Design of identity-based 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

Inspired from the Identity-based cryptosystem proposed by Adi Shamir, and Boneh and Franklin, this paper designed a new Identity-based digital signature (ECM-IDS) scheme using extended chaotic maps. The ECM-IDS scheme is secure based on the difficulties of integer factorization problem.

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

1. Introduction

In the public key infrastructure-based cryptosystems, the public key certificate that is generated and signed by a certificate authority (CA) is required for authentication of the public keys of the entities, and, as a result, it creates a heavy management burden for maintaining and using the public key certificate by developing a global infrastructure. As a remedy, Shamir [1] proposed the concept of an identity-based cryptosystem (IBC) that supports the users' authentication through the use of a public identity. In other words, a user's public key in IBC is computed from an email identity, a social security number, a passport number or other identifiers and a private key generator (PKG); a trusted third party generates the user's private key by using the user's identity and his/her master private key. The private key generated by PKG is communicated to the user through a secure channel, for which its legitimacy can be verified by the user publicly. However, as such, no practical implementation for IBC was proposed by Shamir, and in 2001, Boneh and Franklin [2] first proposed a practical identity-based encryption (IBE) using elliptic curve bilinear pairing. The IBE scheme is secure based on the Bilinear Diffie Hellman (BDH) assumption.

Recently, the extended chaotic maps are extensively studied in cryptography, many schemes [3, 4, 5, 6, 7, 8, 9, 10, 11, 12] have been proposed in cryptography based on extended chaotic maps. In 2004, Fee and Monagan [17] extended the RSA cryptosystem using extended chaotic maps and its security is based on the integer factorization problem (IFP) as in original RSA system. Based on Fee works [1, 2, 17], this paper designed a new ECM-IDS scheme. The security of the ECM-IDS scheme is based on the hardness assumption of IFP problem.

The paper is organized in the following ways. The Section

2. Preliminaries

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

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 [11],

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

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

The recurrence relation of Chebyshev polynomial is defined as:

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

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 [12, 13]:

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:

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

In 2005, Bergamo et al. [14] analyzed that that public key cryptography based on the semigroup property of Chebyshev polynomial map is not secure and Zhang [15] demonstrated that semigroup property holds on interval $(-\infty, +\infty)$, which can enhance the property as follows:

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

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

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

3. Proposed ECM-IDS scheme

Based on the extended chaotic map and the concepts proposed in [1, 2, 17], a new identity-based digital signature (ECM-IDS) scheme is presented in this section.

3.1. 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*.

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* computes $M = pq$ and $L = (p^2 - 1)(q^2 - 1)$.

(c). *PKG* chooses his public key e as $0 < e < M$ and private key as $d = e^{-1} \bmod L$.

(d). *PKG* chooses a one-way secure hash function $H : \{0, 1\}^* \rightarrow Z_M^*$.

(e). *PKG* publishes $\langle M, H(\cdot), e\rangle$ as system's parameter and keep d secret.

3.1.2. Key extraction phase

Alice selects his/her identity ID_a and sends it to PKG over a secure channel. Then the PKG computes Alice's private key as $D_a = T_d(h_a) \bmod M$ and sends it to Alice through secure channel. The identity-based identity-based public key of Alice is $h_a = H(ID_a)$. Alice verifies his private key as

$$\begin{aligned} T_e(D_a) \bmod M &= T_e(T_d(h_a)) \bmod M \\ &= T_{e \cdot d}(h_a) \bmod M \\ &= T_1(h_a) \bmod M \\ &= h_a \end{aligned}$$

3.1.3. Signing phase

Alice selects a message m and then executes the followings:

(a). Choose a number $r_a \in_R Z_M^*$ and compute $R_{a_1} = T_{r_a}(h_a) \bmod M$ and $R_{a_2} = T_{|r_a - l_a|}(h_a) \bmod M$, where $l_a = H(m, R_{a_1})$.

(b). Compute $S_a = T_{(r_a + l_a)}(D_a) \bmod M$.

(c). Output the signature $\langle R_{a_1}, R_{a_2}, S_a \rangle$.

3.1.4. Verification phase

Upon receiving the signature $\langle R_{a_1}, R_{a_2}, S_a \rangle$, Bob executes the followings:

(a). Compute Alice's public key as $h_a = H(ID_a)$.

(b). Compute $l_a = H(m, R_{a_1})$.

(c). Accept the signature if $T_e(S_a) \bmod M = 2 \cdot R_{a_1} \cdot T_{l_a}(h_a) \bmod M - R_{a_2}$, reject otherwise.

3.2. Correctness of the proposed ECM-IDS scheme

Since, we have

$$\begin{aligned} S_a &= T_{(r_a + l_a)}(D_a) \bmod M \\ &= T_{(r_a + l_a)}(T_d(h_a)) \bmod M \\ &= T_{(r_a + l_a) \cdot d}(h_a) \bmod M \end{aligned}$$

Therefore, we have

$$\begin{aligned} T_e(S_a) \bmod M &= T_{e \cdot}(T_{(r_a + l_a) \cdot d}(h_a)) \bmod M \\ &= T_{e \cdot (r_a + l_a) \cdot d}(h_a) \bmod M \\ &= T_{e \cdot d \cdot (r_a + l_a)}(h_a) \bmod M \\ &= T_{(r_a + l_a)}(h_a) \bmod M \\ &= 2 \cdot T_{r_a}(h_a) \cdot T_{l_a}(h_a) \bmod M - T_{|r_a - l_a|}(h_a) \bmod M \\ &= 2 \cdot R_{a_1} \cdot T_{l_a}(h_a) \bmod M - R_{a_2} \end{aligned}$$

3.3. Security analysis of the proposed ECM-IDS scheme

The proposed ECM-IDS scheme is secure based on the difficulties of solving the IFP problem. It can be seen that S_a cannot be computed without $D_a = T_d(h_a) \bmod M$. The computation of D_a is as difficult as the computation of d from e.

4. Conclusion

The author of this paper proposed an Identity-based digital signature (ECM-IDS) scheme using extended chaotic map. The proposed ECM-IDS scheme is secure against the hardness assumption of IFP problem.

References

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

[2] 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).

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

[4] Wang, K., Pei, W., Zhou, L., Cheung, Y., He, Z.: Security of public key encryption technique based on multiple chaotic system. Physics Letters A (2006) 360: 259-262.

[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] Deng, S., Li, Y., Xiao, D.: Analysis and improvement of a chaos-based Hash function construction. Communications in Nonlinear Science and Numerical Simulation (2010) 15(5): 1338-1347.

[11] 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.

[12] 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.

[13] 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

[14] 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.

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

[16] 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

[17] Fee, G. J., Monagan, M. B.: Cryptography using Chebyshev polynomials. In: Proceedings of the Maple Summer Workshop. Wilfrid Laurier University, Waterloo, pp. 1-15, 2004.