Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2012, Article ID 454823, 17 pages
doi:10.1155/2012/454823

Research Article

Applying Semigroup Property of Enhanced Chebyshev Polynomials to Anonymous Authentication Protocol

Hong Lai,[1,2,3] Jinghua Xiao,[1] Lixiang Li,[2,3] and Yixian Yang[2,3]

[1] *School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *Information Security Center, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[3] *National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China*

Correspondence should be addressed to Lixiang Li, li_lixiang2006@yahoo.com.cn

Received 15 May 2012; Accepted 22 June 2012

Academic Editor: Ming Li

We apply semigroup property of enhanced Chebyshev polynomials to present an anonymous authentication protocol. This paper aims at improving security and reducing computational and storage overhead. The proposed scheme not only has much lower computational complexity and cost in the initialization phase but also allows the users to choose their passwords freely. Moreover, it can provide revocation of lost or stolen smart card, which can resist man-in-the-middle attack and off-line dictionary attack together with various known attacks.

1. Introduction

With rapid developments in limits and possibilities of communications and information transmissions, there is a growing demand of authentication protocol, which has greatly spurred research activities in authentication protocols' study. In general, the server authenticates the users by matching the user's identity and password after establishing a secure channel [1]. Since the server establishes a secure channel before asking identity/password information, an attacker can open a connection to a server that does not respond when identity/password information is inquired by the server, which results in the consumption of the resources of the server. Moreover, the attacker can set up many connections and consume all the resources of the server. However, this method is vulnerable to denial of service (DoS) attack and cannot discriminate an impostor who fraudulently obtains access privileges (e.g., user's identity and password) from the real user. Later, Li and Hwang [2]

proposed a biometrics-based remote user authentication scheme using smart cards. Soon, Li et al. [3, 4] improved Li and Hwang's scheme. There is no doubt that most existing authentication protocols only achieve "heuristic" security, that is, the underlying hardness assumptions of these protocols are not perfect. However, we discover the references [5–9], which contain the detection of the DDOS attacks by consuming all, or mostly, the resources of the server can be assured, providing a more hopeful line of investigation for us to future study.

Later, Bellovin and Merritt [10] firstly presented a two-party password authenticated key exchange (2PAKE) protocol which permits a user and a server to establish a session key over an insecure channel to address the problem mentioned above. In their protocol, each user just shares an easy-to-remember password with the trusted server. Regretfully, Patel [11] pointed out that it was easy for an adversary to guess the passwords used for authentication in Bellovin and Merritt's protocol. In order to avoid these attacks, many 2PAKE protocols with weak passwords for authentication have been presented by the researchers [12–18]. However, in these 2PAKE protocols, every user has to share a different password with his/her peer. It is usually rather inconvenient for applications in large-scale communication environments. To surmount this weakness, three-party PAKE (3PAKE) protocols have been proposed in [19–22]. Unlike 2PAKE protocols, 3PAKE protocol is a very practical mechanism to establish secure session key through authenticating each other with a trusted server's help. There are two common weaknesses in these schemes as follows. (1) They needs more communications rounds to reduce computational load. However, as early as in 1995, Gong pointed out that the number of rounds is a key standard for weighing against the performance of a protocol. (2) The sensitive table that stores the shared secret between the server and the designed users will be an attractive target leading to potential server compromise. In 2008, Chen et al. [23] proposed a round and computation-efficient three-party authenticated key exchange protocol, which addressed the above mentioned problems. However, we find that their scheme still exist following four drawbacks. (1) It has computational efficiency problems in initialization phase. (2) User has no choice in choosing his password. (3) It cannot protect user anonymity. (4) There is no provision for revocation of lost or stolen smart card, which is susceptible to man-in-the-middle attack.

Therefore, in this paper, password-based anonymous authentication protocol defined over enhanced Chebyshev polynomials is proposed. A number of outstanding mathematicians and numerical analysts have said that Chebyshev polynomials are everywhere dense in numerical analysis. There is scarcely any area of numerical analysis where Chebyshev polynomials do not drop in like surprise visitors, and indeed there are now a number of subjects in which these polynomials take a significant position in modern developments [24]. One is taken on a journey which leads into all areas of numerical analysis by studying Chebyshev polynomials. Moreover, due to the semigroup property of enhanced Chebyshev polynomials, the well-known discrete logarithm problem and the Diffie-Hellman problem are proved to hold in enhanced Chebyshev polynomials [25]. Thus, we apply semigroup property of enhanced Chebyshev polynomials to present an anonymous authentication protocol. Moreover, our proposed protocol has the following features.

(1) It has much lower computational complexity and cost in the initialization phase.

(2) It allows the users to choose their passwords freely.

(3) It can provide revocation of lost or stolen smart card, which can resist man-in-the-middle attack.

(4) There is no need to find primitive elements, large prime, and even large number.

The rest of this paper is organized as follows. Section 2 gives description of enhanced Chebyshev polynomials and some hard problems based on them. Section 3 briefly reviews Chen et al.'s protocol and describes its disadvantages. In Section 4, we apply semigroup property of enhanced Chebyshev polynomials to design an anonymous authentication protocol. We analyze the security of proposed scheme in Section 5, and computational efficiency analysis is made in Section 6. Finally, we conclude this paper in Section 7.

2. Preliminaries

In this section, we review some basic definitions concerning enhanced Chebyshev polynomials and some hard problems based on the enhanced Chebyshev polynomials [26].

Definition 2.1 (Chebyshev polynomials). The Chebyshev polynomials of degree n are defined as

$$T_n(x) = \cos(n \times \arccos(x)), \quad \{x \mid -1 \leq x \leq 1\}, \tag{2.1}$$

The recurrent formulas are

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x), \tag{2.2}$$

where $n \geq 2$, $T_0(x) = 1$, and $T_1(x) = x$.

