This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

Provably Secure Anonymous Single-Sign-On Authentication Mechanisms Using Extended Chebyshev Chaotic Maps for Distributed Computer Networks

Tian-Fu Lee

***Abstract*—Single-sign-on authentication mechanisms enable a legal user to access various service providers efficiently and conveniently by using a unitary token. These mechanisms are widely used in distributed computer networks. This investigation proposes an efficient and secure single-sign-on authentication scheme that uses extended chaotic maps, exhibits operations that satisfy the semigroup property and commutative under composition, and has a higher efficiency than modular exponential computations and scalar multiplications on the elliptic curve. The session key security of the proposed scheme is based on Chebyshev chaotic-map-based assumptions, and the scheme is proven to be secure using the real-or-random model. The proposed authentication scheme retains the security properties of earlier schemes, requires fewer transmissions, has a lower computational cost, and uses fewer variables; it is therefore efficient in computation and communication.**

***Index Terms*—Anonymity, authentication, chaotic map, key distribution, network communication.**

I. Introduction

USER authentication approaches enable users to access the remote resources efficiently and conveniently. Traditional authentication schemes only provide a user with accessing service providers from a single authentication server and cannot allow legal users to access different services over an open network with a single secret key [1]–[9]. That is, if a user tries to access multiple independent service providers by using these authentication schemes, then he/she must keep many secret keys. In order to solve this problem, many single-sign-on authentication mechanisms were proposed so that a legal user can access different and independent service providers in distributed computer networks by using a unitary token [10]–[15].

In 2012, Chang and Lee [16] developed a nonce-based single-sign-on authentication scheme to eliminate the security weaknesses and to solve the synchronization problem associated with earlier methods [12], [14], [17], [18]. Subsequently, Wang *et al.* [19] demonstrated that the scheme of Chang and Lee violated credential privacy and the soundness of authentication. Wang *et al.* presented an improved scheme. However, all of these authentication schemes used too many exponential operations, variables, and messages in transmission, and so, they were inefficient in both computation and communication.

The Chebyshev polynomial has recently been revealed to exhibit the semigroup property and to satisfy commutation under composition. Additionally, cryptosystems that use chaotic maps have higher efficiency than traditional cryptosystems that use modular exponential computations and scalar multiplications on an elliptic curve [20]–[27]. Accordingly, this work develops an efficient single-sign-on authentication scheme using extended Chebyshev chaotic maps [24], [28]–[33]. The proposed scheme does not have the redundant variables and reschedules transmitted messages; it also hides the real identities of users by exploiting the semigroup property and commutativity under composition in extended chaotic maps. In the proposed scheme, the user negotiates the session key with the service provider in few steps. Therefore, the proposed scheme can be executed using few communicating messages. It not only retains the security properties of previous schemes and requires fewer transmissions but also has a lower computational cost and uses fewer variables. Moreover, the proposed scheme is proven to be secure using the real-or-random model [34]–[37] and the sequence of games (SOG) technique [38].

The remainder of this paper is organized as follows. Section II reviews the concepts associated with Chebyshev chaotic maps and related assumptions. Section III presents the proposed single-sign-on authentication mechanism. Section IV analyzes the security and performance of the proposed mechanism. Finally, Section V draws the conclusion.

II. Preliminaries

This section presents the notations and definitions and then briefly reviews the Chebyshev chaotic maps and related assumptions.

A. Notations

Assume that a smart card producing center $SCPC$ is a trusted authority; U_i is a user, and P_j is a service provider. Table I lists the notation that is used throughout this paper.

Manuscript received April 17, 2015; revised June 20, 2015; accepted August 18, 2015. This work was supported by the Ministry of Science and Technology of the Republic of China, Taiwan, under Contract No. MOST 103-2221-E-320-003, MOST 104-2221-E-320-002, and TCRPP103008.

The author is with the Department of Medical Informatics, Tzu Chi University, Hualien 97004, Taiwan (e-mail: jackytflee@mail.tcu.edu.tw).

Digital Object Identifier 10.1109/JSYST.2015.2471095

TABLE I
NOTATION

Notation	Description
ID_X	The identity of the entity X
sk_X	The secret key of the entity X
$E_k(\cdot)$ / $D_k(\cdot)$	A secure symmetric en/decryption algorithm with the secret key k
l	The secure parameter size
$h(\cdot)$	A collision-resistant cryptographic one-way hash function and $h:\{0,1\}^* \to \{0,1\}^l$
$A \to B : M$	A sends message M to B through a common channel
$M_1 \| M_2$	Message M_1 concatenates to message M_2.

B. Definitions

1) Session Key Security (AKE Security): This definition defines that an adversary fails to effectively distinguish between two messages from a challenger. One message is encrypted by the real session key, and the other one is encrypted by a random string via an unbiased coin c. The adversary selects one message and sends to the challenger. The challenger then flips an unbiased coin $c \in \{0, 1\}$ and decides to return the message encrypted by the real session key if $c = 1$ or encrypted by a random string if $c = 0$. The adversary intends to correctly guess the value of the hidden bit. The advantage that an adversary violates the indistinguishability of a scheme $\mathbf{P}$ is $\mathrm{Adv}_P^{\mathrm{ake}}$ (A). The scheme $\mathbf{P}$ is AKE-secure if $\mathrm{Adv}_P^{\mathrm{ake}}$ (A) is negligible [24], [31]–[33].

