International Journal of Sciences & Applied Research

International Journal of Sciences & Applied Research

www.ijsar.in

NTRU cryptosystem with Jordan canonical form

Khushboo Thakur*, B.P. Tripathi

Department of Mathematics, Govt. N.P.G. College of Science, Raipur (C.G.), India.

Correspondence Address: *Khushboo Thakur, Department of Mathematics, Govt. N.P.G. College of Science, Raipur (C.G.), India.

Abstract

The NTRU encryption scheme is an appealing another to well-known encryption schemes such as RSA, ElGamal, and ECIES. The security of NTRU relies on the hardness of computing short lattice vectors and thus is a capable candidate for being quantum computer resistant. There has been extensive research on efficient implementation of the NTRU encryption scheme. In this paper, we proposed new cryptosystem which is improvement of Nanda and Nayak scheme, which is based on Jordan canonical form replacing Gaussian Integer Matrix. New scheme is more efficient and low time consuming.

Keywords: NTRU, Jordan Canonical Form, Encryption, Decryption

Introduction

Public key encryption schemes commonly used today are RSA [9], ElGamal [4], and ECIES [8]. The security of those schemes relies on the difficulty of factoring large composite integers or computing discrete logarithms. However, it is unclear whether these computational problems remain intractable in the future. For example, Shor [12] showed that quantum computers can be used to factor integers and to compute discrete logarithms in the relevant groups in polynomial time. Also, in the past thirty years there has been significant progress in solving the integer factorization and discrete logarithm problems using classical computers [10, 11, 3, 2]. It is therefore necessary to develop alternative encryption schemes which do not rely on the difficulty of factoring or computing discrete logarithms and which are considered secure even against quantum computer attacks. A promising candidate for such a quantum secure encryption scheme is the lattice-based public-key cryptosystem NTRU [5] in its NAEP/SVES-3 variant [6, 7].

Now in this paper, we proposed the Gaussian Integer matrix of Nanda et al. [18] design replacing the Jordan Canonical Form. Recently, Nanda et al. [18] have proposed Gaussian Integer Matrix in NTRU cryptosystem [13]. They have given a PKC by method, which is suitable to send in the key generation phase of large message in the form of complex matrices. In our opinion Jordan Canonical Form makes the PKC more efficient as compare to Gaussian Integer matrix.

Review of Nanda et al. [18] Algorithm: The Nanda et al. [18] give the Key generation, encryption and decryption for their cryptosystem as below-

Key Generation:

Bob creates a public and private key pair. He first randomly chooses two matrices X and Y, where matrix X be an invertible matrix (modulo p). Bob keeps the matrices X and Y private, since anyone who knows any one of them will be able to decrypt messages sent to Bob. Bob's next step is to compute the inverse of X modulo q and the inverse of X modulo p. Thus he computes matrix Xq and Xp which satisfies X *Xq = I (modulo q) and X *Xp = I (modulo p). Bob then ensures the existence of inverse of matrix X by checking f is non-singular and f is invertible mod p (i.e.[det[X]](mod p 6= 0). Otherwise he needs to go back and choose another matrix X. Now Bob computes the product H = p*Xq *Y (modulo q). Bob's private key becomes the pair of matrices X and Xp and his public key is the matrix H.

Encryption:

Alice wants to send the message “I Like You" 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 of same order as X and Y) and whose elements are chosen with modulo p. Next, she randomly chooses another matrix R of the same order as X. This and its size is same as private key X and Y. To create an encrypted message she then chooses a Random matrix R of size X and Y. 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), and Bob'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.

Decryption:

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

Proposed Algorithm:

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

Definition of Jordan Canonical Form:

Let $\lambda \in$ C. A Jordan block $J_k(\lambda)$ is a k × k upper triangular matrix of the form

$$J_k(\lambda) = \begin{bmatrix} \lambda & 1 & & \\ & & & 0 \\ & \lambda & 1 & \\ 0 & & & 1 \\ & & & \lambda \end{bmatrix}$$

A Jordan matrix is any matrix of the form

$$j = \begin{bmatrix} J_{n1}(\lambda_1) & 0 \\ & \\ 0 & J_{nk}(\lambda_k) \end{bmatrix}$$

where the matrices J_{n1} are Jordan blocks. If J $\in$ Mn(C), then n1 +n2nk = n.

