Multi Message Signcryption Based On Chaos With Public Verifiability

Aditya Kumar, Mohd Mohiuddin Ansari

***Abstract*:** Chaos is one type of complex dynamic behaviour generated by determined nonlinear dynamic systems. Dependency on initial conditions and highly unpredictable nature of chaotic signals lead to novel cryptographic applications. Cryptography and chaos have some common features, the most prominent being sensitivity to parameters' and variables' changes. This paper focuses on multi-message signcryption schemes based on chaoswith public verifiability. In this paper we purpose two signcryption schemes for single and multiple recipients. The purposed schemes use a chaos based multi-key generator to generate multiple keys for signcryption scheme and are publicly verifiable, highly sensitive to the initial conditions, and provide high security due to its chaotic nature.

Index Terms: Chaos, Signcryption, Chebyshev polynomial, Hash function, Keyed Hash Function, Encryption, Signature.

1 INTRODUCTION

Now-a-days, as the computational power of the system and communicational technology are growing rapidly, the demand of highly secured cryptographic system shows its requirement. Chaos is one type of complex dynamic behaviour generated by determined nonlinear dynamic systems, which is greatly sensitive to initial conditions and parameters, and accurate duplication of it is impossible. Therefore, chaotic systems have more useful and practical applications. Generally, in a typical communication system the communication channel is considered to be insecure. Confidentiality, integrity and non-repudiation are the most desirable features of cryptographic system. To achieve these goals, in traditional approaches, the information is digitally signed and then encrypted before transmitting over an unsecure network. The sender signs the message using digital signature scheme and then encrypts the message (and the signature) using a private key encryption algorithm under an encryption key, chosen randomly. The randomly chosen encryption key is then encrypted using the recipient's public key. This two-step approach is called "signature then encryption". In 1997, Y. Zheng combined these two steps into one and purposed a new scheme called "Signcryption"[9]. The idea behind Zheng's scheme is to perform signature and encryption in a single logical step with a cost significantly lower than required by the traditional signature-then-encryption approach.Since 1997, many signcryption schemes have been proposed [3][5][6][7][11].

- Aditya Kumar is currently pursuing masters degree program in Computer Science and Engineering in SET, Sharda University, India, E-mail: aditya_brt@hotmail.com
- Mohd Mohiuddin Ansari is a faculty of engineering in SET, Sharda University, India, E-mail: mohiuddin.ansari@sharda.ac.in

A signcryption scheme should have the following properties:[1]

1. **Correctness:** Any signcryption scheme should be correctly verifiable i.e. signcrypted text formed by signcryption algorithm must be accepted by the unsigncryption algorithm.
2. **Efficiency:** Computational costs and communication costs of signcryption scheme should be less than those best known traditional signature then encryption schemes with the same provided functionality.
3. **Security:** A signcryption scheme should simultaneously fulfil the security attributes such as:
   - **a)** Confidentiality: It should be computationally infeasible for an attacker to observe any partial information of a signcrypted text, without knowledge of the sender's or designated recipient's private key.
   - **b)** Unforgeability: It should be computationally infeasible for an attacker to masquerade a sender to create an authentic signcrypted text that can be accepted by an unsigncryption algorithm.
   - **c)** Non-repudiation: The recipient should be able to prove to a third party that the sender has sent the signcrypted text. This ensures that the sender cannot deny his signcrypted texts.
   - **d)** ntegrity: The recipient should have the ability to verify that the received message is the original one, sent by the sender.
   - **e)** Public verifiability: Any third-party without any practice on the private key of the sender or the recipient can verify that the signcrypted text message is a valid signcryption of its corresponding message.

However, signcryption schemes purposed earlier do not provide public verifiability and non-repudiation. Later, various signcryption schemes with public verifiability have also been purposed [4][8][13].Rapid development in computational power of today's systems increases the demand of highly secure communication systems. During the last years, the study of chaotic system and its possible applications to Cryptography has received considerable attention in a part of the scientific community. Chaotic systems are defined by sensitive dependence on initial conditions, similarity to random behaviour, and accurate duplication of it is impossible. In The last several years increasing efforts have been made to usechaotic systems for enhancing some features of