2) Chebyshev Chaotic Maps [20]–[23]: 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 semigroup 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 $n > 1$, the Chebyshev polynomial map $T_n : [-1, 1] \to [-1, 1]$ of degree n is a chaotic map with its invariant density

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

for Lyapunov exponent $\ln n > 0$.

In 2005, Bergamo *et al.* [20] demonstrated that public-key cryptosystems based on Chebyshev polynomials had the security weakness that one malicious participant can predetermine the session key alone. In 2008, Zhang [33] enhanced the Chebyshev polynomials to eliminate this security weakness and proved that the semigroup property and commutativity under composition held on the 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.

Enhanced Chebyshev polynomials are associated with three hard problems, which are the extended chaotic-map-based discrete logarithm, the computational Diffie–Hellman problems (CDHPs), and the decisional Diffie–Hellman problem (DDHP) [24], [28]–[33], described in the following discussion.

3) Extended Chaotic-Map-Based DLP: Given x, y, and p, finding the integer r satisfying $y = T_r(x) \bmod p$ is computationally infeasible.

4) Extended Chaotic-Map-Based 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.

5) Extended Chaotic-Map-Based DDHP: Given $T_r(x)$, $T_s(x)$, $T_z(x)$, $T(\cdot)$, and x, deciding whether

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

holds or is not computationally infeasible.

III. PROPOSED SINGLE-SIGN-ON AUTHENTICATION MECHANISM

This section presents a secure and efficient single-sign-on mechanism that is based on extended chaotic maps. First, the proposed authentication scheme hides the real identities of users by using a temporary secret key, which security is based on extended chaotic-map-based Diffie–Hellman problem. Next, it generates the session keys by using the extended chaotic-map-based Diffie–Hellman key exchange and enables a service provider P_j and a user U_i to compute their session keys in early steps. Additionally, the redundant parameters are removed. Therefore, the proposed scheme retains the security properties and requires fewer computations, transmissions, and used variables than comparable schemes. It consists of the system initialization phase, the registration phase, and the user identification phase, which are described in the following.

A. System Initialization Phase

Fig. 1 displays the system initialization phase of the proposed authentication scheme.

1) The smart card producing center $SCPC$ generates a random number x and a large prime number n.
2) The $SCPC$ generates two nonces s and K_S.
3) For each service provider P_j whose identity is ID_j, $SCPC$ computes $PID_j = h(ID_j \| K_S)$ and $sk_j = T_{PID_j \cdot s}(x) \bmod n$.
4) The $SCPC$ sends (PID_j, K_S, sk_j) to P_j through a secure channel.

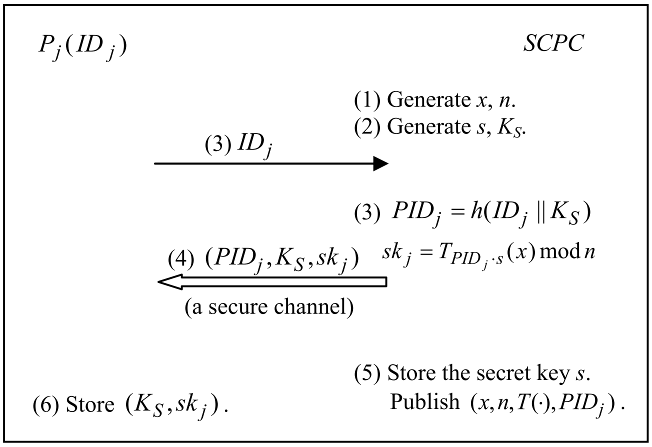

Fig. 1. System initialization phase of the proposed scheme.

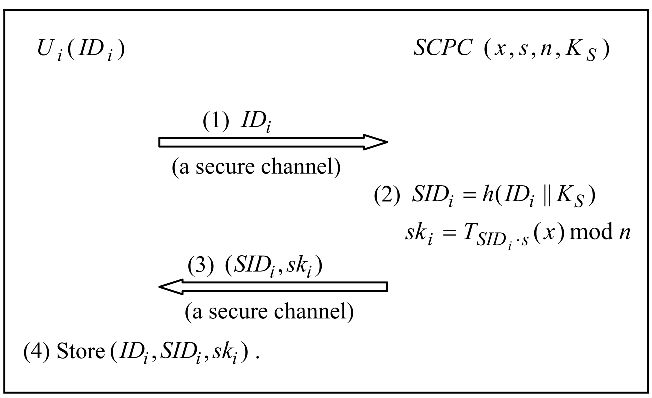

Fig. 2. Registration phase of the proposed scheme.

