RESEARCH ARTICLE

Enhanced smartcard-based password-authenticated key agreement using extended chaotic maps

Tian-Fu Lee[1,2], **Chia-Hung Hsiao**[1], **Shi-Han Hwang**[1], **Tsung-Hung Lin**[3]*

1 Department of Medical Informatics, Tzu Chi University, Hualien, Taiwan, ROC, **2** Department of Medical Informatics, Institute of Medical Sciences, Tzu Chi University, Hualien, Taiwan, ROC, **3** Department of Computer Science and Information Engineering, National Chin-Yi University of Technology, Taichung, Taiwan, ROC

* duke@ncut.edu.tw

Abstract

A smartcard based password-authenticated key agreement scheme enables a legal user to log in to a remote authentication server and access remote services through public networks using a weak password and a smart card. Lin recently presented an improved chaotic maps-based password-authenticated key agreement scheme that used smartcards to eliminate the weaknesses of the scheme of Guo and Chang, which does not provide strong user anonymity and violates session key security. However, the improved scheme of Lin does not exhibit the freshness property and the validity of messages so it still fails to withstand denial-of-service and privileged-insider attacks. Additionally, a single malicious participant can predetermine the session key such that the improved scheme does not exhibit the contributory property of key agreements. This investigation discusses these weaknesses and proposes an enhanced smartcard-based password-authenticated key agreement scheme that utilizes extended chaotic maps. The session security of this enhanced scheme is based on the extended chaotic map-based Diffie-Hellman problem, and is proven in the real-or-random and the sequence of games models. Moreover, the enhanced scheme ensures the freshness of communicating messages by appending timestamps, and thereby avoids the weaknesses in previous schemes.

Citation: Lee T-F, Hsiao C-H, Hwang S-H, Lin T-H (2017) Enhanced smartcard-based password-authenticated key agreement using extended chaotic maps. PLoS ONE 12(7): e0181744. https://doi.org/10.1371/journal.pone.0181744

Editor: Muhammad Khurram Khan, King Saud University, SAUDI ARABIA

Received: December 1, 2016

Accepted: July 6, 2017

Published: July 31, 2017

Data Availability Statement: All relevant data are within the paper.

Funding: This research was supported by Ministry of Science and Technology under the grants MOST 105-2221-E-320-003 and Tzu Chi University under the grants TCRPP105004.

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

Introduction

Smartcard-based password-authenticated key agreement supports a communicating platform that enables legitimate users to log in to, and access, systems conveniently and securely over an open network. In a smartcard-based password-authenticated key agreement system, users register their identities and passwords with a trusted server. The trusted server is then responsible for generating authentication information and secrets of users and providing smartcards to legitimate users over a secure and authenticated channel. Finally, legitimate users conveniently and securely log in and enjoy remote services using their weak passwords and smartcards [1–8].

Recently, Chen et al. [9] developed a smartcard-based password authentication scheme based on the Discrete Logarithm problem and claimed that their scheme can withstand potential attacks. However, Jiang et al. [10] stated that their scheme is insecure against offline password guessing attacks, and presented an improved authentication scheme based on the Diffie-Hellman problem to solve the security flaw of the scheme of Chen et al. and to keep efficiency. In 2013, Wen [11] designed an enhanced user authentication scheme based on the quadratic residue problem [12, 13] to overcome the weaknesses of previous schemes [14, 7]. However, Islam et al. [15] pointed out the security weaknesses of Wen's scheme, and showed that their scheme cannot resist some possible attacks, including impersonation and privileged-insider attacks. Islam et al. also presented a new user authentication scheme based on the quadratic residue problem for the application of integrated EPR information system. Additionally, Li [16] developed a two-factor authentication scheme with user anonymity based on elliptic curve cryptography. But, Wang et al. [17] showed that his scheme may suffer from smart-card loss and de-synchronization attacks, and provided a better understanding of the underlying evaluation metric for anonymous two-factor schemes. These schemes [9–16] are developed by using public-key cryptosystem to have higher security. Nevertheless, time-consuming modular exponential computations are required so that these schemes are inefficient in computation.

Since cryptography that uses chaotic maps was demonstrated to exhibit the semi-group property and cryptosystems that use chaotic map operations were shown to be more efficient than cryptosystems that use modular exponential computations and scalar multiplications on the elliptic curve [18–20], many chaotic map-based authentication approaches [21–29] have been developed. However, in 2005, Bergamo et al. [20] showed the security weakness of public-key cryptosystems that are based on Chebyshev polynomials, and that therefore some authentication schemes have security limitations and lack the contributory property of key agreements. In 2008, Zhang [30] enhanced the Chebyshev polynomials to eliminate this security weakness. Zhang also demonstrated that the enhanced Chebyshev polynomials support the semi-group property and the commutivity under composition on interval $(-\infty,+\infty)$. Additionally, extended Chebyshev chaotic maps are utilized in solving the extended chaotic map-based discrete logarithm and Diffie-Hellman problems [30–32]. In 2013, Guo and Change [33] were the first to present a novel chaotic map-based password-authenticated key agreement scheme using smartcards to increase efficiency. In 2014, Lin [34] developed a mobile user authentication scheme using dynamic identity and chaotic map, and declared that their scheme offers mutual authentication, session key security and user anonymity, and resilience against possible attacks. Later, Islam et al. [35] stated that Lin's scheme had some design flaws and limitations, and cannot resist user impersonation attack. Islam et al. also presented a provably secure scheme using extended chaotic map to solve the weaknesses of Lin's scheme. Additionally, Islam [36] in 2014 proposed a dynamic identity-based three-factor scheme using extended chaotic maps three-factor authentication to offer more security properties. However, Jiang et al. [37] pointed out the processing flaws of Islam's scheme, and showed that his scheme is also vulnerable to some potential attacks. To solve these limitations, Jiang et al. also presented a more secure robust three-factor authentication scheme. Subsequently, Hao et al. [38], Lee [39] and Lin [40] noted that the scheme developed by Guo and Chang had weaknesses that included an inability to ensure strong user anonymity, inefficiency in hiding double secrets, and violation of both the session key security and the contributory property of key agreements. Lin [41] also proposed an improved scheme to eliminate the weaknesses in the scheme of Guo and Chang. However, Lin's scheme also failed to withstand some attacks and to meet all security requirements. In the password change phase of that scheme, the server does not confirm the freshness of the messages from the users, and the smartcard does not verify the updated data from the server, so the scheme fails efficiently to protect against replay and denial of service attacks. Additionally, in the authenticated key exchange phase, a malicious server can control the value of a session key by the method that was introduced by Bergamo et al. [20] so Lin's scheme also the fails to provide the contributory property of key agreements. Moreover, in that scheme, every legitimate user can derive session key that is shared between another user and the server by the method of Bergamo et al. [20]. A malicious user can even forge validate request messages and to impersonate other users, so Lin's scheme fails to withstand privileged-insider attacks.

To address the weaknesses of Lin's scheme, this work develops a more secure and efficient smartcard-based password-authenticated key agreement scheme that is based on the schemes of both Guo and Chang [33] and Lin [40]. The enhanced scheme constructs the session key using extended chaotic maps, and so the session key of security is based on the extended chaotic map-based Diffie-Hellman problem. The enhanced scheme eliminates the security weakness that was identified by Bergamo et al.; ensures the contributory property of key agreements, and withstands attacks by privileged insiders. Moreover, in the password change phase of the enhanced scheme, the messages are guaranteed to exhibit freshness property owing to the appending of timestamps, so the enhanced scheme withstands replay and denial-of-service attacks. Therefore, the proposed scheme does not have any of the weaknesses of previous schemes.

The remainder of this article is organized as follows. Section 2 describes the notation and the definitions used in this paper. Section 3 reviews the authenticated key agreement scheme of Lin and elucidates its weaknesses. Section 4 presents the enhanced smartcard-based password-authenticated key agreement that uses extended chaotic maps. Section 5 analyzes the security and performance of the enhanced scheme. Finally, Section 6 draws conclusions.

Preliminaries

This section presents the notation and the definitions that are used herein this work.

Notation

The followings detail the notation that is utilized herein.