The first few Chebyshev polynomials are

$$\begin{aligned} T_2(x) &= 2x^2 - 1, \\ T_3(x) &= 4x^3 - 3x, \\ T_4(x) &= 8x^4 - 8x^2 + 1. \end{aligned} \tag{2.3}$$

It can be identified that Chebyshev polynomial has the following properties:

(1) semigroup property as

$$T_r(T_s(x)) = \cos r * \arccos(\cos(s * \arccos(x))) = \cos rs * \arccos(x) = T_s(T_r(x)) = T_{rs}(x), \tag{2.4}$$

(2) chaotic property,

When $n > 1$, Chebyshev polynomials map $T_n(x) : [-1,1] \rightarrow [-1,1]$ of degree n is a chaotic map with its invariant density as

$$f^*(x) = \frac{1}{\pi\sqrt{1-x^2}}, \tag{2.5}$$

for Lyapunov exponent $\lambda = \ln n > 0$.

Table 1: Some of the notations used in Chen et al.'s protocol.

Symbol	Definition
$\mathrm{ID}_A, \mathrm{ID}_B$	Identities of users A and B, respectively
ID_S	Identity of the authentication server S
p, q, g	The large primes p and q, a generator g of group G with the order q
x, y	The long-term key of S, and $y = g^x \bmod p$
δ_A, δ_B	Components of authentication information V_A and V_B
a, b	Random number privately chosen by A and B, respectively
R_A, R_B	Components of session key, where $R_A = g^a \bmod p$ and $R_B = g^b \bmod p$
$h(\cdot)$	Collision-free one-way hash function
C_{XY}	Evidence generated by user X for user Y

Definition 2.2 (enhanced Chebyshev polynomials). In order to enhance the property of the Chebyshev chaotic map, Zhang [27] proved that the semigroup property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$. This paper uses the following enhanced Chebyshev polynomials:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \pmod N, \tag{2.6}$$

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

$$T_r(T_s(x)) = T_s(T_r(x)) = T_{rs}(x). \tag{2.7}$$

So the semigroup property still holds and the enhanced Chebyshev polynomials also commute under composition.

Definition 2.3 (the discrete logarithm problem (DLP)). DLP is explained by the following. Given an element α, find the integer r, such that $T_r(x) = \alpha$.

Definition 2.4 (the Diffie-Hellman problem (DHP)). DHP is explained by the following. Given an element x, and the values of $T_r(x)$, $T_s(x)$, what is the value of $T_{rs}(x)$?

3. Review of Chen et al.'s Protocol

This section reviews Chen et al.'s protocol (showed in Figure 1). Some of the notations used in this protocol are defined in Table 1.

3.1. Initialization Phase

In this phase, A and B ought to register with S to be legal participants, and S should choose issue secret keys, which will be used in the subsequent phase. Through taking A for an example, S executes the following steps to authorize A:

(1) Randomly choose $1 \leq \delta_A < q$ and calculate $V_A = h(\mathrm{ID}_A, \delta_A)$.

(2) Generate signature (e_A, s_A) as A's self-verified token, where $r_A = g^{\delta_A} \bmod p$, $e_A = h(r_A, \mathrm{ID}_A)$, and $s_A = (\delta_A - xe_A) \bmod q$.

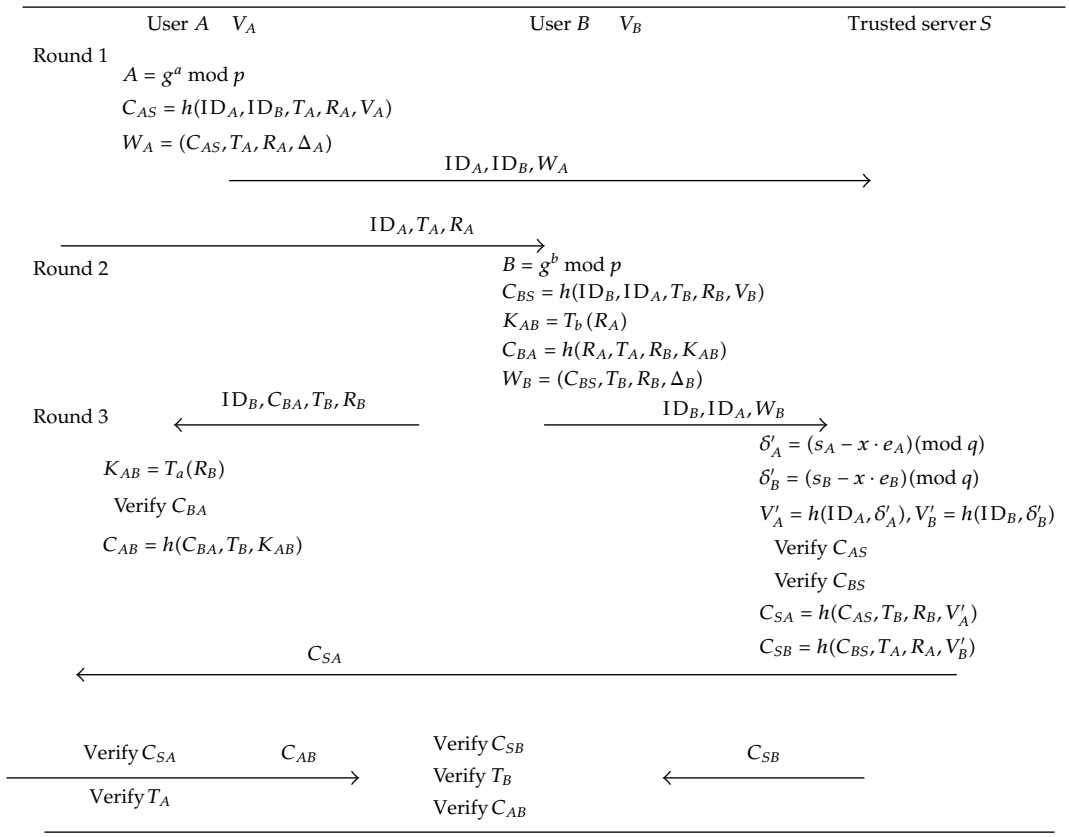

Figure 1: Authenticated key exchange phase in Chen et al.'s protocol.

