An overview of number theory research unit variant development security

Saba Alaa Abdulwahhab[1], Qasim Mohammed Hussien[1], Imad Fakhri Al-Shaikhli[2]
[1]Department of Computer, College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq
[2]Kulliyyah of Information and Communication Technology, IIUM Gombak Campus, Gombak, Malaysia

Article Info

Article history:

Received Apr 25, 2022
Revised Aug 19, 2022
Accepted Aug 30, 2022

Keywords:

Cryptography
NIST
NTRU
Post-quantum
Quantum

ABSTRACT

Number theory research unit (NTRU) become the most important of security in recent, with its modification of their variant, this paper search of the literature and A number of studies have examined the in public key variant development and security. In general, prior work is limited to a subset of public key increasing complexity but the benefits of speed up encryption/ decryption have not been fully established. So this paper will be the basis for those who want to develop and find proposed solutions for new studies of the NTRU algorithm. This paper aims to develop a framework to investigate the NTRU development, had been discovered that despite its development over the years and even its acceptance in round three of post quantum cryptograph, then found that limit study in the new scope of quantum facility and the ability of hybrid of new study.

Corresponding Author:

Saba Alaa Abdulwahhab
Department of Computer Science, College of Computer Science and Mathematics, Tikrit University
Tikrit, Salahuddin, Iraq
Email: saba.programmer12@tu.edu.iq

1. INTRODUCTION

Cryptography is a technique developed in data security to ensure that the original message is not accessed by an unauthorized person or entity [1]. Hoffstein and colleagues created the Number theory research unit (NTRU) cryptosystem in 1996, they looked for an efficient public-key cryptosystem that is based on restricted polynomials over polynomial rings [2], NTRU's computational complexity is O (N^2) [2]. The hard problems make the security of NTRU strong and resistant to both classical and quantum attacks. NTRU is most important post-quantum cryptosystems. The security of NTRU is linked to a very difficult problem in lattice reduction called the shortest vector problem (SVP) [3], and it is thought that there is no polynomial-time algorithm to solve this problem. The main theory used to build the NTRU cryptosystem, talk about its classical security as well as its resistance to quantum attacks [4]-[6].

In the NTRU cryptosystem, the key generation is more than 200 times faster than in the Rivest-Shamir-Adleman (RSA) cryptosystem, and the encryption is almost 3 times faster. The decryption is about 30 times faster [7] Preliminary results was showed on the working [8]. Some variants of NTRU, like Construction Throy Research Unit (CTRU), Quaternionic Theory Research Unit (QTRU), Matrix Formulation (MaTRU), Eisenstein Throy Research Unit (ETRU), a noncommutative analogue of NTRU (NNRU), Ideal lattices Throy Research Unit (ILTRU), and others are called NTRU variants [2]. The NTRU cryptosystem is more efficient and may be able to withstand quantum computers in the long run. It's because the encryption (or signature) and decryption (or varication) speeds are very fast and only use a small amount of space [6]. NTRU is based on reducing the number of lattices. The main attacks on NTRU primitives haven't focused on the hard lattice problems for the last 20 years or so. They have instead focused on other things [8]. Shor's Algorithm broke RSA and Elliptic-curve cryptography (ECC) in 1994 [9], which is why lattice-based cryptography is so important now. Good understanding of the hard problem Hardware-friendly, fast, and able to run in groups [10]. It will be about 15 years before the quantum computer is ready to be used [11], Forecasting and improving lattice reduction algorithms is still an active research subject after almost 40 years [12].

So in this paper, will review the NIRU algorithms, most of the improvements that worked on over the previous work, review and analyze them, and why they choose for the third round of post-quantum cryptography of National Institute of Standards and Technology (NIST) candidates, also this paper comparative between NTRU variant especially in public key with efficacy and their security, our contribution proposed to find by Searching most of previous studies and trying to answer the question: is quantum mechanics use to generate the public key of NTRU algorithm in those studies as a parameter or totally generation with eliminate the inverse polynomial?.

2. RESEARCH METHOD OF NTRU

The number theory research unit (NTRU) is a collection of mathematical algorithms for manipulating lists of very small integers and polynomials [9]. NTRU operations are based on objects in the $R = \frac{Z[X]}{X^N - 1}$truncated polynomial ring As a consequence [12], NTRU may achieve high speeds while using little computing resources [13]. The NTRU key generation technique requires computing the modular multiplicative inverse of F modulo p and q [14], making it the first secure public-key cryptosystem that does not depend on factorization or discrete logarithm concerns [15]. Let f, g polynomial of the form:

$$f = a_{0^{\cdot}} + a_1 X^{\cdot} + a_2 X0^1 + a_3 X1^3 + \ldots\ldots\ldots\ldots\ldots.. + a_{n-1} X^{N-1} + a_n X^N \quad (1)$$

$$g = a_{0^{\cdot}} + a_1 X^{\cdot} + a_2 X0^1 + a_3 X1^3 + \ldots\ldots\ldots\ldots\ldots.. + a_{n-1} X^{N-1} + a_n X^N \quad (2)$$

and NTRU [16] parameter is shown in detail in Table 1.

