving $\{m_1\}$, U_B selects a random number $b \in [1, p-1]$ and calculates $K_{BS} = T_bT_k(ID_B)$, $H_B = h(T_b(ID_B)||ID_B)$ and $C_B = E_{K_{BS}}(ID_B \,||\, H_B \,||\, T_b(ID_B))$. Then, U_B sends $\{m_1, m_2\}$ to S where $m_2 = \{T_b(ID_B), C_B\}$.

Step 3. Upon receiving $\{m_1, m_2\}$, S first calculates $K_{SA} = T_kT_a(ID_A)$, $K_{SB} = T_kT_b(ID_B)$, $D_A = D_{K_{SA}}(C_A)$, and $D_B = D_{K_{SB}}(C_B)$. Note that $D_{key}()$ means a symmetric decryption function with key key and k means S's secret key respectively. Then, S first checks ID_A and ID_B. S also checks if H_A is equal to $h(T_a(ID_A)||ID_A||ID_B)$ and H_B is equal to $h(T_b(ID_B)||ID_B)$ respectively. If both hold, S computes $H_{SA} = h(T_k(ID_A)||T_a(ID_A))$, $H_{SB} = h(T_k(ID_B) \,||T_b(ID_B))$, $C'_A = E_{K_{SA}}(ID_A \,||\, ID_B \,||\, T_b(ID_B) \,||\, H_{SA})$, and $C'_A = E_{K_{SB}}(ID_A \,||\, ID_B \,||\, T_a(ID_B) \,||\, H_{SB})$ and sends C'_A and C'_B to U_B.

Step 4. U_B obtains and checks ID_A and H_{SB} by decrypting C'_B. After that, U_B computes $K = T_bT_a(ID_B)$ and $H_{BA} = h(K||C'_A)$. U_B then sends C'_A and H_{BA} to U_A.

Step 5. U_A first checks H_{SA} by decrypting C'_A and then computes $K = T_aT_b(ID_B)$. After that, U_A checks if H_{BA} is equal to $h(K||C'_A)$. If it holds, U_A computes $H_{AB} = h(K||ID_A||T_a(ID_B))$ and sends H_{AB} to U_B.

Now, U_A, U_B and S can authenticate each other and establish the confidential channel using the session key SK.

