International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013
ISSN 2229-5518

Chaos Based Signcryption Scheme

Richa

Abstract— Chaos is one type of complex dynamic behaviour generated by determined nonlinear dynamic systems. One of the soul parts of chaos theory is pretty easy to understand, though. It's often called the "*butterfly effect*". Chaos functions have mainly used to develop mathematical models of non linear systems .Chaotic systems have many important properties, such as sensitive dependence on initial conditions, system parameters, density of point set topology of all cycles passed. Most properties such as mixing and diffusion are related to some requirement in the sense of cryptography. Therefore, provide more useful and practical applications of chaotic cryptosystems. In this paper, we investigate the utility of such functions in signcryption scheme for secure communication. An algorithm using a simple chaotic function $f(x) = 3*x*(1 - x^2)$ is proposed .The proposed scheme is highly sensitive to the initial conditions. This paper presents chaos based Multi message signcryption scheme. The proposed scheme works for both single recipient and multiple recipients. The proposed scheme uses a chaos based dynamic multi key generator to generate multiple keys for signcryption scheme, and provides high security due to its chaotic nature. This represents important improvements over the chaotic key multi-message multi-recipient signcryption (CPK-MM-MRS) scheme proposed earlier.

Index Terms—Chaos**,** Signcryption , Choatic function, Hash function, Keyed Hash Function, Encryption, Signature.

1 INTRODUCTION

As the internet becomes an increasingly important means of conducting transactions and the volume of e-business grows exponential, a secure infrastructure is needed to provide authenticate, confidentiality and access control. The modern era has been well-developed and extremely advanced. Security has become an essence in almost all areas of communication. Security has evolved from a basic password scheme to a complex key infrastructure. Cryptography is the study of mathematical techniques related to aspects of information security, such as privacy or confidentially, entity authentication and data integrity. While sending a message over an insecure channel such as internet we must provide security features such as confidentiality, integrity, authenticity and non-repudiation.

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. 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".

Yuliang Zheng in 1997 [2], presented a positive answer to the following question: "Is it possible to transmit the message of arbitrary length in the way of security and authentication with costs below the required signature –then- encryption scheme?" This is the first time, since the public key encryption technology has been invented, that the problem is addressed in the literature. He found a new cryptographic primitive called signcryption which meets the functions of digital signature and public key encryption in a logical single step and cost significantly less than the required signatures-then-encryption scheme [3].

The proposed cryptography primitive is more efficient for both type of cost involved: Computation cost and communication overhead. The computational cost represents how much computing effort investment by the sender and the receiver of the message. It is by a quantity related to the dominant operation count. The communication overhead represents the extra bits which are appended to a message in case of a digital signature or encryption based on public key

- *Richa is currently pursuing masters degree program in Computer Science and Engineering in Deenbandhu Chottu Ram University Of Science And Engineering, India, PH- +91-9896044274. E-mail: richa.dahiya2@gmail.com*

cryptography. Encryption and digital signatures are two basic encryption tool, that can guarantee the confidentiality, integrity and non-repudiation. Until signcryption, they are seen as important, but distinct building blocks of different encryption systems.

In many applications, the confidentiality and authenticity are needed together. These applications include secure mail (S / MIME), Secure Shell (SSH), and secure web browser (HTTPS). In order to achieve these two objectives, many cryptography schemes have been created: Schnorr signature-then-ElGamal encryption, DSS-then-ElGamal encryption, RSA signature-then-RSA encryption. Any signcryption scheme should have the following properties:

1. Correctness: Any signcryption scheme should be correct verifiable.
2. Efficiency: The computational cost and communication overhead of the signcryption scheme should be less than the best known signature –then- encryption scheme.
3. Security: A signcryption scheme should also meet the security attributes of an encryption scheme and digitalsignatures. This additional properties mainly include:

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) Integrity: 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.

Some signcryption scheme provide further properties, such as public verifiability and forward secrecy of message confidentiality, while others do not provide them .

Part of in the past few years, the study of chaotic systems in the scientific community and its possible application to cryptography has been great concern.

