Journal of Wasit for Science and Medicine 2024: 17 (1), 1-10

Proposed Development of NTRU Public Key Cryptosystem

Marwah Aearaby Sayyid

Wasit Education Directorate, Al-Rabab High School for Distinguished Students

Abstract

As life progresses and develops, cryptography has become an indispensable science. The development of this science has given flexibility and security in exchanging information and data of various kinds by making it difficult for unauthorized persons to access them.

In this paper, we proposed a new NTRU-like encryption scheme using a different mathematical structure for the public key, as well as for text encryption and decryption to have more resistance to attacks, which makes this method suitable for many applications.

1. Introduction

Online banking and shopping have made cryptography commonplace. Many users also prefer to encrypt their data, while others encrypt emails. As a result, to comprehend modern encryption, one must first comprehend the mathematics that underpins it. The strength of encryption is affected by the computational complexity of the algorithms employed to decrypt it. In 1997, Coppersmith and shamir [1] demonstrated the NTRU encryption effectiveness against Lattice attacks. In 2002, Gaborit et al. [2], introduced a new cipher system analogous to NTRU called CTRU, which is based on the $F_2[x]\ /(x^N - 1)$. In 2005, Coglianese and Goi [3] presented an improved cipher system for NTRU called MaTRU, which uses a more efficient linear transformation with a security level like that of NTRU. In 2007, Sari and Puri [4] used the same key to encrypt and decrypt data using a stream of ciphers. In 2009, a quaternion-based public key cryptosystem QTRU is constructed by Malekian et al. [5], the conclusion is that QTRU is more resistant to some attacks than NTRU.

In 2010, a new version of the NTRU cipher system was introduced by researchers Nevins et al. [6] in which the original NTRU ring is replaced by the Einstein integers

ring, such that $Z + \omega Z = \{ a + \omega b \mid a, b \in Z, i^2 = -1, \omega = e^{2i\frac{\pi}{3}} \}$. In 2010, Malekian and Zakerolhosseini [7] suggested a new algebra called Octonion algebra which is characterized by being noncommutative, non-associative, and by having alternative algebraic structure, this algebra is used to structure a new public key cryptosystem called OTRU. In 2013, Lei and Liao [8] used the NTRU lattice cryptosystem to create a new NTRU key exchange protocol. In 2015, Majeed [9] proposed CQTRU, a new cryptosystem based on commutative quaternion algebra, CQTRU is more resistant to attacks than NTRU.

In 2016, Yassein and Al-saidi [10], [11], [12] presented the binary and hexadecnion algebras and this algebra is used to structure BITRU and HXDTRU, respectively.

in 2018, Yassein and Al-saidi [13], [14] suggested a new public key cryptosystem analogous to NTRU based on bi-cartesian algebra which is called BCTRU. In 2019, Lyubashevsky and Seiler [15] created NTTRU, which creates public keys and cipher text with an approximate size of 1.25 KB at the 128- bit security level using the number theoretic transform (NTT) over the cyclotomic ring $Z_{7681}[x] \ / \ (x^{768} - x^{384} + 1)$. In 2020, Yassein et al. [16] suggested a new algebra called carternion algebra. This algebra is used to structure a new cipher system called QOB_{TRU}. In 2020, Yassein et al. [17] proposed a new commutative quaternion algebra to create a new public key cryptosystem called NTRTE.

In 2021, Yassein et al. [18] presented QMNTR, a new mathematical structure with two public and five private keys, as an enhanced cipher system for QTRU. Shihadi and Yassein [19] introduced a new public key cryptosystem analogous NTRU based on tripternion algebra which is called NTRS. Also, Abo-alsood and Yassein [20] suggested the bi-octonion subalgebra of octonion algebra, which is used to create a new public key cryptosystem called BOTRU. Shihadi and Yassein [21] introduced a new public key cryptosystem analogous NTRU based on tripternion algebra which is called NTR_{SH}. Abo-alsood and Yassein [22] suggested the subalgebra of octonion algebra called Qu-octonion subalgebra, which is characterized as being non-commutative and associative. This algebra is used to structure the cipher system called QOTRU.

In 2022, Shihadi and Yassein [23] suggested an improved NTRU system called NTR_{TRN}. Also, Abo-alsood and Yassein [24] proposed an encryption system that is characterized by its security and high efficiency, called TOTRU.

In 2023, Yassein et al. [25] design Secure Variant of NTRU-encrypt called QuiTRU via multi-dimensional HH-Real algebra. Also, Yassein et al. [26] proposed an alternative to QTRU called AH_{QTR} depends on sign based on quaternion algebra.