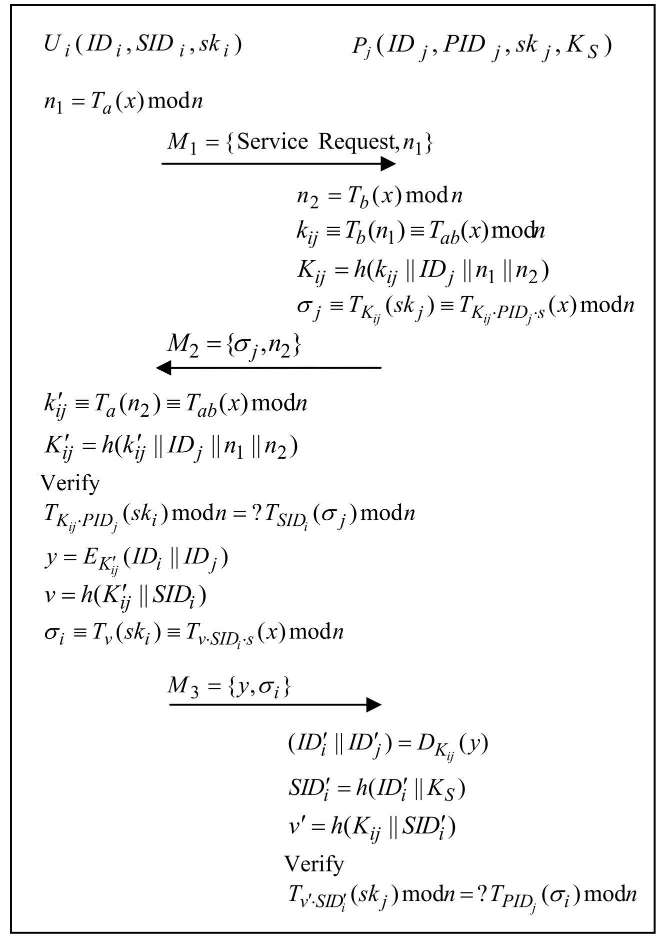

Fig. 3. User identification phase of the proposed scheme.

5) The $SCPC$ stores s as its secret key and publishes parameters $(x, n, T(\cdot))$ and (PID_j).
6) P_j stores its secret keys (K_S, sk_j).

B. Registration Phase

In the registration phase, user U_i registers his/her identity ID_i to enable service provider P_j to authenticate the legitimacy of U_i. Fig. 2 displays the registration phase.

1) Each user U_i registers his/her identity ID_i via a secure channel.
2) The $SCPC$ computes $SID_i = h(ID_i \| K_S)$ and $sk_i = T_{SID_i \cdot s}(x) \bmod n$.
3) The $SCPC$ returns secret tokens (SID_i, sk_i) to U_i via a secure channel.
4) U_i stores its secret keys (ID_i, SID_i, sk_i).

C. User Identification Phase

In the user identification phase, provider P_j authenticates the legitimacy of U_i when U_i wants to access the resources of P_j. Fig. 3 displays the user identification phase.

1) $U_i \to P_j : M_1 = \{\text{Service Request}, n_1\}$
   The U_i selects a nonce a, computes $n_1 = T_a(x) \bmod n$, and sends a service request $M_1 = \{\text{Service Request}, n_1\}$ to P_j.
2) $P_j \to U_i : M_2 = \{\sigma_j, n_2\}$
   Upon receiving M_1 from U_i, P_j selects a nonce b, computes $n_2 = T_b(x) \bmod n$, $k_{ij} = T_b(n_1) \bmod n$, $K_{ij} = h(k_{ij} \| ID_j \| n_1 \| n_2)$, and $\sigma_j \equiv T_{K_{ij}}(sk_j) \equiv T_{K_{ij} \cdot PID_j \cdot s}(x) \bmod n$. Next, P_j sends the message $M_2 = \{\sigma_j, n_2\}$ to U_i.
3) $U_i \to P_j : M_3 = \{y, \sigma_i\}$
   Upon receiving M_2 from P_j, U_i computes $k'_{ij} = T_a(n_1) \bmod n$, $K'_{ij} = h(k'_{ij} \| ID_j \| n_1 \| n_2)$, and verifies σ_j by checking $T_{K'_{ij} \cdot PID_j}(sk_i) \bmod n =?\ T_{SID_i}(\sigma_j) \bmod n$. If unsuccessful, U_i aborts this request. Otherwise, U_i successfully authenticates P_j and makes sure that P_j is an authorized service provider. Then, U_i computes $y = E_{K_{ij}}(ID_i \| ID_j)$, $v = h(K'_{ij} \| SID_i)$, and $\sigma_i \equiv T_v(sk_i) \equiv T_{v \cdot SID_i s}(x) \bmod n$, and sends $M_3 = \{y, \sigma_i\}$ to P_j.
4) Upon receiving M_3 from U_i, if P_j retrieves $(ID'_i \| ID_j)$ by decrypting ciphertext y with K_{ij}, computes $SID'_i = h(ID'_i \| K_S)$, $v' = h(K_{ij} \| SID'_i)$, and validates ID_i by checking $T_{v' \cdot SID'_i}(sk_j) \bmod n =?\ T_{PID_j}(\sigma_i) \bmod n$. If true, P_j successfully authenticates U_i and accepts this

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

service request. Then, P_j and U_i obtain the common session key $k_{ij} = T_{ab}(x) \bmod n$.

IV. Security and Performance Analyses

This section provides security analyses of the proposed scheme and compares its performance with that of other related schemes.

A. Security Analyses

The following descriptions analyze that the proposed authentication scheme provides session key security, mutual authentication, and user anonymity, and withstands privileged insider attacks and stolen-verifier attacks.

The Difference Lemma [38] is made used within our SOG 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

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

1) Session Key Security (AKE Security): The following theorem shows that the proposed scheme has AKE security if the used hash function is secure and the extended chaotic-map-based DDHP holds.

Theorem 1: The probability that an adversary breaks the AKE security of the proposed authentication scheme P

$$\mathrm{Adv}_P^{\mathrm{ake}} \leq \frac{1}{2^{l-1}} + 2 \cdot \mathrm{Adv}^{\mathrm{ddh}}$$

where $\mathrm{Adv}^{\mathrm{ddh}}$ is the advantage that an extended chaotic-map-based DDH attacker solves the extended chaotic-map-based DDHP and l is a secure parameter size.

Proof: Game G_i^{ake} defines the probability of the event E_i that the adversary wins this game. The start game G_0^{ake} is the real attack against the proposed scheme. The final game G_2^{ake} concludes a negligible advantage to break the AKE security of the proposed scheme.

