SECRET SHARING SCHEME TO GENERATE MULTIPLE KEY IN NTRU CRYPTOSYSTEM

S.SRILAKSHMI

Abstract : A secret sharing scheme is a method of distributing a message in parts among participants, each of which is allocated a share of the message. The message can be accessed completely, only when the group of participants come together, thus ensuring the safety of the message.
A public key cryptosystem is the most adopted method to achieve security, in which one key is made public so that outsiders can encrypt their message using that key. The private key is used to decrypt the secured encrypted message. RSA and NTRU are the two most popular public key cryptosystems which uses these methods. Although the owner creates his own private key, but there is no certainty that he can keep it intact for a long time. Problems like virus can corrupt that private key. In that case, decryption really becomes a challenge even for the owner of the key. For MNCs, the public key is same but to decrypt the same message different people may use different private key pair.
In this paper it is proposed a method that will help in generating different pair of private key for the same public key.

Keywords: Cryptosystems, RSA,NTRU Cryptosystems, private key.

Mathematical Preliminary

Modular arithmetic: if m is a positive integer, and a,b are two integers then, a is said to be congruent to b modulo m, if a-b is divisible by m denoted by a≡b modulo m or simply a≡b mod m. if a≡b mod m and c≡d modm then ax+cy≡bx+dy mod m for all integers x and y. if $a^n \equiv b^n$mod m for any positive integer n. if a≡b mod m the F(a)≡F(b) mod m ,for any polynomial F(x) with integer coefficients.

Truncated polynomials

NTRU public key cryptosystem are based on polynomials R(x)of degree n-1 having integer coefficients of polynomials in R(x). Arithmetic operations are done not in usual way. Since multiplication is done using truncated polynomials.

If f(x) and g(x) are two polynomials of degree n-1 in single variable x i.e.,

f(x)= $a_0 + a_1 x + \ldots\ldots\ldots + a_{n-1} x^{n-1}$ and g(x)= $b_0 + b_1 x + \ldots\ldots\ldots + b_{n-1} x^{n-1}$

Then define a new polynomial h(x) =f(x)*g(x) = $c_0 + c_1 x + \ldots\ldots\ldots + c_{n-1} x^{n-1}$

Where

$c_i = a_0 b_i + a_1 b_{n-i} + \ldots.a_i b_o + a_{i+1} b_{n-1} + \ldots\ldots\ldots + a_{n-1}$

Modulo operations on truncated polynomials

if f(x) is congruent to k modulop, if p divides every coefficient of f(x), except the constant term f(0)and p divides f(0)-k. this is denoted by f(x)≡k modp.

Inverse in truncated polynomials

the inverse modp of a polynomial f(x) is another polynomial F(x), if it satisfies the property f*F=1 modp. Not every polynomial has an inverse modulo p but is easy to determine if f has an inverse and compute the inverse if it exists.

Outline of the NTRU algorithm

The NTRU PKCS[1][2][3][4] uses a ring that consists of truncated polynomials of degree n-1 denoted by $Z[X]/x^{n-1}$.select a large modulus q and small modulus p , so that ged(q,p)=1. The coefficients of the truncated polynomial in $Z[X]/x^{n-1}$ will be reduced mod q. In the final step of decryption, the coefficients of polynomial are reduced modulo p.

First select two small polynomials f and g . a small polynomial is one in which all the coefficients are either 0.or-1 or1.

Key creation

Step1 compute inverse of f modq =fq, and inverse of f modp=fp with the property that f .fp =1modp and f.fq=1 modq.

Step2 compute the public key h=p*fq*g mod q public key polynomial =h, private key polynomial = {f,fp}.

Encryption

Step1 select a message m and put it in the form of a polynomial m with the coefficient between –p/2 and p/2.

Steps 2 pick a random small polynomial r with coefficient 1 or -1 or 0.

Step 3 encrypt the message m as c=r*h+m modq

Decryption

Step1 upon receiving the ciphered text c, compute a=f*c modq

Step 2 express the coefficients of a in the range- q/2 toq/2.

Step3 compute b=a*fp mod p.

Step 4 original message m=b. [5]

The proposed method

To generate secret sharing messages with multiple key generation basing on NTRU, everybody knows their private key {fi.fipi}. Assume that there is a trusted third party, and given shares of the

polynomials it will compute the inverse and distribute share of inverse to the participants. It is assumed that all participants agreed upon a common degree of the polynomial, and the values of p's and q

We have to share the message m=m1,m2,m3,m4.....mn among n participants. Let p1,p2,p3.....pn and q are n+1 large primes

Trusted third party gives the inverses of private key and shares the inverse to the participants.

Algorithm to encrypt the message

Step 1 TTP calculates the inverses of fipi where fi 's are the private key of the n participants, after receiving them

Step 2 TTP calculate the private key hi=pi *fiq*g modq where g is small polynomial kept secret

And sends the cipher text as ci =hi+mi (i=1,n)

Algorithm to decrypt the message

Step 1 fi ci = fi hi +fi mi mod q =fi pi fiqi g +fi mi modq =pi g+fimi modq

Fipi fi ci = fi pi g +mi modpi = mi since pi fipi g mod pi =0

Analysis of the algorithm

The strength of the NTRU algorithm lies in keeping fi and g secret. Though fi is to be maintained secret it is fipi that is commonly used hence this paper has concentrated in keeping both f and fp's confidential. By dividing m's into shares and each party involved in the communication have to keep their shares of fi secret. The inverses of fi's are calculated by the trusted third party, after receiving the shares of fi from each participant calculates its fips with respect to pi and fiq with respect to q.

Encryption and Decryption

The encryption is done by ci=hi+mi mod q, where hi=pi*fiq*g, where g is any small polynomial.

To decrypt the message of the following steps are performed

Ci=hi+mi mod q

Fi ci= fi hi +fi mi

Fi ci =fi pi fiq g +fi mi modq

= pig + fi mi modq

Fipi fi ci = fipi pi g + fi mi mod q

Ci = mi since fipi fi ci = 0+mi mod q mod pi , fi fipi =1 mod p

Conclusions : This paper proposes algorithm for sharing the message among n participants and to generate multiple keys, encryption and decryption based on NTRU. The paper assumed that one party is communicating with n participants.

References

1. C.Cocks, "split Knowledge generation of RSA parameters, cryptography and coding" 6 th IMA conference , lecture notes in computerscience style, vol 1423, pp237 -251,spinger verlag, new York, 1997.
2. Boneh.D., Franklin M., "efficient generation of shared RSA keys "proceedings of crypto 97, 1997 pp425 – 439.
3. Bruce schneier "Applied cryptography". Wiely and sons 1994, ISBNo-471-597562-2.
4. Rivest R.L.Shamir.A,and Adleman.L " A method for obtaining Digital signature and public key cryptosystem".Comm. ACM.Vol 21 , No 2 1978,pp120-126.
5. J. Hoffstein D.Lieman, J.Silverman "polynomial rings and efficient public key Authentication". Proceeding of the international workshop on cryptographic techniques and e- commerce (Cry TEC '99) M.Blum and C.H. Lee, eds city university of Hong Kong press, 1999.

***

Department of Mathematics ,J.N.T.U.A College of Engineering ,Anantapur ,515002

Mail id srilakshmi.sirivaram@gmail.com

Phone 09440686983