Theorem: Let A $\in$ Mn(C). Then there is a nonsingular matrix S $\in$ Mn , such that

$$A = S \begin{bmatrix} J_{n1}(\lambda_1) & 0 \\ & \\ 0 & J_{nk}(\lambda_k) \end{bmatrix} S^{-1} = SJS^{-1}$$

where Jni is a Jordan block, where n1+n2+ +nk = n. J is unique up to permutations of the blocks. The eigenvalues $\lambda_1 \cdots\cdots\cdots \cdots\cdots \lambda_k$ are not necessarily distinct. If A is real with real eigenvalues, then S can be taken as real.

NTRU Operation:

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

Key Generation

To create a public/private key pair, Bob chooses two k by k upper triangular matrices A,B,W$\in L_A$. Next, Bob randomly selects short polynomials $\alpha_0,\alpha_1\dots,\alpha_{k-1}\in R$, $\beta_0,\beta_1\dots,\beta_{k-1}\in R$ and $\lambda_0,\lambda_1\dots,\lambda_{k-1}\in R$. Bob then constructs the upper triangular matrix f, g$\in L_f$ and c$\in L_c$ by taking

$f=\sum_{i=0}^{k-1}\alpha_i A^i$, $g=\sum_{i=0}^{k-1}\beta_i B^i$ and $c=\sum_{i=0}^{k-1}\gamma_i W^i$

The matrices f and g must have inverses modulo p and modulo q. This will generally be the case, given suitable parameter choices. We denote the inverses as Fp, Fq, Gp,Gq and Cp,Cq, where

$F_p * f = I(\bmod p)$ and $F_q * f = I(\bmod q)$;

$G_p * g = I(\bmod p)$ and $G_q * g = I(\bmod q)$,

$C_p * c = I(\bmod p)$ and $C_q * c = I(\bmod q)$

Note that I is a k by k identity matrix. Bob now has his private key, (f, g), although in practice he will want to store the inverses Fp, Gp and Cp and constructs the matrix h $\in$ M by taking

$h = p * F_q * G_q (\bmod q)$

Bobs public key consists of the three matrices,(h, A,B).

Encryption

To encrypt a message to send to Bob, Alice randomly generates the short polynomials $\phi_0,\phi_1\dots,\phi_{k-1}\in R$ and $\psi_0,\psi_1\dots,\psi_{k-1}\in R$. Alice then constructs the matrices $\phi,\psi\in L_\phi$ by taking

$\phi=\sum_{i=0}^{k-1}\phi_i A^i$ and $\psi=\sum_{i=0}^{k-1}\psi_i B^i$

Alice then takes her message m $\in$ Lm, and computes the encrypted message
e = $\phi * h * \psi$ + mc (mod q).
Alice then sends e to Bob.

Decryption

To decrypt, Bob computes
a = f *e* g (mod q) .

Bob translates the coefficients of the polynomials in the matrix a to the range -q/2 to +q/2 using the centring techniques as in the original NTRU paper [8]. Then, treating these coefficients as integers, Bob recovers the message by computing
d = Fp*a*Gp* Cp (mod p).

Correctness of algorithm:

Theorem 1. The equation d = M is correct.
Proof
a = f* e*g (mod q)
a = f* ($\phi * h * \psi$ + mc)*g(mod q)
a = (f*$\phi * h * \psi$ * g + f *m *c*g) (mod q)
a = (f *ϕ *p*Fq*Gq *ψ *g + f *m*c*g) (mod q)
a = (p*$\phi * \psi$ + f *m *c *g) (mod q)
Now
d = Fp *a *Gp*Cp (mod p)
d = Fp *(p*$\phi * \psi$ + f *m *c *g) *Gp *Cp (mod p)
d = Fp *p * $\phi * \psi$ * Gp* Cp (mod p) + Fp * f* m* c* g* Gp * Cp (mod p)
d=0 + Fp *f * m * c* g * Gp *Cp (mod p)
d = 0 + m
d = m

Conclusion

In this paper we have proposed a method for choosing the Jordan Canonical Form for Key generation, Encryption and decryption using by matrices of taking f as proposed in the Gaussian Integer matrix for NTRU cryptosystem. The advantage of using Jordan Canonical Form is improve the efficiency of lattice based cryptosystem in terms of key length and computation time without compromising their security. This method is more efficient and more secure as compare to the Nanda et al. [18]. There is always a Jordan Canonical Form in the form of upper triangular matrix which speeds up the key generation.