U,	The user;
ID,	The identity of U;
PW,	The password of U;
S,	The remote server, which U is registered in;
T_1,	The user's time stamp;
T_2,	The server's time stamp;
ΔT,	The time threshold;
$E_k(\cdot)/D_k(\cdot)$,	A secure symmetric en/decryption algorithm with the secret key k;
λ,	The session key generated between U and S;
l,	The secure parameter size;
$h(\cdot)$,	A one-way hash function and $h:\{0,1\}^*\to\{0,1\}^l$;
$H(.)$,	A one-way hash function and $H:[-1,1]\to\{0,1\}^l$;
$A\to B : M$,	A sends message M to B through a common channel.;
$M_1\|\|M_2$,	Message M_1 concatenates to message M_2.

Definition

Session key security (AKE security). This definition defines that an adversary $\mathcal{A}$ fails to effectively distinguish between two messages from a challenger $\mathcal{C}$. One message is encrypted with the real session key λ and the other one is encrypted with a random string λ' via an unbiased coin c. $\mathcal{A}$ selects one message and sends it to $\mathcal{C}$. Then $\mathcal{C}$ flips an unbiased coin $c \in \{0,1\}$ and decides to return the message encrypted with λ if $c = 1$ or encrypted with λ' if $c = 0$. $\mathcal{A}$ intends to correctly guess the value of the hidden bit. The advantage that an adversary $\mathcal{A}$ violates the indistinguishability of a scheme **P** is denoted as $Adv_{P}^{ake}(\mathcal{A})$. The scheme **P** is AKE-secure if $Adv_{P}^{ake}(\mathcal{A})$ is negligible. [41–44]

Chebyshev chaotic maps. The Chebyshev polynomial $T_n(x)$ is a polynomial in x of degree n and is defined by the following relation:

$$T_n(x) = \cos n\theta, \text{ where } x = \cos\theta.$$

The recurrence relation of $T_n(x)$ is defined as:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x),$$

for any $n \geq 2$, with $T_0(x) = 1$ and $T_1(x) = x$.

The Chebyshev polynomial satisfies the semi-group property and satisfies:

$$T_r(T_s(x)) = T_{sr}(x) = T_s(T_r(x)),$$

for $s,r \in Z^+$.

The Chebyshev polynomial satisfies chaotic property: When $n > 1$, Chebyshev polynomial map T_n: $[-1,1] \rightarrow [-1,1]$ of degree n is a chaotic map with its invariant density

$$f^*(x) = 1/(\pi\sqrt{1-x^2}),$$

for Lyaounov exponent $\ln n > 0$.[29–32]

Zhang [30] in 2008 enhanced the Chebyshev polynomials for avoiding the security weakness showed by Bergamo et al. [20] in 2005, and also proved that the enhanced Chebyshev polynomials still satisfy the semi-group property and the commutative under composition on interval $(-\infty,+\infty)$. That is,

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

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

$$T_r(T_s(x)) \equiv T_{rs}(x) \equiv T_s(T_r(x)) \bmod p$$

holds.

The enhanced Chebyshev chaotic maps also exhibit the Discrete Logarithm and Diffie-Hellman problems [30–32], which are described as follows.

Extended chaotic map-based discrete logarithm problem (DLP). Given x, y and p, finding the integer r satisfying $y = T_r(x) \bmod p$ is computationally infeasible. The advantage that an adversary solves the extended chaotic map-based DLP is denoted as Adv^{dlp}, and thus is negligible.

Extended chaotic map-based computational Diffie-Hellman problem (CDHP). Given $T_r(x)$, $T_s(x)$, $T(\cdot)$, x and p, where $r, s \geq 2$, $x \in (-\infty,+\infty)$ and p is a large prime number, calculating

$$T_{rs}(x) \equiv T_r(T_s(x)) \equiv T_s(T_r(x)) \bmod p$$

is computationally infeasible. The advantage that an adversary solves the extended chaotic map-based CDHP is denoted as Adv^{cdh}, and thus is negligible.

Extended chaotic map-based decisional Diffie-Hellman problem (DDHP). Given $T_r(x)$, $T_s(x)$, $T_z(x)$, $T(\cdot)$, x and p, deciding whether

$$T_{rs}(x) \equiv T_z(x) \bmod p$$

holds or not is computationally infeasible. The advantage that an adversary solves the extended chaotic map-based DDHP is denoted as Adv^{ddh}, and thus is negligible.

The authenticated key agreement scheme of Lin and its limitations

The authenticated key agreement scheme of Lin

Lin [40] recently presented an improved chaotic maps-based password authenticated key agreement scheme using smartcards. The four phases of the improved scheme are system initialization, user registration, authenticated key exchange and password change phases, which are discussed further below.

System initialization phase. The remote server S setups the system's parameters by performing the following steps:

1. S generates a random number r as the private key and a random number $x \in [-1,+1]$.
2. S chooses a master key s, a secure symmetric en/decryption algorithm $E_k(\cdot)/D_k(\cdot)$ and a one-way hash function $h(\cdot)$.

Registration phase. A user U registers his/her identity and password by performing the following steps.

1. U chooses his identity ID, password PW and a random number t and sends ID and $H = h(PW \parallel t)$ to S via a secure channel.
2. S verifies ID and computes $R = E_s(ID \parallel H)$ and $D = H \oplus (x \parallel T_r(x))$ by using its master key s.
3. S stores $(R,h(\cdot),E_k(\cdot),D)$ into a smartcard SC, and issue SC to U through a secure channel.
4. U inserts t into it and finishes the registration.

Authenticated key exchange phase. In this phase, as shown in Fig 1, U and S authenticate each other by performing the following steps.

1. U inserts his SC into a card reader and inputs PW. Then SC generates a random number j, computes $T_j(x)$, $(x \parallel T_r(x)) = h(PW \parallel t) \oplus D$, $v = T_j(T_r(x))$, $Q = h(ID \parallel H)$, $E_v(Q \parallel R \parallel T_1)$, where T_1 is the current timestamp, and sends $M_1 = \{T_j(x),E_v(Q \parallel R \parallel T_1)\}$ to S.
2. On receiving M_1, S computes $v = T_r(T_j(x))$, obtains $(Q \parallel R \parallel T_1)$ by decrypting $E_v(Q \parallel R \parallel T_1)$ with v, and checks T_1. If unsuccessful, S rejects this service request. Otherwise, S obtains $(ID' \parallel H')$ by decrypting R with its master key s and checks whether $Q' = ?h(ID' \parallel H')$. If unsuccessful, S rejects this service request. Otherwise, S generates a random number j', and computes $T_{j'}(x)$ and $E_v(T_{j'}(x) \parallel h(ID \parallel T_2) \parallel T_2)$, where T_2 is the current timestamp, and sends $E_v(T_{j'}(x) \parallel h(ID \parallel T_2) \parallel T_2)$ to SC.
3. On receiving $E_v(T_{j'}(x) \parallel h(ID \parallel T_2) \parallel T_2)$, SC obtains $(T_{j'}(x) \parallel h'(ID \parallel T_2) \parallel T_2)$ by decrypting $E_v(T_{j'}(x) \parallel h(ID \parallel T_2) \parallel T_2)$ with v and checks T_2. If unsuccessful, the SC aborts this service request. Otherwise, SC checks whether $h'(ID \parallel T_2) = ?h(ID \parallel T_2)$. If unsuccessful, SC aborts this service request. Finally, both U and S share a common session key $\lambda = T_{j'}(T_j(x)) = T_j(T_{j'}(x))$.

