Identity-based encryption and digital signature schemes using extended chaotic maps

SK Hafizul Islam [a]

Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani, Rajasthan 333 031, India

Abstract

This paper designed a new extended chaotic map-based Identity-based encryption (ECM-IBE) scheme and Identity-based digital signature (ECM-IDS) scheme using extended chaotic maps. The security of the ECM-IBE scheme is based on the hardness assumption of chaotic maps-based decisional DiffieHellman (CDDH) problem, whereas the ECM-IDS scheme is secure based on the difficulties of chaotic maps-based discrete logarithm (CDL) problem.

Keywords: Chaotic maps; Identity-based encryption; Digital signature; Hash function; Diffie-Hellman problem.

1. Introduction

The public key cryptography (PKC) was proposed by Diffie and Hellman [1] in which two keys are used, called private key and public key. The user chooses his private key that is to be kept secret while the corresponding public key is known to all and thus, it needs to be authenticated by a trusted third party, named as a certificate authority (CA). The CA uses a global public key infrastructure (PKI) in order to manage the public keys and certificates. However, in PKI-based scheme, users must have additional computation ability to verify the other's public key certificate. In 1984, Shamir [2] introduce the notion of identity-based cryptography (IBC) in which user's public key is an easily computable function of his email address, physical IP address etc., where the corresponding private key is generated by binding the user's identity with the master secret key of the trusted authority, called private key generator (PKG). The user's private key is given using a secure channel and known to only user and PKG, but its legitimacy can be verified publicly. The IBC avoids the use of public key certificates, so it can save system resources and improve the system efficiency. Thus, IBC seems to be an alternative solution to the PKI-based cryptosystem. After Shamir's work, several ID-based schemes have been proposed, but Boneh and Franklin proposed the scheme satisfying ID-based encryption scheme (IBE) [3] using bilinear pairing over elliptic curve group.

Recently, the extended chaotic maps are extensively studied in cryptography, many schemes [4, 5, 6, 7, 8, 9, 10, 11] have been proposed in cryptography based on extended chaotic maps. This paper designed a new ECM-IBE scheme and ECM-IDS scheme. The security of the ECM-IBE scheme is based on the hardness assumption of CDDH problem, whereas ECM-IDS scheme is secure based on the difficulties of CDL problem.

The paper is organized in the following ways. The Section 2, described the theory and properties of the extended chaotic maps and two computational problems. The Section 3 described the proposed ECM-IBE scheme and its security analysis. The Section 4 described the proposed ECM-IDS scheme and its security analysis. Finally, the Section 5 concludes the paper.

2. Preliminaries

In the following, the description of chebyshev chaotic map and some hard problem are described briefly.

[a]Corresponding author: hafi786@gmail.com, hafizul.ism@gmail.com, Ph.: +91-8797369160

2.1. Chebyshev chaotic maps

Definition 1 (Chaotic map)**.** Let n be an integer x is a real number from the set $[-1, 1]$, the Chebyshev polynomial $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ is defined as [10],

$$T_n(x) = cos(n \cdot cos^{-1}(x)) \tag{1}$$

The recurrence relation of Chebyshev polynomial is defined as:

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

where, $n > 2$, $T_0(x) = 1$, $T_1(x) = x$. Some of other Chebyshev polynomials are $T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$, $T_5(x) = 16x^5 - 20x^3 + 5x$.
The Chebyshev polynomials has the following two interesting properties [11, 12]:

Definition 2 (Semigroup property)**.** The semigroup property of the Chebyshev polynomial $T_n(x)$ is defined as follows:

$$\begin{aligned} T_r(T_s(x)) &= cos(r\, cos^{-1}(cos(s\, cos^{-1}(x)))) \\ &= cos(rs\, cos^{-1}(x)) \\ &= T_{sr}(x) \end{aligned} \tag{3}$$

where r and s are positive integer and $x \in [-1, 1]$. Chebyshev polynomials also satisfy the commutative property under composition as follows:

$$T_r(T_s(x)) = T_s(T_r(x)) \tag{4}$$

In 2005, Bergamo et al. [13] analyzed that that public key cryptography based on the semigroup property of Chebyshev polynomial map is not secure and Zhang [14] demonstrated that semigroup property holds on interval $(-\infty, +\infty)$, which can enhance the property as follows:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \bmod p, n > 2 \tag{5}$$

where $x \in (-\infty, +\infty)$ and p is a large prime. Therefore, the property $T_r(T_s(x)) = T_{sr}(x) = T_s(T_r(x)) \bmod p$ and the semigroup property also holds. The extended Chebyshev polynomials still commute under composition.