Table 1. Detail of NTRU parameters

Parameter of NTRU	Detail
N	Each truncated polynomial has degree N.
P	Small modulo
q	Large modulo
r	Random polynomial
m	Message

2.1. NTRU Key generation

To make public and private keys, first need to find the multiplicative inverse of $f\ mod\ p$ and $g\ mod\ q$ so that the public and private keys match [13], [17]. A polynomial multiplicative inverse is not always easy to find. In this case, the extended euclidean algorithm is used to find the greatest common divisor (GCD), and then a series of polynomial factorizations are used [13].

$$F_p * F \equiv 1 \quad (modp) \qquad G_p * G \equiv 1 \qquad (mod\ p) \quad (3)$$

$$F_q * F \equiv 1 \quad (modq) \qquad G_q * G \equiv 1 \qquad (mod\ q) \quad (4)$$

Public key[16] H is obtained by using the inverses of the F and G matrices to (mod q) and a random polynomial.

$$h = F_q \star g\ mod\ \mathrm{q} \quad (5)$$

2.2. Encryption of NTRU

Sender can transmit an encrypted message to recevier using the NTRU equation and a public key [18]:

$$e = \mathrm{rh} + \mathrm{m}(\mathrm{mod\ q})\ (6)$$

Receiver encrypted message now. Receiver may now transmit e to sender as (6).

2.3. Decryption of NTRU

Reciver wants to decrypt sender message that is received. Then trying to computes the polynomial, it defined by the (7) [18]-[20]:

$$a = f_e(\text{mod q}) \quad (7)$$

then computes the polynomial b defined by the expression as (8).

$$\mathbf{b} = \mathbf{a}(\text{mod}\,\mathbf{p}) \quad (8)$$

Finally, receiver computes the polynomial **C** defined by the expression as (9).

$$\mathbf{c} = \boldsymbol{f}_p\mathbf{b}\ (\text{mod p}) \quad (9)$$

The original message m will be represented by this polynomial **C**.

3. SUMMARIZE DEVELOPMENT NTRU

Many non-invertible polynomial NTRU variants exist [21], including CTRU, MaTRU, matrix formulation, QTRU, NNRU, ETRU, ILTRU, and others in Table 2 with detail. while some variations suggest using polynomial rings with coefficients in other rings or another formula [22]. The work was carried out in two phases. The first phase was to prepare an integrated table key generation, encryption, and decryption in Table 2. As for the second phase, these improvements were summarized in detail, and work on analyzing each of these parts to make this paper the basis for those who want to delve into this wide field in Table 3.

Table 2. The efficient and provably secure cryptosystem

N0.	Algorithm	key Generation	Encryption	Decryption
1	NTRU [3]	1Ć	1Ć and 1Ą	2Ć and 1Ą
2	BITRU [3], [23]	8 Ć	8Ć and 1Ą	16Ć and 1Ą
3	BOTRU [24]	8 Ć	8Ć and 4Ą	24Ć and 4Ą
4	BCTRU [25]	16 Ć	16Ć and 8Ą	32Ć and 12Ą
5	QTRU [11], [26]	16 Ć	16Ć and 4Ą	32Ć and 4Ą
6	PQTRU [3]	32 Ć	32Ć and 4Ą	64Ćand 4Ą
7	NTRS [27]	36 Ć	18Ćand 6Ą	45Ć and 6Ą
8	NTRSH [28]	54 Ć	18Ćand 6Ą	189Ć and 6Ą
9	OTRU [23]	64 Ć.	64Ć and 8Ą	1024Ć and 8Ą
10	NTRTE [11]	64 Ć	6Ć and 8Ą	96Ć and 8Ą
11	QOBTRU [23]	64 Ć.	64Ć and 8Ą	256Ć and 8Ą
12	QMNTR [29]	80 Ć	80Ć and 4Ą	1088Ć and 4Ą
13	QOTRU [30]	80 Ć	32Ćand 8Ą	38Ćand 8Ą
14	TOTRU [31]	128 Ć	128Ć and 16Ą	1536Ć and 16Ą
15	HXDTRU [3], [32]	256 Ć.	256Ć and 16Ą	4096Ć and 16Ą

Table 2 shows Ć it is the mean convolution multiplication, and Ą it is the mean polynomial addition the addressed algorithms in Table 2 displayed the ratio of convolution in key generation and encryption/decryption arranged from low to high security with better efficiency. The increased value of convolution made the algorithm more efficient but with the lowest speed encryption-decryption process.

3.1. NTRU variant

Table 3 in APPENDIX shows the surmise of previous research in the same algorithm. But different in public key or finite field based on year. There is an increment in research done in the NTRU algorithm as shown below.

