Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 1s (2025)

A Novel NTRU Cryptosystem with Gell Maan Matrix

Swati Verma[1], Debasmita Samal[2], Khushboo Thakur[3], Priya Verma[4]

[1, 2] O. P. Jindal University, Raigarh (C.G.), India.
[3]Govt. Shahid Koushal Yadav College, Gundardehi, Dhamtari (C.G).
[4]Department of Mathematics, Kalinga University, Raipur (C.G.), India.
[1] swati.verma@opju.ac.in,
[2]debasmita.samal@opju.ac.in, [3]khushboo.thakur784@gmail.com,
[4]priyavermatanu15@gmail.com

Article History:

Received: 30-09-2024

Revised: 15-11-2024

Accepted: 20-01-2025

Abstract:

The NTRU public key cryptosystem was first presented by J. Hoffstein,J. H. Silverman and J. Pipher in 1996. This system is based on shortest and closest vector problem in a lattice and its operations are based on objects of a truncated polynomial ring. In this paper, we have show that applying Gell Maan Matrix for the matrix formulation algorithm in 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 Gell Maan Matrix facilitates the development and understanding of numerical algorithms.

Keywords: Gell Maan Matrix, NTRU, Encryption, Decryption, Security Analysis. .

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

1. INTRODUCTION

Lattices were first studied by mathematician Joseph Louis Lagrange and Carl 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 Nayak et al. [8] was designed with invertible matrix. In this paper PKC were found use and introduce NTRU cryptosystem for companion matrix. We also find Key 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 presented at the crypto 96 conference [4]. The computational basis of the NTRU lies in polynomial algebra and it is a relatively new cryptosystem. NTRU is based on lattice-based cryptography it has different cryptographic properties from RSA and ECC [3]. The strength of cryptographic NTRU performs valuable private key operations much faster in comparison to RSA. Polynomial algebra is the basic 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 relatively prime 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, which is suitable to send in the key generation phase of large message in the form of matrices. Now in this paper,

we consider Gall Maan matrix [13] during key generation replacing the invertible matrix of Nayak et al. [8] design. In our opinion, Gall Maan matrix makes the PKC more efficient as compare to invertible matrix because Gell Maan matrix is traceless Hermitian matrices consequently 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 (receiver) creates a public and private key pair. For this purpose he first randomly chooses two matrices f and g, where matrix f be 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's next 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 matrix f by checking f is non-singular and f is invertible mod p (mod p NTRU 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 become the 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 of same 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 its size 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), 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.

2.3 Decryption

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 f to compute the matrix. A = f* 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 fp to compute C = fp*B(modulo p) in order to get the matrix C which is Alice's original message M.

3. Proposed NTRU with Gell-Mann Matrix Integration

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

3.1 Definition of Gell-Mann Matrix

The **Gell-Mann matrices**, developed by Murray Gell-Mann, are a set of eight linearly independent 3×3 traceless Hermitian matrices used in the study of the strong interaction in particle physics. They span the Lie algebra of the SU(3) group in the defining representation.

These matrices are traceless, Hermitian, and obey the extra trace orthonormality relation, so they can generate unitary matrix group elements of SU(3) through exponentiation[1]. These properties were chosen by Gell-Mann because they then naturally generalize the Pauli matrices for SU(2) to SU(3), which formed the basis for Gell-Mann's quark model[2]. Gell-Mann's generalization further extends to general SU(*n*).

Gell-Mann matrices, denoted as λi, are the generators of the SU(3) Lie algebra and are widely used in quantum mechanics for their algebraic and symmetry properties. Their non-commutativity and orthogonality properties can be utilized to introduce additional mixing in polynomial coefficients during encryption and key generation.

Example: $\lambda_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ $\lambda_2 = \begin{bmatrix} 0 & -i & 0 \\ i & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ $\lambda_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ $\lambda_4 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & & \end{bmatrix}$

$$\lambda_5 = \begin{bmatrix} 0 & 0 & -i \\ 0 & 0 & 0 \\ i & 0 & 0 \end{bmatrix} \lambda_6 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \lambda_7 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -i \\ 0 & i & 0 \end{bmatrix} \lambda_8 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{bmatrix}.$$

Trace Orthonormality

An Orthonormality typically implies a norm which has a value of unity (1). Gell-Mann matrices, however, are normalized to a value of 2. Thus, the trace of the pair wise product results in the ortho-normalization condition $tr(\lambda_i \lambda_j) = \delta_{ij}$. where δ_{ij}. is the Kronecker delta.

This is so the embedded Pauli matrices corresponding to the three embedded subalgebras of *SU*(2) are conventionally normalized. In this three-dimensional matrix representation, the Cartan subalgebra is the set of linear combinations (with real coefficients) of the two matrices λ_3 and λ_8 which commute with each other.