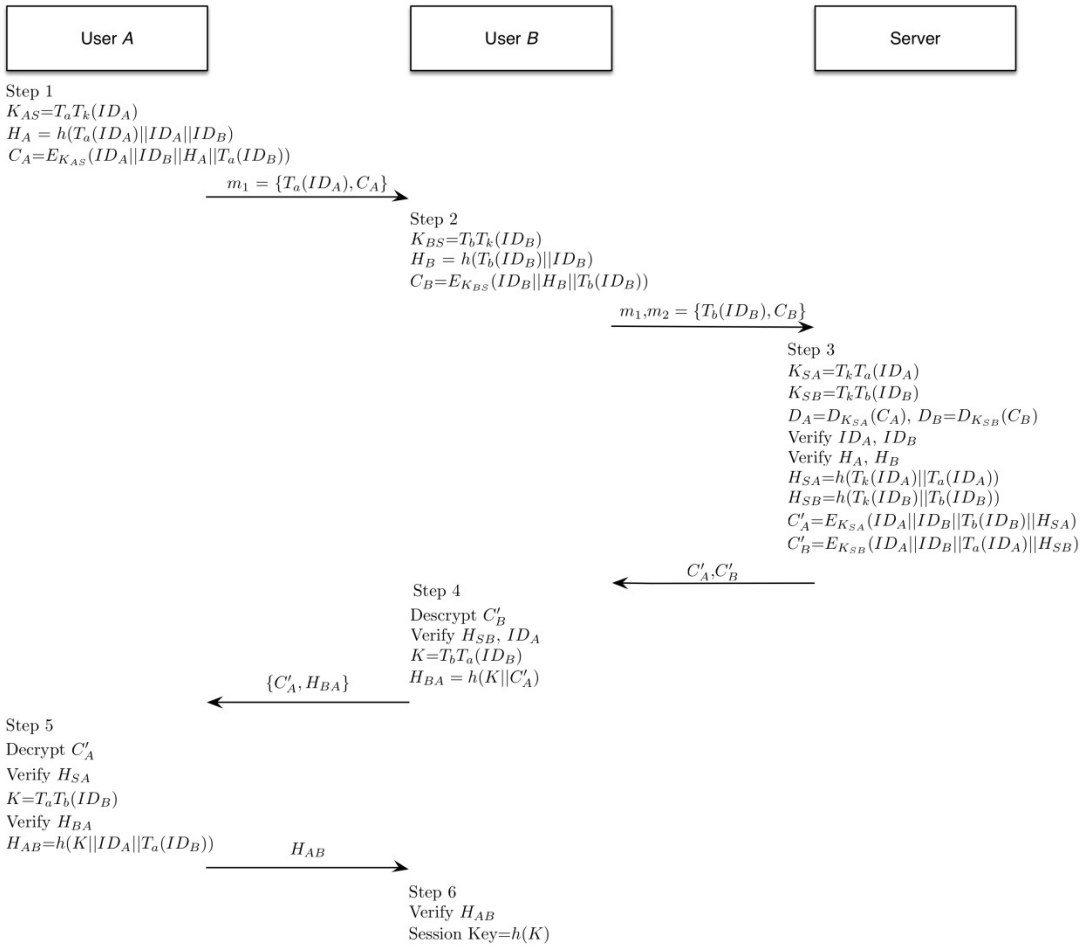

Figure 1. Lee et al.'s protocol

3.2 Cryptanalysis of Lee et al.'s Protocol

After the protocol, U_A and U_B shall be authenticated by the server S as they have demonstrated the knowledge of the certificates. However, we argue that is not true. In fact, under a replay attack described below, S still cannot confirm whether U_A and U_B are really initiating a 3AKE protocol or not. Sequently, the impact of this vulnerability will lead to an incorrect login status to the server and releasing unauthorized access of content, for example.

The replay attack is described as follows. Assume that there is a passive adversary E eavesdrops $m_1 = \{T_a(ID_A), C_A\}$ from U_A and $m_2 = \{T_b(ID_B), C_B\}$ from U_B. Later E sends m_1 and m_2 to S. Since these two messages m_1 and m_2 are generated by honest clients, the identities of U_A and U_B are authenticated by S although U_A and U_B are not intended to initiate a protocol. It shows that E can successfully convince S to authenticate two phantom clients in initiating the protocol. Consequently this will lead to an incorrect login record at the server and may release unauthorized access of content. Similar attack also applies to other protocols [14, 17].

4 The Proposed Protocol

Here we propose an efficient chaos-based 3AKE protocol. The notations used in the section are listed in Table 1. The proposed protocol has three phases, the initialization phase, the registration phase, and the authentication and key exchange phase.

Table 1. Notations used in this section

Notations	Descriptions
U_i	a legitimate user i
S	server
ID_i	user i's identity
PW_i	user i's password
$h_1(\cdot)$, $h_2(\cdot)$, $h_3(\cdot)$	three secure one-way hash functions
SK	session key

4.1 The Initialization Phase

In this phase, the server S initializes and selects the following system parameters.

- A large prime number p
- $\alpha \in Z_p$, such that the minimal period of Chebyshev polynomial sequence $(T_n(\alpha) \bmod p)_{n>0}$ is $p+1$
- Three hash functions $h_1(\cdot)$, $h_2(\cdot)$ and $h_3(\cdot)$

Finally, S publishes the above parameters $\{p, \alpha, h_1(\cdot), h_2(\cdot), h_3(\cdot), ID_S\}$.

4.2 The Registration Phase

This phase is invoked if a user U_i desires to register himself to a server S. The detailed steps are described as follows.

Step 1: U_i selects his ID_i and password PW_i and then sends ID_i and PW_i to S through a secure channel.

Step 2: S randomly selects a number $r_{s_i} \in_R [1, p+1]$ and computes $R_{s_i} = (r_{s_i}(\alpha) + PW_i) \bmod p$. Then S stores $\{ID_i, r_{s_i}\}$ in its database and sends ID_i and R_{s_i} to U_i through a secure channel.

Step 3: U_i keeps R_{s_i} as a secret and does not reveal it to any other users.

4.3 The Authentication and Key Exchange Phase

Figure 2 illustrates the authentication and key exchange phase. Assume two users U_A and U_B attempt to authenticate each other and establish a common session key, they perform the following steps.