3.2. Discussion

Overall the summary show a high level of agreement in the majority of cases of the mechanism of encryption/decryption of the NTRU expect their key generation is change of the most previous studies as Table 3 shows as many study had been checked in literature finding more information on topic of NTRU public key generation where it was found some of NTRU public key development dependent on multidimensional others depended on replacing the original ring in NTRU like quaternion algebra or Eisenstein, integer algebra and others mathematic algebra. The public key system has been modified and made more secure as a result of this change. In this case, an analytical solution cannot be easily obtained when comparison between the complexity as increasing but lowest speed of encryption and decryption, in this case lead as to ask question how to balance between the complexity of public key and speed of encryption/decryption, this question lead as to think a new method of public key generation is presented and compared with classical way and try to think is quantum is efficient to solve this problem Research in these areas requires studies of topic quantum area. And if the properties of quantum mechanics are used, the degree of complexity can be $\sqrt{N}$, and it is better from the original case is N^2. These findings could also be applicable in cases of better speed up the time execution. While maintaining or even increasing the complexity of the data. The result of the study now provides evidence to it is still open way further thinking about the mechanism of evolution, although NTRU was chosen on third round of post quantum cryptography and also it resistance to Shor's algorithm.

4. CONCLUSION

NTRU was discovered to have an edge over the method in terms of arithmetic operations since it is both quick and requires less storage space. As a result, NTRU has become an extremely ideal alternative for a wide range of applications. as this paper has been presented the most of the wide NTRU development variants, collected these studies and summarized them to be a basic base for those who want to research About the mechanism and how to develop this algorithm, and this is very important for future works, especially NTRU since it was chosen from NIST in round 3 of post-quantum cryptography. Also, this paper, has founded that quantum mechanics has never been used in generating the public key, as a parameter or totally generation with eliminate the inverse polynomial, so this is the answer of the question has been asked at the beginning this paper.

APPENDIX

Table 3. NTRU Previous work with variant and our analysis

N0. Ref	Algorithm	Principle	Finite field /deg	Public key	Attacks	Analysis
[33], [34]	NTRU Non-inveritable	It is possible to use NTRU with non-invertible polynomials to extend the capabilities of NTRU Encrypt to include non-invertible polynomials as a means of overcoming the difficulty in locating an invertible polynomial using NTRU Encrypt.	$R_p = \frac{Z_p[x]}{(x^N-1)}$ $R_q = \frac{Z_q[x]}{(x^N-1)}$	$h = F_q \star g \bmod q$	• Attack on private key • Brute force attack • Meet in the middle attack • Lattice attack	• it speedup than original NTRU This extension avoids the challenge of finding "enough" invertible polynomials.
[8], [25], [35], [36]	C_TRU	CTRU develops NTRU encrypt over a binary finite field F2 that is safe against Popov normal form attacks but is entirely vulnerable to linear algebra-based attacks. As a result, CTRU has a non-commutative, secure variation known as NETRU.	$\frac{f_2[T][X]}{X^N-1}$	$H = g / f \ (mod\ Q)$	• Private Attack on the key, • Meet in the middle attack, • Multiple transmission attack • Attack on public key using Popov normal form	• CTRU is completely insecure to meet the security criterion for valid decryption • CTRU neither improves Performance protects linear algebra attacks
[16], [37]	Ma_TRU	MaTRU uses the linear transformation of two-sided matrix multiplication to work on the ring of k by k matrices of a polynomial in R. MaTRU uses the same number of bits per message as NTRU Encrypt when nk2 = N	$\frac{M_k(L)[X]}{X^{11}-I_{k\times k}}$	$h = F_q \star W * G_q modq$	• Brute force attack • Lattice attack	• MaTRU's mproved linear transformation efficiency results in significant speed increases of a factor of O(k) over NTRU.

Table 3. NTRU Previous work with variant and our analysis (*continue*)