Definition 3 (Chaotic property)**.** The Chebyshev map $T_n(x) : [-1, 1] \rightarrow [-1, 1]$ of degree $n > 1$ is a chaotic map with invariant density $f^*(x) = \frac{1}{\pi\sqrt{(1-x^2)}}$ for positive Lyapunov exponent $\lambda = (\ln n) > 0$.

Definition 4 ([15])**.** Let p be a large prime number, $x \in Z_p$ and $m, n \in Z_p^*$, then

$$2 \cdot T_m(x) \cdot T_n(x) \bmod p = T_{m+n}(x) \bmod p + T_{|m-n|}(x) \bmod p \tag{6}$$

2.2. Computational problems

In this section, we described some computational problems based on Chebyshev polynomials, which are assumed to be intractable within polynomial time bound [11].

Definition 5 (Chaotic maps-based discrete logarithm (CDL) problem)**.** For given a random tuple $\langle x, y \rangle$, it is infeasible to find the integer r by any polynomial time bounded algorithm, where $y = T_r(x) \bmod p$.

Definition 6 (Chaotic maps-based Diffie-Hellman (CDH) problem)**.** For given a random tuple $\langle x,\ T_r(x) \bmod p,\ T_s(x) \bmod p \rangle$, it is infeasible to find the $T_{rs}(x) \bmod p$ by any polynomial time bounded algorithm.

Definition 7 (Chaotic-based decisional DiffieHellman (CDDH) problem)**.** For given a random tuple $\langle x, T_r(x) \bmod p,\ T_s(x) \bmod p,\ T_z(x) \bmod p \rangle$, decide whether or not $T_z(x) \bmod p = T_{rs}(x) \bmod p$ by any polynomial time bounded algorithm i.e., decide $z = rs \bmod p$.

3. Proposed ECM-IBE scheme

Based on the extended chaotic map, we proposed a new identity-based encryption scheme (ECM-IBE) in this section.

3.1. Description of ECM-IBE scheme

In the proposed scheme, the the trusted third party, called private key generator (PKG) generates all the system's parameter, *Alice* is the sender and *Bob* is the receiver. The proposed scheme has the following phases: *Setup phase*, *Key extraction phase*, *Encryption phase*, and *Decryption phase*.

3.1.1. Setup phase

(a). *PKG* selects two sufficiently large prime numbers p and q, such that $p = (k \cdot q \pm 1)$, where k is an integer.

(b). *PKG* selects a number $x = g^{(p-1)/q} \bmod p$ for some $g \in Z_p^*$ and a one-way secure hash function $H : \{0,1\}^* \rightarrow Z_q^*$.

(c). *PKG* chooses a number $y \in Z_q^*$ as his/her secret key and computes the corresponding public key as $P_0 = T_y(x) \bmod p$.

(d). *PKG* publishes $\langle p, q, H(\cdot), x, P_0 \rangle$ as system's parameter and keep y secret.

3.1.2. Key extraction phase

Bob selects his/her identity ID_b and sends it to *PKG* over a secure channel. Then the PKG executes the followings:

(a). Choose a number $z_b \in_R Z_q^*$, then compute $Z_b = (T_{z_b}(x) \bmod p) \bmod q$ and $l_b = H(ID_b, Z_b, X_b)$.

(b). Compute $X_b = (T_{|z_b - l_b \cdot y|}(x) \bmod p) \bmod q$ and $d_b = (z_b + l_b \cdot y) \bmod p$.

