International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 7, Issue 8
August 2019.
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395

Received on: 04.08.2019 Published on: 28.08.2019 Pages : 9 - 14

SECURE DIGITAL SIGNATURE AUTHENTICATION SCHEME BASED ON EXTENDED CHEBYSHEV POLYNOMIAL OVER FINITE FIELDS

Dr. R. Varalakshmi
Assistant Professor – TNDALU
swiss_vara@msn.com

Abstract

Digital signature technology is a cryptographic mechanism that uses public key and private key which is very secure and sophisticated technology, and can also be encrypted and/or decrypted. This technology is mainly used for reducing the cost, to save valuable time and speedup of work. The usage of digital signature or the e-signature technology is increasing day by day in banking, insurance, corporate sector as well as in many fields of e-commerce, where the usage of electronic instruments / tools is essential. Therefore, this manuscript reviews different authors works involved in the process of digital signature. In this paper, a secure digital signature authentication scheme which extends Chebyshev polynomials from real field to finite field has been proposed, and it also suggests a trap-door one-way function for better performance.

Keywords: Digital Signature, e-Signature Technology, Cryptographic mechanism, Electronic tools

1.0 Introduction

Authentication of messages protects all the users involved in communication. In circumstances, where there are no comprehensive trust between sender and receiver, something more than authentication is desired. The only solution to this problem is a mathematical scheme named digital signature. The digital signature is comparable to the handwritten signature. A digital signature is valid only if it satisfies the following properties i. It must verify the author and time & date of the signature. ii. It must authenticate the contents at the time of signature. iii. It must be verifiable by the third parties, to resolve disputes. Thus, a digital signature should be in a bit pattern which depends on the message being signed. It must be always easy to produce, recognize and verify a digital signature. It must be computationally infeasible to forge enough a digital signature, either by creating a new message for the present digital signature or by creating a fraudulent digital signature for a certain message. At last, it must be applied to make a recall of a copy of the digital signature in storage for future purpose. A digital signature is to be a part of data which is involved to a message and it can be used to find out if the message was altered during the conversation.

2.0 Literature Survey

Digital signature is a paperless process where an individual person can sign a document or paper with the help of some electronic software, wherein two keys are generated namely public key and private key. From these keys, private key is confidential and is remains with the signatory and public key remains with the software. Both the keys are necessary to use this technology known as cryptographic mechanism. A unique public key system is that both private and public keys are related in such a way that only the public key is used for encryption of messages and the corresponding private key is used for decryption. However, it is virtually impossible to deduce the private key, if you know the public key. This technology was invented by Whitfield Diffie and Martin Hellman in 1976 and also called as asymmetric encryption, because it uses two keys instead of one key (Source: Anonymous, 2016-2019). The Chebyshev polynomials have semi-group property [6-8] on real field R, as well as over integer Z. Section 3 carries with the proposed system preliminaries. Section 3.1 with the proposed Digital Signature Authentication Scheme. Section 3.2 explains the extension of Chebyshev polynomial map over finite fields. Section 3.3 implements a trap-door one-way function based on the extension of Chebyshev polynomial map over finite field. Section 3.4 shows how Public key encryption algorithm is applied on the new trap-door one-way function. Section 4 justifies the security analysis of the proposed scheme. And Section 5 ends with the conclusion.

3.0 Proposed System Preliminaries

It is obvious from the properties of group digital signature, the progress of a public-key scheme depends on finding the outcome of a suitable trap-door one-way function. The trap-door one-way functions definition says that it is easy to calculate the function in one direction and infeasible to calculate the function in the other direction unless and until some of the additional information's are known. A trap-door one-way function is an invertible function, such that

Y= $f_k(X)$ calculation is ease, only if k and x are known

X= $f_k^{-1}(Y)$ calculation is ease, only if k and Y are known

X= $f_k^{-1}(Y)$ calculation is infeasible, only if Y is known but k is not known

3.1 The Proposed Digital Signature Authentication Scheme

In this manuscript, a star-based architecture achieves an authentication of messages using digital signature for a scalable broadcast group efficiently. The architecture is illustrated in fig 1 in which the central node represents the TEK which is used to encrypt data in group communications and known only to the key server. The users U_1….U_n are the various users involved in group communication.