References

[1] Coppersmith and A. Shamir, Lattice attacks on NTRU, in Proc. of EUROCRYPT 97", Lecture Notes in Computer Science, Springer-Verlag, 1997.

[2] K. Aoki, J. Franke, T. Kleinjung, A. K. Lenstra, and D. A. Osvik., A kilobit special number Field sieve factorization. Cryptology ePrint Archive, Report 2007/205, 2007. Available at http://eprint.iacr.org/2007/205.

[3] S. Cavallar, B. Dodson, A. K. Lenstra, W. M. Lioen, P. L. Montgomery., Factorization of a 512-Bit RSA Modulus. In Advances in Cryptology EUROCRYPT 2000, volume 1807 of Lecture Notes in Computer Science, pages 1-18. Springer Verlag, 2000.

[4] T. Elgamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In Advances in Cryptology -CRYPTO '84, volume 196 of Lecture Notes in Computer Science, pages 10-18. Springer Verlag, 1985.

[5] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. In Proceedings of the Third International Symposium on Algorithmic Number Theory, volume 1423 of Lecture Notes in Computer Science, pages 267-288. Springer Verlag, 1998.

[6] N. Howgrave-Graham, J. H. Silverman, A. Singer, and W. Whyte. NAEP: Provable Security in the Presence of Decryption Failures. Cryptology ePrint Archive, Report 2003/172, 2003. Available at http://eprint.iacr.org/2003/172.

[7] N. Howgrave- Graham, J. H. Silverman, and W. Whyte. Choosing Parameter Sets for NTRUEncrypt with NAEP and SVES-3. In Topics in Cryptology CT-RSA 2005, volume 3376 of Lecture Notes in Computer Science, pages 118-135. Springer Verlag, 2005.

[8] IEEE. IEEE Standard Specifications for Public-Key Cryptography, January 2000. See also IEEE 1363 Amendment 1: Additional Techniques".

[9] RSA Laboratories.,RSA Cryptography Standard (version 2.1). Available at http://www.rsa.com/rsalabs/node., June 2002.

[10] A. K. Lenstra and H. W. Lenstra, Jr., editors. The development of the number eld sieve, volume 1554 of Lecture Notes in Mathematics. Springer Verlag, 1993.

[11] A. K. Lenstra and E. R. Verheul. Selecting cryptographic key sizes. Journal of Cryptology, 14(4): 255-293, 2001.

[12] P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science (FOCS 1994), pages 124-134. IEEE Computer Society Press, 1994.

[13] Hoffstein J., Pipher J. and Silverman J.H., Silverman "Invertibility in Truncated Polynomial Rings", NTRU Cryptosystems, Technical Report No.9. Available at http://www.ntru.com, (1998).

[14] Hoffstein J., Lieman D., Silverman J. Polynomial Rings and Efficient Public Key Authentication", Proceeding of the International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC 99), M. Blum and C.H. Lee, eds., City University of Hong Kong Press, 1999.

[15] Silverman J.H., NTRU: A Ring Based Public Key Cryptosystem, In Proc. Of ANTS III, of volume 1423 LNCS.Springer-Verlag, Available at http://www.ntru.com, pp. 267-288, 2001.

[16] Roja P.Prapoorna, Avadhani P.S. and Prasand E.V. An Efficient Method of Shared Key Generation Based on Truncated Polynomials", IJCSNS International Journal of Computer Science and Network Security, VOL. 6 No. 8B, pp. 156-161, 2006.

[17] 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.

[18] Nanda Ashoke Kumar and Nayak Rakesh, NTRU with Gaussian Integer Matrix International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5(2), 2015.