International Journal of Mathematics and
Computer Science, **16**(2021), no. 4, 1515–1522

A New Design of NTRUEncrypt-analog Cryptosystem with High Security and Performance Level via Tripternion Algebra

Sarah Hussain Shahhadi, Hassan Rashed Yassein

Department of Mathematics
College of Education
University of Al-Qadisiyah
Al Diwaniyah, Iraq

email: math.post05@qu.edu.iq, hassan.yaseen@qu.edu.iq

(Received March 12, 2021, Accepted May 6, 2021)

Abstract

With the progress and development of life, cryptography became an indispensable science. As its usefulness is not limited to changing the form of information and making it in the form of symbols that are difficult to understand (even if it reaches unauthorized persons) but through it becomes known that the information is original and coming from its source and has not been modified during the sending or saving process.
In this paper, we make an improvement and modification *NTRU* cryptosystem by using a new tripternion algebra and changing the mathematical structure for public and private keys, as well as for text encryption and decryption to obtain higher security.

1. Introduction

Encryption has been in use for thousands of years ago to protect confidential information. Historically, used in wars to prevent the enemy from obtaining secret messages, it has become nowadays an urgent necessity for other

Key words and phrases: NTRU, tripternion algebra, NTRS, security level.
AMS (MOS) Subject Classifications: 94A60.
ISSN 1814-0432, 2021, http://ijmcs.future-in-tech.net

purposes. This has led to the necessity of discovering encryption systems to preserve this information and ensure that it is not tampered with by pirates. In 1996, Hoffstein et al. constructed a public key cryptosystem $NTRU$ [1] based on the convolution polynomial ring of degree $N-1$, denoted by $Z[x]/(x^N-1)$. An overview of some of these studies is abstracted as follows. In 2002, drawing on the $F_2[x]/(x^N-1)$, Gaborit et al. [2] proposed an alternative of $NTRU$, called $CTRU$. In 2005, Kouzmenko [3], designed a system $GNTRU$ that depends on Gaussian integers. Also, by replacing the ring of polynomials with the ring of $k \times k$ matrices of polynomials, Coglianese and Goi introduced the $MaTRU$ cryptosystem [4]. In 2009, Nevins et al. [5] proposed a new variant, to $NTRU$ by replacing the original $NTRU$ ring with Einstein integers. Also, Malekian et al. [6] introduced a public key cryptosystem $QTRU$ depending on the Quaternion. $NTRU$ is less resistant to some attacks compared to $QTRU$. In 2010, Malekian et al. [7] proposed an alternative of $NTRU$, called $OTRU$, by replacing the original ring of $NTRU$ with Octonion Algebra. It encrypts eight data carriers per round and has a very secure, complex core. In 2016, Yassein and Al-Saidi [8, 9, 10] introduced $HXDTRU$ and $BITRU$ depending on the hexadecnion and binary algebras respectively. In 2019, they also introduced another multidimensional analog $NTRU$ called $BCTRU$ using bicartesian algebra [11, 12]. In 2020, Yassein et al. [13] introduced the QOB_{TRU} cryptosystem based on Carternion Algebra. In addition, Yassein et al. [14] introduced a new $NTRU$ alternative cryptosystem, called $NTRTE$, that depends on a commutative quaternion algebra with a new structure which is multi-dimensional. In this paper, we use Tripternion Algebra and make a change to the mathematical structure to design a new alternative cryptosystem, called $NTRS$.

2. NTRU Cryptosystem

$NTRU$ cryptosystem depends on a truncated polynomial ring of degree $N-1$, denoted by $K = Z[x]/(x^N-1)$, such that N is a prime number. The rings of truncated polynomial *mod* p, denoted by the symbol $K_p = Z_p[x]/(x^N-1)$ and the rings of truncated polynomial *mod* q, denoted by the symbol $K_q = Z_q[x]/(x^N-1)$, such that p, q are integers and gcd $(p,q)=1$, where p is smaller than q. The subset $L_f, L_g, L_r,$ and L_m is defined as follows:
$L_f = \{f \in K \ : f \text{ satisfies } \ell_{(d_f, d_f-1)}\}$
$L_g = \{g \in K \ : g \text{ satisfies } \ell_{(d_g, d_g)}\}$
$L_r = \{r \in K \ : r \text{ satisfies } \ell_{(d_r, d_r)}\}$

$L_m = \{m \in K$: coefficients of M are chosen mod p between $-p/2$ and $p/2\}$ where $\ell_{(d_x,d_y)}$=$\{f\epsilon\ K\backslash f$ has d_x coefficients equal 1, d_y coefficients equal -1, the remaining equal 0$\}$
The *NTRU* Cryptosystem passes the following stages:

Key Generation

We randomly choose two polynomials f and g from L_f and L_g such that f has an inverse concerning p *and* q. f_p^{-1} denotes the inverse of f concerning p and f_q^{-1}denotes the inverse of f concerning q. The public key is calculated by the law $h = f_q^{-1} * g\ (mod\ q)$, f and g are special keys that are known to the recipient only, while h is known to both the sender and the recipient.