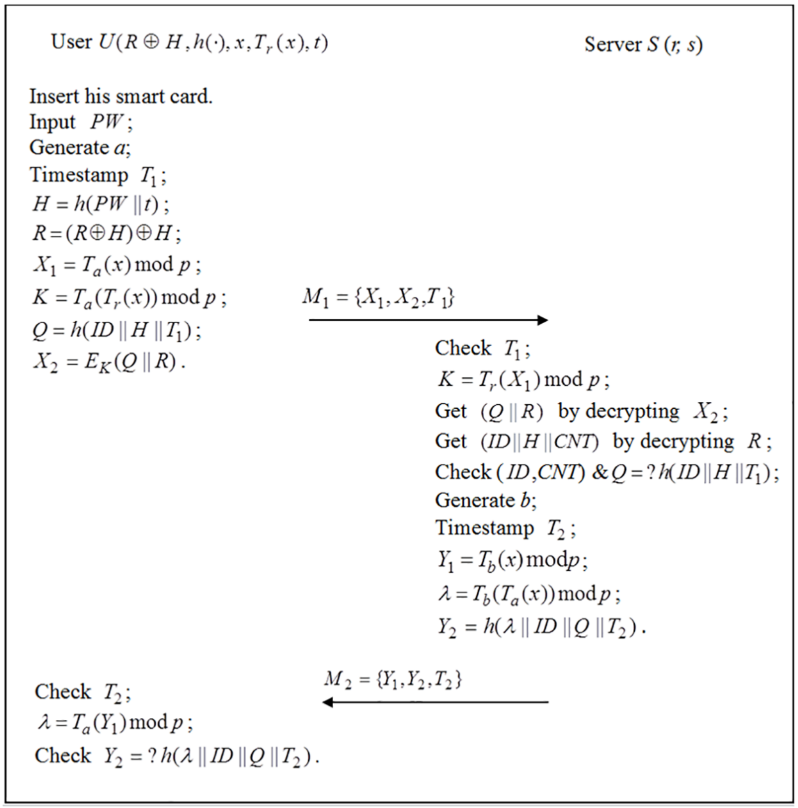

User $U(R \oplus H, h(\cdot), x, T_r(x), t)$
Server S (r; s)
Insert his smart card.
Input PW;
Generate a;
Timestamp T_1;
$H = h(PW \| t)$;
$R = (R \oplus H) \oplus H$;
$X_1 = T_a(x) \bmod p$;
$K = T_a(T_r(x)) \bmod p$;
$Q = h(ID \| H \| T_1)$;
$X_2 = E_K(Q \| R)$.
$M_1 = \{X_1, X_2, T_1\}$
Check T_1;
$K = T_r(X_1) \bmod p$;
Get $(Q \| R)$ by decrypting X_2;
Get $(ID \| H \| CNT)$ by decrypting R;
Check (ID, CNT) & $Q = ?\, h(ID \| H \| T_1)$;
Generate b;
Timestamp T_2;
$Y_1 = T_b(x) \mathrm{mod} p$;
$\lambda = T_b(T_a(x)) \bmod p$;
$Y_2 = h(\lambda \| ID \| Q \| T_2)$.
$M_2 = \{Y_1, Y_2, T_2\}$
Check T_2;
$\lambda = T_a(Y_1) \bmod p$;
Check $Y_2 = ?\, h(\lambda \| ID \| Q \| T_2)$.

Fig 1. The authenticated key exchange phase of the enhanced scheme.

https://doi.org/10.1371/journal.pone.0181744.g001

Password change phase. A legal user U inserts his SC into a card reader and inputs the old password PW and a new password PW^* and changes his/her password by performing the following steps.

1. The SC generates a random number i, computes $H' = h(PW \| t)$, $(x \| T_r(x)) = h(PW \| t) \oplus D$, $\eta = T_i(T_r(x))$, $H^* = h(PW^* \| t)$, and sends $(T_i(x), E_\eta(H' \| H^* \| R))$ to S.
2. On receiving $(T_i(x), E_\eta(H' \| H^* \| R))$, S computes $v = T_r(T_i(x))$, obtains $(H^* \| Q \| R)$ by decrypting $E_\eta(H' \| H^* \| R)$ with v and obtains $(ID \| H)$ by decrypting R with s, respectively. Then S checks whether $H' = ?H$ holds or not. If successful, S computes $R^* = E_s(ID \| H^*)$ and sends R^* to SC.
3. After receiving R^*, SC updates R as R^*.

Weaknesses in the authenticated key agreement scheme of Lin

This subsection elucidates the weaknesses of the improved scheme of Lin, which suffers from denial-of-service attacks and privileged-insider attacks, and violation of the contributory property of key agreements.

Suffering from denial-of-service attacks. In the password change phase, the smartcard does not validate the updated data R so an attacker can easily perform a denial-of-service by the following steps.

1. On receiving message ($T_i(x)$,$E_\eta(H'$,H^*,R)) from a user, the server computes $\eta = T_r(T_i(x))$, decrypts $E_\eta(H',H^*,R)$ and $R = E_s(ID \parallel H)$ using η and the server's master key s, respectively, and then checks whether $H' = ?H$.
2. If $H' = H$, then S returns $R^* = E_s(ID \parallel H^*)$ to the smart card. At this time, an attacker intercepts R^* and replaces it with a nonce $\hat{R}$.
3. On receiving message $\hat{R}$, the smartcard does not verify it but updates R as $\hat{R}$. Thereafter, when the user attempts to implement the steps of the authenticated key exchange phase or the password change phase, the failed request message $(T_j(x), E_v(Q, \hat{R}, T_1))$ or $(T_i(x), E_\eta(H', H^*, \hat{R}))$ will be detected by the server because the user does not have the correct R. Thereafter, the server always rejects the service requests made by the user. Therefore, the scheme of Lin is insecure against denial-of-service attacks.

Moreover, in the password change phase, the server does not verify the freshness of messages from the users so an attacker can exhaust computational resources in the server by replaying previous request messages. Possible scenarios are as follows.

1. After the user sends the message ($T_i(x)$, $E_\eta(H',H^*,R)$) to the server, an attacker can copy it and successively re-send it to the server.
2. Upon receiving each message ($T_i(x)$, $E_\eta(H',H^*,R)$) from the attacker, the server computes $\eta = T_r(T_i(x))$, decrypts $E_\eta(H',H^*,R)$ and $R = E_s(ID \parallel H)$, and successfully checks whether $H' = H$. Then, the server computes and returns $R^* = E_s(ID \parallel H^*)$. The server may exhaust computational resources and cannot efficiently prevent denial-of-service attacks since the server does not verify the freshness of these request messages.

Suffering from privileged insider attacks. In Lin's authentication scheme, every legitimate user can derive ($x \parallel T_r(x)$) from his/her smartcard. A malicious user U^* still can derive the session key that is shared between another user U and the server using the method that was introduced by Bergamo et al. [20]. The details are as follows.

1. After the user U sends out the message ($T_j(x)$,$E_v(Q,R,T_1)$), U^* receives $T_j(x)$. By the method of Bergamo *et al.*, U^* possesses x, $T(\cdot)$, $T_r(x)$ and $T_j(x)$, and so can compute an integer solution j^* that satisfies the equation $T_{j^*}(x) = T_j(x)$:

$$j^* = \frac{\arccos(T_j(x)) + 2k\pi}{\arccos(x)} \bigg| k \in Z.$$

2. U^* can compute the secret key $v = T_{j^*}(T_r(x))$ since $T_{j^*}(T_r(x)) = T_r(T_{j^*}(x)) = T_r(T_j(x)) = v$. Then, U^* receives R by decrypting $E_v(Q,R,T_1)$ using v, and can determine whether two request messages came from the same user.
3. After the server returns the message $E_v(T_{j'}(x)$, $h(ID \parallel T_2)$, $T_2)$, U^* receives $T_{j'}(x)$ and so can compute the session key $\lambda = T_{j^*}(T_{j'}(x))$ since $T_{j^*}(T_{j'}(x)) = T_{j'}(T_{j^*}(x)) = T_{j'}(T_j(x)) = \lambda$. Furthermore, U^* can impersonate another user U by forging a request message $(T_{j^*}(x), E_{v^*}(Q, R, T'_1))$, where T'_1 is an acceptable timestamp and $v^* = T_{j^*}(T_r(x))$, since U^* has x, $T_r(x)$, Q and R.

Therefore, Lin's authentication scheme fails to withstand privileged insider attacks since every legitimate user has x and $T_r(x)$, and can derive users' hidden information concerning Q and R.

Lack of the contributory property of key agreements. In the authenticated key exchange phase of the authenticated key agreement scheme of Lin, the malicious server alone can control the value of the session key using the method proposed by Bergamo et al. [20]. The details are as follows.

1. Upon receiving the message from a user, the malicious server S receives $T_j(x)$ and computes an integer solution j^* to the equation $T_{j^*}(x) = T_j(x)$:

$$j^* = \frac{\arccos(T_j(x)) + 2k\pi}{\arccos(x)} \bigg| k \in Z.$$

2. S uses a predetermined value λ_0 to find an integer j′, using

$$j' = \frac{\arccos(\lambda_0) + 2k\pi}{j^* \cdot \arccos(x)} \bigg| k \in Z;$$

   calculates $E_v(T_{j'}(x) \| h(ID \| T_2) \| T_2)$, and sends it to the smart card.