N0. Ref	Algorithm	Principle	Finite field /deg	*Public key*	Attacks	Analysis
[2], [38]	GN_TRU	NTRU Encrypt over the ring of Gaussian integers Z[i] = $\{a+ib: a,b \in \mathbb{Z}, i^2=-1\}$ Is proposed by GNTRU. GNTRU is significantly more resistant to lattice attacks than NTRU Encrypt but is not as efficient.	$\frac{\mathbb{Z}[i][X]}{X^N-1}$	$h = f_q \star g \; modq$	Brute force attack	That the security of NTRU, ETRU, and GNTRU in terms of decryption failure is very similar.
[14], [39], [40]	Matrix_NTRU	Matrix NTRU is the matrix formulation of NTRU Encrypt. This is because the matrix formulation form is more secure when the matrix is invertible or when the matrix has a determinant. Additionally, it may verify that encryption and decryption operate properly without requiring the parameters p and q to be fixed.	$\frac{M(\mathbb{Z})[X]}{X^n-I}$	H = p$^*Xq^*$Y(modulo q)	A matrix is only invertible when it is determinant is discovered	has the capability of transmitting massive amounts of data in the form of matrices, but drawback of If one of the matrix positions is identified
[41]	GB_NTRU	GB-NTRR generalizes NTRU Encrypt to a multivariate polynomial, which in its system is a bivariate polynomial. GB-NTRU may be extended to a twisted group ring variation of NTRU, which contains NTRU defined by x N + 1 and QTRU. It is a critical future task to explore the security of variation of NTRU in the broad framework	$\frac{\mathbb{Z}[X,Y]}{(X^N-1, Y^N-1)}$	$h = p \cdot g/f + \alpha$	Lattice attack Brute force attack	It may allow for the selection of smaller f and g allowing for the selection of larger r and m.
[2], [42], [43]	NNRU	NNRU operates on the ring of k by k polynomial matrices in R. In comparison to NTRU Encrypt, NNRU is considered to be more secure against lattice-based attacks. By setting N equal to n(k2), NTRU Encrypt and NNRU have the same plaintext block size.	$\frac{M_k(\mathbb{Z})[X]}{X^n-I_{k\times k}}$	$h \equiv wG_q(modq)$ $H \equiv F_q c(modq)$	• Brute force attack, • Meet in the middle attack, • Multiple transmission attacks.	NNRU is fully safe against lattice attacks and has a large speed boost.
[38]	G_TRU	NTRU Encrypt is generalized over a larger algebra than the Dedekind domain, D. GTRU's underlying algebra can be non-commutative (quaternion algebra or four-dimensional algebra) or even non-associative (octonion algebra or algebra of dimension eight).	$\frac{\mathcal{D}[X]}{X^N-1}$	$\mathfrak{h} = \bar{\pi}_Q(\mathfrak{f}_Q \circ \mathfrak{g})$	Lattice attack	The suggested GTRU for IoT is more secure than NTRU. As a result, the GTRU for IoT
[2], [24], [23]	O_TRU	The octonion variant of NTRU Encrypt is proposed by OTRU. OTRU's operation is based on a non-associative octonion algebra, $\mathbb{A} := \{a_0(x) + \sum_{i=1}^{7} a_i(x)e_i \mid a_0(x), \cdots, a_7(x) \in R\}$ where $R = \mathbb{Z}[X]/(X^N-1)$ OTRU is faster than NTRU Encrypt	$\frac{\mathbb{Z}[X]}{X^N-1}$ Octonion algebra (non-associative algebra)	$H = F_q^{-1} \circ G \in A_q$	• Brute force attack, • Meet in the middle attack, • Multiple transmission attack, • Message expansion	OTRU design and execution will be simple, quick dependable, and cost-effective. It slower than original NTRU

Table 3. NTRU Previous work with variant and our analysis (*continue*)

N0. Ref	Algorithm	Principle	Finite field /deg	Public key	Attacks	Analysis
[12], [44], [2], [30], [31]	Q_TRU	NTRU Encrypt quaternion version is presented. QTRU's operation necessitates the use of a noncommutative quaternion algebra, $\mathbb{H} = \{a + ib + jc + kd \mid a, b, \mathbb{Z}, i^2 = j^2 = k^2 = ijk = -1\}$.	$\frac{(-1,-1)}{\mathbb{Z}[X]/(X^N-1)}$ Based on quaternion algebra	H= H*P mod q	• Brute force attack, • Lattice attack, • Message expansion	• It has a very complicated and secure fundamental structure. • Hard to be attack by LLL
[45]	DB_TRU	NTRU designs Encrypt over a ring of binary truncated polynomials with positive integer coefficients that are dual special types, $R_N[x] = GF(2)[x]/(x^N - 1) \mid N \in Z^+$. DBTRU outperforms NTRU Encrypt in terms of theoretical performance and security.	$\frac{GF(2)[x]}{x^N-1} \mid N$	$h = g * F_l * SmodL$	• Meet-in-the-middle attacks • Multiple transmission attacks • Brute-force attacks. • Attack on f by using algebraic linear equations	DBTRU equals NTRU in speed DBTRU's massage-expansion factors are somewhat greater than NTRU's.
[11], [46], [47]	E_TRU	NTRU Encrypt is presented over the Eisenstein integer ring, $\mathbb{Z}[\omega] = \{a + \omega b \mid a, b \in \mathbb{Z}, i^2 = -1, \omega = e^{2i\frac{\pi}{3}}\}$	$\frac{\mathbb{Z}[\omega][X]}{X^N-1}$ Ring of Eisenstein integers Z[W]	H= f*g mod q	• Brute force attack, • Attack on the private key, • Meet in the middle attack, • Multiple transmission attack	The security of NTRU, ETRU, and GNTRU in terms of decryption failure is very similar. However, in the most recent security releases.
[2], [38]	GR-NTRU	NTRU is derived Over a group ring, encrypt: $\mathbb{Z}[G] = \{\sum_{g\in G} a_g[g] \mid a_g \in \mathbb{Z}(\forall g \in G)\}$. GR-NTRU is less safe than NTRU Encrypt, according to the security comparison.	$\frac{\mathbb{Z}[G][X]}{X^N-1}$	$h \equiv f'^{-1}g' \ MOD \ q$ f successful keys are more than 1/1000	• Brute force attack, • Attack on the private key, • Meet in the middle attack, • Multiple transmission attacks, Lattice attack	Among these GR-NTRUs, the original NTRU and multivariate NTRU are the most secure. It is possible to expand the encryption to a functional level.
[48]	BI_TRU	Suggests NTRU Encrypt as an alternative to binary algebra, $BN_{R=} \{a + bj \mid j^2 = 1, a, b \in \mathbb{R}\}$ BITRU is a multidimensional cryptosystem that can encrypt two independent communications from two different sources using two public keys, h and k. BITRU Encrypt has a higher level of security than NTRU Encrypt.	$\frac{\mathbb{Z}[X]}{X^N-1}$	$h = \phi\, f_q \ mod\ (q)$ $k = g_q\, w \ mod\ (q)$	• Attacking on private key	BITRU has four times the security of NTRU due to the presence of two public keys h,k and four polynomial private keys.
[49]	CQ_TRU	NTRU Encrypt is presented over a commutative quaternion ring, $A = \{a + bi + cj + dk \mid a, b, c, K, i^2 = a, j^2 = b, ij = k\}$. CQTRU is capable of encrypting and decrypting four messages concurrently and is immune to alternate key attacks, brute force attacks, and lattice attacks. CQTRU is a more secure encryption method than NTRU Encrypt.	$\frac{A[X]}{X^N-1}$	$H = F_q \cdot G \ mod\ q$	• Brute Force Attacks • Lattice Attack	-CQTRU allows for small polynomial dimensions while maintaining a high level of security. -CQTRU has four dimensions, so it can encrypt and decrypt four messages at same time