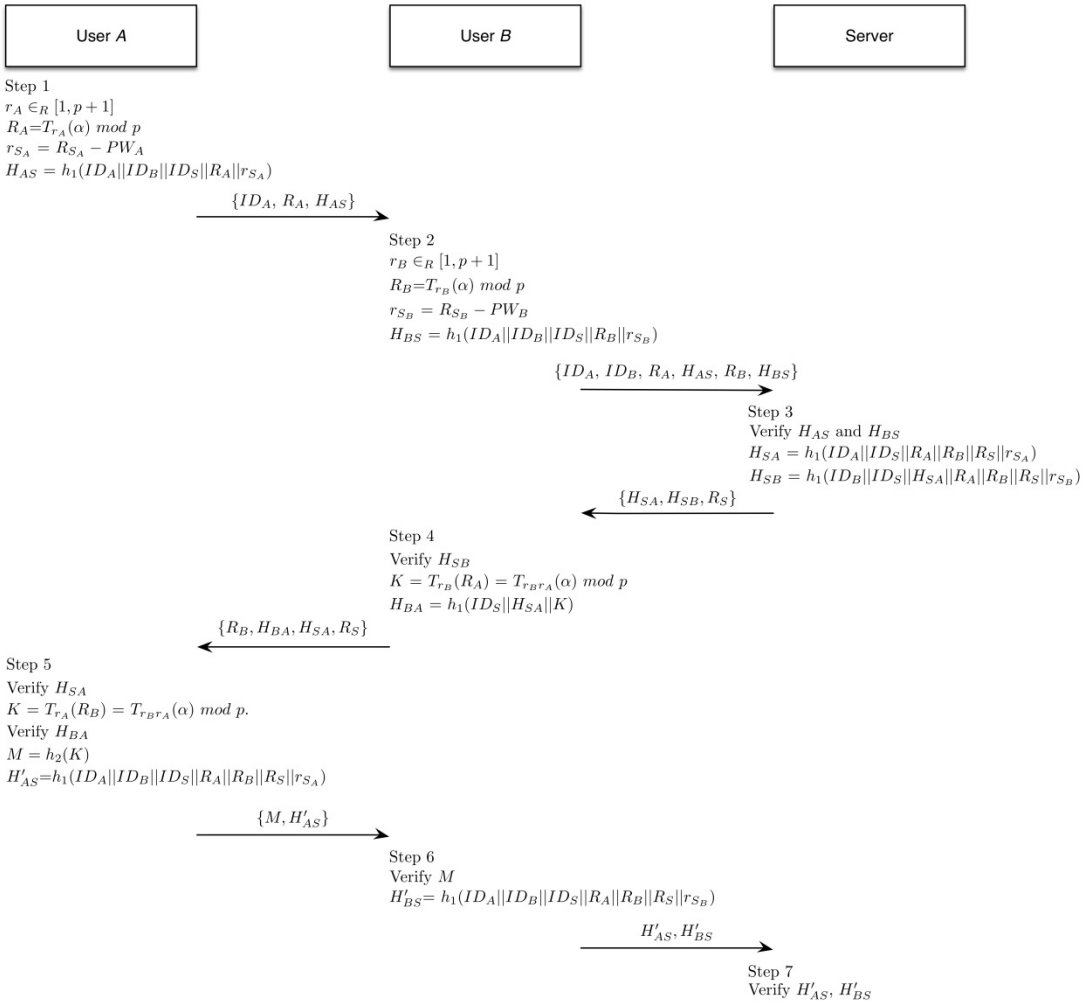

Figure 2. The authentication and key exchange phase

Step 1: U_A randomly chooses $r_A \in_R [1, p+1]$ and computes $R_A = T_{r_A}(\alpha) \bmod p$ and $r_{S_A} = R_{S_A} - PW_A$. U_A also computes $H_{AS} = h_1(ID_A \| ID_B \| ID_S \| R_A \| r_{S_A})$. Then U_A sends $\{ID_A, R_A, H_{AS}\}$ to U_B.

Step 2: U_B chooses a random number $r_B \in_R [1, p+1]$ and then computes $R_B = T_{r_B}(\alpha) \bmod p$ and $r_{S_B} = R_{S_B} - PW_B$. U_B also computes $H_{BS} = h_1(ID_A \| ID_B \| ID_S \| R_B \| r_{S_B})$. Then U_B sends $\{ID_A, ID_B, R_A, H_{AS}, R_B, H_{BS}\}$ to S.

Step 3: Upon receiving the messages sent from U_B, S first verifies H_{AS} and H_{BS}. If both hold, S chooses a random number R_S and computes $H_{SA} = h_1(ID_A \| ID_S \| R_A \| R_B \| R_S \| r_{S_A})$ and $H_{SB} = h_1(ID_B \| ID_S \| H_{SA} \| R_A \| R_B \| R_S \| r_{S_B})$ and then sends $\{H_{SA}, H_{SB}, R_S\}$ to U_B.

Step 4: U_B verifies if H_{SB} is equal to $h_1(ID_B \| ID_S \| H_{SA} \| R_A \| R_B \| R_S \| r_{S_B})$. If it holds, U_B computes $K = T_{r_B}(R_A) = T_{r_B r_A}(\alpha) \bmod p$ and $H_{BA} = h_1(ID_S \| H_{SA} \| K)$ and then sends $\{R_B, H_{BA}, H_{SA}, R_S\}$ to U_A.