(3) Store the authentication information $(V_A, (e_A, s_A))$ into a smart card and then deliver it to A in a secure way.

To test whether (e_A, s_A) is authorized by S, A retrieves r'_A as $r'_A = g^{s_A} \cdot y^{e_A} \bmod p$, and then verifies $h(r'_A, \mathrm{ID}_A) \stackrel{?}{=} e_A$.

Similarly, after B obtains the authorization information $(V_B, (e_B, s_B))$ stored in the smart card from S, he can ensure that whether (e_B, s_B) is valid by using the method mentioned above.

3.2. Authentication key Exchange Phase

This phase aims to establish the session key SK with S's help. It just needs three rounds to achieve this goal.

Round 1:

$$\begin{aligned} A &\longrightarrow S : (\mathrm{ID}_A, \mathrm{ID}_B, W_A), \\ A &\longrightarrow B : (\mathrm{ID}_A, T_A, R_A). \end{aligned} \tag{3.1}$$

(1) Randomly choose an integer a and compute $R_A = g^a \bmod p$, $C_{AS} = h(\mathrm{ID}_A, \mathrm{ID}_B, T_A, R_A, V_A)$, then transmits $\mathrm{ID}_A, \mathrm{ID}_B$ and $W_A = (C_{AS}, T_A, R_A, (e_A, s_A))$ to S; where T_A is the time stamp obtained by A from the local clock to ensure the freshness of the message.

(2) A transmits ID_A, T_A and R_A to B.

Round 2:

$$\begin{aligned} &B \longrightarrow S : (\mathrm{ID}_B, \mathrm{ID}_A, W_B), \\ &B \longrightarrow A : (\mathrm{ID}_B, T_B, R_B, C_{BA}). \end{aligned} \tag{3.2}$$

After receiving the message from A, B does the following steps.

(1) Randomly choose an integer b and compute $R_B = g^b \bmod p$, $C_{BS} = h(\mathrm{ID}_B, \mathrm{ID}_A, T_B, R_B, V_B)$, and send $W_B = (C_{BS}, T_B, R_B, (e_B, s_B))$ to S, where T_B is the time stamp obtained by B from the local clock to ensure the freshness of the message.

(2) Calculate the session key $SK = (R_A)^b \bmod p$ and then transmit $C_{BA} = h(T_A, R_A, R_B, SK)$ to A.

Round 3:

$$\begin{aligned} &S \longrightarrow A : C_{SA}, \\ &S \longrightarrow B : C_{SB}, \\ &A \longrightarrow B : C_{AB}. \end{aligned} \tag{3.3}$$

In this round, S does the following steps.

(1) Verify whether T_A is fresher than the one received in the last request. If so, apply x to computing $\delta'_A = (s_A + xe_A) \bmod q$ and $V'_A = h(\mathrm{ID}_A, \delta'_A)$, and then compute $C'_{SA} = h(\mathrm{ID}_A, \mathrm{ID}_B, T_A, R_A, V'_A)$. In the following, test $C'_{AS} \stackrel{?}{=} C_{AS}$ to authenticate the identity of A; if it holds, S calculates $C_{SA} = h(C_{AS}, T_B, R_B, V'_A)$ and transmits it to A.

(2) Test whether T_B is fresher than the one received in the last request. If so, S calculates $V'_B = h(\mathrm{ID}_B, \delta'_B)$ and computes $C'_{BS} = H(\mathrm{ID}_A, \mathrm{ID}_B, T_B, R_B, V'_B)$. Then, check $C'_{BS} \stackrel{?}{=} C_{BS}$ to authenticate the identity of B; if it holds, S calculates $C_{SB} = h(C_{BS}, T_A, R_A, V'_B)$ and transmits it to B.

(3) Independently, A tests whether $(T - T_A)$ is in a valid period, where T is the time when the message transmitted from B after Round 2 was received. If so, A uses the received R_B to compute the session key $SK' = (R_B)^a \bmod p$. Then, it computes $C'_{BA} = h(T_A, R_A, R_B, SK')$ and checks $C'_{BA} \stackrel{?}{=} C_{BA}$ to authenticate B; if it holds, A computes $C_{AB} = h(C_{BA}, T_B, SK')$ and sends it to B.

After this round, A tests whether $(T' - T_A)$ is in a valid period, where T' is the time when C_{SA} was received. If so, A calculates $C'_{SA} = h(C_{AS}, T_B, R_B, V_A)$ and tests $C'_{SA} \stackrel{?}{=} C_{SA}$ to verify the correctness of C_{SA}. If it holds, A finishes this protocol.

Similarly, B tests if $(T'' - T_B)$ is in a valid period, where T'' is the time when C_{SB} was received. If so, B calculates $C'_{SB} = h(C_{BS}, T_A, R_A, V_B)$ and tests $C'_{SB} \stackrel{?}{=} C_{SB}$ to verify the correctness of C_{SB}. If it holds, B completes this protocol.

3.3. Disadvantages of Chen et al.'s Protocol

In this section, we argue that Chen et al.'s scheme still has four disadvantages. The detailed description of the weaknesses is as follows.

3.3.1. Computational Efficiency Problem

In the initialization phase of Chen et al.'s protocol, S has to compute all the authenticated information $(\delta_A, r_A, e_A, s_A)$ for A and $(\delta_B, r_B, e_B, s_B)$ for B. Server has to perform two modular exponentiation operations, which are more expensive than other operations in Chen et al.'s protocol. Hence, it has low efficiency in this phase.

3.3.2. Lack of User Friendliness

In Chen et al.'s scheme, the password is chosen by the server S without the consent of A/B, thus, A/B can only passively accept the password from S. It is not practical for real life applications, such as on-line banking and e-mail subscription. Moreover, $\delta_A/\delta_B \in [1, q]$ chosen by the server could be long and random (e.g., 160 bits), which might be difficult for a registered user A/B to remember easily, and it is most likely that A/B may forget this long and random password if he is not frequently using the system. Hence, Chen et al.'s scheme has lack of user friendliness.