Encryption

The message $m \in L_m$ is encrypted after selecting a random polynomial $r \in L_r$ and using the formula

$$e = ph * r + m\ (mod\ q).$$

Decryption

After receiving the encrypted text, the original text is obtained through steps:

$$f * e\,(mod\, q) = (pf * h * r + f * m)\,(mod\ q)$$

Take

$$\begin{aligned} B &= f * e\ (mod\ p) \\ &= f * m\ (mod\ p) \\ f_p^{-1} * B\ (mod\ p) &= m\ (mod\ p). \end{aligned}$$

3. Tripternion Algebra

In this section, we introduce a new multidimensional algebra over the field F which called Tripternion Algebra T as follows:
Let $T = \{a + bx + cx^2$ where $a, b, c\ \in F\}$, where $\{1, x, x^2\}$ forms the basis of this algebra. To define the operation on this algebra, assume that $A, B \in T$ such that
$A =\ a_0 + a_1x + a_2x^2$ and $B = b_0 + b_1x + b_2x^2$

The addition, multiplication of two tripternions, scalar multiplication, and inverse multiplication are defined by:
$A + B = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2$
$A * B = (a_0 b_0) + (a_1\ b_1)x + (a_2\ b_2)x^2$
$\beta A = \beta a_0 + \beta a_1 x + \beta a_2 x^2$, for any scalar β
$A^{-1} = \frac{1}{a_0} + \frac{1}{a_1}x + \frac{1}{a_2}x^2, a_0\ , a_1,\ a_2\ \neq 0,$
where the identity element in T is given by $1 + x + x^2$. It is clear that the tripternion algebra T is associative and commutative.

4. NTRS Cryptosystem

*NTR*S cryptosystem depends on generic parameters in $NTRU$ and the algebras A, A_p, A_q which defined as follows:

$$\begin{aligned} A &= \{a_0 + a_1 x + a_2 x^2 | a_0, a_1,\ a_2 \in K\}, \\ A_p &= \{a_0 + a_1 x + a_2 x^2 | a_0, a_1,\ a_2 \in K_p\}, \\ A_q &= \{a_0 + a_1 x + a_2 x^2 | a_0, a_1,\ a_2 \in K_q\}, \end{aligned}$$

The subsets $L_F, L_V, L_U, L_G, L_R, L_\theta$ and L_M are defined as follows:

$$\begin{aligned} L_F &= \{f_0 + f_1 x + f_2 x^2 \in A \text{ satisfies } \ell_{\left(d_f, d_f - 1\right)}\} \\ ies L_V &= \{v_0 + v_1 x + v_2 x^2 \in A \text{ satisfies } \ell_{(d_v, d_v)}\} \\ L_U &= \{u_0 + u_1 x + u_2 x^2 \in A \text{ satisfies } \ell_{(d_u, d_u - 1)}\} \\ L_G &= \{g_0 + g_1 x + g_2 x^2 \in A \text{ satisfies } \ell_{(d_g, d_g)}\} \\ L_R &= \{r_0 + r_1 x + r_2 x^2 \in A \text{ satisfies } \ell_{(d_r, d_r)}\} \\ L_\theta &= \{\theta_0 + \theta_1 x + \theta_2 x^2 \in A \text{ satisfies } \ell_{(d_\theta, d_\theta)}\} \end{aligned}$$

$L_M = \{m_0 + m_1 x + m_2 x^2$ |coefficients of m are chosen mod p between $-p/2$ and $p/2\}$, such that $d_f,\ d_v, d_u, d_g, d_r\ d_\theta$ and d_m are constant integers less than N, where $\ell(x,\ y)$=$\{f \epsilon\ K\ | f\ $ has d_x coefficients equal $1, d_y$ coefficients equal -1, the remaining equal $0\}$.

Key Generation

The public key and the private key are generated such that the receiver first randomly chooses four small polynomials (the number of nonzero coefficients is small) F, G, U, and V from $L_F, L_G, L_U,$ and L_V respectively such that

1. F must be invertible *mod* q, denoted by F_q^{-1}, such that $F * F_q^{-1} = 1$
2. U must be invertible *mod* p, denoted by U_p^{-1}, such that $U * U_p^{-1} = 1$.

The public keys H and K are computed in following manner

$$H = F_q^{-1} * V * G(mod\ q)$$

$$K = F_q^{-1} * U(mod\ q).$$

Encryption

The system initially selects a random polynomial $R \in L_R$ and $\theta \in L_\theta$, called the blinding polynomial, and converts the input message to a polynomial $M \in L_M$. The ciphertext is computed as follows:

$$E = p\,(H * R + \theta) + M * K\ \ (mod\ q)\,.$$

Decryption

For the purpose of obtaining the original message, the following steps should be followed:
After receiving the encrypted text, the original text is obtained through steps

$$\begin{aligned} F * E\,(mod\ q) &= F * (pH * R + p\theta + M * K)\,(mod\ q) \\ &= (pF * H * R + pF * \theta + F * M * K)\,(mod\ q) \\ &= \left(pF * F_q^{-1} * V * G * R + pF * \theta + F * M * F_q^{-1} * U\right)(mod\, q) \\ &= (pV * G * R + pF * \theta + M * U)(mod\ q). \end{aligned}$$