Table 3. NTRU Previous work with variant and our analysis (*continue*)

N0. Ref	Algorithm	Principle	Finite field /deg	Public key	Attacks	Analysis
[32]	HXD_TRU	NTRU is derived Encrypt hexadecimal algebraically $\Psi = \{r_0 + \sum_{i=1}^{15} r_i x_i \mid r_0, r_1, \dots, r_{15} \in K\}$ where: $\frac{\mathbb{Z}[X]}{X^N - 1}$ HXDTRU with an N-dimensional array is sixteen times faster than NTRU Encrypt with a 16-dimensional array.	$\frac{\mathbb{Z}[X]}{X^N - 1}$	$H = F_q \cdot G \in \Psi_q$	• Brute Force Attack • Alternate Keys Attack • Lattice based Attacks	The HXDTRU is a multidimensional cryptosystem capable of encrypting messages of length 16N in a single round (i.e. sixteen messages from a single source.
[42], [50], [30]	I_TRU	NTRU Encrypt is presented over the ring of integers modulo n denoted by Z=nZ. As the comparison in the key generation, ITRU is only required O(N2) whereas NTRU Encrypt is required O $\left(N^2(\log^2 p + \log^2 q)\right)$	$\frac{(\mathbb{Z}/n\mathbb{Z})[X]}{X^N - 1}$ Based on ideal lattices	$h = pg/f \in R_q^*$	• Brute force attack, • Attack on the private key, • Meet in the middle attack,	ITRU provides several advantages over NTRU, including a simpler parameter selection process, inevitability.
[51]	SQ_TRU	Presents NTRU Encrypt over coquaternions (also known as spit quaternion algebra), which is a new type of encryption over coquaternions. $H = \{q = q_0 + q_1 i + q_2 j + q_3 k; q_0, q_1, q_2, q_3 \in R\}$ where Ty $R = \mathbb{Z}[x]/(x^N - 1)$.	$\frac{(-1,-1)}{\mathbb{Z}[x]/(x^N - 1)}$	$H = F \circ G_q(modq)$	• Brute Force Attack • Lattice based attacks	The present lattice attack algorithms have a hard time attacking it.
[49], [52]	Pair_TRU	In this step, will create an NTRU Encrypt over the non-commutative matrix ring composed of k*k matrixes of polynomials for Z*Z and establish the NTRU Encrypt over it. In comparison to NTRU Encrypt, PairTRU is more resistant to linear algebra-based and lattice-based attacks.	$\frac{M(k, \mathbb{Z} \times \mathbb{Z})[x]}{(I_{k\times k}, I_{k\times k})x^N - (I_{k\times k}, \quad {}_{k\times k}}$	$h \equiv w * G_(q,q)mod(q$ $H \equiv F_(q,q) * cmod(q$	• Brute Force Attack • Chosen Ciphertext Attacks • Message Expansion • Multiple Transmission Attack • Lattice Attack	PairTRU, the cryptosystem is resistant to linear algebra and Lattice-based attacks. PairTRU is based on the NTRU core and use two-sided matrix multiplication.
[53]	D_NTRU	The definition of the truncated polynomial ring is introduced using the NTRU Encrypt as a point of reference. To complete its security proof of IND-CPA (Indistinguishability under Chosen Plaintext Attack), DNTRU additionally makes use of another cryptosystem, namely C-NTRU, as an aid.	$\frac{\mathbb{Z}[X]}{X^N - 1}$	$h_1 = \langle p \otimes f_{q_1}^{-1} \otimes g \rangle_{q_1}$ $h_2 \leftarrow_R \mathrm{R}_{q_2}$	Brute force attacks	The D-NTRU PKC algorithm uses a smaller ciphertext expansion than the original NTRU algorithm and is more efficient than NTRU.