3.3.3. No Protecting User Anonymity

In authenticated key exchange phase of Chen et al.'s scheme, $\mathrm{ID}_A, \mathrm{ID}_B$ are sent to S over insecure channel in the authentication message: $(\mathrm{ID}_A, \mathrm{ID}_B, W_A)$, $(\mathrm{ID}_B, \mathrm{ID}_A, W_B)$. In certain authentication scenarios, such as e-voting and secret online-order placement, it is fairly crucial to protect the privacy of a user. Once an attacker sniffs the communication parties involved in the authentication process, he can easily analyze the transaction being performed by users. Hence, Chen et al.'s scheme fails to provide the user anonymity in the authentication phase.

3.3.4. No Provision for Revocation of Lost or Stolen Smart Card

In case the smart card is lost or stolen, the attacker may impersonate the legal user using the lost or stolen smart card, so there should be a mechanism to ensure that the system can revoke the lost or stolen smart card to avoid the possible attacks. Providing for revocation is also one of the requirements of smart card-based authentication protocols. By keeping

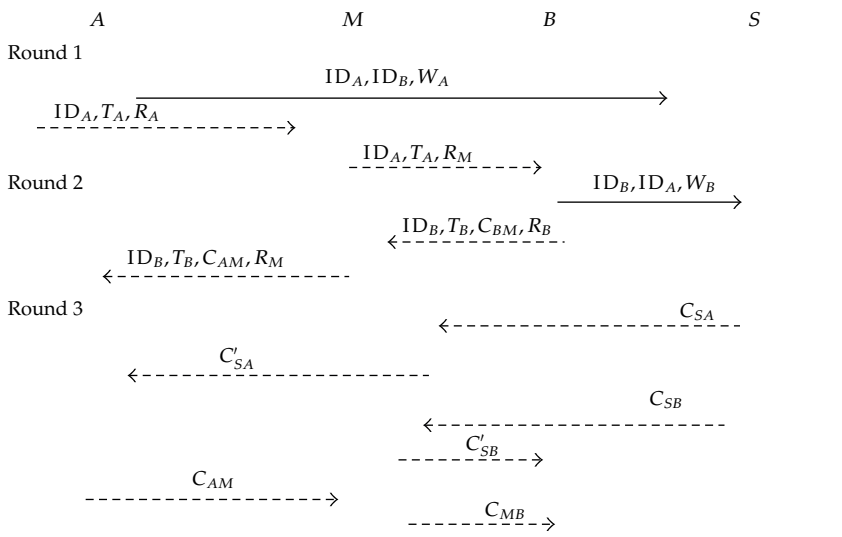

Figure 2: Man-in-the-middle attack in Chen et al.'s protocol.

record of valid card identifier of every registered user, the authentication system can tell the valid card from the invalid one. Regretfully, Chen et al.'s scheme ignored this feature and there is no mechanism to revoke the lost smart card. Moreover, the drawback would become catastrophic if an attacker has got the lost smart card by accident and has revealed the authentication message of a legal user by any means to login into the system for performing secure transaction, such as on-line banking and e-commerce. Thus, Chen et al.'s scheme failed to provide the important feature of smart card-based authentication for revoking the lost smart cards without changing the user's identities.

3.3.5. Man-in-the-Middle Attack

Due to Section 3.3.4, unqualified users can easily launch a man-in-the-middle attack when the smart card is stolen. The steps of the attack is outlined in Figure 2 and explained as follows.

Suppose an adversary M had stolen the smart card from the legal user, then he can obtain the authenticated values V_A and V_B. Let $R_M = g^m \bmod p$ be M's ephemeral public key, and $m \in z_p^*$ is chosen by M. Then, he replaces C_{SA} and C_{SB} with C'_{SA} and C'_{SB} in Round 3. The notation "$\dashrightarrow$" denotes the transmitted message that is manipulated by M. The purpose of M is to share a session key with A by posing as B and to share a session key with B by posing as A. The specific process is as follows.

Round 1:

$$\begin{aligned} A &\longrightarrow S : (\mathrm{ID}_A, \mathrm{ID}_B, W_A), \\ A &\dashrightarrow M(B) : (\mathrm{ID}_A, T_A, R_A), \\ M(A) &\dashrightarrow B : (\mathrm{ID}_A, T_A, R_M). \end{aligned} \tag{3.4}$$

Round 2:

$$\begin{aligned} &B \longrightarrow S : (\mathrm{ID}_B, \mathrm{ID}_A, W_B), \\ &B \dashrightarrow M(A) : (\mathrm{ID}_B, T_B, R_B, C_{BM}). \\ &M(B) \dashrightarrow A : (\mathrm{ID}_B, T_B, R_M, C_{MA}). \end{aligned} \tag{3.5}$$

When receiving the message from $M(A)$, B calculates the session key with $M(A)$, as $SK_{MB} = g^{bm} \bmod p$, $C_{BM} = h(T_A, R_M, R_B, SK_{MB})$, then M calculates the session key with A as $SK_{AM} = g^{am} \bmod p$, $C_{AM} = h(T_A, R_M, R_B, SK_{AM})$.

Round 3:

$$\begin{aligned} &S \dashrightarrow M(A) : C_{SA}, \\ &M(S) \dashrightarrow A : C'_{SA}, \\ &S \dashrightarrow M(B) : C_{SB}, \\ &M(S) \dashrightarrow B : C'_{SB}, \\ &A \dashrightarrow M(B) : C_{AM}, \\ &M(A) \dashrightarrow B : C_{MB}. \end{aligned} \tag{3.6}$$

In this round, because M obtains the value V_A, he can compute $C'_{SA} = h(C_{AS}, T_B, R_M, V_A)$ for mutual authentication with A; similarly, M can also use V_B to calculate $C'_{SB} = h(C_{BS}, T_A, R_M, V_B)$ for mutual authentication with B.