Step 5: U_A verifies if H_{SA} is equal to $h_1(ID_A \| ID_S \| R_A \| R_B \| R_S \| r_{S_A})$. If it holds, U_A computes $K =$

$T_{r_A}(R_B) = T_{r_B r_A}(\alpha) \bmod p$. U_A further checks if H_{BA} is equal to $h_1(ID_S \| H_{SA} \| K)$. If it holds, U_A sets $SK = h_3(K)$ as a session key. After that, U_A computes $H'_{AS} = h_1(ID_A \| ID_B \| ID_S \| R_A \| R_B \| R_S \| r_{S_A})$ and $M = h_2(K)$ and then sends $\{H'_{AS}, M\}$ to U_B.

Step 6: U_B verifies if M is equal to $h_2(K)$. If it holds, U_B sets $SK = h_3(K)$ as a session key. U_B computes $H'_{BS} = h_1(ID_A \| ID_B \| ID_S \| R_A \| R_B \| R_S \| r_{S_B})$ and then sends $\{H'_{AS}, H'_{BS}\}$ to S.

Step 7: S verifies the integrity of received $\{H'_{AS}, H'_{BS}\}$. If both hold, S can assure that U_A and U_B have successfully established a common session key.

5 Security Analysis

In this section, we demonstrate the security of our protocol. We first analyze our protocol using the BAN logic [26]. Then we show that our protocol is secure against several kinds of attacks.

5.1 BAN Logic

The BAN logic is widely used to analyze the security of authenticated key agreement protocol. The detailed steps are listed in the following subsections.

Notations of BAN logic. Here we define some notations used in this analysis.

(1) $P \mid\equiv X$: P believes X or called P would be entitled to believe X. In particular, P may act as though X is true.

(2) $P \lhd X$: P sees X. Someone has sent a message containing X to P and P can read and repeat X.

(3) $P \mid\sim X$: P once said X. P sent a message including X at some time. Note that it does not know whether the message was sent long ago or during the current run of the protocol, but it knows that $P \mid\equiv X$ when the message was sent.

(4) $P \mid\Rightarrow X$: P has jurisdiction over X. P controls X which is subject to jurisdiction of P and P is trusted for X.

(5) $\#(X)$: X is fresh. X has not been sent in a message at any time before the execution of current round of the protocol.

(6) $P \overset{K}{\leftrightarrow} Q$: P and Q may use the shared key K to communicate securely. We say that K is good, if K will never be discovered by any principal except P or Q, or a principal trusted by either P or Q.

(7) $P \overset{X}{\Leftrightarrow} Q$: The formula X is a secret known only to P and Q, and possibly to principals trusted by P and Q.

(8) $\{X\}_K$: The formula X is encrypted under a key K.

(9) $<X>_Y$: The formula X is combined with a secret Y.

BAN logic rules.

(1) Message meaning rule for shared keys: $\dfrac{P \mid\equiv P \overset{K}{\leftrightarrow} Q, P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$. It means that if P believes that K is a shared key with Q and P sees X encrypted under K, then P believes that Q once said X.

(2) Message meaning rule for shared secrets: $\dfrac{P \mid\equiv P \overset{Y}{\Leftrightarrow} Q, P \lhd <X>_Y}{P \mid\equiv Q \mid\sim X}$. It means that if P believes that Y is a secret known only to P and Q and P sees X under Y, then P believes that Q once said X.

(3) Nonce verification rule: $\dfrac{P \mid\equiv \#(X), P \mid\equiv Q, \sim X}{P \mid\equiv Q \mid\equiv X}$. It means that if P believes that X is fresh and Q once said X, then P believes Q believes X.

(4) Jurisdiction rule: $\dfrac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$. It means that if P believes that Q has jurisdiction over X and believes Q believes X, then P believes X.

(5) Belief rule I: $\dfrac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X, Y)}$. It means that if P believes X and P believes Y then P believes (X, Y).

(6) Belief rule II: $\dfrac{P \mid\equiv Q \mid\equiv (X, Y)}{P \mid\equiv Q \mid\equiv X}$. It means that if P believes Q believes (X, Y) then P believes Q believes X.

Goals. We want to show that our proposed 3AKE protocol should achieve the following goals:

G_1: $A \mid\equiv (A \overset{SK}{\leftrightarrow} B)$..

G_2: $B \mid\equiv (A \overset{SK}{\leftrightarrow} B)$..

G_3: $S \mid\equiv (A \overset{SK}{\leftrightarrow} B)$..

G_4: $A \mid\equiv B \mid\equiv (A \overset{SK}{\leftrightarrow} B)$..

G_5: $B \mid\equiv A \mid\equiv (A \overset{SK}{\leftrightarrow} B)$..