Now PKG sends the tuple $\langle d_b, Z_b, X_b \rangle$ to ID_b through secure channel. The identity-based private key of ID_b is d_b and the identity-based public key is $Q_b = (T_{d_b}(x) \bmod p) \bmod q$. ID_s validates his private key by checking whether the equation $T_{d_b}(x) \bmod p) \bmod q = 2 \cdot Z_b \cdot (T_{l_b}(P_0) \bmod q) - X_b$ holds. The private key d_b is valid if the above equation holds and vice-versa. Since we have

$$\begin{aligned}
Q_b &= 2 \cdot Z_b \cdot (T_{l_b}(P_0) \bmod q) - X_b \\
&= 2 \cdot (T_{z_b}(x) \bmod p) \bmod q \cdot T_{l_b}(T_y(x) \bmod p) \bmod q - (T_{|z_b - l_b \cdot y|}(x) \bmod p) \bmod q \\
&= 2 \cdot (T_{z_b}(x) \bmod p) \bmod q \cdot (T_{l_b \cdot y}(x) \bmod p) \bmod q - (T_{|z_b - l_b \cdot y|}(x) \bmod p) \bmod q \\
&= (T_{z_b + l_b \cdot y}(x) \bmod p) \bmod q + (T_{|z_b - l_b \cdot y|}(x) \bmod p) \bmod q - (T_{|z_b - l_b \cdot y|}(x) \bmod p) \bmod q \\
&= T_{z_b + l_b \cdot y}(x) \bmod p) \bmod q \\
&= T_{d_b}(x) \bmod p) \bmod q \qquad (7)
\end{aligned}$$

The identity-based public key of Bob is $Q_b = 2 \cdot Z_b \cdot T_{l_b}(P_0) \bmod q - X_b$. After that Bob publishes $\langle ID_b, Z_b, X_b \rangle$.

3.1.3. Encryption phase

Alice selects a message $m \in \{0,1\}^q$ and then executes the followings:

(a). Obtain the information $\langle ID_b, Z_b, X_b \rangle$ of Bob and then compute $l_b = H(ID_b, Z_b, X_b)$.

(b). Compute Bob's public key as $Q_b = 2 \cdot Z_b \cdot T_{l_b}(P_0) \bmod q - X_b$.

(c). Choose a number $\sigma_a \in_R Z_q^*$ and compute $r_a = H(m, \sigma_a)$.

(d). Compute $U_a = (T_{r_a}(x) \bmod p) \bmod q$ and $V_a = \sigma_a \oplus H(T_{r_a}(Q_b) \bmod q)$.

(e). Compute $W_a = m \oplus H(\sigma_a)$ and output the ciphertext $\langle U_a, V_a, W_a \rangle$.

3.1.4. Decryption phase

Upon receiving the ciphertext $\langle U_a, V_a, W_a \rangle$, Bob executes the followings:

(a). Compute $\sigma_a = V_a \oplus H(T_{d_b}(U_a) \bmod p)$.

(b). Compute $m = W_a \oplus H(\sigma_a)$.

(c). Compute $r_a = H(m, \sigma_a)$.

(d). Test $U_a = T_{r_a}(x) \bmod q$, if yes output m and reject the ciphertext otherwise.

3.2. Correctness of the proposed ECM-IBE scheme

Since we have,

$$\begin{aligned} V_a \oplus H(T_{d_b}(U_a) \mod p) &= V_a \oplus H(T_{d_b}(T_{r_a}(x) \bmod q \mod p)) \\ &= V_a \oplus H(T_{r_a}(T_{d_b}(x) \bmod p \mod q) \\ &= V_a \oplus H(T_{r_a}(Q_b) \bmod q) \\ &= \sigma_a \oplus H(T_{r_a}(Q_b) \bmod q) \oplus H(T_{r_a}(Q_b) \bmod q) \\ &= \sigma_a \end{aligned}$$

Therefore, $W_a \oplus H(\sigma_a) = m \oplus H(\sigma_a) \oplus H(\sigma_a) = m$, $r_a = H(m, \sigma_a)$ and $U_a = T_{r_a}(x) \bmod p$.

3.3. Security analysis of the proposed ECM-IBE scheme

According to the the security analysis given in [16], the proposed ECM-IBE scheme is secure based on the difficulties of solving the CDDH problem. Since the secrecy of the scheme relies on the computation of $T_{d_b \cdot r_a}(x) \mod p \mod q = T_{d_b}(T_{r_a}(x) \mod q) \mod p = T_{r_a}(T_{d_b}(x) \mod p) \mod q$. However, the computation of $T_{d_b \cdot r_a}(x) \mod p \bmod q$ from the the public parameter $\langle U_a \bmod q, Q_b \bmod q \rangle = \langle T_{r_a}(x) \mod p \mod q, T_{d_b}(x) \mod p \mod q \rangle$ is computationally difficult by any polynomial time bounded algorithm due to CDH problem.