Table 3. NTRU Previous work with variant and our analysis (*continue*)

N0. Ref	Algorithm	Principle	Finite field /deg	Public key	Attacks	Analysis
[54], [52]	D_TRU1	Designs on the ring of dual integers (or the ring with no divisors) are shown. $\mathbb{D}=\mathbb{Z}+\epsilon\mathbb{Z}, \epsilon^2=0$ At	$\frac{\mathbb{D}[X]}{X^N-1}$	$h=p$ t $.(f_q*g)(modq)$	• Brute force attacks • Meet-in-the-Middle attack • Lattice attacks	Provides the same degree of security as NTRU while more secure than NTRU, it is also less efficient.

REFERENCES

[1] J. I. Ahmad, R. Din, and M. Ahmad, "Analysis review on public key cryptography algorithms," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 2, pp. 447–454, Nov. 2018, doi: 10.11591/ijeecs.v12.i2.pp447-454.

[2] S. Singh and S. Padhye, "Generalisations of NTRU cryptosystem," *Security and Communication Networks*, vol. 9, no. 18, pp. 6315–6334, Dec. 2016, doi: 10.1002/sec.1693.

[3] H. R. Yassein and N. M. G. Al-Saidi, "A comparative performance analysis of NTRU and its variant cryptosystems," in *International Conference on Current Research in Computer Science and Information Technology, ICCIT 2017*, Apr. 2017, pp. 115–120, doi: 10.1109/CRCSIT.2017.7965544.

[4] A. Nitaj, "The mathematics of the NTRU public key cryptosystem," *Mathematical Concepts IGI Global*, pp. 1–16, 2012, [Online]. Available: https://nitaj.users.lmno.cnrs.fr/ntru3final.pdf.

[5] H. Wu and X. Gao, "Efficient multiplier and FPGA implementation for NTRU Prime," in *Canadian Conference on Electrical and Computer Engineering*, Sep. 2021, vol. 2021-September, pp. 1–5, doi: 10.1109/CCECE53047.2021.9569160.

[6] J. Bi and L. Han, "Lattice attacks on NTRU revisited," *IEEE Access*, vol. 9, pp. 66218–66222, 2021, doi: 10.1109/ACCESS.2021.3076598.

[7] H. R. Hashim, A. Molnár, and S. Tengely, "Cryptanalysis of ITRU," *Rad Hrvatske Akademije Znanosti i Umjetnosti, Matematicke Znanosti*, vol. 25, pp. 181–193, 2021, doi: 10.21857/yrvgqtexl9.

[8] H. R. Yassein and N. M. G. Al-Saidi, "An innovative bicartisian algebra for designing of highly performed NTRU like cryptosystem," *Malaysian Journal of Mathematical Sciences*, vol. 13, pp. 77–91, 2019.

[9] A. Bhowmik and U. Menon, "Enhancing the NTRU Cryptosystem," *International Journal of Computer Applications*, vol. 176, no. 29, pp. 46–53, Jun. 2020, doi: 10.5120/ijca2020920320.

[10] J. Y. Baek, "NTRU hardware accelerator based on fast convolution methods for post-quantum cryptography," Doctoral Theses, 2021.

[11] H. R. Yassein, N. M. G. Al-Saidi, and A. K. Jabber, "A multi-dimensional algebra for designing an improved NTRU cryptosystem," *Eurasian Journal of Mathematical and Computer Applications*, vol. 8, no. 4, pp. 97–107, 2020, doi: 10.32523/2306-6172-2020-8-4-97-107.

[12] M. Albrecht and L. Ducas, "Lattice attacks on NTRU and LWE: A history of refinements," computational cryptography, pp. 15–40, 2021, doi: 10.1017/9781108854207.004.

[13] G. J. Nyokabi, M. Salleh, and I. Mohamad, "NTRU inverse polynomial algorithm based on circulant matrices using gauss-jordan elimination," in *2017 6th ICT International Student Project Conference (ICT-ISPC), May 2017*, vol. 2017-Janua, pp. 1–5, doi: 10.1109/ICT-ISPC.2017.8075326.

[14] J. N. Gaithuru, M. Salleh, and I. Mohamad, "NTRU inverse polynomial algorithm based on the LU decomposition method of matrix inversion," in *2017 IEEE Conference on Applications, Information and Network Security, AINS 2017*, Nov. 2017, vol. 2018-January, pp. 1–6, doi: 10.1109/AINS.2017.8270415.

[15] Z. Qin, R. Tong, X. Wu, G. Bai, L. Wu, and L. Su, "A compact full hardware implementation of PQC algorithm NTRU," in *2021 IEEE 3rd International Conference on Communications, Information System and Computer Engineering, CISCE 2021*, May 2021, pp. 792–797, doi: 10.1109/CISCE52179.2021.9446042.

[16] S. Akleylek and N. Kaya, "New quantum secure key exchange protocols based on MaTRU," in *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding*, Mar. 2018, vol. 2018-January, pp. 1–5, doi: 10.1109/ISDFS.2018.8355362.

[17] M. Bufalo, D. Bufalo, and G. Orlando, "A note on the computation of the modular inverse for cryptography," *Axioms*, vol. 10, no. 2, p. 116, Jun. 2021, doi: 10.3390/axioms10020116.

[18] B. Clark, Understanding the NTRU Cryptosystem. Williams Honors College, Honors Research Projects, 2019.