Take

$$\begin{aligned} B &= F * E\,(mod\ p) = (pV * G * R + pF * \theta + M * U)\ (mod\ p) \\ &= M * U\,(mod\ p)\,. \end{aligned}$$

Take,

$$\begin{aligned} Y &= B * U_p^{-1}(mod\ p) \\ &= M * U * U_p^{-1}(mod\ p) \\ &= M\,(mod\ p) \end{aligned}$$

5. Comparison between *NTRS* and *NTRU*

5.1 Mathematical Operation and Speed

The comparison of the mathematical operations (convolution multiplication and addition) of key generation, encryption and decryption between *NTRS* and *NTRU* are shown in Table 1.

TABLE 1: Mathematical operations of *NTRS* and *NTRU*.

	NTRS	*NTRU*
Key Generate	36 convolution multiplications	1 convolution multiplications
Encryption	18 convolution multiplications, 6 polynomial addition	1 convolution multiplications, 1 polynomial addition
Decryption	45 convolution multiplications , 6 polynomial addition	2 convolution multiplications, 1 polynomial addition

The speed of *NTRS* and *NTRU*. For addition, time is denoted by t and multiplication is t_1 are shown in Table 2. It is calculated as follows:

TABLE 2: Speed of *NTRS* and *NTRU*

	NTRS	*NTRU*
Speed	$12t + 99t_1$	$2t + 4t_1$

5.2 Level of Security

The key security level and the message security level in *NTRS* and *NTRU* are in accordance with the same general parameters and are shown in Table 3.

TABLE 3: Level of security comparison of key and message between *NTRS* and *NTRU*

	Key security	Message security
NTRS	$(\frac{N!}{(dg!)^2(N-2d_g)!})^3(\frac{N!}{(d_v!)^2(N-2d_v)!})^3$ $(\frac{N!}{(d_u!)^2(N-2d_u)!})^3$	$(\frac{N!}{(d_r!)^2(N-2d_r)!})^3$ $(\frac{N!}{(d_\theta!)^2(N-2d_\theta)!})^3$
NTRU	$(\frac{N!}{(dg!)^2(N-2d_g)!})$	$(\frac{N!}{(d_r!)^2(N-2d_r)!})$

6. Conclusion

NTRS is a multidimensional public key cryptosystem via tripternion algebra guarantees high security against attacks, as brute force and good efficiency. Even though its speed is less than *NTRU*, it reduces the value of N while maintaining a high level of security. With these characteristics, *NTRS* is suitable for many applications that require more than one data source and even one source as electronic voting.

References

[1] J. Hoffstein, J. Pipher, J. Silverman, NTRU: A ring based public key cryptosystem, Proceeding of ANTS III, LNCS, Springer-Verlag, **1423,** (1998) 267–288

[2] P. Gaborit, J. Ohler, P. Soli, CTRU, a polynomial analogue of NTRU, INRIA. Rapport de recherche, No. 4621, 2002.

[3] R. Kouzmenko, Generalizations of the NTRU cryptosystem, M.Sc., Montreal, Canada, 2006.

[4] M. Coglianese, B. Goi, MaTRU: A new NTRU based cryptosystem, Springer-Verlag, Berlin, Heidelberg, (2005) 232–243.

[5] M. Nevins, C. Karimian Pour, A. Miri, NTRU over rings beyond Z, Designs, Codes and Cryptography, **56,** (2009), 65–78

[6] E. Malecian, A. Zakerolhsooeini, A. Mashatan, QTRU: a lattice attack resistant version of NTRU PCKS based on quaternion algebra, ISC Int. Journal of Information Security, **3,** no. 1 (2011) 29–42.

[7] E. Malecian, A. Zakerolhsooeini, OTRU: A non-associative and high speed public key cryptosystem, IEEE Computer Society, **16,** (2010), 83–90.

[8] H. R. Yassein, N. M. G. Al-Saidi, HXDTRU Cryptosystem Based on Hexadecnion Algebra, Cryptology Conference, 2016.

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

[10] N. M. G. Al-Saidi, H. R. Yassein, BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra, International Journal of Advanced Computer Science and Applications, **7,** no. 11, (2016), 1–6.

[11] H. R. Yassein, N. M. G. Al-Saidi, BCTRU: A New Secure NTRU Crypt Public Key System Based on a Newly Multidimensional Algebra, The 6th International Cryptology and Information Security Conference, 2018.

[12] 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, **13,** no. S,(2019), 77–91.

[13] H. R. Yassein, N. M. G. Al-Saidi, 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, **23,** no. 2 , (2020) 1–20.

[14] H. R. Yassein, N. M. G. Al-Saidi, A. K. Almosawi, A multi-dimensional algebra for designing an improved NTRU cryptosystem, Eurasian Journal of Mathematical and Computer Applications, **8,** no. 4, (2020), 97–107.