3. Upon receiving the message from S, the smartcard receives $(T_{j'}(x) \| h(ID \| T_2) \| T_2)$ by decrypting $E_v(T_{j'}(x) \| h(ID \| T_2) \| T_2)$; it then computes $T_j(T_{j'}(x))$ as the session key. Therefore, U obtains the session key λ_0 because $T_j(T_{j'}(x)) = T_{j'}(T_j(x)) = T_{j'}(T_{j^*}(x)) = \lambda_0$.

Therefore, Lin's scheme does not support the contributory property of key agreements because the malicious server can control the value of the session key.

Enhanced smartcard-based password-authenticated key agreement scheme

This section elucidates the enhanced smartcard-based password-authenticated key agreement scheme that uses extended chaotic maps. The session key security of the enhanced scheme is based on the extended chaotic map-based Diffie-Hellman problem so one malicious participant cannot alone predetermine the value of the session key. Additionally, malicious users cannot derive the mutually session key that is shared between another user and the server, and they cannot forge validate request messages or impersonate other users. Thus, the enhanced scheme withstands privileged insider attacks. Moreover, in the password change phase of the enhanced scheme, the appending of timestamps guarantees the freshness of messages that are sent from users, and the smartcard can validate the updated data from the server, so the enhanced scheme withstands replay and denial-of-service attacks.

The enhanced scheme consists of five phases, which are system initialization, user registration, authenticated key exchange, password change, and smartcard revocation phases. The system initialization phase is similar to those of Lin's scheme, except that it uses enhanced Chebyshev chaotic maps and the parameter x on interval $(-\infty,+\infty)$, requires a large prime number p for the modular arithmetic, and maintains a smartcard revocation table in the system initialization phases. The registration, authenticated key exchange, password change and smartcard revocation phases are described further below.

Registration phase

A user U registers his/her identity and password to be a legal user by performing the following steps.

1. U chooses his identity ID, password PW and a random number t and sends ID and $H = h(PW \| t)$ to S via a secure channel.
2. S verifies ID and computes $R = E_s(ID \| H \| CNT)$ by using its master key s, where $CNT = 0$ and indicates the revocation times.
3. S stores $(R \oplus H,h(\cdot),E_k(\cdot),x,T_r(x))$ into a smartcard SC, issue the SC to U through a secure channel.
4. After receiving SC, U inserts t into it and finishes the registration.

Authenticated key exchange phase

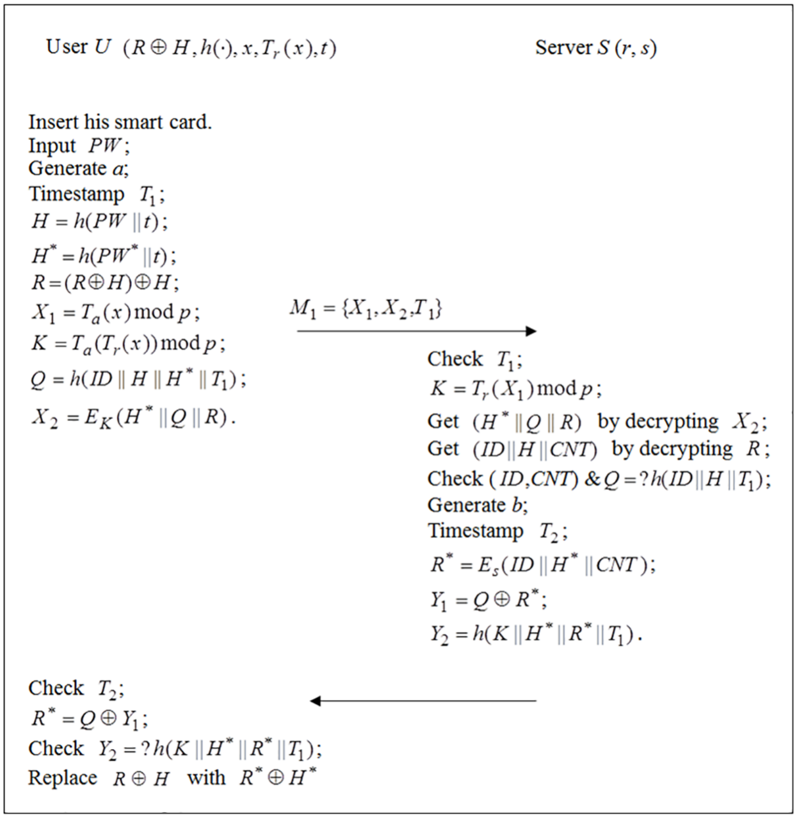
In this phase, as shown in Fig 1, the user U and the server S authenticate each other and negotiate a common session key by performing the following steps.

1. U inserts his SC, inputs PW, computes $H = h(PW \| t)$ and $R = (R \oplus H) \oplus H$, generates a random number a, calculates $X_1 = T_a(x)$mod p, $K = T_a(T_r(x))$mod p, $Q = h(ID \| H \| T_1)$, $X_2 = E_K(Q \| R)$, where T_1 is the current timestamp, and sends $M_1 = \{X_1,X_2,T_1\}$ to S.
2. On receiving M_1, S checks whether $T'-T_1 \leq \Delta T$ holds or not, where T' is the current timestamp. If unsuccessful, S aborts this service request; Otherwise S computes $K = T_r(X_1)$ mod p, obtains $(Q \| R)$ by decrypting $X_2$with K and obtains $(ID \| H \| CNT)$ by decrypting with s, respectively. Then S checks whether (ID, CNT) is recorded in its revocation table or not and verifies $Q = ?h(ID \| H \| T_1)$. If unsuccessful, S still rejects this service request; Otherwise S generates random numbers b, computes $Y_1 = T_b(x)$mod$p$, the session key $\lambda = T_b(T_a(x))$mod p and $Y_2 = h(\lambda \| ID \| Q \| T_2)$, where T_1 is the current timestamp, and sends $M_2 = \{Y_1,Y_2,T_2\}$ to U.
3. On receiving M_2, U checks whether $T''-T_2 \leq \Delta T$ holds or not, where T'' is the current timestamp. If unsuccessful, U omits this service request; Otherwise U computes the session key $\lambda = T_a(Y_1)$mod$p$ and checks whether $Y_2 = ?h(\lambda \| ID \| Q \| T_2)$ holds or not. If unsuccessful, U still omits this service request.

Password change phase

In this password change phase, as shown in Fig 2, a legal user inserts his/her smartcard SC and inputs the old password PW and a new password PW^*, and then changes the password by performing the following steps.

1. SC computes $H = h(PW \| t)$, $H^* = h(PW^* \| t)$, generates a random number a, calculates $X_1 = T_a(x)$ mod p, $K = T_a(T_r(x))$ mod p, $Q = h(ID \| H \| H^* \| T_1)$, $R = (R \oplus H) \oplus H$ and $X_2 = E_K(H^* \| Q \| R)$, where T_1 is the current timestamp, and sends $M_1 = \{X_1,X_2,T_1\}$ to the server.
2. On receiving M_1, S checks whether $T'-T_1 \leq \Delta T$ holds or not, where T' is the current timestamp. If unsuccessful, S aborts this service request; Otherwise S computes $K = T_r(X_1)$ mod p, obtains $(H^* \| Q \| R)$ by decrypting X_2 with K and obtains $(ID \| H \| CNT)$ by decrypting with s, respectively. Then S checks whether (ID, CNT) is recorded in its revocation table or



User U $(R\oplus H, h(\cdot), x, T_r(x), t)$

Server S (r, s)

Insert his smart card.
Input PW;
Generate a;
Timestamp T_1;
$H = h(PW \| t)$;
$H^* = h(PW^* \| t)$;
$R = (R \oplus H) \oplus H$;
$X_1 = T_a(x) \bmod p$;
$K = T_a(T_r(x)) \bmod p$;
$Q = h(ID \| H \| H^* \| T_1)$;
$X_2 = E_K(H^* \| Q \| R)$.

$M_1 = \{X_1, X_2, T_1\}$

Check T_1;
$K = T_r(X_1) \bmod p$;
Get $(H^* \| Q \| R)$ by decrypting X_2;
Get $(ID \| H \| CNT)$ by decrypting R;
Check (ID, CNT) & $Q = ?h(ID \| H \| T_1)$;
Generate b;
Timestamp T_2;
$R^* = E_s(ID \| H^* \| CNT)$;
$Y_1 = Q \oplus R^*$;
$Y_2 = h(K \| H^* \| R^* \| T_1)$.