4. Proposed ECM-IDS scheme

Based on the extended chaotic map, we proposed a new identity-based digital signature (ECM-IDS) scheme in this section.

4.1. Description of ECM-IDS scheme

In this scheme, *Alice* is the signer and *Bob* is the public verifier. The proposed scheme consists of the following phases: *Setup phase*, *Key extraction phase*, *Signing phase*, and *Verification phase*.

4.1.1. Setup phase

(a). *PKG* selects two sufficiently large prime numbers p and q, such that $p = (k \cdot q \pm 1)$, where k is an integer.

(b). *PKG* selects a number $x = g^{(p-1)/q} \bmod p$ for some $g \in Z_p^*$ and a one-way secure hash function $H : \{0,1\}^* \rightarrow Z_q^*$.

(c). *PKG* chooses a number $y \in Z_q^*$ as his/her secret key and computes the corresponding public key as $P_0 = T_y(x) \bmod p$.

(d). *PKG* publishes $\langle p, q, H(\cdot), x, P_0 \rangle$ as system's parameter and keep y secret.

4.1.2. Key extraction phase

Alice selects his/her identity ID_a and sends it to *PKG* over a secure channel. Then the PKG executes the followings:

(a). Choose a number $z_a \in_R Z_q^*$, then compute $Z_a = (T_{z_a}(x) \bmod p) \bmod q$ and $l_a = H(ID_a, Z_a, X_a)$.

(b). Compute $X_a = (T_{|z_a - l_a \cdot y|}(x) \bmod p) \bmod q$ and $d_a = (z_a + l_a \cdot y) \bmod p$.

Now PKG sends the tuple $\langle d_a, Z_a, X_a \rangle$ to ID_a through secure channel. The identity-based private key of ID_a is d_a and the identity-based public key is $Q_a = (T_{d_a}(x) \bmod p) \bmod q$. ID_a validates his private key by checking whether the equation $(T_{d_a}(x) \bmod p) \bmod q = 2 \cdot Z_a \cdot (T_{l_a}(P_0) \bmod q) - X_a$ holds. The identity-based public key of Alice is $Q_a = 2 \cdot Z_a \cdot T_{l_a}(P_0) \bmod q - X_a$. After that Alice publishes $\langle ID_a, Z_a, X_a \rangle$.

4.1.3. Signing phase

Alice selects a message m and then executes the followings:

(a). Choose a number $r_a \in_R Z_q^*$ and compute $R_a = (T_{r_a}(x) \bmod p) \bmod q$.

(b). Compute $h_a = H(m, R_a)$.

(c). Compute $S_a = (T_{r_a + h_a \cdot d_a}(x) \bmod p) \bmod q$.

(d). Compute $L_a = (T_{|r_a - h_a \cdot d_a|}(x) \bmod p) \bmod q$.

(e). Output the signature $\langle Z_a, X_a, R_a, S_a, L_a \rangle$.

4.1.4. Verification phase

Upon receiving the signature $\langle Z_a, X_a, R_a, S_a, L_a \rangle$, Bob executes the followings:

(a). Compute Alice's public key as $Q_a = 2 \cdot Z_a \cdot T_{l_a}(P_0) \bmod q - X_a$, where $l_a = H(ID_a, Z_a, X_a)$.

(b). Compute $h_a = H(m, R_a)$.

(c). Accept the signature if $2 \cdot R_a \cdot T_{h_a}(Q_a) \bmod q = S_a + L_a$, reject otherwise.