communications systems. Dependency on initial conditions and highly unpredictable nature of chaotic signals is the most attractive feature of chaotic systems that leads to novel cryptographic applications. Cryptography and chaos have some common features, the most prominent being sensitivity to parameters' and variables' changes.In 2008 H. Elkamchouchi [2] proposed chaos based signcryption scheme for multi messages multi recipient, however the scheme does not provide public verifiability andno significant research has been carried out on chaos based signcryption schemes.In this paper, Chaos based signcryption schemes for multi messages single receipt and multi message multi receipt is proposed. The scheme also provides the public verifiability. The main idea, behind the purposed scheme, is to achieve very high security by using chaotic keys for the encryption algorithm, generated by chaotic key generator. This paper is structured as follows. In second section chebyshev chaotic map is discussed. The third section describes the purposed scheme which includes description of parameters used in purposed scheme, the key generation phase, dynamic chaotic key generator, and multi message signcryption schemes for single recipient and multiple recipients. In the third section analysis of the purposed scheme for the proof of correctness and public verification is performed.

2 CHAOTIC MAP

Chaotic functions were first studied in the 1960's and show numerous interesting properties. Chaos is greatly sensitive to initial conditions and parameters and accurate duplication of it is impossible. Therefore, chaotic systems have more useful and practical applications. Cryptography and chaos have some common features, the most prominent being sensitivity to parameters' and variables' changes. We define here a chaotic system used to generate chaotic keys, based on the Chebyshev polynomial. A very unique property of Chebyshev polynomial is that it is always restricted to the interval [-1 1] even the degree of the polynomial is changed [12]. This property is shown in Fig. 1-Fig. 3 where first few Chebyshev polynomials are shown. This is the property we are interested in and use in the purposed scheme. Chebyshev polynomial map$Tl: R \to R$of degree *l* is defined as

$$T_{l+1} = 2kT_l(k) - T_{l-1}(k) \quad (1)$$

Where $T_0 = 1, T_1 = k, T_2 = 2k^2 - 1, T_3 = 4k^3 - 3k, T_4 = 8k^4 - 8k^2 + 1$.

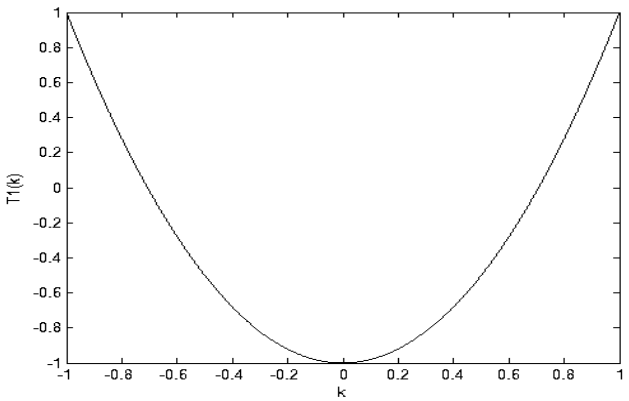

Figure 1. Chebyshev polynomial of degree 1.

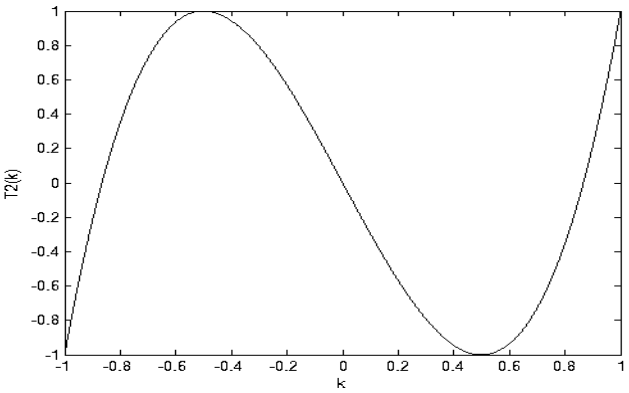

Figure 2. Chebyshev polynomial of degree 2.

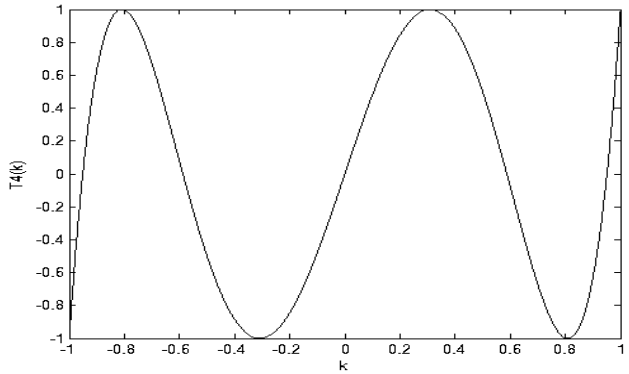

Figure3. Chebyshev polynomial of degree 4.