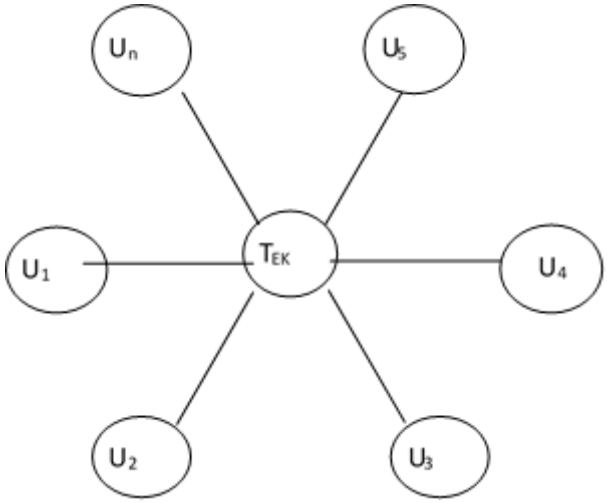

Fig. 1 Star Architecture based Digital Signature

Each peripheral node represents a secret key which is used to decrypt data and held only by an individual member. A new trap-door one-way function based on the extension of Chebyshev polynomials applied to star architecture has been proposed. In this section, a new signature scheme with a trap-door one-way function based on extended Chebyshev map over finite fields is proposed. The proposed signature scheme involves the one-to-one interactions between a signer and a verifier to execute the system initialization phase, the key generation phase, the signature generation phase, and the signature verification phase, described in the upcoming sections.

3.2 Extended Chebyshev polynomial map over finite fields

The Chebyshev polynomials has its semi-group property [6-8] on real field R, as well as over integer Z. Then it also further outspreads the definition field and the value field of Chebyshev polynomials over finite fields ZP, where P is a prime number. Over the finite field ZP it can be said as definite with Chebyshev polynomials as the following.

Let n $\rightarrow$ Z and the variable $x \in Z_P$.

The polynomial $T_n(x) : Z_P \rightarrow Z_P$ can be recursively defined as

$$T_n(x) \equiv (2xT_{n-1}(x) - T_{n-2}(x)) \pmod{P} \qquad n \geq 2 \tag{1}$$

Where $T_0(x) \equiv 1 \pmod{P}$ & $T_1(x) \equiv x \pmod{P}$.

Thus, Chebyshev polynomials over finite field ZP can be derived as the following:

$$T_0(x) \equiv 1 \pmod{P} \qquad T_1(x) \equiv x \pmod{P}$$
$$T_2(x) \equiv (2x^2 - 1) \pmod{P} \quad T_3(x) \equiv (4x^3 - 3x) \pmod{P}$$
$$T_4(x) \equiv (8x^4 - 8x^2 + 1) \pmod{P} \tag{2}$$

$T_n(x)$ is algebraic polynomial, so the following equation becomes:

$$T_n(x) \pmod{P} = T_n(x \pmod{P}) \pmod{P} \tag{3}$$

The semi-group property of the extended Chebyshev polynomials over finite fields[7] is that:

$$T_r(T_s(x \pmod{P})) \pmod{P} = T_{rs}(x) \pmod{P}$$
$$= T_s(T_r(x \pmod{P})) \pmod{P}$$
$$\Rightarrow T_r(T_s(x)) \pmod{P} = T_{rs}(x) \pmod{P}$$
$$= T_s(T_r(x)) \pmod{P} \qquad r, s \in Z \tag{4}$$

3.3 A new trap-door one-way function based on extended Chebyshev polynomials over finite fields.

It is known that the Chebyshev polynomial $T_n(x)$ is written as:

$$T_n(x) \equiv (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0) \pmod{P} \tag{5}$$

In equation (5), gaining $T_n(x)$ given value of n and x is very easy, but gaining n given $T_n(x)$ and x is very difficult, and almost computation is infeasible. The difficulty can be compared with the discrete logarithm problem. When the value of n in equation (5) is equal to that of the value of discrete logarithm, solving n of equation (5) is more difficult and complex than solving the value of discrete logarithm for the presence of other low power elements in equation (5), such as xn-1, xn-2, and so on. So it is understood that equation (5) has a good one-way property in computation. Likewise, Chebyshev polynomials over finite fields also have good one-way property.