Game G_0^{ake}: This game corresponds to the real attack. By definition, we have

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

Game G_1^{ake}: This game transforms game G_0^{ake} into game G_1^{ake} by using a triple (X, Y, Z) sample from a random distribution $(T_a(x) \bmod p, T_b(x) \bmod p, T_z(x) \bmod p)$, instead of an extended chaotic-map-based DDH triple. Then, G_0^{ake} is equivalent to G_1^{ake}, and we have

$$\Pr[E_0] = \Pr[E_1]. \tag{2}$$

Assume that a challenger $\mathrm{A}_{\mathrm{ddh}}$ tries to violate the indistinguishability of the extended chaotic-map-based DDHP, and an adversary $\mathrm{A}_{\mathrm{ake}}$ is constructed to break the session key security. $\mathrm{A}_{\mathrm{ddh}}$ returns the real key k_{ij} to $\mathrm{A}_{\mathrm{ake}}$ if the flipping unbiased coin bit $c = 1$; otherwise, it returns a random string to $\mathrm{A}_{\mathrm{ake}}$ if $c = 0$. Then, $\mathrm{A}_{\mathrm{ake}}$ outputs its guess bit c' and wins if $c' = c$. $\mathrm{A}_{\mathrm{ddh}}$ returns the output exactly as executing the previous experiment except for (X, Y, Z) that it had received as input. 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, $\mathrm{A}_{\mathrm{ddh}}$ runs $\mathrm{A}_{\mathrm{ake}}$ in G_0^{ake}, and thus, the probability of the event that $\mathrm{A}_{\mathrm{ddh}}$ outputs 1 is equal to the probability of the event E_0. If (X, Y, Z) is a random triple, $\mathrm{A}_{\mathrm{ddh}}$ runs $\mathrm{A}_{\mathrm{ake}}$ in G_1^{ake}, and thus, the probability of the event that $\mathrm{A}_{\mathrm{ddh}}$ outputs 1 is equal to the probability of E_1. Therefore, we have

$$|\Pr[E_0] - \Pr[E_1]| \leq \mathrm{Adv}^{\mathrm{ddh}}(\mathrm{A}_{\mathrm{ddh}}). \tag{3}$$

Game G_2^{ake}: This game transforms game G_1^{ake} into game G_2^{ake}, computing K_{ij} by simply choosing it at random, rather than as a hash. Then, games G_1^{ake} and G_2^{ake} are undistinguishable, except collisions of a hash function in G_2^{ake}. Thus, according to the birthday paradox [35], we have

$$|\Pr[E_1] - \Pr[E_2]| \leq \frac{1}{2^l}. \tag{4}$$

Additionally, since all session keys are random and independent and no information about the value of c is revealed, we have

$$\Pr[E_2] = \frac{1}{2}. \tag{5}$$

By combining (1)–(5) and using Lemma 1, we have

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

Then, the proof is concluded. ■

2) Mutual Authentication:

Theorem 2: Let Adv_P^{ma} denote the advantage in violating the mutual authentication of the proposed scheme P. Then, we have Adv_P^{ma} as negligible, and thus, the proposed scheme provides mutual authentication.

Proof: An adversary breaks mutual authentication (MA security) for the proposed scheme if he/she successfully fakes the authenticator σ_i or σ_j. Assume that an adversary E whose identity is PID_E and has secret key $sk_E = T_{PID_E \cdot s}(x) \bmod n$, and tries to forge an authenticator σ_j^*. Then, the adversary must have the secret K_{ij} and be able to derive either s or $T_s(x) \bmod p$ from PID_E, sk_E, and public information.

Case I: The adversary E tries to derive s from PID_E, sk_E, and public information $T(\cdot)$, x, and p. Assume that $x_0 \equiv T_{PID_E}(x) \bmod p$; then, we have $sk_E \equiv T_{PID_E \cdot s}(x) \equiv T_s(T_{PID_E}(x)) \equiv T_s(x_0) \bmod p$. Given $sk_E \equiv T_s(x_0) \bmod p$, $T(\cdot)$, x_0, and p, finding the integer s' satisfying $sk_E \equiv T_{s'}(x_0) \bmod p$ is computationally infeasible because of the extended chaotic-map-based discrete logarithm problem (DLP). Let $\mathrm{Adv}_{\mathrm{dlp}}$ denote the advantage that an attacker breaks the extended chaotic-map-based DLP. Then, the advantage that an attacker derives the secret key s is bounded on $\mathrm{Adv}_{\mathrm{dlp}}$, and thus, it is negligible.

Case II: The adversary E tries to derive $T_s(x) \bmod p$ from PID_E, sk_E, and public information $T(\cdot)$, x, and p.

Then, finding the integer PID_E satisfying $T_{PID_E^{-1}}(T_{PID_E \cdot s}(x)) \equiv T_s(x) \bmod p$ is computationally infeasible because the extended Chebyshev chaotic maps provide semigroup properties [20]–[23] and it is hard to find a value PID_E^{-1} satisfying $T_{PID_E^{-1}}(sk_E) \equiv T_{PID_E^{-1} \cdot PID_E \cdot s}(x) \equiv T_s(x) \bmod n$. Let $\mathrm{Adv}_{\mathrm{inv}}$ denote the advantage that an attacker violates the extended chaotic-map-based inverse problem. The advantage that an attacker derives $T_s(x) \bmod p$ is bounded on $\mathrm{Adv}_{\mathrm{inv}}$, and thus, it is negligible.

