A NEW NTRU CRYPTOSYSTEM WITH BLOCK MATRIX FORMULATION

Priya Verma[1], Swati Verma[2*], G.V.V J. Rao[3]

Article Computer Science And Applied Mathematics:
Received: 05:01:2023 **Revised: 07.04.2023** **Accepted: 10.05.2023**

Abstract
The NTRU public key cryptosystem was first presented by J. Hoffstein, J. H. Silverman and J. Pipher in 1996 [7]. This system is based on shortest and closest vector problem in a lattice and its operations is based on objects of a truncated polynomial ring. In this paper, we have shown that applying block matrix for the matrix formulation algorithmin NTRU public key cryptosystem substantially increases its efficiency as compared to other matrix formulation for NTRU cryptosystem with invertible matrix, such as Nayak et al. [8]. The block matrix facilitates the development and understanding of numerical algorithms.

Keywords: NTRU, Block-Matrix, Encryption, Decryption.

[2*]OP Jindal University, Raigarh (C.G.), Email: swati.verma@opju.ac.in
[1,3]Kalinga University, Raipur (C.G.), Email: gvvjagan1@gmail.com, priyavermatanu15@gmail.com

***Corresponding Author:** Swati Verma
*OP Jindal University, Raigarh (C.G.), Email: swati.verma@opju.ac.in

(AMS) Mathematics Subject Classification No: 94A60, 15A23, 15A57

DOI: - 10.48047/ecb/2023.12.si5a.0237

1. INTRODUCTION

Lattices were first studied by mathematician Joseph Louis Lagrange andCarl Friedrich Gauss. Later lattices have been used in public key cryptosystems by Ajtai Dwork (Ajtai and Dwork 1997), Goldreich Goldwasser Halevi (Goldreich et al. 1997) and NTRU (Hoffstein et al.1998) cryptosystem. NTRU the best among the other lattice based cryptosystems. The NTRU PKC of J.Hoffstein, Silverman [4] was designed with lattice of polynomial. Next PKC of J. Hoffstein [10] was designed with vector space in Rn dimension and Nayaket al. [8] was designed with invertible matrix. In this paper PKC were founduse and introduce NTRU cryptosystem for companion matrix. We also findKey generation, Encryption and Decryption by companion matrix. This cryptosystem is new design of Matrix formulation algorithm. NTRU allegedly stands for "Nth Degree Truncated Polynomial Ring Units".NTRU is a public key cryptosystem presented by J. Hoffstein, J. Pipher and J. Silverman [4]. The first version of the NTRU encryption system was presentedat the crypto 96 conference [4]. The computational basis of the NTRU lies inpolynomial algebra and it is a relatively new cryptosystem. NTRU is based onlattice-based cryptography it has different cryptographic properties from RSAand ECC [3]. The strength of cryptographic NTRU performs valuable privatekey operations much faster in comparison to RSA. Polynomial algebra is thebasic building block of the NTRU Encryption system. The truncated polynomials given in J. Silverman [9], P.Prapoorna [5] in the ring R = Z[x]/(x^n -1)are basic objects and the reduction of polynomials with respect to relativelyprime moduli i.e., p and q are the basic tools.Recently, Nayak et al. [8] have proposed taking invertible or non singular matrix in NTRU cryptosystem [4]. They have given a PKC by method, whichis suitable to send in the key generation phase of large message in the form ofmatrices.Now in this paper, we consider companion matrix during key generationreplacing the invertible matrix of Nayak et al. [8] design. In our opinion companion matrix makes the PKC more efficient as compared to invertible matrix because companion matrix is always upper triangular matrix hence easily reducible.

2. REVIEW OF NAYAK et al. [8] SYSTEM:

The Nayak et al. [8] give the Key generation, encryption and decryption for their cryptosystem as below:

2.1 Key Generation:

Bob (receive) creates a public and private key pair. For this purpose he first randomly chooses two matrices f and g, where matrix f is an invertible matrix (modulo p). Bob keeps the matrices f and g private, since anyone who knows any one of them will be able to decrypt messages sent to Bob. Bob'snext step is to compute the inverse of f modulo q and the inverse of f modulo p. Thus he computes matrix fq and fp which satisfies f *fq= I (modulo q) and f *fp= I (modulo p). Bob then ensures the existence of inverse of matrixf by checking f is non- singular and f is invertible mod p (i.e.[det[f]](mod pNTRU Cryptosystem with Companion Matrix 36= 0). Otherwise he needs to go back and choose another matrix f. Now Bob computes the product H = p*fq*g (modulo q). Bob's private key becomethe pair of matrices f and fp and his public key is the matrix H.