Check T_2;
$R^* = Q \oplus Y_1$;
Check $Y_2 = ?h(K \| H^* \| R^* \| T_1)$;
Replace $R \oplus H$ with $R^* \oplus H^*$

Fig 2. The password change phase of the enhanced scheme.

https://doi.org/10.1371/journal.pone.0181744.g002

not and verifies $Q = ?h(ID \| H \| T_1)$. If successful, S computes $R^* = E_s(ID \| H^* \| CNT)$, $Y_1 = Q \oplus R^*$ and $Y_2 = h(K \| H^* \| R^* \| T_1)$, and sends $M_2 = \{Y_1, Y_2\}$ to the smartcard.

3. On receiving M_2, SC computes $R^* = Q \oplus Y_1$ and checks whether $Y_2 = ?h(K \| H^* \| R^* \| T_1)$ holds or not. If successful, the smartcard replaces $R \oplus H$ with $R^* \oplus H^*$.

Smartcard revocation phase

This phase enables a legal user to revoke his/her old smartcard and to issue a new smartcard by performing the following steps.

1. U inputs his/her identity ID, password PW, selects a random number t_{new}, computes $H_{new} = h(PW \| t_{new})$, and sends $\{ID, H_{new}, \textit{Smartcard Revocation Request}\}$ to S via a secure channel.
2. S searches (ID,CNT) in its revocation table, computes $CNT_{new} = CNT+1$ and $R_{new} = E_s(ID \| H_{new} \| CNT_{new})$ by using its master key s, and stores (ID,CNT_{new}) in its revocation table.
3. S stores $(R_{new},h(\cdot),E_k(\cdot),x,T_r(x))$ into a smartcard, and issue the smartcard to U through a secure channel.
4. After receiving the smartcard, U inserts t_{new} into it and finishes the smartcard revocation processes.

Security and performance analyses

Security analysis

This subsection analyzes the security of the enhanced scheme, with reference to session key security, the contributory property of key agreements, and the withstanding of replay, denial-of-service and privileged-insider attacks.

Since the enhanced scheme is based on the schemes of Guo and Chang and Lin, the analyses of security requirements and the withstanding of possible attacks closely resemble those for the schemes of Guo and Chang and Lin, and so are not presented here.

Providing session key security (AKE security). The following descriptions reveal that the enhanced scheme provides session key security by adopting the real-or-random (ROR) and the sequence of games (SOG) models [41–45].

The Difference Lemma [45] is used for the sequence of games and is described as follows:

Lemma 1 (Difference Lemma). Let A, B and F be events defined in some probability distribution, and suppose that $A \wedge \neg F \Leftrightarrow B \wedge \neg F$. Then

$$|\Pr[A] - \Pr[B]| \leq \Pr[F].$$

The following theorem shows that the proposed scheme has AKE security if the extended chaotic map-based DDHP holds.

Theorem 1. The probability that an adversary breaks the AKE security of the enhanced authenticated key agreement scheme P satisfies,

$$Adv_P^{ake} \leq 2 \cdot Adv^{ddh} + \frac{2}{N} + \frac{1}{2^{l-1}},$$

where Adv^{ddh} is the advantage that an extended chaotic map-based DDH attacker can gain by solving the extended chaotic map-based $DDHP$, N is the size of password lists, and l is a secure parameter size.

Proof: Game $\mathbf{G}_i^{ake}$ defines the probability of the event E_i that the adversary wins this game. The start game $\mathbf{G}_0^{ake}$ is a real attack against the proposed scheme, and the final game $\mathbf{G}_1^{ake}$ ends a negligible advantage gained by an attacked by breaking the AKE security of the enhanced scheme.

Game $\mathbf{G}_0^{ake}$: This game corresponds to the real attack. By definition,

$$Adv_P^{ake}(\mathrm{A}) = |2\Pr[E_0] - 1|. \tag{1}$$

Game $\mathbf{G}_1^{ake}$: This game considers password-guessing attacks. Each $X_2 = E_K(Q \parallel R)$ is different, where $Q = h(ID \parallel H \parallel T_1)$, $H = h(PW \parallel t)$ and $K = T_a(T_r(x)) \bmod p$, since t and a are random numbers selected by user U, and T_1 is the timestamp. Thus, the adversary has no information for verifying his/her password guesses. This implies that the security against password attacks is measured by the probability that exists messages of the form $X_2 = E_K(Q \parallel R)$ such that the guessing password is correct. Then, we have

$$|\Pr[E_0] - \Pr[E_1]| \leq \frac{1}{N}. \tag{2}$$

Game $\mathbf{G}_2^{ake}$: This game transforms game $\mathbf{G}_1^{ake}$ into game $\mathbf{G}_2^{ake}$, getting Q by choosing a random number, instead of computing a hash. Then, games $\mathbf{G}_1^{ake}$ and $\mathbf{G}_2^{ake}$ are undistinguishable except collisions of a hash function in $\mathbf{G}_2^{ake}$. Thus, according to the birthday paradox [42] and

Lemma 1, we have

$$|\Pr[E_1] - \Pr[E_2]| \leq \frac{1}{2^l}. \tag{3}$$

Game $\mathbf{G}_3^{ake}$: This game is transformed from game $\mathbf{G}_2^{ake}$ by using a triple (X,Y,Z) sample from a random distribution $(T_a(x) \bmod p, T_b(x) \bmod p, T_z(x) \bmod p)$, rather than an extended chaotic map-based DDH triple. $\mathbf{G}_2^{ake}$ is therefore equivalent to $\mathbf{G}_3^{ake}$, and

$$\Pr[E_2] = \Pr[E_3]. \tag{4}$$

Let a challenger $\mathrm{A}_{\mathrm{ddh}}$ attempt to violate the indistinguishability of the extended chaotic map-based DDHP, and let an adversary $\mathrm{A}_{\mathrm{ake}}$ be created to violate the session key security. $\mathrm{A}_{\mathrm{ddh}}$ returns the real key λ to $\mathrm{A}_{\mathrm{ake}}$ if the flipping unbiased coin bit $c = 1$; otherwise, $c = 0$ and it returns a random string to $\mathrm{A}_{\mathrm{ake}}$. Then $\mathrm{A}_{\mathrm{ake}}$ outputs its guess bit c' and wins if $c' = c$. $\mathrm{A}_{\mathrm{ddh}}$ returns the output exactly as in the preceding experiment, except with (X, Y, Z) that was input to it. If $\mathrm{A}_{\mathrm{ake}}$ outputs c, then $\mathrm{A}_{\mathrm{ddh}}$ outputs 1; otherwise, it outputs 0. If (X, Y, Z) is a real extended chaotic map-based Diffie-Hellman triple, then $\mathrm{A}_{\mathrm{ddh}}$ executes $\mathrm{A}_{\mathrm{ake}}$ in $\mathbf{G}_3^{ake}$ and so Prob. [event that $\mathrm{A}_{\mathrm{ddh}}$ outputs 1] equals the Prob.$[E_3]$. If (X, Y, Z) is a random triple, then $\mathrm{A}_{\mathrm{ddh}}$ runs $\mathrm{A}_{\mathrm{ake}}$ in $\mathbf{G}_4^{ake}$ and so Prob. [event that $\mathrm{A}_{\mathrm{ddh}}$ outputs 1] equals Prob.$[E_4]$. Therefore,

$$|\Pr[E_3] - \Pr[E_4]| \leq Adv^{ddh}(\mathrm{A}_{ddh}). \tag{5}$$

No information about flipping unbiased coin bit c is revealed, and all session keys are random and independent among all executions of the enhanced scheme. Thus,

$$\Pr[E_4] = \frac{1}{2}. \tag{6}$$

Combining Eqs (1)–(6) and using Lemma 1, yields

$$Adv_P^{ake}(\mathrm{A}_{ake}) \leq 2 \cdot Adv^{ddh}(\mathrm{A}_{ddh}) + \frac{2}{N} + \frac{1}{2^{l-1}}.$$

The proof is thus concluded.

Providing the contributory property of key agreements. Theorem 2. The enhanced scheme provides the contributory property of key agreements.

Proof: By Theorem 1, the session key security of the enhanced scheme is based on the extended chaotic map-based Diffie-Hellman problem. Therefore, the enhanced scheme avoids the security weakness that was proposed by Bergamo et al. [20] and neither a user nor the server alone can determine a session key. Thus, the enhanced scheme satisfies the contributory property of key agreements.