2. NTRU Cryptosystem

This section proposed a brief about the NTRU [1]. It based on the truncated polynomial ring of degree $N-1$, where N is prime number. NTRU indicated by $K = Z[x]/(x^N-1)$, such that $K_p = Z_p[x]/(x^N-1)$ and $K_q = Z_q[X]/(x^N-1)$ refer to ring of truncated polynomial $mod\ p$ and $mod\ q$ respectively, where $gcd(N,q)=1$ and $gcd(p,q)=1$ with q is significantly larger than p. The basic subsets which used in NTRU defined as the following:

such that $f(x)$ has d_f coefficients equal to 1, d_f-1 equal to -1 and $L_f = \{f \in K|$ the rest 0$\}$.

such that $g(x)$ has d_g coefficients equal to 1, d_g equal to -1 and the $L_g = \{g \in K|$ rest 0$\}$.

such that $r(x)$ has d_r coefficients equal to 1, d_r equal to -1 and the $L_r = \{r \in K|$ rest 0$\}$.

$L_m = \{m(x) \in K|\ m(x)$ is chosen modulo p between $-p/2$ and $p/2\}$.

Table 1 shows the three phases of the NTRU cryptosystem:

Table 1: Summarize of NTRU cryptosystem

Alice	Bob
Key generation	
Choose private $f \in L_f$ that invertible in K_q and K_p. Choose private $g \in L_g$. Compute f_q^{-1} inverse of f in K_q. Compute f_p^{-1} inverse of f in K_p. Compute $h = f_q^{-1} * g(mod\ q)$. Send h to Bob	
Encryption	

	Choose the plaintext $m \in L_m$. Choose a random $r \in L_r$. Use the public key h to compute $e = ph * r + m(mod\ q)$. Send the ciphertext e to Alice.
Decryption	
Compute $a = f * e(mod\ q)$ $= pg * r + f * m(mod\ q)$. Compute $m = f_p^{-1} a(mod\ p)$.	

3. TATRU Cryptosystem

A new public key cryptosystem is introduced called TATRU which depends on truncated polynomial rings $K = Z[x]/(x^N - 1)$, $K_p = Z_p[x]/(x^N - 1)$ and $K_q = Z_q[x]/(x^N - 1)$ and the same public parameters (N, p, q), L_f, L_r, L_g, and L_m in NTRU and subsets L_w, L_φ and L_α which are defined as following:

$L_w = \{w \in K|$ such that w has d_w coefficients equal to 1, $(d_w - 1)$ equal to -1 and the rest $0\}$,

$L_\varphi = \{\varphi \in K|$ such that φ has d_φ coefficients equal to 1, $(d_\varphi - 1)$ equal to -1 and the rest $0\}$,

$L_\alpha = \{\alpha \in K|$ such that α has d_α coefficients equal to 1, d_α equal to -1 and the rest $0\}$.

The TTRU cryptosystem goes through three phases, which are summarized as follows:

I. Key generation phase

The recipient generates the public key h by selecting four private keys $f \in L_f, g \in L_g$, and $\varphi \in L_\varphi$, such that f has an inverse f_q^{-1} and f_p^{-1} ($f_q^{-1} * f \equiv 1\ mod\ q$ and $f_p^{-1} * f \equiv 1\ mod\ p$), φ has an inverse $mod\ q$ denoted by φ_q^{-1} ($\varphi_q^{-1} * \varphi \equiv 1\ mod\ q$), and the following formulas:

$$h = f_q^{-1} * g * \varphi_q^{-1}\ (mod\ q)$$

The private key set is $\{f, g, \varphi\}$.

II. Encryption phase

At this phase, the sender encrypts the plaintext $m \in L_m$ and makes it ciphertext e by selecting two private ephemeral keys $r \in L_r$ and $\alpha \in L_\alpha$ and using the following formula:

$$e = p\,(h * r + \alpha) + m \ (mod\ q).$$

III. Decryption phase

After receiving the encrypted message, the recipient takes several steps to retrieve the plaintext m, as follows:

Compute:

$$\begin{aligned} a &= f * e\ (mod\ q\ ) \\ &= f * (p(h * r + \alpha) + m)\ (mod\ q) \\ &= pf * (h * r + \alpha) + f * m\ (mod\ q) \\ &= pf * (h * r) + pf * \alpha + f * m(mod\ q) \\ &= pf * \left(\left(f_q^{-1} * g * \varphi_q^{-1}\right) * r\right) + pf * \alpha + f * m(mod\ q) \\ &= pg * \varphi_q^{-1} * r + pf * \alpha + f * m\ (mod\ q) \end{aligned}$$

Take

$$\begin{aligned} b &= a * \varphi\ (mod\ q) \\ &= pg * r + pf * \alpha * \varphi + f * m * \varphi\ (mod\ q). \end{aligned}$$

The coefficient of the polynomial $pg * r + pf * \alpha * \varphi + f * m * \varphi\ (mod\ q)$ most lie in the interval $(-q/2\,, q/2]$.