When receiving the values C'_{SA} and C'_{SB}, A and B authenticate the server using their own parameters. Then A computes $C_{MB} = h(C_{BM}, T_B, SK_{AM})$ for $M(B)$, it confirms if C_{MB} is valid from its own knowledge. M calculates $C_{MB} = h(C_{MA}, T_B, SK_{MB})$ and sends it to B to achieve session key agreement.

Finally, M has shared the session key $SK_{AM} = g^{am}\, p$ with A and $SK_{BM} = g^{bm} \bmod p$ with B. In this case, the authenticate mechanism of the Chen et al.'s protocol does not help.

4. An Anonymous Authentication Protocol Using Semiproperty of Enhanced Chebyshev Polynomials

To surmount serious latency security problems in the Chen et al.'s protocol, we apply semigroup property of enhanced Chebyshev polynomials to designing a new anonymous authentication protocol.

4.1. Notations

In the section, we describe some of the notations used in our protocol (Table 2).

Table 2: Some of the notations used in our paper.

Symbol	Definition
$\mathrm{ID}_A, \mathrm{ID}_B$	Identities of users A and B, respectively
ID_S	Identity of the authentication server S
N	The large prime N
x_1, y, n	The long-term key of S, and $y = T_{x_1}(x)$
x	x is the seed of the enhanced Chebyshev polynomial
P_A, P_B	Passwords of A and B, respectively
a, b	Random large integer number chosen by A and B, respectively
R_A, R_B	Components of session key, where $R_A = T_a(x)$ and $R_B = T_b(x)$
$H(\cdot)$	Collision resistant secure one-way chaotic hash function
C_{XY}	Evidence generated by user X for user Y

4.2. Initialization Phase

In this phase, the users and the server need some intercommunication for user's registration.

We take A for an example. To register with S to become a valid user A, A and S will do the following steps.

(1) $A \rightarrow S$: (D_A, ID_A)

A freely chooses an easy-to-remember password P_A and identity ID_A, then computes $D_A = T_{P_A}(x)$ and sends (D_A, ID_A) to S.

(2) When receiving D_A from A, S first tests if $D_A \stackrel{?}{=} D_I$. If $D_A = D_I$, S should ask A to submit a different password.

(3) $S \rightarrow A$: $(\Delta_A, H(\cdot))$

Then, S computes $\Delta_A = E_n(T_{P_A}(x) \| \mathrm{ID}_A)$, for convenience, S stores $(\Delta_A, H(\cdot))$ into a smart card and then delivers it to A face to face.

Of course, B registers with S in the same way.

4.3. Authentication Key Exchange Phase

This phase aims to establish a session key SK. To achieve this goal, A and B first compute $V_A = H(T_{P_A}(y))$ and $V_B = H(T_{P_B}(y))$ using their own passwords and the public key of S as their authentication information respectively. Note that V_A, V_B can be precomputed. This phase also includes three rounds (shown phase in Figure 3) and the detailed descriptions are as follows.

Round 1:

$$\begin{aligned} A &\longrightarrow S : (\mathrm{ID}_A, \Delta_A, W_A) \\ A &\longrightarrow B : (\Delta_A, T_A, R_A). \end{aligned} \tag{4.1}$$

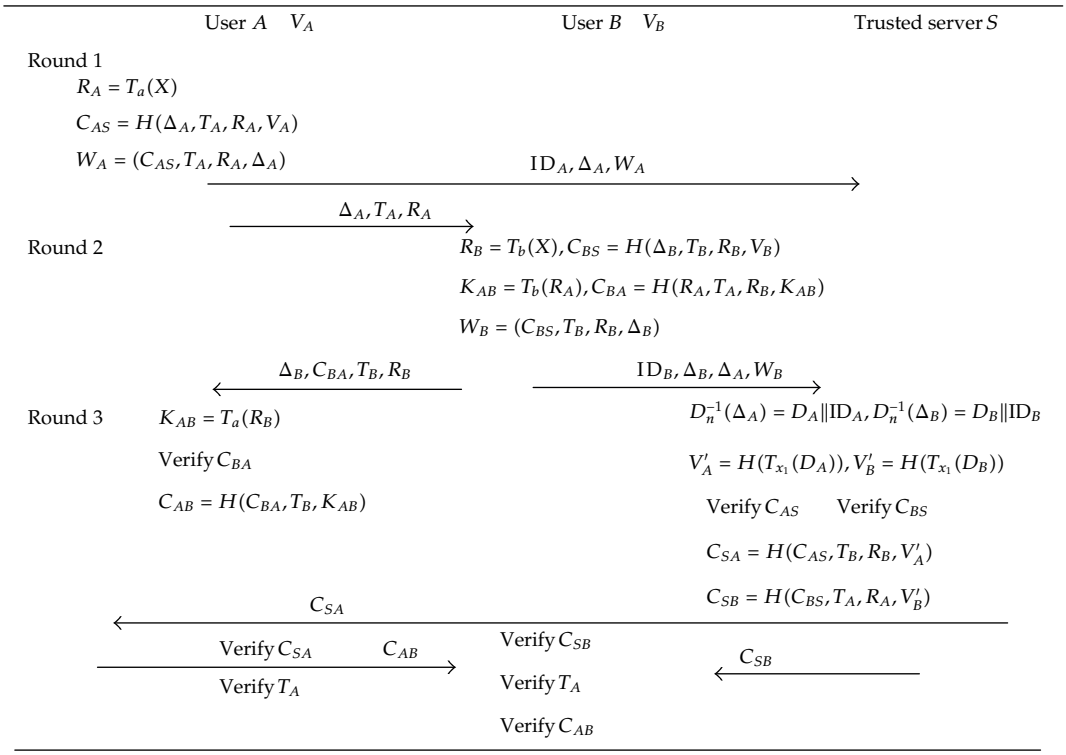

Figure 3: Authenticated key exchange phase in our proposed protocol.