Therefore, the adversary fails to derive s and $T_s(x) \bmod p$ since both $\mathrm{Adv}_{\mathrm{dlp}}$ and $\mathrm{Adv}_{\mathrm{inv}}$ are assumed as negligible. Additionally, by Theorem 1, the advantage that an adversary breaks the AKE security of the proposed scheme P is $\mathrm{Adv}_P^{\mathrm{ake}} \leq (1/2^{l-1}) + 2 \cdot \mathrm{Adv}^{\mathrm{ddh}}$ and is negligible. Then, the adversary fails to obtain the session key K_{ij}. The advantage that the adversary successfully forges an authenticator σ_j^* is bounded on $\mathrm{Adv}_p^{\mathrm{ake}} \cdot (\mathrm{Adv}_{\mathrm{dlp}} + \mathrm{Adv}_{\mathrm{inv}})$. By using similar arguments, we have that the adversary E has difficulty in forging an authenticator σ_i^*, and the advantage is also bounded on $\mathrm{Adv}_p^{\mathrm{ake}} \cdot (\mathrm{Adv}_{\mathrm{dlp}} + \mathrm{Adv}_{\mathrm{inv}})$. Thus, the advantage that the adversary violates the mutual authentication of the proposed scheme is

$$\begin{aligned}\mathrm{Adv}_P^{ma} &\leq 2 \cdot \mathrm{Adv}_p^{\mathrm{ake}} \cdot (\mathrm{Adv}_{\mathrm{dlp}} + \mathrm{Adv}_{\mathrm{inv}}) \\ &\leq 2 \cdot \left(\frac{1}{2^{l-1}} + 2 \cdot \mathrm{Adv}^{\mathrm{ddh}}\right) \cdot (\mathrm{Adv}_{\mathrm{dlp}} + \mathrm{Adv}_{\mathrm{inv}})\end{aligned}$$

and thus is negligible. ■

3) User Anonymity:

Theorem 3: The proposed scheme provides user anonymity.

Proof: In the proposed scheme, y and σ_i implicitly involve the user U_i's identity ID_i, where $y = E_{K_{ij}}(ID_i \| ID_j)$, $\sigma_i \equiv T_v(sk_i) \bmod n$, and $v = h(K'_{ij} \| SID_i)$. The attacker cannot obtain the derived ID_i from y because of the session key security and using secure symmetric cryptosystems such as Triple-DES and AES [35]. Also, they cannot derive ID_i from σ_i due to the extended chaotic-map-based DLP and the one-way property of the hash function. Thus, the proposed scheme provides user anonymity. ■

4) Withstanding Privileged Insider Attacks:

Theorem 4: The proposed scheme withstands privileged insider attacks.

Proof: Assume that a legitimate service provider P_E tries to derive the secret key s of $SCPC$ or the secret key sk_j of other legitimate service provider P_j by using his/her secret key sk_E and public parameters, where $sk_E = T_{PID_E \cdot s}(x) \bmod n$ and $sk_j \equiv T_{PID_j \cdot s}(x) \bmod n$. The arguments are similar with those of Theorem 2. Given $T_{PID_E \cdot s}(x) \equiv T_s(x') \bmod n, T(\cdot)$, x', and p for some $x' \equiv T_{PID_E}(x) \bmod n$, the secret key s cannot be determined since the extended chaotic-map-based DLP cannot be solved in polynomial time. Additionally, the Chebyshev polynomials provide the semigroup property [20]–[23]. Thus, it is hard to find a value PID_E^{-1} satisfying $T_{PID_E^{-1}}(sk_E) \equiv T_{PID_t^{-1} \cdot PID_t \cdot s}(x) \equiv T_s(x) \bmod n$. Then, the advantage that the adversary successfully derives the secret key s or the secret key sk_j is bounded on $(\mathrm{Adv}_{\mathrm{dlp}} + \mathrm{Adv}_{\mathrm{inv}})$, where $\mathrm{Adv}_{\mathrm{dlp}}$ is the advantage that an attacker breaks the extended chaotic-map-based DLP and $\mathrm{Adv}_{\mathrm{inv}}$ is the advantage that an attacker violates the extended chaotic-map-based inverse problem, and thus, it is negligible.

Moreover, a malicious service provider P_E, who has (ID_E, PID_E, sk_E, K_S), tries to impersonate U_i, whose identity is ID_i and secret key is SID_i, and to access the other service provider P_j. Since P_E cannot compute $\sigma_i \equiv T_v(sk_i) \bmod n$ without U_i's secret key sk_i, he/she still cannot correctly send out $M_3 = \{y, \sigma_i\}$. By using the similar arguments of Theorem 2, the advantage that the adversary successfully fakes the authenticator σ_i is bounded on

$$\left(\frac{1}{2^{l-1}} + 2 \cdot \mathrm{Adv}^{\mathrm{ddh}}\right) \cdot (\mathrm{Adv}_{\mathrm{dlp}} + \mathrm{Adv}_{\mathrm{inv}})$$

and is negligible. Hence, a fail login will be detected by some service providers P_j in step 4.

Similarly, using similar arguments, the advantage that a legitimate user derives other legitimate users' secret keys or impersonates other legitimate users to access service providers can be bounded on a negligible probability. Therefore, the proposed scheme withstands the privileged insider attacks. ■

5) Withstanding Stolen-Verifier Attacks:

Theorem 5: The proposed scheme withstands stolen-verifier attacks.