3 PURPOSED SCHEME

The purposed signcryption scheme consists of four algorithm namely, key generation algorithm, Dynamic chaotickey generator, signcryption algorithm and unsigncryption algorithm. The parameters used in the purposed scheme are:
p: a large prime number.
q: a prime factor of p-1
g: a integer with order $q \ mod \ p$in [1,…,p-1]
n: total numbers of messages.

3.1 Key Generation

The private and public keys of sender and receiver are generated in the following manner:

Pair of sender's key (x_a, y_a) is computed as follow:
x_a: Sender's private keychosen randomly from [1,...,*q*-1]
y_a:Sender's public key computed as:

$$y_a = g^{x_a} \bmod p$$

Pair of sender's keys (x_b, y_b) is computed as follow:
x_b:Receiver's private keychosen randomly from [1,...,*q*-1]
y_b:Receiver's public key computed as:

$$y_b = g^{x_b} \bmod p$$

3.2 Dynamic Chaotic Key Generator (DCKG)

The dynamic chaotic keys generator DCKG(e, k_1, n)proposed here is three tuple, wheree is generated using receiver's public key (y_b) or sender's public key (y_a) and receiver's private key (x_b) (as shown below), k_1 is digest of *e* and *n* is the total number of messages.

$$e = y_b^x \bmod p = (y_a . g^{\sum_{i=1}^{n} r_i})^{s.x_b} \bmod p$$

$$k_1 = hash(e)$$

Suppose sender A wants to send n messages$(m_1, m_2, \dots, m_n)$ to receiver B, he will generate n chaotic keys $(ck_1, ck_2, \dots, ck_n)$for encryption as follow:

a) Represent $k_1$as a number$k_1 \epsilon [-1, 1]$
b) $ck_i = T_e(T_i(ck_{i-1})$ for i= 1,…,n (2)

Where $ck_0 = k_1 \epsilon [-1\ 1]$

The computation of $T_l(k)$ takes linear time in *l*. For the implementation this can be reduced to logarithmic number of steps using the following relation [10]:

$$T_l(k) = \begin{cases} 2.T_{\frac{l}{2}}^2(k) - 1, & l \text{ even} \\ 2.T_{\frac{l-1}{2}}(k).T_{\frac{l+1}{2}}(k) - k, & l\ odd \end{cases} \quad (3)$$

It is recommended to generate a random number *x* such that *e*is a large number (see (4), (18)). User can also change the degree of the polynomial $T_i(k)$ in (2) to achieve higher security, by initiating the system with a large value of *i*.The chaotic keys generated $(ck_1, ck_2, \dots, ck_n)$ by the DCKG is then used by the encryption and decryption algorithms.

3.3 Signcryption Schemes

This section defines two multi messages signcryption schemes. First scheme is defined for the single recipient and the second is defines for the multi recipient. In describing the schemes, we use *hash* or H(.)to denote the one way hash function, KH to denote keyed one way hash function, DCKG to denote dynamic chaotic key generator and (E, D) to denote private key encryption and decryption algorithm.

3.3.1 Multi MessageSingle Recipient Signcryption Scheme

The Graphic representation of the scheme is shown in Fig.4. To signcrypt the n messages, a user calculates n chaotic keys ($ck_1, ck_2, \dots, ck_n$) used to encrypt the n messages($m_1, m_2, \dots, m_n$) and then creates signature on n messagesusing his private key(x_b).*n* chaotic keys are generated using DCKG which takes 3 input *e* (see(4)), k_1(see (5)), and *n*total number of messages.The signcryption algorithm is as follow:

Signcryption algorithm:

1. Compute $e = y_b^x \bmod p$ (4)
2. Compute$k_1 = hash(e)$ (5)
3. Calculate$k_2 = hash(g^x \bmod p)$ (6)
4. For n messages compute n chaotic keys using:

$$(ck_1, ck_2, \dots, ck_n) = DCKG(e, k_1, n) \quad (7)$$

5. Compute cipher text $(c_1, c_2, \dots, c_n)$using encryption algorithm underchaotic keys $(ck_1, ck_2, \dots, ck_n)$ as follow:

$$c_i = E_{cki}(m_i) \text{for } i = 1,...,n \quad (8)$$

6. Compute keyed hash values (r1, r2,…, rn) for n messages using k_2 as follow:

$$r_i = KH_{k2}(m_i) \text{for } i = 1,...,n \quad (9)$$

7. Compute multi message signature using:

$$s = x(x_a + \sum_{i=1}^{n} r_i)^{-1} \bmod q \quad (10)$$

Sender sends signcrypted text $(c_i, r_i, s)$to receiver

On the receiver side, receiver can recover k_1 , k_2 ande successfully by using sender's public key and his private key (see (13), (14) and (12), respectively). Receiver then computes the chaotic keys to decrypt the messages and recover the plain messages. He then checks the integrity of the messages by computing keyed hash values of decrypted messages under k_2 and comparing it to the received keyed hash values ($(r_1, r_2, \dots, r_n)$.The unsigncryption algorithm is as follow:

Unsigncryption algorithm:

1. Calculate $t = (y_a . g^{\sum_{i=1}^{n} r_i})^s \bmod p$ (11)
2. Calculatee $= t^{xb} \bmod p$ (12)
3. Calculate $k_1 = hash(e)$ (13)
4. Calculate $k_2 = hash(t)$ (14)
5. For n messages compute n chaotic keys using $(ck_1, ck_2, \dots, ck_n) = DCKG(e, k_1, n)$ (15)
6. Recover messages using $m_i = D_{cki}(c_i) \text{for } i = 1,...,n$ (16)
7. Accept if $KH_{k1}(m_i) = r_i \text{for } i = 1,...,n$ (17)

3.3.2 Multi Message Multi Recipient Signcryption Scheme

Let the total numbers of receivers be*v*. For a receiver B_j, his key pair is (x_b^j, y_b^j) for j=1,…,*v*the sender calculates e^jusing the jth user public key y_b^j and k_1^j using the one way hash function over ej. He then computes n chaotic keys $(ck_1^j, ck_2^j, \dots, ck_n^j)$ to encrypt n messages $(m_1, m_2, \dots, m_n)$for the jth receiver. The sender then signs the n messages using his private key (x_a) and sends the signcrypted text to receiver j. The signcryption algorithm is as follow:

Signcryption algorithm:

1. Calculate $e^j = (y_b^j)^x \bmod p$ (18)
2. Calculate $k_1^j = hash(e^j)$ (19)
3. Calculate $k_2 = hash(g^x \bmod p)$ (20)
4. for i =1,…,n

