PLOS ONE

RESEARCH ARTICLE

# An Extended Chaotic Maps-Based Three-Party Password-Authenticated Key Agreement with User Anonymity

**Yanrong Lu[1,2], Lixiang Li[1,2]*, Hao Zhang[1,2], Yixian Yang[1,2]**

**1** Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China, **2** National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China

* lixiang@bupt.edu.cn





**Citation:** Lu Y, Li L, Zhang H, Yang Y (2016) An Extended Chaotic Maps-Based Three-Party Password-Authenticated Key Agreement with User Anonymity. PLoS ONE 11(4): e0153870. doi:10.1371/journal.pone.0153870

**Editor:** Kim-Kwang Raymond Choo, University of South Australia, AUSTRALIA

**Received:** December 8, 2015

**Accepted:** April 5, 2016

**Published:** April 21, 2016



**Data Availability Statement:** All relevant data are within the paper and its Supporting Information files.

**Funding:** This paper is supported by the National Natural Science Foundation of China (Grant Nos. 61472045, 61573067), the Beijing Natural Science Foundation (Grant No. 4142016), the BUPT Excellent Ph.D. Students Foundation (Grant No. CX2015310), and the Asia Foresight Program under NSFC Grant (Grant No. 61411146001). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

## Abstract

User anonymity is one of the key security features of an authenticated key agreement especially for communicating messages via an insecure network. Owing to the better properties and higher performance of chaotic theory, the chaotic maps have been introduced into the security schemes, and hence numerous key agreement schemes have been put forward under chaotic-maps. Recently, Xie et al. released an enhanced scheme under Farash et al.'s scheme and claimed their improvements could withstand the security loopholes pointed out in the scheme of Farash et al., i.e., resistance to the off-line password guessing and user impersonation attacks. Nevertheless, through our careful analysis, the improvements were released by Xie et al. still could not solve the problems troubled in Farash et al Besides, Xie et al.'s improvements failed to achieve the user anonymity and the session key security. With the purpose of eliminating the security risks of the scheme of Xie et al., we design an anonymous password-based three-party authenticated key agreement under chaotic maps. Both the formal analysis and the formal security verification using AVISPA are presented. Also, BAN logic is used to show the correctness of the enhancements. Furthermore, we also demonstrate that the design thwarts most of the common attacks. We also make a comparison between the recent chaotic-maps based schemes and our enhancements in terms of performance.

## 1 Introduction

Authenticated key exchange protocols, are among the core cryptographic mechanisms for ensuring network security, which aims at establishing a common session key between the communicated participates. For authenticated key exchange through an open environment, both security and privacy are desired. Over the past few decades, many works on authenticated key-exchange have been done referring to kinds of cryptographic primitives (e.g., symmetric cryptography, public key cryptography, hash functions, etc.) applied for different applications [1–11].

**Competing Interests:** The authors have declared that no competing interests exist.

With infiltration and mergence of many scientific branches, chaotic theory has entered the field of vision of the cryptography researchers. Chaotic theory possesses the properties of unpredictability and sensitivity to parameters and initial conditions, which meet some essential requirements of cryptography. Subsequently, cryptography based on chaos theory has been studied widely. The chaotic maps have been applied in the design of symmetric encryption [12–13], S-boxes [14], signature [15] and hash functions [16]. Additionally, chaotic systems have also been applied to design the key agreements, various chaotic maps-based key agreements and related approaches have been presented recently [17–20], owing to that chaotic maps operations offer the semi-group property, and have a better efficiency than point multiplications on an elliptic curve and modular exponential operations [21–22].

According to the numbers of participants for an authenticated key exchange scheme, there are two-party authenticated key exchange schemes, three-party authenticated key exchange schemes, and multi-party authenticated key exchange schemes. Two-party authenticated key exchange schemes are used to establish a session key under environment of client-server. In particular, the suggestion of three-party authenticated key exchange schemes are considered for solving the infeasibility of two-party schemes exchange session keys in large-scale communication environments. In 2011, Wang et al. [23] developed a three-party authenticated key agreement scheme using chaotic maps. However, Yoon et al. [24] declared that the scheme of Wang et al. violated an illegal message modification attack and then they presented an improvement. Next, Lee et al. [25] presented a chaotic maps based three-party authenticated key agreement scheme without using smart card. However, Hu et al. [26] proved that their scheme was not secure against the man-in-the-middle attack in condition that the identity was lost. After that, Farash et al. [27] proposed a three-party authenticated key agreement without applying symmetric cryptography and server's public key. Nevertheless, Xie et al. [28] pointed out three-party authenticated key agreement proposed by Farash et al. could not withstand off-line password guessing attack, thus suffering user impersonation attack. In order to prevent the security threats, Xie et al. presented an enhancement without using server's public key. Obviously, both of Farash et al. and Xie et al.'s schemes are efficient, but without using server's public key is no guarantee of safety. The most important thing to consider that the identity of user is a key personal privacy. Generally, there is a growing requirement for protecting user privacy information from being leaked and abused, which outlines the needs for designing schemes that can attain user anonymity. The adoption of public key cryptography is essential needed to protect user anonymity, which has been verified by the excellent works [29]. Through our carefully analysis, we found that the proposed scheme by Xie et al. could not achieve user anonymity. In addition, their scheme could not resist off-line password guessing, thus notwithstanding user impersonation attack. Furthermore, the session key security could not provide in their scheme. Motivated by it, we design an extended chaotic maps-based three-party password-authenticated key agreement with user anonymity. Both the formal analysis and the formal security verification using AVISPA [30–31] are presented. Also, BAN logic [32] is used to show the correctness of the enhancements. Furthermore, we also demonstrate that the design thwarts most of the common attacks. We also make a comparison between the recent chaotic-maps based schemes and our enhancements in terms of performance.

The outline of the paper are arranged as follows. The Chebyshev chaotic maps and the related intractable problems are introduced in Section 2. The cryptanalysis of Xie et al.'s scheme is presented in Section 3. Section 4 proposes a chaotic maps-based three-party authenticated key agreement. The security analysis of our scheme and comparison with other works are described in Sections 5 and 6, respectively. We summarize the whole paper in Section 7.

## 2 Preliminaries

We will introduce the Chebyshev chaotic maps and the related intractable problems [33–34].

**Chebyshev polynomial** Let $n$ be an integer and $x \in [-1, 1]$. The Chebyshev polynomial $T_n(x)$: $[-1, 1] \rightarrow [-1, 1]$ can be defined as: $T_n(x) = cos(n \cdot arccos(x))$. The recurrent formulas of the Chebyshev polynomial is shown as: $T_0(x) = 1$, $T_1(x) = x$, $T_2(x) = 2x^2 - 1$, $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$.

**Semi-group property** For $p, q \in \mathcal{N}$, $T_p(T_q(x)) = T_{pq}(x) = T_q(T_p(x))(mod\mathcal{N})$.

**Discrete logarithm problem** Known the parameters $x$ and $y$, it is intractable to find an integer $p$ such that $T_p(x) = y$.

**Diffie-Hellman problem** Known the parameters $x$, $T_p(x)$, and $T_q(x)$, it is intractable to compute the value $T_{pq}(x)$.

## 3 Review of Xie et al.'s scheme

In this section, we shall review Xie et al.'s chaotic-maps based authenticated key agreement. Their scheme consists of four phases: system setup, registration, authentication and key exchange and password change. The registration and authentication and key exchange phases are shown in Fig 1. The notations used throughout this study are listed as follows.

$S$: a remote server.

$A$ and $B$: two users.

$ID_A$ and $ID_B$: users' identities of $A$ and $B$.

$pw_A$ and $pw_B$: users's passwords of $A$ and $B$.

$k$ and $T_k(x)$: private and public keys of $S$.

$s$: a secret key of $S$.

$r$: shared secret key between $A$ and $S$.

$h_1()$: a one-way hash function $h_1$: $\{0, 1\}^* \rightarrow \{0, 1\}^l$.

$h()$: a chaotic maps-based one-way hash function $h : \{0, 1\}^* \rightarrow \mathcal{Z}_p$.

$\mathcal{Z}$: ring of integer.

$p$: a large prime number.

### 3.1 System setup

The server $S$ performs the following steps:

Selects its secret key $s$;

Selects a large prime number $p$, $x \in \mathcal{Z}_p$;

Selects a secure one-way hash function $h_1$;

Selects a chaotic maps-based one-way hash function $h()$.

At last, $S$ maintains the secret key $s$ and releases the parameters $\{p, x, h_1(), h()\}$.

### 3.2 Registration

The user $A$ registers the server $S$ as below:

Step 1: User $A$ computes $PW_A = T_{pw_A}(x)modp$ and sends $\{ID_A, PW_A\}$ to $S$ through a secure channel, where $ID_A$ and $pw_A$ are the identity and password of $A$, respectively.

Step 2: The server $S$ computes $VPW_A = h_1(ID_A, s) + PW_A$ and stores $\{ID_A, VPW_A\}$ in its database.