2.2 Encryption:

Sender wants to send a message to Bob using Bob's public key H. For this she first put her message in the form of binary matrix M, (which is a matrix ofsame order as f and g) and whose elements are chosen with modulo p. Next,she randomly chooses another matrix R of the same order as f. This and itssize is same as private key f and g. To create a encrypted message she then chooses a Random matrix R of size f and g. This matrix is based on blind value, which is used to obscure the message (similar to the ElGamal algorithm which uses a onetime random value when encrypting).To send message M, Alice chooses a random matrix R (which is of same order as matrix X), andBob's public key H to compute the matrix.

E = R *H +M (modulo q). The matrix E is the encrypted message which Alice sends to Bob.

2.3 Decryption:

Now Bob has received Alice's encrypted message E and thus he can decryptit. He begins to decrypt the encrypted message by using his private matrix f to compute the matrix. A = f* E (modulo q).Bob next computes the matrixB = A (modulo p).This way he reduces each of the coefficients of A (modulop). Finally Bob uses his other private matrix fpto compute C = fp*B(modulo p) in order to get the matrix C which is Alice's original message M.

3. PROPOSED ALGORITHM

The required definition and NTRU Operation for proposed scheme as below:

3.1 Definition of Block Matrices:

A block matrix is defined in terms of a partitioning, which breaks a matrix into contiguous pieces. The most common and important case is for an $n \times n$ matrix to be partitioned as a 2×2 block matrix (two block rows and two block columns). For $n = 4$, partitioning into 2×2 blocks gives

$$A = \left[\begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array}\right] = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix},$$

where

$$A_{11} = A(1:2, 1:2) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

and similarly for the other blocks. The diagonal blocks in a partitioning of a square matrix are usually square (but not necessarily so), and they do not have to be of the same dimensions.

This same4× 4 matrix could be partitioned as

$$A = \left[\begin{array}{c|ccc} a_{11} & a_{12} & a_{13} & a_{14} \\ \hline a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array}\right] = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix},$$

where $A_{11} = (a_{11})$ is a scalar, A_{21} is a column vector, and A_{12} is a row vector.

The sum $C = A + B$ of two block matrices $A = (A_{ij})$ and $B = (B_{ij})$ of the same dimension is obtained by adding blockwise as long as A_{ij} and B_{ij} have the same dimensions for all i and j, and the result has the same block structure: $C_{ij} = A_{ij} + B_{ij}$,

The product $C = AB$ of an $m \times n$ matrix $A = (A_{ij})$ and an $n \times p$ matrix $B = (B_{ij})$ can becomputed as $C_{ij} = \sum_k A_{ik}B_{kj}$ as long as the products $A_{ik}B_{kj}$ are all defined. In this case the matrices A and B are said to be conformably partitioned for multiplication. Here, C has as many block rows as A and as many block columns as B. For example,

$$AB = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} A_{11}B_{11} + A_{12}B_{21} & A_{11}B_{12} + A_{12}B_{22} \\ A_{21}B_{11} + A_{22}B_{21} & A_{21}B_{12} + A_{22}B_{22} \end{bmatrix}$$

as long as all the eight products $A_{ik}B_{kj}$ are defined.

Block matrix notation is an essential tool in numerical linear algebra. Here are some examples of its usage.

3.2NTRU Operation:

1. Star Multiply.
2. Rand Poly.
3. Inverse Poly-Fq.
4. Inverse Poly - Fp.
5. Create Key.
6. Encode.
7. Decode.

Following the modular arithmetic on companion matrix give the Key generation, encryption and decryption for their cryptosystem as below-

3.3 Key Generation

Bob randomly chooses f , $g \in Lg$ and w $\in$ Lw and c $\in$ Lc. Matrices f must satisfy additional requirement to have inverse modulo p and q. Matrices g andc should have inverse modulo p.We denote these inverse by notation Fp, FQ,Gp, Cp respectively.

f * Fq= I(mod q);
g *Gp= I(mod p)
Gq* g = I(mod q)
Cp *c = I(mod p)
and
Wq* w = I(mod q)

Bob next compute the companion matrices
h =p*Gq(mod q). (1)
H=w *Fq*c(mod q) (2)
Bob publish the pair of matrices (h,H) M as his public key, (f,g,c) has his private key.