Chaos is one kind of complex dynamic behavior generated by determined nonlinear dynamic system, which is greatly sensitive to initial conditions and parameters, to repeat that it is impossible. This is a complex and dynamic activities, widely represent in the non-linear system. Its properties, such as the initial conditions and parameters, similar to the statistical properties of the noise makes it difficult to predict. It is widely used in cryptography. The appearance of the enigmatic and random nature is the most attractive features of deterministic chaotic system signals lead to new (engineering) applications due to the sensitivity and unpredictability of the chaos.

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 [5] proposed chaos based signcryption scheme for multi messages multi recipient, no 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 main idea, behind the proposed scheme, is to achieve very high security by using chaotic keys for the encryption algorithm, generated by chaotic key generator.

Use of mathematical functions to generate multiple keys or a time slice has been largely unexplored ideas. This function is recommended in [1]. However, a simple mathematical function is not enough. Always assumed that the encryption algorithm is public, and this means that the function to generate multiple keys is known to the hacker as well. This means that, once the hacker is able to find a key, he immediately access other keys. Here a chaotic function can play an important role. This paper presents an algorithm, the use of the chaotic function $f(x) = 3*x*(1-x^2)$ explore signcryption scheme to generate multiple keys.

This paper is structured as follows. Chaotic function i.e $f(x) = 3*x*(1-x^2)$ is discussed in Section II. The third section describes the proposed scheme which includes description of parameters, 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 proposed scheme for the proof of correctness and for the assessment of algorithm. Section V presents the conclusions and scope for futhur work in this area.

2 CHAOS FUNCTION FOR SIGNCRYPTION SCHEME

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.

One of the simple chaotic function $f(x) = r*x*(1 - x^2)$ is used here, where r is the control parameter and this function is bounded to $0 < r < 3$. This function can be written for the iterative form $x_{n+1}=r*x_n*(1-x_n^2)$ where x_0 is used as a starting point. In this paper some of the important properties of this function that are of relevance are described.

Fig1. shows a bifurcation diagram of this function. This is a plot of the parameter 'r' with the values that are obtained after some number of iterations i.e f(x). For 0<r<2, the function is seen to converge to a particular value after some number of iterations. As 'r' increases to just greater than 2 the graph is divided into two branches. Now the value of this function takes oscillation between two different values.

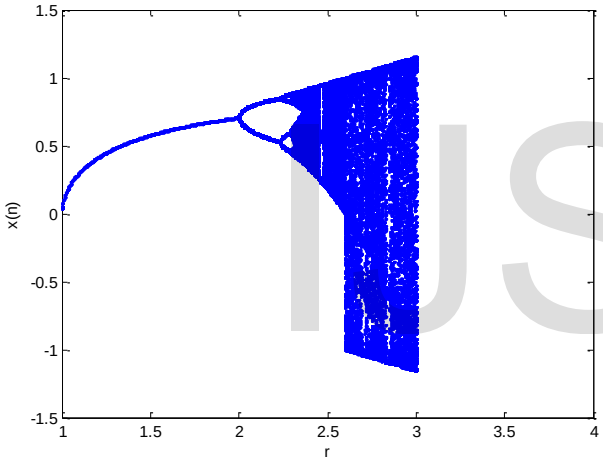

Fig 1. The bifurcation diagram for the function $f(x)=r*x*(1-x^2)$

The x-axis gives the 'r' value and corresponding y-axis denotes the f(x) value. When the parameter 'r' further increases , the curve again bifurcate and now the value of the current oscillations are seen in between 4 values. For the 'r' in the current situation, the increase in branch becomes faster and faster, 8,16 then 32. Periodicity of 'r' is called "point of accumulation" exceeds a certain value gives a chaos to complete. It is found when (r > 2.37), the chaos generated values are considered to be restricted to two different boundary. As the value of the 'r' increases, the two boundaries gave way to a single way. Also the range between which chaos values are yielded increases constantly as the value of 'r' is increased . Finally when r = 3, we observed that the chaos generating the full range of (-1.25 to 1.25). Precisely at this point, we are interested in the chaos function. Therefore the chaos function that we investigate for applications in generation of multiple keys for Signcryption scheme in this paper is $f(x) = 3*x*(1-x^2)$.

We are using this function for generation of multiple keys for the Signcryption scheme as it is simple to use, one Dimensional in nature and it also provides a high range for key generation which provides more security to the scheme proposed before. Hence we can also experiment with some complex chaotic functions for generation of chaotic keys in near future.