The user $B$ also registers $S$ as the above processes, we omit it.

### 3.3 Authentication and key exchange

The establishment of the session key among $A$, $B$ and $S$ are described in the following:


**Fig 1. Mutual authentication and key agreement of Xie et al.'s scheme.**

doi:10.1371/journal.pone.0153870.g001

Step 1: User $A$ computes $R_A = T_a(x)modp$ and sends $\{ID_A, ID_B, R_A\}$ to $S$, where $a \in [1, p+1]$.

Step 2: Once receiving the login message, $S$ computes $PW_A = VPW_A - h(ID_A, s)$, $PW_B = VPW_B - h(ID_B, s)$, $R_{S1} = T_{S1}(x) - PW_A\ modp$, $R_{S2} = T_{S2}(x) - PW_B\ modp$ and sends back $\{ID_A, R_{S2}\}$ to $B$, sends $\{ID_B, R_{S1}\}$ to $A$.

Step 3: Upon receiving $\{ID_A, R_{S2}\}$ from $S$, $B$ computes $R_B = T_b(x)modp$, $K_{BS} = T_b(R_{S2} + PW_B) = T_{bS2}(x)modp$, $Z_{BS} = h(0, ID_B, ID_A, R_B, R_{S2}, K_{BS})$. Then, $B$ sends $\{R_B, Z_{BS}\}$ to $S$. After $A$ receives $\{ID_B, R_{S1}\}$ from $S$, he computes $K_{AS} = T_a(R_{S1} + PW_A) = T_{aS1}(x)modp$, $Z_{AS} = h(0, ID_A, ID_B, R_A, R_{S1}, K_{AS})$. Then, $A$ sends $\{Z_{AS}\}$ to $S$.

Step 4: Upon receiving the messages from $A$ and $B$, $S$ computes $K_{SB} = T_{S2}(R_B) = T_{S2b}(x)\ modp$ and checks whether $h(0, ID_B, ID_A, R_B, R_{S2}, K_{SB}) \stackrel{?}{=} Z_{BS}$. If it is true, $S$ then computes $K_{SA} = T_{S1}(R_A) = T_{S1a}(x)modp$ and checks whether $h(0, ID_A, ID_B, R_A, R_{S1}, K_{SA}) \stackrel{?}{=} Z_{AS}$. If holds, $S$ computes $Z_{AB} = h(1, ID_A, ID_B, R_A, R_B, K_{SA})$, $Z_{BA} = h(1, ID_B, ID_A, R_B, R_A, K_{SB})$ and sends $\{R_B, Z_{AB}\}$ and $\{R_A, Z_{BA}\}$ to $A$ and $B$, respectively.

Step 5: When $A$ gets $\{R_B, Z_{AB}\}$, he verifies whether $h(1, ID_A, ID_B, R_A, R_B, K_{AS}) \stackrel{?}{=} Z_{AB}$. If holds, $A$ can compute $K_{AB} = T_a(R_B) = T_{ab}(x)modp$ and the session key $SK = h(2, ID_A, ID_B, R_A, R_B, K_{AB})$. Similarly, once $B$ gets $\{R_A, Z_{BA}\}$, he verifies whether $h(1, ID_B, ID_A, R_B, R_A, K_{BS}) \stackrel{?}{=} Z_{BA}$. If it is valid, $B$ can compute $K_{BA} = T_b(R_A) = T_{ba}(x)modp$ and the session key $SK = h(2, ID_A, ID_B, R_A, R_B, K_{BA})$.

### 3.4 Password change

If user $A$ attempts to update his password as a new one, he can perform the following steps:

Step 1: User $A$ computes $PW_A^{new} = T_{pw_A^{new}}(x)modp$, $PWD = h(K_{AS}, ID_A) + PW_A modp$, $V_A = h(K_{AS}, PW_A)$, $Z_{AS} = h(1, ID_A, R_A, S_1, K_{AS}, V_A, M_A)$ and sends $\{ID_A, R_A, Z_{AS}, PWD, V_A, M_A\}$ to $S$, where $M_A$ = {Password update request}.

Step 2: $S$ first checks whether $h(1, ID_A, R_A, R_{S1}, K_{SA}, V_A, M_A) \stackrel{?}{=} Z_{AS}$. If it holds, $S$ computes $PW_A = PWD - h(K_{SA}, ID_A)modp$ and checks whether $h(K_{SA}, PW_A) \stackrel{?}{=} V_A$. If it holds, $S$ computes $R_1 = h(1, ID_A, PWD, V_A, K_{SA})$, $VPW_A = h(ID_A, s) + PW_A\ modp$, replaces $VPW_A$ with $VPW_A^{new}$ in its database, and sends $\{Accept, R_1\}$ to $A$. Otherwise, $S$ sends $\{Reject, R_2\}$ to $A$, where $R_2 = h(0, ID_A, PWD, V_A, K_{SA})$.

Step 3: When $A$ receives $\{Accept, R_1\}$, he verifies if $h(1, ID_A, PWD, V_A, K_{AS}) \stackrel{?}{=} R_1$. If true, $A$ accepts $pw_A^{new}$ as his new password. Otherwise, he verifies whether $h(0, ID_A, PWD, V_A, K_{AS}) \stackrel{?}{=} R_2$ and returns Step 1 to execute the above steps again.

## 4 Cryptanalysis of Xie et al.'s scheme

Xie et al.'s scheme declared that their improvements could withstand the password off-line guessing attack and the user impersonation attack which Farash et al.'s scheme failed to resist. However, we will demonstrate their improvement cannot really resist the off-line password guessing attack, thus suffering the user impersonation attack. Besides, we also demonstrate their improvements cannot achieve the session key security as they stated. Furthermore, user anonymity is also not able to provide in their improvements. In order to launch the attacks, we adopt the attack model proposed by Xu et al. [35]. According to their assumption, an attacker $\mathbb{U}$ can completely monitor the open communication channel, thus inserting, deleting, and modifying any messages among correspondents.

### 4.1 Off-line password guessing attack

$\mathbb{U}$ can easily perform the attack by intercepting the transmitted messages $\{ID_A, ID_B, R_A\}$ and $Z_{AS}$ from $A$ to $S$ as below:

Step 1: $\mathbb{U}$ computes $R_A = T_a(x)modp$ and sends $\{ID_A, ID_B, R_A\}$ to $S$, where $a \in [1, p+1]$ is a random number.

Step 2: $S$ computes $PW_A = VPW_A - h(ID_A, s)$, $PW_B = VPW_B - h(ID_B, s)$, $R_{S1} = T_{S1}(x) - PW_A\ modp$, $R_{S2} = T_{S2}(x) - PW_B\ modp$, where $S1, S2 \in [1, p+1]$. Next, $S$ sends $\{ID_B, R_{S1}\}$ to $A$.

Step 3: $\mathbb{U}$ guesses a candidate password $PW'_A$ and computes $K_{AS} = T_a(R_{S1} + PW'_A) = T_{aS1}(x)modp$. After that, $\mathbb{U}$ checks whether $Z_{AS} \stackrel{?}{=} h(0, ID_A, ID_B, R_A, R_{S1}, K_{AS})$. If the equation is true, which means $\mathbb{U}$ gets the correct password. Otherwise, $\mathbb{U}$ performs the above steps again until he succeeds.

## 4.2 User impersonation attack

After obtaining the password of user $A$(or user $B$), $\mathbb{U}$ can masquerade as a legitimate user $A$ (or user $B$) to cheat the server $A$ and the user $B$ (or user $A$). Following previous subsection, once $\mathbb{U}$ guesses correctly, he then sends $\{Z_{AS}\}$ to $S$. Upon receiving the messages from $\mathbb{U}$, $S$ executes the original scheme without any detection. Finally, $S$ sends $\{R_B, Z_{AB}\}$ to $\mathbb{U}$. After receiving the messages from $S$, $\mathbb{U}$ verifies whether $Z_{AB} = h(1, ID_A, ID_B, R_A, R_B, K_{AS})$. If it is true, $\mathbb{U}$ computes $K_{AB} = T_a(R_B) = T_{ab}(x)modp$ and the session key $SK_{AB} = h(2, ID_A, ID_B, R_A, R_B, K_{AB})$. That is, $\mathbb{U}$ successfully wormed himself into $S$ and $B$s' confidence.

## 4.3 Anonymity of users

The user identity is an important personal privacy. In many cases, $\mathbb{U}$ may exploit the user identity to link different login sessions together to trace user activities [29]. Moreover, the violation of user identity and activities may also facilitate an unauthorized entity to trace the user's login history and even current location [36]. In Xie et al.'s scheme, the messages transmitted from $A$ to $S$ $\{ID_A, ID_B, R_A\}$, sent from $S$ to $A$ $\{ID_B, R_{S1}\}$, the message transmitted from $S$ to $B$ $\{ID_A, R_{S2}\}$, are all exposed the identity of $A$ and $B$. It is a good chance for $\mathbb{U}$ to obtain the identity and know who is requiring the service and further trace the position. This means Xie et al.'s scheme fails to achieve user anonymity.