(1) Calculates $C_{AS} = H(\Delta_A, T_A, R_A, V_A)$ and $W_A = (C_{AS}, T_A, R_A, \Delta_A)$, then transmits Δ_A and W_A to S; where the meaning of T_A is the same as that in the Chen et al.'s protocol.

(2) A transmits Δ_A, T_A and R_A to B.

Round 2:

$$\begin{aligned} B &\longrightarrow S : (\mathrm{ID}_B, \Delta_A, \Delta_B, W_B) \\ B &\longrightarrow A : (\Delta_B, T_B, R_B, C_{BA}). \end{aligned} \tag{4.2}$$

On receiving the request transmitted from A, B does the following steps.

(1) B calculates $C_{BS} = H(\Delta_B, T_B, R_B, V_B)$ and sends $W_B = (C_{BS}, T_B, R_B, \Delta_B)$ to S; the meaning of T_B is the same as that in the Chen et al.'s protocol.

(2) B calculates the session key $SK = T_b(R_A)$ and transmits $C_{BA} = H(T_A, R_A, R_B, SK)$ to A.

Round 3:

$$\begin{aligned} &S \longrightarrow A : C_{SA}, \\ &S \longrightarrow B : C_{SB}, \\ &A \longrightarrow B : C_{AB}. \end{aligned} \tag{4.3}$$

In this round, S does the following steps.

(1) Verify if T_A is in a valid time interval. If so, S decrypts Δ_A, Δ_B with his private key n to reveal $T_{P_A}(x)\|\mathrm{ID}_A$ and $T_{P_B}(x)\|\mathrm{ID}_B$. Then, S calculates $V'_A = H(T_{x_1}(D_A))$ and computes $C'_{SA} = H(\Delta_A, T_A, R_A, V'_A)$. Finally, test $C'_{AS} \stackrel{?}{=} C_{AS}$, if it holds, S calculates $C_{SA} = H(C_{AS}, T_B, R_B, V'_A)$ and transmits it to A.

(2) Test whether T_B is in a valid time interval. If so, S calculates $V'_B = H(T_{x_1}(D_B))$ and computes $C'_{BS} = H(\Delta_B, T_B, R_B, V'_B)$. Then, he tests $C'_{BS} \stackrel{?}{=} C_{BS}$, if it holds, S calculates $C_{SB} = H(C_{BS}, T_A, R_A, V'_B)$, and transmits it to B.

(3) Independently, A tests if $(T - T_A)$ is in a valid period, where T is the time when B received the message from S. If so, A calculates $SK' = T_a(R_B)$ and $C'_{BA} = H(T_A, R_A, R_B, SK')$; then, tests $C'_{BA} \stackrel{?}{=} C_{BA}$; if it holds, A calculates $C_{AB} = H(C_{BA}, T_B, SK')$ and sends it to B.

After this round, A tests if $(T' - T_A)$ is in a valid period, where T' is the time when C_{SA} was received. If so, A calculates $C'_{SA} = H(C_{AS}, T_B, R_B, V_A)$ and tests $C'_{SA} \stackrel{?}{=} C_{SA}$ to verify the correctness of C_{SA}. If it holds, A finishes this protocol.

Similarly, B tests if $(T'' - T_B)$ is in a valid period, where T'' is the time when C_{SB} was received. If so, B calculates $C'_{SB} = H(C_{BS}, T_A, R_A, V_B)$ and tests $C'_{SB} \stackrel{?}{=} C_{SB}$ to verify the correctness of C_{SB}. If it holds, B finishes this protocol.

5. Security Analysis

The enhanced scheme is a modified form of the Chen et al.'s scheme. Hence, we just discuss the enhanced and some important security features of the proposed scheme instead of discussing the security analysis that has been already shown in [23]. Before analyzing the security properties, we stress the following two facts to prove security that authenticated key agreement protocol should meet. (1) It is widely believed that there is no polynomial-time algorithm to solve DLP and DHP based on enhanced Chebyshev polynomials with nonnegligible probability. (2) The chaotic hash function has collision-free and irreversible properties.

5.1. Securely Chosen and Update Password

In our proposed scheme, A/B is able to freely choose and change his password without any hassle of contacting the server S. Any users except A/B cannot change or update the password without knowing the corresponding valid $\mathrm{ID}_A/\mathrm{ID}_B$ and P_A/P_B of the smart card holder.

5.2. Revocation of Smart Card

In our proposed scheme, if (A/B)'s smart card is stolen or lost, he can request the server S to revoke his smart card for future use. S can revoke the smart card directly. If an adversary who steals (A/B)'s smart card wants to derive P_A from $\Delta_A = E_n(T_{P_A}(x)\|\mathrm{ID}_A)$, this will be impossible, because just S knows the secret key n, and he is faced with the discrete logarithm problem (DLP) too. Hence, the old smart card becomes useless for future use.

5.3. The Proposed Protocol Can Resist Man-in-the-Middle Attack

Due to $V_A = H(T_{P_A}(y)) = H(T_{x_1}(D_A))$, if the adversary attempts to login to S, it needs to derive x_1/P_A from y/Δ_A. However, it is widely believed that there is no polynomial-time algorithm to solve DLP based on enhanced Chebyshev polynomials with nonnegligible probability. Moreover, because just S knows the secret key n, he even cannot obtain D_A. So the adversary cannot compute V_A. Due to the same reason, the adversary cannot calculate V_B either, that is, our protocol can resist man-in-the-middle attack.

5.4. Protection of User Anonymity

The anonymity feature of users is that the real identity of user should be protected from being revealed by any other entity except S. Our protocol can preserve the identity anonymity for any user which can be explained as follows.

ID_A is hidden in $\Delta_A = E_n(T_{P_A}(x)\|\mathrm{ID}_A)$. Because just S knows the secret key n, even if adversary can obtain Δ_A from the stolen smart card, he still cannot decrypt Δ_A.