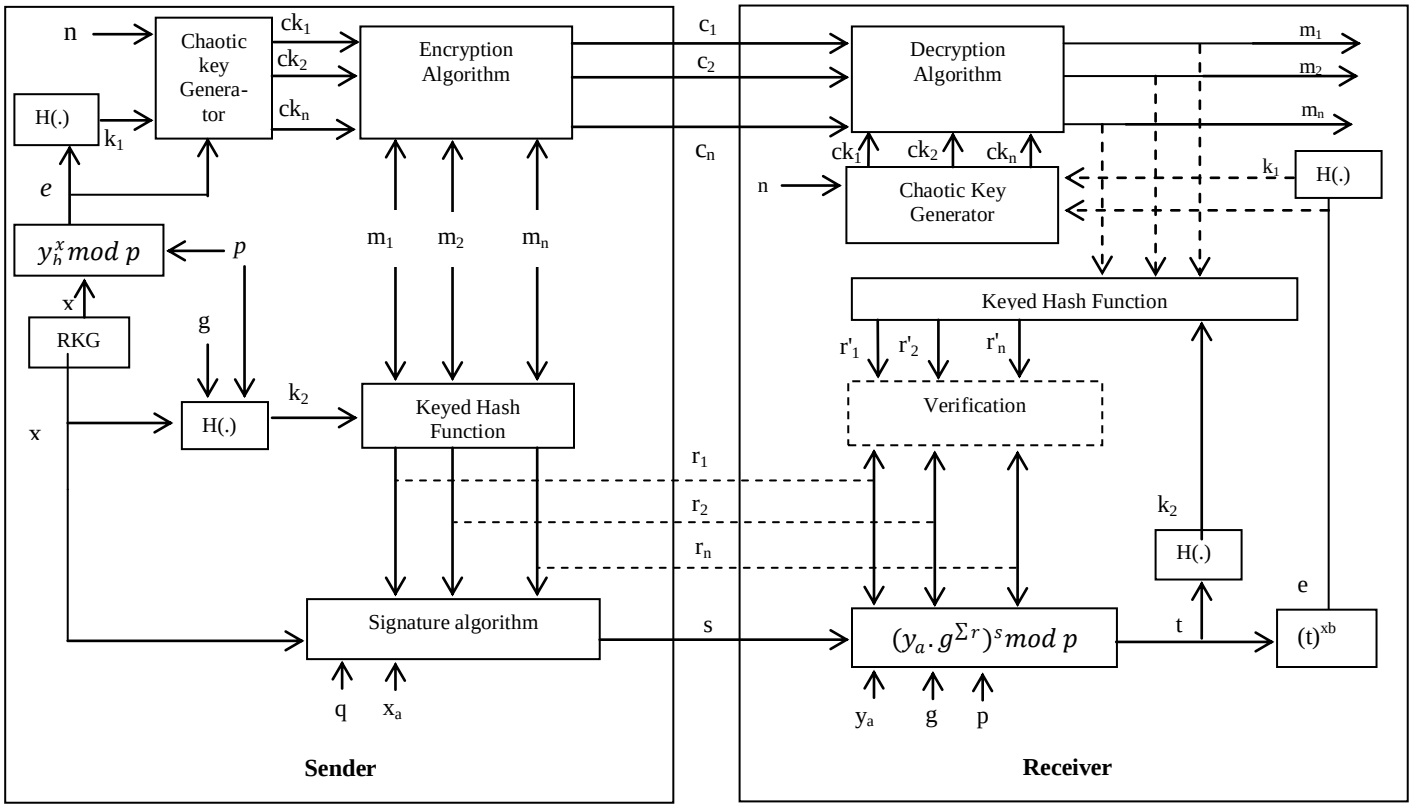

Figure 4. A multi message signcryption scheme with single recipient

a. $ck_i^j = DCKG(e^j, k_1^j, n)$ (21)
b. $c_i^j = E_{ck_i^j}(m_i)$ (22)
c. $r_i = KH_{k2}(m_i)$ (23)

5. $s = x(x_a + \sum_{i=1}^{n} r_i)^{-1} \bmod q$ (24)

Sender sends signcrypted text (c_i^j, r_i, s) to receiver j.

The jth receiver recovers the parameters e^j, k_1^j and k_2 (see (26), (27)and (28) respectively) using his private key (x_b^j) and sender's public key (y_a) and computes chaotic keys $(ck_1^j, ck_2^j, \dots, ck_n^j)$ to decrypt the messages. After decrypting the messages, he then checks the integrity of the messages by computing keyed hash values of decrypted messages under k_2 and comparing it to the received keyed hash values$(r_1, r_2, \dots, r_n)$. The unsigncryption algorithm is as follow:

Unsigncryption algorithm:

1. Calculate $t = (y_a . g^{\sum_{i=1}^{n} r_i})^s \bmod p$ (25)
2. Calculate $e^j = t^{x_b^j} \bmod p$ (26)
3. Calculate $k_1^j = hash(e^j)$ (27)
4. Calculate k2 = hash (t) (28)
5. For i = 1,…,n
   a. $ck_i^j = DCKG(e^j, k_1^j, n)$ (29)
   b. $m_i = D_{ck_i^j}(c_i)$ (30)
   c. Accept if$KH_{k2}(m_i) = r_i$ (31)

4 Analysis of Purposed Scheme

The purposed scheme is analyzed for its correctness and the public verifiability as follow:

4.1 Correctness of the Purposed Scheme

Messages $(m_1, m_2, \dots, m_n)$can be recovered on receiver's B_j side, for j=1,…,*v*, if the signcrypted text is generated honestly by the sender, as the jth receiver can recover the parameters $e^j, k_1$by using his private key (x_b^j) and sender's public key (y_a) and can compute chaotic keys $(ck_1, ck_2, \dots, ck_n)$which are used to decrypt the encrypted messages. jth user can recover e^j and $k_1^j$by using (26) and (27), since

1) $e^j = t^{x_b^j} \bmod p$
$= (y_a . g^{\sum_{i=1}^{n} r_i})^{s.x_b^j} \bmod p$
Since, $t = (y_a . g^{\sum_{i=1}^{n} r_i})^s \bmod p$
$= (g^{x_a} . g^{\sum_{i=1}^{n} r_i})^{s.x_b^j} \bmod p$
$= (g^{x_a + \sum_{i=1}^{n} r_i})^{s.x_b^j} \bmod p$
$= (g^{x_b^j . (x_a + \sum_{i=1}^{n} r_i)})^s \bmod p$
$= (y_b^j)^{(x_a + \sum_{i=1}^{n} r_i).s} \bmod p$
$= (y_b^j)^x \bmod p$
= value generated on sender's side
Since, $s = x(x_a + \sum_{i=1}^{n} r_i)^{-1} \bmod q$