## 4.4 Violation of the session key security

After deriving password $PW_A$ by performing the off-line password guessing attack, $\mathbb{U}$ can easily derive the mutually shared session key between $A$ and $B$ after intercepting the transmitted messages $R_A$ and $R_B$. And thus, $\mathbb{U}$ can compute an integer solution $a^*$ (or $b^*$) to satisfy the equation $T^*_a(x) = T_a(x)$(or $T^*_b(x) = T_b(x)$) by adopting the method of Bergamo et al. [22]:

$$a^* = \frac{arccos(T_a(x))+2k\pi}{arccos(x)} | k \in \mathcal{Z} \left( b^* = \frac{arccos(T_b(x))+2k\pi}{arccos(x)} | k \in \mathcal{Z} \right)$$

With the value $a^*$ and $b^*$, $\mathbb{U}$ can compute the session key: $T^*_a(T^*_b(x))modp = T^*_a(T_b(x))modp = T_b(T^*_a(x))modp = T_b(T_a(x))modp = T_{ba}(x)modp = K_{AB}$

In this regard, $\mathbb{U}$ can compute the session key $SK = h(2, ID_A, ID_B, R_A, R_B, K_{BA})$ since all the parameters contained in $SK$ can be obtained only by intercepting the communication channel.

# 5 Proposed scheme

This section presents our enhanced scheme which inherits the advantages and avoids the disadvantages of the scheme proposed by Xie et al.. The proposed scheme contains four phases: system initialization, registration, the session key establishment and password updating. The registration and the session key establishment phases are shown in Fig 2.

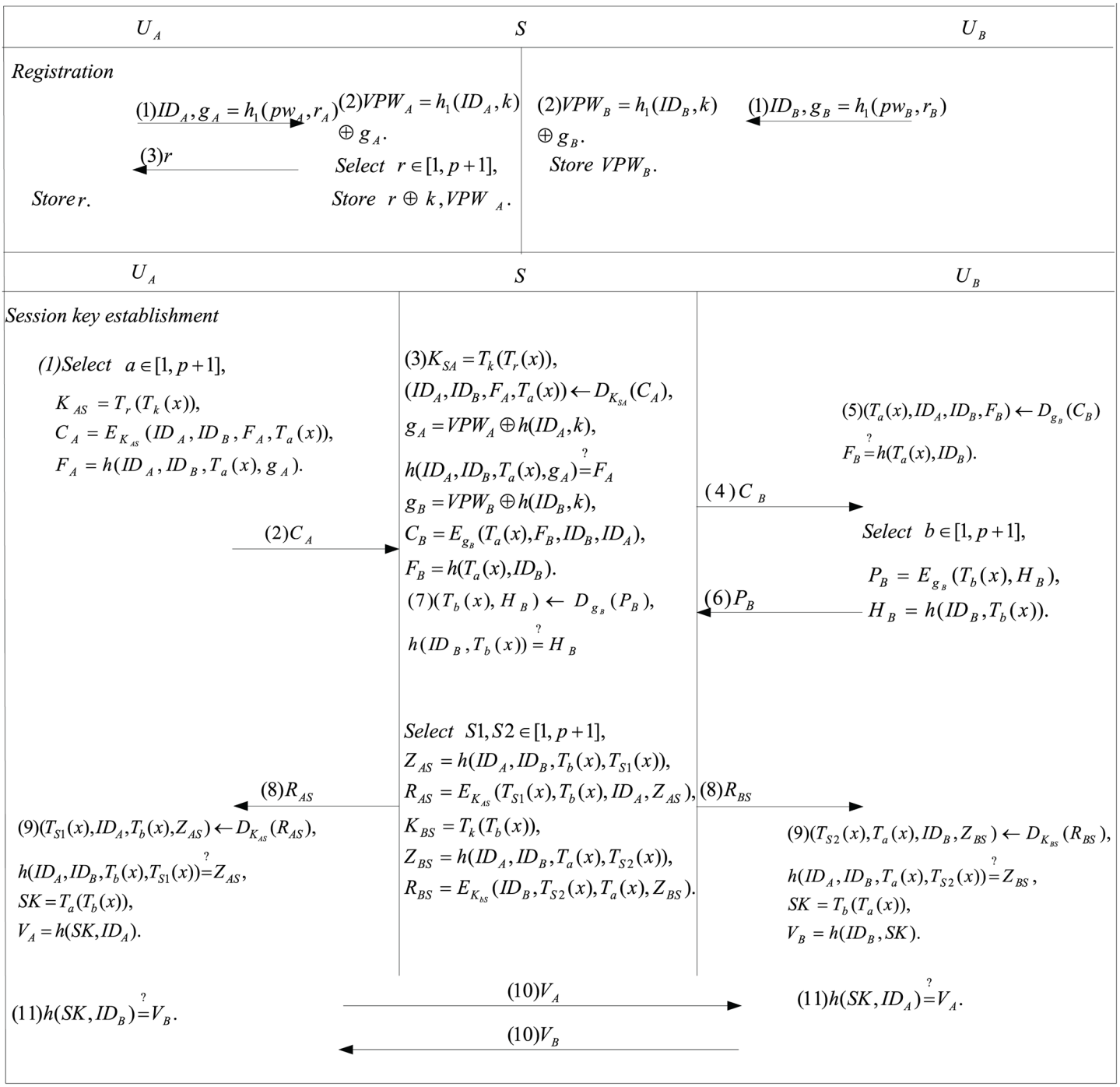


**Fig 2. Mutual authentication and key agreement of our scheme.**

doi:10.1371/journal.pone.0153870.g002

## 5.1 System initialization

The server $S$ performs the following steps:

Step 1: Selects a random number $x \in \mathcal{Z}_p$;

Step 2: Selects a private key $k \in [1, p+1]$ and computes $T_k(x)modp$ as its public key;

Step 3: Selects a chaotic map hash function $h()$, $S$ maintains the secret key $k$ and releases the parameters $\{p, x, T_k(x)modp, h()\}$.

## 5.2 Registration

The registration phase of $A/B$ as below:

Step 1: User $A/B$ submits $\{ID_A, g_A = h_1(pw_A, r_A)\}/\{ID_B, g_B = h_1(pw_B, r_B)\}$ to the server $S$, where $r_A$ and $r_B$ are the random numbers;

Step 2: Upon receiving the registration request, $S$ computes $VPW_A = h_1(ID_A, k) \oplus g_A$/ $VPW_B = h_1(ID_B, k) \oplus g_B$. Next, $S$ randomly chooses a secret key $r$ for $A$ and sends it to $A$ via the private channel. Noth that $r$ is kept securely by $A$ and is different for each user $A$. Finally, $S$ stores $k \oplus r$ and $VPW_A/VPW_B$ into its memory.

## 5.3 Session key establishment

After registering the server $S$, users $A$ and $B$ establish the session key with the help of $S$ in the following manner:

Step 1: Using the stored shared secret key $r$, user $A$ computes his own version of $C_A = E_{K_{AS}}(ID_A, ID_B, T_a(x), F_A)$ and sends them to $S$, where $K_{AS} = T_r(T_k(x))$, $F_A = h(ID_A, ID_B, T_a(x), g_A)$ and $a \in [p+1]$ is a random number.

Step 2: Once receiving the message, $S$ first derives $r$ by computing $k \oplus r \oplus k$ and derives $\{ID_A, ID_B, T_a(x), F_A\}$ by decrypting $C_A$ with computed symmetric key $K_{AS} = T_k(T_r(x))$. Next, $S$ checks whether $h(ID_A, ID_B, T_a(x), g_A) \stackrel{?}{=} F_A$, where $g_A = VPW_A \oplus h(ID_A, k)$. If the equation is true, $S$ computes $C_B = E_{g_B}(T_a(x), F_B, ID_A, ID_B)$ and sends back it to user $B$, where $F_B = h(T_a(x), ID_B)$.

Step 3: After receipt of the authentication message from $S$, user $B$ first retrieves $\{T_a(x), ID_A, ID_B, F_B\}$ by decrypting $C_B$ and checks the validness of $F_B$. If it is correct, $B$ computes $P_B = E_{g_B}(T_b(x), H_B)$ and sends back an authentication message via an unsecure channel to $S$ with the following values $\{P_B\}$, where $H_B = h(ID_B, T_b(x))$ and $b \in [1, p+1]$ is a random number at $B$ side.

Step 4: $S$ decrypts $P_B$ to get $T_b(x)$ and $H_B$ using $g_B$. After that, $S$ examines whether $h(ID_B, T_b(x)) \stackrel{?}{=} H_B$. If it is correct, $S$ computes $Z_{AS} = h(ID_A, ID_B, T_b(x), T_{S1}(x))$, $R_{AS} = E_{K_{AS}}(T_{S1}(x), T_b(x), ID_A, Z_{AS})$ and returns $R_{AS}$ to $A$, where $S1$ is the random number and $K_{AS} = T_k(T_r(x))$ is a shared key between $A$ and $S$. At the same time, $S$ also computes $Z_{BS} = h(ID_A, ID_B, T_a(x), T_{S2}(x))$, $R_{BS} = E_{K_{BS}}(T_{S2}(x), T_a(x), ID_B, Z_{BS})$ and returns $R_{BS}$ to $B$, where $S2$ is the random number and $K_{BS} = T_k(T_b(x))$.