Proof: In the proposed scheme, the service provider does not keep users' secrets in its database. If an adversary A steals a copy of the verifier (ID_j, PID_j, sk_j, K_S) for the service provider P_j and tries to impersonate a user U_i, then he/she cannot compute $y = E_{K_{ij}}(ID_i \| ID_j)$, $v = h(K_{ij} \| SID_i)$, and $\sigma_i \equiv T_v(sk_i) \bmod n$ without ID_i, SID_i, and sk_i. Even though A is able to get ID_i and SID_i by tricking U_i, he/she still cannot correctly compute $\sigma_i \equiv T_v(sk_i) \bmod n$ without U_i's secret key sk_i and send out $M_3 = \{y, \sigma_i\}$. Hence, a fail login will be detected by some service providers P_j in step 4. Thus, the proposed scheme withstands the stolen-verifier attacks. ■

6) Withstanding Replay Attacks:

Theorem 6: The proposed scheme withstands replay attacks.

Proof: The proposed scheme realizes the freshness of communicating messages by using the challenge/response interactive technique [39]–[41]. The user U_i guarantees the freshness of communicating messages by verifying σ_j containing n_1 generated by U_i. Similarly, the provider P_j guarantees the freshness of communicating messages by verifying σ_i containing n_2 generated by P_j. Therefore, the proposed scheme is secure against replay attacks. ■

B. Performance Analyses and Comparisons

Tables II and III compare the performance and the functionality of the proposed scheme with that of comparable schemes, where T_I denotes the time taken to execute a modular multiplicative inverse; T_E denotes the time taken to execute a modular exponentiation; T_M denotes the time taken to execute a modular multiplication; T_S denotes the time taken to execute a symmetric encryption/decryption; T_C denotes the time taken

TABLE II
PERFORMANCE COMPARISON

	Computational cost		Communication cost	
	Computations	Simulat.(ms)	Overhead	Bit length
Yang et al. [14]	$9T_E+2T_S+5T_M+2T_H$	4.74	$3\|N\|+\|ID\|+\|T\|$	3136
Mangipudi-Katti[12]	$12T_E+2T_S+6T_M+4T_H$	6.33	$4\|N\|+\|ID\|+2\|T\|$	4192
Chien [17]	$T_I+8T_E+2T_M+2T_H$	3.91	$4\|N\|+\|T\|$	4128
Hsu-Chuang [18]	$T_I+11T_E+4T_M+4T_H$	5.73	$4\|N\|+\|ID\|+2\|T\|$	4352
Chang-Lee [16]	$9T_E+2T_S+11T_H$	4.30	$2\|N\|+\|ID\|+2\|n\|+4\|R\|+\|H\|$	3392
Wang et al. [19]	$15T_E+2T_S+7T_H$	7.16	$2\|N\|+\|ID\|+2\|n\|+4\|R\|+\|H\|$	3392
Guo-Chang [27]	$5T_S+6T_C+5T_H$	0.36	$2\|n\|+2\|ID\|+2\|T\|+3\|H\|$	1656
Lin [44]	$4T_S+6T_C+5T_H$	0.31	$2n\|+\|ID\|+2\|T\|+3\|H\|$	1624
Proposed scheme	$2T_S+10T_C+5T_H$	0.26	$4\|n\|+2\|ID\|$*$+\|H\|$	2344

*: The bit length is 128 bits by using the AES encryption algorithm.

TABLE III
FUNCTIONALITY COMPARISON

	Computations	Msg.	Used variables	P1	P2	P3
Yang et al. [14]	Heavy	3	3 (k,t,T)	No	No	Yes
Mangipudi-Katti[12]	Heavy	3	3 (k,t,T)	No	No	Yes
Chien [17]	Heavy	3	3 (k,t,T)	No	Yes	Yes
Hsu-Chuang [18]	Heavy	4	2 (k,t)	Yes	No	Yes
Chang-Lee [16]	Heavy	4	5 (n_1,n_2,n_3,k,t)	Yes	No	Yes
Wang et al. [19]	Heavy	4	7(n_1,n_2,n_3,k,t,r,r_1)	Yes	Yes	Yes
Guo-Chang [27]	Low	2	4 (j,f,T_1,T_2)	No	No	No
Lin [44]	Low	2	4 (j,j',T_1,T_2)	No	No	No
Proposed scheme	Low	3	2 (a,b)	Yes	Yes	Yes

P1: No synchronized clocks
P2: Resisting possible attacks
P3: Multiple service providers

TABLE IV
SIMULATION ENVIRONMENT

Hardware/ Software Specification
Service provider P_j
Intel Xeon CPU E3-1231 v3 3.4GHz 3.4GHz
8G Memory
Windows Server 2008
User U_i
Pentium Dual-core CPU E5700 3.0GHz 3.0GHz
6G Memory
Win7
Used Algorithms
Asymmetric en/decryption algorithm: RSA
Symmetric en/decryption algorithm: AES
Extended Chebyshev chaotic maps
Hash function: SHA-1

to compute a Chebyshev polynomial; T_H denotes the time taken to execute a hash operation; T_C approximates T_H [42], [43]; all the bit lengths of the timestamp T, the nonce R, and the identity ID are 32 b; the bit lengths of the large prime numbers, i.e., p, q, and n, are 512 b; the bit length of the composite number N is 1024 b, where $N = p \times q$; the bit length of the hash value is 160 b; and $|X|$ denotes the bit length of X [16]. Table IV lists our simulation environment, including hardware/software specifications and used algorithms.