4.2. Correctness of the proposed ECM-IDS scheme

Since, we have

$$\begin{aligned} 2 \cdot R_a \cdot T_{h_a}(Q_a) \bmod q &= 2 \cdot (T_{r_a}(x) \bmod p) \bmod q \cdot (T_{h_a}(T_{d_a}(x) \bmod p) \bmod q) \\ &= 2 \cdot (T_{r_a}(x) \bmod p) \bmod q \cdot (T_{h_a \cdot d_a}(x) \bmod p) \bmod q \\ &= (T_{r_a + h_a \cdot d_a}(x) \bmod p) \bmod q + (T_{|r_a - h_a \cdot d_a|}(x) \bmod p) \bmod q \\ &= S_a + L_a \end{aligned}$$

4.3. Security analysis of the proposed ECM-IDS scheme

The proposed ECM-IDS scheme is secure based on the difficulties of solving the CDL problem. It can be seen that $\langle S_a, L_a \rangle = \langle T_{r_a + h_a \cdot d_a}(x), T_{|r_a - h_a \cdot d_a|}(x) \rangle$ cannot be computed from the publicly known value $\langle R_a, T_{l_a}(Q_a) \rangle = \langle T_{r_a}(x), T_{l_a \cdot y}(x) \rangle$. In order to compute $\langle T_{r_a + h_a \cdot d_a}(x), T_{|r_a - h_a \cdot d_a|}(x) \rangle$, the knowledge of r_a and d_a is required. However, the computation of r_a from $R_a = (T_{r_a}(x) \bmod p) \bmod q$ and d_a from $Q_a = (T_{d_a}(x) \bmod p) \bmod q$ are computationally difficult by any polynomial time bounded algorithm due to CDL problem.

5. Conclusion

The author of this paper proposed identity-based encryption (ECM-IBE) scheme an identity-based digital signature (ECM-IDS) scheme with extended chaotic maps. The proposed ECM-IBE scheme is secure against the hardness assumption of CDDH problem and the ECM-IDS scheme is secure based on the difficulties of CDL problem.

References

[1] Diffie, W., Hellman, M.: New directions in cryptography, IEEE Transactions on Information Theory (1976) 22(6): 644-654.

[2] Shamir, A.: Identity-based cryptosystems and signature schemes. In: Proceedings of the Advances in Cryptology (CRYPTO '84), Springer-Verlag, pp. 47-53 (1948).

[3] Boneh, D., Franklin, M. K.: Identity-based encryption from the Weil pairing. In: Proceedings of the Advances in Cryptology (EUROCRYPT '01). LNCS, vol. 2139, Springer-Verlag, pp. 213-229 (2001).

[4] Zhang, L. H.: Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos, Solitons and Fractals (2008) 37: 669-74.

[5] Wang, X. Y., Zhao, J. F.: An improved key agreement protocol based on chaos. Communications in Nonlinear Science and Numerical Simulation (2010) 15: 4052-4057.

[6] Xie, Q., Tu, X.: Chaotic maps-based three-party password-authenticated key agreement scheme. Nonlinear Dynamics (2013) 74: 1021-1027.

[7] Farash, M. S., Attari, M. A.: An efficient and provably secure three-partypassword-based authenticated key exchange protocol based on Chebyshev chaotic maps. Nonlinear Dynamics (2014). DOI 10.1007/s11071-014-1304-6.

[8] Wang, X., Wang, X., Zhao, J.: Chaotic encryption algorithm based on alternant of stream cipher and block cipher. Nonlinear Dynamics (2011) 63: 587-597.

[9] Jye, S.: A speech encryption using fractional chaotic systems. Nonlinear Dynamics (2011) 65: 103-108.

[10] 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.

[11] Guo, Cheng, Chang, C-C.: Chaotic maps-based password-authenticated key agreement using smart cards. Communications in Nonlinear Science and Numerical Simulation (2013) 18: 1433-1440.

[12] Lee, C-C., Lou, D-C., Li, C-T.: An extended chaotic-maps-based protocol with key agreement for multiserver environments. Nonlinear Dynamics (2013). DOI:10.1007/s11071-013-1174-3

[13] Bergamo, P., Arco, P., Santis, A., Kocarev, L.: Security of public key cryptosystems based on Chebyshev polynomials. IEEE Transaction on Circuits and Systems-I (2005) 52: 1382-1393.

[14] Zhang, L.: Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos, Solitons and Fractals (2008) 37(3): 669-674.

[15] Farash, M. S., Attari, M. A.:Cryptanalysis and improvement of a chaotic map-based key agreement protocol using Chebyshev sequence membership testing. Nonlinear Dynamics (2014). DOI 10.1007/s11071-013-1204-1

[16] Shoup, V.: Sequences of Games: A Tool for Taming Complexity in Security Proofs. Technical report 2004/332, IACR (2004). http://eprint.iacr.org/2004/332