5.5. The Proposed Protocol Can Provide Mutual Authentication

Similarly to Chen et al.'s scheme, we analyze this property from three aspects: authentications among A, B, and S.

Case 1. A and B To authenticate A, S needs to suppose that they own the same session key. In this protocol, S is responsible for confirming both the origin and integrity of the received message in step (2) to help them authenticate each other. S ensures that the received messages T_A, R_A, V_A and T_B, R_B, V_B are truly sent from A and B, respectively, and that no modification has occurred. Meanwhile, S sends the respective evidence C_{SA} and C_{SB} for the origin and the integrity of (T_A, R_A) and (T_B, R_B). Based on the premise that S is trustworthy, A/B is convinced that the origin of $(T_B, R_B)/(T_A, R_A)$ is B/A when the validity of C_{SA}/C_{SB} is verified. As only A/B knows the secret a/b of R_A/R_B, the common session key is generated by A/B as $T_a(R_B)/T_b(R_A)$. Because the session key is only known by A/B, no one can forge a valid $C_{BA} = H(T_A, R_A, R_B, SK)$ or $C_{AB} = H(C_{BA}, T_B, SK')$. Therefore, mutual authentication between A and B is achieved while the session key confirmation is guaranteed.

Case 2. A and S To achieve the mutual authentication between A and S, on the one hand, S has to verify the validity of the evidence $C_{AS} = H(\Delta_A, T_A, R_A, V_A)$. On the other hand, A must

test the validity of $C_{SA} = H(C_{AS}, T_B, R_B, V'_A)$ to authenticate S. These evidences are computed with the common secret key. Because only A and S know the common secret key V_A, where V_A equals V'_A, no one can counterfeit the evidence. When validity of C_{AS} and C_{SA} is tested by S and A, respectively, the integrity of the transmitted message from S that contains T_A, R_A is confirmed by S and the integrity of evidence C_{SA} from S is confirmed by A. Thus, mutual authentication between A and S is achieved.

Case 3. B and S The analysis of the mutual authentication between B and S is done likewise. Except B and S, no one knows the secret key V_B. Therefore, mutual authentication between B and S is achieved by verifying the validity of $C_{BS} = H(\Delta_B, T_B, R_B, V_B)$ and $C_{SB} = H(C_{BS}, T_A, R_A, V'_B)$, respectively.

5.6. The Proposed Protocol Can Resist Bergamo et al.'s Attack

In addition, because our protocol is based on semigroup property of enhanced Chebyshev polynomials, we should consider Bergamo et al.'s attack [20]. Bergamo et al.'s attack is based on the condition that an adversary can obtain the related elements $x, N, T_a(x)$ and $T_b(x)$. In the proposed protocol, an attacker could get x and N easily, but they cannot obtain $T_a(x)$ and $T_b(x)$, even though the attacker is a legal user. Besides, the proposed protocol utilizes the enhanced Chebyshev polynomials, in which the periodicity of the cosine function is avoided by extending the interval of x from $(-1, +1)$ to $(-\infty, +\infty)$. Therefore, the attacker have no way to perform a successful attack using Bergamo et al.'s method.

5.7. The Proposed Protocol Can Resist Off-Line Dictionary Attack

In the off-line dictionary attack, the adversary can recode all transmitted messages in the initialization phase and attempt to guess using $A's/B's$ identities $\mathrm{ID}_A/\mathrm{ID}_B$ and passwords P_A/P_B from the recorded massages. An attacker tries to obtain identity and password verification information from Δ_A, he must guess n, P_A, ID_A correctly at the same time. However, the probability of guessing the three numbers correctly in the same attempt is nearly zero. Furthermore, even if the attacker guesses one parameter correctly, he or she cannot verify it with any password verifier information. Hence, the proposed protocol is secure against off-line dictionary attack.

According to the above analysis, we list the security properties' comparison of Chen et al.'s protocol and our protocol in Table 3.

6. Computational Efficiency Analysis

The proposed protocol is achieved through DLP and DHP problems based on enhanced Chebyshev polynomials. It enjoys the following advantages. (1) In the initial phase, we take A for example, S only needs to test $D_A \stackrel{?}{=} D_I$, where D_I denotes the users' component of authentication information and computes Δ_A. However, in Chen et al.'s protocol, S has to compute (V_A, r_A, e_A, s_A). In a word, our protocol greatly reduces the computational complexity and computational cost. Hence, our scheme is more efficient and practical. (2) V'_A, V'_B can be precomputed off-line in our protocol, which improves the computational

Table 3: Comparison of security properties.

Security properties	Chen et al.'s protocol	Our protocol
Anonymity	No	Yes
Man-in-the-middle attack	No	Yes
DoS attack	Yes	Yes
Mutual authentication among three parties	Yes	Yes
Perfect forward secrecy	Yes	Yes
Provision for revocation of lost or stolen smart card	No	Yes
Insider attack	Yes	Yes
User friendliness	No	Yes
Replay attack	Yes	Yes

Table 4: Comparison of computation overhead in initialization phase.

	Chen et al.'s protocol	Our protocol
Random number $(A/B/S)$	$0/0/0$	$1/1/0$
Symmetric encryption/decryption $(A/B/S)$	$0/0/0$	$0/0/2$
Modular exponentiation $(A/B/S)$	$1/1/2$	$0/0/0$
Hash operation $(A/B/S)$	$1/1/4$	$1/1/2$
Chebyshev polynomial computing $(A/B/S)$	$0/0/0$	$1/1/0$

efficiency and saves communication bandwidth. The detailed comparison is shown in Table 4.

7. Conclusion

In this paper, we have applied semigroup property of enhanced Chebyshev polynomials to present a novel authenticated key exchange protocol. To the best of our knowledge, it is the first time to realize three-party authenticated key exchange protocol preserving user anonymity with semigroup property of enhanced Chebyshev polynomials. First, we argued that Chen et al.'s protocol has computational efficiency problem in initialization phase and cannot protect user anonymity, user has no choice in choosing his password, and there is no provision for revocation of lost or stolen smart card leading to man-in-the-middle attack. To surmount these identified drawbacks, we have proposed an enhanced protocol to reduce computational complexity and computational cost in initialization phase and improve security. Hence, our proposed protocol is more efficient and practical. Furthermore, analysis shows that our protocol can resist various kinds of attacks.