According to suppositions, when reduce $pg * r + pf * \alpha * \varphi + f * m * \varphi\ (mod\ q)$ to $mod\ p$, the term $pg * r + pf * \alpha * \varphi$ vanishes and the term $f * m * \varphi\ (mod\ p)$ remains.

Assume, $s = f * m * \varphi\ (mod\ p)$

$$f_p^{-1} * s = m * \varphi\ (mod\ p)$$

$$f_p^{-1} * s * \varphi_p^{-1} \equiv m\ (mod\ p),$$

the coefficients within range $(-p/2\,, p/2]$ are then adjusted. Pseudocode (3.3) demonstrates decryption phase.

Table 2: Summarize of TTRU cryptosystem

Alice	Bob
Key generation	
Choose private $f \in L_f$ that invertible in K_q and K_p. Choose private $\varphi \in L_\varphi$ hat invertible in K_q and K_p. Choose private $g \in L_g$ that invertible in K_q and K_p. Compute f_q^{-1} inverse of f in K_q . Compute f_p^{-1} inverse of f in K_p . Compute φ_q^{-1} inverse of φ in K_q . Compute φ_p^{-1} inverse of φ in K_p Compute $h = f_q^{-1} * g * \varphi_q^{-1}(mod\ q)$. Send h to Bob	
Encryption	
	Choose the plaintext $m \in L_m$. Choose a random $r \in L_r$. Choose a random $\alpha \in L_\alpha$. Use the public keys h to compute $e = p(h * r + \alpha) + m(mod\ q)$. Send the ciphertext e to Alice.
Decryption	
Compute $a = f * e(mod\ q)$ $= f * (p(h * r + \alpha) * m)\ (mod\ q)$ Compute $b = a * \varphi\ (mod\ q)$ $b = a * \varphi\ (mod\ q)$ $= pg * r + pf * \alpha * \varphi + f * m * \varphi\ (mod\ q)$. $s = b\ (mod\ p)$ $m = f_p^{-1} * s * \varphi_p^{-1}(mod\ p)$.	

4. Performance Analysis of TTRU

4.1 Security of TTRU

TTRU security is based on the security of the key and the security of the message (ciphertext) through the private keys that make up the public keys h and the private keys on which the ciphertext e is based.

Assuming the space L_g shall be larger than the spaces L_f and L_φ, the security of key depends on the site of spaces L_f and L_φ of private key f and φ respectively, which are given as following:

$$|L_f| = \begin{pmatrix} N \\ d_f \end{pmatrix} \begin{pmatrix} N - d_f \\ d_f \end{pmatrix} = \frac{N!}{(d_f!)^2(N-2d_f)!},$$

and

$$|L_\varphi| = \begin{pmatrix} N \\ d_\varphi \end{pmatrix} \begin{pmatrix} N - d_\varphi \\ d_\varphi \end{pmatrix} = \frac{N!}{(d_\varphi!)^2(N-2d_\varphi)!},$$

Therefore, the space of key security is equal to

$$\frac{(N!)^2}{(d_f! d_\varphi!)^2(N-2d_f)!(N-2d_\varphi)!}.$$

Depending on the space L_r and L_α of the private keys r and α respectively, which are given as the following:

$$|L_r| = \begin{pmatrix} N \\ d_r \end{pmatrix} \begin{pmatrix} N - d_r \\ d_r \end{pmatrix} = \frac{N!}{(d_r!)^2(N-2d_r)!},$$

and

$$|L_\alpha| = \begin{pmatrix} N \\ d_\alpha \end{pmatrix} \begin{pmatrix} N - d_\alpha \\ d_\alpha \end{pmatrix} = \frac{N!}{(d_\alpha!)^2(N-2d_\alpha)!}.$$

Therefore, the space of message security is equal to:

$$\frac{(N!)^2}{(d_r! d_\alpha!)^2\,(N-2d_r)!(N-2d_\alpha)!}.$$

4.2 Execution Time of TTRU

The TTRU time depends on the number of mathematical operations (convolutional multiplication and polynomial addition) for the key generation,

encryption, and decryption phases. Table 2 shows the execution time of the TTRU encryption scheme.

Table 2: Execution time of TTRU

Phases	Mathematical operations
Key generation	Three convolution multiplications
Encryption	Two polynomial addition and one convolution multiplications
Decryption	Two polynomial addition and five convolution multiplications

Therefore, execution time is equal to $9t + 4t_1$ where t is number of multiplication times and t_1 is addition times.

5. Conclusion

TTRU is like NTRU public key cryptosystem depends on truncated polynomials ring. In terms of key security and message security, TTRU is more secure than NTRU. In terms of time, TTRU is a slower than NTRU, But this problem can be addressed by reducing the value of the degree of the polynomial. NTRU is a special case of TTRU in which the private keys is $\varphi = \alpha = 1$.