G_6: $S \mid\equiv A \mid\equiv (A \overset{SK}{\leftrightarrow} B)$..

G_7: $S \mid\equiv B \mid\equiv (A \overset{SK}{\leftrightarrow} B)$..

Idealize the communication messages. We idealize the communication messages of proposed protocol listed as below:

M_1: $A \rightarrow B$: $\{ID_A, R_A\}$.

M_2: $A \rightarrow S$: $\{ID_A, R_A, H_{AS}\}$.

M_3: $B \rightarrow S$: $\{ID_B, R_B, H_{BS}\}$.

M_4: $S \rightarrow A$: $\{H_{SA}, R_S\}$.

M_5: $S \rightarrow B$: $\{H_{SB}, R_S\}$.

M_6: $B \rightarrow A$: $\{R_B, H_{BA}\}$.

M_7: $A \rightarrow B$: $\{M\}$.

M_8: $A \rightarrow S$: $\{H'_{AS}\}$.

M_9: $B \rightarrow S$: $\{H'_{BS}\}$.

Initial state assumptions. We define some initial state assumptions of the proposed protocol as follows:

A_1: $A \mid\equiv \#(r_A)$.

A_2: $B \mid\equiv \#(r_B)$.
A_3: $A \mid\equiv \#(R_A)$.
A_4: $B \mid\equiv \#(R_B)$.
A_5: $A \mid\equiv A \overset{r_{S_A}}{\Leftrightarrow} S$.
A_6: $S \mid\equiv A \overset{r_{S_A}}{\Leftrightarrow} S$..
A_7: $B \mid\equiv B \overset{r_{S_B}}{\Leftrightarrow} S$..
A_8: $S \mid\equiv B \overset{r_{S_B}}{\Leftrightarrow} S$..
A_9: $A \mid\equiv B \mid\Rightarrow R_B$.
A_{10}: $B \mid\equiv A \mid\Rightarrow R_A$.

A_1 and A_2 mean that A and B generate fresh random values r_A and r_B, respectively. Hence, we assume that they are freshness. Since $R_A = T_{r_A}(\alpha) \bmod p$ and $R_B = T_{r_B}(\alpha) \bmod p$, A_3 and A_4 are reasonable according to A_1 and A_2. A_5 and A_6 are valid because the secret r_{S_A} is chosen by the server S and can be revived by the user A. Similarly, A_7 and A_8 are valid. By A_2 and $R_B = T_{r_B}(\alpha) \bmod p$, we have A_9 is valid. By the similar approach, A_{10} is valid.

Detailed description. Based on the rules of the BAN logic, we prove the proposed three parties key agreement protocol can achieve the defined goals using the initial state assumptions.

For G_1. By M_6, we have $S_1 : A \mid\equiv B \mid\equiv R_B$. According to A_9 and S_1, we can obtain $A \mid\equiv R_B$ applying the jurisdiction rule. Since $SK = h_3(K) = h_a(T_{r_A}(R_B))$, , it implies $A \mid (A \overset{SK}{\leftrightarrow} B)$.

For G_2. By M_1, we have S_2: $B \mid\equiv A \mid\equiv R_A$. According to A_{10} and S_2, we can obtain $B \mid\equiv R_A$. applying the jurisdiction rule. Since $SK = h_3(K) = h_a(T_{r_B}(R_A))$, it implies $B \mid\equiv (A \overset{SK}{\leftrightarrow} B)$. .

For G_3. By M_8, we have S_3: $S \triangleleft < H'_{AS} > r_{S_A}$. . According to A_6 and S_3, we can obtain S_4: $S \mid\equiv A \mid\sim H'_{AS}$ applying the message meaning rule for shared secrets. Since H'_{AS} is fresh, it implies S_5: $S \mid\equiv \#(H'_{AS})$. According to S_5 and S_4, we can obtain S_6: $S \mid\equiv A \mid\equiv H'_{AS}$ applying the nonce verification rule. Since H'_{AS} contains R_B, we can obtain S_7: $S \mid\equiv A \mid\equiv B_B$ applying the belief rule II. By M_9, we have S_8: $S \triangleleft < H'_{BS} > r_{S_B}$. According to A_8 and S_8, we can obtain S_9: $S \mid\equiv B \mid\equiv H'_{BS}$ applying the message meaning rule for shared secrets. Since H'_{BS} is fresh, we have S_{10}: $S \mid\equiv \#(H'_{BS})$.. According to S_{10} and S_9, we can obtain S_{11}: $S \mid\equiv B \mid\equiv H'_{BS}$ applying the nonce verification rule. Since H'_{BS} contains R_A, we can obtain S_{12}: $S \mid\equiv B \mid\equiv R_A$ applying the belief rule II. Finally, according to S_7 and S_{12} we can obtain $S \mid\equiv (A \mid\equiv R_B, B \mid\equiv R_A)$ applying the belief rule I. Since $SK = h_3(K) = h_a(T_{r_B}(R_A)) = h_a(T_{r_A}(R_B))$, it implies $S \mid\equiv (A \overset{SK}{\leftrightarrow} B)$.