[19] A. Pellet-Mary and D. Stehlé, "On the Hardness of the NTRU Problem," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13090 LNCS, 2021, pp. 3–35.

[20] R. Asif, "Post-quantum cryptosystems for internet-of-things: a survey on lattice-based algorithms," IoT, vol. 2, no. 1, pp. 71–91, Feb. 2021, doi: 10.3390/iot2010005.

[21] W. D. Banks and I. E. Shparlinski, "A variant of NTRU with non-invertible polynomials," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2551, 2002, pp. 62–70.

[22] J. N. M. S. Gaithuru, "ITRU: NTRU-based cryptosystem using ring of integers," *International Journal of Innovative Computing*, vol. 7, no. 1, pp. 33–38, 2017.

[23] H. R. Yassein, N. M. G. Al-Saidi, and A. K. Farhan, "A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 2, pp. 523–542, Feb. 2022, doi: 10.1080/09720529.2020.1741218.

[24] H. H. Abo-Alsood and H. R. Yassein, "Design of an alternative NTRU encryption with high secure and efficient," *International Journal of Mathematics and Computer Science*, vol. 16, no. 4, pp. 1469–1477, 2021.

[25] H. R. Yassein and N. M. G. Al-Saidi, "BCTRU: A new secure NTRUCrypt public key system based on a newly multidimensional algebra," in *Proceedings of the 6th International Cryptology and Information Security Conference 2018, CRYPTOLOGY 2018*, 2018, pp. 1–11.

[26] O. S. Guma'a, Q. M. Hussein, and Z. T. M. Al-Ta'i, "Q-NTRU cryptosystem for IoT applications," *Journal of Southwest Jiaotong University*, vol. 54, no. 4, 2019, doi: 10.35741/issn.0258-2724.54.4.15.

[27] S. H. Shahhadi and H. R. Yassein, "A new design of NTRUEncrypt-analog cryptosystem with High security and performance level via tripternion Algebra," *International Journal of Mathematics and Computer Science*, vol. 16, no. 4, pp. 1515–1522, 2021.

[28] S. H. Shahhadi and H. R. Yassein, "NTRsh: A new secure variant of NTRUEncrypt based on tripternion *Algebra," Journal of Physics: Conference Series*, vol. 1999, no. 1, p. 012092, Sep. 2021, doi: 10.1088/1742-6596/1999/1/012092.

[29] H. R. Yassein, A. A. Abidalzahra, and N. M. Al-Saidi, "A new design of ntru encryption with high security and performance level," *AIP Conference Proceedings*, vol. 2334, 2021, doi: 10.1063/5.0042312.

[30] H. H. Abo-Alsood and H. R. Yassein, "QOTRU: A new design of NTRU public key encryption via Qu-Octonion Subalgebra," *Journal of Physics: Conference Series*, vol. 1999, no. 1, p. 012097, Sep. 2021, doi: 10.1088/1742-6596/1999/1/012097.

[31] H. H. Abo-Alsood and H. R. Yassein, "Analogue to NTRU public key cryptosystem by multi-dimensional algebra with high security," in *AIP Conference Proceedings*, 2022, vol. 2386, p. 060006, doi: 10.1063/5.0067033.

[32] H. R. Yassein and N. M. G. Al-Saidi, "HXDTRU cryptosystem based on hexadecnion algebra," in *Proceedings of the 5th International Cryptology and Information Security Conference 2016, CRYPTOLOGY 2016*, 2016, pp. 1–10.

[33] G. De Micheli, N. Heninger, and B. Shani, "Characterizing overstretched NTRU attacks," *Journal of Mathematical Cryptology*, vol. 14, no. 1, pp. 110–119, Jun. 2020, doi: 10.1515/jmc-2015-0055.

[34] N. M. G. Al-Saidi and H. R. Yassein, "A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure," *Malaysian Journal of Mathematical Sciences*, vol. 11, no. S3, pp. 29–43, 2017.

[35] N. Vats, "Algebraic Cryptanalysis of CTRU Cryptosystem," in *Computing and Combinatorics*, vol. 5092 LNCS, Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 235–244.

[36] R. E. Atani, S. E. Atani, and A. H. Karbasi, "NETRU: A non-commutative and secure variant of CTRU Cryptosystem," *The ISC International Journal of Information Security*, vol. 10, no. 1, pp. 45–53, 2018, [Online]. Available: http://www.isecure-journal.org.

[37] M. Coglianese and B.-M. Goi, "MaTRU: A new NTRU-based cryptosystem," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3797 LNCS, 2005, pp. 232–243.

[38] L. Shuai, H. Xu, L. Miao, and X. Zhou, "A group-based NTRU-like public-key cryptosystem for IoT," *IEEE Access*, vol. 7, pp. 75732–75740, 2019, doi: 10.1109/ACCESS.2019.2920860.

[39] B. P. Tripathi and K. Thakur, "NTRU cryptosystem with companion matrix," *International Journal of Pure and Applied Mathematical Sciences*, vol. 9, no. 2, pp. 203–209, 2016.