In equation (5), the value of n is equal to a trapdoor. If the values of n and x are known, it is easy and fast to compute the value of $T_n(x)$ by using the following fast algorithm. According to semi-group property in equation (4), and the value of $n = s_1^{k_1} \cdot s_2^{k_2} \cdot \cdots \cdot s_m^{k_m}$, $T_n(x)$ can be computed by:

$$T_n(x) \pmod P = T_{s_1}^{k_1}(T_{s_2}^{k_2}(\cdots T_{s_m}^{k_m}(x)\cdots)) \pmod P \quad (6)$$

The number of iterations are $k^1+k^2+\ldots+k^m$. If the value of n isn't known, the one and only possible way is by computing $T_k(x)$ for all k=2,…,n, and to find out whether $T_k(x) = T_n(x)$ is one by one. However, if the value of n is a large number, then it is impossible to do so.

Due to the one-way trapdoor semi-group property of Chebyshev polynomials on finite fields, it can be used to construct public key encryption algorithm and an entity authentication scheme. Because the proposed scheme extends the Chebyshev polynomials between $x \in [-1, 1]$ and $x \in Z_P$, the attack by the way of [7] is invalid to this cryptosystem. Furthermore, it is clear that proposed scheme is more secure than RSA and ElGamal system. Here the assumption that ZP is a finite field and Zn is of integer ring. All the computations of the following are over ZP and Zn.

3.4 Algorithm based on the new trap-door one-way function

For the one-way trapdoor and the semi-group property of Chebyshev polynomials over finite fields, it is used to construct the public key encryption algorithm, which includes three processes: key generation, encryption and decryption.

Parameters and Key generation phase

According to Chebyshev polynomials over finite fields, the key pair generation process is given as:

(1) Select a large integer $SK \in Z_n^*$ and an integer $x \in Z_P^*$ randomly, and then compute $PK = T_{SK}(x)(mod\ P)$.

(2) Let SK be a private key and {x, PK} be public key.

Signature Generation Phase:

To create a signature for the message m,1 < m < n, the signer first hashes the message to obtain h(m). Next, the signer randomly chooses a secret integer r,1 < r < n such that gcd(r,n) = 1. The signer does the following steps.

Assume that the Key server would send message $M \in Z_P^*$ to User, and uses User's public key for encryption of message. The process is that:

(1) Key server selects a larger integer $R \in Z_n^*$ randomly, and uses User's public key {x, PK} to compute the following:

$K1 = T_R(x)(mod\ P)$ and $K2 = T_R(PK)(mod\ P)$.

(2) Key server Computes Cipher text $C = M \cdot K2 \pmod{P}$.

(3) Key server sends encrypted message {C, K1} to User.

Signature Verification Phase:

Verifier confirms the validity of the signature (K, γ,s) by testing the following equation whether it holds the encrypted signature can be decrypted by manager with the group key and can check the hash value that is encrypted with the manager's key. As manager has the key hashed with respect to each member so can say who has generated the signature.

After receiving the sender's encrypted message, the user decrypts it by his private key. The process is that:

(1) User would computes $K2 = T_{SK}(K1)(mod\ P)$.

(2) User decrypts the given message as that: $M = C \bullet (K2)^{-1}\ (mod\ P)$.

From the equation (4), it is known that:

$T_{SK}(K1) \pmod{P} = T_{SK}(T_R(x)) \pmod{P}$

$= T_R(T_{SK}(x)) \pmod{P}$

$= T_R(PK) \pmod{P} = K2$

So the message M can be decrypted correctly.