3 Proposed Scheme

The proposed signcryption scheme consists of four algorithm namely, key generation algorithm, chaotic multi-key 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.
w: total no of receivers.

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 key chosen 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 key chosen randomly from [1,...,q-1]
y_b: Receiver's public key computed as:

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

3.2 Chaotic multi-Key Generator (CMKG)

The chaotic multi- key generator CMKG

$$CMKG(k, n)$$

proposed here is two tuple, where k 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), and n is the total number of messages.

1) Calculate a message encryption key " k" for every receiver which is called the master key and Pick a random number x from [1,…, q].

$$k = y_b^x mod p \quad (1)$$

$t = hash(k)$ (2)

2) Compute the secret multi-keys for block cipher algorithm using the CMKG . Suppose sender A wants to send n messages $(m_1, m_2, \dots, m_n)$ to receiver B, he will generate n chaotic keys $(k_1,k_2 \dots k_n)$ for encryption as follow:

$(K_1,K_2,\dots K_n)=CMKG(k,n)$ (3)

By using Chaotic function ,i.e $K_i=r*k_{i-1}*(1-k_{i-1})$, we will find multiple keys. For i=1…n.

3.3 Signcryption Schemes

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

3.3.1 Multi Message Single Recipient Signcryption Scheme

The Graphic representation of the scheme is shown in Fig.2. To signcrypt the n messages, a user calculates n chaotic keys ($k_1,k_2 \dots k_n$) used to encrypt the n messages$(m_1, m_2, \dots, m_n)$ and then creates signature on n messages using his private key(x_b).

Signcryption algorithm:

1. Compute $k = y_b^x mod\ p$ (4)
2. Compute $t = hash(k)$ (5)
3. For n messages compute n chaotic keys using:
   $(k_1,k_2 \dots k_n) = CMKG(k, n)$ (6)
4. Compute cipher text $(c_1, c_2, \dots, c_n)$ using encryption algorithm under chaotic keys ($k_1,k_2 \dots k_n$) as follow:
   $c_i = E_{ki}(m_i)$ for i = 1,...,n (7)
5. Compute keyed hash values (r1, r2,…,rn) for n messages using c as follow:
   $r_i = KH_t(m_i)$ for i = 1,...,n (8)
6. Compute multi message signature using:
   $S = x(x_a + \sum_{i=1}^{n} r_i)^{-1} mod\ q$ (9)

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

On the receiver side, receiver can recover k and c successfully by using sender's public key and his private key. 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 c 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. Compute $d = (y_a . g^{\sum_{i=1}^{n} r_i})^s mod p$ (10)
2. Calculate $k = d^{x_b} mod\ p$ (11)
3. Calculate $t = hash(k)$ (12)
4. For n messages compute n chaotic keys using
   $(k_1,k_2,\dots k_n) = CMKG(k,n)$ (13)
5. Recover messages using
   $m_i = D_{ki}(c_i)$ for i = 1,...,n (14)
6. Accept if $KH_t(m_i) = r_i$ for i = 1,.n (15)

3.3.2 Multi Message Multi Recipient Signcryption Scheme

Let the total numbers of receivers be w. For a receiver b_j, his key pair is (x_b^j, y_b^j) for j=1,…,w the sender calculates k^i using the jth user public key y_b^j and t^j using the one way hash function . He then computes n chaotic keys($k_1^j,k_2^j \dots k_n^j$) 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 $k^j = (y_b^j)^x\ modp$ (16)
2. Calculate $t^j = hash(k^j)$ (17)
3. For i = 1,…,n
   a) $k_i^j = CMKG(k^j,n)$ (18)
   b) $c_i^j = E_{k_i^j}(m_i)$ (19)
   c) $r_i^j = KH_t^j(m_i)$ (20)
4. $s = x(x_a + \sum_{i=1}^{n} r_i)^{-1} \mathrm{mod}\ q$ (21)

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

The jth receiver recovers the parameters k^j ,t^j using his private key (x_b^j) and sender's public key (y_a)and computes chaotic keys ($k_1^j,k_2^j,\dots k_n^j$) 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 t^j 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 $d = (y_a . g^{\sum_{i=1}^{n} r_i})^s mod\ p$ (22)