Withstanding replay attacks. Theorem 3. The password change phase of the enhanced scheme withstands replay attacks.

Proof: In the password change phase of the enhanced scheme, the smartcard sends the request message $M_1 = \{X_1, X_2, T_1\}$ to the server, where T_1 is the current timestamp, $X_1 = T_a(x)$ mod p, $X_2 = E_K(H^* \parallel Q \parallel R)$, $K = T_a(T_r(x))$ mod p, $H^* = h(PW^* \parallel t)$ and $Q = h(ID \parallel H \parallel H^* \parallel T_1$. By validating timestamp T_1 and $Q = ?h(ID \parallel H \parallel H^* \parallel T_1$, the server can easily verify the freshness of the request messages that are received from the users, so the enhanced scheme withstands replay attacks.

Withstanding denial of service attacks. Theorem 4. The password change phase of the enhanced scheme withstands denial-of-service attacks.

Proof: Since the smartcard validates updated data R^* by checking $Y_2 = h(K \parallel H^* \parallel R^* \parallel T_1$ and then replaces R with R^*, where the timestamp T_1 is generated by the smartcard and $H^* = h(PW^* \parallel t)$, an attacker has difficulty in modifying the response message $M_2 = \{Y_1, Y_2\}$. Therefore, the enhanced scheme withstands denial-of-service attacks.

Withstanding privileged insider attacks. Theorem 5. The password change phase of the enhanced scheme withstands privileged-insider attacks.

Proof: In the enhanced scheme, every legitimate user has $(x, T_r(x))$ in his/her smartcard. By Theorem 1, the session key security of the enhanced scheme is based on the extended chaotic map-based Diffie-Hellman problem. Thus, a malicious user cannot derive the secret key K and the session key λ that is shared between another user and the server in the authenticated key exchange and the password change phases. Consequently, a malicious user cannot receive $(Q \parallel R)$ and $(ID \parallel H \parallel CNT)$ in the authenticated key exchange phase, and $(H^* \parallel Q \parallel R)$ and $(ID \parallel H \parallel CNT)$ in the password change phases. Such a user has difficulty in forging valid request messages and impersonating other users. Thus, the enhanced scheme withstands privileged insider attacks.

Logical analyses

This subsection describes the logical analyses of the proposed scheme by using the logical tool, which was defined and presented by Burrows et al. [46] in 1990 and Buttyan et al. [47] in 1998.

Assume that P and Q range over principals. C denotes a communicating channel and X and Y are messages. Table 1 defines the notation used for logical analyses [46–48].

Table 2 lists the used assumptions and Table 3 lists the used logical description [46–48], where A and B are S and U, but $A \neq B$.

Then, according to [46–48], the proposed scheme is described in logic as follows.

$$\text{Step 1. } S \lhd \left(\xrightarrow[\text{ECMDH(public)}]{T_a(x) \bmod p} U, C_{S,U}(h(ID||H||T_1), R), T_1 \right)$$

$$\text{Step 2. } U \lhd \left(\xrightarrow[\text{ECMDH(public)}]{T_b(x) \bmod p} S, (ID, h(ID||h(PW||t)||T_1), T_2)_\lambda, T_2 \right)$$

Table 1. The notation used for logical analyses.

Symbol	Description
$C(X)$	The message X is transited via channel C.
$r(C)$	The set of readers of channel C.
$w(C)$	The set of writers of channel C.
$P \mid\equiv X$	P believes the statement X.
$P \mid\sim X$	P once said X.
$P \lhd C(X)$	P sees $C(X)$. The message X is transited via channel C and can be observed by P. P must be a reader of channel C to read message X.
$P \lhd X \mid C$	P sees X via C. The message X is transited via channel C and can be received by P.
$(X)_K$	X is hashed with the key K.
$P \overset{K}{\longleftrightarrow} Q$	P and Q can establish a secure communication channel by using the shared key K.

https://doi.org/10.1371/journal.pone.0181744.t001

Table 2. The assumptions of the proposed scheme.

(A1) $A \in r(C_{A,B})$: A can read from the channel $C_{A,B}$.
(A2) $A \equiv (w(C_{A,B}) = \{A,B\})$: A believes that A and B can write on $C_{A,B}$.
(A3) $A \equiv (B \parallel \sim \Phi \rightarrow \Phi)$: A believes that B only says what it believes.
(A4) $A \equiv \# (N_A)$: A believes that N_A is fresh.
(A5) $A \equiv \overset{a}{\underset{\text{ECMDH(secret)}}{\rightarrow}} A$: A believes that a is its extended chaotic map-based Diffie–Hellman secret.

https://doi.org/10.1371/journal.pone.0181744.t002

On the basis of to the assumptions and logical analyses, the proposed scheme must realize the following four goals of authentication and key agreement.

Goal 1: $U \equiv U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S$: User U believes that $\lambda = T_{ab}(x) \bmod p$ is a symmetric key shared between participants U and S.

Goal 2: $S \equiv U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S$: Server S believes that $\lambda = T_{ab}(x) \bmod p$ is a symmetric key shared between U and S.

Goal 3: $U \equiv S \equiv U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S$: User U believes that S is convinced of $\lambda = T_{ab}(x) \bmod p$ is a symmetric key shared between U and S.

Table 3. The inference rules of the logic of the proposed scheme.

Seeing rules
(S1) $\frac{P \lhd C(X), P \in r(C)}{P \equiv (P \lhd X \mid C), P \lhd X}$: If P receives and reads X via C, then P believes that X has arrived on C and P sees X.
(S2) $\frac{P \lhd (X,Y)}{P \lhd X, P \lhd Y}$: If P sees a hybrid message (X, Y), then P sees X and Y separately.
Interpretation rules
(I1) $\frac{P \equiv (w(C)=\{P,Q\})}{P \equiv (P \lhd X \mid C) \rightarrow Q \mid\sim X}$: If P believes that C can only be written by P and Q, then P believes that if P receives X via C, then Q said X.
(I2) $\frac{P \equiv (Q \mid\sim (X,Y))}{P \equiv (Q \mid\sim X), P \equiv (Q \mid\sim Y)}$: If P believes that Q said a hybrid message (X, Y), then P believes that Q has said X and Y separately.
(I3) $\frac{P \equiv (\overset{a}{\underset{\text{ECMDH(secret)}}{\rightarrow}} P), P \equiv (\overset{T_b(x)\bmod p}{\underset{\text{ECMDH(public)}}{\rightarrow}} Q)}{P \equiv (P \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} Q)}$: If P believes that a is its extended chaotic map-based Diffie–Hellman secret and that $T_a(x)$ mod p is the extended chaotic map-based Diffie–Hellman component from Q, then P believes that $T_{ab}(x)$ mod p is the symmetric key shared between P and Q.
Freshness rules
(F1) $\frac{P \equiv (Q \mid\sim X), P \equiv \# (X)}{P \equiv (Q \mid\sim X)}$: If P believes that another Q said X and P also believes that X is fresh, then P believes that Q has recently said X.
(F2) $\frac{P \equiv \# (X)}{P \equiv \# (X,Y)}$: If P believes that a part of a mixed message X is fresh, then it believes that the whole message (X, Y) is fresh.
Rationality rules
(R1) $\frac{P \equiv (\Phi_1 \rightarrow \Phi_2), P \equiv \Phi_1}{P \equiv \Phi_2}$: If P believes that Φ_1 implies Φ_2 and P believes that Φ_1 is true, then P believes that Φ_2 is true.

https://doi.org/10.1371/journal.pone.0181744.t003

Goal 4: $S \equiv U \equiv U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S$: Server S believes that U is convinced of $\lambda = T_{ab}(x)$ mod p is a symmetric key shared between U and S.

To accomplish the Goal 1, we have that

$$U \equiv \underset{\text{ECMDH(secret)}}{\overset{a}{\rightarrow}} U \tag{7}$$

and

$$U \equiv \underset{\text{ECMDH(public)}}{\overset{T_a(x)\bmod p}{\rightarrow}} U \tag{8}$$

must hold because of the interpretation rule (I3) and assumption (A5).