There are three significant SU(2) sub algebras:

- $\{\lambda_1, \lambda_2, \lambda_3,\}$
- $\{\lambda_4, \lambda_5,$ x$\}$
- $\{\lambda_6, \lambda_7,$ y$\}$

where the x and y are linear combinations of λ_3 and λ_8. The SU(2) Casimirs of these subalgebras mutually commute. However, any unitary similarity transformation of these subalgebras will yield SU(2) subalgebras. There is an uncountable number of such transformations.

Casimir Operators and Invariants

The squared sum of the Gell-Mann matrices gives the quadratic Casimir operator, a group invariant,

$$C = \sum_{i=0}^{8} \lambda_i \lambda_j = \frac{16}{3} I.$$

where I is 3×3 identity matrix. There is another, independent, cubic Casimir operator, as well.

3.2 NTRU Operations

Traditional NTRU's polynomial structure can be predictable, allowing lattice reduction attacks to target weak instances. By integrating Gell-Mann matrices into the key generation and encryption phases, we induce additional algebraic diversity.

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

Key Generation:

- Bob randomly Choose small polynomials f, g ∈ R with invertibility modulo *p* and *q*.
- Construct $\mathbf{F=\lambda_i \cdot f}$ and $G=\lambda_j \cdot g$ where λi, λj are selected Gell-Mann matrices, operating on the polynomial coefficient vectors.
- Public Key: $h=p*G*F^{-1} \bmod q$.
- Private Key: F.

Matrices f must satisfy additional requirement to have inverse modulo p and q. Matrices g and C should have inverse modulo p. We denote these inverse by notation Fp, FQ, Gp, Cp respectively.

$f * Fq = I \pmod q$;
$g * Gp = I \pmod p$
$Gq * g = I \pmod q$

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) $\in$ 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 from the set of plaintext Lm. Next, Alice randomly choose a matrices $\phi \in L_\phi$ and Bob's public key (h, H) to compute,

For message polynomial m, select a random small polynomial r.

Compute ciphertext: c=h∗r+m mod q. (3)

where r is premultiplied by a randomly chosen Gell-Mann matrix λ_k before multiplication with h. Alice then transmit c to Bob. A different random choice of blinding value is made for each plaintext m[12].

3.5 Decryption

Compute: a=F∗c mod q.

Reduce a modulo p to recover m.

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 lie in 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 [11]. 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 compute

$D \equiv Cp * B * Gp * Wp (\text{mod } p)$ (4)

The matrix D will be Alice's original message M.

3.6 Correctness of Algorithm

Theorem 1.The equation D = M (mod p) is correct.

Proof: $D \equiv Cp * B * Gp * Wp (\text{mod } p)$
$D \equiv Cp * (w * c * M * g) * Gp * Wp (\text{mod } p)$
$D \equiv (Cp * c * M * g * Gp * w * Wp) (\text{mod } p)$
$D \equiv M.$

4. Security Analysis

- **Lattice Attack Resistance:** The Gell-Mann matrix integration randomizes the structured lattice, increasing the difficulty of applying lattice reduction methods like LLL and BKZ.
- **Quantum Security:** Retains the underlying hardness of SVP and Ring-LWE assumptions, providing post-quantum security.
- **Side-Channel Resilience:** The added randomness complicates timing and power analysis attacks due to unpredictable coefficient manipulations.

5. Conclusion

This paper propose a method, which is suitable to send large messages in the form of Gell Maan matrix and this method is more secure, since Gell Maan matrix is easy calculate for large degree of polynomial. This method is more efficient and more secure as compare to the Nayak et al [8]. This paper also introduces a **new variant of NTRU** by integrating Gell-Mann matrices to enhance algebraic randomness, improving resistance against advanced lattice attacks while preserving the lightweight nature of the NTRU cryptosystem. This method contributes towards practical post-quantum cryptography in low-resource environments.

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 in Truncated 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 Efficient Public 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 on Network(ICON-2008), New Delhi, India, pp. 12-14, 2008.
[9] Peikert, C. (2016). A Decade of Lattice Cryptography. Foundations and Trends® in Theoretical Computer Science.
[10] Roja P. P., 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.
[11] Silverman J. H., “NTRU": A Ring Based Public Key Cryptosystem, In Proc. Of ANTS III, volume 1423 of LNCS.Springer-Verlag, Available athttp://www.ntru.com, pp. 267-288, 2001.
[12] Wells A. L., “A polynomial form for logarithms modulo a prime", IEEE Transactions on Information Theory, pp. 845-846, 1984.
[13] Gell-Mann, M. (1962). Symmetries of Baryons and Mesons. Physical Review, 125(3), 1067–1084.