2) $k_1^j = hash(e^j)$

4.2 Nonrepudiation and public verifiability

If the sender A denies his signcrypted text, the receiver B_j can prove the dishonesty of the sender by sending data (mi, ri, s) for i = 1,…,n , to trusted third party(TTP) who can verify the origin of the message by calculating key k2 using senders public key (ya). TTP then calculate keyed hash values of messages and match them with received keyed hash values

(ri) to verify the origin of the messages. The TTP performs the following steps:

1. Calculate $k_2 = \text{hash}((y_a . g^{\sum_{i=1}^{n} r_i})^s \bmod p)$
2. Check whether $KH_{k2}(m_i) = r_i$ to ensure if the origin of the messages is sender A.

This verifiability does not affect the confidentiality of the scheme, since the third party does not need sender's or receiver's private key to verify signature. Thus the purposed scheme provides public verifiability.

5 CONCLUSION

In this paper, new multi message chaos based signcryption schemes are proposed for both single and multi recipient. The purposed schemes achieve the public verifiability. This signifies that the signature of the sender can be verified publicly without the knowledge of sender's or receiver's private key. The main idea behind the purposed scheme is to develop a chaotic key generator whichgenerates chaotic keys for the encryption and decryptionphases. Due to chaotic nature of the keys, it provides very high security. A user can also increase the strength of chaotic keys by using large degree of polynomials. However, large degree of polynomial may affect the efficiency of the system in some cases in comparison to non-chaotic signcryption schemes; but on the other hand,it increases the strength of chaotic keysand therefore the strength of signcrypted text which is highly desirable when the high computational power systems are being used.

ACKNOWLEDGEMENT

The author(s) would like to thankfaculty members andother contributor for their very useful advises.

REFERENCES

[1] M.Toorani, A. Beheshti, "Cryptanalysis of an Elliptic Curve-based Signcryption Scheme," International Journal of Network Security, Vol.10, No.1, PP.51-56, Jan 2010.

[2] Dalia H. Elkamchouchi: "A Chaotic Public Key Multi-Message Multi-Recipients Signcryption Scheme (CPK-MM-MR-SS),"12th World Multi-Conference on Systemics, Cybernetics and Informatics: (WMSCI), 2008

[3] M. Elkamchouchi, A-A. M. EmarahEsam A. A. Hagras: "Public Key Multi-Message Signcryption (PK-MMS) Scheme For Secure Communication Systems," Fifth Annual Conference on Communication Networks and Services Research(CNSR), 2007

[4] H. Elkamchouchi, Mohammed Nasr, and R. Ismail, "A New Efficient Multiple Messages Signcryption Scheme with Public Verifiability," L. Qi (Ed.): FCC 2009, CCIS 34, pp. 193–200, 2009.

[5] Benoit Libert, J- J.Quisquater: "A new identity based signcryption scheme from pairing," IW2003, Paris, France, March 31 -April 4, 2003, paper 11.3.4, p. 109.

[6] Y. Zheng, H. Imai, "How to construct efficient Signcryption Schemes on elliptic curves," Proc. of IFIP/SEC'98, Chapman & Hall, 1998

[7] Yuliang Zheng, "Efficient Signcryption Schemes on Elliptic Curves," Advances in cryptology, Vol.10, pp.15-19, 2000.

[8] Yiliang Han, XiaolinGui, "Multi-recipient Signcryption for Secure Group Communication,"Industrial Electronics and Applications, 2009 ICIEA 2009. 4th IEEE conference on, pp. 161-164, 25-27 May 2009

[9] Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)," Advances in Cryptology - Crypto'97, LNCS 1294, Springer, pp. 165-179, 1997

[10] Fateman, R.J, "Lookup tables, recurrences, and complexity," In Proc. Int. Symp. Sym-bolic and Algebraic Computation. ISSAC, pp. 68–73, 1989

[11] Y. Zheng, "Signcryption and its applications in efficient public key solutions," Proceeding of ISw97, pp. 291-312,1998.

[12] LjupcoKocarev , ShiguoLian (Eds.), Chaos-Based Cryptography, Springer, chapter 2,2011

[13] Xuanwu Zhou, "Improved Signcryption Scheme with Public Verifiability," Knowledge Engineering and Software Engineering, 2009 (KESE '09) Pacific Asia Conference on,pp. 178-181, 19-20 Dec. 2009