6. References

1. D. Coppersmith and A. Shamir, Lattice attacks on NTRU, Eurocrypt, p.p. 52-61, Springer-Verlag Berlin Heidelberg, 1997.
2. P. Gaborit, J. Ohler and P. Soli, CTRU, a polynomial Analogue of NTRU, INRIA. Rapport de recherche, no. 4621, 2002.
3. M. Coglianese and B. Goi, MaTRU: A new NTRU based cryptosystem, Springer Verlag Berlin Heidelberg, vol. 3797 p.p. 232-243, 2005.
4. P. R. Suri and p. puri, Application of LFSR with NTRU Algorithm. Innovative Algorithms and Techniques in Automation, Industrial Electronice and Telecommunications, Springer, pp.369-373. 2007.

5. E. Malecian, A. Zakerolhsooeini and A. Mashatan, QTRU: Quaternionic Version of the NTRU Public-Key Cryptosystems, The ISC Int'l Journal of Information Security, vol. 3, no. 1, pp. 29-42, 2011.
6. M. Nevins, C. KarimianPour and A. Miri, NTRU over rings beyond Z , Designs, Codes and Cryptography, vol.56, no.1, pp.65-78, 2010.
7. E. Malecian and A. Zakerolhosseini, OTRU: A non-associative and high speed public key cryptosystem, IEEE Computer Society, p.p. 83-90, 2010.
8. X. Lei and X. Liao, NTRU-KE: A Lattice-based Public Key Exchange Protocol, IACR Cryptology ePrint Archive, 718, 2013.
9. A. Majeed, CQTRU Cryptosystem based on commutative ring of quaternion, M.Sc. Thesis, University of Technology, Iraq, 2015.
10. H. R. Yassein and N. M. G. Al-Saidi, "HXDTRU Cryptosystem Based on Hexadecnion Algebra," in Proc. 6th International Cryptology and Information Security Conference, Sabah, Malaysia, pp. 1–10, 2016.
11. 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. S, pp. 29-43, 2017.
12. N. M. G. Al-Saidi and H. R. Yassein, BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra, International Journal of Advanced Computer Science and Applications, vol. 7, no. 11, pp. 1-6, 2016.
13. H. R. Yassein and N. M. G. Al-Saidi, BCTRU: A New Secure NTRUCrypt Public Key System Based on a Newly Multidimensional Algebra, in Proc. the 6th International Cryptology and Information Security Conference, Negeri Sembilan, Malaysia, pp. 1–11, 2018.
14. H. R. Yassein, N.M.G. Al-Saidi, An Innovative Bi-Cartesian Algebra for Designing of Highly Performed NTRU Like Cryptosystem, Malaysian Journal of Mathematical Sciences, vol.13, no. S, pp.77-91, 2019.
15. V. Lyubashevsky, G. Seiler, NTTRU: Truly Fast NTRU Using NTT, IACR Transactions on Cryptographic Hardware and Embedded Systems ISSN 2569-2925, No. 3, pp. 180-201, 2019.
16. 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 & Cryptography, vol. 23, no. 2, pp. 1-20, 2020.

17. H. R. Yassein, N.M.G. Al-Saidi and A. K. Almosawi, 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.
18. H. R. Yassein, A. A. Abidalzahra and N.M.G. Al-Saidi, "A new design of NTRU encryption with high security and performance level," AIP Conference Proceedings 2334,080005, 2021.
19. S. H. Shihadi, 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.
20. 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.
21. S. H. shahhadi and H. R. Yassein, NTRsh: A New Secure Variant of NTRUEncrypt Based on Tripternion Algebra," in Journal of physics conference series, University of Al-Qadisiyah, Diwaniyah, Iraq, pp. 2-6, 2021.
22. 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, University of Al-Qadisiyah, Diwaniyah, Iraq, pp. 2-7, 2021.
23. S. H. Shihadi, H.R. Yassein, An innovative tripternion algebra for designing NTRU-like cryptosystem with high security, AIP Conference Proceedings 2386, 060009, 2022.
24. H. H. Abo-alsood, H.R. Yassein, Analogue to NTRU public key cryptosystem by multi-dimensional algebra with high security, AIP Conference Proceedings 2386, 060006, 2022.
25. H. R. Yassein, H. N. Zaky, H. H. Abo-Alsoo, I. A. Mageed, W. I. El-Sobky, QuiTRU: Design Secure Variant of Ntruencrypt Via a New Multi-Dimensional Algebra, Appl. Math, vol. 17, no. 1, pp. 49-53, 2023.
26. H. R. Yassein, A. H. Reshan, N. M. G. Al-Saidi, AHQTR: A New NTRU Variant based on Quaternion Algebra, Proceeding of 8th International Cryptology and Information Security Conference, vol. 2022, pp. 100-108, 2023.