3.4 Encryption

Suppose Alice wants to send a message to Bob. Alice selects a message m fromthe set of plaintext Lm. Next, Alice randomly choose a matrices $\phi \in L\phi$ and Bob's public key (h,H) to compute,
E = ϕ * h + H *M (mod q) (3)

Alice then transmit E to Bob.A different random choice of blinding value ϕ is made for each plaintext m.

3.5 Decryption

To decrypt the ciphertext, Bob first compute
A = f * E *g(mod q)
A = f * (ϕ * h + H *M) *g(mod q)

A = (f*ϕ * h * g + f * H *M *g)(mod q)
A = (f * ϕ *(p *Gq) *g + f * (w *Fq* c) *M * g)(mod q)
A = (f * ϕ * p *Gq*g + f *w*Fq*c *M*g) (mod q)
A = (pf *ϕ + w *c * m * g)(mod q)

Where he choose the coefficients of the polynomial of the matrices A to liein interval of -q/2 to q/2. Matrices ϕ, g, f, m, c and w have polynomial with small coefficients and p is much larger than q. Now bob's next computes the matrices
B = A (mod p)
B = (pf *ϕ + w *c *M *g) (mod p)
B = pf * ϕ (mod p) + w *c *M *g(mod p)
B = 0 + w *c *M *g (mod p)
B = w * c *M *g(mod p)

Finally Bob uses his private matrix Cp, Gp and Wp to computeD = Cp *B *Gp*Wp (mod p) (4)
The matrix D will be Alice's original message M.

3.6Correctness of Algorithm:

Theorem 1. The equation
D = M (mod p) is correct.
D = Cp *B *Gp*Wp (mod p)
D = Cp * (w * c *M * g) *Gp?Wp(mod p)
D = (Cp *c *M * g *Gp* w *Wp)(mod p)
D = M

5. CONCLUSION

This paper propose a method, which is suitable to send large messages in the form of block matrix and this method is more secure since blockmatrix is easy calculate for large degree of polynomial. This method is more efficient and more secure as compare to the Nayak et al [8] cryptosystem.

REFERENCES

1. Brassard G. and Bratley P. “Fundamentals of Algorithm", PHI, 1996.
2. Cohen H., “A Course in Computational Algebraic Number Theory", Springer-Verlag, Berlin, 1993.
3. Coppersmith and A. Shamir,” Lattice attacks on NTRU, in Proc. of EUROCRYPT 97", Lecture Notes in Computer Science, Springer-Verlag, 1997.
4. Hoffstein J., Pipher J. and Silverman J.H., Silverman "Invertibility inTruncated Polynomial Rings", NTRU Cryptosystems, Technical Report No.9. Available at http://www.ntru.com, (1998).
5. Hoffstein J., Lieman D., Silverman J. Polynomial Rings and EfficientPublic Key Authentication", Proceeding of the International Workshopon Cryptographic Techniques and E-Commerce (CrypTEC 99), M. Blumand C.H.Lee, eds., City University of Hong Kong Press, 1999.
6. Horowitz E., Sahani S., and Rajasekharan S. “Fundamental of computer algorithm", Galgotia, 1998.
7. J. Hoffstein, J. Pipher and J. H. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem". Algorithmic Number Theory (ANTS III), Springer- Verlag, 1998, pp. 267-288.
8. Nayak R., Sastry C. V., and Pradhan J. “A Matrix Formulation for NTRU Cryptosystems", Proc. 16th IEEE International conference onNetwork(ICON-2008), New Delhi, India, pp. 12-14, 2008.
9. Roja P. P., Avadhani P. S. and Prasand E. V. “An Efficient Methodof Shared Key Generation Based on Truncated Polynomials", IJCSNSInternational Journal of Computer Science and Network Security, VOL.6 No. 8B, pp. 156-161, 2006.
10. Silverman J. H., “NTRU": A Ring Based Public Key Cryptosystem, InProc. Of ANTS III, volume 1423 of LNCS. Springer-Verlag, Available athttp://www.ntru.com, pp. 267-288, 2001.
11. Wells A. L., “A polynomial form for logarithms modulo a prime", IEEE Transactions on Information Theory, pp. 845-846, 1984.