Step 5: When receiving the message from $S$, $A$ checks whether $h(ID_A, ID_B, T_b(x), T_{S1}(x)) \stackrel{?}{=} Z_{AS}$ which is decrypted from $R_{AS}$. If it holds, $A$ computes the session key $SK = T_a(T_b(x))$ and $V_A = h(ID_A, SK)$, and then sends $V_A$ to $B$. Similarly, $B$ verifies the validity of $Z_{BS} = h(ID_A, ID_B, T_a(x), T_{S2}(x))$ which is derived from $R_{BS}$. If it holds, $B$ computes the session key $SK = T_b(T_a(x))$ and $V_B = h(ID_B, SK)$, and then sends $V_B$ to $A$.

Step 6: Upon receiving the message from $B$, $A$ verifies whether $h(ID_B, SK)$ is equal to the received $V_B$. If the verification holds, $A$ negotiates $SK$ as the shared session key to encrypt the following messages. Otherwise, $A$ aborts the session. At the same time, $B$ checks the correctness of $V_B = h(ID_A, SK)$. Once the result is true, $B$ agrees the session key $SK$ with $A$.

### 5.4 Password update

When $A$ intends to change his password after successful handshake between $A$ and $S$, he can perform the following steps:

Step 1: $A$ selects a new password $pw_A^*$ and computes $R_A = E_{T_r(x)}(ID_A, h_1(pw_A^*, r_A), h_1(pw_A, r_A), Z_{AS})$ and $Z_{AS} = h(ID_A, T_{S1}(x), K_{AS})$ to $S$.

Step 2: $S$ decrypts $R_A$ to retrieve $\{ID_A, h_1(pw_A^*, r_A), h_1(pw_A, r_A), Z_{AS}\}$ using the shared secret key $r$ and verifies whether $h(ID_A, T_{S1}(x), K_{AS}) \stackrel{?}{=} Z_{AS}$. If it is correct, $S$ computes $VPW_A^* = h_1(pw_A, r_A) \oplus VPW_A \oplus h_1(pw_A^*, r_A)$. Next, $S$ updates $VPW_A$ with $VPW_A^*$.

If $B$ plans to change his password into a new one after successful authentication process between $B$ and $S$, he performs the following steps:

Step 1: $B$ selects a new password $pw_B^*$ and computes $R_B = E_{K_{BS}}(ID_B, h_1(pw_B^*, r_B), h_1(pw_B, r_B), Z_{BS})$ and $Z_{BS} = h(ID_B, T_{S2}(x), K_{BS})$ to $S$.

Step 2: $S$ decrypts $R_B$ to retrieve $\{ID_B, h_1(pw_B^*, r_B), h_1(pw_B, r_B), Z_{BS}\}$ by the shared key $K_{BS}$ and verifies whether $h(ID_B, T_{S2}(x), K_{BS}) \stackrel{?}{=} Z_{BS}$. If it is correct, $S$ computes $VPW_B^* = h_1(pw_B, r_B) \oplus VPW_B \oplus h_1(pw_B^*, r_B)$. Next, $S$ updates $VPW_B$ with $VPW_B^*$.

## 6 Security analysis of the proposed scheme

In this part, we first present a formal security analysis and then adopt the well-known formal tool for analyzing cryptographic protocol, i.e., BAN logic, to demonstrate the validness of the established session key between $A$ and $B$ in the help of the server $S$. After that, we conduct a security discussion for the proposed scheme according to the known kinds of security attributes. Next, we adopt the formal verification software to demonstrate our scheme is secure.

### 6.1 Formal security proof of the proposed scheme

Based on the one-way property of hash function [16] and ciphertext indistinguishability of symmetric cryptography algorithm [37], this part gives the formal analysis of the proposed scheme.

*Symmetric cryptography algorithm* Θ *assumption*: Denote the Θ advantage by $Adv_P^{\Theta}$. Θ is secure if $Adv_P^{\Theta}$ is negligible for any probabilistic, polynomial time adversary.

***Theorem 1*** Let Θ is secure. Assume that the one-way hash function $h(\cdot)$ behaves as a random oracle, then our proposed password-authentication key agreement defends against an adversary $\mathbb{U}$ for extracting the identity $ID_A$ of the user $A$, and the session key $SK$ between the user $A$ and the user $B$.

*Reveal 1*: This oracle unconditionally outputs the cleartext $m$ using symmetric cryptography algorithm Θ under the corresponding ciphertext $C = Enc_k(m)$.

*Reveal 2*: This oracle unconditionally outputs the input $x$ using hash function under the corresponding hash value $y = h(x)$.

***Proof.*** The adversary $\mathbb{U}$ executes the experiments $Exp1^{\Theta}_{\mathbb{U},TPPPAKA}$ (Table 1) and $Exp2^{Hash}_{\mathbb{U},TPPPAKA}$ (Table 2) for our three-party password-authentication key agreement. Suppose that the adversary $\mathbb{U}$ could get the identity $ID_A$ of the user $A$, and the session key $SK$ between the user $A$ and the user $B$, which means $\mathbb{U}$ has an extremely high probability $Max_{\mathbb{U}}Succ_1$ and $Max_{\mathbb{U}}Succ_2$ to win the game within the running time $t_i$ and the number of queries $q_i (i = 1, 2)$, where $Succ_1 = |Pr(Exp1^{\Theta}_{\mathbb{U},TPPPAKA} = 1) - 1$ and $Succ_2 = |Pr(Exp2^{Hash}_{\mathbb{U},TPPPAKA} = 1) - 1$. However, they are both computationally infeasible problems under the symmetric cryptography algorithm Θ assumption without the knowledge of the secret key $k$ and non-invertibility of hash function, i.e., $Adv^{\Theta}_{\mathbb{U},TPPPAKA}(t_1) \leqslant \varepsilon_1$, $Adv^{hash}_{\mathbb{U},TPPPAKA}(t_2) \leqslant \varepsilon_2$, for any sufficiently small $\varepsilon_i > 0 (i = 1, 2)$. That is,

**Table 1. Algorithm 1.**

| |
|---|
| 1. Intercept the login message $\{C_A\}$, $C_A = E_{K_{AS}}(ID_A, ID_B, T_a(x), F_A)$ |
| 2. Call Reveal oracle 1. Let $(ID'_A, ID'_B, T_a(x)', F'_A) \leftarrow Reveal(C_A)$ |
| 3. Intercept the authenticated message $\{C_B\}$, where $C_B = E_{g_B}(ID_A, ID_B, T_a(x), F_B)$ |
| 4. Call Reveal oracle 1. Let $(ID''_A, ID''_B, T_a(x)'', F''_B) \leftarrow Reveal(C_B)$ |
| 5. **If** $(T_a(x)'' = T_a(x)')$ **then** |
| 6. Accept $ID'_A$ as the true identity of the user $A$ |
| 7. **return 1** |
| 8. **else** |
| 9. **return 0** |
| 10. **end if** |

doi:10.1371/journal.pone.0153870.t001

**Table 2. Algorithm 2.**

| |
|---|
| 1. Intercept the login message $\{V_A\}$, where $V_A = h(ID_A, SK)$ |
| 2. Call Reveal oracle 2. Let $(ID'_A, SK') \leftarrow Reveal(V_A)$ |
| 3. Intercept the authenticated message Intercept the login message $\{V_A\}$, |
| where $V_B = h(ID_B, SK)$ |
| 4. Call Reveal oracle 1. Let $(ID''_A, SK'') \leftarrow Reveal(V_B)$ |
| 5. **If** $(ID'_A = ID''_A)$ **then** |
| 6. Accept $SK'$ as the correct session key between $A$ and $B$ |
| 7. **return 1** |
| 8. **else** |
| 9. **return 0** |
| 10. **end if** |

doi:10.1371/journal.pone.0153870.t002

$Max_{\mathbb{U}}Succ_1 \leqslant \varepsilon_1$ and $Max_{\mathbb{U}}Succ_2 \leqslant \varepsilon_2$ since both they depend on the advantage $Adv^{\Theta}_{\mathbb{U},TPPPAKA}$ and $Adv^{hash}_{\mathbb{U},TPPPAKA}$, respectively. As a result, no adversary $\mathbb{U}$ has the ability to derive the identity $ID_i$ of the $A$ and the session key $SK$ between the user $A$ and the user $B$.