For G_4. Since $SK = h_3(K)$, by G_1 it implies S_{13}: $A \mid\equiv (A \overset{K}{\leftrightarrow} B)$. . By M_6, we have S_{14}: $A \triangleleft \{H_{BA}\}_K$. According to S_{13} and S_{14}, we can obtain S_{15}: $A \mid\equiv B \mid\equiv \sim H_{BA}$ by the message meaning rule for shared keys. Since H_{BA} is fresh, it implies S_{16}: $A \mid\equiv \#(H_{BA})$. . By S_{16} and S_{15}, we can obtain $A \mid\equiv B \mid\equiv H_{BA}$ applying the nonce verification rule. Because H_{BA} contains H_{SA} and H_{SA} contains R_A, we can obtain $A \mid\equiv B \mid\equiv R_A$.. Since $SK = h_3(K) = h_a(T_{r_B}(R_A))$, we have $A \mid\equiv B \mid\equiv (A \overset{SK}{\leftrightarrow} B)$.

For G_5. Since $SK = h_3(K)$, by G_2 we can obtain S_{17}: $B \mid\equiv (A \overset{K}{\leftrightarrow} B)$. . By M_7, we have S_{18}: $B \triangleleft \{M\}_K$. . According to S_{17} and S_{18}, we can obtain S_{19}: $B \mid\equiv A \mid\sim M$ applying the message meaning rule for shared keys. Since M is fresh, we have S_{20}: $B \mid\equiv \#(M)$. By S_{20} and S_{19}, we can obtain $B \mid\equiv A \mid\equiv M$ applying the nonce verification rule. Because $M = h_2(K)$ contains R_B, we can obtain $B \mid\equiv A \mid\equiv R_B$. Since $SK = h_3(K) = h_a(T_{rA}(R_B))$, it implies $B \mid\equiv A \mid\equiv (A \overset{SK}{\leftrightarrow} B)$. .

For G_6. By S_7, we have $S \mid\equiv A \mid\equiv R_B$.. Since $SK = h_3(K) = h_a(T_{rA}(R_B))$, it implies $S \mid\equiv A \mid\equiv (A \overset{SK}{\leftrightarrow} B)$. .

For G_7. By S_{12}, we have $S \mid\equiv B \mid\equiv R_A$.. Since $SK = h_3(K) = h_a(T_{rB}(R_A))$, it implies $B \mid\equiv B \mid\equiv (A \overset{SK}{\leftrightarrow} B)$. .

5.2 Security Issues

Known session key attack. In an authenticated key agreement protocol, a known session key attack means that an adversary E still cannot compute the further session keys even if E obtains the session key SK. In the proposed protocol, the session key $SK = T_{r1r2}(\alpha)$ only relies on the random values r_1 and r_2. Since the two values of one session are independent on once of other sessions. Hence, even if an adversary E obtains a session key $SK = T_{r1r2}(\alpha)$, it cannot compute the further session key $SK' = T_{r1'r2'}(\alpha)$ without knowing r_1' and r_2'. In other words, the proposed protocol is secure against a known session key attack.

Providing perfect forward secrecy. An authenticated key agreement protocol is said to provide perfect forward secrecy if an adversary E having both two user's password and secret information R_{S_i}, still unable to get previously generated session keys. To compute a session key in our protocol users choose their new random r_i unique for each session, so fressness of session key is guaranteed. The adversary

having password and secret information R_{S_i} still need to know the session specific r_i. Therefore the proposed protocol provides perfect forward secrecy.

Impersonation attack. If an adversary E wants to impersonate the user A, he must obtain the key point $r_{S_A} = R_{S_A} - PW_A$ for A. However, it is impossible because A's password PW_A and secret information R_{S_A} are kept secret. Hence, if E eavesdrops the message $\{ID_A, R_A, H_{AS}\}$ it still cannot impersonate A. By the similar reason, E cannot impersonate the user B. Thus, the proposed protocol is secure against impersonation attacks.

Resistance of password guessing attack. As mentioned above, several 3AKE protocols suffered from password guessing attacks. In our protocol, the value R_{S_i} referred to password is kept secret. In other aspect, $H_{AS} = h_1 (ID_A \| ID_B \| ID_S \| R_A \| r_{S_A})$, where $r_{S_A} = R_{S_A} - PW_A$ is stored in database. Hence, it is not easy to guess the A's password PW_A. In other words, our protocol is secure against password guessing attacks.