2. Calculate $k^j = d^{x_b^j} mod p$ (23)
3. Calculate $t^j = hash(k^j)$ (24)

4 ANALYSIS OF PROPOSED SCHEME

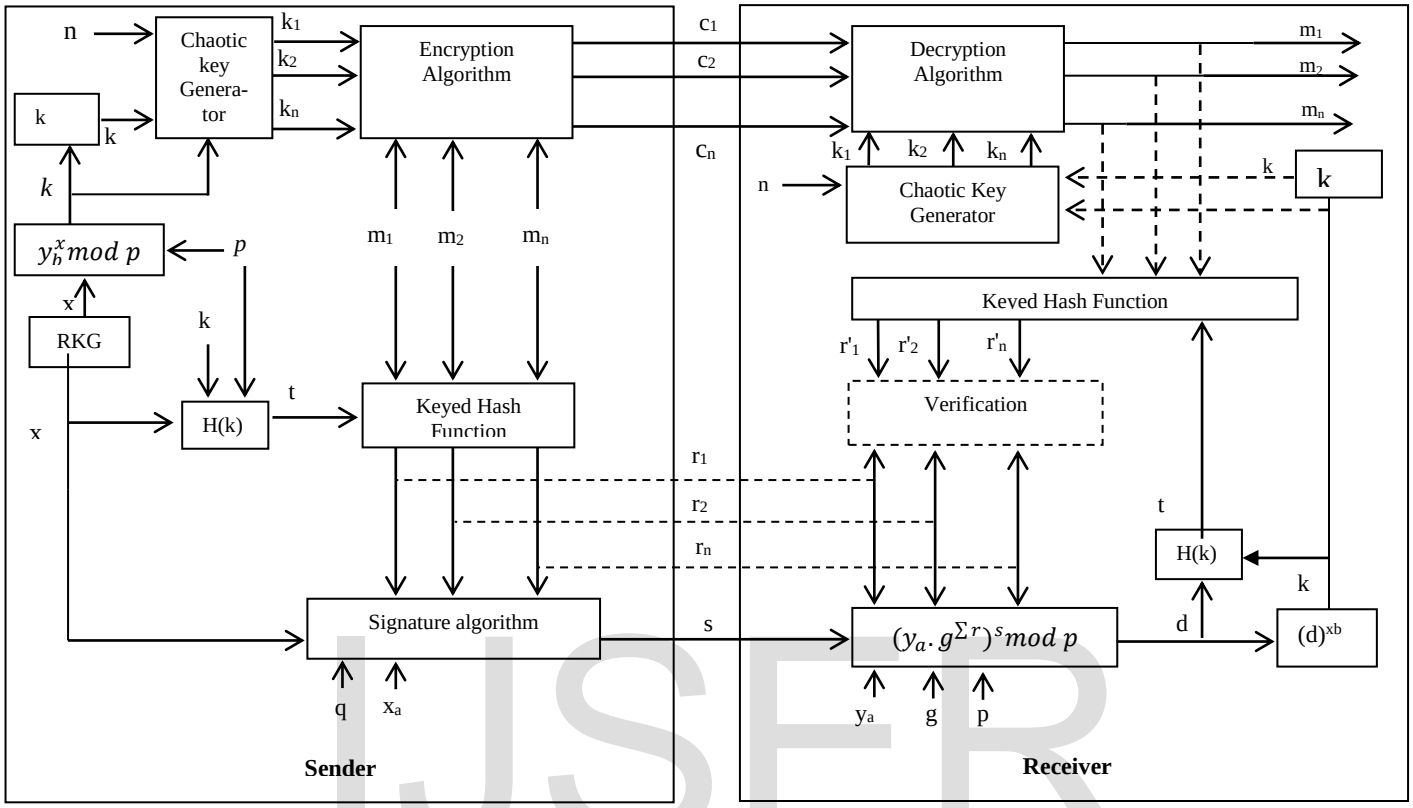

Fig 2. A multi message signcryption scheme with single recipient

For i = 1,…,n

a) $(k^j) = CMKG(k^j, n)$ (25)

b) $M_i = D_{k^j}(c_i)$ (26)

c) Accept if $KH_t^j(m_i) = r_i^j$ (27)

4.1 Correctness of the Proposed Scheme

Messages $(m_1, m_2, \dots, m_n)$ can be recovered on receiver's b_j side, for j=1,…,w, if the signcrypted text is generated by the sender, as the jth receiver can recover the parameters (k^j, t^j) by using his private key (x_b^j) and sender's public key (y_a) and can compute chaotic keys $(k_1.k_2 \dots k_n)$ are used to decrypt the encrypted messages.