Next, to accomplish Eq (8), we have that

$$U \equiv (S|| \sim (\underset{\text{ECMDH(public)}}{\overset{T_b(x)\bmod p}{\rightarrow}} S, (ID, h(ID||H||T_1), T_2)_{\lambda}, T_2) \longrightarrow \underset{\text{ECMDH(public)}}{\overset{T_b(x)\bmod p}{\rightarrow}} S) \tag{9}$$

and

$$U \equiv (S|| \sim \underset{\text{ECMDH(public)}}{\overset{T_b(x)\bmod p}{\rightarrow}} S) \tag{10}$$

must hold because of assumption (A3) and the rationality rule (R1). To accomplish Eq (10), we have that

$$U \equiv \#\, (\underset{\text{ECMDH(public)}}{\overset{T_b(x)\bmod p}{\rightarrow}} S) \tag{11}$$

must hold because of the freshness rules (F1), (F2) and assumption (A4).

To accomplish Eq (11), we have that

$$U \in r(C_{S,U}), \tag{12}$$

$$U \equiv (w(r(C_{S,U}) = \{U, S\}) \tag{13}$$

and

$$U \equiv \lhd C_{S,U}(\underset{\text{ECMDH(public)}}{\overset{T_b(x)\bmod p}{\rightarrow}} S) \tag{14}$$

must hold because of the interpretation rules (I1), the seeing rules (S1), (S2), assumptions (A1) and (A2). By using the interpretation rules (I3) and, we have the proposed scheme realizes

$$\text{Goal 1}: U \equiv U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S.$$

Similarly, we have that the proposed scheme realizes Goal 2: $S \equiv U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S$ by using the same arguments of Goal 1.

To accomplish Goal 3, we have that

$$U \equiv ((S|| \sim U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S) \longrightarrow (S \equiv U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S)) \tag{15}$$

and

$$U \equiv (S|| \sim U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S) \tag{16}$$

must hold because of the rationality rule (R1) and assumption (A3). To accomplish Eq (16), we have that

$$U \equiv (S| \sim U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S) \tag{17}$$

and

$$U \equiv \# (U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S) \tag{18}$$

must hold because of the freshness rules (F1), (F2) and assumption (A4). To accomplish Eq (18), we have that

$$U \in r(C_{U,S}) \tag{19}$$

$$U \equiv (w(C_{U,S}) = \{U, S\}), \tag{20}$$

and

$$U \lhd C_{U,S}(U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S) \tag{21}$$

must hold because of the interpretation rule (I1), the assumptions (A1), (A2) and the seeing rules (S1) and (S2).

Thus, the proposed protocol realizes

$$\text{Goal 3}: \ U \equiv S \equiv U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S.$$

Similarly, using the same arguments of Goal 3, the proposed scheme realizes Goal 4: $S \equiv U \equiv U \overset{T_{ab}(x)\bmod p}{\longleftrightarrow} S$.

Therefore, the proposed scheme realizes Goals 1, 2, 3 and 4.

Performance analysis and comparisons

Table 4 compares the performance and security properties of the enhanced scheme with related approaches [7, 9, 10, 15, 36, 37, 40, 49–53], where T_H denotes the time of executing a hash function operation; T_C denotes the time of executing a chaotic map operation; T_S denotes

Table 4. Performance and security properties comparison.

Schemes	Computations	Transmissions	P_1	P_2	P_3
Islam et al.'s scheme [15]	$5T_H+T_{SQ}+T_{SR}$	2	Yes	Yes	Yes
Chen et al.'s scheme [9]	$5T_H+3T_M+3T_E$	2	No	No	Yes
Jiang et al.'s scheme [10]	$5T_H+T_M+5T_E$	2	No	Yes	Yes
Wang et al.'s scheme [49]	$10T_H$	2	No	No	No
Lee et al.'s scheme [7]	$16T_H$	3	No	No	No
Yan et al.'s scheme [50]	$11T_H$	3	No	Yes	No
Das-Goswami's scheme [51]	$2T_H+12T_C$	2	Yes	Yes	Yes
Lee et al.'s scheme [52]	$12T_H+4T_C$	2	No	No	Yes
He et al.'s scheme [53]	$10T_H+6T_C$	2	Yes	No	Yes
Islam et al.'s scheme [36]	$18T_H+10T_C$	2	Yes	No	Yes
Jiang et al.'s scheme [37]	$21T_H+6T_C$	2	Yes	Yes	Yes
Lin's scheme [40]	$5T_H+5T_S+6T_C$	2	Yes	No	Yes
Enhanced scheme	$5T_H+3T_S+5T_C$	2	Yes	Yes	Yes

P_1: Resisting possible attacks; P_2: User anonymity; P_3: Perfect forward secrecy.

https://doi.org/10.1371/journal.pone.0181744.t004

the time of executing a symmetric encryption/decryption operation; T_{SQ} denotes the time of executing a squaring operation; T_{SR} denotes the time of executing a squaring root solving operation; T_M denotes the time of executing a multiplication/division operation and T_E denotes the time of executing a modular exponential computation.

The schemes proposed by Islam et al. [15], Chen et al. [9] and Jiang et al. [10] use the public key cryptosystem, require time-consuming modular exponential computations, and thus are inefficient. Although the schemes proposed by Wang *et al.* [49], Lee et al. [7] and Yan et al. [50] only employ the hash function operations and are more efficient than other schemes, these schemes fail to resist possible attacks and cannot provide perfect forward secrecy. The schemes proposed by Das and Goswami [51], Lee *et al.* [52], He et al. [53], Islam et al. [36], Jiang et al. [37] and Lin [40] and the enhanced scheme are based on chaotic maps and retain low computations and communications. Additionally, only the schemes proposed by Das and Goswami [51] and Jiang et al. [37] and the enhanced scheme resist potential attacks and provide more functions.

Conclusions

This study addresses the weaknesses of Lin's improved scheme including its vulnerability to denial-of-service attacks and privileged-insider attacks, and its inability to support the contributory property of key agreements. An enhanced smartcard-based password-authenticated key agreement scheme that is based on extended chaotic maps is presented. The session key security of the enhanced scheme is proven secure using the real-or-random and the sequence-of-game models, and it is based on the extended chaotic map-based DDHP. Thus, malicious users cannot derive a session key between another user and the server, and they cannot forge valid request messages or impersonate other users. Accordingly, the enhanced scheme withstands privileged insider attacks. Additionally, in the enhanced scheme, the messages that are sent from users are guaranteed to be fresh by the appending of timestamps, and the smartcard validates updated data from the server so the enhanced scheme withstands replay and denial-of-service attacks. Therefore, the enhanced scheme eliminates the weaknesses in previous schemes.

Acknowledgments

This research was supported by Ministry of Science and Technology under the grants MOST 105-2221-E-320-003 and by Tzu Chi University under the grants TCRPP105004. Ted Knoy is appreciated for his editorial assistance.

Author Contributions

Data curation: Shi-Han Hwang.

Formal analysis: Tian-Fu Lee, Tsung-Hung Lin.

Funding acquisition: Tian-Fu Lee, Chia-Hung Hsiao.

Investigation: Tian-Fu Lee, Chia-Hung Hsiao, Shi-Han Hwang.

Methodology: Tian-Fu Lee, Shi-Han Hwang.

Project administration: Tian-Fu Lee.

Resources: Chia-Hung Hsiao.

Supervision: Chia-Hung Hsiao.

Validation: Chia-Hung Hsiao, Tsung-Hung Lin.

Writing – original draft: Tian-Fu Lee, Shi-Han Hwang, Tsung-Hung Lin.

Writing – review & editing: Tian-Fu Lee, Tsung-Hung Lin.