6 Performance Evaluation

In this section, we evaluate the performance of our proposed protocol and then compare it with other well-known chaos-based 3PAKE protocols [6, 8-12, 26] in Table 2. *C*, *H* and *S* refer to a Chebyshev polynomial computation operation, a hash function operation and a symmetric encryption/decryption operation, respectively. Here we utilize the experimental results from Xue and Hong in 2011 [28]. According to their results, time consumptions for Chebyshev polynomial computation, symmetric encryption, and one-way hash function are 32.2ms, 0.45ms and 0.2ms, respectively under the environment of 3.2 GHz CPU and 3.0G RAM.

Table 2. Performance comparisons

	User A	User B	Server	Total cost	Time cost (ms)
Lai et al. [6]	3C+5H	3C+5H	2C+6H+2S	8C+16H+2S	261.7
Zhao et al. [8]	3C+6H+1S	3C+6H+1S	2C+8H+2S	8C+20H+4S	263.2
Lee et al. [9]	3C+4H	3C+5H	2C+7H	8C+16H	260.8
Farash et al. [23]	3C+4H	3C+5H	2C+7H	8C+16H	260.8
Hu et al. [11]	3C+5H	3C+6H	2C+7H	8C+18H	261.2
Xie et al. [10]	3C+5H+2S	3C+5H+2S	2C+4H+4S	8C+14H+8S	264
Lee et al. [12]	4C+4H+2S	3C+4H+2S	4C+4H+4S	11C+12H+8S	360.2
Ours	2C+6H	2C+6H	2C+6H	6C+18H	196.8

As shown in Table 2, our protocol is the most efficient one since it uses less Chebyshev polynomial computation.

7 Conclusion

In this paper we identified a replay attack on a few existing 3AKE protocols. We then also proposed a new protocol. According to the security and performance analysis, our new protocol is secure against various kinds of attacks and has better efficiency compared with previous works.

Acknowledgement

The work was supported in part by Shenzhen Technical Project under Grant number JCYJ2017030 7151750788, in part by Shenzhen Technical Project under Grant number KQJSCX20170327161755, and in part by the Natural Science Foundation of Fujian Province under Grant number 2018J01636.

References

[1] X. Cao, W. Kou, X. Du, A Pairing-free Identity-based Authenticated Key Agreement Protocol with Minimal Message Exchanges, *Information Sciences*, Vol. 180, No. 15, pp. 2895-2903, August, 2010.

[2] Y. J. Choie, E. Jeong, E. Lee, Efficient Identity-based Authenticated Key Agreement Protocol from Pairings, *Applied Mathematics and Computation*, Vol. 162, No. 1, pp. 179-188, March, 2005.

[3] H. Zhu, Sustained and Authenticated of a Universal Construction for Multiple Key Agreement Based on Chaotic Maps with Privacy Preserving, *Journal of Internet Technology*, Vol. 17, No. 5, pp. 869-878, September, 2016.

[4] S. Bala, A. K. Verma, A Non-interactive Certificateless Two-party Authenticated Key Agreement Protocol for Wireless Sensor Networks, *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 21, No. 2, pp. 140-155, March, 2016.

[5] H.-M. Sun, B.-Z. He, C.-M. Chen, T.-Y. Wu, C.-H. Lin, H. Wang, A Provable Authenticated Group Key Agreement Protocol for Mobile Environment, *Information Sciences*, Vol. 321, pp. 224-237, November, 2015.

[6] B.-Z. He, C.-M. Chen, T.-Y. Wu, H.-M. Sun, An Efficient Solution for Hierarchical Access Control Problem in Cloud Environment, *Mathematical Problems in Engineering*, Vol. 2014, Article ID 569397, October, 2014.

[7] M. Abdalla, D. Pointcheval, Interactive Diffie-Hellman

Assumptions with Applications to Password-based Authentication, *Financial Cryptography and Data Security*, Roseau, Dominica, 2005, pp. 341-356.

[8] M. Bellare, P. Rogaway, Provably Secure Session Key Distribution: The Three Party Case, *Twenty-seventh Annual ACM Symposium on Theory of Computing*, ACM, Las Vegas, Nevada, 1995, pp. 57-66.

[9] C.-M. Chen, K.-H. Wang, T.-Y. Wu, J.-S. Pan, H.-M. Sun, A Scalable Transitive Human-verifiable Authentication Protocol for Mobile Devices, *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 8, pp. 1318-1330, August, 2013.

[10] H. Lai, J. Xiao, L. Li, Y. Yang, Applying Semigroup Property of Enhanced Chebyshev Polynomials to Anonymous Authentication Protocol, *Mathematical Problems in Engineering*, Vol. 2012, Article ID 454823, June, 2012.