The schemes of Mangipudi–Katti [12], Yang *et al.* [14], Chang–Lee [16], Chien [17], Hsu–Chuang [18], and Wang *et al.* [19] all involve many time-consuming modular exponential computations and modular multiplicative inverses and thus require much longer simulation time than other schemes. Although the schemes of Guo–Chang [27] and Lin [44] are also developed by using chaotic maps and have fewer messages in transmission and less communication cost, these two schemes use more variables, including nonces and timestamps, and symmetric en/decryptions than the proposed scheme, and are not suitable for the environment of multiple service providers. Additionally, these two schemes [27], [44] and the schemes of Yang *et al.* [14], Hsu–Chuang [18], Mangipudi–Katti [12], and Chien [17] require constructing complicated synchronized clocks in a network environment [39], [41], [45], [46]. The schemes in [12], [14], [16], [18], [27], and [44] fail to resist possible attacks. The proposed scheme, which uses extended chaotic maps, is therefore more efficient than comparable related schemes. Moreover, it requires fewer variables and messages in transmission, and withstands possible attacks.

V. CONCLUSION

This paper has developed an efficient single-sign-on mechanism for distributed computer networks using extended chaotic maps, in which the security is based on the extended chaotic-map-based DLP and DHP. The proposed scheme does not require time-consuming modular exponential computations or scalar multiplications on the elliptic curve. Also, it does not have redundant parameters, requires fewer computations than other schemes, and enables the user and service provider to compute their session key in earlier steps than in other schemes. Therefore, the efficiency of computation and communication is improved. The proposed scheme not only retains the advantages and security properties of previous schemes but also uses fewer variables. What is more, it involves fewer computations and the transmission of fewer messages. The proposed scheme outperforms comparable schemes, and thus, it is suitable for practice environments. In the future, we shall extend the research results in wireless sensor networks, telecare medicine information systems, healthcare information and management systems, and Internet of things.

ACKNOWLEDGMENT

The author would like to thank T. Knoy for his editorial assistance.

REFERENCES

[1] Y. J. Huang, C. C. Yuan, M. K. Chen, W. C. Lin, and H. C. Teng, “Hardware implementation of RFID mutual authentication protocol,” *IEEE Trans. Ind. Electron.*, vol. 57, no. 5, pp. 1573–1582, May 2010.

[2] M. S. Hwang and L.-H. Li, “A new remote user authentication scheme using smart cards,” *IEEE Trans. Consum. Electron.*, vol. 46, no. 1, pp. 28–30, Feb. 2000.

[3] Q. Jiang, J. Ma, G. Li, and L. Yang, “An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks,” *Wireless Pers. Commun.*, vol. 68, no. 4, pp. 1477–1491, Feb. 2013.

[4] C. C. Lee, M. S. Hwang, and I. E. Liao, “Security enhancement on a new authentication scheme with anonymity for wireless environments,” *IEEE Trans. Ind. Electron.*, vol. 53, no. 5, pp. 1683–1687, Oct. 2006.

[5] T. F. Lee, “User authentication scheme with anonymity, unlinkability and untrackability for global mobility networks,” *Security Commun. Netw.*, vol. 6, no. 11, pp. 1404–1413, Nov. 2013.

[6] T. F. Lee and C. M. Liu, “A secure smart-card based authentication and key agreement scheme for telecare medicine information systems,” *J. Med. Syst.*, vol. 37, no. 3, pp. 9933:1–9933:8, Mar. 2013.

[7] X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, “Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards,” *IEEE Trans. Ind. Electron.*, vol. 57, no. 2, pp. 793–800, Feb. 2010.

[8] W. Li, Q. Wen, Q. Su, and Z. Jin, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," *Comput. Commun.*, vol. 35, no. 2, pp. 188–195, Jan. 2012.

[9] W. S. Juang, S. T. Chen, and H. T. Liaw, "Robust and efficient password authenticated key agreement using smart cards," *IEEE Trans. Ind. Electron.*, vol. 55, no. 6, pp. 2551–2556, Jun. 2008.

[10] C. C. Lee, "Two attacks on the Wu–Hsu user identification scheme," *Int. J. Netw. Security*, vol. 1, no. 3, pp. 147–148, Nov. 2005.

[11] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer networks," *Comput. Syst. Sci. Eng.*, vol. 15, no. 4, pp. 211–214, 2000.

[12] K. Mangipudi and R. S. Katti, "A secure identification and key agreement protocol with user anonymity (SIKA)," *Comput. Security*, vol. 25, no. 6, pp. 420–425, Sep. 2006.

[13] T. S. Wu and C. L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks," *Comput. Security*, vol. 23, no. 2, pp. 120–125, Mar. 2004.

[14] Y. Yang, S. Wang, F. Bao, J. Wang, and R. H. Deng, "New efficient user identification and key distribution scheme providing enhanced security," *Comput. Security*, vol. 23, no. 8, pp. 697–704, Dec. 2004.

[15] E. J. Yoon and K. Y. Yoo, "Cryptanalysis of two user identification schemes with key distribution preserving anonymity," in *Proc. 7th Int. Conf. Inf. Commun. Security*, Beijing, China, 2005, pp. 315–322.

[16] C. C. Chang and C. Y. Lee, "A secure single sign-on mechanism for distributed computer networks," *IEEE Trans. Ind. Electron.*, vol. 59, no. 1, pp. 629–637, Jan. 2012.

[17] H. Y. Chien, "Practical anonymous user authentication scheme with security proof," *Comput. Security*, vol. 27, no. 5/6, pp. 216–223, Oct. 2008.