References

1. Juang W. Efficient password authenticated key agreement using smart cards, Computers & Security 2004; 23: 167–173.
2. Fan CI, Chan YC, Zhang ZK. Robust remote authentication scheme with smart cards, Computers & Security 2005; 24: 619–628.
3. Juang WS, Chen ST, Liaw HT. Robust and efficient password-authenticated key agreement using smart card, IEEE Transactions on Industrial Electronics 2008; 55: 2551–2556.
4. Sun DZ, Huai JP, Sun JZ, Li JX, Zhang JW, Feng ZY. Improvements of Juang et al'.s password-authenticated key agreement scheme using smart cards, IEEE Transactions on Industrial Electronics 2009; 56: 2284–2291.
5. Yeh KH, Su C, Lo NW, Li YJ, Hung YX. Two robust remote user authentication protocols using smart cards, Journal of Systems and Software 2010; 83: 2556–2565.
6. Li XX, Qiu WD, Zheng D, Chen KF, Li JH. Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards, IEEE Transactions on Industrial Electronics 2010; 57: 780–793.
7. Lee TF, Chang IP, Lin TH, Wang CC. A secure and efficient password-based user authentication scheme using smart cards for the integrated EPR information system, Journal of Medical Systems 2013; 37(3): 9941. https://doi.org/10.1007/s10916-013-9941-8 PMID: 23553734
8. Lee TF, Liu CM. A secure smart-card based authentication and key agreement scheme for telecare medicine information systems, Journal of Medical Systems 2013; 37 (9933): 1–8.
9. Chen BL, Kuo WC, Wuu LC. Robust smart-card-based remote user password authentication scheme, International Journal of Communication Systems 2012;
10. Jiang Q, Ma J, Li G, Li X. Improvement of robust smart-card-based password authentication scheme, International Journal of Communication Systems 2015 28(2): 383–393, https://doi.org/10.1002/dac.2644
11. Wen FT. A robust uniqueness and anonymity preserving remote user authentication scheme for connected health care, Journal of Medical System 2013; 37(6): 9980. https://doi.org/10.1007/s10916-013-9980-1 PMID: 24146334
12. Chen Y, Chou J, Sun H. A novel mutual-authentication scheme based on quadratic residues for RFID systems, Computer Networks 2008; 52(12): 2373–2380. https://doi.org/10.1016/j.comnet.2008.04.016

13. Rosen K. Elementary number theory and its applications. Reading. MA: Addison-Wesley, 2008.

14. Wu ZY, Lee YC, Lai F, Lee HC, Chung Y. A secure authentication scheme for telecare medicine information systems, Journal of Medical System 2012; 36(3): 1529–1535. https://doi.org/10.1007/s10916-010-9614-9 PMID: 20978928

15. Islam SH, Khan MK, Li X. Security Analysis and Improvement of 'a More Secure Anonymous User Authentication Scheme for the Integrated EPR Information System', PLOS ONE 2015, http://dx.doi.org/10.1371/journal.pone.0131368

16. Li CT. A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card, IET Inform. Security 2013; 7(1): 3–10.

17. Wang D, He D, Wang P, Chu CH. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment, IEEE Transactions on Dependable and Secure Computing 2015; 12(4): 428–442.

18. Kocarev L, Tasev Z. Public-key encryption based on Chebyshev maps, Proc. of the International Symposium on Circuits and Systems 2003; 3: III-28–III-31.

19. Mason JC, Handscomb DC. Chebyshev polynomials. Chapman & Hall/CRC, Boca Raton, Florida, 2003.

20. Bergamo P, D'Arco P, Santis A., Kocarev L. Security of public-key cryptosystems based on Chebyshev polynomials, IEEE Transactions on Circuits and Systems I 2005; 52: 1382–1393.

21. Xiao D, Liao X, Deng S. A novel key agreement protocol based on chaotic maps, Information Sciences 2007; 177: 1136–1142.

22. Han S. Security of a key agreement protocol based on chaotic maps, Chaos, Solitons & Fractals 2008; 38: 764–768.

23. Xiao D, Liao XF, Deng SJ. Using time-stamp to improve the security of a chaotic maps-based key agreement protocol, Info. Sci. 2008; 178: 1598–1602.

24. Tseng H, Jan, R, Yang W. A chaotic maps-based key agreement protocol that preserves user anonymity, IEEE International Conference on Communications (ICC09) 2009, pp. 1–6.

25. Wang X, Zhao J. An improved key agreement protocol based on chaos, Communications in Nonlinear Science and Numerical Simulation 2010; 15: 4052–4057.

26. Guo XF, Zhang JS. Secure group key agreement protocol based on chaotic hash, Information Sciences 2010; 180: 4069–4074.

27. Niu Y. Wang X. An anonymous key agreement protocol based on chaotic maps, Communications in Nonlinear Science and Numerical Simulation 2011; 16: 1986–1992.

28. Xue K, Hong P. Security improvement on an anonymous key agreement protocol based on chaotic maps, Communications in Nonlinear Science and Numerical Simulation 2012; 17: 2969–2977.

29. 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.

30. Zhang L. Cryptanalysis of the public key encryption based on multiple chaotic systems, Chaos Solitons Fractals 2008; 37(3): 669–674.

31. Lee CC, Chen CL, Wu CY, Huang SY. An extended chaotic maps-based key agreement protocol with user anonymity, Nonlinear Dynamics 2012; 69: 79–87.

32. Lee CC, Hsu CW. A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps, Nonlinear Dynamics 2013; 71: 201–211.

33. Guo C, Chang CC. Chaotic maps-based password-authenticated key agreement using smart cards, Communications in Nonlinear Science and Numerical Simulation 2013; 18: 1433–1440.

34. Lin HY. Chaotic map based mobile dynamic ID authenticated key agreement scheme, Wireless Personal Communications 2014; 78(2):1487–1494.

35. Islam SH., Obaidat MS, Amin R. An anonymous and provably secure authentication scheme for mobile user, International Journal of Communication Systems 2016. https://doi.org/10.1002/dac.3126

36. Islam SKH. Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps, Nonlinear Dyn. 2014; 78(3), 2261–2276. https://doi.org/10.1007/s11071-014-1584-x

37. Jiang Q, Wei F, Fu S, Ma J, Li G, Alelaiwi A. Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy, Nonlinear Dyn. 2016; 83(4), 2085–2101. https://doi.org/10.1007/s11071-015-2467-5

38. Hao X, Wang J., Yang Q, Yan X, Li P. A chaotic map-based authentication scheme for telecare medicine information systems, Journal of Medical Systems 2013; 37 (9919): 1–7.

39. Lee TF. An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems, Journal of Medical Systems 2013; 37 (9958): 1–9.

40. Lin HY. Improved chaotic maps-based password-authenticated key agreement using smart cards, Communications in Nonlinear Science and Numerical Simulation 2015; 20: 482–488.

41. Bellare M, Pointcheval D, Rogaway P. Authenticated key exchange secure against dictionary attacks, Proc. of Advances in Cryptology—Eurocrypt 2000, Lecture Notes in Computer Science 1807, pp 139–155.

42. Boyko V, MacKenzie P, Patel S. Provably secure password-based authenticated key exchange protocols using Diffie-Hellman, Proc. of Advances in Cryptology—Eurocrypt 2000, Lecture Notes in Computer Science 1807, pp. 156–171.

43. Abdalla M, Fouque PA, Pointcheval D. Password-based authenticated key exchange in the three-party setting, Proc. of Public Key Cryptography—PKC 2005, Lecture Notes in Computer Science 3386, pp. 65–84.

44. Abdalla M, Pointcheval D. Simple password-based authenticated key protocols, Topics in Cryptology—CT-RSA 2005, Lecture Notes in Computer Science 3376, pp. 191–208.

45. Shoup V. Sequences of games: A tool for taming complexity in security proofs, manuscript, www.shoup.net, 2005.

46. Burrows M, Abadi M, Needham R. A logic of authentication, ACM Trans. Comput. Syst. 1990; 8(1): 18–36.

47. Buttyan L, Staamann S, Wilhelm U. A simple logic for authentication protocol design, Proc. of the 11th IEEE Computer Security Foundation Workshop, June 1998, Rockport, MA.

48. Aslan HK. Logical analysis of AUTHMAC_DH: a new protocol for authentication and key distribution, Comput. Secur. 2004; 23: 290–299.

49. Wang YY, Liu JY, Xiao FX, Dan J. A more efficient and secure dynamic ID-based remote user authentication scheme, Comput. Commun. 2009; 32:583–585.

50. Yan X, Li W, Li P, Wang J, Hao X, Gong P. A secure biometrics-based authentication scheme for telecare medicine information systems, Journal of Medical Systems 2013; 37: 9972, https://doi.org/10.1007/s10916-013-9972-1 PMID: 23996083

51. Das AK, Goswami A. An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function, Journal of Medical Systems 2014; 38: 27, https://doi.org/10.1007/s10916-014-0027-z PMID: 24888983

52. Lee CC, Chen CL, Wu CY, Huang SY. An extended chaotic maps-based key agreement protocol with user anonymity, Nonlinear Dynamics 2012; 69(1–2): 79–87.

53. He D, Chen Y, Chen J, Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol, Nonlinear Dynamics 2012; 69(3): 1149–1157.