Acknowledgments

The authors are grateful to the anonymous referees for their valuable comments and suggestions to improve the presentation of this paper. This work is supported by the National Basic Research Program of China (973 Program) (Grant no. 2010CB923200), the National Natural Science Foundation of China (Grant nos. 61003285, 61121061), the Foundation for the Author of National Excellent Doctoral Dissertation of PR China (Grant no. 200951), the Asia Foresight Program under NSFC Grant (Grant no. 61061040320), and the Specialized Research Fund for the Doctoral Program of Higher Education (Grant no. 20100005110002).

References

[1] T. Dierks, "The transport layer security (tls) protocol version 1.2 s," no. 5246, August 2008, http://www.ietf.org/rfc/rfc5246.txt.

[2] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smartcards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, 2010.

[3] X. Li, J. W. Niu, J. Ma, W. D. Wang, and C. L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 73–79, 2011.

[4] X. Li, Y. P. Xiong, J. Ma, and W. D. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 763–769, 2012.

[5] M. Li and W. Zhao, "A model to partly but reliably distinguish DDOS flood traffic from aggregated one," *Mathematical Problems in Engineering*, vol. 2012, Article ID 860569, 12 pages, 2012.

[6] M. Li, "An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern recognition," *Computers and Security*, vol. 23, no. 7, pp. 549–558, 2004.

[7] M. Li, "Change trend of averaged Hurst parameter of traffic under DDOS flood attacks," *Computers and Security*, vol. 25, no. 3, pp. 213–220, 2006.

[8] M. Li and W. Zhao, "Representation of a stochastic traffic bound," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 9, pp. 1368–1372, 2010.

[9] R. Bettati, W. Zhao, and D. Teodor, "Real-time intrusion detection and suppression in ATM networks," in *Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, Santa Clara, Calif, USA, April 1999.

[10] S. M. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," in *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 72–84, Oakland, Calif, USA, 1992.

[11] S. Patel, "Number theoretic attacks on secure password schemes," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 236–247, 1997.

[12] N. McCullagh and P. S. L. M. Barreto, "A new two-party identity-based authenticated key agreement," in *Topics in Cryptology—CT-RSA 2005*, vol. 3376 of *Lecture Notes in Computer Science*, pp. 262–274, Springer, Berlin, Germany, 2005.

[13] M. Abdalla, D. Catalano, C. Chevalier, and D. Pointcheval, "Efficient two-party password-based key exchange protocols in the UC framework," in *Topics in Cryptology—CT-RSA 2008*, vol. 4964 of *Lecture Notes in Computer Science*, pp. 335–351, Springer, Heidelberg, Germany, 2008.

[14] G. Xie, "Cryptanalysis of Noel McCullagh and Paulo S.L.M. Barretos twoparty identity-based key agreement, Cryptology ePrint Archive," Report 2004/308, 2004, http://eprint.iacr.org/2004/308.

[15] N. McCullagh and P. S. L. M. Barreto, "A new two-party identity-based authenticated key agreement, Cryptology ePrint Archive," Report 2004/122, 2004, http://eprint.iacr.org/2004/122.

[16] J. Kwon, K. Sakurai, and D. Lee, "One-round protocol for two-party verifierbased password-authenticated key exchange," in *Communications and Multimedia Security*, H. Leitold and E. Markatos, Eds., vol. 4237 of *Lecture Notes in Computer Science*, pp. 87–96, Springer, Heidelberg, Germany, 2006.

[17] K. P. Xue and P. L. Hong, "Security improvement on an anonymous key agreement protocol based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, pp. 2969–2977, 2012.

[18] J. Kwon, K. Sakurai, and D. Lee, "One-round protocol for two-party verifierbased password-authenticated key exchange," in *Communications and Multimedia Security*, H. Leitold and E. Markatos, Eds., vol. 4237 of *Lecture Notes in Computer Science*, pp. 87–96, Springer, Heidelberg, Germany, 2006.

[19] O. K. Jeong, I. R. Jeong, K. Sakurai, and D. H. Lee, "Efficient verifierbased password-authenticated key exchange in the three-party setting," *Computer Standards and Interfaces*, vol. 29, pp. 513–520, 2007.

[20] C. L. Lin, H. M Sun, M. Steiner, and T. Hwang, "Three-party encrypted key exchange without server public-keys," *IEEE Communication Letters*, vol. 5, pp. 497–499, 2001.

[21] C. C. Chang and Y. F. Chang, "A novel three-party encrypted key exchange protocol," *Computer Standards and Interfaces*, vol. 26, pp. 471–476, 2004.

[22] D. Wang and X. Wei, "A new key exchange scheme based on extended chebyshev polynomials," in *Proceedings of the 4th WSEAS International Conference on Applied Mathematics and Computer Science*, pp. 1–5, Rio de Janeiro, Brazil, 2005.

[23] T. H. Chen, W. B. Lee, and H. B. Chen, "A round- and computation-efficient three-party authenticated key exchange protocol," *The Journal of Systems and Software*, vol. 81, pp. 1581–1590, 2008.

[24] G. J. Fee and M. B. Monagan, "Cryptography using chebyshev polynomial," Maple Summer Workshop, Burnaby, Canada, 2004, http://oldweb.cecm.sfu.ca/CAG/papers/Cheb.pdf.

[25] H. Tseng, R. Jan, and W. Yang, "A chaotic maps-based key agreement protocol that preserves user anonymity," in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, pp. 1–6, 2009.

[26] E.-J. Yoon and I.-S. Jeon, "An efficient and secure Diffie-Hellman key agreement protocol based on Chebyshev chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 6, pp. 2383–2389, 2011.

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