## 6.2 Authentication proof based on BAN logic

BAN logic is an important formal mean and is widely applied for the security analysis of authentication schemes. Verification process for the protocol using BAN logic is mainly composed of four parts: ***Goals***, ***Idealisation***, ***Assumptions*** and ***Analysis***. Goals, as its name suggests, the objectives of the verification; Idealisation aims at formulating the protocol step in a way for each ciphertext communication; Assumptions state some essential information, such as, which principals have generated which fresh random numbers, what keys are originally shared between the principals, and which principals are trusted in special ways. Upon all the aforementioned basis, BAN logic analysis on the protocol step by step is a natural procedure. BAN logic defines some notations and rules to verify whether the mutual authentication is achieved between corresponds. We first introduce some common notations and rules related with our analysis in the following.

***Notations***

$P \lhd X$: principal $P$ sees a message containing $X$

$P| \equiv X$: $P$ believes $X$ is true

$P|\sim X$: $P$ is known to have sent a message including $X$

$P \overset{K}{\leftrightarrow} Q$: $P$ and $Q$ communicate with a shared key $K$

$\#X$: formula $X$ is fresh

$P \Rightarrow X$: $P$ has jurisdiction over $X$

$<X, Y>_K$: $X$ and $Y$ are encrypted with the key $K$

$\{X, Y\}$: $X$ or $Y$ is a part of the message $\{X, Y\}$

$\frac{Statement1, Statement2}{Statement3}$: a conjunction of *statements*1 and 2 can infer *statement*3

***Rules***

$\frac{A|\equiv A \overset{K}{\leftrightarrow} B,\ \ A \trianglelefteq \{X\}_K}{A|\equiv |B\sim X}$(Message-meaning rule): if $A$ believes that the key $K$ is shared with $B$ and and receives a message containing $X$ encrypted under $K$, then $A$ believes that $B$ once said $X$.

$\frac{A|\equiv \#X,\ \ A|\equiv B|\sim X}{A|\equiv B|\equiv X}$(Nonce-verification rule): if $A$ once said $X$, and $A$ believes that $B$ once said $X$, then $A$ believes that $A$ believes $X$.

$\frac{A|\equiv \#X}{A|\equiv \#(X,\ \ Y)}$(Fresh conjuncatenation rule): if $A$ believes a component of a formula $(X, Y)$ is fresh, then $A$ believes the formula is fresh.

$\frac{A|\equiv B \Rightarrow X,\ \ A|\equiv B|\equiv X}{A|\equiv X}$(Jurisdiction rule): if $A$ believes that $B$ has controlled over $X$, and $A$ believes that $B$ believes $X$, then $A$ trusts $B$ on the truth of $X$.

(1) We establish the following ***goals*** which the session key agreement protocol should achieve:

$goal_1.\ A| \equiv A \overset{SK}{\longleftrightarrow} B$

$goal_2.\ A| \equiv B| \equiv A \overset{SK}{\longleftrightarrow} B$

$goal_3.\ A|\equiv B|\equiv ID_B$

$goal_4.\ B| \equiv A \overset{SK}{\longleftrightarrow} B$

$goal_5.\ B|\equiv ID_A$

$goal_6.\ B|\equiv A|\equiv ID_A$

$goal_7.\ B| \equiv A| \equiv A \overset{SK}{\longleftrightarrow} B$

(2) We ***idealize*** the communication messages of the proposed scheme as below:

$A \rightarrow S$:

$C_A :< ID_A, ID_B, F_A, T_a(x) >_{A \overset{K_{AS}}{\longleftrightarrow} S}$,

$F_A :< ID_A, ID_B, T_a(x) >_{A \overset{g_A}{\longleftrightarrow} S}$.

$S \rightarrow A$:

$R_{AS} :< T_{S1}(x), T_b(x), Z_{AS}, ID_A >_{A \overset{K_{AS}}{\longleftrightarrow} S}$,

$Z_{AS}$: $(ID_A, ID_B, T_b(x), T_{S1}(x))$.

$S \rightarrow B$:

$C_B : \{T_a(x), ID_A, ID_B, F_B\}_{A \overset{g_B}{\longleftrightarrow} S}$,

$F_B$: $h(T_a(x), ID_B)$,

$R_{BS} :< ID_B, T_{S2}(x), T_a(x), Z_{BS} >_{B \overset{K_{BS}}{\longleftrightarrow} S}$,

$Z_{BS}$: $h(ID_A, ID_B, T_a(x), T_{S2}(x))$.

$B \rightarrow S$:

$P_B :< T_b(x), H_B >_{B \overset{g_B}{\longleftrightarrow} S}$,

$H_B$: $(ID_B, T_b(x))$.

$A \rightarrow B$:

$V_A :< ID_A, SK >_{A \overset{SK}{\longleftrightarrow} B}$.

$B \rightarrow A$:

$V_B :< ID_B, SK >_{A \overset{SK}{\longleftrightarrow} B}$.

(3) We make some initial ***assumptions*** for the proposed scheme as follows:

$A_1$. $A| \equiv \#a$

$A_2$. $B| \equiv \#b$

$A_3$. $B| \equiv ID_B$

$A_4$. $A| \equiv ID_A$

$A_5$. $A| \equiv A \overset{K_{AS}}{\longleftrightarrow} S$

$A_6$. $S| \equiv A \overset{K_{AS}}{\longleftrightarrow} S$

$A_7$. $A| \equiv ID_B$

$A_8$. $A| \equiv A \overset{T_r(x)}{\longleftrightarrow} S$

$A_9$. $S| \equiv A \overset{T_r(x)}{\longleftrightarrow} S$

$A_{10}$. $A| \equiv A \overset{T_{aS1}(x)}{\longleftrightarrow} S$

$A_{11}$. $S| \equiv A \overset{T_{aS1}(x)}{\longleftrightarrow} S$

$A_{12}$. $B| \equiv B \overset{T_{bS2}(x)}{\longleftrightarrow} S$

$A_{13}$. $S| \equiv B \overset{T_{bS2}(x)}{\longleftrightarrow} S$

$A_{14}$. $B| \equiv B \overset{K_{BS}}{\longleftrightarrow} S$

$A_{15}$. $B| \equiv B \overset{g_B}{\longleftrightarrow} S$

Now, using the rules of the BAN logic, we ***demonstrate*** the proposed scheme can attain the intended goals based on the above descriptions:

According to the message $C_A$, we derive:

$D_1$. $S\triangleleft < ID_A, ID_B, F_A, T_a(x) >_{A \overset{K_{AS}}{\longleftrightarrow} S}$

According to $A_6$, $D_1$ and message-meaning rule, we get:

$D_2$. $\frac{S\triangleleft <ID_A, ID_B, F_A, T_a(x)>_{A \overset{K_{AS}}{\longleftrightarrow} S},\ S| \equiv A \overset{K_{AS}}{\longleftrightarrow} S}{S| \equiv A| \sim \{ID_A, ID_B, F_A, T_a(x)\}}$

According to $R_{AS}$, we obtain:

$D_3$. $A\triangleleft < T_{S1}(x), T_b(x), Z_{AS}, ID_A >_{A \overset{K_{AS}}{\longleftrightarrow} S}$

According to $A_5$, $D_3$ and message-meaning rule, we get:

$D_4$. $\frac{A\triangleleft <T_{S1}(x), T_b(x), Z_{AS}, ID_A>_{A \overset{K_{AS}}{\longleftrightarrow} S}, A| \equiv A \overset{K_{AS}}{\longleftrightarrow} S}{A| \equiv S| \sim \{T_{S1}(x), T_b(x), Z_{AS}, ID_A\}}$

According to $D_4$, $A_4$ and fresh conjuncatenation rule, we obtain:

$D_5$. $\frac{A| \equiv ID_A, A| \equiv S| \sim \{T_{S1}(x), T_b(x), Z_{AS}, ID_A\}}{A| \equiv \{T_b(x), T_{S1}(x), Z_{AS}\}}$

According to $D_5$, we immediately retrieve:

$D_6$. $\frac{A| \equiv \{T_{S1}(x), T_b(x), Z_{AS}\}}{A| \equiv T_{S1}(x), A| \equiv T_b(x), A| \equiv Z_{AS}}$

According to $D_6$, $SK = T_a(T_b(x))$ and $A_1$, we also eventually achieve:

$goal_1$. $\frac{A| \equiv T_b(x), SK = T_a(T_b(x)), A| \equiv \#a}{A| \equiv A \overset{SK}{\longleftrightarrow} B}$

According to the message $V_B$, we gain:

$D_7$. $A\triangleleft (ID_B, SK)_{A \overset{SK}{\longleftrightarrow} B}$

According to $D_7$, $goal_1$ and message-meaning rule, we get:

$D_8$. $\frac{A\triangleleft (ID_B, A \overset{SK}{\longleftrightarrow} B)_{SK}, A| \equiv A \overset{SK}{\longleftrightarrow} B}{A| \equiv B| \sim \{ID_B, A \overset{SK}{\longleftrightarrow} B\}}$

According to $goal_1$, $D_8$ and nonce-verification rule, we attain:

$goal_2$. $\frac{A| \equiv A \overset{SK}{\longleftrightarrow} B, A| \equiv B| \sim A \overset{SK}{\longleftrightarrow} B}{A| \equiv B| \equiv A \overset{SK}{\longleftrightarrow} B}$

According to $D_8$, $A_7$ and nonce-verification rule, we achieve:

$goal_3$. $\frac{A| \equiv ID_B, A| \equiv B| \sim ID_B}{A| \equiv B| \equiv ID_B}$

According to the message $R_{BS}$, we extract:

$D_9$. $B\triangleleft < ID_B, T_{S2}(x), T_a(x), Z_{BS} >_{B \overset{K_{BS}}{\longleftrightarrow} S}$

According to $A_{14}$, $D_9$ and message-meaning rule, we collect:

$D_{10}$. $\frac{B\triangleleft<ID_B,T_{S2}(x),T_a(x),Z_{BS}>_{B\xleftarrow{K_{BS}}S},B|\equiv B\xleftrightarrow{K_{BS}}S}{B|\equiv S|\sim\{ID_B,T_{S2}(x),T_a(x),Z_{BS}\}}$

According to $A_3$, $D_{10}$ and fresh conjuncatenation rule, we acquire:

$D_{11}$. $\frac{B|\equiv ID_B,B|\equiv S|\sim\{ID_B,T_{S2}(x),T_a(x),Z_{BS}\}}{B|\equiv\{T_{S2}(x),T_a(x),Z_{BS}}$

According to $D_{11}$, we intuitively collect:

$D_{12}$. $\frac{B|\equiv\{T_{S2}(x),T_a(x),Z_{BS}\}}{B|\equiv T_{S2}(x),B|\equiv T_a(x),B|\equiv Z_{BS}}$

According to $A_2$, $D_{12}$ and $SK = T_b(T_a(x))$, we naturally receive:

$goal_4$. $\frac{B|\equiv T_a(x),SK=T_b(T_a(x)),B|\equiv\#b}{B|\equiv A\xleftrightarrow{SK}B}$

According to the message $C_B$, we obtain:

$D_{13}$. $B\triangleleft\{T_a(x),ID_A,ID_B,F_B\}_{A\xleftrightarrow{g_B}S}$

According to $A_{15}$, $D_{13}$ and message-meaning rule, we attain:

$D_{14}$. $\frac{B\triangleleft\{T_a(x),ID_A,ID_B,F_B\}_{A\xleftrightarrow{g_B}S},B|\equiv B\xleftrightarrow{g_B}S}{B|\equiv S|\sim\{T_a(x),ID_A,ID_B,F_B\}}$

According to $A_3$, $D_{14}$ and fresh conjuncatenation rule, we derive:

$goal_5$. $\frac{B|\equiv ID_B,B|\equiv S|\sim\{T_a(x),ID_A,ID_B,F_B\}}{B|\equiv\{ID_A\}}$

According to $V_A$, we collect:

$D_{15}$. $B\triangleleft(ID_A,SK)_{A\xleftrightarrow{SK}B}$

According to $A_{15}$, $goal_4$ and message-meaning rule, we attain:

$D_{16}$. $\frac{B\triangleleft(ID_A,A\xleftrightarrow{SK}B)_{SK},B|\equiv A\xleftrightarrow{SK}B}{B|\equiv A|\sim\{A\xleftrightarrow{SK}B,ID_A\}}$

According to $goal_5$, $D_{16}$ and nonce-verification rule, we get:

$goal_6$. $\frac{B|\equiv ID_A,B|\equiv A|\sim ID_A}{B|\equiv A|\equiv ID_A}$

According to $goal_4$, $goal_5$ and nonce-verification rule, we get:

$goal_7$. $\frac{B|\equiv A|\sim A\xleftrightarrow{SK}B,B|\equiv A\xleftrightarrow{SK}B}{B|\equiv A|\equiv A\xleftrightarrow{SK}B}$

## 6.3 Informal security analysis

In this part, we demonstrate the strong ability of the proposed scheme. Specifically, we will show that the proposed scheme is secure against the loopholes which found in the scheme of Xie et al. Besides, the proposed scheme also provide other common security features. To facilitate the discussion, we also adopt the attack model proposed by Xu et al. [35], that is, an adversary can completely monitor the open communication channel, thus inserting, deleting, and modifying any messages among correspondents.

**6.3.1 User anonymity.** We employ symmetric cryptography to safeguard user identity. Specifically, the identities $\{ID_A, ID_B\}$ are contained only in $C_A$, $R_{AS}$ or $C_B$, $G_B$ and $R_{BS}$ in the form of ciphtertext, where $C_A = E_{K_{AS}}(ID_A, ID_B, F_A)$, $R_{AS} = E_{K_{AS}}(T_{S1}, T_b(x), Z_{AS})$, $Z_{AS} = h(ID_A, ID_B, T_b(x), T_{S_1}(T_a(x)))$, $C_B = E_{g_B}(T_a(x), h(T_a(x), T_{g_B}(ID_B))$, $G_B = E_{K_{BS}}(ID_B, H_B)$, $R_{BS} = E_{K_{BS}}(T_{S2}, T_a(x), Z_{BS})$, $Z_{BS} = h(ID_A, ID_B, T_a(x))$, $K_{AS} = T_a(T_k(x))$, $g_{A(B)} = h_1(pw_{A(B)}, r_{A(B)})$. From the above we can see that both the identities of $A$ and $B$ are protected by the server's public key, chaotic-maps, hash function and symmetric cryptographic operations. Besides, used parameters include secret keys and random numbers are not exposed in the public channel. For example, suppose an adversary $\mathbb{U}$ eavesdrops the message $C_A$ and he plans to derive the identity of $A$. He first needs to know $K_{AS} = T_a(T_k(x))$. To obtain $T_a(x)$ from intercepted $H_A = T_a(x) \oplus T_r(x)$, the shared secret key $r$ is needed. In general, it is hard to derive from the transmitted messages. Our proposed scheme is therefore secure from trace attack.

**6.3.2 Avoidance of insider attack.** In the registration phase of our proposed scheme, $A$ and $B$ send $g_A = h_1(pw_A, r_A)$ or $g_B = h_1(pw_B, r_B)$ to the server $S$, respectively. When $S$ receiving

the registration request, he cannot retrieve the cleartext password $pw_A$ or $pw_B$ owing to the unawareness of the random numbers $r_A$ and $r_B$. Therefore, the proposed scheme can protect against the insider attack.

**6.3.3 Avoidance of off-line password guessing attack.** $\mathbb{U}$ intercepts all the communicated messages $\{C_A, H_A, C_B, P_B, G_B, R_{AS}, R_{BS}\}$, he still cannot derive password of user $B$. Assume that $\mathbb{U}$ steals the stored information $\{VPW_A\}$ or $\{VPW_B\}$, where $VPW_{A(B)} = h_1(pw_{A(B)}, r_{A(B)}) \oplus h_1(ID_{A(B)}, k)$. Even if the secret key $k$ of $S$ is compromised, $\mathbb{U}$ also requires the random number $r_{A(B)}$. In addition, the identity of $A$ or $B$ is also needed. This point has been ensured by user anonymity. This means the off-line password guessing attack is not able to come true in our scheme.

**6.3.4 Avoidance of user impersonation attack.** By virtue of being discussed in the previous subsection, $\mathbb{U}$ is not possible to guess the correct password, let alone masquerade as a legal user to cheat the services provided by the server $S$. Once $\mathbb{U}$ fabricates the password and sends the forged message $\{C_A\}$ or $\{P_B\}$ to the server $S$. After receiving the message, $S$ will decrypt $C_A$ by using its own private key $k$. It is clear that $S$ will detect the attack from user by checking the correctness of $F_A$ or $H_B$ by using its own computed values $g_A = h_1(pw_A, r_A) = VPW_A \oplus h_1(ID_A, k)$ or $g_B = h_1(pw_B, r_B) = VPW_B \oplus h_1(ID_B, k)$. Therefore, $\mathbb{U}$ is also impossible to launch the user impersonation attack.

**6.3.5 Avoidance of man-in-the-middle attack.** Assume that $\mathbb{U}$ intercepts the login message $\{C_A = E_{K_{AS}}(ID_A, ID_B, T_a(x), F_A)\}$ and attempts to modify it. However, he has no way to know the shared symmetric key $K_{AS}$ between $A$ and $S$. Without the important key, he is not possible to decrypt it. Similarly, if $\mathbb{U}$ eavesdrops the message $C_B = E_{g_B}(T_a(x), F_B, ID_A, ID_B)$ and plans to forge it. He also face an embarrassed reality without knowledge of the shared symmetric key $g_B$. Therefore, the proposed scheme protects against the man-in-the middle attack. This point will be verified by the simulation result later.