[40] R. Nayak, C. V. Sastry, and J. Pradhan, "A matrix formulation for NTRU cryptosystem," in *2008 16th IEEE International Conference on Networks*, 2008, pp. 1–5, doi: 10.1109/ICON.2008.4772602.

[41] T. Yasuda, X. Dahan, and K. Sakurai, "Characterizing NTRU-Variants Using Group Ring and Evaluating their Lattice Security.," IACR Cryptology ePrint Archive, vol. 2015, p. 1170, 2015.

[42] N. Salleh and H. Kamarulhaili, "NTRU public-key cryptosystem and its variants : an overview," *International Journal of Cryptology Research*, vol. 10, no. 1, pp. 1–21, 2020.

[43] N. Vats, "NNRU, a noncommutative analogue of NTRU," *arXiv preprint arXiv:0902.1891*, 2009, [Online]. Available: http://arxiv.org/abs/0902.1891.

[44] O. S. Guma'a, Q. M. Hussein, and Z. T. Mustafa Al-Ta'i, "Dynamic keys generation for internet of things," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, p. 1066, May 2020, doi: 10.11591/ijeecs.v18.i2.pp1066-1073.

[45] C. M. Thang and N. Binh, "DBTRU, a new NTRU-like cryptosystem based on dual binary truncated polynomial rings," in *2015 2nd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS)*, Sep. 2015, pp. 11–16, doi: 10.1109/NICS.2015.7302172.

[46] R. E. Atani, S. E. Atani, and A. H. Karbasi, "A provably secure variant of ETRU based on extended ideal lattices over direct product of dedekind domains," *Journal of Computing and Security*, vol. 5, no. 1, pp. 13–34, 2018, doi: 10.22108/jcs.2018.106856.0.

[47] K. Jarvis and M. Nevins, "ETRU: NTRU over the Eisenstein integers," *Designs, Codes and Cryptography*, vol. 74, no. 1, pp. 219–242, Jan. 2015, doi: 10.1007/s10623-013-9850-3.

[48] N. M. G. and H. R., "BITRU: Binary Version of the NTRU public key cryptosystem via binary algebra," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 11, 2016, doi: 10.14569/IJACSA.2016.071101.

[49] A. A. Majid, "CQTRU: A commutative quaternions rings based public key cryptosystem," Engineering and Technology Journal, vol. 34, no. 6, pp. 901–911, 2016.

[50] A. H. Karbasi and R. E. Atani, "ILTRU: An NTRU-Like public key cryptosystem over ideal lattices," IACR Cryptol. ePrint Arch., vol. 2015, p. 549, 2015, [Online]. Available: http://eprint.iacr.org/2015/549.

[51] K. Thakur, "A Variant of NTRU with split quaternions algebra," *Palestine Journal of Mathematics*, vol. 6, no. 2, pp. 598–610, 2017.

[52] A. Hassani Karbasi, S. Ebrahimi Atani, and R. Ebrahimi Atani, "PairTRU: Pairwise Non-commutative extension of The NTRU public key Cryptosystem," *International Journal of Information Security Science*, vol. 7, no. 1, pp. 11–19, 2018.

[53] B. Wang, H. Lei, and Y. Hu, "D-NTRU: More efficient and average-case IND-CPA secure NTRU variant," *Information Sciences*, vol. 438, pp. 15–31, 2018, doi: 10.1016/j.ins.2018.01.037.

[54] M. G. Camara, D. Sow, and D. Sow, "DTRU1: first generalization of NTRU using dual integers," *International Journal of Algebra*, vol. 12, no. 7, pp. 257–271, 2018, doi: 10.12988/ija.2018.311115.

BIOGRAPHIES OF AUTHORS

Saba Alaa Abdulwahhab she has received her bachelor degree from department of computer science, college of Com-puter Science and Mathematics, Tikrit University from 2006-2010. She is currently purse her master degree at same department. Her research interest in cryptography, quantum cryptog-raphy, post quantum cryptography and information security. She can be contacted at email: saba.programmer12@tu.edu.iq.

Prof. Dr. Qasim Mohammed Hussein he has Ph.D degree in computer sciences from Technology University, and currently Professor at Tikrit University. He published 26 journal articles in the fields of cryp-tography and computer security, He participated in writing 5 books in computer science. He was a member of the editorial board of Journal of Pure Science at the University of Tikrit. He attended many conferences and scientific symposia, in-side and outside of Iraq, and has a number of lectures and field studies in the field of computer. He can be contacted at email: kasimalshamry@tu.edu.iq.

Prof. Dr. Imad Fakhri Al-Shaikhli is a professor and the head of research at IIUM (International Islamic University Malaysia). He is also a lecturer at the Faculty of Information and communication Technology. He is a IEEE senior member, obtained his BSc (Hon) in Mathematics, MSc in Computer Science from Iraq, and Ph.D degree from Pune University, India, 2000. He has been the editor in chief of international journal on Advanced Computer Science and Technology Research since 2011 now, and the general chair of the international conference on Advanced Computer Science Applications and Technologies since 2012 till now. Prof. Imad has published more than 100 papers, journals and book chapters in addition to three books. He can be contacted at email: imadf@iium.edu.my.