[11] L. Kocarev, J. Makraduli, P. Amato, Public-key Encryption Based on Chebyshev Polynomials, *Circuits, Systems and Signal Processing*, Vol. 24, No. 5, pp. 497-517, October, 2005.

[12] F. Zhao, P. Gong, S. Li, M. Li, 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, October, 2013.

[13] C.-C. Lee, C.-T. Li, 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, July, 2013.

[14] Q. Xie, J. Zhao, X. Yu, Chaotic Maps-based Three-party Password-authenticated Key Agreement Scheme, *Nonlinear Dynamics*, Vol. 74, No. 4, pp. 1021-1027, December, 2013.

[15] X. Hu, 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, October, 2014.

[16] C.-C. Lee, C.-T. Li, S.-T. Chiu, 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, March, 2015.

[17] X. Li, J. Niu, S. Kumari, M. K. Khan, J. Liao, W. Liang, *Design and Analysis of a Chaotic Maps-based Three-party Authenticated Key Agreement Protocol*, Vol. 80, No. 3, pp. 1209-1220, May, 2015.

[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, pp. 61-66, May, 2016.

[19] J. Fridrich, Image Encryption based on Chaotic Maps, *IEEE International Conference on Computational Cybernetics and Simulation*, Orlando, FL, 1997, pp. 1105-1110.

[20] G. Jakimoski, L. Kocarev, Chaos and Cryptography: Block Encryption Ciphers based on Chaotic Maps, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Vol. 48, No. 2, pp. 163-169, February, 2001.

[21] L. Kocarev, M. Sterjev, A. Fekete, G. Vattay, Public-key Encryption with Chaos, *Chaos: An Interdisciplinary Journal of Nonlinear Science*, Vol. 14, No. 4, pp. 1078-1082, December, 2004.

[22] X. Yi, Hash Function based on Chaotic Tent Maps, *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 52, No. 6, pp. 354-357, June, 2005.

[23] H. Zhu, X. Hao, Y. Zhang, M. Jiang, A Biometrics-based Multi-server Key Agreement Scheme on Chaotic Maps Cryptosystem, *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 6, No. 2, pp. 211-224, March, 2015.

[24] H. Zhu, D. Zhu, Y. Zhang, A Multi-server Authenticated Key Agreement Protocol with Privacy Preserving Based on Chaotic Maps in Random Oracle Model, *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 7, No. 1, pp. 59-71, January, 2016.

[25] X. Liao, F. Chen, K.-W. Wong, On the Security of Public-key Algorithms Based on Chebyshev Polynomials over the Finite Field Z_N, *IEEE Transactions on Computers*, Vol. 59, No. 10, pp. 1392-1401, October, 2010.

[26] M. Burrows, M. Abadi, R. M. Needham, A Logic of Authentication, *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, Vol. 426, No. 1871, pp. 233-271, December, 1989.

[27] M. S. Farash, M. A. Attari, S. Kumari, Cryptanalysis and Improvement of a Three-party Password-based Authenticated Key Exchange Protocol with User Anonymity Using Extended Chaotic Maps, *International Journal of Communication Systems*, Vol. 30, No. 1, January, 2017.

[28] K. Xue, P. Hong, Security Improvement on an Anonymous Key Agreement Protocol based on Chaotic Maps, *Communications in Nonlinear Science and Numerical Simulation*, Vol. 17, No. 7, pp. 2969-2977, July, 2012.

Biographies

Chien-Ming Chen received his Ph.D. from the National Tsing Hua University, Taiwan. He is currently an associate professor in Harbin Institute of Technology Shenzhen Graduate School, China. His current research interests include network security, mobile internet, wireless sensor network and cryptography.

Linlin Xu is currently pursuing the M.S. degree in Harbin Institute of Technology Shenzhen Graduate School, China. His current research interests include security protocol, mobile security, and cryptography.

King-Hang Wang received his Ph.D. from the National Tsing Hua University, Taiwan. He worked in the Hong Kong Institute of Technology in 2010 as a lecturer. He joined the Hong Kong University of Science and Technology in 2015 for teaching. His research focus is cryptography, mobile security, and steganography.

Shuai Liu is currently pursuing the M.S. degree in Harbin Institute of Technology Shenzhen Graduate School, China. His current research interests include security protocol, mobile security, and cryptography.

Tsu-Yang Wu received the Ph.D. degree in Department of Mathematics, National Changhua University of Education, Taiwan, in 2010. He is currently an associate professor in College of Computer Science and Engineering, Shandong University of Science and Technology, China. His research interests include applied cryptography, pairing-based cryptography and information security.