Evaluation

The chief merit of the above algorithm that the multiple keys generated by the algorithm are expected to be completely random and non deterministic in nature .

In determining the keys for the Signcryption scheme , we would like to ensure that even if a potential hacker can get an idea of a key , he should not be able to calculate the other keys with the knowledge of the chaos functions. The proposed scheme is analysed for its correctness as follow:

$k^j = d^{x_b^j} mod\ p$

$= (y_a . g^{\sum_{i=1}^n r_i})^{s.x_b^j} mod\ p$

Since, $d = (y_a . g^{\sum_{i=1}^n r_i})^s mod\ p$

$= (g^{x_a} . g^{\sum_{i=1}^n r_i})^{s.x_b^j} mod\ p$

$= (g^{x_a + \sum_{i=1}^n r_i})^{s.x_b^j} mod\ p$

$= (g^{x_b^j . (x_a + \sum_{i=1}^n r_i)})^s mod\ p$

$= (y_b^j)^{(x_a + \sum_{i=1}^n r_i).s} mod\ p$

$= (y_b^j)^x mod\ p$

= value generated on sender's side

Since, $s = x(x_a + \sum_{i=1}^n r_i)^{-1} mod\ q$

5 CONCLUSION

In this paper,a new multi message chaos based signcryption schemes are proposed for both single recipient and multi recipient. The main idea behind the proposed scheme is to develop a chaotic key generator which generates chaotic keys for encryption algorithm. Due to chaotic nature of the keys, the proposed scheme provides very high security. It increases the strength of chaotic keys and therefore the strength of signcrypted text which is highly desirable when the high computational power systems are being used.

ACKNOWLEDGMENT

The author(s) would like to thank faculty members and other contributor for their very useful advises.

REFERENCES

[1] S. Han, E. Chang, Chaotic map based key agreement with/out clock synchronization, Chaos, Solitons & Fractals 39 , 1283–1289,2009.
[2] Yuliang Zheng, Alexander W. Dent, Moti Yung, "Practical Signcryption", 2010.
[3] Yuliang Zheng "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption) " Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, vol 1294, Springer-Verlag, pp. 165-179,1997.
[4] M.S Baptista "Cryptography with chaos" Physics Letters A 240 ,no.1-2,50 4,1998.
[5] Dalia.H.Elkamchouchi "A chaotic key multi-message multi-recepients signcryption scheme (CPK-MM-MR-SS)." Electronics and Communication Engineering Department, Alexandria Higher Institute of Engineering & Technology (AIET), Alexandria 21311, Alexandria, Egypt.
[6] Dr. Ranjan Bose , Amitabha Banerjee "Implementing symmetric cryptography using chaos function" Electrical Engineering Department, Indian Institute of Technology, HauzKhas, New Delhi.
[7]YuliangZheng, "Signcryption and Its Applications in Efficient Public Key Solutions"First International Workshop, ISW'97 Tatsunokuchi, Ishikawa, Japan,Springer-Verlag, pp 291-312,1997.
[8]J.M. Amigó, L. Kocarev b, J. Szczepanski, "Theory and practice of chaotic cryptography", Physics Letters A 366 ,pp. 211–216,2007.
[9] 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.

[10]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.
[11]Benoit Libert, J- J.Quisquater: "A new identity based signcryption scheme from pairing," IW2003, Paris, France, March 31 -April 4, 2009 paper 11.3.4, p. 103,2009

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

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

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

[15]Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)," Advances in Cryptology - Crypto'97, LNCS 1294, Springe, pp. 165-179,1997
[16]Fateman, R.J, "Lookup tables, recurrences, and complexity," In Proc. Int. Symp. Symbolic and Algebraic Computation. ISSAC1989.

.