**6.3.6 The session key perfect forward secrecy.** The session key $SK = T_a(T_b(x))$, where $T_a(x)$ and $T_b(x)$ are not directly transmitted in the public channel. On the one side, $T_a(x)$ and $T_b(x)$ are encrypted with the symmetric cryptographic technology or the Chebyshev polynomials, where the symmetric key is $g_B$ and chaotic map is $T_r(x)$. The security of symmetric key has been demonstrated in the previous subsection. On the other side, assume that $\mathbb{U}$ has the secret key of $S$ and the stored information $\{VPW_A\}$ or $\{VPW_B\}$. In this case, it is an impossible task for $\mathbb{U}$ to attempt to derive $g_A$ or $g_B$ due to the unknown of the identity $A$ or $B$. In order to know the identity, which goes back to this discussion about user anonymity. Therefore, the proposed scheme is able to provide the session key perfect forward secrecy.

**6.3.7 Mutual authentication.** $A$ sent the message $\{C_A, H_A\}$ to $S$, where $C_A = E_{K_{AS}}(ID_A, ID_B, F_A)$, $F_A = h(ID_A, ID_B, T_a(x), g_A)$ and $H_A = T_a(x) \oplus T_r(x)$. Upon receiving the message, $S$ derives $T_a(x)$ using the shared secret key $r$ and then decrypts $C_A$ to get $\{ID_A, ID_B, F_A\}$ using its private key $k$. Next, $S$ computes $h(ID_A, ID_B, T_a(x), VPW_A \oplus h_1(ID_A, k))$ and checks whether it is equal to the decrypted from $C_A$. If it is correct, $A$ is authenticated. The validness of $F_B$ which is decrypted from $C_B$ to verify the legitimacy of $S$. And the correctness of $H_B$ which is decrypted from $G_B$ to validate the legalization of $B$. Similarly, $A$ authenticates $S$ by checking the verification of $Z_{AS}$ decrypted from $R_{AS}$. Finally, the authentication between $A$ and $B$ are gone through the correctness of $V_A$ and $V_B$.

## 6.4 Formal validation of the proposed scheme using AVISPA software

In this part, we simulate the proposed scheme using the commonly used AVISPA (Automated Validation of Internet Security Protocols and Applications) toolkit [30–31] to validate the

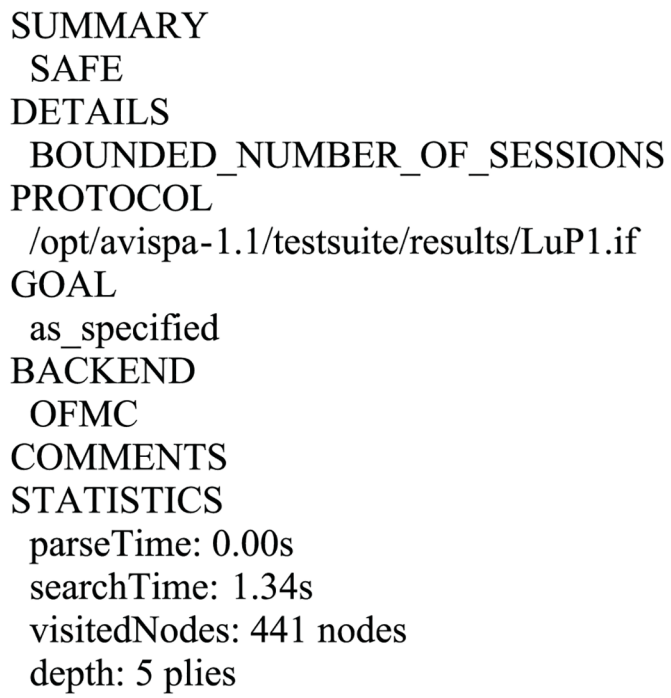


**Fig 3. Simulation result for the OFMC.**

doi:10.1371/journal.pone.0153870.g003

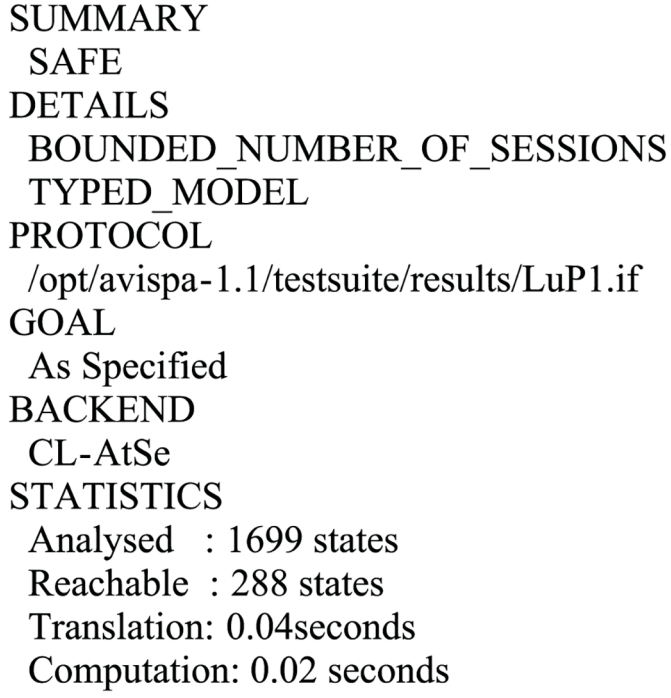


**Fig 4. Simulation result for the CL-AtSe.**

doi:10.1371/journal.pone.0153870.g004

**Table 3. Performance comparison.**

| | Ours | Xie et al. [28] | Chou et al. [2] | He-Wang [4] | Nam et al. [9] |
|---|---|---|---|---|---|
| User | $3T_{cp} + 4T_h + 4T_h$ | $3T_{cp} + 3T_h$ | $3T_{pm} + 2T_h$ | $3T_{pm} + 7T_h$ | $3T_{pm} + 1T_S + 4T_h + 1T_m$ |
| Second party | $2T_{cp} + 3T_S + 5T_h$ | $3T_{cp} + 3T_h$ | $3T_{pm} + 2T_h$ | $2T_{pm} + 5T_h$ | $1T_m + 1T_S + 1T_h$ |
| Third patry | $5T_{cp} + 5T_S + 7T_h$ | $4T_{cp} + 6T_h$ | $3T_{pm} + 8T_h$ | $2T_{pm} + 9T_h$ | $1T_m + 1T_S + 2T_h$ |
| Communication rounds | 6 | 5 | 6 | 6 | 4 |

doi:10.1371/journal.pone.0153870.t003

passive and active attacks including man-in-the-middle and replay attacks that has been withstand. AVISPA integrates four backends: (i)OFMC; (ii)CL-AtSe; (iii)SATMC; (iv)TA4SP for the analysis of security schemes and implements in the role based HLPSL (High Level Protocol Specification Language). After execution through the OFMC and CL-AtSe backends, the results (Figs 3–4) clearly verify that the proposed scheme is secure under the Dolev-Yao model. The specifications for the roles for $U_A$(S1 Fig), $U_B$(S2 Fig), $S$(S3 Fig), the Session(S4 Fig) and the Environment(S5 Fig) in HLPSL are provided in Supporting Information.

## 7 Performance comparisons

In this section, we evaluate the performance of our proposed scheme and make comparisons with the recent chaotic-maps based schemes [28, 2, 4, 9]. The following types of computation costs will be used to evaluate the feasibility of the attack in terms of its computational complexity.

$T_{cp}$: time for computing Chebyshev polynomial;
$T_h$: time for computing hash function;
$T_S$: time for performing symmetric cryptography;
$T_{pm}$: time for computing point multiplication;
$T_m$: time for performing MAC generation/verification.

Table 3 shows the computation overhead comparisons of our proposed scheme and some recent three-party schemes. We mainly address on the consumptions of authentication and session key agreement due to these are the principal parts of an authentication scheme and should be performed for each session. In Table 3, it is obvious that our improvements need a sight higher computational cost than Xie et al.'s scheme while consuming less than others, where the time for performing a point multiplication is much more expensive than the light-weight cryptographic operations, and a symmetric encryption/decryption operation is almost as many costs as a hash function [34]. However, it is worth an additional chaotic-maps and

**Table 4. Security properties comparison.**

| | Ours | Xie et al. [28] | Chou et al. [2] | He-Wang [4] | Nam et al. [9] |
|---|---|---|---|---|---|
| Session key perfect forward secrecy | Yes | No | Yes | Yes | Yes |
| Mutual authentication | Yes | Yes | Yes | Yes | Yes |
| User anonymity | Yes | No | No | Yes | Yes |
| Insider attack | Yes | Yes | - | Yes | No |
| Off-line password guessing attack | Yes | No | - | Yes | No |
| Impersonation attack | Yes | No | No | No | No |

doi:10.1371/journal.pone.0153870.t004

symmetric cryptographic operations to achieve strong security and better functionality attributes compared with Xie et al.'s scheme.

Table 4 lists the security comparisons among our proposed scheme and some recent three-party schemes. It demonstrates that our scheme has many excellent features and is more secure than other recent three-party schemes.