[18] C. L. Hsu and Y. H. Chuang, "A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks," *Inf. Sci.*, vol. 179, no. 4, pp. 422–429, Feb. 2009.

[19] G. Wang, J. Yu, and Q. Xie, "Security analysis of a single sign-on mechanism for distributed computer networks" *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 294–302, Feb. 2013.

[20] P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 52, no. 7, pp. 1382–1393, Jul. 2005.

[21] S. Han, "Security of a key agreement protocol based on chaotic maps," *Chaos Solitons Fractals*, vol. 38, no. 3, pp. 764–768, Nov. 2008.

[22] L. Kocarev and Z. Tasev, "Public-key encryption based on Chebyshev maps," in *Proc. Int. Symp. Circuits Syst.*, 2003, vol. 3, pp. III-28–III-31.

[23] X. Wang and J. Zhao, "An improved key agreement protocol based on chaos," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 12, pp. 4052–4057, Dec. 2010.

[24] X. F. Guo and J. S. Zhang, "Secure group key agreement protocol based on chaotic hash," *Inf. Sci.*, vol. 180, no. 20, pp. 4069–4074, Oct. 2010.

[25] Y. Niu and X. Wang, "An anonymous key agreement protocol based on chaotic maps," *Commun. Nonlinear. Sci. Numer. Simulat.*, vol. 16, no. 4, pp. 1986–1992, Apr. 2011.

[26] K. Xue and P. Hong, "Security improvement on an anonymous key agreement protocol based on chaotic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 7, pp. 2969–2977, Jul. 2012.

[27] C. Guo and C. C. Chang, "Chaotic maps-based password-authenticated key agreement using smart cards," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 6, pp. 1433–1440, Jun. 2013.

[28] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons and Fractals*, vol. 37, no. 3, pp. 669–674, Aug. 2008.

[29] C. C. Lee, C. L. Chen, C. Y. Wu, and S. Y. Huang, "An extended chaotic maps-based key agreement protocol with user anonymity," *Nonlinear Dyn.*, vol. 69, no. 1/2, pp. 79–87, Jul. 2012.

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

[31] A. Kanso, H. Yahyaoui, and M. Almulla, "Keyed hash function based on a chaotic map," *Inf. Sci.*, vol. 186, no. 1, pp. 249–264, Mar. 2012.

[32] D. Xiao, X. Liao, and S. Deng, "A novel key agreement protocol based on chaotic maps," *Inf. Sci.*, vol. 177, no. 4, pp. 1136–1142, Feb. 2007.

[33] D. Xiao, X.-F. Liao, and S.-J. Deng, "Using time-stamp to improve the security of a chaotic maps-based key agreement protocol," *Inf. Sci.*, vol. 178, no. 6, pp. 1598–1602, Mar. 2008.

[34] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *Proc. Adv. Cryptol. Eurocrypt*, 2000, pp. 122–138.

[35] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password-based authenticated key exchange protocols using Diffie–Hellman," in *Proc. Adv. Cryptol. Eurocrypt*, 2000, pp. 156–171.

[36] M. Abdalla, P. A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography*, vol. 3386, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2005, pp. 65–84.

[37] M. Abdalla and D. Pointcheval, "Simple password-based authenticated key protocols," in *Topics in Cryptology—CT-RSA*, vol. 3376, Lecture Notes in Computer Science. Dordrecht, The Netherlands: Springer-Verlag, 2005, pp. 191–208.

[38] V. Shoup, Sequences of Games: A Tool for Taming Complexity in Security Proofs, 2005. [Online]. Available: http://www.shoup.net

[39] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 1999.

[40] S. Suzuki and K. Nakada, "An authentication technique based on distributed security management for the global mobility network," *IEEE J. Sel. Areas Commun.*, vol. 15, pp. 1608–1617, Oct. 1997.

[41] T. F. Lee and T. Hwang, "Provably secure and efficient authentication techniques for the global mobility network," *J. Syst. Softw.*, vol. 84, no. 10, pp. 1717–1725, Oct. 2011.

[42] D. Xiao, X. Liao, and S. Deng, "One-way hash function construction based on the chaotic map with changeable-parameter," *Chaos, Solitons Fractals*, vol. 24, no. 1, pp. 65–71, Apr. 2005.

[43] Z. Y. Cheng, Y. Liu, C. C. Chang, and S. C. Chang, "Authenticated RFID security mechanism based on chaotic maps," *Security Commun. Netw.*, vol. 6, no. 2, pp. 247–256, Feb. 2013.

[44] H. Y. Lin, "Improved chaotic maps-based password-authenticated key agreement using smart cards," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 2, pp. 482–488, Feb. 2015.

[45] D. E. Denning and G. M. Sacco, "Timestamps in key distribution protocols," *Commun. ACM*, vol. 24, no. 8, pp. 533–536, Aug. 1981.

[46] L. Gong, "A security risk of depending on synchronized clocks," *ACM Oper. Syst. Rev.*, vol. 26, no. 1, pp. 49–53, Jan. 1992.

Tian-Fu Lee received the B.S. degree in applied mathematics from the National Chung Hsing University, Taichung, Taiwan, the M.S. degree in computer science and information engineering from the National Chung Cheng University, Chiayi, Taiwan, and the Ph.D. degree from the Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan.

He is an Associate Professor with the Department of Medical Informatics, Tzu Chi University, Hualien, Taiwan. His research interests include cryptography, network security, medical information security, wireless networks, and sensor networks.