4.0 Security Analysis

Entity authentication is the process wherein one party is assured of the identity of the second party involved in a protocol, and that the second has actually participated but the time evidence is acquired. This Entity authentication scheme is based on the new trap-door one-door function. This proposed scheme is based on the extension of Chebyshev polynomials, by means of which a user could efficiently authenticate himself to a server in order to log in. Apart from minor implementation details, the scheme also works as follows:

Within Z_p^*, let m$\in Z_n^*$, and denote by $T_s^i(\cdot) \pmod{p}$ the map $T_s(\cdot) \pmod{p}$ iterated i times, i.e.,

$T_s^i(\cdot) \pmod{p} = T_s(T_s(T_s \cdots T_s(\cdot))\cdots) \pmod{p}$

$= T_{s^i}(\cdot) \pmod{p}$.

Setup Phase – Server Side

1. The server generates any random integer r.

2. It then Computes and sends the value $T_r(m) \pmod{p}$ to the user.

Setup Phase – User Side

1. The user then chooses a random integer s.

i-th Authentication Phase

1. The user first computes $T_s^i(m) \pmod{p}$, and authenticates the value of auth= $T_s^i(T_r(m)) \pmod{p}$, and then sends both the values to the server.

2. The server then computes the value of authentication auth$'$ = $T_s^i(T_r(m)) \pmod{p}$ and checks whether auth=auth$'$. Then, if the checks are satisfied, then access is granted (To ensure Security) else access is denied.

5.0 CONCLUSION

The proposed digital signature scheme satisfies the standard security features like anonymity, unforgeability and unlinkability using Chebyshev polynomials on finite fields. The proposed scheme is member independent so that any

member join or leave operations would not affect the signature generation. Consideration on the size is required. Though the cost of signature verification is somewhat more as compared to other standard signature scheme but on the security feature this would be efficient scheme. The proposed scheme includes i. polynomials which have properties of semi-group and recursion over real field, that can be used in constructing a trap-door one-way function for digital signature. The proposed scheme would be safe against many attacks using architecture mentioned. This scheme can be applicable in evoting system, e-cash system, e-commerce applications and many more. Digital signature or e-signature is an ideal tool for the people involved in the process of managing their business. It helps to everyone involved in either e-banking or e-tendering or e-procurement or e-approvals, etc. or any relevant activities of e-commerce, will helps in reducing cost, saving time and utilization of resources more efficiently. It will prove a milestone for people involved in any business / administration or planning of the state / region / country / world.

REFERENCES

1. *Anonymous (2016) Digital Signature. Web-site: https://en.wikipedia.org/wiki/Digital_signature*
2. *Anonymous (2017) Intro to Digital Signatures, web-site : http://www.securedsigning.com/resources/intro-to-digitalsignatures; web-site accessed on 2019*
3. *Anonymous (2017,a) Legal Validity Promoting Use of Digital Signatures, web-site : http://www.elock.com/legalvalidity-promoting-use-of-digital-signatures.php, web-site accessed on 2019*
4. *Anonymous (2017,b) Digital signature solutions for secure e-transactions. Web-site: http://www.elock.com/digital-signature-for-secure-e-transactions.php web-site accessed on 2019*
5. *Margaret Rouse and Michael Cobb (2014) Digital Signature. web-site; http://searchsecurity.techtarget.com/definition/digital-signature; site visited on 2018.*
6. *Kocarev L., Tasev Z., Public-key encryption based on Chebyshev maps, The 2003 IEEE International Symposium on Circuits and Systems Proceedings, 2003. 28-31.*
7. *Pina Bergamo, Paolo D'Arco, Alfredo De Santis, et al., Security of public key cryptosystems based on Chebyshev polynomials, http://citebase.eprints.org, 2004.*
8. *D Xiao, X Liao, G Tang, Chuandong Li. Using Chebyshev chaotic map to construct infinite length hash chains, Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium , 25-28 May 2004, Volume: 1 ,Pages:11-12.*