## 8 Conclusion and future work

This paper discussed the security of the recent scheme proposed by Xie et al. We showed that the recent scheme had several security pitfalls. Besides, we found that it was insecure only using hash function. To mend all the identified weaknesses, we then presented an enhancement which utilized asymmetric cryptography to conceal the user's identity. We demonstrated that the improvements not only was immune to the loopholes found in Xie et al.'s scheme but also was secure other common attacks. We also performed the BAN logic test and confirmed the mutual authentication is achieved in our scheme. The formal security analysis also shows our scheme supports more security properties. The performance comparison between the recent schemes and the proposed scheme showed our improvements was more secure than other schemes. Actually, it is not negligible that based on chaotic maps has inevitable restrictions in some applications and an ID-based solution is a better one. Therefore, our near future work is to address to design a robust ID-based authenticated key agreement scheme.

## Supporting Information

**S1 Fig. Role specification of $U_A$.**
(EPS)

**S2 Fig. Role specification of $U_B$.**
(EPS)

**S3 Fig. Role specification of *S*.**
(EPS)

**S4 Fig. Role specification of the Session.**
(EPS)

**S5 Fig. Role specification of the Environment.**
(EPS)

## Author Contributions

Conceived and designed the experiments: YRL LXL HZ YXY. Performed the experiments: YRL LXL HZ YXY. Analyzed the data: YRL LXL HZ YXY. Contributed reagents/materials/analysis tools: YRL LXL HZ YXY. Wrote the paper: YRL LXL HZ YXY.

## References

1. Alomair B, Poovendran R. Efficient Authentication for Mobile and Pervasive Computing. IEEE Transactions on Mobile Computing. 2014; 13(3): 469–481. doi: 10.1109/TMC.2012.252
2. Chou CH, Tsai KY, Lu CF. Two ID-based authenticated schemes with key agreement for mobile environments. Journal of Supercomputing. 2013; 66(2):973–88. doi: 10.1007/s11227-013-0962-3
3. Guo LK, Zhang C, Sun JY, Fang YG. A privacy-preserving attribute-based authentication system for mobile health networks. IEEE Transaction on Mobile Computing. 2014; 13(9): 1927–1941. doi: 10.1109/TMC.2013.84
4. He DB, Wang D. Robust Biometrics-Based Authentication Scheme for Multiserver Environment. IEEE Systems Journal.

5. Islam SK, Khan MK. Provably secure and pairing-free identity-based handover authentication protocol for wireless mobile networks. International Journal Communication Systems. 2014. doi: 10.1002/dac.2847
6. Kilinc H, Yanik T. A Survey of SIP authentication and key agreement schemes. IEEE Communications Surveys and Tutorials. 2014; 16(2): 1005–1023. doi: 10.1109/SURV.2013.091513.00050
7. Liu JW, Zhang ZH, Chen XF, Kwak KS. Certificateless remote anonymous authentication schemes for wireless body area networks. IEEE Transactions on Parallel and Distributed Systems. 2014; 25(2): 332–342. doi: 10.1109/TPDS.2013.145
8. Lu RX, Lin XD, Zhu HJ, Liang XH, Shen XM. BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2012; 23(1): 32–43. doi: 10.1109/TPDS.2011.95
9. Nam J, Choo KKR, Han S, Kim M, Paik J, Won D. Efficient and anonymous two-factor user authentication in wireless sensor networks: achieving user anonymity with lightweight sensor computation. PLoS ONE. 2015; 10(4): e0116709. doi: 10.1371/journal.pone.0116709 PMID: 25849359
10. Turkanović M, Brumen B, Hölbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Networks. 2014; 20: 96–112. doi: 10.1016/j.adhoc.2014.03.009
11. Xue KP, Hong PL. Security improvement on an anonymous key agreement protocol based on chaotic maps. Communication in Nonlinear Science and Numerical Simulation. 2012; 17(7): 2969–2977. doi: 10.1016/j.cnsns.2011.11.025
12. Khan M, Shah T, Mahmood H, Gondal MA. An efficient method for the construction of block cipher with multichaotic systems. Nonlinear Dynamics. 2013; 71(3): 489–492. doi: 10.1007/s11071-012-0675-9
13. Lian SG, Sun JS, Wang ZQ. A block cipher based on a suitable use of the chaotic standard map. Chaos Solitons Fractals. 2005; 26: 117–129. doi: 10.1016/j.chaos.2004.11.096
14. ökaynak F, Yavuz S. Designing chaotic S-boxes based on time-delay chaotic system. Nonlinear Dynamics. 2013; 74(3): 551–557. doi: 10.1007/s11071-013-0987-4
15. Chain K, Kuo WC. A new digital signature scheme based on chaotic maps. Nonlinear Dynamics. 2013; 74(4): 1003–1012. doi: 10.1007/s11071-013-1018-1
16. Deng SJ, Li YT, Xiao D. Analysis and improvement of a chaos-based Hash function construction. Communication in Nonlinear Science and Numerical Simulation. 2010; 15(5): 1338–1347. doi: 10.1016/j.cnsns.2009.05.065
17. Lee TF. Enhancing the security of password authenticated key agreement protocols based on chaotic maps. Information Sciences. 2015; 290: 63–71. doi: 10.1016/j.ins.2014.08.041
18. Lin HY. Improved chaotic maps-based password-authenticated key agreement using smart cards. Communication in Nonlinear Science and Numerical Simulation. 2015; 20(2): 482–488. doi: 10.1016/j.cnsns.2014.05.027
19. Li X, Niu JW, Kumari S, Khan MK, Liao JG, Liang W. Design and analysis of a chaotic maps-based three-party authenticated key agreement protocol. Nonlinear Dynamics.
20. Xiao D, Liao XF, Deng SJ. A novel key agreement protocol based on chaotic maps. Information Sciences. 2007; 177: 1136–1142. doi: 10.1016/j.ins.2006.07.026
21. Wang XY, Gao YF. A switch-modulated method for chaos digital secure communication based on user-defined protocol. Communication in Nonlinear Science and Numerical Simulation. 2010; 15(1): 99–104. doi: 10.1016/j.cnsns.2008.05.002
22. Bergamo P, D'Arco P, De Santis A, Kocarev L. Security of public-key cryptosystems based on Chebyshev polynomials. IEEE Transactions Circuits and Systems. 2005; 52: 1382–1393. doi: 10.1109/TCSI.2005.851701
23. Wang XY, Zhao JF. An improved key agreement protocol based on chaos. Communication in Nonlinear Science and Numerical Simulation. 2010; 15(12): 4052–4057. doi: 10.1016/j.cnsns.2010.02.014
24. Yoon EJ, Jeon IS. An efficient and secure DiffieCHellman key agreement protocol based on Chebyshev chaotic map. Communication in Nonlinear Science and Numerical Simulation. 2011; 16(6): 2383–2389. doi: 10.1016/j.cnsns.2010.09.021
25. Lee CC, Li CT, Hsu CW. A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps. Nonlinear Dynamics. 2013; 73(1-2): 125–132. doi: 10.1007/s11071-013-0772-4
26. Hu XX, Zhang ZF. Cryptanalysis and enhancement of a chaotic maps-based three-party password authenticated key exchange protocol. Nonlinear Dynamics. 2014. doi: 10.1007/s11071-014-1515-x

27. Farash MS, Attari MA. An efficient and provably secure three-party password-based authenticated key exchange protocol based on Chebyshev chaotic maps. Nonlinear Dynamics. 2014; 77(1-2): 399–411. doi: 10.1007/s11071-014-1304-6

28. Xie Q, Hu B, Wu T. Improvement of a chaotic maps-based three-party password-authenticated key exchange protocol without using server's public key and smart card. Nonlinear Dynamics. 2015; 79: 2345–2358. doi: 10.1007/s11071-014-1816-0

29. Wang D, He DB, Wang P, Chu CH. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Transactions on Dependable and Secure Computing. 2014; 99.

30. AVISPA, Automated validation of internet security protocols and applications. http://www.avispa-project.org/ (accessed October 2014).

31. AVISPA, AVISPA web tool. http://www.avispa-project.org/webinterface/expert.php/ (accessed on October 2014).

32. Burrows M, Abadi M, Needham RM. A logic of authentication. ACM Transactions on Computer Systems. 1990; 8(1): 18–36. doi: 10.1145/77648.77649

33. Mason JC, Handscomb DC. Chebyshev Polynomials. Chapman & Hall/CRC Press, 2003, London

34. Zhang LH. Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons & Fractals. 2008; 37(3): 669–674. doi: 10.1016/j.chaos.2006.09.047

35. Xu J, Zhu WT, Feng DG. An improved smart card based password authentication scheme with provable security. Computer Standards & Interfaces. 2009; 31(4): 723–728. doi: 10.1016/j.csi.2008.09.006

36. Zhu F, Carpenter S, Kulkarni A. Understanding identity exposure in pervasive computing environments. Pervasive and Mobile. Computing. 2012; 8(5): 777–794.

37. Advanced Encryption Standard, FIPS PUB 197, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf Accessed on November 2010